This document will act as a guide for establishing communication with a HomeWorks 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 ................................................. 2
2.0 Network and IT Considerations ............................................. 3
3.0 Communication Port Diagram ............................................... 5
   3.1 Firewall/Routing Requirements ......................................... 6
4.0 Connecting to the HomeWorks QSX Processors ............................ 8
   4.1 Network Hops with HomeWorks QSX Processors ....................... 11
5.0 Best Practices ................................................................... 12
   5.1 Firewalls and Security Programs .......................................... 12
      5.1.1 Check Inbound Firewall Rules ..................................... 12
      5.1.2 Allow Lutron Programs Through the Firewall ................. 16
      5.1.3 Using a Work or Home Network Connection to the System .. 18
      5.1.4 Changing to TCP Communication in HomeWorks QSX ........ 19
      5.1.5 Disable Firewall Temporarily ..................................... 19
   5.2 Using Wi-Fi with Lutron Programming Software ....................... 21
   5.3 Running Windows OS on Mac ............................................. 22
      5.3.1 Parallels and VMware Fusion ...................................... 22
   5.4 Multiple Network Adapters ............................................... 25
   5.5 VPN Connections ............................................................ 26
   5.6 Internet Group Management Protocol (IGMP) ......................... 27
      5.6.1 How do switches route multicast traffic? ....................... 27
      5.6.2 What is IGMP Snooping? ........................................... 27
      5.6.3 IGMP Snooping and Lutron Residential Systems .............. 27
      5.6.4 Appendix- HWQSX System on Network with Snooping Disabled ... 28
      5.6.5 Appendix- HWQSX System on Network with Snooping Enabled ... 29
   5.7 Setting Static IP Addresses ................................................. 30
      5.7.1 General Static IP Best Practice ................................... 30
      5.7.2 DHCP Reservation vs Setting Static IP in the Programming Software .... 30
      5.7.3 Setting a Static IP Address ........................................ 31
6.0 Troubleshooting ................................................................ 33
   6.1 HomeWorks QSX Activate Processors Error Codes ................... 33
   6.2 Using a Direct Connection to a Lutron Processor .................... 35
      6.2.1 Direct Connection using Static IP Address ...................... 36
      6.2.2 Direct Connection using Link Local Addressing ............... 36
6.7 Frequently Asked Questions .................................................. 37
1.0 Glossary and Abbreviations

**Clear Connect Gateway–Type X** – The HQP7-RF processor. Communicates with compatible Lutron devices in the 2.4 GHz RF band. Each Clear Connect Gateway–Type X has one RJ45 female connector.

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

**Lutron Connect App** – Phone-based user interface (UI) to monitor and control HomeWorks.

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

**HomeWorks Processor** – The HQP7-2 processor. This is the basic HomeWorks QSX controller and will be the main HomeWorks component connected to any network. Each HomeWorks QSX processor has two RJ45 female connectors, one for the HomeWorks QSX LAN/VLAN connection and the other for serviceability.

**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.

**Internet Group Management Protocol (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.

**Master Processor** – Processor #1 in the system. This processor takes on the role of synchronizing timeclocks in the system.

**Multicast Domain Name Service (mDNS)** – Ethernet multicast protocol used for HomeWorks processor discovery.

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

**Protocol Independent Multicast (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.

**Power over Ethernet** – Abbreviation is “PoE”. An Ethernet connection which supplies power to the connected device in addition to standard data transmission.

**Processor**– Can refer to a HomeWorks QSX processor or Clear Connect Gateway – Type X.

**Unicast** – A communication method over Ethernet TCP or point-to-point communication.
2.0 Network and IT Considerations

Network Architecture Overview

What is on the traditional network IP architecture? – The HomeWorks processors, 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.

RF Considerations

While RF occupancy sensors, daylight sensors, and Pico controls operate on a frequency outside of Wi-Fi, the HomeWorks Clear Connect Gateway–Type X, Ketra fixtures and lamps operate on 2.4 GHz. Please see App Note (P/N 048745) at www.lutron.com for Wi-Fi channel coordination and recommendations for more information.

The Clear Connect Gateway–Type X requires at least one HomeWorks QSX processor. A maximum of 16 total combined gateways and wired processors can be on one system.

