PWVIA RM P12 Models

Running firmware 6.1 or later

User Guide

July 2021

Pathway® Connectivity Solutions

© 2021 Acuity Brands, Inc. • One Lithonia Way, Conyers GA 30012
Pathway Connectivity | #103 - 1439 17th Ave SE Calgary, AB Canada T2G 1J9
Phone: + 1 866 617 3074

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media, printed materials and “on-line” or electronic documentation (the “Software Application”) constitutes an unpublished work and contains valuable trade secrets and proprietary information belonging to Pathway and its licensors.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 RACK-MOUNT ETHERNET SWITCHES - PWVIA RM .1

INSTALLATION INSTRUCTIONS.....2

OPTIONAL MOUNTING ACCESSORIES 2

PANEL LAYOUTS 4

FRONT PANEL.....4

MODELS PWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] [NONPOE/POE] 4

MODEL PWVIA RM P12 RJ45EC [DUO/QUAD] POE.....4

REAR PANEL 4

MODEL PWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] NONPOE 4

MODEL PWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] POE 5

MODEL PWVIA RM P12 RJ45EC DUO POE.....5

MODEL PWVIA RM P12 RJ45EC QUAD POE 5

SFP+ PORTS.....6

opticalCON PORTS 6

POWER CONNECTIONS 6

CONFIGURATION 6

SECURITY 7

BACKGROUND INFORMATION 7

WHAT THIS MEANS TO YOU 7

SECURITY DOMAINS 8

RED PADLOCK - “Ready to Secure” device (previously “Unsecured”).....8

AMBER PADLOCK - “Other Domain” name showing device.....8

AMBER PADLOCK - “Read Only” (previously “Locally Secured”).....8

GREEN PADLOCK - “My Domain” shows devices in the current domain....9

NO PADLOCK - “Disabled By User” – Firmware version 6.1 or later - rackmount

devices with front panel UI only....9
EMPTY SECURITY DOMAIN CELL – Firmware version prior to 5.0 - device shipped prior to January 1, 2020....9
CREATING A SECURITY DOMAIN....10
ADMINISTERING A DOMAIN....15
MANAGE SECURITY DOMAIN....15
MANAGE DEVICES....19
RECOVERING A DOMAIN....21
RETAINING DEVICE SETTINGS FROM UNKNOWN DOMAINS....23
USING OLDER VERSIONS OF PATHSCAPE WITH NEW DEVICES....23
LOCAL CONFIGURATION ONLY - Using PWVIA RM without Pathscape....24
DISABLING SECURITY....25
PATHWAY ssACN (Secure sACN)....26
DOMAIN AUTO ssACN PASSWORD....26
CUSTOM ssACN PASSWORD....26
USING PATHWAY ssACN WITH VIA....27
NOTES ABOUT PATHWAY ssACN....28
SOFTWARE (PATHSCAPE) CONFIGURATION....29
NETWORK SETUP....29
DEVICE PROPERTIES....30
PATHWAY SECURITY DOMAIN....30
BASIC PROPERTIES....31
DEVICE INFO....31
DEVICE TIME SETTINGS....32
NETWORK PROPERTIES....32
ADVANCED FEATURES....33
VLAN PROPERTIES....34
Art-Net TRAP AND CONVERT....34
REMOTE MONITORING AND MANAGEMENT....34

RING PROTECT PROPERTIES (EAPS) 35
PoE PROPERTIES (POE Models) 37
ADVANCED PROPERTIES 37
VLAN CONFIG 38
VLAN GLOBAL PROPERTIES 39
⚠ WARNING ⚠ 40
VLAN PROPERTIES/SERVICES 41
RESOLVING VLAN CONFLICTS 44
PORT PROPERTIES AND CONFIGURATION 46
BASIC PROPERTIES 47
LINK DETAILS 47
NETWORK PARTNER (LLDP) 48
VLAN PROPERTIES 49
Art-Net TRAP AND CONVERT 49
POE PROPERTIES (NOT SHOWN ON NONPOE Model) 50
UPGRADING DEVICE FIRMWARE 52
FACTORY DEFAULT 53
FRONT PANEL LOCKOUT 54
FRONT PANEL UI AND MENU 55
SETTING SECURITY MODE 55
MAIN DISPLAY MESSAGES 57
USING THE FRONT PANEL UI 57
MENUS 58
NETWORK SETUP 58
DEVICE INFO/STATUS 60
ADVANCED SETTINGS 61
ADMIN/SECURITY 72
PORT STATUS AND CONFIGURATION MENU 74
PORT 13 & 14: CONFIGURATION/STATUS: SFP+ PORTS 79
APPENDIX 1: SFP/SFP+ FIBER ADAPTER SELECTION 83

APPENDIX 2: VIRTUAL LOCAL AREA NETWORK (VLAN).....84
DEFINITIONS 84
SOFTWARE CONFIGURATION OF VLANs 84
VLAN GUIDELINES.....84
APPENDIX 3: PLANNING CHARTS 85
VLAN PLANNING CHART.....85
SWITCH PLANNING CHARTS.....87
APPENDIX 4: EAPS & RSTP - “RING PROTECTION” 89
Requirements and Limitations 89
Definitions for EAPS 89
Software Configuration of Ring.....90
APPENDIX 5: QoS SETTINGS.....91
APPENDIX 6: ELECTRICAL AND COMPLIANCE INFORMATION.92
ELECTRICAL INFORMATION.....92
MODEL PWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] NONPOE 92
MODEL PWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] POE 92
MODEL PWVIA RM P12 RJ45EC [DUO/QUAD] POE.....92
COMPLIANCE 92
ENVIRONMENTAL.....92
PHYSICAL.....93
PPWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] NONPOE.....93
PPWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] POE.....93
PPWVIA RM P12 RJ45EC [DUO/QUAD] POE 93

ABOUT VIA RACK-MOUNT ETHERNET SWITCHES - PWVIA RM

VIA™ Gigabit Ethernet Switches are designed for live entertainment Ethernet systems, including audio, video and DMX-over-Ethernet networks. This manual covers models **PWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] [NONPOE/POE],** and **PWVIA RM P12 RJ45EC [DUO/QUAD] POE**

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 PWVIA RM P12 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 **PWVIA RM P12 RJ45EC [xxxx] NONPOE** 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 **PWVIA RM P12 RJ45EC [xxxx] POE** feature an integrated 100W PoE supply for powering compatible external devices.

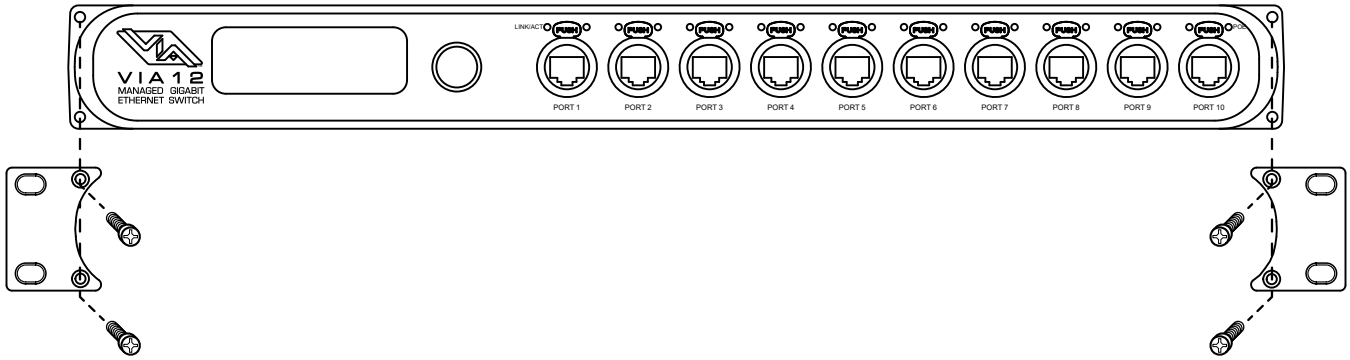
If you connect PoE-enabled devices to a NONPOE model they will not receive power.

INSTALLATION INSTRUCTIONS

PWVIA RM P12 switches are intended for desktop use, or to be mounted in a standard 19” equipment rack, using the integral rack ears (models PWVIA RM P12 RJ45EC [DUO/QUAD] POE) or the included rack ear accessories (models PWVIA RM P12 RJ45EC[SFPSLOT/1GSFP/10GSFPP] [NONPOE/POE]).

Rack ears included with the PWVIA RM P12 RJ45EC[SFPSLOT/1GSFP/10GSFPP] [NONPOE/POE] models for attaching unit to 19” equipment rack

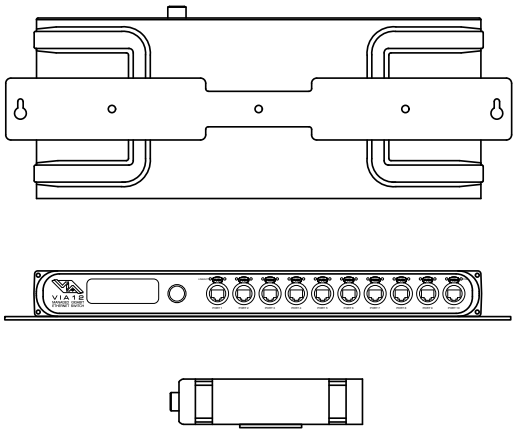
Use the included machine screws (2 per side) to attach the rack ears to the either side of the metal chassis (PWVIA RM P12 RJ45EC[SFPSLOT/1GSFP/10GSFPP] [NONPOE/POE] models).



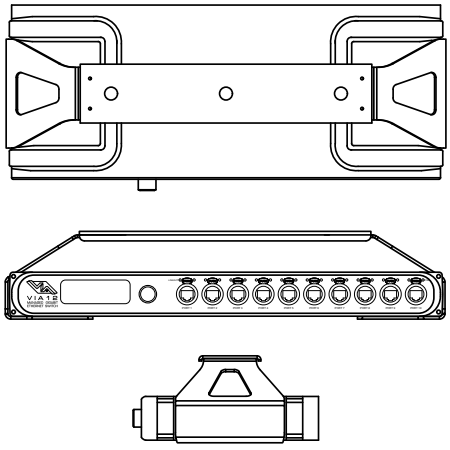
If using the PWVIA RM P12 on a desktop permanently, you may wish to apply the included adhesive rubber feet pads to the bottom of the unit. Simply peel them off the adhesive backing and apply to the bottom of the metal enclosure, with one on each corner.

OPTIONAL MOUNTING ACCESSORIES

Wall-mount kits (PWACC WMLG) and Truss-mount adapters (PWACC TMLG) are available as accessories.



PWACC WMLG Wall-mount Kit



PWACC TMLG Truss-mount Kit

All PWVIA RM P12 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.

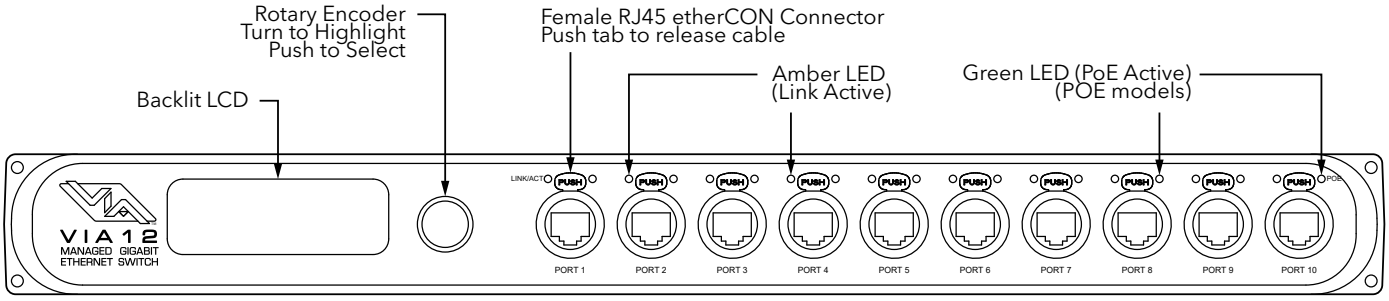
Warning: This equipment relies on building installation primary overcurrent protection.

Warning: Except for the chassis plug marked for AC input, all ports on the PWVIA RM P12 models 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.

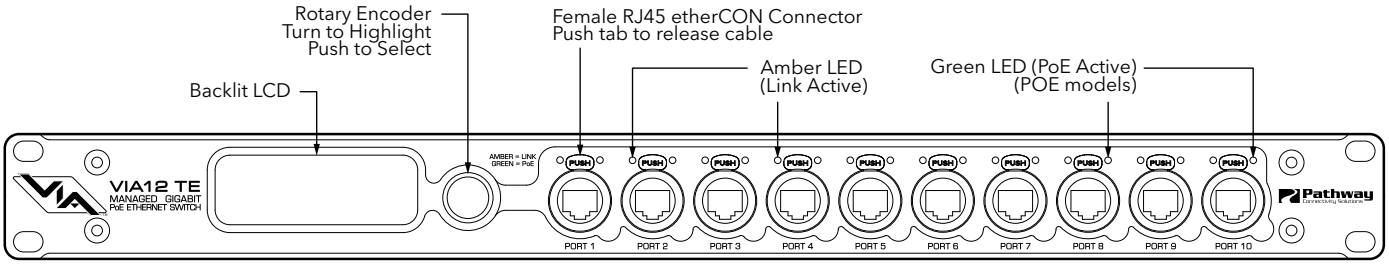
PANEL LAYOUTS

FRONT PANEL

MODELS PWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] [NONPOE/POE]

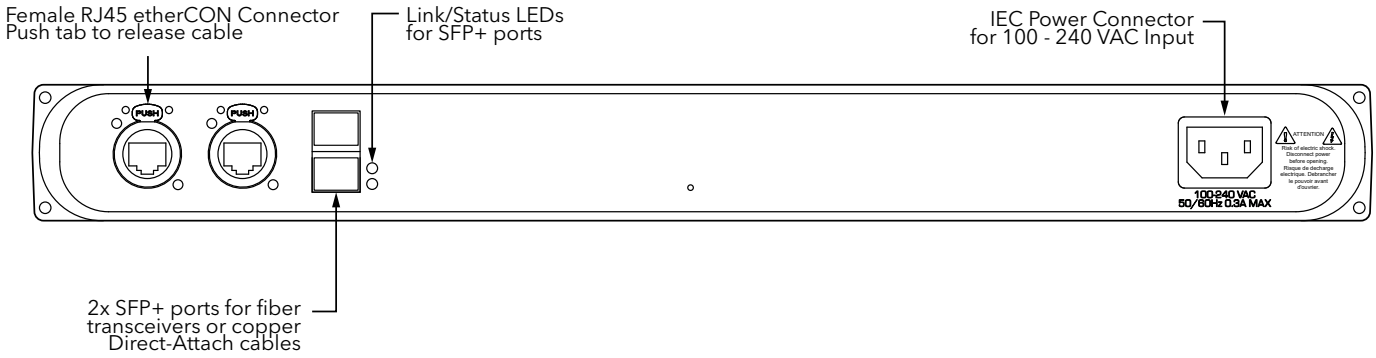


MODEL PWVIA RM P12 RJ45EC [DUO/QUAD] POE

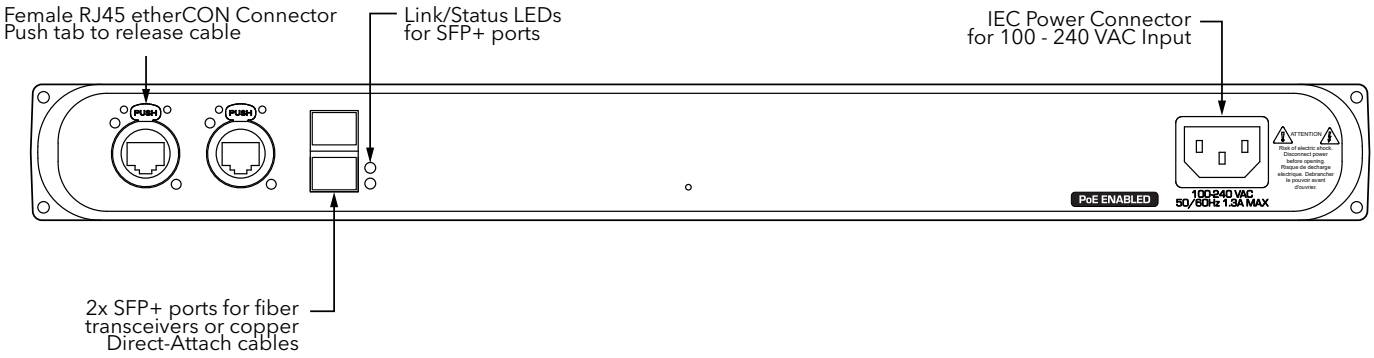


REAR PANEL

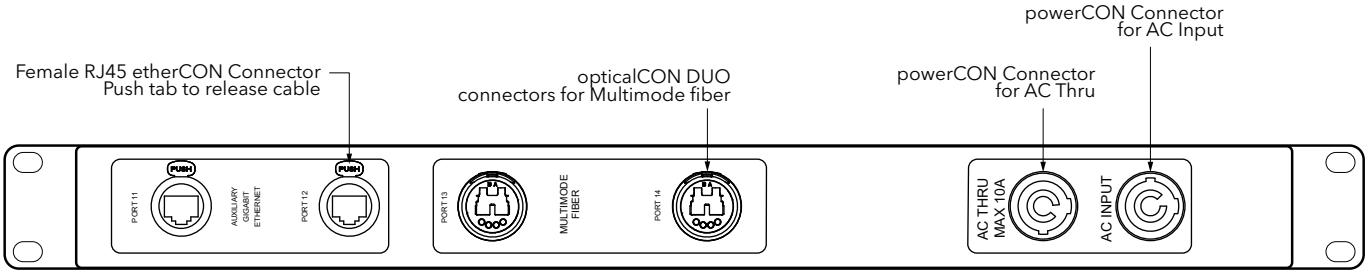
MODEL PWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] NONPOE



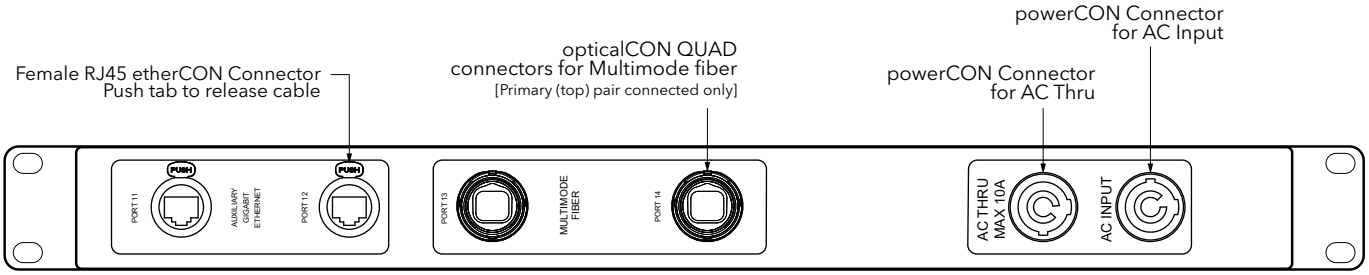
MODEL PWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] POE



MODEL PWVIA RM P12 RJ45EC DUO POE



MODEL PWVIA RM P12 RJ45EC QUAD POE



SFP+ PORTS

The PWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] [NONPOE/POE] models 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

The PWVIA RM P12 RJ45EC [DUO/QUAD] POE models 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 PWVIA RM P12 RJ45EC [DUO/QUAD] POE 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

PWVIA RM models 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 and click the download link for the appropriate operating system.

