Networking Best Practices

1.0 Overview

This document will act as a guide for establishing this communication and will describe various ways to overcome the network and computer challenges that you may encounter. For more information on networking concepts and the various ways to connect to a Lutron system processor via the network, refer to the Networking Guide for the Residential System used in the application.

- The RadioRA 2 Networking Guide can be found under *Service & Support/Application Notes* on the RadioRA 2 Resource Site (www.lutron.com).
- The HomeWorks QS Networking Guide can be found under *Technical Documentation/HWQS/HWQS App Notes/FAQs* on the HomeWorks QS Resource Site (resi.lutron.com).

Table of Contents

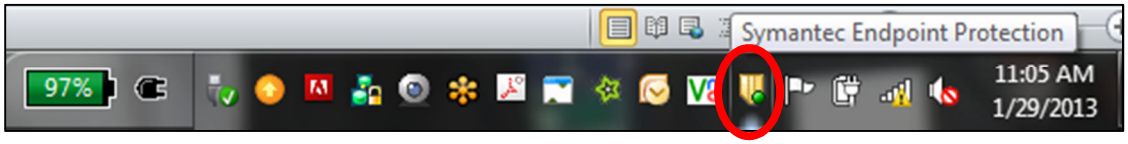
2.0 Firewalls and Security Programs

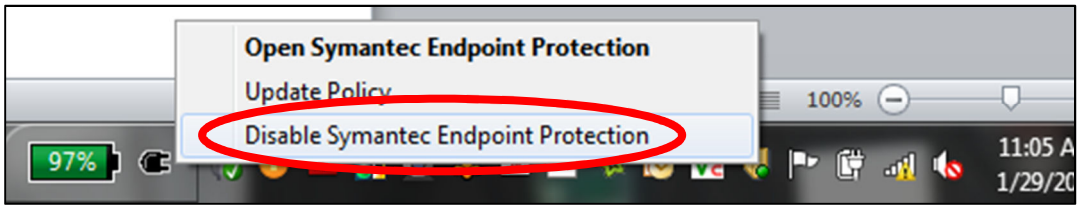
Often times the difficulty of establishing communication between the PC and the processor(s) has to do with a program or programs that are restricting the Lutron Programming Software from sending the necessary communications to the processor. The PC is using these software features to protect itself 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.

2.1 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.





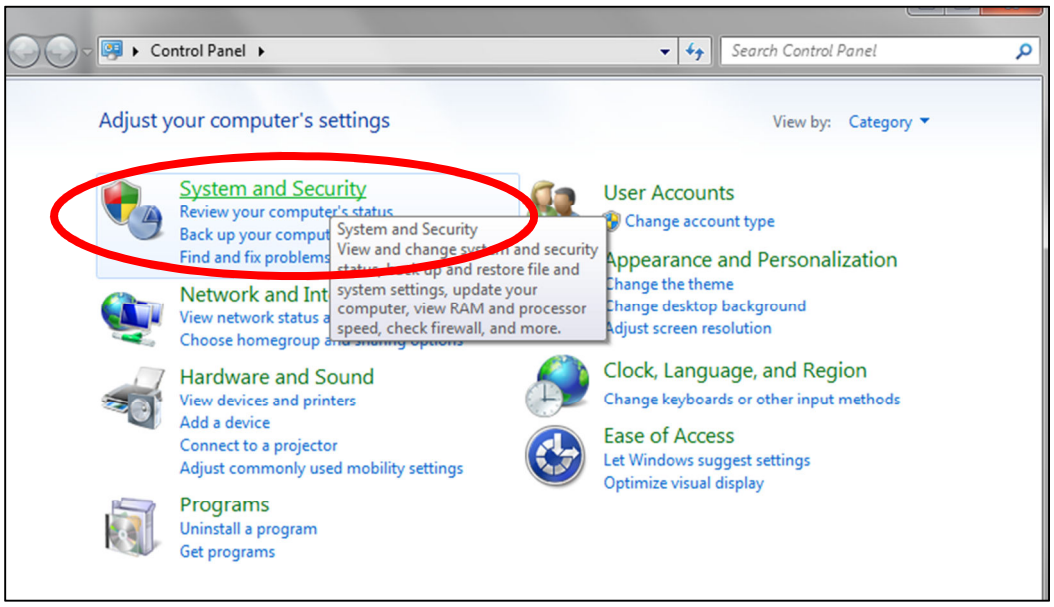
In this case, the security program manages the Windows Firewall so disabling the security program subsequently disables the Windows Firewall. If there is no separate security program, or if the security program is not directly linked to the PC firewall, it may be necessary to disable the firewall or, at the very least, allow the Lutron Programming Software through the firewall (see **Section 2.2**).