Physical Medium

IEEE 802.3 Ethernet – The physical medium standard for the network between HomeWorks. Each HomeWorks processor has female RJ45 connectors for LAN connection.

CAT5e – The minimum network wire specification of the HomeWorks LAN/VLAN.

PoE – Required for each Clear Connect Gateway–Type X. Must be powered by an IEEE 802.3af-2003 or 802.3at-2009 compliant Power over Ethernet (PoE), supply, Lutron model Q-POE-PNL, or by others.

IP Addressing

IPv4 – The addressing scheme used for the HomeWorks QSX system. 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 System – A multicast group of HomeWorks processors sharing a unique and common class D address that need to share events. Maximum 16 HomeWorks QSX processors on a HomeWorks QSX system. Minimum one HomeWorks QSX processor on a HomeWorks QSX system.

Multicast communications – Basic communication to share events between HomeWorks processors 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.

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)

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.

* Note: Telnet is not a supported method of integration to a HomeWorks QSX system starting at HomeWorks version 16.0.

Internet Access

- **Internet connectivity**
  - The processor will ping public DNS servers to verify Internet connectivity:
    - 8.8.4.4, 8.8.8.8, 208.67.220.220, 208.67.222.222, 209.244.0.3, 209.244.0.4
  - The processor will also attempt to make an HTTP connection to www.google.com
- **Time synchronization**
  - Processors will reach out to local time servers on the internet, in order to allow for accurate execution of timeclock and other scheduled events.
- **Automatic firmware updates (If Enabled)**
  - If enabled, the processor may attempt automatic firmware upgrades by accessing an HTTPS site at firmwareupdates.lutron.com which may resolve to one or more other hostnames.
- **Mobile app connectivity**
  - Mobile app connectivity can be used either locally on the same subnet as the processor, or if on a different subnet cloud services are used for control of lights on the processor.
  - Device-login.lutron.com & Lutron.broker.xively.com are used for cloud connectivity.
3.0 Communication Port Diagram

TCP 443
Allows the Lutron software to obtain the latest processor firmware

Internet

TCP 1900, TCP 5353, TCP 7782, TCP 8081, TCP 8083, TCP 8085

Third Party Control System
Integrate directly to the processor

The processor initiates all communication to the Internet. No port is formally required to be opened on the router:
UDP 53, TCP 80, UDP 123, TCP 443, TCP 7446, TCP 8083, TCP 8081, TCP 8090

Commissioning Machine

HomeWorks QSX Designer
Editing UI Application

Microsoft SQL Server

TCP 51023
(Optional) Eliminates the need for the commissioning machine to talk Any-Source Multicast to the processors

Lutron Processors

There can be a maximum of 16 HomeWorks QSX processors per system

Mobile App

For local connections. Remote connections go through an established processor connection to the Internet

TCP 22, UDP 2056, UDP 5353, TCP 8081, TCP 8083

Lutron Processors

There can be a maximum of 16 HomeWorks QSX processors per system

When a system contains multiple processors, the processors will always communicate with each other using Any-Source Multicast UDP 2056
3.1 Firewall/Routing Requirements

Required for system startup and programming

These ports are used for system startup and database transfer to processors and gateways. After the system has been started up, these ports may be closed if desired. If changes to the system are needing to be made, these ports will need to be re-opened to allow upload of programming changes to the system.

<table>
<thead>
<tr>
<th>Source</th>
<th>Source Application</th>
<th>Destination</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commissioning PC IP</td>
<td>HomeWorks Software</td>
<td>224.0.0.251</td>
<td>5353</td>
<td>UDP</td>
<td>mDNS is utilized for processor discovery and initial configuration</td>
</tr>
<tr>
<td>Processor IP</td>
<td>mDNS Response</td>
<td>224.0.0.251</td>
<td>5353</td>
<td>UDP</td>
<td>mDNS is utilized for processor discovery and initial configuration</td>
</tr>
<tr>
<td>Commissioning PC IP</td>
<td>HomeWorks Software</td>
<td>IP Address of All HomeWorks Processors</td>
<td>8083</td>
<td>TCP</td>
<td>These ports are used to configure processors.</td>
</tr>
<tr>
<td>Commissioning PC IP</td>
<td>HomeWorks Software</td>
<td>IP Address of All HomeWorks Processors</td>
<td>22</td>
<td>TCP</td>
<td>Used for database transfer, support file generation and diagnostics</td>
</tr>
<tr>
<td>Commissioning PC IP</td>
<td>HomeWorks Software</td>
<td>sqitofb.lutron.com Firmwareupdates.lutron.com</td>
<td>443</td>
<td>TCP</td>
<td>Allows Lutron Software to obtain the latest processor firmware</td>
</tr>
</tbody>
</table>

Required for system runtime

These ports are required for system runtime and must remain open for system functionality.