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 became 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 Configuration Only** below) or requires the users to change the password before being able to use it (See **Creating a Security Domain** below). With Pathscape V3 and later, we provide features that protect our products from unauthorized access or use by enforcing passwords.

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. Since the release of Pathscape V4, all Pathway Connectivity products can be upgraded to firmware version 6.x. It is suggested you upgrade your devices to take advantage of the most recent security improvements.

2. Products shipped before January 1, 2020, devices with version 3.x and 4.x firmware will continue to function without passwords using either Pathscape version 3 or 4.

3. All products shipped after January 1, 2020 may only be configured using Pathscape 4 or later.

4. Products shipped after January 1, 2020 cannot be downgraded to earlier password-free firmware.

   Using the **Tools >** **Firmware Updater** dialog (see later in the manual for instructions), devices manufactured before January 1, 2020 may show newer firmware versions, but using the **Select Latest** button will not select the latest. These devices do not have a method, like a front panel, to factory default them. You can manually select the latest firmware using the **Select Firmware** button, but do **not forget the new password** as you cannot factory default them.

   We highly recommend printing the Password Recover PDF when creating a Security Domain so you can reset lost passwords.

5. Products that are fully configurable from the front panel can enter **Local Configuration Mode** (**Read-Only mode**). This allows them to be configured locally, but not over the network.

6. You will be encouraged to print or save a recovery key in case you lose the password. Do so when setting up your Security Domain. It is the **only chance** you'll get to save/print/see this Recovery Key.

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.

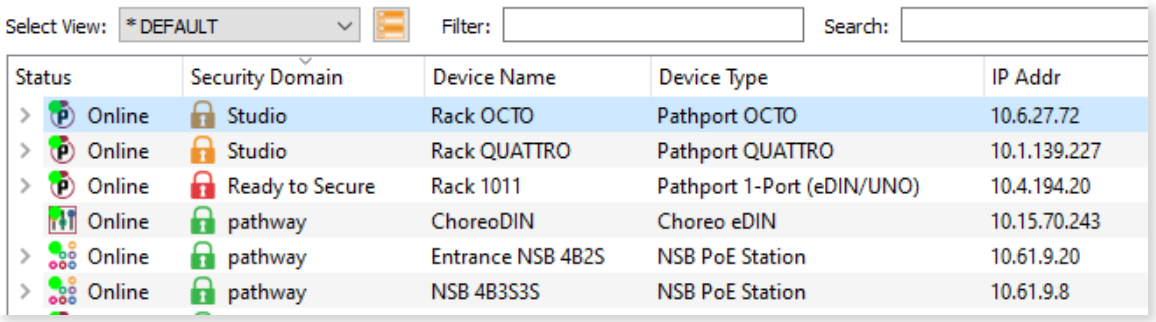
9. Configuring our devices to receive unsecured protocols such as sACN and Art-Net will require you to accept the risks. **See WARNING BOX regarding unsecured protocols below.**

   By default, all Pathway Connectivity products sent and/or receive Pathway ssACN which is an authenticated method of transporting the E1.31 protocol within a Security Domain.

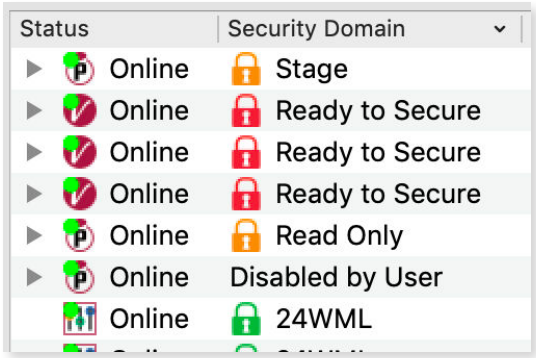
10. Pathway does not store personal information such as names or email addresses on our devices.
11. On products with a front panel display and encoder using firmware release 6.1, it is possible to opt out of the prescribed security features. See **Disabling Security** below.

SECURITY DOMAINS

To simplify the process of managing security on your network, Pathscape introduced 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 there is a column that shows you the name of the devices' domain and a **padlock icon** showing their current state.



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



RED PADLOCK - "Ready to Secure" device (previously "Unsecured")

Prior to Pathscape version 4.1, this was shown as "**Unsecured**".

Any device shipped after **January 1, 2020** will have version 5 or later 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 - "Other Domain" name showing device

Devices that have been added to a security domain will appear with an amber padlock. These 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.)

AMBER PADLOCK - "Read Only" (previously "Locally Secured")

Prior to Pathscape version 4.1, this was shown as "**Locally Secured**".

Read Only 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 Reset Security** settings from the front panel and then add it to the Security Domain using Pathscape.

GREEN PADLOCK - “My Domain” shows devices in the 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/Writable.

NO PADLOCK - “Disabled By User” – Firmware version 6.1 or later - rackmount devices with front panel UI only

With the release of **firmware version 6.1 for rackmount devices with a front panel display and encoder (PWPP RM, PWVIA RM only)**, it is possible to opt out of the security features altogether. This is designed primarily for the rental market where devices may be shipped to various locations for use by different end users, where Domain passwords and Recovery Keys may not be known.

Devices set to **Disabled by User** will behave like legacy devices and are fully Read/Writable by Pathscape without needing to be logged into a Domain.

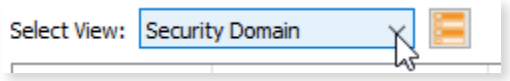
For information on opting out of security features, see **Disabling Security** below.

EMPTY SECURITY DOMAIN CELL – Firmware version prior to 5.0 - device shipped prior to January 1, 2020

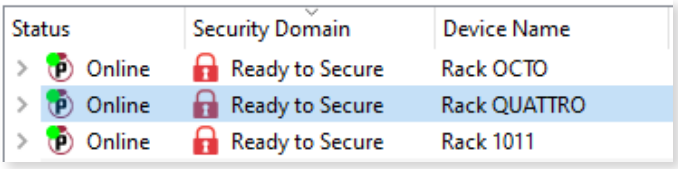
If the Security Domain cell is empty, this device is using Version 4 firmware and cannot be secured. Pathscape 4 will be able to read and write properties exactly like earlier versions of Pathscape. If you upgrade to version 5 or later firmware, the device will appear with a red padlock and you will need to add it to a domain before you can use it.

CREATING A SECURITY DOMAIN

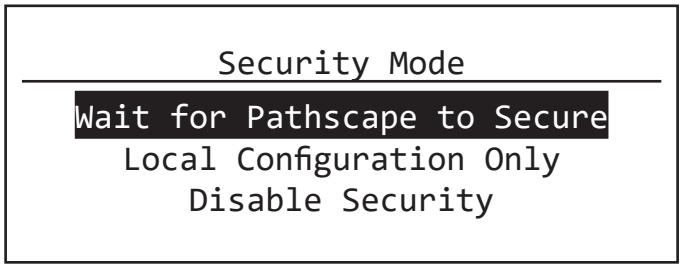
- After starting Pathscape, the online devices will populate the Device View.
- Choose the **Security Domain** view from the **Select View** dropdown

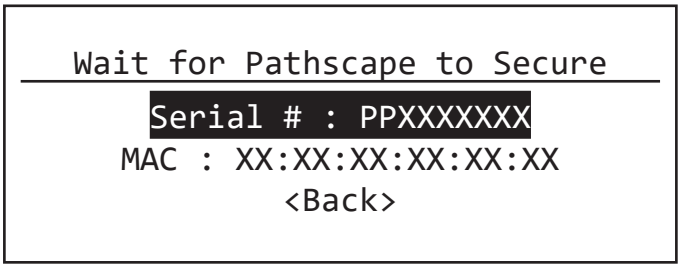


- Each device running V5 or later firmware will have a **Red "Ready to Secure"** value in the **Security Domain** column.



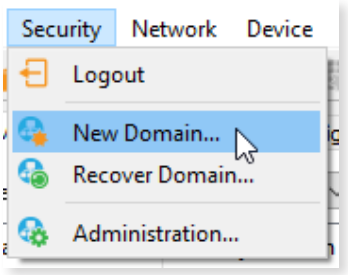
- **NOTE**: VIA switches running **V6.1 firmware or later** will show a **Security Mode** screen on the front panel LCD.



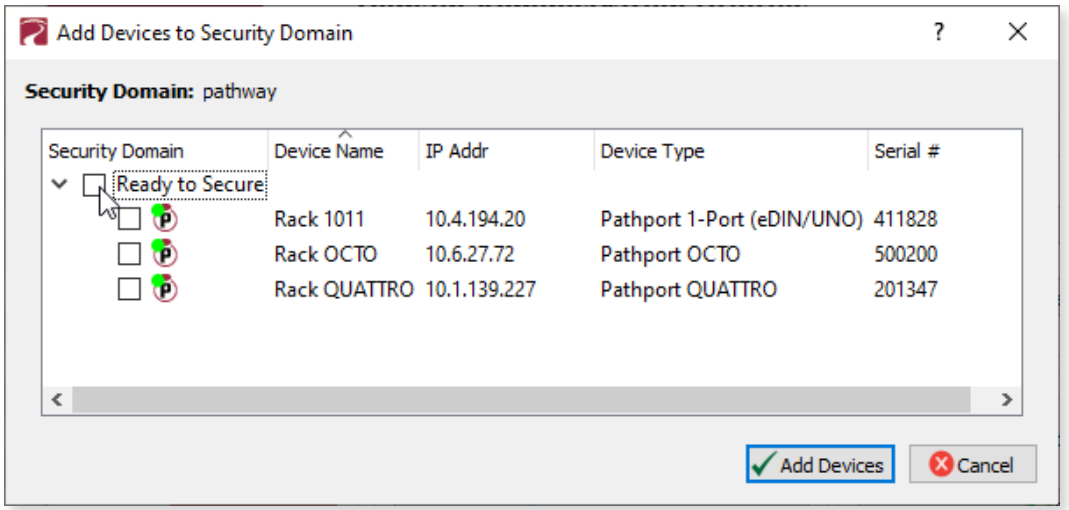


- **No action is required** here to add the device to Pathscape. Clicking the encoder knob to select **Wait for Pathscape to Secure** will show the device Serial Number and MAC Address, in cases where this may be helpful for device identification.
- If you want to configure your devices only VIA the front panel, choose **Local Configuration Only**. If you prefer to opt out of security and the needs for passwords on these devices, choose **Disable Security**.

  See the below for more detail on these options.
- If your devices have old firmware, you may update them to current firmware by going to the **Tools** menu in Pathscape and selecting **Firmware Updater**. 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**.
- From the **Security** menu, choose **New Domain.**



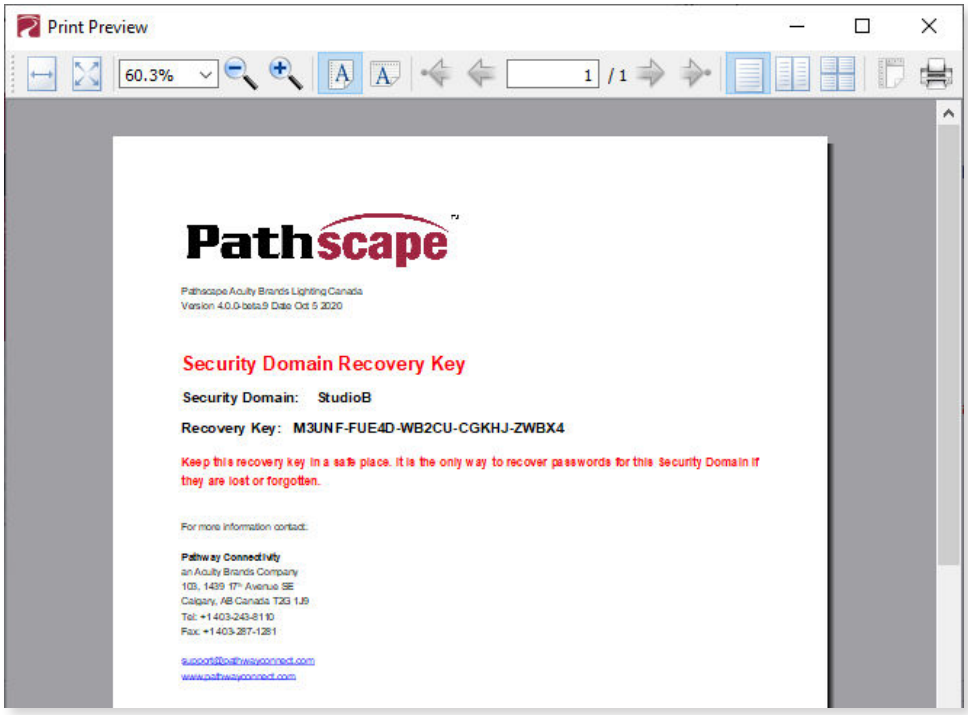
- Enter the new **Domain Name** and **Administrator** and **User passwords**, then click **Next.**
  - The **Administrator** can change passwords, change the Security Domain's name, factory default devices, manage Device Restore Points and add or remove devices from the domain.
  - The **User** can change device properties and save and restore show files, but cannot change domain passwords, factory default devices or add/remove devices. There is one User account password for all users.
- Add all the Ready to Secure devices on your network by checking the top checkbox labeled "**Ready to Secure**" and then click **Next**. If you wish to add some but not all devices to this domain, click on the checkbox next to each device you'd like to add, and then click **Add Devices**.



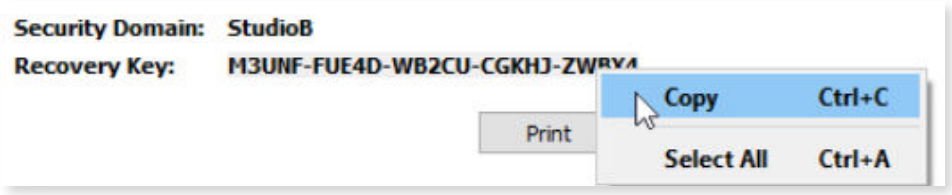
- The next window will show the **Recovery Key**. This key will allow you to recover Security Domain access should the passwords be lost or forgotten.

  It is extremely important to keep a record of this Recovery Key, as this is the only time it will be shown to you. Print the Recovery Key.

- Clicking the **Print** button will open a Print Dialog, from which you may choose a printer to print to.



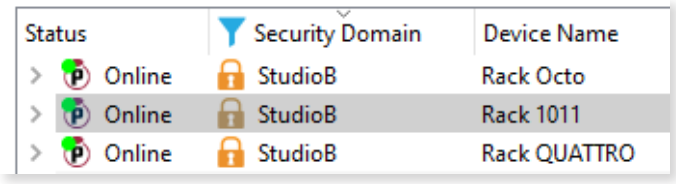
- You may also right-click on the Recovery Key, then **Select All** and **Copy** the key to the clipboard and store it in a safe place.



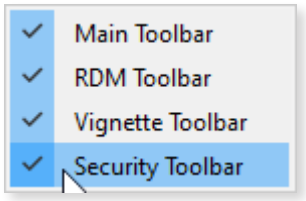
- In order to proceed, you **must click the checkbox** acknowledging you have printed or saved the Recovery Key in some way.

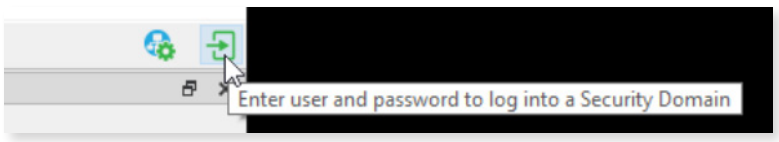
  Managers of the facility should store this key in a safe place, keeping in mind that anybody with this key can change both the Administrator and User passwords at any time.

- Click **Finish** and the window will close, and the devices will be added to the domain. The devices will have an **amber padlock** and their properties will be read-only.

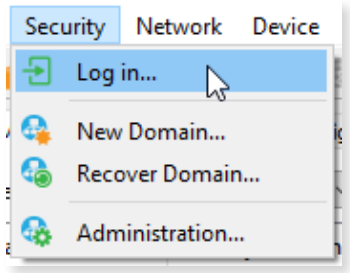


- To configure the devices, you must log in to the domain **as a user** by pressing the Log In button in the toolbar. **Note**: The **Security Toolbar** option under the **Window** menu must be checked.

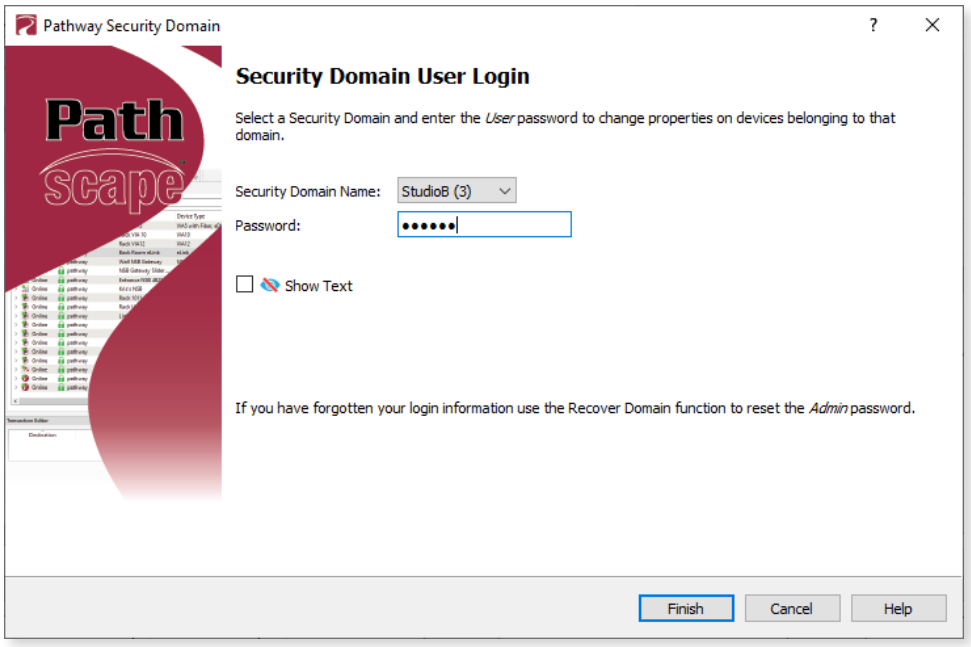




You can also click on the **Security** menu and select the Log In menu item.

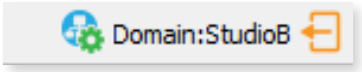


- Enter the **User** password for the Security Domain that was just created, and click **Finish**.



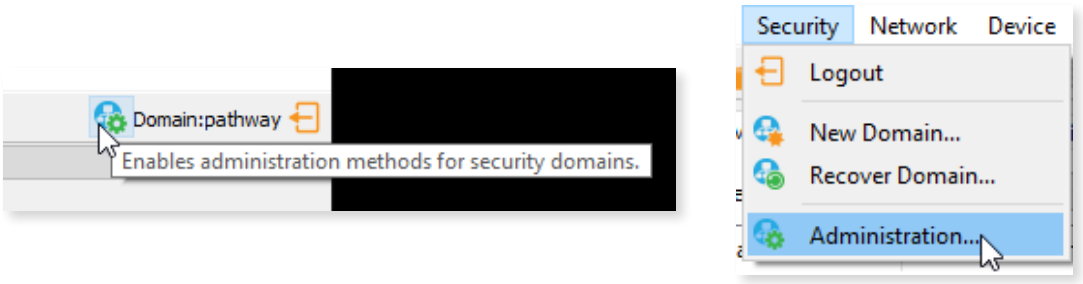
As security parameters are verified, the amber padlocks will turn **green** and the properties of those devices will be read/writable.