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.

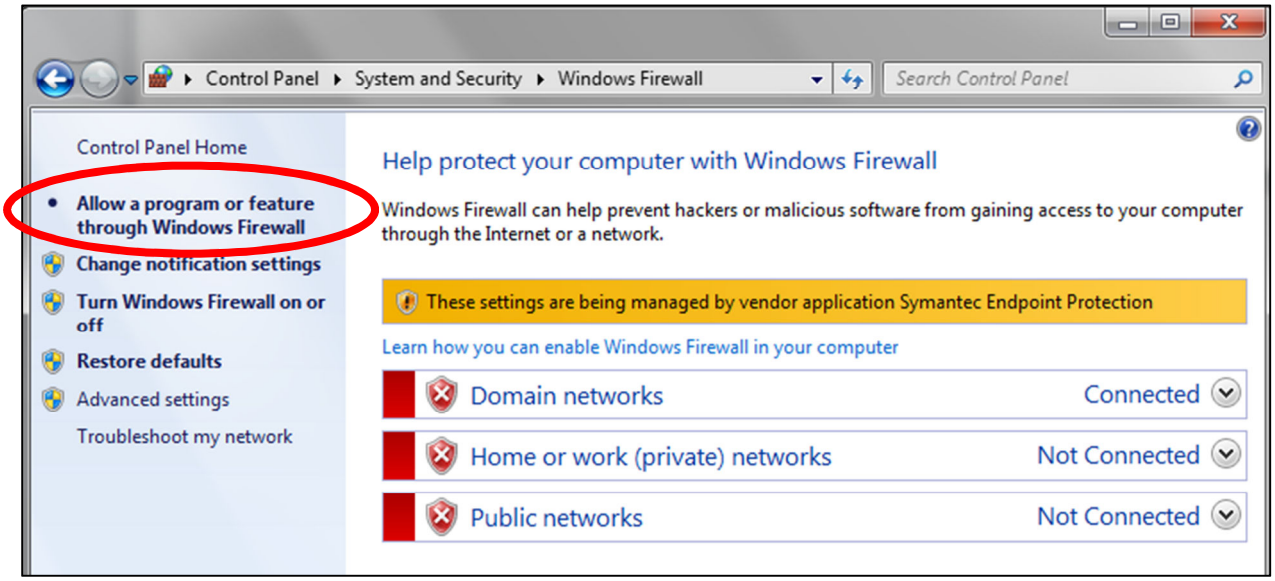
2.2 Allow Lutron Programs through the Firewall

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 7, after proceeding to the Control Panel from the Start Menu. In Windows 7, go to the System and Security section of the control panel to access the Windows Firewall settings.