<table>
<thead>
<tr>
<th>Source</th>
<th>Source Application</th>
<th>Destination</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor and Gateway IPs</td>
<td>Inter-Processor Communication</td>
<td>Multicast Address of Subsystem (239.0.38.1 – 239.0.38.xx)</td>
<td>2056</td>
<td>UDP</td>
<td>Used to share events and status of lights between processors</td>
</tr>
<tr>
<td>Commissioning PC IP</td>
<td>HomeWorks Software</td>
<td>All HomeWorks QSX Processor IPs</td>
<td>51023</td>
<td>TCP</td>
<td>Optional Unicast communication between HomeWorks QSX software and processors</td>
</tr>
</tbody>
</table>

Optional features and functions

<table>
<thead>
<tr>
<th>Source</th>
<th>Source Application</th>
<th>Destination</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Control System IP</td>
<td>TLS</td>
<td>IP Address of HomeWorks QSX Processor</td>
<td>8085 8081 8083</td>
<td>TCP IPv4</td>
<td>For third-party external integration with a processor</td>
</tr>
</tbody>
</table>
## 3.1 Firewall / Routing Requirements (continued)

**Mobile App, Internet and Cloud Connectivity Features**

These ports are used for various cloud and Internet connectivity functions.

<table>
<thead>
<tr>
<th>Source</th>
<th>Source Application</th>
<th>Destination</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Device on Local Processor Network</td>
<td>Mobile App</td>
<td>224.0.0.251</td>
<td>5353</td>
<td>UDP IPv4 Multicast</td>
<td>mDNS is utilized for processor discovery</td>
</tr>
<tr>
<td>Mobile Device on Local Processor Network</td>
<td>Mobile App</td>
<td>Processor IP</td>
<td>8081, 8083</td>
<td>TCP IPv4</td>
<td>Lutron App authentication, configuration and local connection on same network</td>
</tr>
<tr>
<td>Mobile App</td>
<td>Mobile App</td>
<td>Processor IP</td>
<td>22</td>
<td>TCP IPv4</td>
<td>SSH is used for support file generation and diagnostics</td>
</tr>
<tr>
<td>Processor IP</td>
<td>Cloud Connectivity</td>
<td>lutron.broker.xlvely</td>
<td>8883</td>
<td>TCP IPv4</td>
<td>Lutron Cloud connectivity for mobile app runtime on network other than processor network.</td>
</tr>
<tr>
<td>Processor IP</td>
<td>Cloud Connectivity</td>
<td>device-login.lutron</td>
<td>443</td>
<td>TCP IPv4</td>
<td>Device Registration and secure processor remote access</td>
</tr>
<tr>
<td>Processor IP</td>
<td>Internet Connectivity Check</td>
<td>8.8.4.4, 208.67.220.220, 209.244.0.3, 209.244.0.4, 8.8.8.8, 208.67.222.222</td>
<td>ICMP</td>
<td>ICMP</td>
<td>Processor internet connectivity check</td>
</tr>
<tr>
<td>Processor IP</td>
<td>Internet Connectivity Check</td>
<td>Google</td>
<td>80</td>
<td>TCP IPv4</td>
<td>Processor internet connectivity check</td>
</tr>
<tr>
<td>Processor IP</td>
<td>DNS</td>
<td>Customer Specified DNS Server</td>
<td>53</td>
<td>UDP IPv4</td>
<td>DNS resolution is required for cloud connectivity and NTP Time Sync</td>
</tr>
<tr>
<td>Processor IP</td>
<td>NTP</td>
<td>NTP</td>
<td>123</td>
<td>UDP IPv4</td>
<td>NTP is used for automatic time sync which allows time-based events to trigger accurately</td>
</tr>
</tbody>
</table>
4.0 Connecting to HomeWorks QSX Processors

Requirements
1. Windows machine running HomeWorks Designer software version 16.0 or later
2. HomeWorks QSX processor(s)
3. Wired/Wi-Fi router or network switch to place the processors and PC onto the same network
4. Power over Ethernet supply if a Clear Connect Gateway – Type X is present

During system commissioning, the HomeWorks Designer 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.