Once logged into a domain, the **Log In** button will change to the **Log Out** button, and the name of the domain currently logged into will appear next to it.

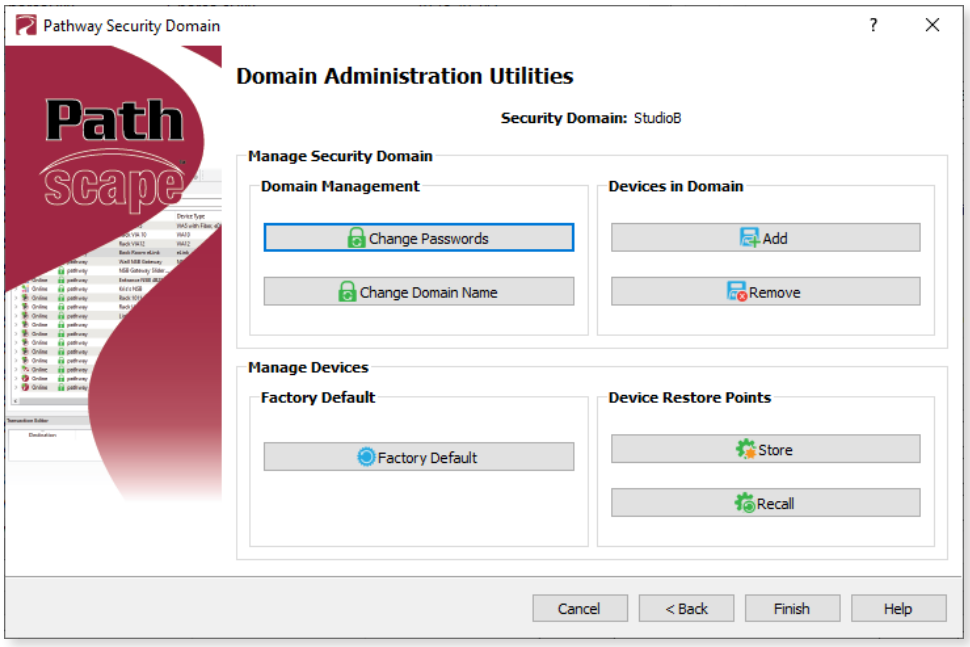


ADMINISTERING A DOMAIN

To administer a domain, click on the **Administration** button on the Security Toolbar, or click the **Security** menu and select **Administration**.



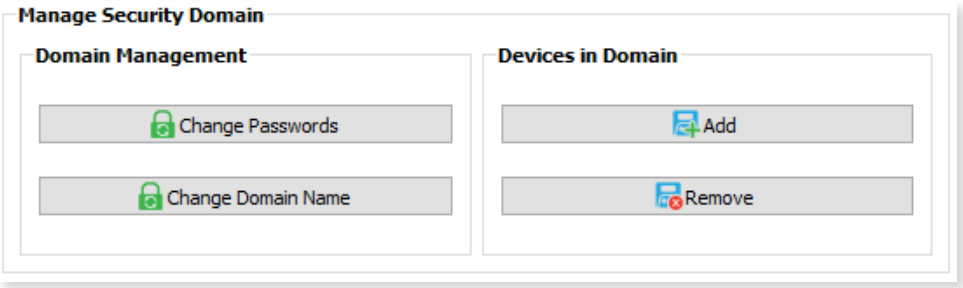
Enter the **Admin** password for the Security Domain, and the **Domain Administrator Utilities** window will appear.



The Domain Admin Utilities window is broken down into to main sections, **Manage Security Domain** and **Manage Devices**.

MANAGE SECURITY DOMAIN

This section is broken down further into functions that relate to **Domain Management**, including Domain Name and Passwords, and **Devices in Domain**, which allows you to add and remove devices in the Domain.



DOMAIN MANAGEMENT

CHANGE PASSWORDS

If your staffing changes, it is a good idea to change the passwords on the domain. Click this button to change the current Security Domain Admin and User passwords. **All devices should be online when you change the password.**

Once you have entered both Admin and User passwords, click the **Change Passwords** button to confirm the changes.

Note: Changing the domain passwords does not generate a new Recovery Key. The original key is still valid, as it is only generated at the time of the Domain's creation.

Note: **If some devices are offline and you change the password**, when those devices come back online, they will coincidently have the same domain name, but will be using the old password. When logging in, there will be two domains with the same name.

You will have to remove the devices on the old domain, then add them to the new domain using the new password. You can remove them using the **Remove** button in the **Domain Administration Utilities** menu (see below for details).

The number in parentheses after the domain name is the number of devices that are in that domain. In the example above, there are 12 devices in the "pathway" domain.

This will help you identify which is the old domain. Log into the old domain using the old password and remove the devices. When they come back online, they will appear as **Ready to Secure**. Add them to the new domain using the new password.

CHANGE DOMAIN NAME

Click this button to change the name of the current Security Domain.

Enter a new name for the current domain, and click **Change Domain Name**.

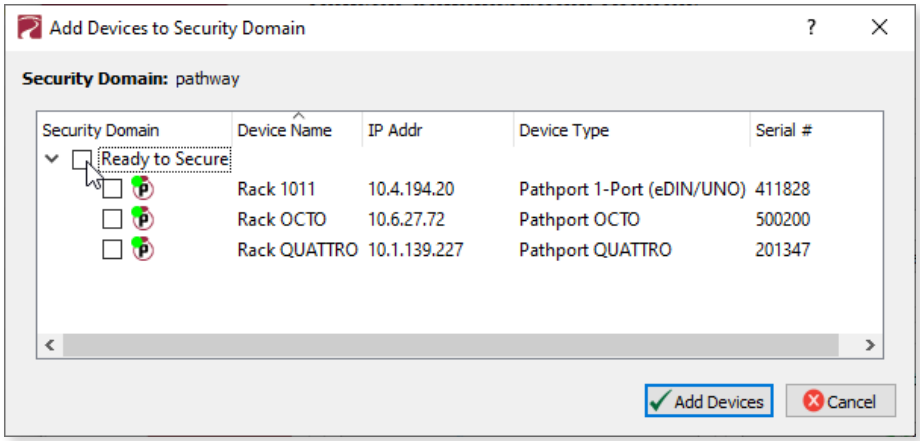
The window will close, and you will be logged out of the current domain, and the Domain Name will be changed to the new value. **You will have to log into the Domain again** to make any further changes.

Note that changing the domain name **does not** generate a new Recovery Key. The original key is still valid, as it is only generated at the time of the domain's creation.

DEVICES IN DOMAIN

ADD

Clicking on this button will bring up the **Add Devices** window, where Ready to Secure devices can be added to the current Security Domain.

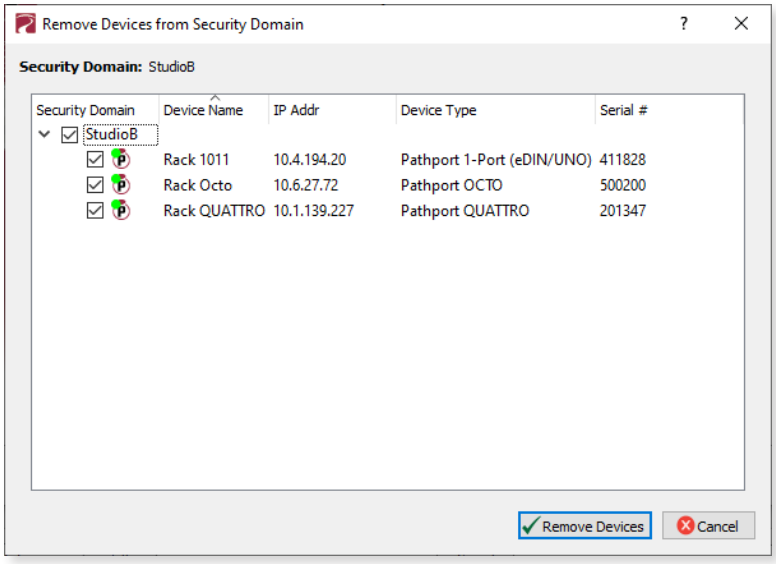


Click on the checkboxes next to the devices you want to add to the Domain, and click the **Add Devices** button. To add

all the listed devices, click the top checkbox next to “Ready to Secure” which will auto-check all the devices’ checkboxes.

REMOVE

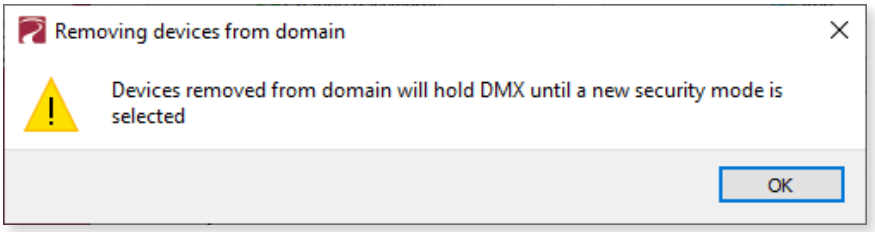
Click this button to remove devices from the current Security Domain.



Click on the checkboxes next to the devices you want to remove from the Domain, and click the **Remove Devices** button. To remove all the listed devices, click the top checkbox next to the Domain Name which will auto-check all the devices’ checkboxes.

The devices will then be removed from the Security Domain, and will appear as **Ready to Secure**. The devices can then be added to another domain as needed.

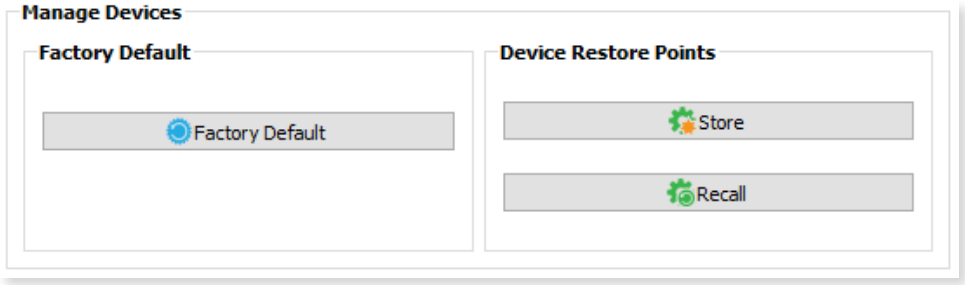
Note: When a device is removed from a domain, a window will appear reminding you that any active Network DMX levels will be held by that device until a new security mode is selected.



If all devices in a domain are removed from the domain, that domain is then deleted. This action cannot be undone. If you remove all devices from a domain and then want to add devices back to that domain, you will have to create a new domain with the same name, copy down the new Recovery Key, and add those devices again. **NOTE**: The original Recovery Key is now useless.

MANAGE DEVICES

This section is broken down further into functions that relate to **Factory Defaulting** devices as well as setting or restoring **Device Restore Points**.



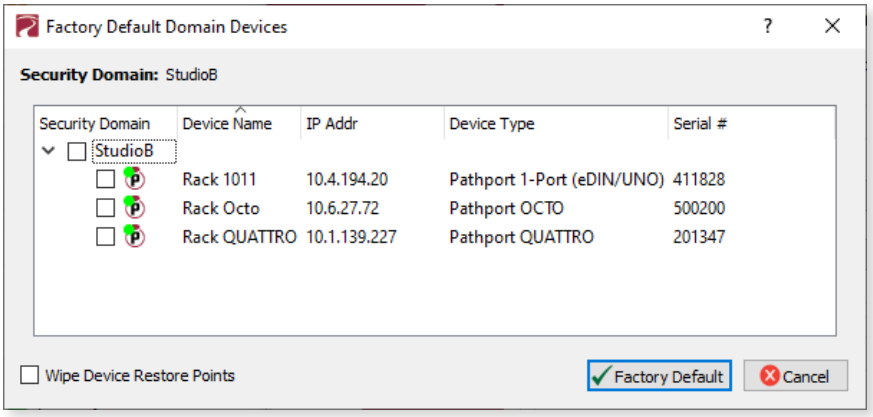
FACTORY DEFAULT

FACTORY DEFAULT

If you want to clear the settings of a device and return it to the factory defaults, click **Factory Default**.

Note that only devices in the Security Domain shown in this dialog box will be available to be defaulted. For devices running firmware V4 or below or devices that opted out of security, select the device and choose Factory Default in the Device menu.

See the Pathway website under **Support > Reference Articles > Factory Defaulting Ethernet Devices** for detailed instructions.



At the bottom of the window, you may optionally **Wipe Device Restore Points** from all checked devices. See below for details on Device Restore Points.

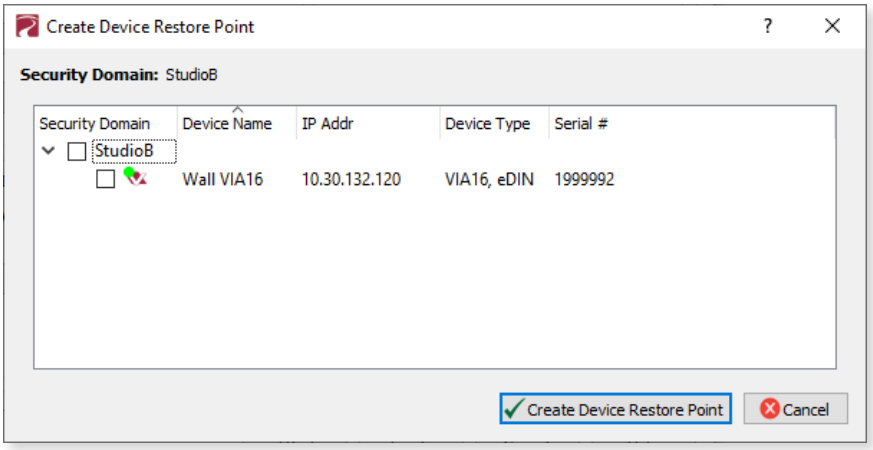
DEVICE RESTORE POINTS

With the release of firmware V6.0, VIA Switches including models PWVIA RM P12, PWVIA DIN P16, and PWVIA DIN P8 will support Device Restore Points.

Creating a Device Restore Point saves the device's current configuration and settings to its internal memory, for later recall. This differs from a Pathscape show file, in that the show file is saved on a PC running Pathscape.

STORE

Click this button to open the **Create Restore Point** window.

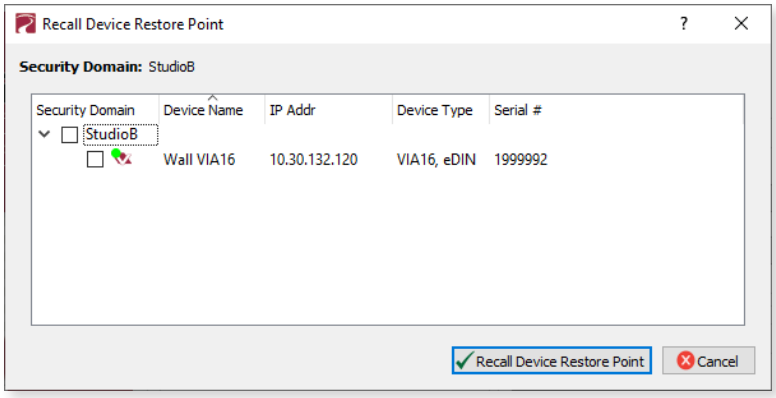


Click the checkbox next to each device on which you'd like to create a restore point. To check all devices, click the topmost checkbox. Click **Create Device Restore Point** to confirm.

Note that if there are no connected devices that support this feature, this button will be grayed out.

RECALL

Click this button to open the **Recall Restore Point** window.



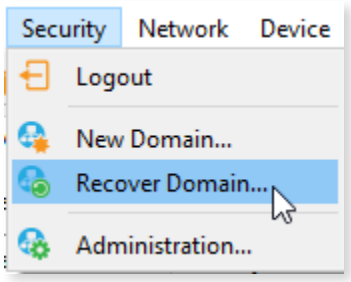
Click the checkbox next to each device on which you'd like to recall its restore point. To check all devices, click the topmost checkbox. Click **Recall Device Restore Point** to confirm.

Note that if there are no connected devices that support this feature, this button will be grayed out.

RECOVERING A DOMAIN

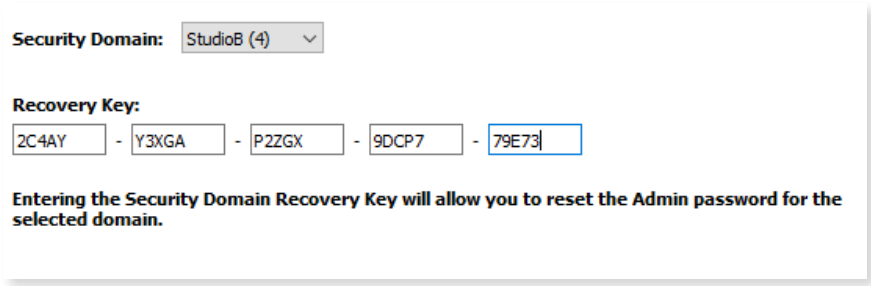
If you lose the Administrator password (or it was maliciously changed without your consent), you can recover the domain, retaining its configuration and set new passwords.

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



- The **Reset Device Security** window will open.

- Type in the 25-digit **Recovery Key** and press **Next**.



- Type in a new **Administrator Password**, and click **Finish**.

- Now you can log into the **Domain Administration Utilities** Panel using the new Admin password you just specified. At this point you can set a new user password as well, using the **Change Passwords** button, as explained above.

RETAINING DEVICE SETTINGS FROM UNKNOWN DOMAINS

In the unlikely event that you don't know the password of a Security Domain, but you'd like to retain all its configuration, try the following:

Without logging in to a Domain, all devices that appear with amber padlocks are **read-only**. Save a show file, and the configuration of all devices is saved. You can then factory default the devices using the prescribed method.

See the Pathway website, under **Support > Reference Articles > Factory Defaulting Ethernet Devices** for detailed instructions.

Once they reappear in Pathscape as **Ready to Secure**, add them to a Security Domain and log in. Once all devices appear with a **Green Padlock**, open the show file and **Send All Transactions** to restore the network configuration and patch.

USING OLDER VERSIONS OF PATHSCAPE WITH NEW DEVICES

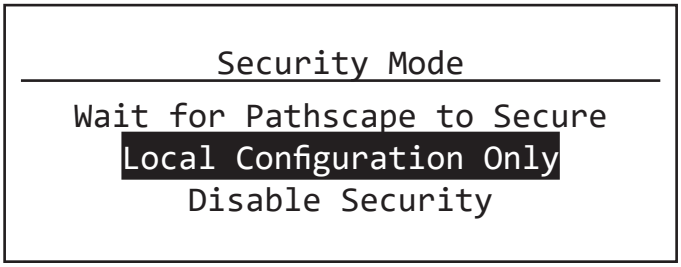
If you use Pathscape 1 or Pathscape 2 with devices shipped after **January 1, 2020 (Version 5 firmware or later)**, you will not be able to configure them. **You must use Pathscape 4 or later**. As a reminder, the device label will appear in the earlier versions of Pathscape as "**Use latest Pathscape PC software to secure**". Other properties will be shown and are correct, but any attempts to change them will fail.