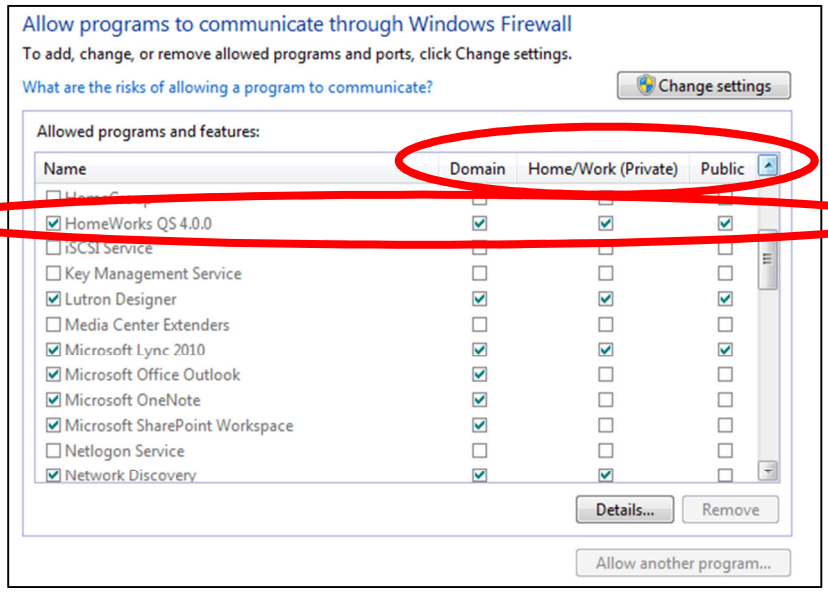


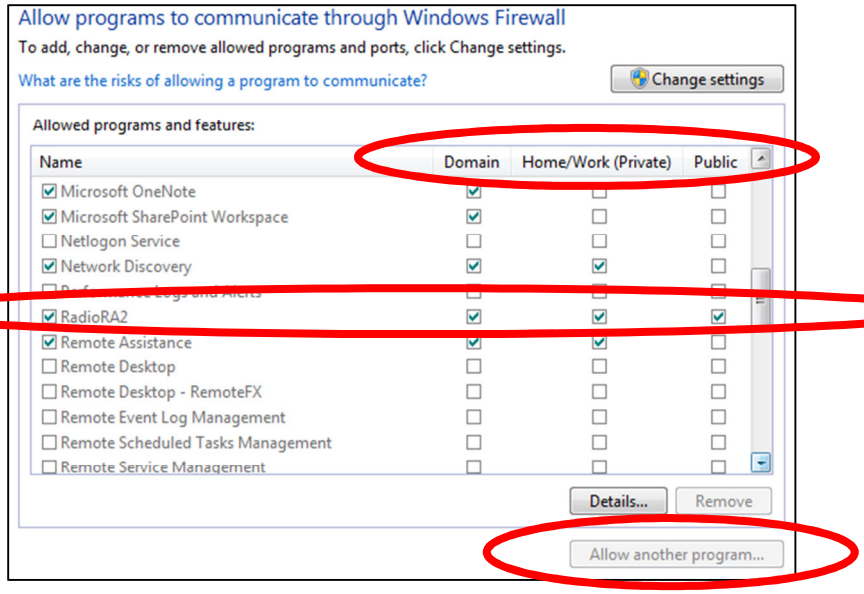
Here you can check on the Windows Firewall status or allow programs through the Windows Firewall.

Viewing the Windows Firewall status, the option to Turn Windows Firewall on or off is available. Use the link on the left of the window to navigate to these controls. In the case of Symantec, it manages the Windows Firewall. If this is not the case, you will be able to turn the firewall on or off from this window. Remember that turning these features off should only be used for a fast and temporary solution to a connection issue.



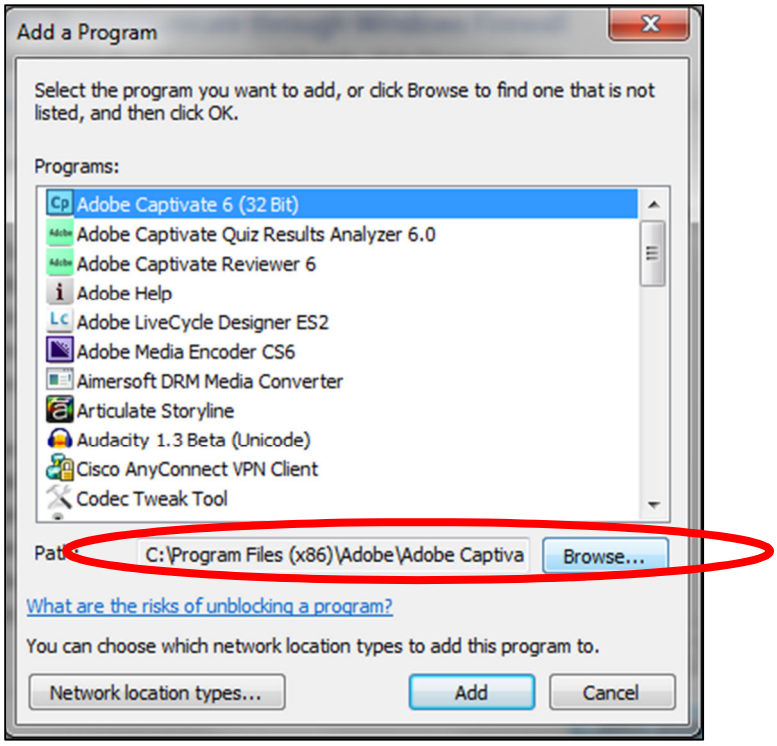
To allow the Lutron Software through the Windows Firewall, simply locate the name of the programming software on the list of Allowed Programs and Features. Once you find it, ensure that the check boxes for all network types are checked.





