



ETHERNET SWITCHES

6750, 6750-P, 6752-P, 6754-P Models
Running firmware 5.X

User Guide

REV 1.0
June 2020



Pathway Connectivity
1439 17 Ave SE • Calgary, AB • T2G 1J9
+1 (403) 243-8110
support@pathwayconnect.com

Copyright © Pathway Connectivity
A Division of Acuity Brands Lighting Canada (“Pathway”) and its licensors.
All rights reserved.

This software and, as applicable, associated media, printed materials and “on-line” or electronic documentation (the “Software Application”) constitutes an unpublished work and contains valuable trade secrets and proprietary information belonging to Pathway and its licensors.

WARNING ABOUT INSECURE PROTOCOLS

Enabling an open protocol that does not use encryption or authentication - these protocols could be eavesdropped or spoofed by malicious parties. You are strongly encouraged to secure access to your network, both physically and technologically. To continue, you must acknowledge that you have read this statement and accept these risks.

CONTENTS

ABOUT VIA ETHERNET SWITCHES.....	1
INSTALLATION INSTRUCTIONS.....	1
PANEL LAYOUTS	3
FRONT PANEL.....	3
MODEL 6750, 6750-P	3
MODEL 6752-P, 6754-P	3
REAR PANEL	3
MODEL 6750.....	3
MODEL 6750-P	4
MODEL 6752-P	4
MODEL 6754-P	4
SFP+ PORTS.....	5
opticalCON PORTS	5
POWER CONNECTIONS	5
CONFIGURATION	5
SECURITY.....	6
BACKGROUND INFORMATION	6
WHAT THIS MEANS TO YOU	6
INTRODUCING SECURITY DOMAINS	7
CREATING A SECURITY DOMAIN	8
ADMINISTERING A DOMAIN	10
LOCAL SECURITY - USING VIA WITHOUT PATHSCAPE	12
RECOVERING A DOMAIN	13

RETAINING DEVICE SETTINGS FROM UNKNOWN DOMAINS	14
USING OLDER VERSIONS OF PATHSCAPE WITH NEW DEVICES	14
SOFTWARE (PATHSCAPE) CONFIGURATION	15
NETWORK SETUP	15
DEVICE PROPERTIES	16
ADVANCED CONFIGURATION	22
PORT PROPERTIES AND CONFIGURATION	32
BASIC PROPERTIES	32
NETWORK PROPERTIES	34
VLAN PROPERTIES	35
NETWORK PROTOCOL SUPPORT	35
PoE PROPERTIES (NOT SHOWN ON VIA12 MODEL 6750)	37
SFP/SFP+ TRANSCEIVER (SFP+ PORTS ONLY)	38
UPGRADING DEVICE FIRMWARE	39
FRONT PANEL UI AND MENU	40
MAIN DISPLAY MESSAGES	40
USING THE FRONT PANEL UI	40
MENUS	41
NETWORK SETUP	41
DEVICE INFO/STATUS	43
ADVANCED SETTINGS	44
PORT STATUS AND CONFIGURATION MENU	55
PORT 13 & 14: CONFIGURATION/STATUS: SFP+ PORTS	60
APPENDIX 1: SFP/SFP+ FIBER ADAPTER SELECTION	63
APPENDIX 2: VIRTUAL LOCAL AREA NETWORK (VLAN)	64

DEFINITIONS	64
SOFTWARE CONFIGURATION OF VLANs	64
VLAN GUIDELINES	64
APPENDIX 3: PLANNING CHARTS	65
VLAN PLANNING CHART	65
SWITCH PLANNING CHARTS.....	67
APPENDIX 4: RING PROTECTION	69
REQUIREMENTS AND LIMITATIONS.....	69
DEFINITIONS	69
APPENDIX 5: RAPID SPANNING TREE PROTOCOL	70
APPENDIX 6: QoS SETTINGS	71
APPENDIX 7: ELECTRICAL AND COMPLIANCE INFORMATION.	72
ELECTRICAL INFORMATION.....	72
MODEL 6750	72
MODEL 6750-P	72
MODEL 6752-P, 6754-P.....	72
COMPLIANCE	72

ABOUT VIA ETHERNET SWITCHES

VIA™ Gigabit Ethernet Switches are designed for live entertainment Ethernet systems, including audio, video and DMX-over-Ethernet networks. This manual covers models **6750, 6750-P, 6752-P and 6754-P**.

VIA Ethernet Switches are intended specifically for signal routing between Pathport DMX-over-Ethernet gateways, or similar equipment, and Ethernet-aware lighting and audio control products, such as consoles and controllers and end equipment. A VIA is a routing device and is not a source of the control protocols or the data being passed. Switches only provide management control over the data path.

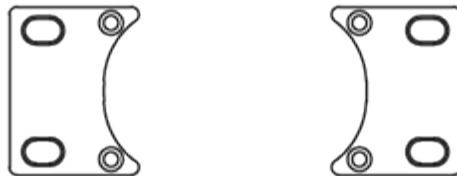
The VIA12 family is easily configured and upgraded using the freely available software tool, **Pathscape**. They are also configurable using the Front Panel UI, which consists of the LCD and rotary pushbutton encoder.

IMPORTANT: VIA model **6750** does not provide hardware support for IEEE 802.3af Power-over-Ethernet (PoE). It does **not provide a way to connect an external PoE supply**. VIA models **6750-P, 6752-P and 6754-P** feature an integrated 100W PoE supply for powering compatible external devices.

If you connect PoE-enabled devices to a 6750 they will not receive power.

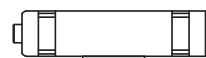
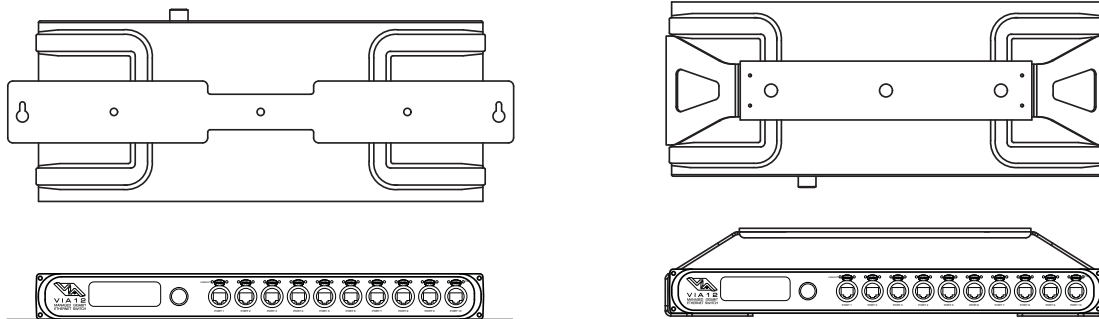
INSTALLATION INSTRUCTIONS

VIA switches are intended for desktop use, or to be mounted in a standard 19" equipment rack, using the integral rack ears (model 6752-P and 6754-P) or the included rack ear accessories (models 6750 and 6750-P). Use the included hex bolts to attach the rack ears to the enclosure.

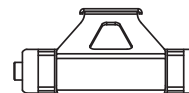


Rack ear accessories included with the 6750 and 6750-P for attaching unit to 19" equipment rack

Truss-mount adaptors (P/N 9003) and wall-mount kits (P/N 9002) are available as accessories.



#9002 Wall-mount Kit



#9003 Truss-mount Kit



All VIA Switches are intended for installation in a dry, indoor location. Ambient operating conditions are **14°F to 122°F (-10°C to 50°C); 5-95% relative humidity, non-condensing.**

Warning: The AC socket outlet shall be installed near the equipment and shall be easily accessible.

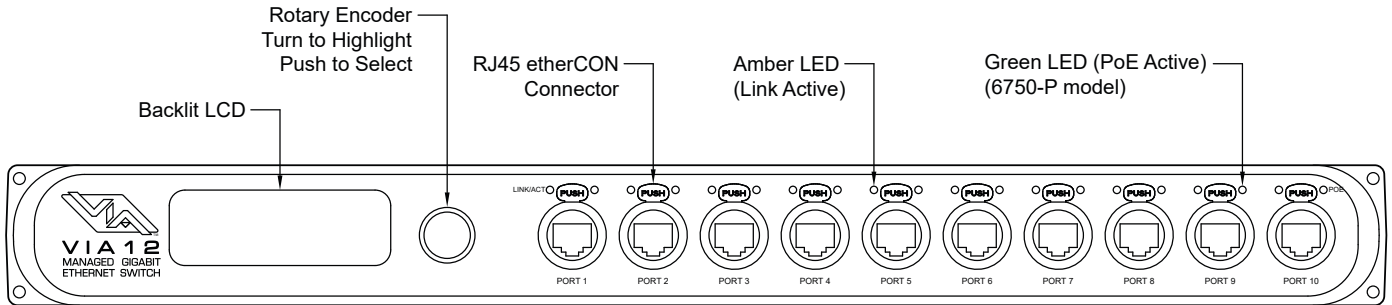
Warning: This equipment relies on building installation primary overcurrent protection.

Warning: Except for the chassis plug marked for AC input, all ports on the VIA12 are intended for low voltage and/or data lines only. Attaching anything other than low voltage sources to the data ports may result in severe equipment damage, and personal injury or death.

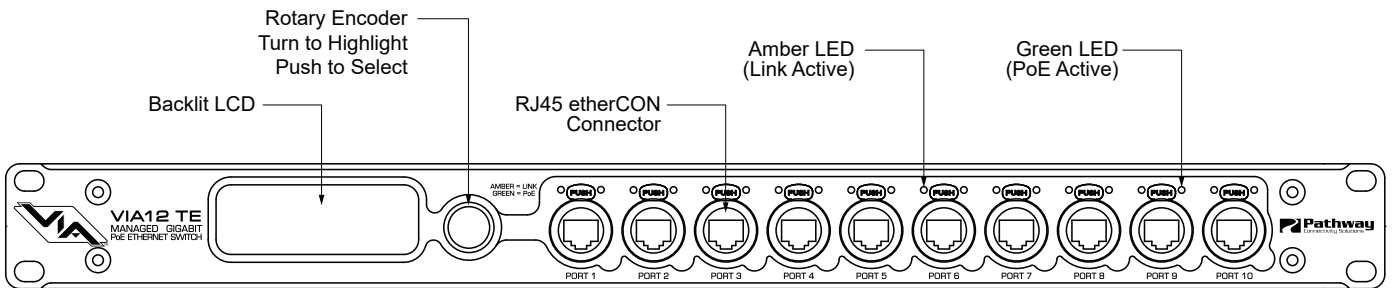
PANEL LAYOUTS

FRONT PANEL

MODEL 6750, 6750-P

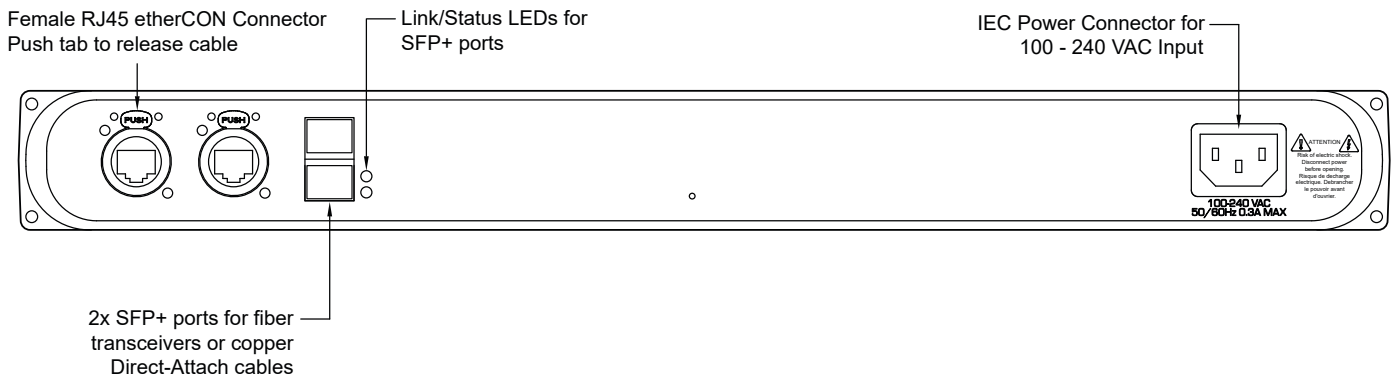


MODEL 6752-P, 6754-P

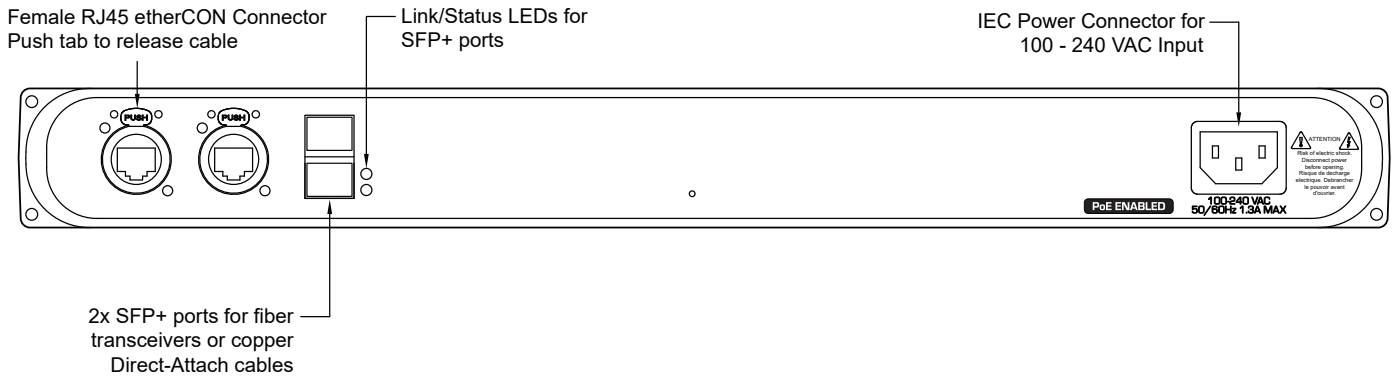


REAR PANEL

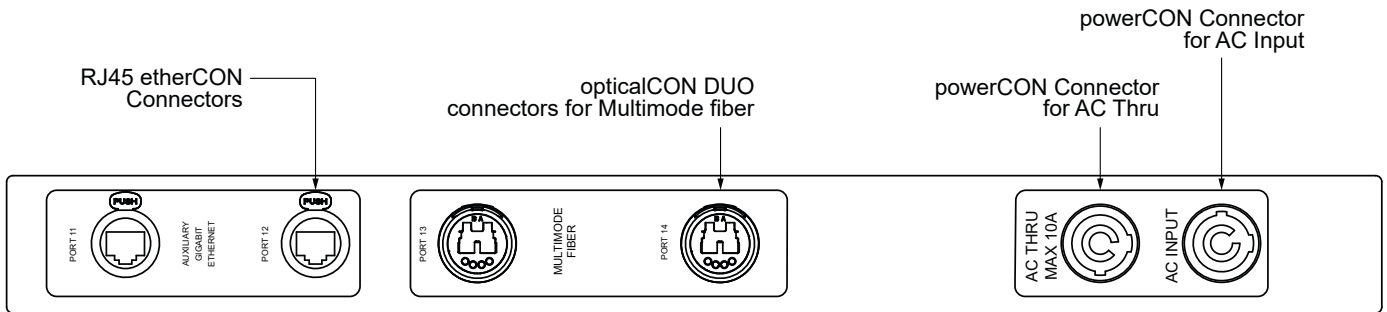
MODEL 6750



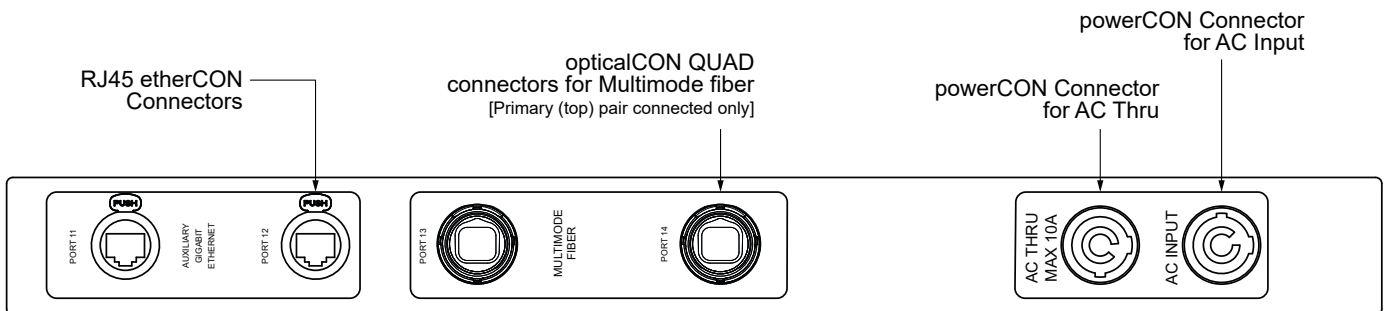
MODEL 6750-P



MODEL 6752-P



MODEL 6754-P



SFP+ PORTS

Models 6750 and 6750-P have two SFP+ compatible ports on the rear of the device. These require the user to provide an SFP or SFP+ fiber transceiver to allow connection to fiber networks. See **Appendix 1: SFP+ Fiber Adapter Selection** for more information on selecting a fiber transceiver.