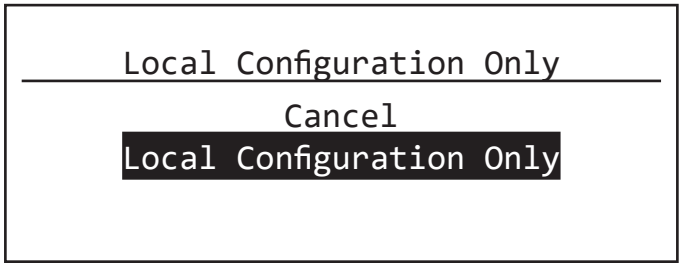
LOCAL CONFIGURATION ONLY - Using PWVIA RM without Pathscape

VIA switches have features that use unsecured protocols, like **Art-Net Trap & Convert**. You may not intend to use Pathscape, but "bad actors" could potentially access the switch and change the configuration. Therefore it is prudent to configure **Local Configuration Only** (Read Only) mode to protect your network if you want to use the VIA, but are not using Pathscape to add your devices to a **Security Domain**.

Enter **Local Configuration** mode by selecting **Local Configuration Only** from the **Security Mode** menu.

This menu is shown upon bootup when no Security Mode has been set, i.e. when first received from the factory, or when the device has been factory defaulted or had its Security settings reset.



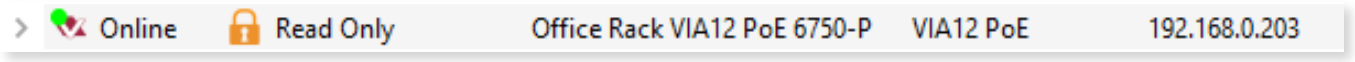


- From the **Security Mode** menu shown on the LCD, turn the encoder to select **Local Configuration Only**. In the submenu, confirm by selecting **Local Configuration Only** again. You will then have full access to the menus.

WARNING ABOUT UNSECURED PROTOCOLS

You are 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 use Pathway ssACN, and secure access to your network, both physically and technologically. To use unsecured protocols, you must acknowledge that you have read this statement and accept these risks.

If you do open Pathscape, any devices secured this way shown as **Read Only**.



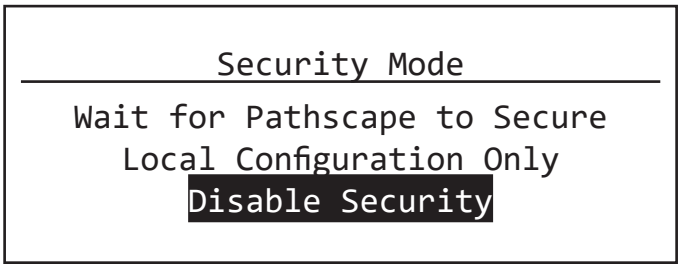
If you want to use a PC for further configuration, you must use the front panel to **Reset Security** settings, then use Pathscape to add it to a Security Domain.

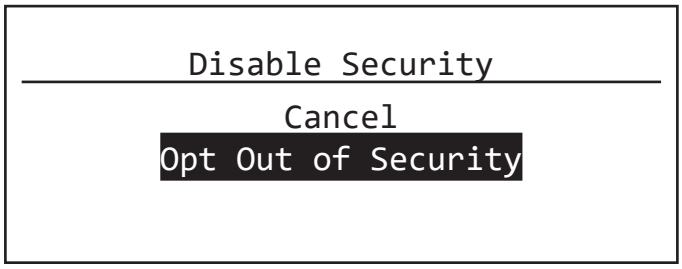
DISABLING SECURITY

With the launch of **firmware version 6.1 for devices with a front panel display and encoder (PWPP RM and PWVIA RM only)**, it is possible to opt out of the security features altogether. This is designed primarily for the rental market where devices may be shipped to various locations for use by different end users, where Domain passwords and Recovery Keys may not be known.

This mode of operation is not a recommended practice. However, if the production is on a dark network with a known crew, risk assessment may be weighed against convenience.

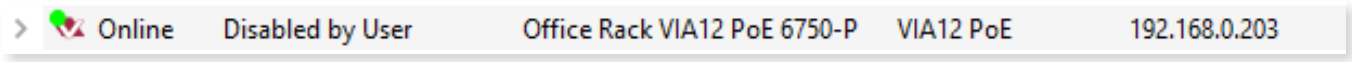
It is only possible to disable security settings from the front panel. **It is not possible to do this from Pathscape. You must perform this action from the Security Mode menu**, which is only shown when no other security mode has been set, i.e. when new from the factory, or after the device has been Factory Defaulted or had its Security Settings reset.





- From the **Security Mode** menu shown on the LCD, turn the encoder to select **Disable Security**. In the submenu, confirm by selecting **Opt Out of Security** again.
- You will then be able to access the menus. The device will appear in Pathscape with the Security Domain shown as "**Disabled by User**".
- On the front panel display, the bottom line will show "`Security: Disabled by User`" as a reminder and warning.

Devices set to **Disabled by User** will behave like legacy devices and are fully Read/Writable by Pathscape **without needing to be logged into a Domain**.



These devices will be fully configurable, resettable and rebootable from any PC that has network access, **including unauthorized parties**.

To re-enable Security on a device that has been **Disabled by User**, use the front panel to Reset Security settings, and add the device to Pathscape as explained above.

PATHWAY ssACN (Secure sACN)

Pathway ssACN (Secure streaming ACN) is a protocol developed by Pathway using much of ANSI E1.31, but adds a layer of authentication. This feature requires **device firmware version 6.0 or later**.

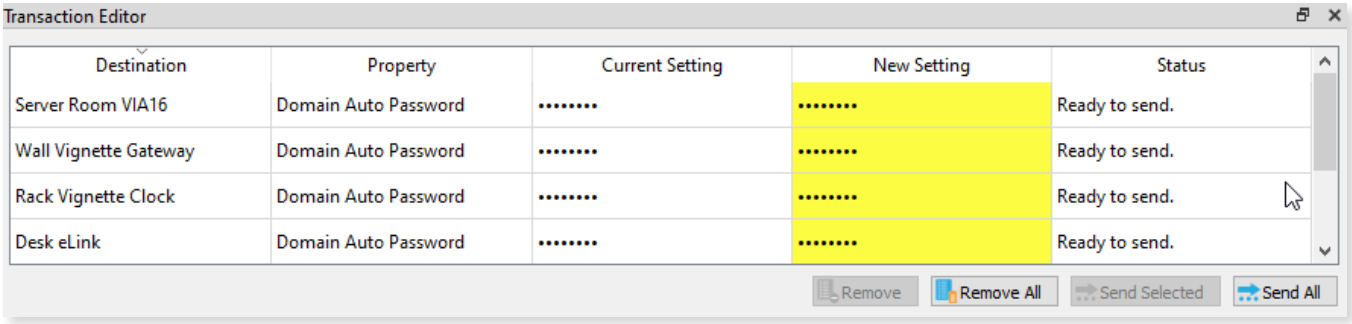
Receiving devices, like Pathport DMX/RDM gateways, share a **secret password** with known controllers in the venue, to verify the data source before driving the lighting rig. A cryptographic hash message is added to each E1.31 packet, verifying the authenticity of the source and the sequence of the data. Any invalid packets are ignored; only the correct lighting data is used during your performances.

If you have disabled security on a device, you will not be offered the ssACN protocol for Tx or Rx.

"Bad actors" cannot spoof a DMX source and send denial-of-service or ransomware attacks as the packets on their unsecured, unauthenticated protocols will be completely ignored by the lighting rig.

DOMAIN AUTO ssACN PASSWORD

When devices are added to a Security Domain, Pathscape generates a secret **Domain Auto ssACN password**, and creates transactions to send this data to each device in the domain. Each Security Domain will have a unique secret Domain Auto password created for it.



NOTE: these transactions will also appear for devices **already** part of a domain, after upgrading those devices to firmware version 6.0 or later.

NOTE that the **Domain Auto** password is **NOT** the same as the **Domain** password. Recall that the Domain password is the password **you chose** when creating the domain, used for logging in. Pathscape generates the Domain Auto password based on an algorithm. It is **NOT** possible to uncover the "•••••••" and see the value of the password, however all devices on the domain know what it is. This is how the authentication is possible.

CUSTOM ssACN PASSWORD

While in most scenarios the Domain Auto ssACN password will be all that is required, it is possible to specify your own custom ssACN password. See below for details on how to set custom TX (Transmit) and RX (receive) passwords.

This is useful in a few situations:

- **If you need to send DMX data across different Security Domains**: specify a custom **ssACN TX password**, and enter the same password on the receiving devices under **ssACN RX passwords**. The receiving devices will then be able to authenticate that data. Domain Auto passwords, as noted above, are unique per Domain, and will work only with devices on the same domain.
- **If you have a network with multiple consoles**: specify a different TX password for each console, and set the appropriate receiving devices to receive only one password or the other, effectively having them "listen" to traffic from the desired console only.

There may be other situations where a custom ssACN password is useful, but we recommend using the Domain Auto password for most systems unless you have unique requirements like the above.

If your console does not support Pathway ssACN and you still want to take advantage of the protocol's security features, consider inserting an eLink between the guest console and your installed network to wrap the generic sACN data for the Security Domain.

USING PATHWAY ssACN WITH VIA

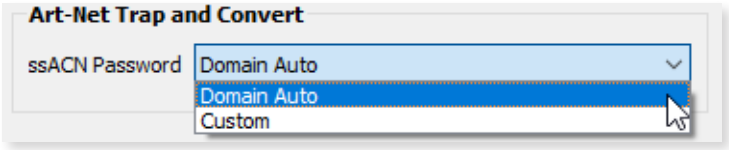
In general, VIA switches do not perform any protocol conversion on data traffic, except with the feature **Art-Net Trap and Convert.**

When **Art-Net Trap and Convert** is enabled on a Port, Art-Net data packets with broadcast address destinations are trapped and converted to E1.31 sACN or Pathway ssACN multicast packets, as the packets enter the Port of the switch.

Because VIA switches can now trap Art-Net and Convert it to Pathway ssACN, there are new properties to configure for this functionality.

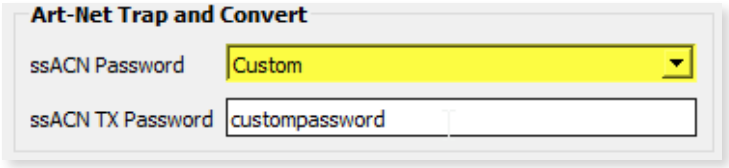
In the VIA **base device** properties, there is the **Art-Net Trap and Convert** section**.**

In the **ssACN Password** drop-down menu, specify whether the switch should use the generated **Domain Auto** password (default) or a **Custom ssACN Password**.

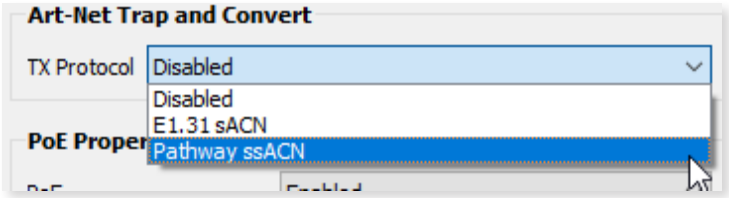


NOTE: This applies only if you choose to convert Art-Net to Pathway ssACN. If you choose to convert Art-Net to standard E1.31 sACN, this setting does not apply.

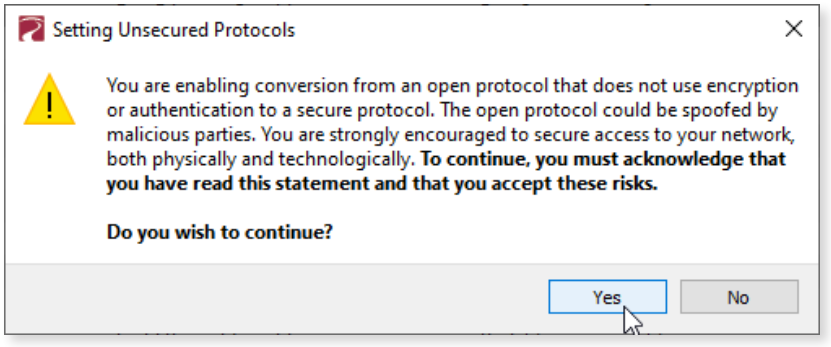
If you select **Custom**, enter the Custom Pathway ssACN password in the **ssACN TX Password** field.



On the relevant VIA switch Ports, under the **Art-Net Trap and Convert** section, select the **TX Protocol** to convert trapped Art-Net packets to for that Port. Options are standard **E1.31 sACN** or **Pathway ssACN**. You may also choose to **disable** the function.



When selecting Pathway ssACN as a TX Protocol, a warning message appears informing you of the risks associated with using an unsecured protocol (Art-Net). While Pathway ssACN itself is secure, the source Art-Net protocol is not. To continue, click the “Yes” button.



NOTE that the individual Port property determines what type of conversion is performed (None/Disabled, E1.31 sACN or Pathway ssACN), and the base device property determines the Pathway ssACN Password type. You may choose to convert to E1.31 sACN on some ports, Pathway ssACN on others, and disable the function on others, or any combination.

See later in this manual for more detail on Art-Net Trap & Convert.

NOTES ABOUT PATHWAY ssACN

A device can only have one TX password at a time. You cannot transmit with multiple TX passwords.

However, receive devices can accept any number of different custom passwords.

See the **Pathscape manual** section on **Pathway ssACN** for more detail about setting and managing Pathway ssACN passwords across your network.

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

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

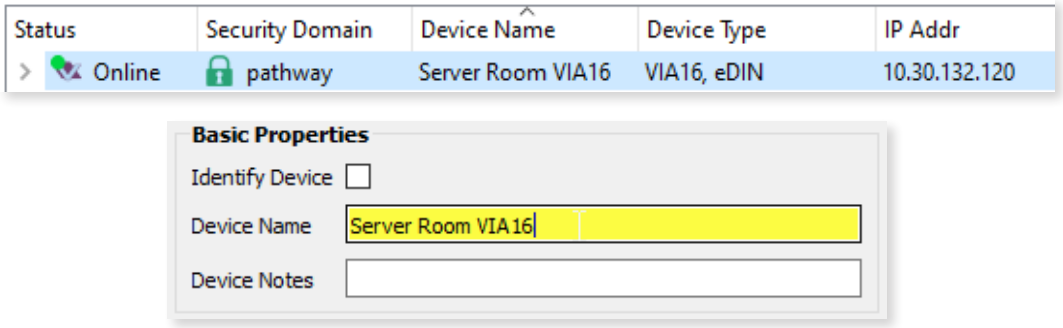
NOTE some features are not available if using only the Front Panel to configure the device.

NETWORK SETUP

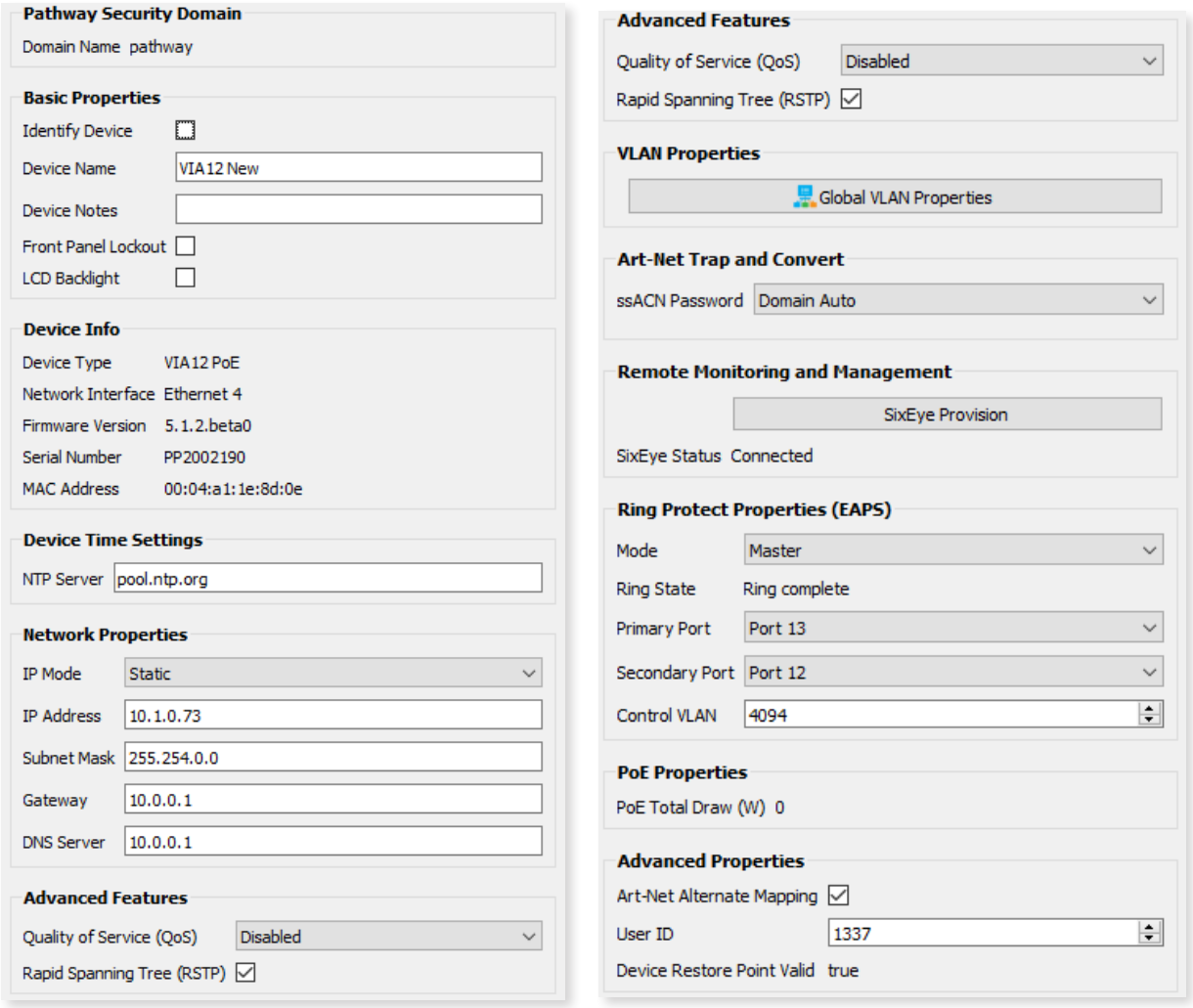
PLEASE NOTE: Before any configuration and network setup can be done, including setting the IP, the VIA switch(es) must be added to a Security Domain. If the device is not added to a Security domain, it will not be possible to configure any properties.