If you do not see the Lutron program on the list, click on *Allow another program*. This will open another window with a list of programs. If the program is not on this new list, browse the C:\ directory for the Lutron programming software Application file.

In most Windows versions, the Lutron Applications are stored in C:\Program Files (x86)\Lutron.



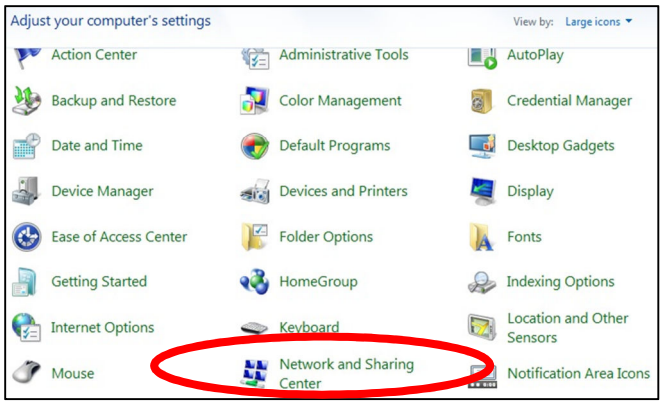
3.0 Running Windows OS on Mac

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.

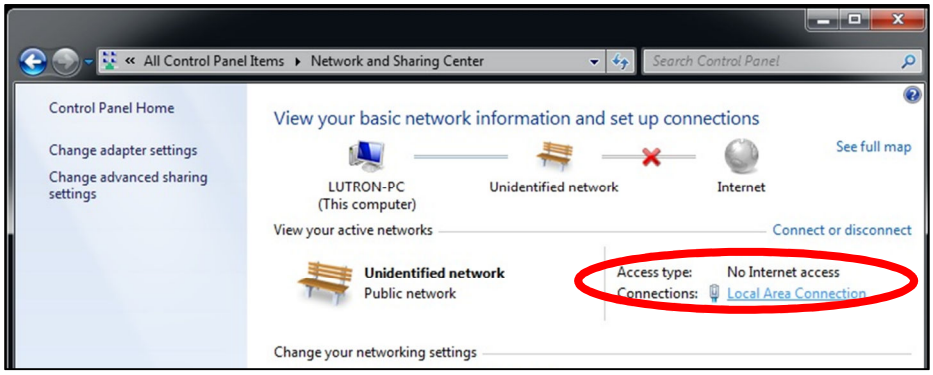
3.1 Parallels and VMware Fusion

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.

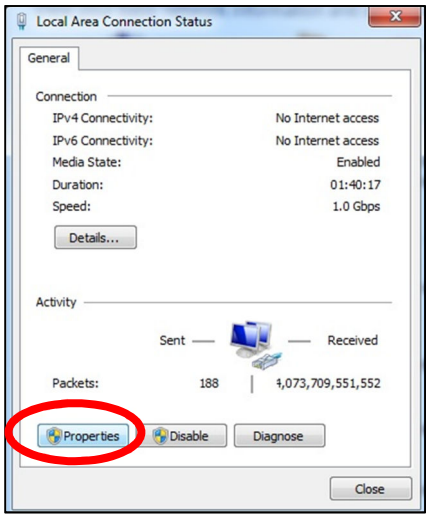
Proper setup can be accomplished in three simple steps. First, go to the Windows OS desktop and set a static IP address. To do this, first go to the **Control Panel**. Click on **Network and Sharing Center**. If you do not see this option, change the View By option to Large or Small Icons.