The user may also use SFP+ Direct Attach cables, both active and passive. This is often the easiest and lowest-cost way to connect multiple switches together, if they are close together in the same enclosure or rack.

opticalCON PORTS

Models 6752-P and 6754-P have opticalCON DUO and opticalCON QUAD ports, respectively, for multimode fiber cables installed instead of SFP+ ports. Additional SFP+ transceivers are not required.

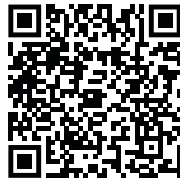
POWER CONNECTIONS

The IEC power plug or powerCON AC Input plug may be connected to an AC power source with a voltage between 100 and 240VAC, either 50 or 60 Hz.

Models 6752-P and 6754-P have an additional powerCON THRU connector to simplify mains power connections in a rack. **DO NOT EXCEED 10A DRAW ON THE FIRST SWITCH.** The powerCON THRU jumper cable is not provided.

CONFIGURATION

Models 6750, 6750-P, 6752-P and 6754-P may be configured from the front panel interface using the LCD and rotary pushbutton encoder. However, we recommend using our free software tool, Pathscape, if possible. To download Pathscape, visit the Pathway website at <https://www.pathwayconnect.com/index.php/products/software/176-pathscape> and click the download link for the appropriate operating system. Use the QR Code below to visit the download page.



For instructions on how to set properties and send transactions to devices, refer to the Pathscape manual.

For instructions on using the LCD and encoder to navigate the switch menus, see the **Front Panel UI and Menu** section.



SECURITY

BACKGROUND INFORMATION

On **January 1, 2020**, California will be the first state to enforce cybersecurity and IoT related legislation. Oregon, New York and Massachusetts are following suit. California's law is Title 1.81.26 "Security of Connected Devices" and mandates that we equip our products with security features that are appropriate to the nature and function of the device. By law, this encompasses all products that are assigned Internet Protocol addresses which can connect to the Internet directly or indirectly. Pathway Connectivity, a division of Acuity Brands, will only ship compliant devices regardless of the jurisdiction into which they are sold.

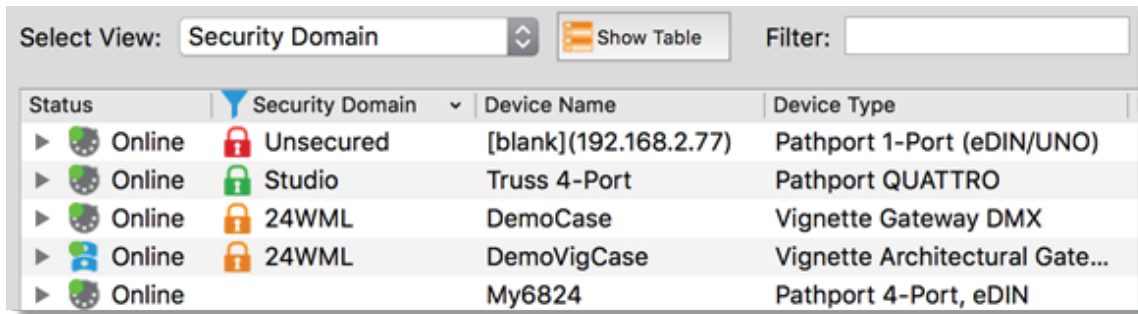
The law requires us to either supply a unique password for our products (see **Local Security** below) or requires the users to change the password before being able to use it (See **Creating a Security Domain** below). With Pathscape V3, we provide features that protect our products from unauthorized access or use by enforcing passwords. Furthermore, Pathway Connectivity does not collect or store personal information on our devices.





WHAT THIS MEANS TO YOU

1. When using products shipped after January 1, 2020, Pathscape will require a single password to allow configuration of all the devices on your network.
2. Products shipped before January 1, 2020 will continue to function without passwords using either Pathscape 2 or Pathscape 3.
3. All products shipped after January 1, 2020 may only be configured using Pathscape 3.
4. Products shipped after January 1, 2020 cannot be downgraded to earlier password-free firmware.
5. Products that are fully configurable from the front panel can create their own unique password. Only with network configured products will you need to type a password; one password for all devices on the network.
6. You will be encouraged to print or save a recovery key in case you lose the password.
7. If you lose the password and lose the recovery key, you will manually have to factory default each device on the network. See the resource section of the Pathway website for a comprehensive document describing how to manually factory default all our devices.
8. The complete network configuration may be saved without a password before factory defaulting devices. Applying the saved configuration will require a new password to be set for the network.
9. Configuring our devices to receive unsecured protocols such as sACN and ArtNet will require you to accept the risks. See **WARNING BOX** regarding unsecured protocols below.
10. Pathway does not store personal information such as names or email addresses on our devices.

INTRODUCING SECURITY DOMAINS

To simplify the process of managing security on your network, Pathscape 3 introduces the concept of a “**Security Domain**”. Below we will describe how to create a Security Domain and add or remove devices from it. In the **Device** tab of Pathscape 3 there is a new view that shows you the name of the device’s domain and a **padlock icon** showing its current state.



Status	Security Domain	Device Name	Device Type
▶ Online	 Unsecured	[blank](192.168.2.77)	Pathport 1-Port (eDIN/UNO)
▶ Online	 Studio	Truss 4-Port	Pathport QUATTRO
▶ Online	 24WML	DemoCase	Vignette Gateway DMX
▶ Online	 24WML	DemoVigCase	Vignette Architectural Gate...
▶ Online		My6824	Pathport 4-Port, eDIN

There are four different ways a device can appear in the **Security Domain** column.

Red Padlock - Unsecured Device

Any device shipped after **January 1, 2020** will have version 5 firmware which includes security. These devices will report their type, name and firmware version **only**. All other properties cannot be read until you add them to a Security Domain (see below on creating domains).

Amber Padlock - Secured Device not in the Current Domain

Devices that have been added to a security domain will appear with an amber padlock. These firmware v5 devices will allow you to read all their properties and even save a show file with the network setup, but the properties are Read-Only. You will have to login to the domain to set any properties. (See **Login procedure** below.) You may also see **Locally Secured** beside an amber padlock. This means the front panel was used to create a unique (and hidden) password to allow front-panel-only configuration. To gain read/write privileges with Pathscape, you **must factory default the device** from the front panel and add it to the local security domain using Pathscape.

Green Padlock - Secured Device in Current Domain

Once you have logged into a Security Domain with a password, any device in your domain will appear with a green padlock and all their properties will be Read/Writeable.

Empty Security Domain cell – Version 4 firmware device shipped prior to January 1, 2020

If the Security Domain cell is empty, this device is using Version 4 firmware and cannot be secured. Pathscape 3 will be able to read and write properties exactly like Pathscape 2. If you upgrade to v5 firmware the device will appear with a red padlock and you will need to add it to a domain before you can use it.

CREATING A SECURITY DOMAIN

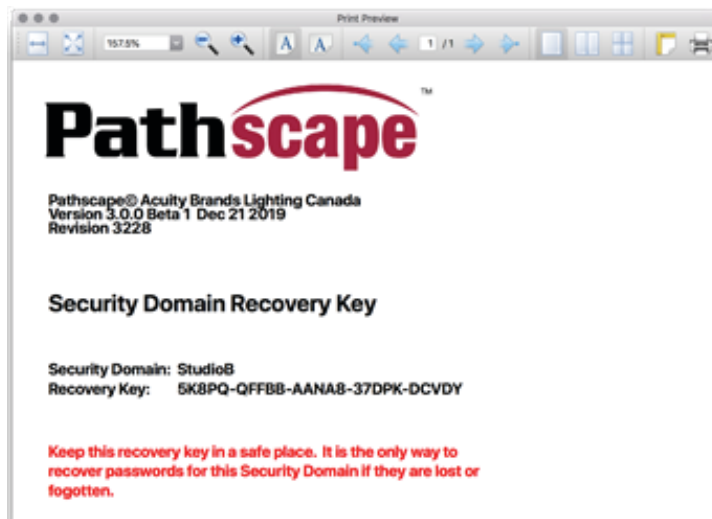
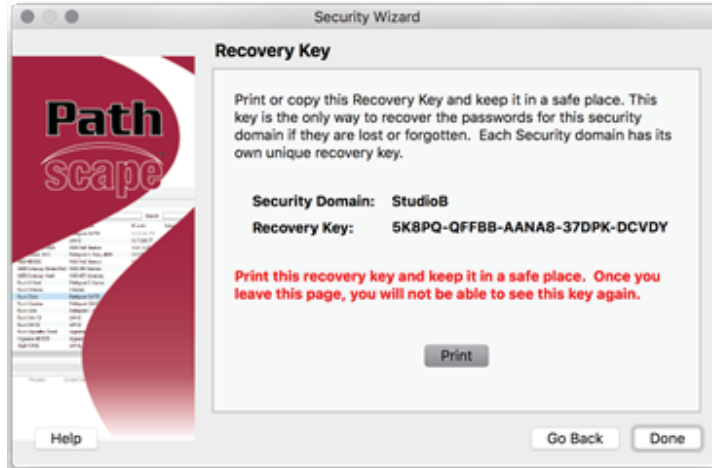
- After starting Pathscope, the online devices will populate the Device View.
- Choose the **Security Domain** view from the **Select View** dropdown
- Each device running V5 firmware will have a **Red “Unsecured”** value in the **Security Domain** column.
- (Optional) You may update devices to Version 5 firmware, by going to the **Tools** menu and selecting **Firmware**. Select the devices to upgrade, and choose **Select Latest**, then **Send Firmware**. (See the **Upgrading Device Firmware** section for more detail). The devices will go offline and come back with a **red padlock**. Remember, Pathscope 3 can configure V4 devices without security. Only update if you desire the security features offered in V5
- From the **Security** menu, choose **New Domain**.



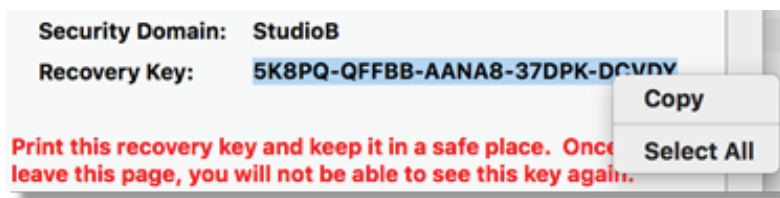
- Enter the new **Domain Name** and **Administrator** and **User passwords**
 - Administrator can change passwords, factory default devices and add devices to the domain.
 - Users can change device properties and save and restore show files. There is one User account password for all users.
- Add the Unsecured devices on your network by checking the Unsecured checkbox and then Continue.



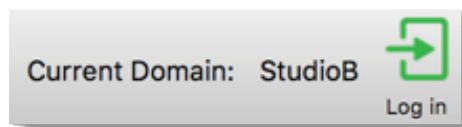
- **Print the Recovery Key.**



- You may also click on the Recovery Key, **Select All** and **Copy** the key to the Clipboard and store it in a safe place.



- Press **Continue** to add the devices to the Domain. The devices will have an **amber padlock** and their properties will be read-only.
- Login to the Domain **as a user** by pressing the button in the toolbar. **Note:** The **Toolbar** option under the **Window** menu must be checked



- As security parameters are verified, the amber padlocks will turn green and the properties of those devices will be read/writable.

ADMINISTERING A DOMAIN

To administer a domain, click on the **Security** menu and select **Administration**. This will bring up the Security Domain Admin Login window.



In the drop-down menu, choose the Domain you wish to log into. **Note that after the domain name, there is a number inside parentheses** - in this example, “(8)”. **This number denotes the quantity of devices currently in that domain.** This may make it easier to differentiate domains, especially if duplicate domain names exist.

Select the domain, and log into it using the Administrator Password you selected during the the domain creation process outlined above. Once logged in using the Administrator Password, the Administrator Utilities window will appear.



Add Devices

Choose this option to add new devices that currently have a red padlock to the domain.

Factory Default

If you want to clear the security settings of a device and remove it from the domain, choose **Factory Default**. Only devices in the Security Domain shown in this dialog box will be available to be defaulted. For devices that you do not have a password for, you must have physical access to factory default them before you regain network configurability. See the **Reference** section under the **Downloads** page the Pathway website for a comprehensive document titled [Factory Defaulting Pathway Ethernet Devices](#), describing how to manually factory default all our devices. See the QR code below for a direct link to the document.



Change Passwords

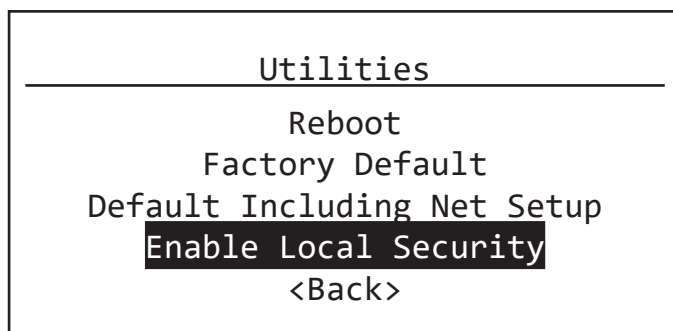
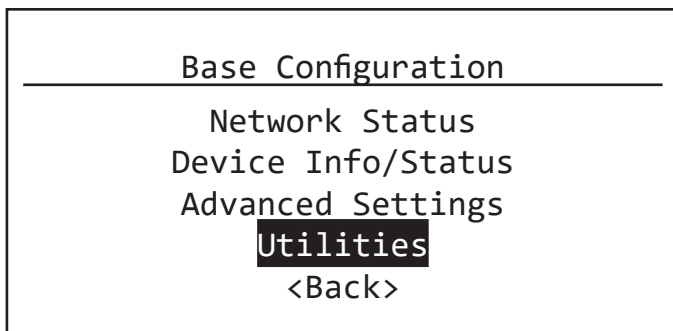
If your staffing changes, it is a good idea to change the passwords on the domain. All devices should be online when you change the password.

Note: If some devices are offline and you change the password, when those devices come back online, they will coincidentally have the same domain name, but use the old password. You will have to factory default them then add them to the new domain using the new password. You can Factory Default them using the **Security > Administration** option in the menu. When asked to login, there will be two domains with the same name. Choose the second one and use the old password and Factory Default the devices listed. When they come back online, they will have red padlocks and be listed as Unsecured. Add them to the new domain using the new password.

LOCAL SECURITY - USING VIA WITHOUT PATHSCAPE

VIA12 switches have features that use insecure protocols, like **Art-Net Trap & Convert**. You may not intend to use Pathscope, but “bad actors” could potentially access the switch and change the configuration. Therefore it is prudent to configure **Local Security** to protect your network if you want to use Art-Net Trap & Convert, but are not using Pathscope to add your devices to a **Security Domain**.

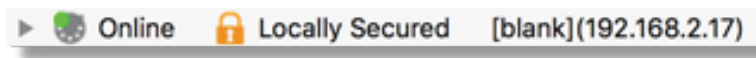
From the **Utilities** menu on the front panel, select **Enable Local Security**.