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



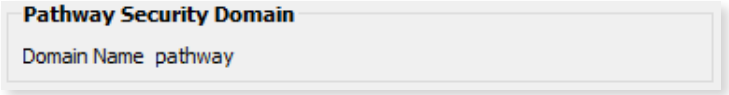
DEVICE PROPERTIES



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

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

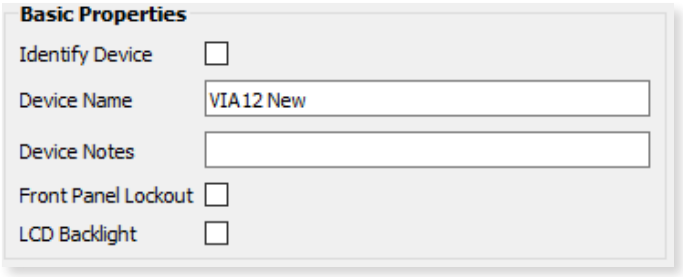
PATHWAY SECURITY DOMAIN



DOMAIN NAME

The name of the Security Domain the device is currently assigned to.

BASIC PROPERTIES



IDENTIFY DEVICE

Checking this box causes device to commence identify behavior (flashing LCD backlight or Identify LED).

DEVICE NAME

A user-configured, soft label for the Gateway. If left blank (and by default) the device name displayed will be the device's IP Address. Shown in the Device window and on Gateway front display.

DEVICE NOTES

A user-configured text description field, shown in the Device view.

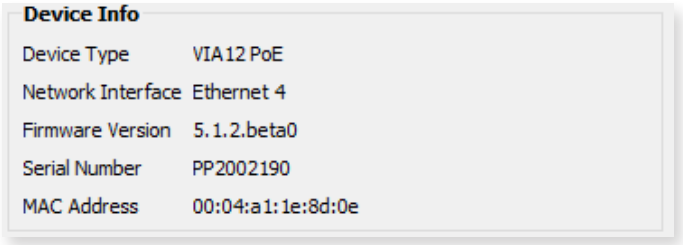
FRONT PANEL LOCKOUT

Rackmount VIA switches (PWVIA RM) only. 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.

LCD BACKLIGHT

Rackmount VIA switches (PWVIA RM) only. Checking this will enable the LCD backlight on the front panel of the device.

DEVICE INFO



DEVICE TYPE

The device type for the currently selected device.

NETWORK INTERFACE

Shows the name of the NIC (Network Interface Card) the device is communicating to the machine running Pathscape on.

FIRMWARE VERSION

Shows current operating firmware version. See the **Firmware Update** section on how to update the firmware. Read-only.

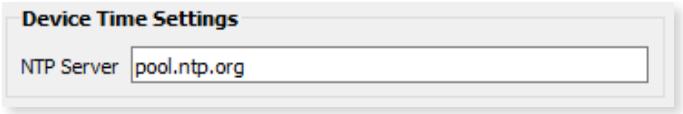
SERIAL NUMBER

Factory-set unique identifier. Read-only.

MAC ADDRESS

Factory-set hardware address. Read-only.

DEVICE TIME SETTINGS

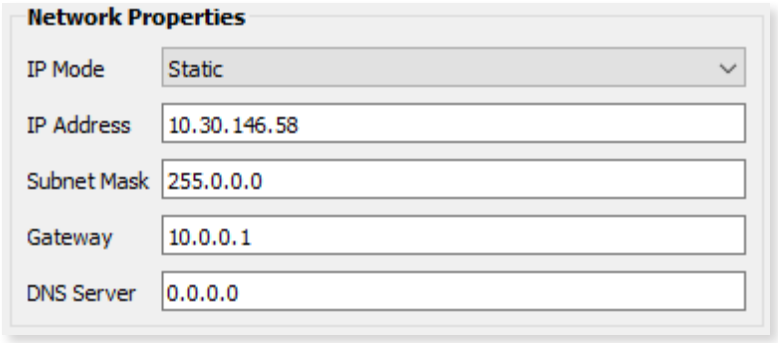


NTP SERVER

Set the server for NTP (Network Time Protocol). This is to ensure that security certificates are valid, when connecting to SixEye RMM. We recommend using **pool.ntp.org, time.windows.com, time.apple.com** or other publicly available servers**.**

If using the NTP server, ensure that the DNS Server and IP Gateway are set so the device knows how to get to the Internet to find a time server.

NETWORK PROPERTIES



IP ADDRESS

Internet Protocol address (IPv4) of the Gateway.

SUBNET MASK

User-configured subnet mask. Typically, 255.255.255.0 but must be set according to general networking rules.

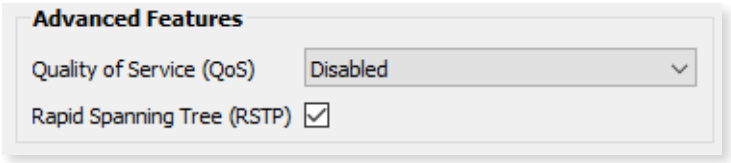
GATEWAY

Specify network gateway address if using **NTP server** and/or **SixEye RMM**.

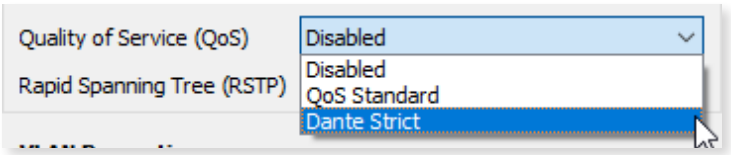
DNS Server

Set Domain Name Server for the device here. The DNS should be specified if using and **NTP server** and/or **SixEye RMM.**

ADVANCED FEATURES



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.

Disabled (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.

NOTE: remember that giving all data high priority is the same as treating all traffic equally.

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

RAPID SPANNING TREE (RSTP)

Click the checkbox to **Enable** / **Disable** (default) Rapid Spanning Tree Protocol (RSTP)

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.

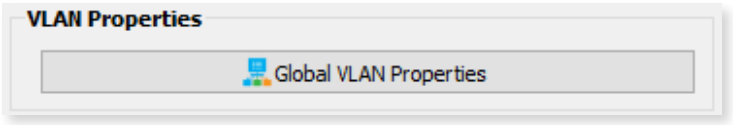
RSTP should be enabled on all switches on the network and not be used in conjunction with EAPS Ring Protection.

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 unmanaged 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: EAPS & RSTP - Ring Protection**.

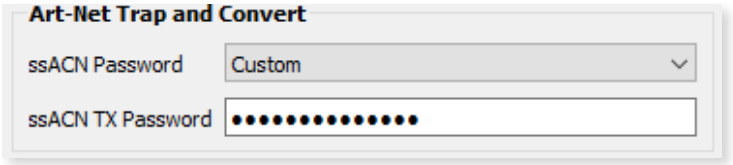
VLAN PROPERTIES



To enable/disable VLANs, click the **Global VLAN Properties** Button.

For more information on setting VLAN Properties, see the **VLAN Configuration** section later in this manual.

Art-Net TRAP AND CONVERT



When enabled, Art-Net data packets with broadcast address destinations are trapped and converted to E1.31 sACN or Pathway ssACN multicast packets, as the packets enter the port of the switch.

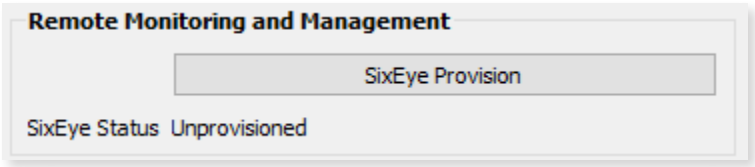
ssACN PASSWORD.

Specifies whether to use the **Domain Auto** or a **Custom** ssACN Transmit password.

If **Custom** is selected, the ssACN TX Password field will appear, as shown. Enter a custom TX password here.

See the **Introducing Pathway ssACN** section earlier in this manual for more details.

REMOTE MONITORING AND MANAGEMENT



For details on how to connect Pathway devices to a SixEye portal, see the **SixEye PROPERTIES** section in the **Pathscape manual**.

SixEye PROVISION

This button will open the SixEye Provision window. In this field, paste the SixEye Device Key and click **Provision**.

SixEye STATUS

This shows the status of the SixEye connection.

Unprovisioned (default).

No Internet Connection. There is a problem with the device finding an Internet connection. Check the device's IP Settings, specifically the Gateway.

DNS Failure. The device has found a connection, but there is a problem with resolving URLs. Check the device's DNS settings.

Invalid System Time. The device has connected to the Internet, but there is a problem with the System Time. Check the device's NTP server settings.

SixEye Init. The device is currently initializing a connection with SixEye.

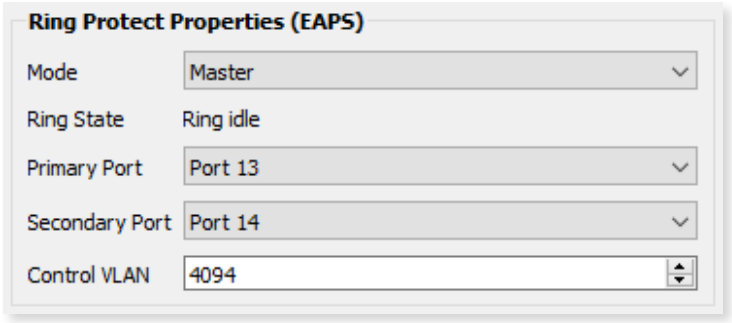
SixEye Init Error. The device could not initiate a connection with SixEye.

Not Connected. The device is not currently connected to SixEye.

Connected. The device is connected to SixEye.

RING PROTECT PROPERTIES (EAPS)

Allows VIA switches to be connected in a physical wiring ring using EAPS (Ethernet Automatic Protection Switching. See **Appendix 4: EAPS & RSTP - Ring Protection** for details).



MODE

Set the function for Ring Protect Mode.

Disable (default): Ring Protect is disabled. **When set to Disabled, the remaining Properties below are hidden**.

Transit: Sets the selected switch to act as a Transit switch.

Master: Sets the selected switch to act as the Master switch.

RING STATE

Shows the current state of the Ring. Values are:

Ring Idle. The ring is not currently doing anything; seen after enabling Ring Protect but before any attempt to initialize the ring has happened.

Ring Complete. The ring is initialized and working. The Master switch is monitoring the health of the ring.

Ring Failed. The ring integrity is broken.

Ring Initializing. The ring is currently initializing.

PRIMARY PORT

Select the port to be used as the Ring Primary Port. The Ring Primary Port must be one of the **last 4 ports** on the switch and must be different from the Secondary Port.

SECONDARY PORT

Select the port to be used as the Ring Secondary Port. The Ring Secondary Port must be one of the **last 4 ports** on the switch and must be different from the Primary Port.

CONTROL VLAN

Specifies dedicated Ring Protect VLAN. Valid range is 1 – 4095. Use of the default (4094) is strongly recommended. The Ring Protect VLAN **must to be outside of defined VLAN range**.

NOTES ON VLAN SETUP

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.

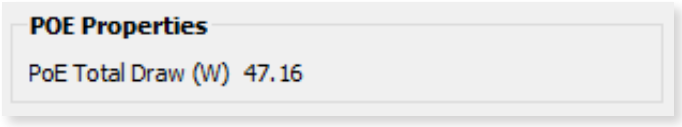
Prior to set up, determine which switch will be the master. Generally, the least busy switch with the most stable power source is the best choice. All other switches must be configured as transit switches.

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.

For additional details, see **Appendix 4: EAPS & RSTP - Ring Protection**.

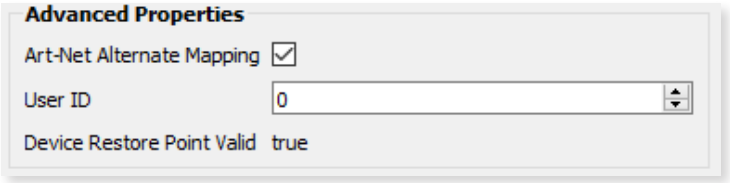
PoE PROPERTIES (POE Models)



PoE TOTAL DRAW (W)

Displays the current power draw from connected PoE devices.

ADVANCED PROPERTIES



ART-NET ALTERNATE MAPPING

Enabled (by default). When enabled, Art-Net Universe 0:0 is treated as Universe 1. When disabled, Art-Net universe 0:0 is ignored.

This feature is used in conjunction with the "**Art-Net Trap and Convert**" 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.

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 Art-Net Alternate Mapping is enabled, VIA switches will map Art-Net Universe 0-0 to Pathscape 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 Pathscape Universe 1.

USER ID

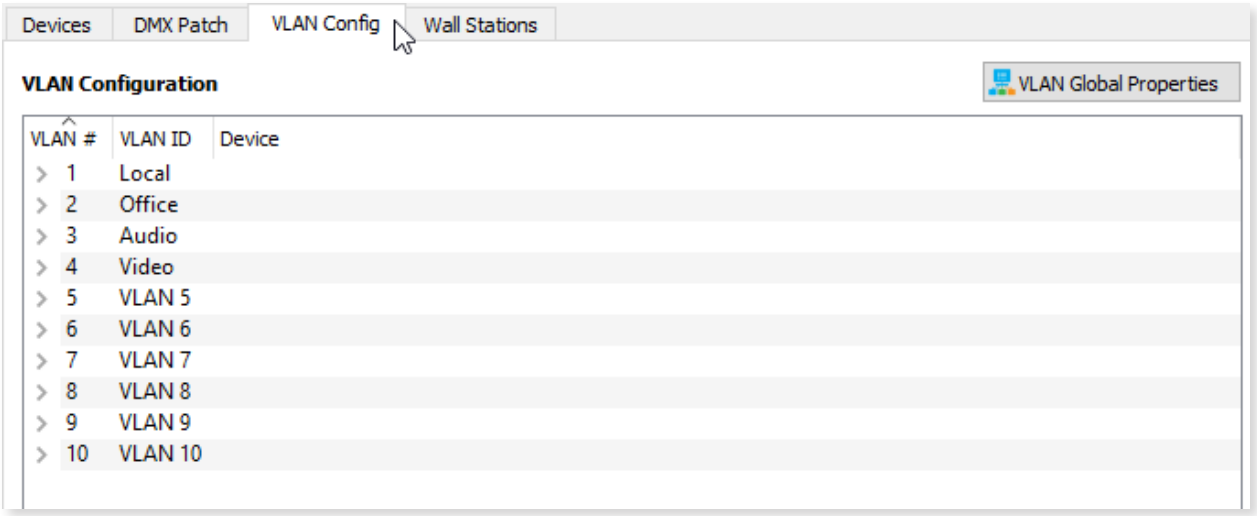
Custom numeric identification for external databases.

DEVICE RESTORE POINT VALID

Shows **True** of **False** depending on whether the current Device Restore Point is valid.

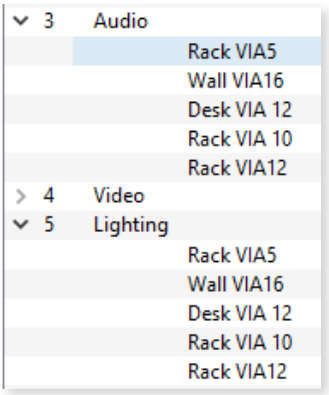
VLAN CONFIG

Use the **VLAN Config** tab to configure network VLANs. A **VLAN** (**V**irtual **L**ocal **A**rea **N**etwork) 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 switches must be "tagged" to pass all VLAN traffic. See **Appendix 3: VLANs** for further details on how to use VLANs.



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 seen in the example above, but simply labeled "VLAN 1", "VLAN 2", etc.

Click on the arrow next to each VLAN to see the Devices (VIA Switches) available for configuration.



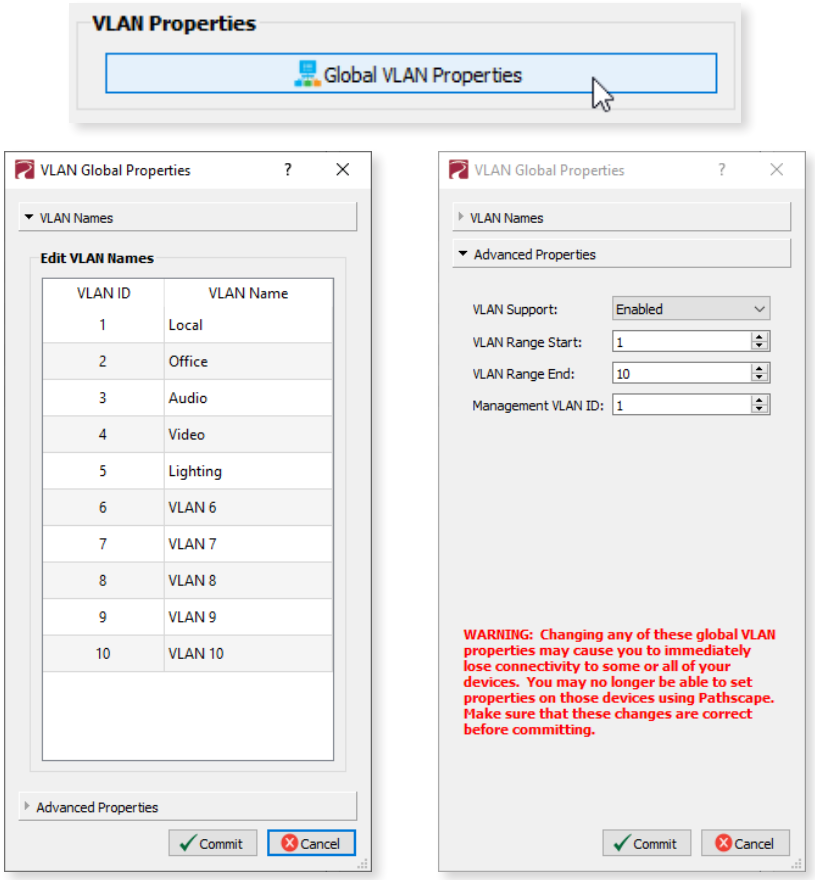
Note that every VIA Switch on the network will show up under every listed VLAN. VLAN ranges are configured Globally; it is not possible to assign a Switch to only one VLAN in this window. At the Subdevice/Port level, VLANs may be assigned as needed.

VLAN Properties such as **IP Address**, **DHCP** and **IGMP** settings are configured per VLAN per Switch. For example, to configure **VLAN 3** (Audio VLAN) as illustrated above, expand **VLAN 3** and click on the Switch device, and edit its Properties in the Properties pane. To edit **VLAN 5** on the same switch, expand **VLAN 5** and click on the Switch to edit **VLAN 5** on that device.

VLAN Properties are described below.

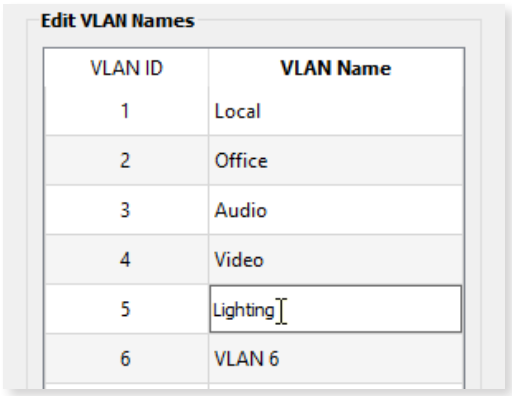
VLAN GLOBAL PROPERTIES

In order to use VLANs, **VLAN Support** must be enabled in **VLAN Global Properties**, which is accessed by clicking the VLAN Global Properties button in the top-right corner of the window. You can also click this button in the **VLAN Properties** section of the base device properties.



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

In the **VLAN Names** panel you may edit the names of any of the available VLANs by double-clicking on the VLAN Name, editing it and then clicking the Commit button.