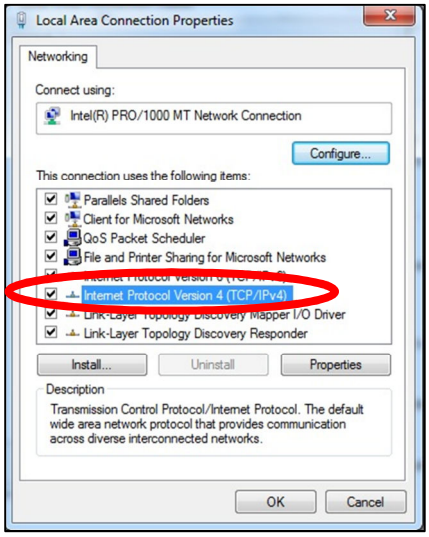
In the Network and Sharing Center window, click on **Local Area Connection** (or sometimes called Ethernet).



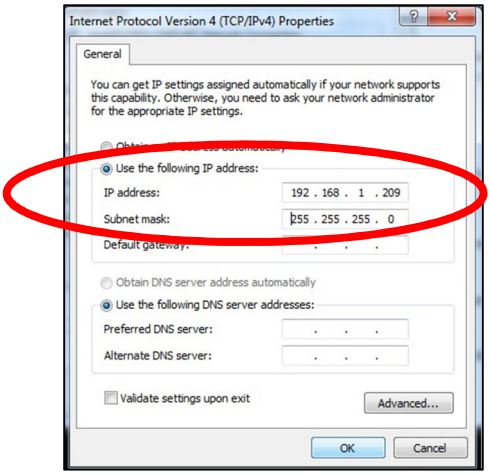
On the Local Area Connection Status window, select the option for **Properties**.



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



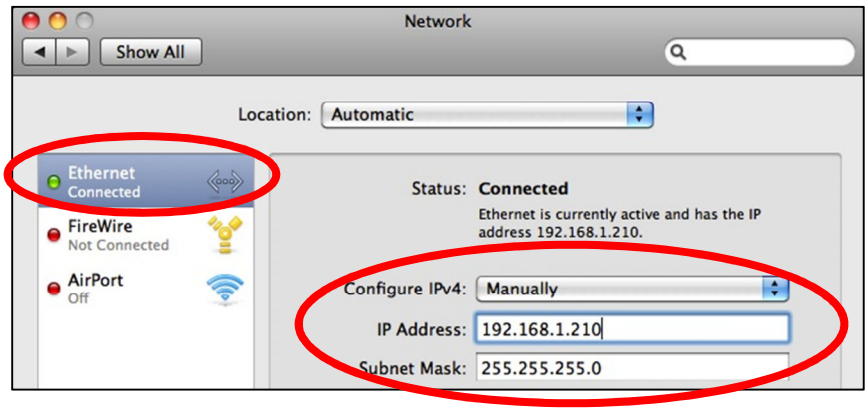
Set up the IP address and subnet mask as a Static IP address. Make sure that this address is outside of the DHCP range of the DHCP server on the LAN router and also does not conflict with any other address on the LAN.



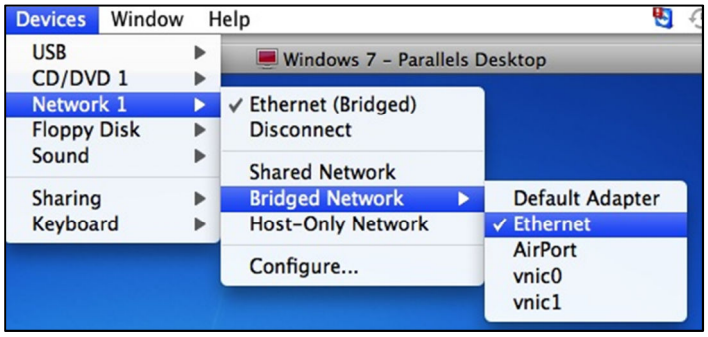
Next, go to the Mac OS side and set a static IP address using the Settings menu. This IP address must be different than the address being used by the Windows OS. This is because there are two machines running on the network (despite the fact that it is the same Mac hardware). First, go to **System Preferences**.