WARNING ABOUT INSECURE PROTOCOLS

Enabling an open protocol that does not use encryption or authentication - these protocols could be eavesdropped or spoofed by malicious parties. You are strongly encouraged to secure access to your network, both physically and technologically. To continue, you must acknowledge that you have read this statement and accept these risks.

If you do open Pathscope, this device will be part of the domain “Locally Secured”.



You cannot login to this security domain. If you want to now use Pathscope to configure this device, you must use the front panel to Factory Default it, then use Pathscope to add it to a Security Domain. You may want to save the Pathscope show file before factory defaulting the VIA, then after adding it to a Security Domain, you can restore its configuration.

RECOVERING A DOMAIN

If you lose the Administrator password (or it was maliciously changed without your consent), you can recover the domain, retaining its configuration and set new passwords.

- From the menu, choose **Security > Recover Domain**.



- Type in the 20-digit **Recovery Key** and press Continue.



- Type in a new **Administrator Password**.

- From the menu choose **Security > Administration** and Change Passwords to set a new User password.



RETAINING DEVICE SETTINGS FROM UNKNOWN DOMAINS

There are times when you don't know the password of a Security Domain, but you'd like to retain all its configuration. Without logging in to a Domain, all devices that appear with amber padlocks are read-only. If you save a show file, the configuration of all devices is saved. You can then factory default the devices using the prescribed method; see the **Reference** section under the **Downloads** page the Pathway website for a comprehensive document titled [Factory Defaulting Pathway Ethernet Devices](#), describing how to manually factory default all our devices. See the QR code below for a direct link to the document.



Once they reappear in Pathscape with a red padlock, add the devices to a Security Domain, then open the show file and **Send All Transactions** to restore the network configuration and patch.

USING OLDER VERSIONS OF PATHSCAPE WITH NEW DEVICES

If you use Pathscape 1 or Pathscape 2 with devices shipped after **January 1, 2020 (Version 5 firmware)**, you will not be able to configure them; **you must use Pathscape 3**. As a reminder, the device label will appear in the earlier versions of Pathscape as **"Use latest Pathscape PC software to secure"**. Other properties will be shown and are correct, but any attempts to change them will fail.

SOFTWARE (PATHSCAPE) CONFIGURATION

Wherever possible, we recommend using a PC with Pathscape to configure your VIA switch(es). For in-depth information on using Pathscape, see the Pathscape manual. Pathscape is available for macOS and Windows from the Software section of our website: <https://www.pathwayconnect.com/index.php/products/software/176-pathscape>. Use the QR Code below to visit the download page.



If using a PC with Pathscape is not possible or practical, see the section **Front Panel UI and Menu** later in this manual.

NETWORK SETUP

PLEASE NOTE: Before any configuration and network setup can be done, including setting the IP, the VIA switch(es) must be added to a Security Domain. If the device is not added to a Security domain, it will not be possible to configure any properties.

From the factory, the VIA12's IP address is static, and set to **10.X.X.X** (where X is between 0 and 254), with a subnet mask of **255.0.0.0** and a default gateway of **10.0.0.1**. Before any additional configuration, set the devices' IP address to the same subnet and IP range as the computer and other devices on the lighting network.

Additionally, the VIA12's name in the device list will be shown as its IP address. Give it a useful name before continuing.

Status	Security Domain	Device Name	Device Type	IP Addr
Online	pathway	10.30.142.169	VIA12 PoE	10.30.142.169

Basic Properties

Device Name:

Device Notes:

MAC Address: 00:04:a1:1e:8e:a9

Firmware Version: 5.0.4.beta2

Identify Device:

Serial Number: PP2102601

Front Panel Lockout:

LCD Backlight:

Device Type: VIA12 PoE

Network Properties

IP Mode:

IP Address:

Subnet Mask:

Gateway:

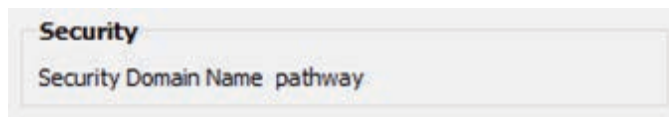
Quality of Service:

DEVICE PROPERTIES

The following fields are shown in the Device Property Panel in Pathscope. Some are editable, while others are read-only.

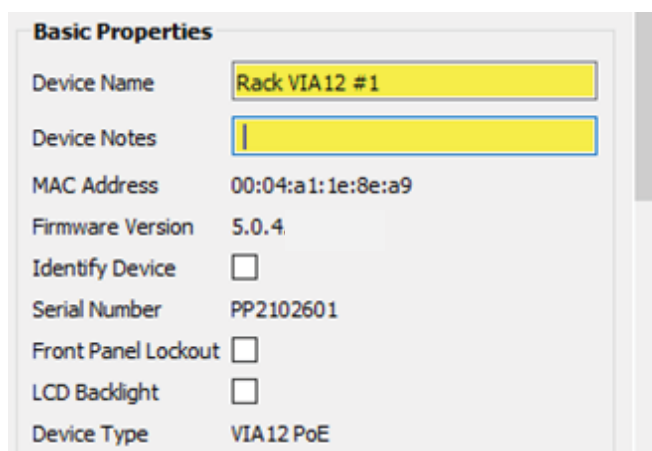
NOTE: If all properties are read-only (greyed out and uneditable), make sure you are logged into the correct Security Domain.

SECURITY PROPERTIES



Property	Description
Security Domain	Name of the security domain the device is currently assigned to

BASIC PROPERTIES



Property	Description
Device Name	A user-configured, soft label for the device. If left blank (and by default) the device name displayed will be the device's IP Address. Shown on the front LCD.
Device notes	A user-configured text description field, shown in the Device view.
MAC Address	Factory-assigned media access control address. Read-only.
Firmware Version	Shows current operating firmware version. See the Firmware Update section on how to update the firmware. Read-only.
Identify Device	Show if the device is in Identify mode. Checking this box causes device to commence identify behavior (flashing LCD backlight).

Property	Description
Serial Number	Factory-assigned, Pathway serial number. Read-only.
Front Panel Lockout	<p>Checking this will lock the local controls on the front panel of the device. Scrolling menus allow you to read properties, but changing properties is disallowed.</p> <p>There is a 30-second delay upon boot before the Front Panel Lockout takes effect. This provides a window where the switch can be accessed to perform a factory default in case communication with the device is lost, etc.</p> <p>See the Front Panel Lockout section under Factory Default later in this manual for more details.</p>
LCD Backlight	<p>Checking this will enable the LCD backlight on the front panel of the device.</p> <p>If not checked, the LCD backlight only comes on during use of the Front Panel encoder knob.</p>
Device Type	Factory-assigned, Pathway model type. Read-only.



NETWORK PROPERTIES

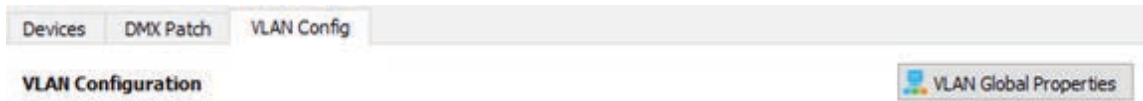
Network Properties


IP Mode	Static
IP Address	10.30.142.169
Subnet Mask	255.0.0.0
Gateway	10.0.0.1
Quality of Service	Disabled
Rapid Spanning Tree	<input checked="" type="checkbox"/>
DNS server	0.0.0.0
NTP server	
Network Interface	Ethernet 4

Property	Description
IP Mode	Determines how IP settings are obtained. Options are Disabled , Static and Dynamic .
IP Address	User-set Internet Protocol address (IPv4) for this switch. If VLANs are enabled, the IP address is applied by default to the Management VLAN ID#.
Subnet Mask	User-set subnet mask. If VLANs are enabled, the subnet mask is used by default by the Management VLAN ID#.
Gateway	Network traffic on this switch (or VLAN if enabled) requesting addresses outside of the assigned subnet will be routed through this IP address.
Quality of Service	QoS Settings for determining the relative priority of different data packets, i.e. Dante.
Rapid Spanning Tree	Enables or disables RSTP (Rapid Spanning Tree Protocol). Rapid Spanning Tree Protocol automatically detects Ethernet loops (two Cat5 cables between the same two switches where the ports are on the same VLAN). Without RSTP on, networks with loops will have very poor performance.
DNS Server	Set the device DNS Server here, if applicable.
NTP Server	Set the device Network Time Protocol server here, if applicable. This is required when using SixEye Remote Monitoring Management.
Network Interface	Shows the Network Interface (NIC) your PC is using to communicate to the device.

VLAN PROPERTIES

To enable/disable VLANs, use  **VLAN Global Properties** under the **VLAN Config** Tab.



The below properties will appear read-only in the Properties Pane (greyed-out); these are only configurable via the  **VLAN Global Properties** button, as shown above.

VLAN Properties

VLAN Support Enabled

VLAN Range Start 1

VLAN Range End 10

Management VLAN 1

Property	Description
VLAN Support	Shows whether VLANs are Enabled or Disabled, globally, on your entire network. To enable/disable VLANs, use VLAN Global Configuration under VLAN Config Tab.
VLAN Range Start	Shows the start ID for range of VLAN IDs available to use
VLAN Range End	Shows the end ID for range of VLAN IDs available to use.
Management VLAN	Shows the VLAN ID used by Management processor. It is strongly recommended that the Management VLAN ID be set to the same value as the VLAN Range Start value.

NETWORK PROTOCOL SUPPORT

Network Protocol Support

Art-Net Alternate Mapping

Property	Description
Art-Net Alternate Mapping	Enabled (by default). Used in conjunction with Art-Net Trap & Convert feature. When enabled, Art-Net Universe 0:0 is treated as Universe 1. When disabled, Art-Net universe 0:0 is ignored. Does not affect unicast Art-Net packets.



RING PROTECT PROPERTIES

Ring Protect Properties

Ring Protect Mode:

Ring Protect Control VLAN:

Ring Protect Primary Port:

Ring Protect Secondary Port:

Ring State: Ring idle

Property	Description
Ring Protect Mode	Set function for Ring Protect Mode.
Ring Protect Control VLAN	Specifies the VLAN ID# used to determine the integrity of the ring. May not be used for any other traffic. Valid ID# is any ID outside the range set in VLAN setup. Default is VLAN 4095.
Ring Protect Primary Port	Designates which port to use as the active uplink port to other switches. Valid range is port 11 through 14.
Ring Protect Secondary Port	Designates which port to use as the fall back link to other switches. Valid range is port 11 through 14.
Ring State	Current state of Ring. Read-only.

PoE PROPERTIES (6750-P, 6752-P, 6754-P)

POE Properties

PoE Total Draw (W) 47.16

Property	Description
PoE Total Draw (W)	Displays the current power draw from connected PoE devices.

ADVANCED PROPERTIES

Advanced Properties

User ID

Property	Description
User ID	Custom numeric identification for external databases.

ADVANCED CONFIGURATION

VLAN CONFIGURATION

As described above, use the **VLAN Config** tab in Pathscape to configure network VLANs. A VLAN (Virtual Local Area Network) is a group of ports on the switch (or switches) that are configured to pass traffic to one another, but not to ports on any other VLAN. When VLANs are established, ports that connect switches to other switches must be “tagged” to pass all VLAN traffic.

VLAN #	VLAN ID	Device
> 1	Local	
> 2	Office	
> 3	Audio	
> 4	Video	
> 5	Lighting	
> 6	VLAN 6	
> 7	VLAN 7	
> 8	VLAN 8	
> 9	VLAN 9	
> 10	VLAN 10	

In the VLAN Configuration window, there are three columns: **VLAN #**, **VLAN ID** and **Device**. By default, the VLAN ID will likely not have unique names (as in the screenshot above) but simply labeled “VLAN 1”, “VLAN 2”, etc. See **VLAN Global Properties** below for details on how to assign custom labels to your VLAN IDs.

Click on the arrow next to each VLAN to the VIA switches available for configuration.

▼ 3	Audio	Rack VIA5
		Wall VIA16
		Desk VIA 12
		Rack VIA 10
		Rack VIA12
> 4	Video	
▼ 5	Lighting	Rack VIA5
		Wall VIA16
		Desk VIA 12
		Rack VIA 10
		Rack VIA12

Note that **every VIA switch on the network** will show up under every listed VLAN. VLAN ranges are configured globally; it is not possible to assign a switch to only one VLAN in this window. At the subdevice/port level, VLANs may be assigned as needed.

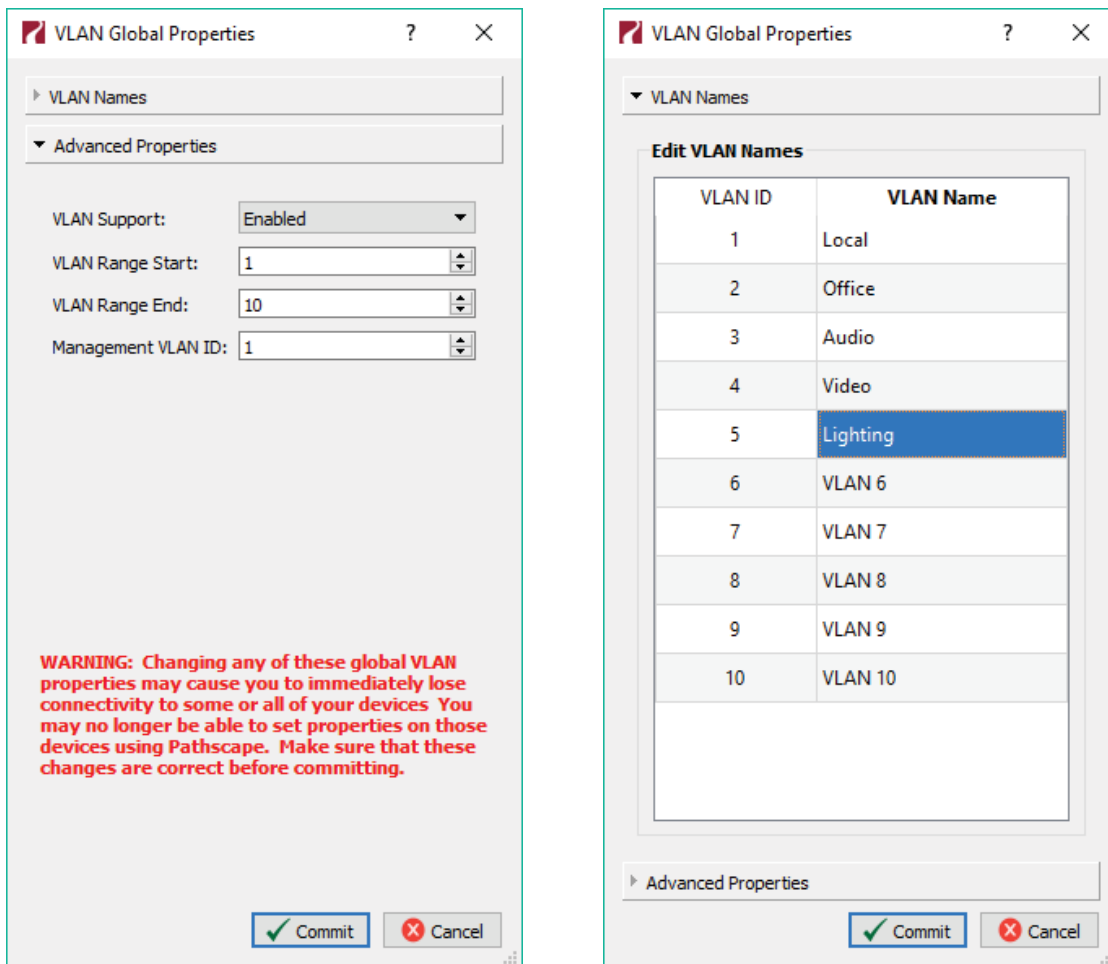
VLAN Properties such as IP Address, DHCP and IGMP settings are configured per VLAN, per switch. For example, to configure **VLAN 3 (Audio)** on the “Rack VIA12” above, expand VLAN 3 and click on the Rack VIA12 device, then edit its properties in the Properties Pane. To edit **VLAN 5** on the same switch, expand VLAN 5 and click on the Rack VIA12 to edit VLAN 5 on that device.