HomeWorks 16.0+ works with HQP7-x processors and gateways. There is no compatibility with HQP6 processors.

Figure 1: PC to Processor(s): Wired or Wi-Fi Connection (Never Ethernet and Wi-Fi at the same time)

![Diagram of PC to Processor(s): Wired or Wi-Fi Connection](image)

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 4.1 for more information on Ethernet hopping of multiple processors from a single switch/router port.

Figure 2: PC to Processor(s): Wired or Wi-Fi Connection w/ Daisy-Chaining (Never Ethernet and Wi-Fi at the same time)

![Diagram of PC to Processor(s): Wired or Wi-Fi Connection w/ Daisy-Chaining](image)

Note: Processors will not pass PoE through daisy-chaining. If a wireless processor is at the end of a daisy chain, the wireless processor must be preceded by a PoE injector supplying power to it.
4.0 Connecting to HomeWorks QSX Processors (continued)

Connect the commissioning machine to the same LAN as the processor(s) and open the HomeWorks Designer 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.
4.0 Connecting to HomeWorks QSX 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 integration or app control
    - **Option 2:** Set to DHCP Enabled when a DHCP Reserved address is set on the DHCP server of the router for the HomeWorks 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 system with a control system or using a Lutron mobile application for control
    - 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 address
- **IP Address:** 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 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
  - Each 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. Mobile app access will not be impacted by this setting.
- **System Communications:** Changes how the software on the commissioning machine communicates with the processors in the system
  - **Use Multicast Address:** The software will communicate to the processors 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 only changes software-to-processor communication to TCP. Inter-processor communication will remain multicast
    - This option is only available when DHCP is disabled
4.0 Connecting to HomeWorks QSX 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 (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.

After completing configuration of all 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.

4.1 Network Hops with HomeWorks QSX Processors

For optimal system performance, no more than five Ethernet hops should exist between any two processors or any processor and the PC in the HomeWorks 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 one Ethernet hop between processor 1 and processor 2, but there are four Ethernet hops between processor 2 and processor 3.
5.0 Best Practices

5.1 Firewalls and Security Programs

Often 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.

5.1.1 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 observed that firewall rules can still block Lutron software and cause it to not 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.
5.0 Best Practices (continued)

5.1 Firewalls and Security Programs (continued)
5.1.1 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. HomeWorks Designer software rules are listed with the name “Lutron Designer”. For the version of software that is having trouble communicating, go to the Lutron Designer rows and find and expand the column names Program to reveal the version number of software to which the rules correspond.

Check the following firewall rule settings for the version of software which is having problems:

- 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.
5.0 Best Practices (continued)
5.1 Firewalls and Security Programs (continued)
5.1.1 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.
5.0 Best Practices (continued)
5.1 Firewalls and Security Programs (continued)
5.1.2 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 and Advanced Security.

In the pane on the left, click Inbound Rules.

All the inbound firewall rules are listed here. HomeWorks software rules are listed with the name "Lutron Designer". For the version of software that is having trouble communicating, go to the Lutron Designer rows and find and expand the column named Program to reveal the version number of software to which the rules correspond.
5.0 Best Practices (continued)
5.1 Firewalls and Security Programs (continued)
5.1.2 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 >.
5.0 Best Practices (continued)
5.1 Firewalls and Security Programs (continued)
5.1.2 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 >.

Select the file path:
"C:\Program Files (x86)\Lutron\HomeWorks QSX <version number>\Lutron.Gulliver.QuantumRest.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 rules. Then click Finish.

• Use "Lutron Designer" when naming a HomeWorks QSX rule.
5.0 Best Practices (continued)
5.1 Firewalls and Security Programs (continued)
5.1.3 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.
5.0 Best Practices (continued)
5.1 Firewalls and Security Programs (continued)
5.1.3 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.

5.1.4 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 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.

5.1.4.1 Changing to TCP Communication in HomeWorks

In order to force the HomeWorks QSX 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.