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

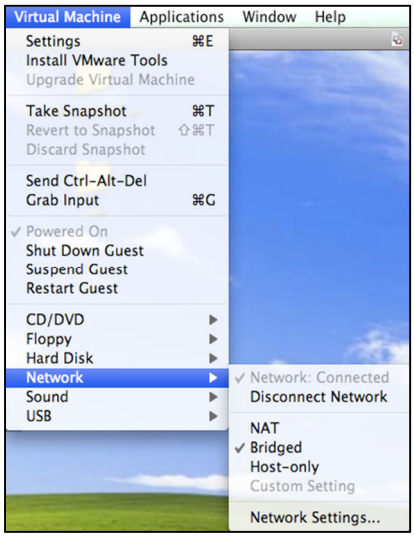
In the Network settings window, set the IP address for the Mac LAN adapter to a different address than all other network devices, including the Windows virtual machine, and click on Apply to save the settings.



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.



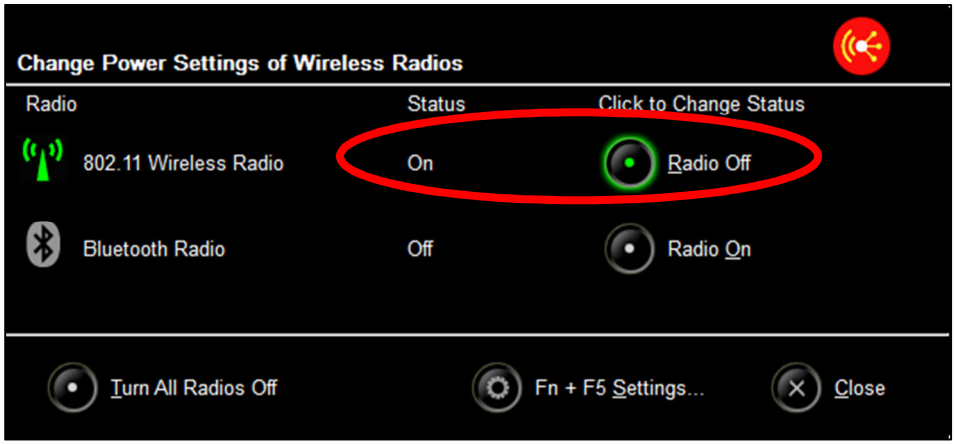
To do this in VMware Fusion, go to the Windows Desktop view and go to the Virtual Machine menu in the upper left (you may need to bring your mouse pointer to the upper left corner for the menu bar to appear). In the **Virtual Machine** menu, select the **Network** sub menu, and then select **Bridged**.



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).

4.0 Network Adapters

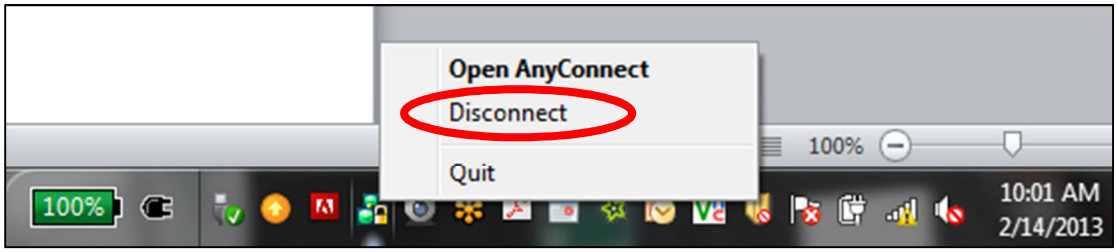
It is recommended that you use a wired LAN connection. When using a wired LAN connection from your PC to the network and/or processor(s) it is good practice to disable the Wi-Fi Network Adapter on the PC. Having the wireless adapter enabled while using the local wired connection will often cause issues 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.

5.0 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.

6.0 Internet Group Management Protocol (IGMP)

Internet Group Management Protocol (IGMP) is an IP networking protocol used to establish multicast groups. It is part of IPv4 and has an IPv6 counterpart called MLD (Multicast Listener Discovery). There are three versions of IGMP: v1, v2, and v3. The HomeWorks QS (HWQS) Processor and RadioRA 2 (RA2) 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 to 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 of 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.

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.

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.