VLAN GLOBAL PROPERTIES

Plan your VLAN layout before attempting configuration. The creation of a map of the network, showing which devices and which ports to associate with a given VLAN, is strongly recommended prior to configuration.

EXTREMELY IMPORTANT NOTE: When configuring one or multiple VIA switches using Pathway’s software-based configuration tools, be certain the port connected to your computer is on the same VLAN ID# as the management and is not on a tagged port. Failure to observe this rule will result in what appears to be a broken network.

In order to use VLANs, VLAN Support must be enabled in VLAN Global Properties, which is access by clicking the **VLAN Global Properties** button in the top-right corner of the VLAN Config Tab.



There are two sections to the **VLAN Global Properties** window: the **Advanced Properties** panel, and the **VLAN Names** panel.

The Advanced Properties panel will allow for global configuration of VLAN Ranges, Management VLAN, and VLAN Support on and off.

▼ **Advanced Properties**

VLAN Support: Enabled

VLAN Range Start: 1

VLAN Range End: 10

Management VLAN ID: 1

Once you have set up the number of VLANs you need, you may edit the names of any of the available VLANs by using the **VLAN Names** panel. Double-click on the VLAN Name, give it a name and then click the ✔ Commit button to save changes. To discard changes, click the ✖ Cancel button.

Edit VLAN Names	
VLAN ID	VLAN Name
1	Local
2	Office
3	Audio
4	Video
5	Lighting
6	VLAN 6

After clicking the **Commit** button, you will then see several transactions in the transaction editor, which will be automatically sent.

Property	Description
VLAN Support	Enable or disable VLANs. Note this is a Global setting and will enable or disable VLANs across the entire network.
VLAN Range Start	Specifies lowest VLAN ID# available. Valid range: 1 to 4093. Default is 1.
VLAN Range End	Specifies highest VLAN ID# available. Valid range: 1 to 4093. Default is 10.
Management VLAN	Specifies the VLAN ID# used by the management processor. Default is 1. This value MUST be within the range specified by the range start and end set above, or you will not be able to configure the switch. It is strongly recommended that the Management VLAN ID be set to the same value as the VLAN Range Start value.

These properties determine the size of the VLAN table, and which VLAN has communication with the switch's management processor. For efficient switch operation, the VLAN range should be kept as small as necessary.

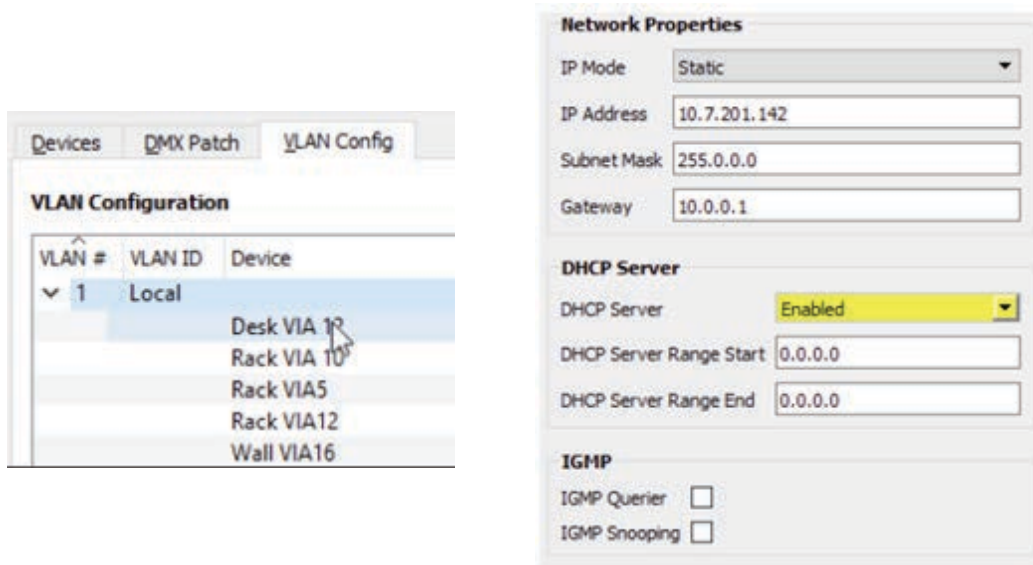
If the **Management VLAN** is accidentally set to a value outside the VLAN range, it may be necessary to use the **Factory Default** option to restore communication with the management processor and allow further configuration. See **Factory Default** section for instructions.

The VLAN range and individual VLAN configuration must be done prior to activating the Ring Protect feature.

Use the “**VLAN Patch**” View in the Device tab to configure individual ports’ VLANs.

VLAN NETWORK PROPERTIES

VLANs must be enabled prior to configuring these properties. Expand a VLAN in the **VLAN Config** tab and select a switch.



Property	Description
IP Mode	Determines how IP settings will be obtained Disabled (default): No IP assigned. Static: IP settings manually set by user. Dynamic: IP settings will be obtained from a DHCP server.
IP Address	Manually set IP address (IPv4).
Subnet Mask	Set subnet mask.
Default Gateway	Set default gateway.

Network Settings must be configured on any VLAN requiring use of multicast filtering (IGMP) or a DHCP server. By default, only the management VLAN (VLAN ID#1 by default) is automatically assigned an IP and subnet mask. All other VLANs default to a null IP address value (0.0.0.0). From the Network Settings for each VLAN, assign a unique IP per switch, a common subnet mask and, where necessary, a default gateway.

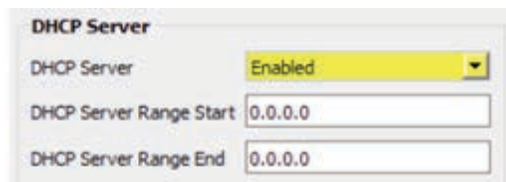
Any Internet access will be through a proxy or NAT gateway (i.e. an Internet router) in which case the default gateway IP should point to this device. If you are using SixEye on this VIA, you must set the Default Gateway for the Management VLAN. If devices on other VLANs are using SixEye, set the VLAN’s Default Gateway.

IP Mode must be set to “Static” if the VIA is to act as a DHCP server. Only one DHCP server may be active on any given VLAN. Setting the IP Mode to “Dynamic” does NOT enable the DHCP server – see below.

If the IP Mode is set to “Dynamic” on a system with no active DHCP server, the switch will auto-generate IP settings in accordance with zeroconf standards, in the IP range of 169.254.x.x/16. This range may not be suitable for connection to entertainment systems.

When in doubt, we recommend using a mode of ‘Static’ and configuring each switch and VLAN combination with a unique IP address and appropriate subnet mask.

VLAN DHCP PROPERTIES



VIA switches can automatically assign IP addresses to connected devices, using a DHCP (dynamic host configuration protocol) server.

Important: Only one DHCP server may be active on any given VLAN at one time. Running multiple DHCP servers will cause network reliability problems. Many WiFi routers and access points typically have a DHCP active, so if there is one as part of your network, make sure you only configure it or the VIA as the DHCP server, **not both**.

The DHCP-hosting VIA switch must first be set to a static IP address on the desired VLAN, **prior to enabling the DHCP server**. The DHCP server should be enabled prior to setting other connected devices to a “Dynamic IP” mode or being connected to the network VLAN.

In some cases, it may be necessary to reboot connected devices to ensure the DHCP server correctly recognizes them and assigns appropriate network settings.

Property	Description
DHCP Server Enable	<p>Disabled (default): DHCP service is turned off. Use this setting for all static (manually-set) IP systems, and for all switches other than the VLAN’s designated DHCP server host.</p> <p>Enabled: Enables DHCP server.</p>
DHCP Server Range Start	<p>Set the first available IP address.</p> <p>The DHCP pool is partially predefined based on the IP address and subnet mask of the host switch, as the host must have proper communication with the requesting device.</p>
DHCP Server Range End	<p>Set the last available IP address.</p>

VLAN IGMP PROPERTIES



When using multicast data packets, such as streaming ACN (sACN), bandwidth efficiency may be improved by using IGMP (Internet group management protocol) to enable multicast filtering.

Property	Description
IGMP Snooping	Enable/disable IGMP snooping – allows the switch to correctly filter multi-cast traffic
IGMP Querier	Enable/disable the IGMP querier – creates the multicast tables used by snooping

The IGMP Querier establishes a table of active multicast groups by querying connected devices about which multicast groups each device wishes to join. For example, a gateway will request the multicast groups associated with the sACN universes that the gateway is patched to.

Each switch operating an IGMP Querier on a VLAN must have valid IP settings on that VLAN. The IP settings may be static or dynamically established using the DHCP.

IMPORTANT: Two IGMP queriers should be active on each VLAN using multicast filtering. If no querier is active, the groupings table will fail after approximately five minutes and filtering will only work erratically or will fail altogether. IGMP should not be enabled on more than four VLANs per switch.

The IGMP Snooper allows the switch to more efficiently route multicast traffic by applying the multicast groupings as a filter. Multicast traffic is only directed to only those ports, i.e. end devices, that have requested to receive that traffic.

Watch the following video on Pathway’s YouTube channel for a detailed explanation of IGMP Snooping:

<https://www.youtube.com/watch?v=0MVE22JCIt4>

And the following video for a real-world example.

https://www.youtube.com/watch?v=CdXI_Q7KZC0

RING PROTECT CONFIGURATION

For Ring Protect mode to function, VLAN support must be enabled.

Ring Protect Properties

Ring Protect Mode: Disable ▼

Ring Protect Control VLAN: 4095 ▲▼

Ring Protect Primary Port: Port 13 ▼

Ring Protect Secondary Port: Port 14 ▼

Ring State: Ring idle

Property	Description
Ring Protect Mode	Status of Ring Protect Mode. Disabled (default): Ring Protection feature is turned off Master: Only one switch may be set as the Master. Transit: All other switches must be set as Transit.
Ring Protect Control VLAN	Specifies the VLAN ID# used to determine the integrity of the ring. May not be used for any other traffic. Valid ID# is any ID outside the range set in VLAN setup. Default is VLAN 4095..
Ring Protect Primary Port	Designates which port to use as the active uplink port to other switches. Valid range is port 11 through 14.
Ring Protect Secondary Port	Designates which port to use as the fall back link to other switches. Valid range is port 11 through 14.

WARNING: Ring Protection should only be configured and enabled after all other VLAN configuration has been completed.

During the setup and configuration of the Ring Protection feature, communication between devices may be erratic or broken. We strongly recommend that all switches be configured using only a single Port-to-Port link with the appropriate Ring Protection settings **PRIOR** to being physically connected together in a ring with two ports active. We also strongly recommend that all switches be disconnected from one another **PRIOR** to disabling the ring feature.

Prior to setup, determine which switch will be the master. Generally, the least busy switch in a position with the most stable power (i.e., not on a roving platform) is the best choice. All other switches must be configured as transit switches.

All switches must have both a primary and a secondary ring port set. These ports will be automatically configured as Tagged (uplink) ports, meaning all traffic on all VLANs will be passed through the ports. Tagged ports must be connected to other tagged ports on other switches. Do not connect end devices like gateways or computers to tagged ports.

If changes are made to the ring configuration while the ring is active, it may be necessary to reboot all switches for the changes to take effect.

RAPID SPANNING TREE

Quality of Service	Disabled
Rapid Spanning Tree	<input checked="" type="checkbox"/>
DNS server	0.0.0.0

Property	Description
Rapid Spanning Tree	Enable / Disable Rapid Spanning Tree Protocol (RSTP)

The Rapid Spanning Tree algorithm detects and prevents network loops. Networks with loops will have very poor performance.

The interaction between RSTP and the Ring Protect system may cause long network re-configuration times when the ring topology is changed. For this reason, it is recommended that RSTP be used during setup and then disabled after verifying there are no loops present.

Warning: Rapid Spanning Tree must be enabled on all switches to detect loops correctly. Network loops created through un-managed switches may not be detected correctly. Pathway’s implementation of Rapid Spanning Tree Protocol should be inter-operable with other switch manufacturer’s implementations.

For more information, please refer to **Appendix 4: Rapid Spanning Tree Protocol**.

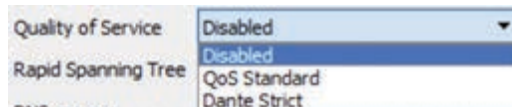
ART-NET ALTERNATE MAPPING

Network Protocol Support

Art-Net Alternate Mapping

This feature is used in conjunction with the “**Art-Net Trap-and-Convert to sACN**” feature. See below under **Network Protocol** support under **Port Properties**

QUALITY OF SERVICE (QoS)



Quality of Service determines the relative priority of different data packets, which in turn determines which packets should receive preferential routing from a VIA switch. QoS is often used for the distribution of video and audio signals, including the Dante® audio standard, to meet the signal's required timing constraints. Please remember that giving all data high priority is the same as treating all traffic equally.

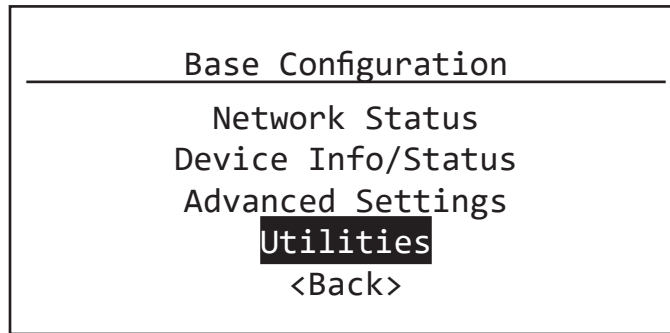
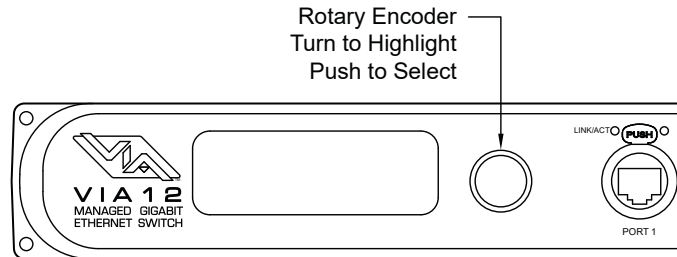
Property	Description
Quality of Service	<p>Disabled (default): Disables QoS-based routing. All traffic is treated equally.</p> <p>Standard: Traffic priority is observed using a weighted algorithm to ensure timely delivery of high priority traffic and eventual delivery of lower priority packets.</p> <p>Dante Strict: Traffic priority is strictly observed, using Dante-specified weighting. Lower priority traffic may be dropped or ignored to ensure delivery of Dante's high priority packets.</p>

For more information, please refer to **Appendix 5: Quality of Service (QoS)**.

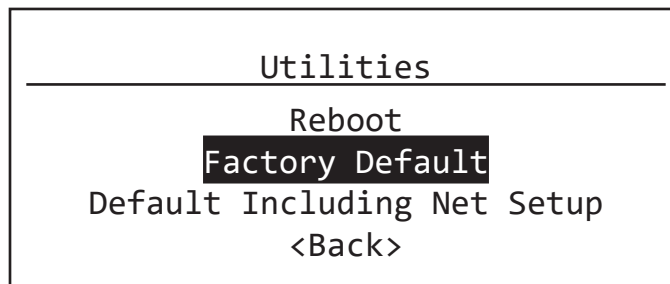
FACTORY DEFAULT

In the event of a loss of communication with the device (eg. Management VLAN accidentally set to a value outside the VLAN range), it is possible to reset the switch to factory settings.

To factory default a switch, turn the encoder knob to the switch main menu, which is the default menu showing the switch's name and IP address. Click in the encoder to access the main menu.



Scroll the encoder knob until “**Utilities**” is highlighted, and click in the knob. Under the Utilities menu, scroll down to “**Factory Default**”, and click in the knob.