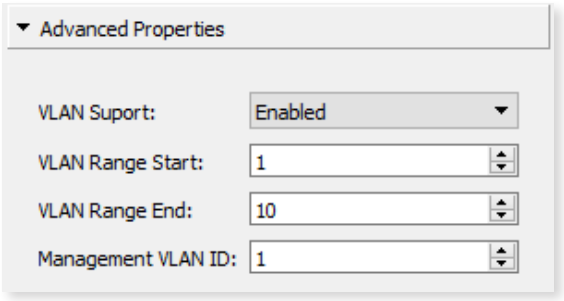
You will then see several transactions populate in the transaction editor, which will be automatically sent. To discard changes, click the Cancel button.

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

⚠ WARNING ⚠

Changing any of these global VLAN properties may cause you to immediately lose connectivity to same or all of your devices. You may no longer be able to set properties on those devices using Pathscape. Make sure that these changes are correct before committing.

See Appendix 3: VLANs for further details on how to use VLANs.



The **VLAN Support** drop-down allows for enabling or disabling of VLANs.

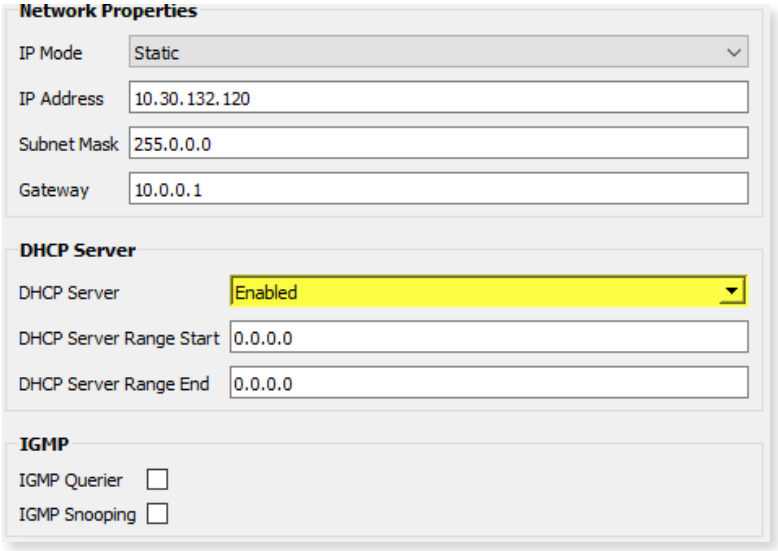
VLAN Range Start and **VLAN Range End** will determine the range of VLAN IDs available to use. Default is 1 and 10, respectively. To edit the start and end ID values, either type into the text fields or click on the up and down arrows to modify the value. To make the desired changes, click the Commit button. You will then see several transactions populate in the transaction editor, which will be automatically sent. To discard changes, click the Cancel button.

Management VLAN ID sets which VLAN is used by the switch management processor(s). Default is 1. **It is strongly recommended that the Management VLAN ID be set to the same value as the VLAN Range Start value. 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.**

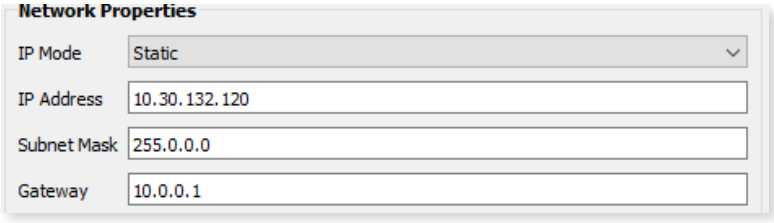
See Appendix 3: VLANs for further details on how to use VLANs.

VLAN PROPERTIES/SERVICES

VLANs must be enabled prior to configuring these services. You will find the VLAN Enable/Disable Property in the **VLAN Global Properties Window** in the VLAN Config window or under the **Settings Menu**.



NETWORK PROPERTIES



IP MODE

Disabled: No IP assigned to this VLAN by this VIA

Static: IP settings manually set by user (default for VLAN ID#1 / management VLAN). You must set a Static IP address if you want to enable DHCP and/or IGMP on this VLAN.

Dynamic: IP settings obtained from DHCP server.

IP ADDRESS

User-configured Internet Protocol address (IPv4) for this switch on the selected VLAN.

SUBNET MASK

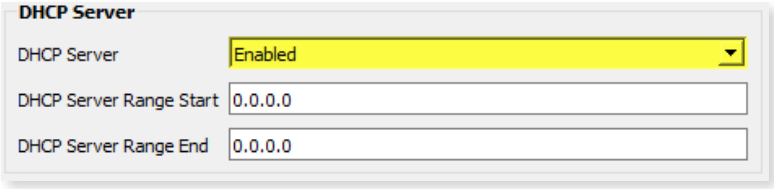
User-configured subnet mask applied to VLAN.

GATEWAY

Network traffic on this VLAN requesting addresses outside of the assigned subnet will be routed through this IP address.

DHCP PROPERTIES

DHCP SERVER



Dynamic Host Configuration Protocol (DHCP).

Disabled (default).

Enabled: Only one switch on a given VLAN may have an active DHCP service, and that VLAN must have a static IP itself. One switch with multiple VLANs may have multiple DHCP servers.

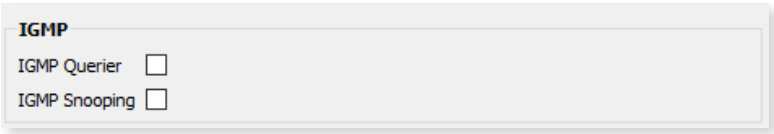
DHCP SERVER RANGE START

Sets start IP address in the DHCP pool. Pool must begin at an address higher than the IP address of the server.

DHCP SERVER RANGE END

Sets last available IP address in the DHCP pool. Cannot exceed the last valid IP value in the IP/Subnet Mask range.

IGMP



Intergroup Management Protocol (**IGMP**) allows for packet filtering and forwarding by the switch based on multicast groups. Networks using sACN can take full advantage of IGMP by reducing the traffic on the link to the gateway to just the Network DMX Universes the gateway is configured to listen to.

IGMP QUERIER

Disabled (default).

Enabled: Allows switch to query and construct a forwarding-table based on end device subscriptions to multicast group addresses. (i.e., the Querier can tell that a 2-port DMX512 gateway is interested in Univ 8 and Univ 37, if so patched, and will route those sACN Universes, and only those, on the link on which the gateway is connected.) One querier is required be active on a given VLAN using IGMP routing. However, for reliability reasons, it is highly recommended to have two or more.

IGMP SNOOPING

Disabled (default)

Enabled: Allows the switch to forward multicast data packets according to IGMP forwarding-tables build by the Querier. All switches on a VLAN using IGMP should have snooping enabled, including the switches acting as an IGMP Querier.

NOTES ON IGMP

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.

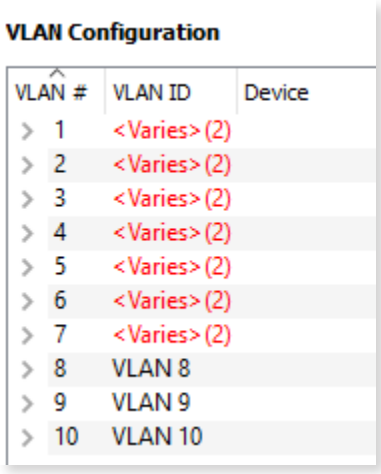
https://www.youtube.com/watch?v=CdXl_Q7KZC0

RESOLVING VLAN CONFLICTS

If you have set up your VLANs as described above, and you later add another VIA switch to your network that has different VLAN settings, you will likely see the following message in red at the bottom of the Pathscape window:

WARNING There are conflicting global VLAN property settings. Open the 'Network > VLAN Global Properties' menu item dialog to resolve the conflicts.

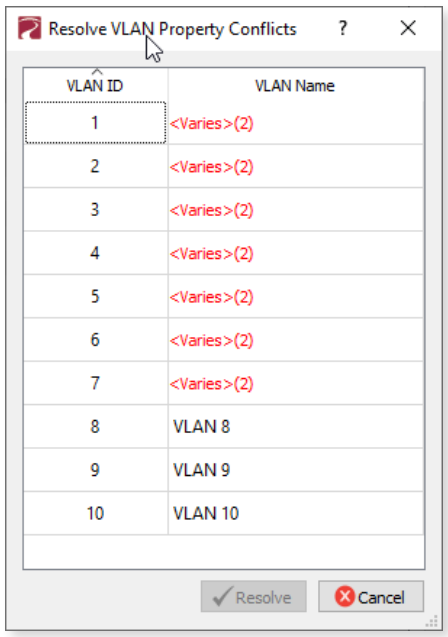
Go to the **VLAN Config** tab and you will see something like this:



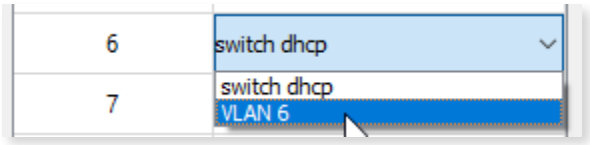
Because the VLAN properties are stored on each physical VIA switch, when a new switch comes online with different property values, Pathscape doesn't know which one(s) to use. For each VLAN ID that has multiple values associated with it, Pathscape will instead list the ID as "**<Varies> (X)**" with X being the number of different values found across all switches.

As described above, Pathscape requires VLAN settings to be Global across the entire network, so only one set of VLAN properties (including ID, VLAN Enable/Disable, VLAN Range, and Management VLAN) may be used.

You will have to resolve the conflicts before you can continue. Click the VLAN Global Properties button, and the **Resolve VLAN Property Conflicts** window will open.



For each VLAN ID with conflicting properties, you will need to double-click on each instance of "**<Varies> (X)**" and then pick the correct VLAN ID from the drop-down menu.



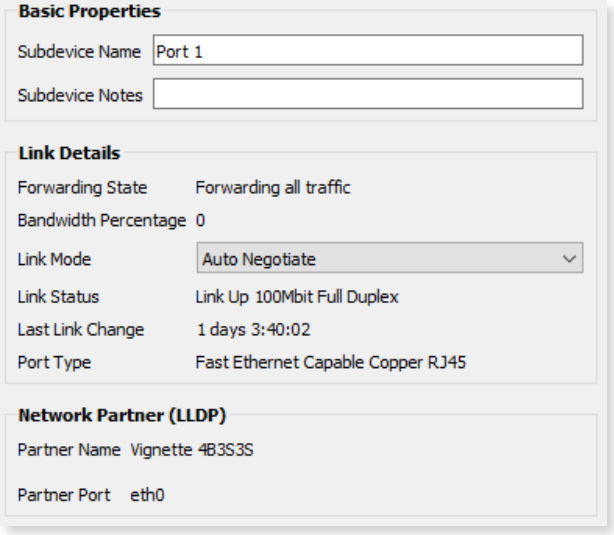
Pathscape will then use the settings associated with those VLAN IDs chosen to clear the found conflicts

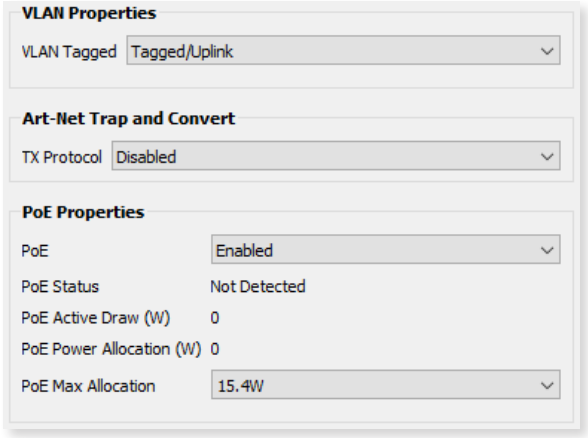
PORT PROPERTIES AND CONFIGURATION

VIA Switch subdevices are Ethernet Ports, either copper RJ45 Ports or SFP/fiber ports. The color of the Port icon reflects its Link Status and Speed.

Icon	Status
Grey RJ45	Copper RJ4: Link Down (no downstream device connected)
Blue RJ45	Copper RJ45: 1 Gigabit
Green RJ45	Copper RJ45: 100 Megabit, full or half duplex
Orange RJ45	Copper RJ45: 10 Megabit full or half duplex
Grey Fiber	SFP/Fiber: Link Down (no downstream device connected)
Blue Fiber	SFP/Fiber: 1Gigabit
Purple Fiber	SFP/Fiber: 10Gigabit

Not all properties are supported by all VIA models. Only the properties supported by the selected switch's port will be shown in the Properties Pane.

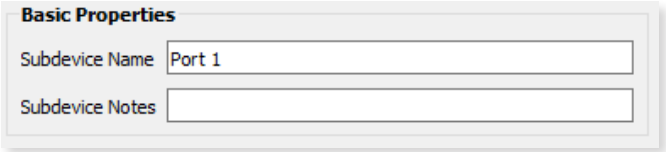




Port status and properties may be reviewed by expanding the device in the device tree, and clicking on the subdevice/port. The properties for that port will then be shown in the Properties Panel.

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

BASIC PROPERTIES



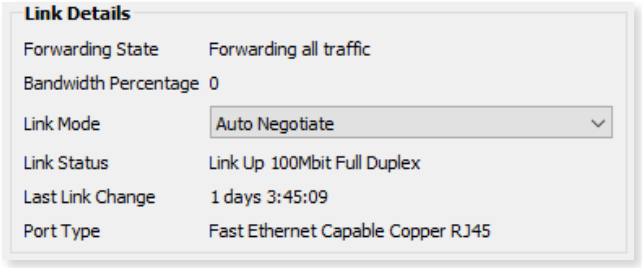
SUBDEVICE NAME

A user-configured, soft label for the subdevice/Port. Shown in the Device view and on the front panel display of the Switch (if equipped).

SUBDEVICE NOTES

A user-configured text description field, shown in the Device window.

LINK DETAILS



FORWARDING STATE

Status of RSTP and EAPS. Read-only.

Forwarding all Traffic: Normal state.

Blocked by RSTP: Loop detected and port blocked to stop feedback.

Blocked by EAPS: Ring using primary port.

BANDWIDTH PERCENTAGE

Reports a number between 0 and 100 based on Link Mode showing the amount of traffic going through the port. Readings are updated every few seconds. Read-only.

LINK MODE

Configures the Link Mode for the specified port.

Disable: Effectively turns port off.

Auto Negotiate (default): Link speed set by negotiation between switch and end device.

10Mbit Half Duplex

10Mbit Full Duplex

100Mbit Half Duplex

100Mbit Full Duplex

1Gbit Full Duplex (1Gbit Copper Ports Only))

10Gbit Full Duplex (SFP+ Ports Only)

LINK STATUS

Reports current link status and speed. Read Only.

LAST LINK CHANGE

Displays the time elapsed since the last change in the Port Link Status. Shown as **X Days, HH:MM:SS** (Hours:Minutes:Seconds). Useful for diagnostic or troubleshooting purposes to determine if a Port has gone down unexpectedly, for example.

SFP+ MODULE TYPE

Reports the detected type of SFP+ (enhanced Small Form-factor Pluggable) fiber optics adapter. Read Only. Applicable to Ports 13 and 14.

PORT TYPE

Reports Port Type. Read-only.

Gigabit Capable Fiber

10 Gigabit Capable Fiber

Gigabit Capable Copper RJ45

Fast Ethernet Capable Copper RJ45

NETWORK PARTNER (LLDP)

PARTNER NAME

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.

PARTNER PORT

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.

If the connected device is not a switch and has only one port, this will show "Eth".

VLAN PROPERTIES

Set VLAN Properties for the selected port.

VLAN TAGGED

When VLANs are enabled, set port as a **Tagged/Uplink** to transmit all VLANs' data between switches. Typically tagged ports are only used to connect a switch to a switch. Although it is possible to make a PC's NIC tagged, Pathway gateways and controllers do not used tagged NICs. If you cannot communicate with a gateway or controller, check that the port your PC is using and the port the devices is on are not tagged and on the same VLAN.

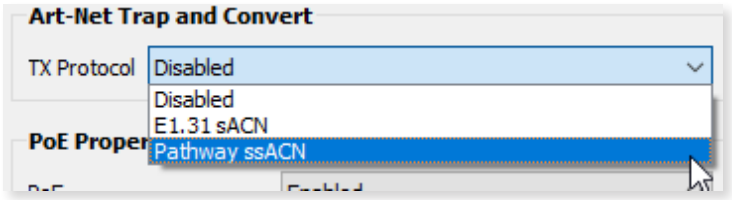
For most applications, **ports connected to end devices** should be set as **Untagged** (default).

VLAN

Sets the VLAN ID# used by the port. Only applies to untagged ports when VLANs have been enabled.

Art-Net TRAP AND CONVERT

See also **Art-Net Alternate Mapping** in the base device properties.



TX PROTOCOL

Disabled (default).

E1.31 sACN: Any inbound Art-Net broadcast packets are converted to **E1.31 sACN** multicast data packets using the same Universe number as originally transmitted. On large systems using sACN, you should enable IGMP to reduce network traffic.

Pathway ssACN: Any inbound Art-Net broadcast packets are converted to **Pathway Secure sACN (ssACN)** multicast data packets using the same Universe number as originally transmitted. On large systems using sACN, you should enable IGMP to reduce network traffic.

NOTES ON Art-Net TRAP AND CONVERT

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.

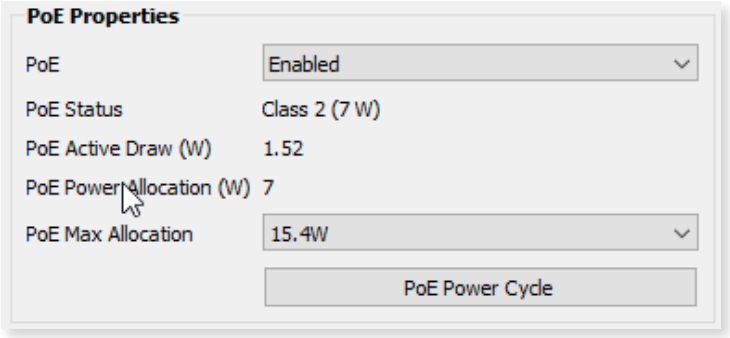
When enabled, Art-Net data packets with broadcast address destinations are trapped and converted to E1.31 sACN multicast packets, as the packets enter the port of the switch. The resulting multicast sACN packets may then be filtered using the IGMP settings. All other Art-Net broadcast packets, such as 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 NONPOE Model)



PoE

Enabled (default): Port will attempt to power any connected PoE-compliant device.

Disabled: PoE will not be provided to end devices.

PoE STATUS

PoE Class as reported by end device. Read-only.

Not Detected (end device not PoE)

Class 0 (15.4W)

Class 1 (5.4W)

Class 2 (11.7W)

Class 3 (15.4W)

PoE ACTIVE DRAW (W)

Reports current PoE device draw in Watts. Read-only.

PoE POWER ALLOCATION (W)

Reports power allocation to port based on end device's reported PoE device classification. Read-only.

PoE MAX ALLOCATION

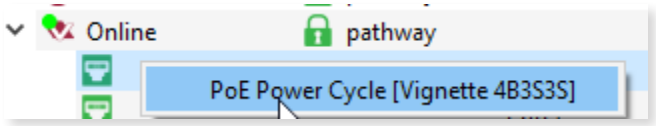
Sets power allocated to port. Allows switch to determine remaining PoE power pool available, but does not prevent end devices from requesting and utilizing power in excess of this value.

