Introduction

This document provides guidelines for when Pharos controllers need to be part of a wider network or are being configured for remote access. In both cases, the network set-up will require the advice, assistance or cooperation of IT experts and network administrators. Please feel free to pass on these guidelines which include specific information as well as reassurances regarding Pharos hardware behaviour on a network and pre-empting security concerns.

Pharos on a Managed Network

- TPCs, LPC 1/2/4s, AVCs and the Management port of the LPC X are designed for connection on a facilities network for internal and remote access. They can be set to DHCP or statically IP addressed within any IP network.
- The LPC X Protocol port is outputting only lighting data, which may be connected to the same IP network as the management port; a different IP network on the same physical network; or a different physical network. The available IP settings for the Protocol port may be restricted by the lighting fixture requirements.
- The TPC & LPC 1/2/4 can also output lighting data on their Ethernet port – in this case IP restrictions may apply as per the LPC X Protocol port.
- Controllers can be connected to the building network, but if required, they can be isolated via a managed switch so they can be accessed, but cannot communicate with other network devices.
- For multicast access the following ports need to be routed on managed switches:

  230.0.0.0 230.0.3.1 230.0.3.2 230.0.3.3
- If using RIO DMX output, the LPC will use the multicast range 230.0.0.51-151 to transmit to RIOs.
- For access via a public IP we just need port 80. There is no full operating system on the LPC, so the only program that will ever run on it is Pharos firmware.
- Accessing the URL will allow remote pages to be viewed showing the status of the LPC including timeline and input status, output values, etc. This is information only - nothing can be changed, edited or entered in these pages. The Control and Configuration pages can be password protected. These allow anyone with access to both the URL & Password to trigger events, change settings and upload new shows.
- The only vulnerability that we could anticipate would be if arbitrary Ethernet data was being sent on to the network from a newly uploaded show, but the network will be protected from this if the LPC is in the DMZ.
- Malicious intervention would require someone knowing and having the correct version of Designer to create a show (you can't update the firmware remotely - **failsafe #1**), knowing to program a show where triggers send out Ethernet commands (**failsafe #2**), knowing the URL of the LPC (**failsafe #3**), knowing the password (**failsafe #4**). At that point it would also be necessary to know the exact IP of another device on the network, and the port, and send commands in UDP or TCP that could do some damage. Frankly the only people that could have access to all that information would be the IT department concerned...

Remote Access

Pharos controllers provide powerful tools for configuring, controlling, managing and troubleshooting through their built-in web interfaces. These tools are useful onsite during commissioning, which is why Pharos always recommends network access if possible. This is also very useful for ongoing support and maintenance – installers often tend to retain control of the show file and wish for full internet-viable access to continue to support the project remotely.

Remote access is a broad subject with a variety of connection options and different levels of access.

Let's start with the basic definition, and then we can look at exceptions to the rule.

Pharos Designer software can only connect to Pharos controllers if the PC running the software is on the same LAN.

Pharos controllers have a built-in web interface. This gives access to status, troubleshooting and triggering pages. These can be accessed via any computer or hand-held device that has a network browser to view the pages hosted on the controller, if provided with a connection to the controller's network.

Being on the same LAN, having wireless access to the same LAN, or security cleared access through internet remote connections are a variety of ways to gain access. It is entirely down to the local IT/Network administration as to what they may provide.

Terminal Services is another approach, which again requires similar permissions to gain access to the network, but this time, instead of directly remote accessing the controllers, this would allow a remote technician to take control of the desktop of a PC on the LAN. This is the only way you can actually run Designer 'remotely' as Designer will actually be local. This does require a dedicated PC to be left on site, permanently switched on.

A Selection of typical 'remote access' solutions

VPN (Virtual Private Network): Commonly used for creating a connection to an office network, it is set up using standard network settings on a computer. Requires an IP address, user name and password – all provided by network administrator. Designer won't work across this connection - only the web interface will be available if you know the IP address of the controller – but you could use terminal services (e.g. Remote Desktop) to connect to a dedicated PC that's on the same network as the LPC and run Designer on this. However, the Setup and Simulate tabs won't show the plan and fixtures.

ADSL: many broadband providers don't make the IP address of your ADSL modem visible to the outside world, so you can't connect from outside. Make sure you know exactly what you're getting. Also, your ADSL modem will probably use Network Address Translation (NAT) to provide IP addresses to any devices connected to it. These IP addresses may not be visible to the outside world.

VLAN (Virtual Local Area Network): allows computers and LPCs to communicate as if they're connected to the same wire, regardless of their geographical locations. If an installation site doesn't want Designer or the web interface running across their network because of security fears or if the existing network configuration blocks multicast packets which Designer uses to find LPCs, then it's possible to set up a VLAN. The VLAN could be configured to forward multicast packets for Designer, and these couldn't jump onto the main building network.

Typical network troubleshooting:

- Multicast data can be blocked by certain 'managed switches'. The following ports need to be routed:

  230.0.0.0
  230.0.3.1
  230.0.3.2
  230.0.3.3
  230.0.0.51-151 (RIO DMX only)

  We recommend simple, unmanaged switches where possible.

- Remote Pharos Devices. Pharos RIOs and BPSs use multicast rather than IP addressing. They too are susceptible to managed switches blocking the above ports and firewall settings.

- Firewalls on PCs can also cause issues with multicast. Windows firewall can be accessed through the Network Connections window. Bear in mind other security software may have their own firewall settings. Whilst you are connected to Pharos on a completely closed (isolated) network you are in no danger from the Internet activities these filters are designed to block, but remember to turn them back on if the PC is then restored to its usual network.

If you need further help please email support@pharoscontrols.com