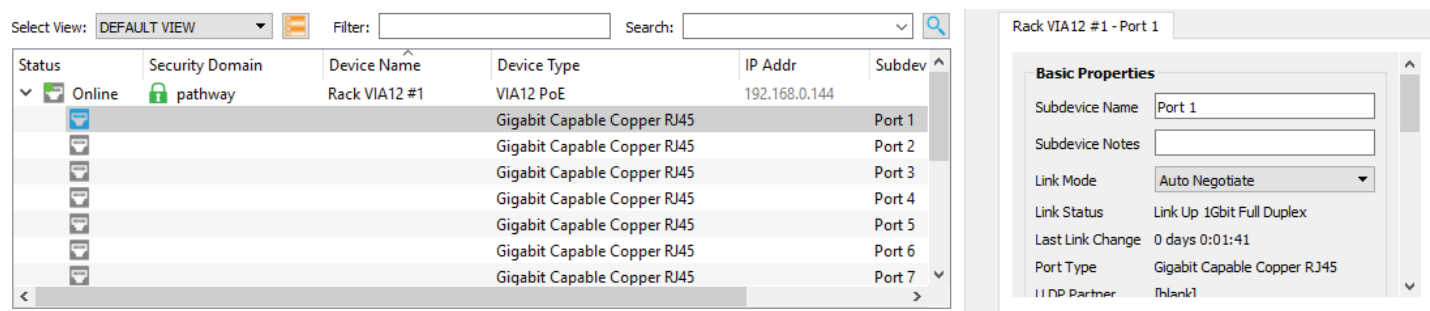


FRONT PANEL LOCKOUT

If the switch has **Front Panel Lockout** enabled, you will not be able to make changes from the front panel. To address this, there is a 30-second delay before the LCD Lockout takes effect, after the switch boots up. First, hard reboot the switch (unplug and re-plug the AC power source), and then within 30 seconds after the switch has booted up, perform the above action. After 30 seconds, the front panel UI will be locked out again.

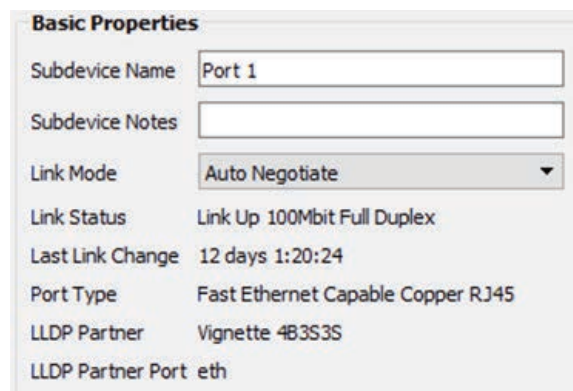
PORT PROPERTIES AND CONFIGURATION

Port status and properties may be reviewed by expanding the device in the device tree, and clicking on the subdevice/port. The properties for that port will then be shown in the Properties Panel.



The following fields are shown in the subdevice/port properties panel. Some are editable, while others are read-only.

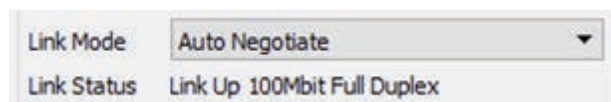
BASIC PROPERTIES



Property	Description
Subdevice Name	Name of the port. Default is the port number. User-defined.
Subdevice Notes	Additional notes. User-defined.

Property	Description
Link Mode	<p>Disable: Disables the port.</p> <p>Auto Negotiate (default, recommended): Allows the switch and the connected device to determine the fastest mutually supported connection speed. Read-only.</p> <p>10Mbit Half Duplex</p> <p>10Mbit Full Duplex</p> <p>100Mbit Half Duplex</p> <p>100Mbit Full Duplex</p> <p>1Gbit Full Duplex</p> <p>10Gbit Full Duplex (SFP+ Ports Only)</p>
Link Status	Shows the status of the link (up or down) and the link mode. Read-only.
Last Link Change	Displays the time elapsed since the last change in the Port Link Status, i.e. connected or disconnected. Shown as X Days, HH:MM:SS (Hours : Minutes : Seconds).
Port Type	Shows the type of port currently selected (e.g. Gigabit Capable Copper RJ45 or Gigabit Capable Fiber). Read-only.
LLDP Partner	If the connected device supports Link Layer Discovery Protocol (LLDP), such as Vignette devices, Pathport gateways and other VIA switches, the connected device's name will appear here. Read-only.
LLDP Partner Port	<p>If the connected device supports Link Layer Discovery Protocol (LLDP), this will show the Port Number on that device that this port is connected to.</p> <p>If the connected device is not a switch and has only one port, this will show "Eth".</p>

LINK MODE



Allows review and editing of the port's communication speed.

Auto-negotiation allows the switch and the connected device to determine the fastest mutually supported connection speed. However, there are some situations where, due to poor cabling, interference or traffic congestion, ability to force the connection to a particular speed is desirable.

For copper RJ45 ports, the range is from 10Mb Half Duplex (a common value for older gateways) to 1Gbit Full Duplex. The port may also be disabled.

NOTE: It is not possible to force a device to connect at a speed faster than the device's network interface hardware will support.

For SFP+ ports, the Link Mode has only two options: **1G Full** or **10G Full** (Duplex).



LLDP PARTNER

LLDP Partner VIA 16

Link Layer Discovery Protocol (LLDP) is an industry-standard method for device announcement and reporting described in the IEEE 802.1AB standard. Any Ethernet-aware device may announce itself using LLDP, not just switches. This feature is particularly useful when using VLANs as you can tell which device is connected to a port, even if the port is not on the management VLAN.

For Pathway devices supporting LLDP, the name shown in the LLDP Partner field will be the device's name, as configured in Pathscape. Other LLDP-enabled devices may return different information.

NETWORK PROPERTIES

Network Properties

Forwarding State Forwarding all traffic

Bandwidth Percentage 1

Property	Description
Forwarding State	Traffic forwarding state of the port: Forwarding all traffic, Blocked by RSTP (detecting a loop), or blocked by Ring Protect (EAPS). RSTP or EAPS must be active. Read-only.
Bandwidth Percentage	Shows the bandwidth used on the selected port. Bandwidth is relative to the port speed as negotiated with the link partner, i.e. if the port is set to 100Mbit, a bandwidth usage of 55% is equal to approximately 55Mbit of traffic per second. Read-only.

FORWARDING STATE

Network Properties

Forwarding State Forwarding all traffic

Shows the forwarding state for the selected Port. Typically, this will show "Forwarding all traffic".

If RSTP is enabled and a network loop is detected, RSTP will block the port that is creating the loop. In this case, the Forwarding State will be shown as "Blocked by RSTP".

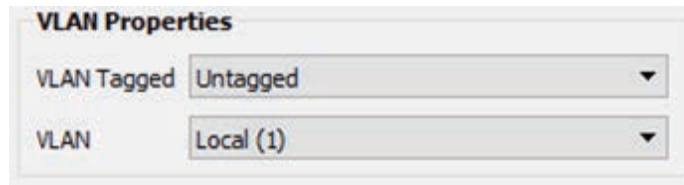
When EAPS is in use and the ring is healthy, the secondary port will report "Blocked by Ring Protect (EAPS)".

BANDWIDTH PERCENTAGE

Bandwidth Percentage 2

Shows, as a percentage value, the bandwidth used on the selected port. Bandwidth is relative to the port speed as negotiated with the link partner, i.e. if the port is set to 100Mbit, a bandwidth use of 55% is equal to approximately 55Mbit of traffic per second.

VLAN PROPERTIES



Property	Description
VLAN Tagged	<p>Untagged (default): Only data belonging to the port's specified VLAN ID# will be transmitted. Typically set when connected to end equipment.</p> <p>Tagged/Uplink: All traffic on all VLANs will be transmitted. Typically set when connected to another switch.</p>
VLAN	Assigns the selected port to the specified VLAN.

Once VLANs are enabled and the VLAN range is set, by default a port is set as **Untagged** with a VLAN ID# of 1, or the lowest ID# of the VLAN range.

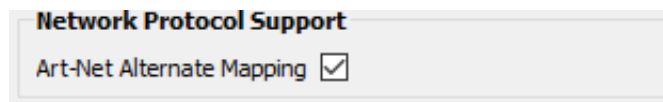
Ports set as Untagged only transmit data packets in the VLAN specified by the ID# and are typically connected to end equipment.

Ports set as **Tagged/Uplink** do not require a VLAN ID#, and this option will not be shown. Tagged ports transmit all data packets regardless of the packet's VLAN ID. Tagged ports should only be connected to other tagged ports, typically on other switches. **Do not connect Pathport gateways or other devices like computers unless you have specifically configured your Ethernet port to receive tagged data (advanced network setup only).**

Generally, a Tagged port on one switch should not be connected to an Untagged port on another switch.

NETWORK PROTOCOL SUPPORT

ART-NET ALTERNATE MAPPING



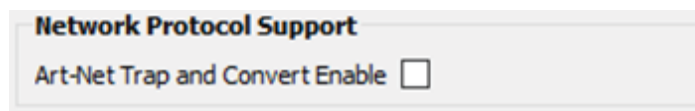
This feature is used in conjunction with the “**Art-Net Trap-and-Convert to sACN**” feature. **It is a device parent-level property;** it is enabled across the entire device. The Art-Net Trap and Convert property can be enabled on a port-by-port basis.

It does not affect unicast Art-Net packets.

The Art-Net protocol uses two hexadecimal numbers, a ‘subnet’ and a ‘universe’, to define its DMX universe numbering. Numbering is usually shown as # - # and the valid range is from 0 - 0 (zero-zero) to F- F.

However, most other common protocols, including sACN, do not have a universe ‘zero’. The issue is compounded because some early Art-Net implementations are shown in a straight decimal representation (1, 2, 3, 4...) without any indication if “1” corresponds to Art-Net universe 0-0 or to 0-1. **Art-Net controllers are strongly urged not to transmit on 0-0.**

By default, Art-Net Universe 0-0 is ignored by the VIA and the packets discarded. When Alternate Art-Net Mapping is enabled, VIA switches will map Art-Net Universe 0-0 to sACN Universe 1. When Alternate Art-Net Mapping is disabled, Art-Net Universe 0-0 will be ignored by the VIA and Art-Net Universe 0-1 will be routed as sACN Universe 1.



Property	Description
Art-Net Trap and Convert Enable	When enabled, Art-Net data packets with broadcast address destinations are trapped and converted to E1.31 sACN multicast packets, as the packets enter the port of the switch. The resulting sACN packets may then be filtered using the IGMP settings.

Art-Net Trap and Convert is a port-level property; it can be enabled on a port-by-port basis.

When enabled, Art-Net data packets with broadcast address destinations are trapped and converted to E1.31 sACN multicast packets, as the packets enter the port of the switch. The resulting multicast sACN packets may then be filtered using the IGMP settings. All other Art-Net broadcast packets, such as ArtPoll, are discarded. Depending on the amount of Art-Net data traffic, this operation could significantly improve bandwidth usage efficiency and reduce the amount of unnecessary traffic seen by end devices.

The Art-Net packet will be converted to the analogous sACN universe. Due to how Art-Net universes are numbered, there is the possibility of an off-by-one error. Change the “Art-Net Alternate Mapping” option should the universe mapping seem incorrect.

Although performance depends on DMX frame rate, conversion of no more than 48 Art-Net universes by one VIA at one time is recommended.

When this feature is disabled, Art-Net data will be routed as normal broadcast traffic to all devices on the current VLAN.

PoE PROPERTIES (NOT SHOWN ON VIA12 MODEL 6750)

POE Properties

PoE Enabled ▾

PoE Status Class 2 (7 W)

PoE Active Draw (W) 1.52

PoE Power Allocation (W) 7

PoE Max Allocation 15.4W ▾

PoE Power Cycle

Property	Description
PoE	Enabled by default, this option allows the user to completely disable PoE on a given port. Any PoE allocation set with the following parameter will be ignored. Ports 1-12 only.
PoE Status	The PoE class as reported by connected device. Read-only. Not Detected: not a PoE device Class 0: No class reported, 15.4W draw assumed Class 1: Uses up to 4W Class 2: Uses up to 7W Class 3: Uses up to 15.4W
PoE Active Draw (W)	Consumption as reported by the PoE controller, in watts.
PoE Power Allocation (W)	Reports the maximum draw, in watts, allowed by the PoE class, or the limit set by the user, whichever is less.
PoE Max Allocation	Sets the PoE allocation for the port. Default is 15.4W, regardless of the size of the power supply. Allocation options range from 0.9W to 15.4W, in 900mW increments.
PoE Power Cycle	Pressing this button will disable and then re-enable PoE on the selected port, in order to power cycle the end device.



PoE MAX ALLOCATION

PoE Max Allocation	15.4W
--------------------	-------

Allows you to set an upper limit to the power available to a connected device, such as a Pathport gateway or Vignette wall station. Use Max Allocation to ensure critical devices will have power. Also use Max Allocation to compensate for Class 0 device power allocation; many older PoE devices cannot report their class. The switch automatically treats these devices as Class 0 and allocates the full, default 15.4W to their ports.

If Maximum Allocation for every port is left at 15.4W, PoE is allocated by the switch: a) when the switch is powered up, PoE is allocated starting with Port 1, then port-by-port through the last port; or b) PoE is allocated on a first-come, first-serve basis, dependent on the order links become active.

SFP/SFP+ TRANSCEIVER (SFP+ PORTS ONLY)

SFP+ Module Type	10GBASE-SR
Port Type	Gigabit Capable Fiber

Property	Description
SFP+ Module Type	<p>Shows the detected SFP/SFP+ Transceiver type.</p> <p>Not Detected: No module inserted</p> <p>Not Support: Module is not compatible/supported</p> <p>1000Base-SX: Module is recognized as 1000Base-SX</p> <p>1000Base-LX: Module is recognized as 1000Base-LX</p> <p>10GBase-SR: Module is recognized as 10GBase-SR</p> <p>10GBase-LR: Module is recognized as 1000Base-LR</p> <p>Dual Rate 1/10G Multi Mode: Module is recognized as dual rate 1G/10G Multimode type</p>

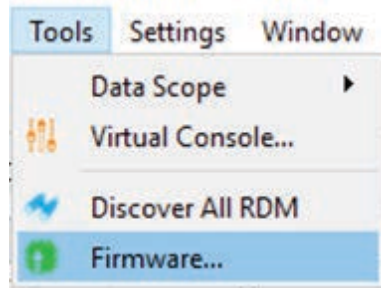
See **Appendix 1: SFP Fiber Adapter Selection** for more information on choosing an appropriate SFP/SFP+ Fiber Transceiver.

UPGRADING DEVICE FIRMWARE




Firmware upgrades may only be done using Pathscope.

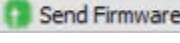
The most recently released firmware is bundled with the most recent version of Pathscope. To ensure you have the most up-to-date firmware available for upgrading, ensure you have downloaded the most recent version of Pathscope from the Pathway site, <https://www.pathwayconnect.com>.

To upgrade a VIA switch, ensure the device's IP address is configured correctly and is on the same subnet and IP range as the computer. Open Pathscope, click the Tools menu, then select Firmware...



This will bring up the Firmware Update window.

 Rack Vignette Clock	Vignette Clock	10.61.9.44	5.0.4	5.0.4	Up to date.
 VIA8	VIA8, eDIN	10.30.132.120	5.0.4	5.0.4	Up to date.
 Vignette 4B3S3S	Vignette PoE Station	10.61.9.12	5.0.4	5.0.4	Up to date.

Select the device(s) you want to upgrade and click the **Select Latest** button at the bottom of the window. The latest firmware version will be shown in the table next to **Current**. Click the  **Send Firmware** button and wait for the progress bar(s) to finish. After the device(s) reboot, the firmware will be updated.

WARNING: Be careful when updating firmware on multiple devices at once.

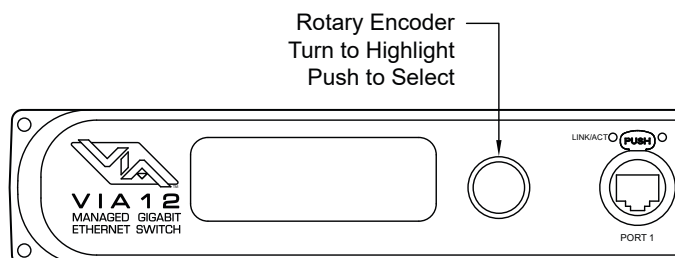
It is strongly recommended that you do not update VIA Switches and connected PoE devices at the same time. It is possible for the firmware update process to reboot the Switch before the data has finished writing to the PoE devices' memory. If the VIA Switch reboots at this point, the connected PoE devices' power will be cut off, and could be rendered inoperable, in a "bricked" state.