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.
5.0 Best Practices (continued)

5.1 Firewalls and Security Programs (continued)

5.1.5 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 intended 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.
5.0 Best Practices (continued)
5.2 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 products of information to go from your laptop, through the network and to the processor.

The HomeWorks Designer software uses User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) for communication over Ethernet to the HomeWorks processor. TCP is a reliable means of communication between network devices involving several 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.

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.
5.0 Best Practices (continued)

5.3 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 as either 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.

5.3.1 Parallels and VMware Fusion

Parallels and VMware Fusion software 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 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.
5.0 Best Practices (continued)
5.3 Running Windows OS on Mac (continued)
5.3.1 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.
5.0 Best Practices (continued)
5.3 Running Windows OS on Mac (continued)
5.3.1 Parallels and VMware Fusion (continued)

In the Network setting 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.

In the Network setting 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 to 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 task 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 the 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 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).
5.0 Best Practices (continued)
5.4 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 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.
5.0 Best Practices (continued)

5.5 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 system over a local network. When trying to communicate with the Lutron system, it will be prudent to disconnect from the VPN connection. The image below shows the Disconnect option for the Cisco AnyConnect VPN connection.

![Disconnect option for Cisco AnyConnect VPN](image)

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.

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
5.0 Best Practices (continued)

5.6 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 processor supports 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 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.

5.6.1 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 member 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 may cause an intermittent loop where traffic is repeated unnecessarily.

IGMP Snooping allows network switches to handle multicast network traffic correctly.

5.6.2 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.

5.6.3 IGMP Snooping and Lutron Residential Systems?

The HomeWorks systems relies heavily on multicast traffic to cut back on total network traffic and provide a 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 system is connected to a switch with IGMP Snooping enabled, no multicast traffic generated by the HomeWorks processors will ever enter the rest of the network. By the same token the HomeWorks 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 from it should not 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.
5.0 Best Practices (continued)
5.6 Internet Group Management Protocol (IGMP) (continued)

5.6.4 Appendix – HomeWorks System on Network with Snooping Disabled
5.0 Best Practices (continued)
5.6 Internet Group Management Protocol (IGMP) (continued)
5.6.5 Appendix – HomeWorks System on Network with Snooping Enabled
5.0 Best Practices (continued)

5.7 Setting Static IP Addresses

5.7.1 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 letter. If the address of the home randomly changed after an electrical brown out, the Postal Service would be confused and would likely deliver the letter to the incorrect house. The latter scenario is similar to network devices configured as DHCP, where the network device requests an 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 occurs.

1. All addresses must be unique so be sure to map out 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 is typically printed on a label that is on the router).

5.7.2 DHCP Reservation vs. Setting Static IP in the Programming Software

There are two different ways to set a static IP address on HomeWorks 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 table below illustrates this.

<table>
<thead>
<tr>
<th></th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programming Software</td>
<td>– Easy to do, using the same screen used to discover and activate the Lutron processor</td>
<td>– Cannot easily change the address without having the programming software</td>
</tr>
<tr>
<td>DHCP Reservation</td>
<td>– Easy for network management since Lutron processors will be handed the same way as all other network devices</td>
<td>– Router could get replaced with little warning and all addressing lost – Requires additional coordination with the party responsible for the networking equipment on the site.</td>
</tr>
</tbody>
</table>
5.0 Best Practices (continued)
5.7 Setting Static IP Addresses (continued)
5.7.3 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.
5.0 Best Practices (continued)
5.7 Setting Static IP Addresses (continued)
5.7.3 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.
## 6.0 Troubleshooting