Values are **900mW, 1.8W, 2.7W, 3.6W, 4.5W, 5.4W, 6.3W, 7.2W, 8.1W, 9W, 9.9W, 10.8W, 11.7W, 12.6W, 13.5W, 14.4W and 15.4W**.

PoE POWER CYCLE

Clicking this button will disable and then re-enable PoE on the selected port, in order to power cycle the end device.

You can also right-click any VIA Port in the Device view and select PoE Power Cycle.



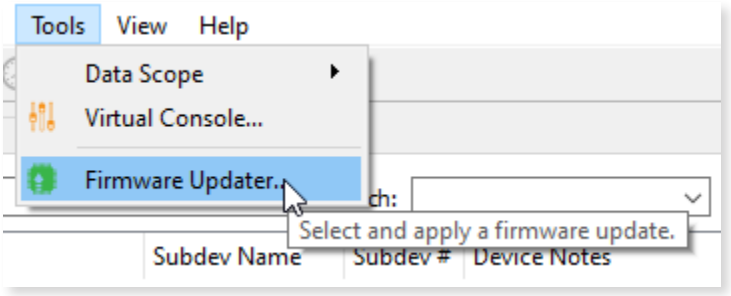
If the connected device supports LLDP, the device's name will appear so you know exactly what device you're power cycling

UPGRADING DEVICE FIRMWARE

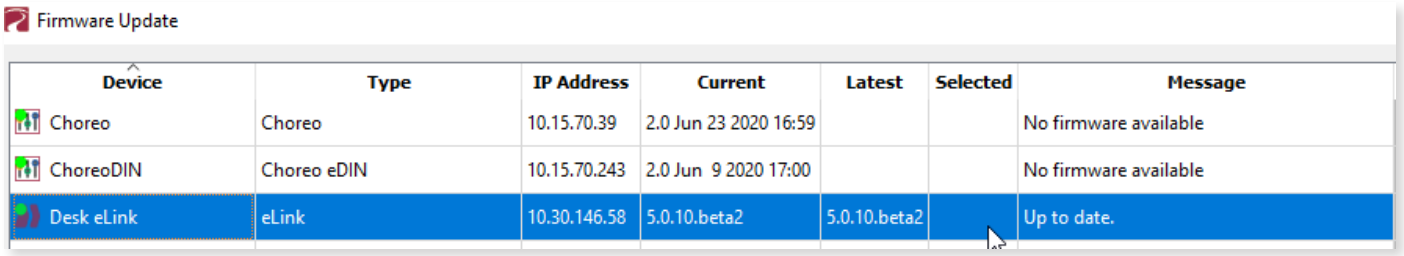
Firmware upgrades may only be done using Pathscape.

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

To upgrade a device, ensure the device's IP address is configured correctly and is on the same subnet and IP range as the computer. Open Pathscape, click the Tools menu, and select the **Firmware Updater...** menu item.



This will bring up the Firmware Update window.



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.**

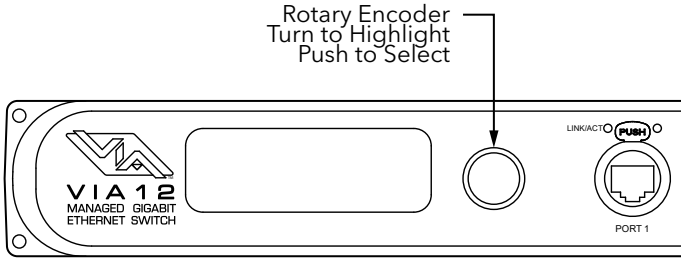
It is strongly recommended that you do not update VIA Switches and connected PoE devices at the same time. It is possible for the firmware update process to reboot the Switch before the data has finished writing to the PoE devices' memory. If the VIA Switch reboots at this point, the connected PoE devices' 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.

FACTORY DEFAULT

In the event of a loss of communication with the device (e.g. 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.




```
Base Configuration
Network Setup
Device Info/Status
Advanced Settings
Admin/Security
<Back>
```

Scroll the encoder knob until "**Admin/Security"** is highlighted, and click in the knob. Under the Admin/Security menu, scroll down to "**Factory Default**", and click in the knob.

```
Admin/Security
Factory Default
Manage Restore Point
Reset Security
Reboot
<Back>
```

This will show the Factory Default menu. Here you have several options.

```
Factory Default
Keep Net Setup & Restore Pt.
Keep Restore Point
Wipe All Configuration
<Back>
```

If you choose **Wipe All Configuration** it will completely restore the device to the same state as it left the factory. This will erase any Device Restore Point saved on the unit.

You can also choose **Keep Restore Point** to preserve any saved Restore Point, but be aware that the restore point could have saved properties that are the cause of the communication loss, and recalling that restore point could cause the same issues.

The device will then reboot, having reset itself to the Factory settings. Before configuration can be restored, the unit must be secured (either by adding to a Security Domain, or enabling Local Security).

FRONT PANEL LOCKOUT

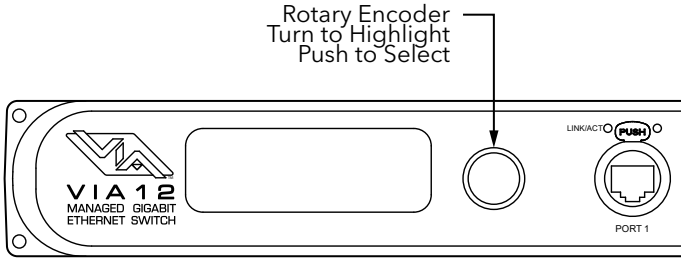
If the device has **Front Panel Lockout** enabled, you will not be able to make changes from the front panel. To address this, there is a 30-second delay before the LCD Lockout takes effect, after the switch boots up.

First, hard reboot the device (unplug and re-plug the AC power source), and then **within 30 seconds** after the device has booted up, perform the above action. After 30 seconds, the front panel UI will be locked out again.

FRONT PANEL UI AND MENU

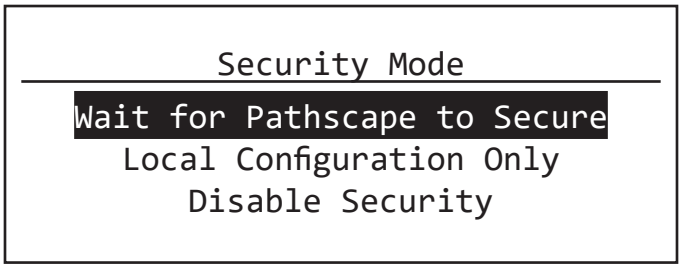
The PWVIA RM P12 models feature a front panel UI, consisting of an LCD and a rotary pushbutton encoder for navigating menus and selecting options.

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.



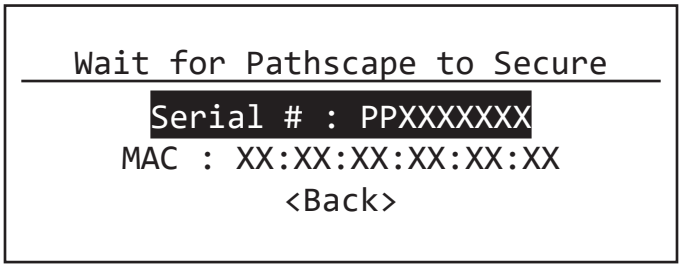
SETTING SECURITY MODE

When the device boots up for the first time, or if it has been Factory Defaulted or had its Security Settings reset, the Security Mode screen will be shown.

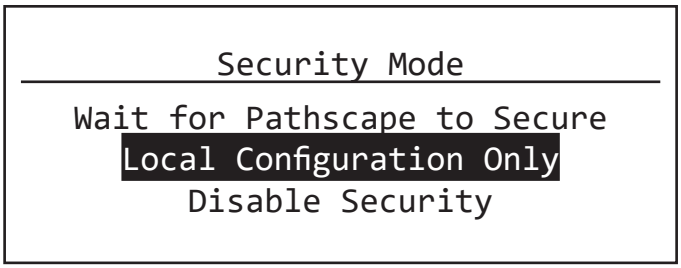


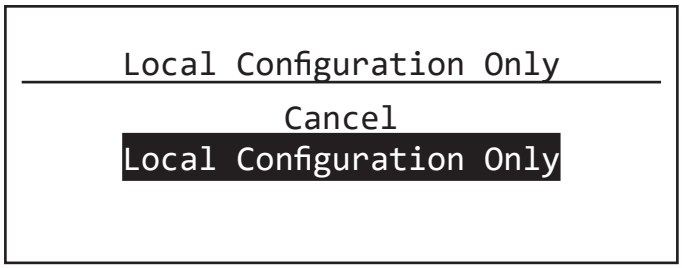
Before you can configure and use the device, you must either:

- **Use Pathscape to Secure the device** (Add it to a Security Domain). **No input from the front panel is required here**. Clicking the encoder knob to select **Wait for Pathscape to Secure** will show the device Serial Number and MAC Address, in cases where this may be helpful for device identification.



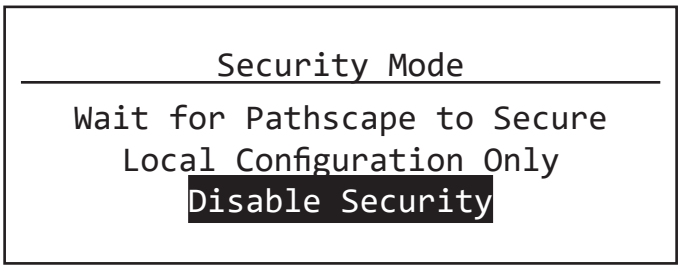
- Enable **Local Configuration Only** (Read only) mode. Turn the encoder to select **Local Configuration Only**. In the submenu, confirm by selecting **Local Configuration Only** again. You will then have full access to the menus.

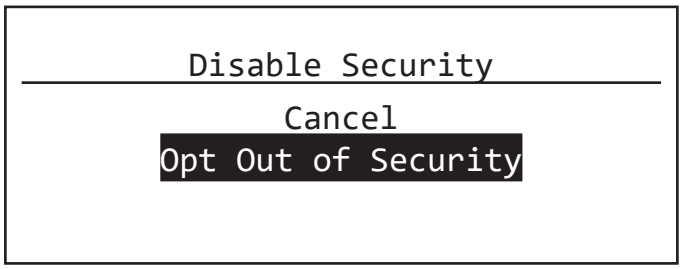




In Local Configuration / Read Only mode, **Pathway ssACN** (Secure sACN) is not available for use with **Art-Net Trap & Convert**. As explained above, you cannot use Pathscape to configure the device in this mode.

- **Disable (Opt out of) Security features** altogether. **This mode of operation is not a recommended practice**. However, if the production is on a dark network with a known crew, risk assessment may be weighed against convenience.





- From the **Security Mode** menu shown on the LCD, turn the encoder to select **Disable Security**. In the submenu, confirm by selecting **Opt Out of Security** again.
- You will then be able to access the menus. The device will appear in Pathscape with the Security Domain shown as "**Disabled by User**". It will behave like a legacy device; all properties will be Read/Writable.
- On the front panel display, the bottom line will show "`Security: Disabled by User`" as a reminder and warning.

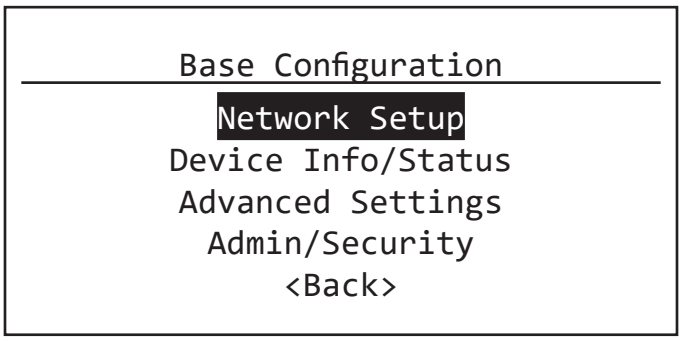
MAIN DISPLAY MESSAGES

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.

If the switch has been set to Disable security features, it will show "`Security: Disabled by User`" as a reminder and warning.

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

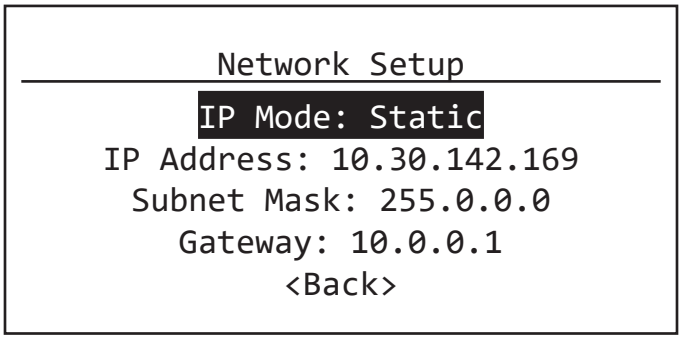
If using Pathscape, it is possible to enable the option **Front Panel Lockout**, which disables the ability to make any changes to the switch from the front panel UI. You can still navigate the menus to review settings, but cannot change any properties.

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

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.**

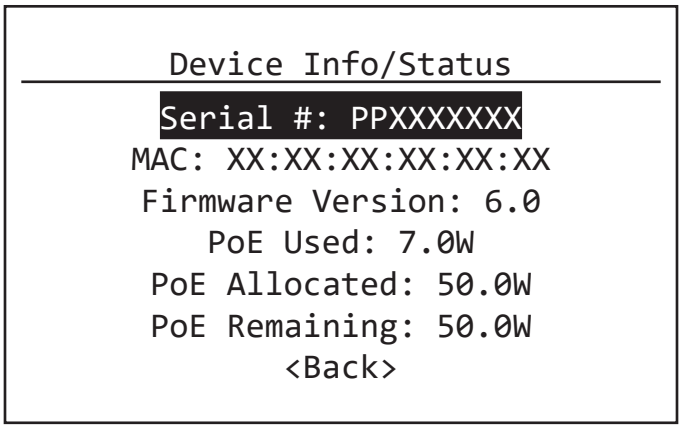
If the IP Mode is set to “Dynamic” on a system with no active DHCP server, the switch will auto-generate IP settings in accordance with zeroconf standards, in the IP range of 169.254.x.x/16. This range may not be suitable for connection to entertainment systems.

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.



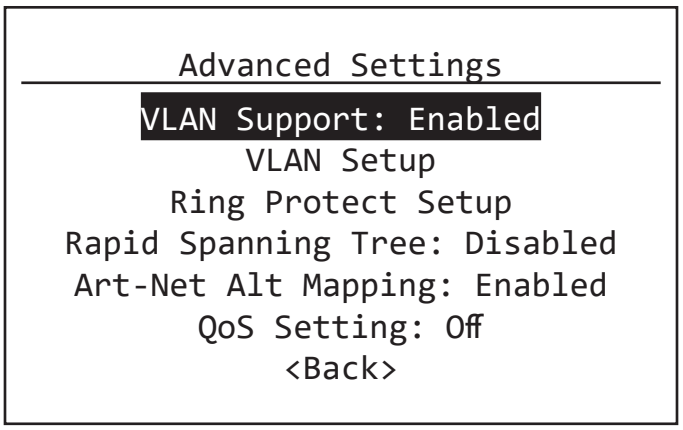
Menu Item	Description
Serial #	Factory-assigned, Pathway serial number. Read-only.
MAC	Factory-assigned media access control (MAC) address. Read-only.
Firmware Version	Current operating firmware version. Firmware may be updated using Pathscape. Read-only.
Ring Protect State (if enabled)	**OK**: Ring 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 **PWVIA RM P12 RJ45EC [xxxx] NONPOE** hardware does not support PoE. **Connected PoE-enabled devices will not receive power from the switch.**

VIA models PWVIA RM P12 RJ45EC [xxxx] POE 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.

Menu Item	Description			
VLAN Setup	VLAN Config/Status	VLAN ID#	Network Setup	See below
			DHCP Server (available if IP Mode set to Static)	See below **Disabled (default)** **Enabled**
			IGMP Snooping	**Disabled (default)** **Enabled**
			IGMP Querier	**Disabled (default)** **Enabled**
			Current Multicast Groups	See below
Ring Protect Setup	Ring Protect Mode	**Disabled (default)**: Ring is turned off. **Transit**: All switches but one Master are set at Transit. **Master**: Switch with master responsibility for monitoring Ring. Only one Master is allowed.		
	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.		
	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 *outside* the range set in VLAN setup. Default is **VLAN 4095**.		
Rapid Spanning Tree	**Enabled (Default)** **Disabled**			
Art-Net Alt Mapping	Art-Net Alternate Mapping. **Enabled (Default)** **Disabled**			

Menu Item	Description
QoS Settings	Quality of Service Settings. **Off (Default)** **Standard** **Date Strict**
<Back>	Returns to previous menu.

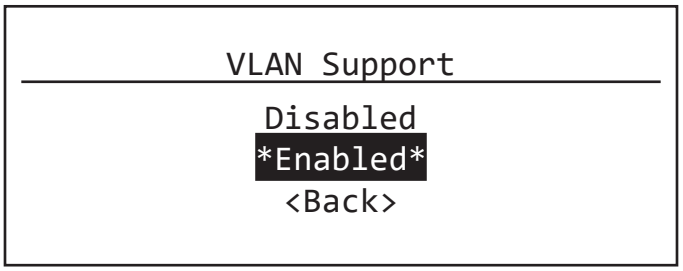
Plan your VLAN layout before attempting configuration. The creation of a map of the network, showing which devices and which ports to associate with a given VLAN, is strongly recommended prior to configuration.

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)**.

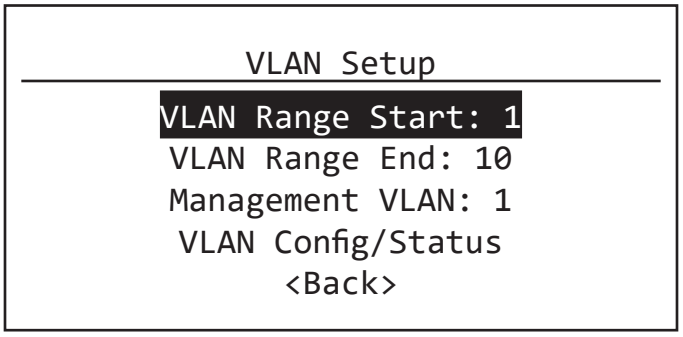
VLAN SUPPORT

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.

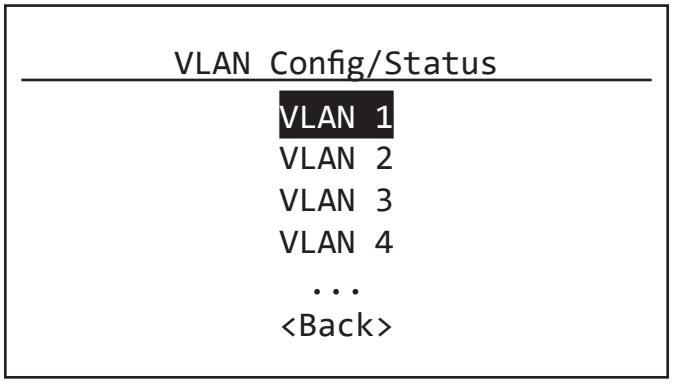


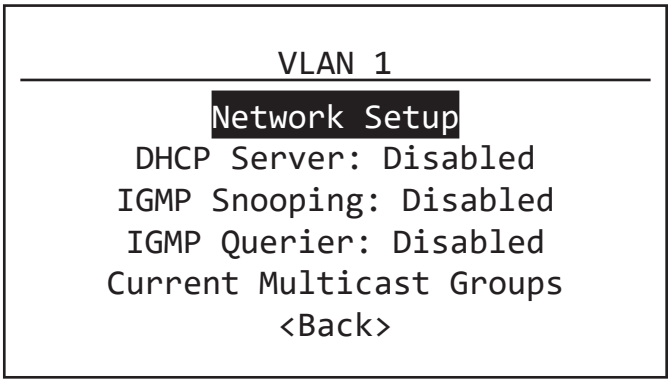
If the **Management VLAN** is accidentally set to a value outside the VLAN range, it may be necessary to use the **Factory Default** function from the **Utilities** menu to restore communication with the management processor and allow further configuration.