It is advised to update the Switch first, wait for it to reboot, and then update the connected PoE devices, or vice versa.

FRONT PANEL UI AND MENU

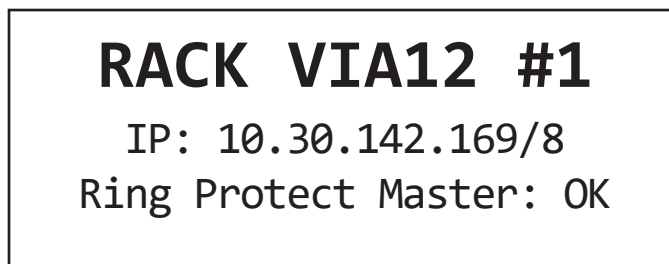
The VIA12 models 6750, 6750-P, 6752-P and 6754-P feature a front panel UI, consisting of an LCD and a rotary pushbutton encoder for navigating menus and selecting options.

If configuring the switch via a PC and Pathscape is not possible or practical, it is still easy to do using the front panel UI. This section will show the menu structure and descriptions of menu options.



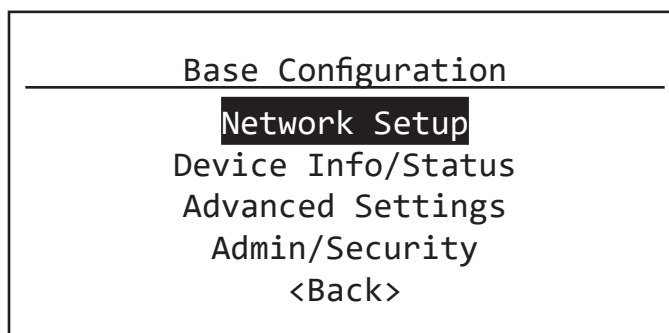
MAIN DISPLAY MESSAGES

When idle, the main LCD will show the switch soft label (Name) and its IP address. If the Ring Protect feature is enabled, it will also display status of the Ring.



USING THE FRONT PANEL UI

With the main screen (above) showing on the LCD, press in the encoder knob. The base configuration menu will be shown.



Turn the knob to scroll up or down the menu. The currently selected menu item is shown in **White on Black**. Push the knob to enter sub-menus. Top-level menu entries are shown above.

For all menus and submenus, the current selection will be highlighted in **White on Black**. Push the encoder knob to reach further options, or to select the currently selected item. If choosing from a list of options, the currently enabled option will be shown with asterisks on either side of it, e.g. *** Current Property Value ***.

Some menus, such as Network Settings, require the user to scroll down to accept or discard any changes made. The **<Back>** option will always move the menu up one level. The current menu will time out after approximately 30 seconds.

FRONT PANEL LOCKOUT

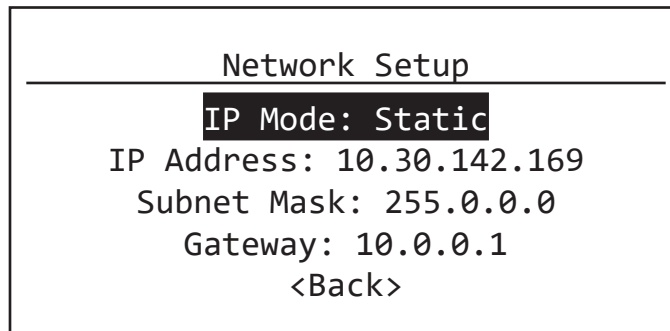
If using Pathscape, it is possible to enable the option **Front Panel Lockout**, which disables the ability to make any changes to the switch from the front panel UI. You can still navigate the menus to review settings, but cannot change any properties.

The Front Panel Lockout is temporarily disabled for 30 seconds after the switch boots up. This window allows for changes to be made when a Pathscape connection is not available.

NOTE: It is not possible to disable the Front Panel Lockout from the front panel itself; it must be done from Pathscape.

MENUS

NETWORK SETUP



This menu allows review and changes to the switch IP mode, IP address, subnet mask, and default gateway. These settings are the default values for the Management VLAN (typically VLAN 1) and will be used if VLANs are disabled. Scroll the encoder knob to highlight the property you want to edit, and push the knob to edit the value. Scroll the knob again to choose the new value, and push the knob to confirm.

Depending on the item you are editing, you may have to scroll down to select the **<Back>** option to return to the previous menu, or select **Save and Apply** to confirm. In some menus you may also select **Discard Changes** to return to the previous menu without committing changes.

Menu Item	Description
IP Mode	<p>Determines how the VLAN's IP settings will be obtained.</p> <p>Static (default for VLAN 1): IP Settings manually set by user.</p> <p>Dynamic: IP Settings will be obtained from a DHCP server.</p> <p><Back>: Return to previous menu</p>
IP Address	<p>Manually sets IP address (IPv4).</p> <p>Turn encoder to set each octet. Push to accept and move to next octet. Illegal values are not accepted.</p>



Menu Item	Description
Subnet Mask	Set subnet mask to be used by the management processor. Only valid masks are shown. Turn knob to select from list of valid masks.
Gateway	Set default gateway for the management processor. Only valid gateways are accepted. Turn knob to set each octet. Push to accept. Illegal values are not shown. Gateways will need to be set for access to the Internet for SixEye Cloud Management.
<Back>	Return to previous menu.

IP Mode must be set to “Static” if the VIA is to act as a DHCP server on the current VLAN. Setting the IP Mode to “Dynamic” does NOT enable the DHCP server. DHCP service is enabled under Advanced Settings > VLAN Setup > VLAN Config > VLAN <#> DHCP Server. **NOTE: each VLAN should only have one DHCP server.**

If the IP Mode is set to “Dynamic” on a system with no active DHCP server, the switch will auto-generate IP settings in accordance with zeroconf standards, in the IP range of 169.254.x.x/16. This range may not be suitable for connection to entertainment systems.

When IP Mode is set to “Dynamic”, it is still possible to manually adjust the IP settings. This practice is not recommended as the changes will not stick.

Once the values have been set, acceptance options appear on the bottom line of the screen. By default, **Discard Changes** will be highlighted. Click the knob to cancel and return to previous menu. Turn the knob to select **Save and Apply** to save changes and return to the **Network Setup** menu.

DEVICE INFO/STATUS

This menu allows review of several device properties. These are non-editable.

Device Info/Status
Serial #: PPXXXXXXX MAC: XX:XX:XX:XX:XX:XX Firmware Version: 5.0.4 PoE Used: 7.0W PoE Allocated: 50.0W PoE Remaining: 50.0W <Back>

Menu Item	Description
Serial #	Factory-assigned, Pathway serial number. Read-only.
MAC	Factory-assigned media access control (MAC) address. Read-only.
Firmware Version	Current operating firmware version. Firmware may be updated using Pathscape. Read-only.
Ring Protect State (if enabled)	OK: Ring is intact Init: Ring is initializing Failed: Link between two ports has failed. Communication now relies on secondary links. Fault should be located and repaired immediately.
PoE Used	Total Power-over-Ethernet being drawn by all connected devices, in Watts.
PoE Allocated	Total current Power-over-Ethernet budgeted to all ports, in Watts
PoE Remaining	Total unallocated Power-over-Ethernet available from PoE power supply
<Back>	Returns to previous menu

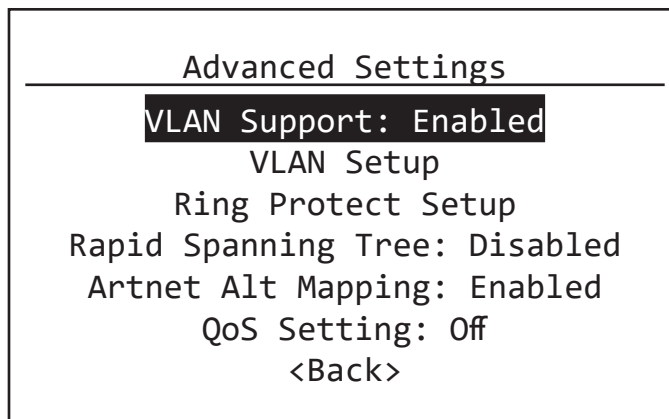
IMPORTANT: VIA model **6750** hardware does not support PoE. **Connected PoE-enabled devices will not receive power from the switch.**

VIA models 6750-P, 6752-P and 6754-P have 100W of on-board PoE power. Connecting PoE-enabled devices will allow them to be powered by the switch.



ADVANCED SETTINGS

This menu contains advanced settings pertaining to VLANs, Ring Protect, Rapid Spanning Tree, Art-Net Alternate Mapping, and QoS (Quality of Service). There are several sub-menus here for VLAN Setup and Configuration.



Menu Item	Description			
VLAN Support	Disabled (default) Enabled. Must be enabled to show VLAN Setup and Ring Protect feature.			
VLAN Setup	VLAN Range Start: <x>	Specifies lowest VLAN ID# available. Valid range: 1 to 4095. Default is 1 .		
	VLAN Range End: <x>	Specifies highest VLAN ID# available. Valid range: 1 to 4095. Default is 10 .		
	Management VLAN: <x>	Specifies the VLAN ID# used by the management processor. Default is 1 . This value MUST be within the range specified by the VLAN Range Start and VLAN Range End properties (above) or you will not be able to configure the switch.		
	VLAN Config/Status	VLAN ID#	Network Setup	See below
			DHCP Server (available if IP Mode set to Static)	Disabled (default) Enabled
IGMP Snooping			Disabled (default) Enabled	
IGMP Querier			Disabled (default) Enabled	
Ring Protect Mode	Disabled (default): Ring is turned off. Master: Switch with master responsibility for monitoring Ring. Only one Master is allowed. Transit: All other switches are set at Transit.			
Ring Protect Setup	Primary Port: <x>	Designates which port to use as the active uplink port to other switches. Valid range is port 11 through 14 only.		
	Secondary Port: <x>	Designates which port to use as the fall-back link to other switches. Valid range is port 11 through 14 only.		



Menu Item	Description	
Ring Protect Setup	Control VLAN: <x>	Specifies the VLAN ID# used to determine the integrity of the ring. It may not be used for any other traffic. Valid ID# is any ID <i>outside</i> the range set in VLAN setup. Default is VLAN 4095 .
Rapid Spanning Tree	Enabled (Default) Disabled	
ArtNet Alt Mapping	Art-Net Alternate Mapping. Enabled (Default) Disabled	
QoS Settings	Quality of Service Settings. Off (Default) Standard Date Strict	
<Back>	Returns to previous menu.	

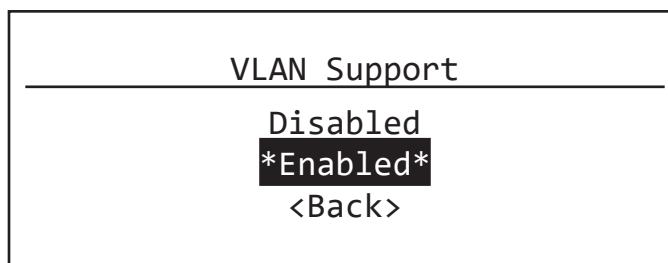
Plan your VLAN layout before attempting configuration. The creation of a map of the network, showing which devices and which ports to associate with a given VLAN, is strongly recommended prior to configuration.

EXTREMELY IMPORTANT NOTE: When configuring one or multiple VIA switches using Pathway's software-based configuration tools, be certain all switches are set to the same Management VLAN ID#. Be certain that the port connected to your computer is also connected to a VIA port on the same VLAN ID#. Failure to observe this rule will result in what appears to be a broken network.

For more information on VLANs and definition of terms, see **Appendix 2: Virtual Local Area Network (VLAN)**.

VLAN SUPPORT

VLAN Support must be enabled to allow access to the **Ring Protect, IGMP and DHCP** features and to the **VLAN Setup** and **VLAN Config** menus. Once Ring Protection is enabled, VLAN support cannot be disabled.



VLAN SETUP

These properties determine the size of the VLAN table, and which VLAN has communication with the switch management processor. For efficient switch operation, the VLAN range should be kept as small as necessary.

```

VLAN Setup
-----
VLAN Range Start: 1
VLAN Range End: 10
Management VLAN: 1
VLAN Config/Status
<Back>
    
```

If the **Management VLAN** is accidentally set to a value outside the VLAN range, it may be necessary to use the **Factory Default** function from the **Utilities** menu to restore communication with the management processor and allow further configuration.

VLAN CONFIG/STATUS: VLAN ID#

Each VLAN is identified by its VLAN ID#.

Each VLAN ID# must be configured separately, and each switch must be uniquely identified on each VLAN in use on that switch. There is currently no way of copying properties from one VLAN to another.

```

VLAN Config/Status
-----
VLAN 1
VLAN 2
VLAN 3
VLAN 4
...
<Back>
    
```

```

VLAN 1
-----
Network Setup
DHCP Server: Disabled
IGMP Snooping: Disabled
IGMP Querier: Disabled
Current Multicast Groups
<Back>
    
```

The VLAN ID# is assigned to individual ports from the Port Configuration menu (see below for **Port Status and Configuration Menu**).



VLAN CONFIG/STATUS: NETWORK SETUP

This menu operates the same as the switch's main **Network Setup** menu. Configure these for each VLAN ID#.

Network Setup
IP Mode: Static
IP Address: X.X.X.X
Subnet Mask: X.X.X.X
Gateway: X.X.X.X
<Back>

Menu Item	Description
IP Mode	<p>Determines how IP settings will be obtained.</p> <p>Disabled (default): No IP assigned.</p> <p>Static: IP Settings manually set by user.</p> <p>Dynamic: IP Settings will be obtained from a DHCP server.</p> <p><Back>: Return to previous menu</p>
IP Address	<p>Manually sets IP address (IPv4).</p> <p>Turn encoder to set each octet. Push to accept and move to next octet. Illegal values are not accepted.</p>
Subnet Mask	<p>Set subnet mask for VLAN. Only valid masks are shown.</p> <p>Turn knob to select from list of valid masks.</p>
Gateway	<p>Set default gateway for VLAN. Only valid gateways are accepted.</p> <p>Turn knob to set each octet. Push to accept. Illegal values are not shown. Gateway setup is needed for Internet access for SixEye Remote Monitoring and Management.</p>
<Back>	<p>Return to previous menu.</p>

Network Settings must be configured on all VLAN requiring use of multicast filtering (IGMP) or a DHCP server. By default, only the management VLAN (VLAN ID#1 by default) is automatically assigned an IP and subnet mask. All other VLANs default to a null IP address value (0.0.0.0). From the Network Settings for each VLAN, assign a unique IP per switch, a common subnet mask and, where necessary, a default gateway.

Typically, Internet access will be through a proxy or NAT gateway, in which case the default gateway IP should point to this device.

IP Mode must be set to "Static" if the VIA is to act as a DHCP server. Only one DHCP server may be active on any given VLAN. Setting the IP Mode to "Dynamic" does NOT enable the DHCP server – see below.

If the IP Mode is set to “Dynamic” on a system with no active DHCP server, the switch will auto-generate IP settings in accordance with zeroconf standards, in the IP range of 169.254.x.x/16. This range may not be suitable for connection to entertainment systems

VLAN CONFIG/STATUS: DHCP SERVER

VIA switches can automatically assign IP addresses to connected devices, using a DHCP (Dynamic Host Configuration Protocol) server.

IMPORTANT: Only one DHCP server may be active on any given VLAN at one time. Running multiple DHCP servers will cause network reliability problems.

The DHCP-hosting VIA switch *must first be set to a static IP* address on the desired VLAN, prior to enabling the DHCP server. The DHCP server should be enabled prior to setting other connected devices to a “**Dynamic IP**” mode or being connected to the network VLAN.