### 6.1 HomeWorks Activate Processors Error Codes

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

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Remedy</th>
</tr>
</thead>
</table>
| 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.  
2. Verify that the processors are activated using Activate > Processors.          |
| Communication to one or more processors failed.                              | 1. Check that the processor(s) are powered and connected to the network.  
2. Allow exception for the software through the firewall or turn off firewall.  
   See Section 5.1.2/5.1.5.  
3. Turn off any active VPN connections. See Section 5.5.  
4. If using a wired LAN connection, disconnect from any Wi-Fi networks.  
   Vice versa for when using Wi-Fi. See Section 5.4.  
5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1.  
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.  
2. Allow exception for the software through the firewall or turn off firewall.  
   See Section 5.1.2/5.1.5.  
3. Turn off any active VPN connections. See Section 5.5.  
4. If using a wired LAN connection, disconnect from any Wi-Fi networks.  
   Vice versa for when using Wi-Fi. See Section 5.4.  
5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1.  
6. Re-try Activate > Processors                                                  |
| Communications to one or more processors failed. Would you like to continue the OS upgrade? This may cause the system to behave in an unexpected manner. | 1. Check that the processor(s) are powered and connected to the network.  
2. Allow exception for the software through the firewall or turn off firewall.  
   See Section 5.1.2/5.1.5.  
3. Turn off any active VPN connections. See Section 5.5.  
4. If using a wired LAN connection, disconnect from any Wi-Fi networks.  
   Vice versa for when using Wi-Fi. See Section 5.4.  
5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1.  
6. Re-try Activate > Processors                                                  |
| Transfer cannot complete because there are no components to transfer.         | Nothing is activated to the system; activate devices.                                                                                   |
6.0 Troubleshooting *(continued)*

6.1 HomeWorks Activate Processors Error Codes *(continued)*

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Remedy</th>
</tr>
</thead>
</table>
| 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. 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.  
2. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2 / 5.1.5.  
3. Turn off any active VPN connections. See Section 5.5.  
4. If using a wired LAN connection, disconnect from any Wi-Fi networks. Vice versa for when using Wi-Fi. See Section 5.4.  
5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1.  
6. Re-try Activate > Processors |
| Status while activating a processor shows "Subnet Conflict". | Some other device on the network is using the same IP address; change the processor IP address of 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.  
2. Allow exception for the software through the firewall or turn off firewall. See Section 5.1.2 / 5.1.5.  
3. Turn off any active VPN connections. See Section 5.5.  
4. If using a wired LAN connection, disconnect from any Wi-Fi networks. Vice versa for when using Wi-Fi. See Section 5.4.  
5. For Macs running Parallels or VM, ensure that you are using a Bridged network connection. See Section 5.3.1.  
6. Re-try Activate > Processors |
6.0 Troubleshooting (continued)

6.2 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. A direct connection is not valid for connecting to Clear Connect Gateway–Type X.

Figure 3: PC to HomeWorks QSX Processor: Direct Connection

Figure 4: PC to Multiple HomeWorks QSX Processors: Direct Connection
6.0 Troubleshooting (continued)

6.2 Using a Direct Connection to a Lutron Processor (continued)

6.2.1 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 HomeWorks Designer software is setup with a static IP address, open the programming software and open the database for the residence.

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

6.2.2 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 6.2. 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 HomeWorks Designer software and attempt to locate the processors using Activate > Processors.
7.0 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 uniquely 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 four "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 network 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 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 2 minutes. Link Local IP addresses all begin with 169.254.x.x.

*Example:*
Local Link IP address: 169.254.1.123

*Can I mix a DHCP network with a static IP address?*
Yes, however careful planning must be given to the static IP addresses. The static IP addresses cannot be the same as the DHCP hosts 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 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.
7.0 Frequently Asked Questions (continued)

**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 four “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 four 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 QSX.

**What is a Wide Area Network?**
A wide area network is a 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

**What is Power over Ethernet?**
Power over Ethernet (PoE) is a way to power devices over Ethernet on a network which are compatible with PoE. Both power and data are transmitted along the wire. The Clear Connect Gateway–Type X is the only Lutron device which is compatible with PoE. The Gateway must be powered by an IEEE 802.3af.2003 or 802.3at.2009 compliant Power over Ethernet (PoE), supply, Lutron model Q-POE-PNL, or by others.

**Can a HQP7-2 processor be connected to Power over Ethernet?**
A PoE port on a PoE switch will not supply power to the HQP7-2 processor. Data transmission will still work.
7.0 Frequently Asked Questions (continued)

What is 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.

What 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 to work?
As Lutron systems, such as HomeWorks, 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, HomeWorks, and Clear Connect are trademarks or registered trademarks of Lutron Electronics Co., Inc. in the US and/or other countries.
Mac and macOS are trademarks of Apple Inc., registered in the U.S. and other countries.
All other product names, logos, and brands are property of their respective owners.

**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