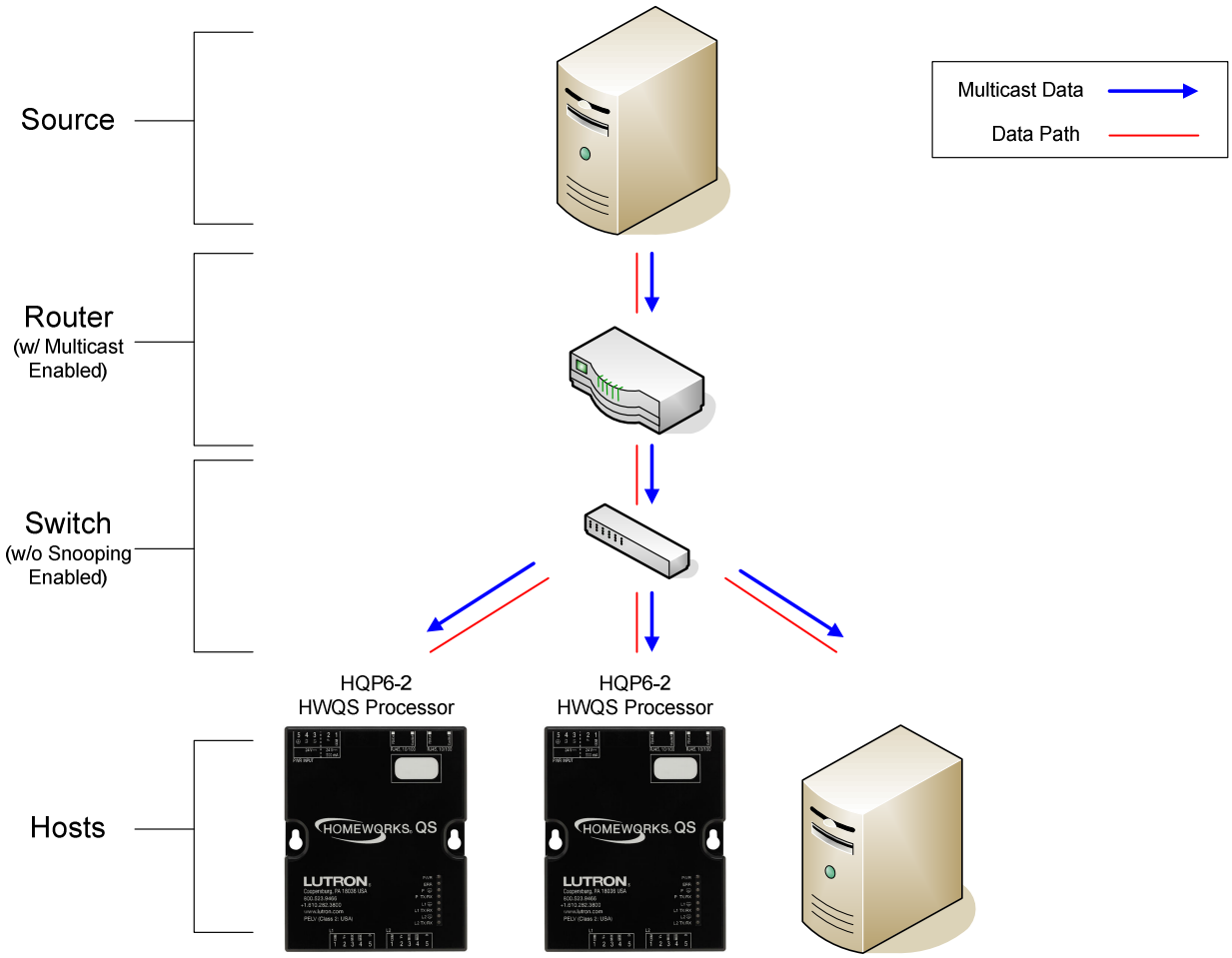
6.3 IGMP Snooping and Lutron Residential Systems

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 only effective when network switches can properly direct multicast traffic and not broadcast it. If, for instance, a two processor HomeWorks QS system is conned 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 must 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). An example of an issue caused by a network loop would be a command that is received by the HWQS system multiple times from a 3rd party touch screen. A button press heard twice for a toggle action would temporarily turn the lights on and then subsequently back off when the echo is sent from the loop.

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.

7.0 Appendix – HWQS System on Network with Snooping Disabled



8.0 Appendix – HWQS System on Network with Snooping Enabled