In some cases, it may be necessary to reboot connected devices to ensure the DHCP server correctly recognizes them and assigns appropriate network settings.

```

DHCP Server
-----
Pool Start: X.X.X.X
Pool End: X.X.X.X
Server Config: Valid
Enable Server and Exit
Exit
    
```

Menu Item	Description
Disabled	DHCP Service is turned off. Use this setting for all static (manually-set) IP systems, and for all switches other than the VLAN’s designated DHCP server host. To enable DHCP , click the knob in and set up the DHCP Pool Start and End, as below.
Enabled	Enables DHCP server. Requires setting valid DHCP Pool Start and End values and selecting the Enable Server and Exit menu item. Pool Start: Set the first available IP address. Turn the knob to set each octet, and click the knob to confirm and move to the next octet. Pool End: Set the last available IP address. Turn the knob to set each octet, and click the knob to confirm and move to the next octet. The DHCP pool is partially predefined based on the IP address and subnet mask of the host switch, as the host must have proper communication with the requesting device. Invalid pool ranges are not accepted.



Menu Item	Description
Server Config	Shows if currently entered DHCP Server Pool entries are valid. This property is not editable, it is simply a check to ensure DHCP Server is setup correctly. Valid: Pool range is valid and can be applied. Invalid: Pool range is invalid. Try again.
Enable Server and Exit	Accept the designated pool and start the DHCP Service. Option only available if the Server Config is valid.
Revert and Exit	Abandon configuring the DHCP server and return to previous menu.
Disable Server and Exit	Turn DHCP server off. Warning: Devices relying on dynamically-obtained IP addresses require an active DHCP server to function.

VLAN CONFIG/STATUS: IGMP AND MULTICAST GROUPS

When using multicast data packets, such as streaming ACN (sACN), bandwidth efficiency may be improved by using IGMP (Internet group management protocol) to enable multicast filtering.

```

VLAN 1
-----
IGMP Snooping
IGMP Querier: Disabled
Current Multicast Groups
<Back>

```

Menu Item	Description
IGMP Snooping	Allows the switch to correctly filter multicast traffic. Disabled (Default) Enabled (Each switch having devices that can use IGMP should have this enabled)
IGMP Querier	Creates the multicast tables used by IGMP Snooping. Disabled (Default) Enabled (Each network should have two Queriers)
Current Multicast Groups	Shows the table of multicast groups in use on the VLAN. Use the knob to scroll through the list and click the knob on a group to see which ports are subscribers to that group.
<Back>	Return to previous menu.

The IGMP Querier establishes a table of active multicast groups by querying connected devices about which multicast groups each device wishes to join. For example, a gateway will request the multicast groups associated with the sACN universes that the gateway is patched to.

Each switch operating an IGMP Querier on a VLAN must have valid IP settings on that VLAN. The IP settings may be static or dynamically established using the DHCP.

IMPORTANT: Two IGMP queriers should be active on each VLAN using multicast filtering. If no querier is active, the groupings table will fail after approximately five minutes and filtering will only work erratically or will fail altogether. IGMP should not be enabled on more than four VLANs per switch.

The IGMP Snooper allows the switch to more efficiently route multicast traffic by applying the multicast groupings as a filter. Multicast traffic is only directed to only those ports, i.e. end devices, that have requested to receive that traffic.

The Current Multicast Groups is a list of the multicast addresses currently maintained in the Querier’s table. The list provides a troubleshooting check. Click on a listed group to see what ports are requesting that address. For example, the multicast groups 239.255.237.1, 239.255.237.2 and 239.255.237.255 indicate traffic between Pathport devices, and all ports connected to Pathports (on that VLAN) should be shown.

RING PROTECT SETUP

VIA ring protection configured here enables **EAPS**. This automatic protection system can detect a break in the ring and heal it in milliseconds. Once your network has been setup and is stable, for speedy redundancy during show situations, it is best to use EAPS vs RSTP (see below for RSTP setup). This option will only be shown if VLAN support is enabled.

WARNING: Ring Protection should only be configured and enabled after all other VLAN configuration has been completed.

```

Ring Protect Setup
-----
Ring Protect Mode: Disabled
Primary Port: 13
Secondary Port: 14
Control VLAN: 4095
<Save and Apply>
<Discard Changes>
    
```

Menu Item	Description
Ring Protect Mode	Shows the current state of the switch. Press knob to change between: Disabled (Default): Ring Protection feature is turned off. Master: Set switch as the Master. Only one switch should be set as Master. All other switches should be set as Transit switches. Transit: Set switch as a Transit switch.
Primary Port: <x>	Designates which port to use as the active uplink port to other switches. Valid range is the last four ports of the switch.
Secondary Port: <x>	Designates which port to use as the fallback link to other switches. Valid range is the last four ports of the switch.



Menu Item	Description
Control VLAN: <x>	Specifies the VLAN ID# used to determine the integrity of the ring. This VLAN may not be used for any other traffic. Valid ID# is any ID <i>outside</i> the range set in VLAN setup. Default is VLAN 4095 .
<Save and Apply>	Saves current settings and returns to previous menu.
<Discard Changes>	Discards current changes and returns to previous menu.

During the set up and configuration of the Ring Protection feature, communication between devices may be erratic or broken. We strongly recommend that all switches be configured with the appropriate Ring Protection settings **PRIOR** to be connected together. We also strongly recommend that all switches be disconnected from one another **PRIOR** to disabling the ring feature.

Prior to set up, determine which switch will be the master. **Generally, the least busy switch with the most stable power source is the best choice.** All other switches must be configured as transit switches.

All switches must have both a primary and a secondary ring port set. These ports will be automatically configured as Tagged (uplink) ports, meaning all traffic on all VLANs will be passed through the ports.

If changes are made to the ring configuration while the ring is active, it may be necessary to reboot all switches for the changes to take effect.

RAPID SPANNING TREE

The Rapid Spanning Tree algorithm detects and prevents network loops. The interaction between RSTP and the Ring Protect system may cause long network reconfiguration times when the ring topology is changed. For this reason, it is recommended that RSTP be used during setup and then disabled after verifying there are no loops present. EAPS ring protection (see above) is much faster than RSTP and should be used during performances.

WARNING: Rapid Spanning Tree must be enabled on all switches to detect loops correctly. Network loops created through un-managed switches may not be detected correctly. Pathway's implementation of Rapid Spanning Tree Protocol is interoperable with other switch manufacturer's implementations.

Menu Item	Description
Rapid Spanning Tree	Turn Rapid Spanning Tree on or off. Disabled (Default) Enabled
<Back>	Return to previous menu.

For more information, please refer to **Appendix 5: Rapid Spanning Tree Protocol**.

ART-NET ALTERNATE MAPPING

This feature is used in conjunction with the **Art-Net Trap-and-Convert** option, which is set from the Port Configuration menu. This feature does not affect unicast Art-Net packets.

Menu Item	Description
ArtNet Alt Mapping	Turn Art-Net Alternate Mapping on or off. Enabled (Default) Disabled
<Back>	Return to previous menu.

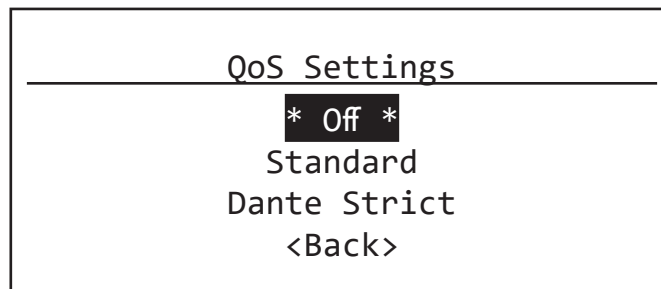
The Art-Net protocol uses two hexadecimal numbers, a 'subnet' and a 'universe', to define its DMX universe numbering. Numbering is usually shown as # - # and the valid range is from 0 - 0 (zero-zero) to F- F.

However, most other common protocols including sACN do not have a universe 'zero'. The issue is compounded because some Art-Net implementations are shown in a straight decimal representation (1, 2, 3, 4...) without any indication if "1" corresponds to Art-Net universe 0-0 or to 0-1.

By default, Art-Net Universe 0-0 is ignored by the VIA and the packets discarded. When Alternate Art-Net Mapping is enabled, VIA switches will map Art-Net Universe 0-0 to sACN Universe 1. When Alternate Art-Net Mapping is disabled, Art-Net Universe 0-0 will be ignored by the VIA and Art-Net Universe 0-1 will be routed as sACN Universe 1.

QoS (QUALITY OF SERVICE)

Quality of Service determines the relative priority of different data packets, which in turn determines which packets should receive preferential routing from a VIA switch. QoS is often used for the distribution of video and audio signals, including the Dante® audio standard, to meet the signal's required timing constraints. Please remember that giving all data high priority is the same as treating all traffic equally.





Menu Item	Description
Off (Default)	Disables QoS-based routing. All traffic is treated equally.
Standard	Traffic priority is observed using a weighted algorithm to ensure timely delivery of high priority traffic and eventual delivery of lower priority packets.
Dante Strict	Traffic priority is strictly observed, using Dante-specified weighting. Lower priority traffic may be dropped or ignored to ensure delivery of Dante's high priority packets
<Back>	Return to previous menu.

For more information, please refer to **Appendix 6: QoS Settings**.

UTILITIES

This menu contains menu items to Reboot and Factory Default the switch.

Utilities <hr/> Reboot Factory Default Default Including Net Setup <Back>
--

Menu Item	Description
Reboot	Restarts the switch with current configuration. This action must be confirmed before being applied. After confirmation, the knob will be locked out, and about 15-20 seconds will pass before the switch fully reboots.
Factory Default	Disables all VLANs and returns all properties to their default values, except any changes made to the network settings of VLAN #1 (base switch), which will be retained.
Default Including Net Setup	Disables all VLANs and returns all properties to their default values. The network settings of VLAN #1 (base switch) are also returned to their factory values.
<Back>	Return to previous menu.

PORT STATUS AND CONFIGURATION MENU

Port Status may be reviewed by turning to encoder knob to reach the desired port, from the main screen showing the switch name and IP address. The LCD shows the following information.

<Switch Name>
 IP: 10.30.142.169/8

<Port Name>
 Port <x>: <Link Speed>
 <VLAN ID#>

The port's soft label is shown on the top line. By default, the label is the port number. Below is shown the port number and the link status or speed. If VLANs are enabled, the bottom line shows the VLAN ID# currently assigned to the port.

From the Port Status screen of the desired port, push the button. The Port Configuration menu will be shown.

Port <x> Configuration

VLAN: Untagged (Normal)
 VLAN ID: <x>
 Artnet Input Handler: Pass All
 PoE: Enabled
 PoE Setup/Status
 Link Mode: Auto Negotiate
 LLDP Link Partner
 Bandwidth Use: 1%
 Current Multicast Groups
 <Back>

Some menu items may not be displayed; ie. VLANs, LLDP Link Partner, Current Multicast Groups, if VLANs are not enabled, or LLDP-compliant devices are not detected.

VLAN TYPE

VLANs must be enabled from the **Advanced Settings** menu for this option to be shown.

Menu Item	Description
Untagged (Normal)	Only data belonging to the port's specified VLAN ID# will be transmitted. Typically connected to end equipment
Tagged (Uplink)	All traffic on all VLANs will be transmitted. Typically connected to another switch.
<Back>	Return to previous menu.



Once VLANs are enabled and the VLAN range is set from the Base Configuration menu, by default a port is set as Untagged (Normal) with a VLAN ID# of 1, or the lowest ID# of the VLAN range.

Ports set as Untagged only transmit data packets in the VLAN specified by the ID# and are typically connected to end equipment.

Ports set as Tagged do not require a VLAN ID#, and this option will not be shown. Tagged ports transmit all data packets regardless of the packet's VLAN ID. Tagged ports are typically connected to other switches.

Generally, a Tagged port on one switch should not be connected to an Untagged port on another switch.

VLAN ID

The VLAN ID option is shown only for ports set as **Untagged**.

Menu Item	Description
VLAN ID#	Sets the VLAN tag used by the port. Only data packets belonging to this VLAN ID will be transmitted by the port. Property is only shown for Untagged ports. Only VLAN ID#s within the range defined in the VLAN Setup menu will be shown.
<Back>	Return to previous menu.

NOTE: It is not currently possible to set a soft label for VLAN ID# from the front panel. To set a soft label for VLAN ID, use Pathscope.

ARTNET INPUT HANDLER

This option is only shown for ports set as Untagged (Normal). This menu item is the same property as **Art-Net Trap and Convert**.

Menu Item	Description
Pass All	Art-Net data is routed as normal broadcast traffic to all devices on the current VLAN.
Convert	Art-Net data packets with broadcast address destinations are trapped and converted to E1.31 sACN multicast packets, as the packets enter the port of the switch. The resulting sACN packets may then be filtered using the IGMP settings. All other Art-Net broadcast packets, such as ArtPoll, are discarded.
<Back>	Return to previous menu.

Depending on the amount of Art-Net data traffic, this operation could significantly improve bandwidth usage efficiency and reduce the amount of unnecessary traffic seen by end devices.

The Art-Net packet will be converted to the analogous sACN universe. Due to how Art-Net universes are numbered, there is the possibility of an off-by-one error. Change the **Art-Net Alternate Mapping** option should the universe mapping seem incorrect.

Although performance depends on DMX frame rate, conversion of no more than 48 Art-Net universes by one VIA at one time is recommended.

To take advantage of IGMP, this feature assumes the DMX gateways can receive sACN instead of Art-Net.

PoE

Enabled by default, this menu item allows the user to completely disable PoE on a given port. Any PoE allocation set with the following parameter will be ignored.

Menu Item	Description
Disabled	PoE completely disabled for the selected port. PoE-enabled end devices will not receive power.
Enabled (Default)	PoE enabled for selected port.
<Back>	Return to previous menu.

PoE SETUP/STATUS

Allows review and management of power consumption used by devices running on Power-over-Ethernet (PoE).

<p>PoE Setup/Status</p> <hr/> <p>PoE: Class 2 PoE Used: 7.0W PoE Allocated: 10W Max PoE Allocation: 15.4W <Back></p>

Menu Item	Description
PoE: Class <x>	Shows the PoE Class as reported by the connected device. PoE: Not Detected: Not a PoE device Class 0: No Class reported. 15W Draw assumed Class 1: Uses up to 5W Class 2: Uses up to 10W Class 3: Uses up to 15W
Poe Used: <x>	PoE consumption, in Watts, as reported by the PoE controller.



Menu Item	Description
PoE Allocated: <x>	Reports the maximum draw allowed by the PoE class, or the limit set by the user, whichever is the lower amount.
Max PoE Allocation: <x>	Sets the PoE allocation for the port. Default is 15.4W . Allocation options range from 0.9W to 15.4W , in 900mW increments.
<Back>	Return to previous menu.

Except for Maximum Allocation, the PoE settings are not user-editable. The Maximum PoE Allocation allows you to set an upper limit to the power available to a connected device, such as a gateway. Use Maximum Allocation to ensure critical devices will have power. Also use Maximum Allocation to compensate for Class 0 device power allocation. Many older PoE devices cannot report their class. The switch automatically treats these devices as Class 0 and allocates the full, default 15.4W to their ports.

If Maximum Allocation for every port is left at 15.4W, PoE is allocated by the switch: a) when the switch is powered up, PoE is allocated starting with Port 1, then port-by-port through port 12; or b) PoE is allocated on a first-come, first-serve basis, dependent on the order devices are plugged into the switch.

IMPORTANT NOTE: VIA model 6750 does not have hardware to support IEEE 802.3af Power-over-Ethernet. Any PoE-enabled devices connected to a 6750 switch will not be powered. Models 6750-P, 6752-P and 6754-P have 100W of onboard PoE to power external devices.

LLDP LINK PARTNER

Link Layer Discovery Protocol (LLDP) is an industry-standard method for device announcement and reporting described in the IEEE 802.1AB standard. Any Ethernet-aware device may announce itself using LLDP, not just switches. The latest Pathport, Vignette and VIA firmware enables this protocol.

The information shown in the chart may be retrieved and shown on the VIA12's LCD, for each Pathport LLDP-enabled device connected to the switch, on a port-by-port basis. It can take up to 30 seconds for this menu item to appear once a link goes active. Other LLDP-enabled devices may return different information. **This property is only shown when a LLDP-compliant device is connected to the port in question.**

Menu Item	Description
Product Name	Device Name. For example, "Stage Left U1-8"
IP Address	Device IP Address
Subnet Mask	Device Subnet Mask
Gateway	Device Default Gateway
Manufacturer	Device Manufacturer. For example, "Pathway Connectivity"

Menu Item	Description
Device Model	Product Model name. For example, "Pathport OCTO"
Serial Number	Device Serial Number
Firmware Version	Current device operating firmware version
MAC Address	Device Media Access Control (MAC) Address

PORTS 1-12: LINK MODE

Allows review and editing of the port's communication speed.

```

Link Mode
-----
Disabled
*Auto Negotiate*
10M Half Duplex
10M Full Duplex
100M Half Duplex
100M Full Duplex
1G Full Duplex
<Back>
  
```

Menu Item	Description
Link Mode	<p>Disabled. Turns port off.</p> <p>Auto Negotiate (Default, recommended): Switch and connected device determine fastest mutually supported speed.</p> <p>10Mbit Half Duplex</p> <p>10Mbit Full Duplex</p> <p>100Mbit Half Duplex</p> <p>100Mbit Full Duplex</p> <p>1Gbit Full Duplex</p>
<Back>	Returns to previous menu.

Auto-negotiation allows the switch and the connected device to determine the fastest mutually supported connection speed. However, there are some situations where, due to poor cabling, interference or traffic congestion, ability to force the connection to a particular speed is desirable.



Range is from 10Mb – Half Duplex (a common value for older devices) to 1Gb – Full Duplex. The port may also be disabled.

NOTE: It is not possible to force a device to connect at a speed faster than the device’s network interface hardware will support.

BANDWIDTH USE

Shows bandwidth used on the selected port as a percentage value. Bandwidth is relative to the port speed as negotiated by the link partner, i.e. if the port is set to 100Mbit, a bandwidth use of 55% is equal to approximately 55Mbit of traffic per second.

This menu item is read-only.

CURRENT MULTICAST GROUPS

Displays a list of the multicast addresses used by the end device connected to the selected port.

It is not possible to block a specific multicast group. The menu list is read-only.

PORT 13 & 14: CONFIGURATION/STATUS: SFP+ PORTS

Ports 13 and 14 are SFP+ ports. These behave the in the same manner as ports 1-12 for configuration from the front UI menu, however have slightly different menu items.

```

Port <x> Configuration
-----
SFP Module: 10GBase-SR
Link Mode: 10G Full Duplex
VLAN: Tagged (Uplink)
Bandwidth Use: 1%
Current Multicast Groups
<Back>

```

Menu Item	Description
SFP Module	Shows the type of SFP/SFP+ module detected. Read-only. Not Detected: No module inserted Not Support: Module is not compatible/supported 1000Base-SX: Module is recognized as 1000Base-SX 1000Base-LX: Module is recognized as 1000Base-LX 10GBase-SR: Module is recognized as 10GBase-SR 10GBase-LR: Module is recognized as 10GBase-LR Dual Rate 1/10G Multi Mode: Module is recognized as Dual-rate 1/10G Multi-mode.

Menu Item	Description
Link Mode	<p>Disabled. Turns port off.</p> <p>1Gbit Full Duplex</p> <p>10G Full Duplex</p>
VLAN	<p>VLANs must be enabled in the Advanced Settings menu for this option to be shown.</p> <p>Untagged (Normal): Only data belonging to the port's specified VLAN ID# will be transmitted. Typically connected to end equipment.</p> <p>Tagged (Uplink): All traffic on all VLANs will be transmitted. Typically connected to another switch.</p>
LLDP Partner	<p>Shows LLDP Partner device attached to this port, if applicable.</p> <p>This property is only shown when a LLDP-compliant device is connected to the port in question.</p>
Bandwidth Use	<p>Shows bandwidth used on the selected port as a percentage value. Bandwidth is relative to the port speed as negotiated by the link partner, i.e. if the port is set to 1Gbit, a bandwidth use of 10% is equal to approximately 100Mbit of traffic per second.</p> <p>This menu item is read-only</p>
Current Multicast Groups	<p>Displays a list of the multicast addresses used by the end device connected to the selected port.</p> <p>It is not possible to block a specific multicast group. The menu list is read-only</p>
<Back>	Returns to previous menu.

The majority of these menu items are the same and function in the same way as on the RJ45 ports 1-12. The main difference is the **Link Mode** item, where you may choose between 1Gbit and 10Gbit only; as these are the speeds SFP/SFP+ support.



APPENDIX 1: SFP/SFP+ FIBER ADAPTER SELECTION

The VIA Gigabit switches allow the end user to provide a fiber adaptor. The adaptors are typically referred to as an SFP (Small Form Pluggable transceiver) or mini-GBIC (gigabit interface converter).

Pathway part number 6799 is an SFP 850nm Ethernet Optical Transceiver that is compatible with VIA12, VIA16 and VIA8, capable of 1Gbps. Part number 6798 is a dual-rate SFP+ 850nm Ethernet Optical Transceiver capable of 10Gbps, compatible with the VIA8 and VIA12 models 6750 and 6750-P. These fiber links can go up to 550 m (1800 feet) without issue. In some situations, the run lengths may lead you to choose a different SFP. Follow these guidelines when choosing your SFP:

1. The form factor must be stated as SFP or SFP+ (not XENpack or others).
2. The fiber connector is LC Duplex.
3. The SFP must support Optical Gigabit Ethernet (typically referred to as 1000BASE-SX, 1000BASE-LX, 10GBase-SR or 10GBase-LR)
4. The SFP must match the type of fiber installed, either Single Mode or Multi-Mode.
5. The SFP must support the distance required, which in turn determines the optical wavelength. 850nm is typically used for runs up to 550m, while 1310nm is typically used for runs up to 10km.

We strongly recommend each end of the connection use an identical SFP.

When the SFP module is inserted in the switch, the Link/Status LED will light up **green**. If an incompatible module is detected, the Link/Status LED will light up **red**. In Pathscope the Subdevice properties panel will indicate the link status, SFP module type, as well as the LLDP partner.

NOTE: The 6750 and 6750-P will work with 1000BASE-SX, 1000BASE-LX (1Gbps) and 10GBase-SR and 10GBase-LR (10Gbps) fiber modules.

The 6750 and 6750-P also support SFP+ 10G Direct Attach cables, both active and passive. This is often the easiest and lowest-cost solutions to connect multiple switches if they are close together.

When connecting a VIA to another manufacturer's switch using fiber, please bear in mind that some switches check the manufacturer's ID, as announced by the SFP module, and will only connect to a matching brand. VIA switches do not perform a manufacturer's ID check, and should work with any SFP module meeting the criteria above (Cisco, Finisar, Netgear, etc.)



APPENDIX 2: VIRTUAL LOCAL AREA NETWORK (VLAN)

A VLAN (Virtual Local Area Network) is a group of ports on the switch (or switches) that are configured to pass traffic to one another, but not to ports on any other VLAN. When multiple VLANs are established, some ports on the switch may need to be configured specifically to pass all VLAN traffic, to ensure overall traffic is routed correctly.

This feature allows the user to arrange lighting consoles, gateways and other network gear into groups of equipment. The usual purpose is to minimize unnecessary traffic to the equipment, or to segregate different types of equipment (lighting, audio, video) so that each network does not get flooded with superfluous data.

DEFINITIONS

The following terms are paired interchangeably in this manual: Normal and Untagged; Uplink and Tagged.

Normal/Untagged ports belong to a specific VLAN as configured by the user, and will only pass traffic that belongs to that VLAN. Typically connected to end equipment.

Uplink/Tagged ports pass all network traffic with VLAN “tags” within the VLAN range established for that switch (see Range Configuration below). Typically connected to other switches.

Tag refers to the marker added to (or removed from) the data packet as the packet enters or exits from a Normal/Untagged port on the switch. The “Tag” determines which VLAN the data packet is assigned to.

Management VLAN refers to the VLAN that the switch’s management processor is assigned to use. Care must be taken that the Management VLAN is used by at least one Normal/Untagged port on the switch, or the ability to configure the switch may be lost. It is strongly recommended that the Management VLAN be identical to the VLAN Range Start.

VLAN ID (ID#) is assigned to Normal/Untagged ports and determines which VLAN that port operates within.

A Normal/Untagged port may only be associated with one VLAN ID# at a given time.

SOFTWARE CONFIGURATION OF VLANs

VLANs may be configured using Pathscope software. Refer to the Pathscope documentation for in-depth configuration instructions.

When using software to configure the switch, make sure your computer is connected to a Normal (Untagged) port set to the same VLAN ID# as used by the management processor. Failure to do so will prevent configuration from being applied.

VLAN GUIDELINES

Plan the VLAN layout first. The creation of a map of the network, showing which devices to associate with which VLAN, is strongly recommended prior to configuration.

Generally speaking, ports connected to end devices will be configured as Normal/Untagged and given a VLAN ID#.

Ports connected to other VIA switches will typically be set as Uplink/Tagged, so multiple VLANs may be forwarded between switches, or when a VLAN must be forwarded through an intermediate switch (where that VLAN is not in use) on to a third switch beyond. It is possible to set the ports to Normal/Untagged, and given a VLAN ID#, in cases where it’s desirable to pass only one VLAN between switches, but this is not a normal practice.

When configuring VLANs, remember that each switch must be uniquely identified on each VLAN in use on that switch. By default, only the management VLAN is automatically assigned an IP and subnet mask. All other VLANs default to a null IP address value (0.0.0.0). Use the Network Configuration options available from the VLAN configuration screen to configure the desired IP settings for each VLAN.

APPENDIX 3: PLANNING CHARTS

VLAN PLANNING CHART

VLAN ID #	1	2	3	4
Label				
IP Address				
Subnet Mask				
Default Gateway				
IGMP Snooping				
IGMP Querier				
DHCP Server				
Art-Net Alternate Mapping				
QoS Level				

VLAN ID #	5	6	7	8
Label				
IP Address				
Subnet Mask				
Default Gateway				
IGMP Snooping				
IGMP Querier				
DHCP Server				
Art-Net Alternate Mapping				
QoS Level				



VLAN ID #	9	10	11	12
Label				
IP Address				
Subnet Mask				
Default Gateway				
IGMP Snooping				
IGMP Querier				
DHCP Server				
Art-Net Alternate Mapping				
QoS Level				

VLAN ID #	13	14	15	16
Label				
IP Address				
Subnet Mask				
Default Gateway				
IGMP Snooping				
IGMP Querier				
DHCP Server				
Art-Net Alternate Mapping				
QoS Level				

SWITCH PLANNING CHARTS

SWITCH LABEL:		
Base IP:	Subnet:	Gateway:
QoS (Off/Standard/Dante):		
VLAN (Enable/Disable):	Range:	Management ID#:
Art-Net Alternate Mapping (On/Off - On is default):		



PORT	1	2	3	4	5	6	7
Connected Device							
Normal/Tagged(Uplink)							
VLAN ID#							
ArtNet to sACN							
PoE Max Allocation							
Link Mode							
SFP Type							

PORT	8	9	10	11	12	13	14
Connected Device							
Normal/Tagged(Uplink)							
VLAN ID#							
ArtNet to sACN							
PoE Max Allocation							
Link Mode							
SFP Type							

APPENDIX 4: RING PROTECTION

Ethernet wiring schemes are based on a 'star'-wiring topology. Ring (or loop) data wiring – where the last device in a chain is wired back to the first device – is forbidden. Only one data path between any two devices is allowed.

But star-wiring layouts are prone to single point failures. Unlike DMX512 transmission, passive data 'thru' connections are not possible with Ethernet, which means there is no redundancy under normal operation. A severed cable or power loss to a switch can mean the loss of some or even all show control.

EAPS (Ethernet Automatic Protection Switching) allows the deliberate – and designed – use of a ring wiring system for Ethernet communications. When in this mode, VIA switches ignore data traffic on one segment of the ring, while monitoring the integrity of the remaining connections. If an interruption is detected, the unused ring segment is activated and full communication is restored. Fail-over time is between 50 and 75 milliseconds, or two to four DMX packets.

REQUIREMENTS AND LIMITATIONS

VLANs must be enabled to use Ring Protection. The mode uses a dedicated VLAN to monitor the integrity of the ring, called a Control VLAN. All switches must use the same Control VLAN. By default, VLAN 4095 is used. This does not mean your VLAN range needs to extend to 4095. Typically an entertainment network may use 1-3 or 1-10 VLANs.

Only the **last 4 ports on the switch (ports 11-14)** may be used with this feature.

If the ring is intact, the front display of the VIA12 will say "Ring is healthy". If the Ring fails, the front menu will report as such and flash the backlight of the display.

Ring Protection works with Pathway VIA switches only. Switches from other manufacturers can co-exist on the network, but should not be placed in-line with the ring.

DEFINITIONS

Master switch monitors the integrity of communications. Only one switch on the network may be configured as the master. If choice is available, the least busy switch, with the most reliable power source, preferably on an uninterruptible power supply, should be chosen as the master.

Transit switches receive and forward the ring monitoring packets. All switches other than the Master must be set as transit switches.

NOTE: Ring Protection wiring topology is not structured. A Primary port on one switch may be connected to a Secondary port on the next switch – any arrangement is acceptable. The link status in Pathscape will either be "Forwarding all traffic" or "Blocked by EAPS".

Primary Port is the main (active) UPLINK connection link on the Master switch, joining to the rest of the network. All transit switches must also have one port configured as the primary. Only ports 11 through 14 are available to be used as the primary port. If using copper, typically port 11 will be primary and 12 will be secondary. If using fiber, port 13 is primary and port 14 is secondary.

Secondary Port is an UPLINK port "ignored" (logically blocked) by the Master switch to break the ring topology. All transit switches also must have one port configured as the secondary port. The secondary port is actively used on transit switches. Only ports 11 through 14 are available to be used as the secondary port.



APPENDIX 5: RAPID SPANNING TREE PROTOCOL

The Rapid Spanning Tree Protocol (RSTP) is another technology to prevent network loops. EAPS (described above in Ring Protection) requires more setup, as it needs a dedicated master and multiple transit switches, but this allows it to function within a few DMX frames during fail-over. RSTP only requires you to turn on the feature on all the switches in the network. No further dedicated port configuration or special wiring considerations need to be adhered to.

VIA will block data flow on redundant links and report “Blocked by RSTP” in the link status. The algorithm that decides which ports to block is based on a stringent set of rules that ensure the fastest network possible.

APPENDIX 6: QoS SETTINGS

Quality of Service priorities are determined by the Differentiated Services Code Point (DSCP) field contained in each data packet header. DSCP values may range from 1 to 64, and are mapped to four egress (output) queues. The egress queues are, in turn, numbered from 1 (Best Effort) to 4 (Highest Priority).

The DSCP mappings and related QoS settings used by VIA switches is shown in the following table:

QoS Setting	Description
Disabled (default)	Disables QoS-based routing. All traffic is treated equally.
QoS Standard	Queue 1: DSCP values 1-16 Queue 2: DSCP values 17-32 Queue 3: DSCP values 33-48 Queue 4: DSCP values 49-64 A weighted fair queuing algorithm is used to prevent the starvation of lower queues by higher priority traffic.
Dante Strict	Queue 1: All DSCP values except: Queue 2: DSCP 8 Queue 3: DSCP 46 Queue 4: DSCP 56 Queue 3 and 4 are handled by strict priority, while the two lower queues are handled by the weighted algorithm.



APPENDIX 7: ELECTRICAL AND COMPLIANCE INFORMATION

ELECTRICAL INFORMATION

MODEL 6750

- Power input: 100-240VAC, 50/60Hz
- 0.3A Maximum current draw

MODEL 6750-P

- Power input: 100-240VAC, 50/60Hz
- 1.3A Maximum current draw
- Integrated PoE supply: 100W; Class 3 PoE (15.4W maximum per port)

MODEL 6752-P, 6754-P

- Power input: 100-240VAC, 50/60Hz
- 11.3A Maximum current draw
- Integrated PoE supply: 100W; Class 3 PoE (15.4W maximum per port)

COMPLIANCE

- IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
- IEEE 802.3af - Class 3 Power-over-Ethernet (PoE) (6750-P, 6752-P, 6754-P)
- California Title 1.81.26, Security of Connected Devices