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.

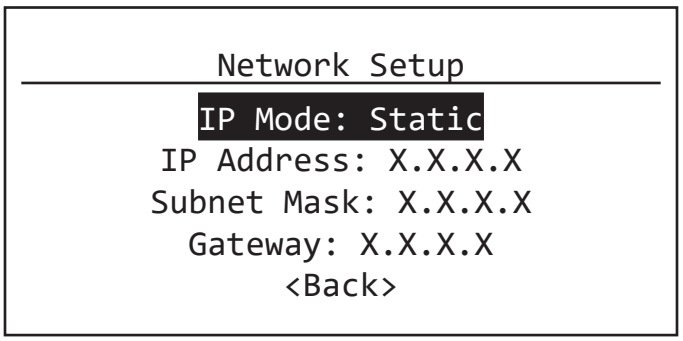




The VLAN ID# is assigned to individual ports from the Port Configuration menu (see below for **Port Status and Configuration Menu**).

VLAN CONFIG/STATUS: NETWORK SETUP

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



Menu Item	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. **<Back>**: Return to previous menu
IP Address	Manually sets IP address (IPv4). Turn encoder to set each octet. Push to accept and move to next octet. Illegal values are not accepted.
Subnet Mask	Set subnet mask for VLAN. Only valid masks are shown. Turn knob to select from list of valid masks.
Gateway	Set default gateway for VLAN. Only valid gateways are accepted. 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.
<Back>	Return to previous menu.

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

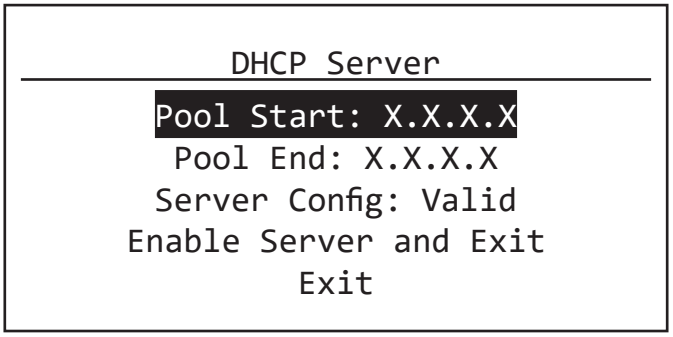
VLAN CONFIG/STATUS: DHCP SERVER

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.

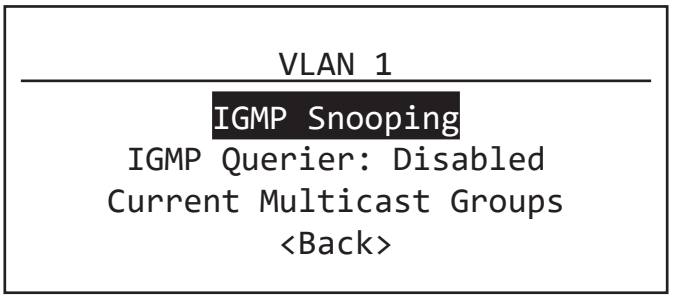


Menu Item	Description
Disabled	DHCP Service is turned off. Use this setting for all static (manually-set) IP systems, and for all switches other than the VLAN’s designated DHCP server host. **To enable DHCP**, click the knob in and set up the DHCP Pool Start and End, as below.
Enabled	Enables DHCP server. 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 entires 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.



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.

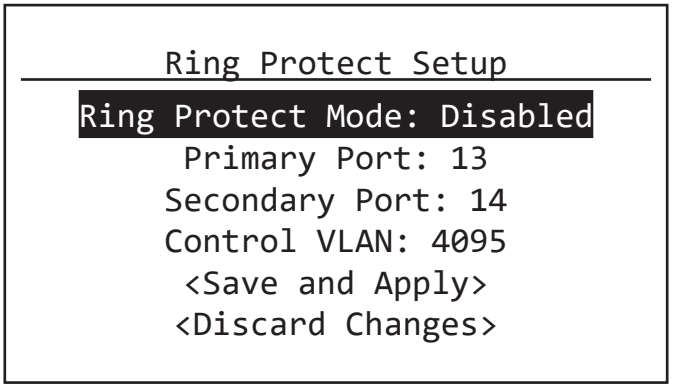
The IGMP Snooper allows the switch to more efficiently route multicast traffic by applying the multicast groupings as a filter. Multicast traffic is only directed to only those ports, i.e. end devices, that have requested to receive that traffic.

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.



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 fall-back 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 *outside* 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 unmanaged switches may not be detected correctly. Pathway's implementation of Rapid Spanning Tree Protocol is inter-operable 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
Art-Net Alt Mapping	Turn Art-Net Alternate Mapping on or off. **Enabled (Default)** **Disabled**
<Back>	Return to previous menu.

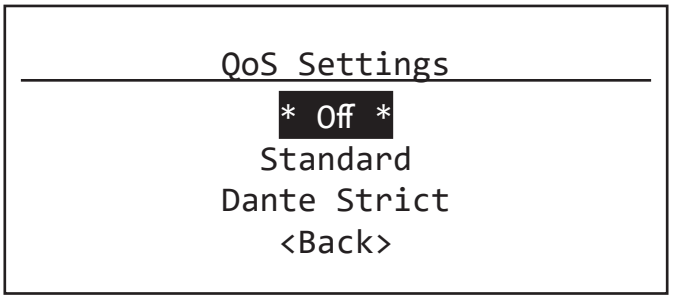
The Art-Net protocol uses two hexadecimal numbers, a 'subnet' and a 'universe', to define its DMX universe numbering. Numbering is usually shown as # - # and the valid range is from 0 - 0 (zero-zero) to F- F.

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.

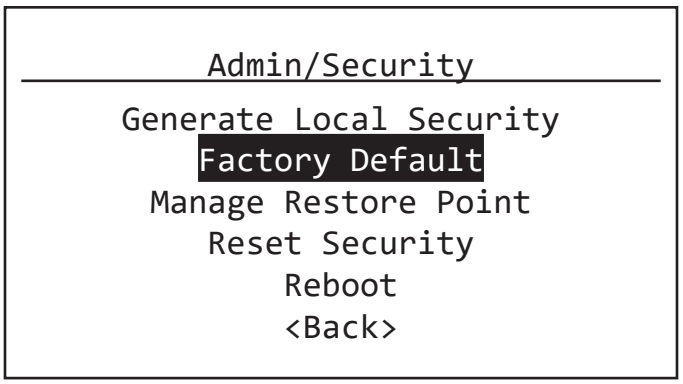


Menu Item	Description
Off (Default)	Disables QoS-based routing. All traffic is treated equally.
Standard	Traffic priority is observed using a weighted algorithm to ensure timely delivery of high priority traffic and eventual delivery of lower priority packets.
Dante Strict	Traffic priority is strictly 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**.

ADMIN/SECURITY

This menu contains settings and sub-menus pertaining to rebooting or factory defaulting the device, creating or recalling device restore points, or generating or resetting security settings.

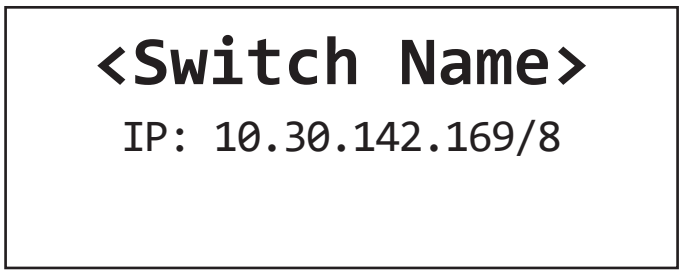


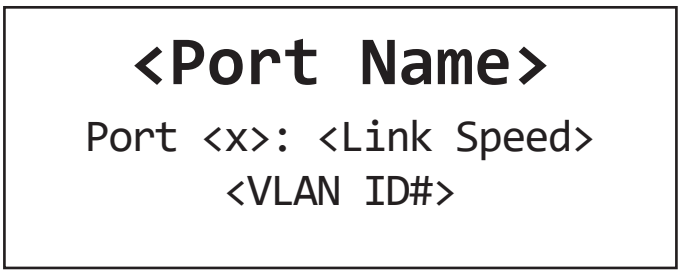
Menu Item	Description
Generate Local Security	**Will appear only when device is not secured,** e.g. when powered on for the first time, or after being factory defaulted or after having security settings reset. Selecting this will generate local security for the device. You will be able configure the device using the front panel **only**; you will **not** be able to change settings using Pathscape. Additionally, some functionality will be **unavailable** (i.e. Pathway ssACN and Custom Patches). To enable Pathway ssACN and configuration using Pathscape, the device must be added to a Security Domain. If already Locally Secured, you must factory default the device or reset its security settings, then use Pathscape to add it to a Security Domain. See the Security section earlier in the manual for detailed instructions. Once the device is secured (whether by Local Security or a Security Domain) this menu item will not be shown.
Factory Default	Allows you to restore the device to its factory settings, with a few options. You may choose to: **Keep Net Setup & Restore Pt.**: Resets all device settings except current network settings and any saved restore point. **Keep Restore Point**: Resets all device settings, including network settings, but keeps any saved restore point. **Wipe All Configuration**: Resets all device settings, including all network settings, security settings and deletes any restore point. For each option, you will have to confirm your decision to factory default the device. <Back>: Return to previous menu without resetting the device.

Menu Item	Description
Manage Restore Point	Allows you to create, update or recall the Device Restore Point. A Device Restore Point is a saved copy of all device settings, allowing you to restore the device back to a known state or preferred configuration at any time. Note that there can only be one restore point on a device at a time. **Create**: Saves a new restore point if none already exists, copying all the device's current settings. **Update**: Overwrites the existing restore point with the device's current settings. **Recall**: Recalls the restore point and overwrites the current device settings with those saved in the restore point. <Back>: Return to previous menu.
Reset Security	Allows you to reset the device's security settings without affecting the rest of the device configuration. You will then be able to choose a new Security Mode for the device. After selecting this menu item you will be asked to **confirm** your decision.
Reboot	Will cause the device to soft reboot. After selecting this menu item you will be asked to **confirm** your decision.
<Back>	Return to previous menu.

PORT STATUS AND CONFIGURATION MENU

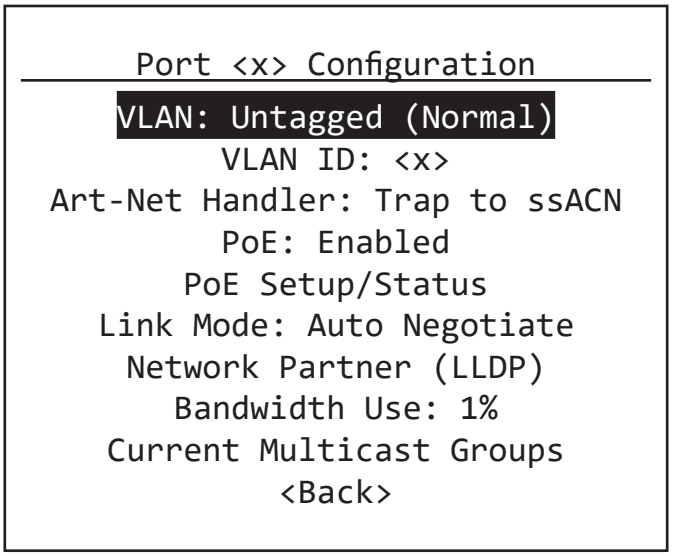
Port Status may be reviewed by turning to encoder knob to reach the desired port, from the main screen showing the switch name and IP address. The LCD shows the following information.





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.



Some menu items may not be displayed; i.e. VLANs, Network Partner (LLDP), Current Multicast Groups, if VLANs are not enabled, or LLDP-compliant devices are not detected.

VLAN

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 Pathscape.

Art-Net 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
Disabled (default)	Art-Net Trap and Convert is disabled. Art-Net data is routed as normal broadcast traffic to all devices on the current VLAN
Trap to sACN	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.
Trap to ssACN	Same as the above, only Art-Net data packets are converted to Pathway ssACN (Secure sACN).
<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.

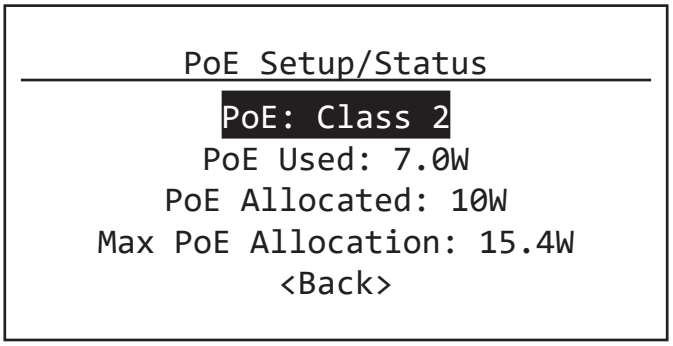
PoE

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).



Menu Item	Description
PoE: Class <x>	Shows the PoE Class as reported by the connected device. Read-only. **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. Read-only.

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. Read-only.
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 PWVIA RM P12 RJ45EC [xxxx] NONPOE does not have hardware to support IEEE 802.3af Power-over-Ethernet. Any PoE-enabled devices connected to a this model switch will not be powered. Models PWVIA RM P12 RJ45EC [xxxx] POE have 100W of on-board PoE to power external devices.

NETWORK PARTNER (LLDP)

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.

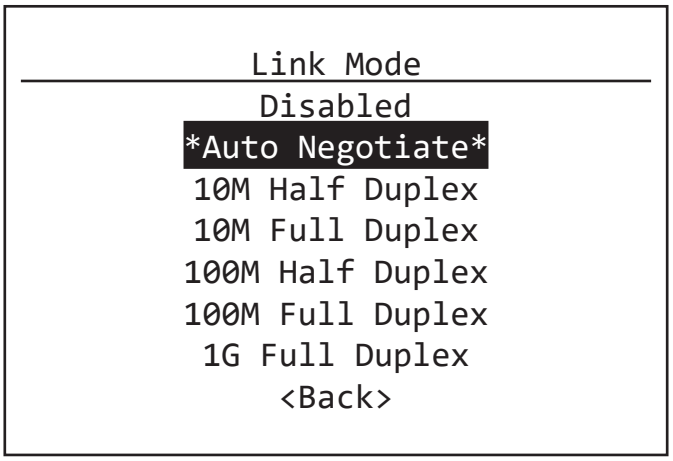
The information shown in the chart may be retrieved and shown on the VIA RM P12's LCD, for each Pathport LLDP-enabled device connected to the switch, on a port-by-port basis. It can take up to 30 seconds for this menu item to appear once a link goes active. Other LLDP-enabled devices may return different 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, “VIA Rack-mount PoE Switch”
Serial Number	Device Serial Number
Firmware Version	Current device operating firmware version
MAC Address	Device Media Access Control (MAC) Address
<Back>	Return to previous menu.

PORTS 1-12: LINK MODE

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



Menu Item	Description
Link Mode	**Disabled**. Turns port off. **Auto Negotiate (Default, recommended)**: Switch and connected device determine fastest mutually supported speed. **10Mbit Half Duplex** **10Mbit Full Duplex** **100Mbit Half Duplex** **100Mbit Full Duplex** **1GBit Full Duplex**
<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.

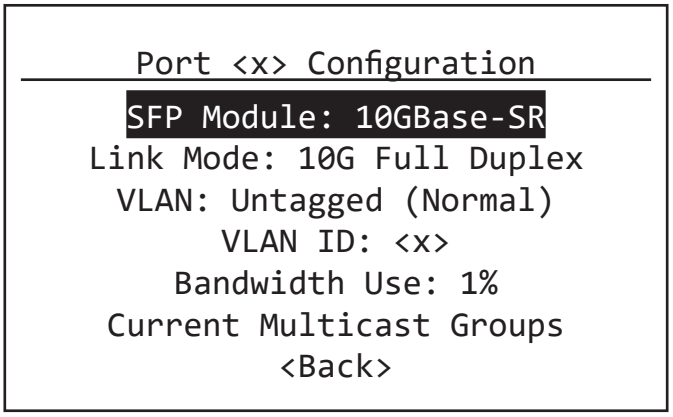
CURRENT MULTICAST GROUPS

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.



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.
Link Mode	**Disabled**. Turns port off. **1GBit Full Duplex** **10G Full Duplex**
VLAN	VLANs must be enabled in the Advanced Settings menu for this option to be shown. **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.
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.
Network Partner (LLDP)	Shows LLDP Partner device attached to this port, if applicable. **This property is only shown when a LLDP-compliant device is connected to the port in question.**
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 1GBit, a bandwidth use of 10% is equal to approximately 100Mbit of traffic per second. This menu item is read-only

Menu Item	Description
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
<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 PWVIA RM P12 Gigabit switches allow the end user to provide a fiber adapter. The adapters are typically referred to as an SFP (Small Form Pluggable transceiver) or mini-GBIC (gigabit interface converter).

Pathway catalog number PWACC SFP is an SFP 850nm Ethernet Optical Transceiver that is compatible with PWVIA RM P12, PWVIA DIN P16 and PWVIA DIN P8, capable of 1Gbps. Catalog number PWACC SFPP is a dual-rate SFP+ 850nm Ethernet Optical Transceiver capable of 10Gbps, compatible with the PWVIA DIN P8 and PWVIA RM P12 models. 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 Pathscape the Subdevice properties panel will indicate the link status, SFP module type, as well as the LLDP partner.

NOTE: The PWVIA RM P12 RJ45EC NONPOE and PWVIA RM P12 RJ45EC POE will work with 1000BASE-SX, 1000BASE-LX (1Gbps) and 10GBase-SR and 10GBase-LR (10Gbps) fiber modules.

The PWVIA RM P12 RJ45EC NONPOE and PWVIA RM P12 RJ45EC POE 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 Pathscape software. Refer to the Pathscape 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 PWVIA 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#							
Art-Net to sACN							
PoE Max Allocation							
Link Mode							
SFP Type							

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

APPENDIX 4: EAPS & RSTP - “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 without RSTP or EAPS setup will quickly ‘break’ your network. **Only one data path between any two devices is allowed.**

Pure star-wiring layouts leave your network prone to a single point of failure. Unlike DMX512 networks, passive data “thru” connections are not possible with Ethernet. A severed cable or power loss to a switch can mean the loss of some or even all show control.

Ring Protection allows the deliberate – and designed – use of a ring wiring system for Ethernet communications. With EAPS or RSTP enabled, PWVIA 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.

Ethernet Automatic Protection Switching (EAPS) uses dedicated tagged ports whereas **Rapid Spanning Tree Protocol (RSTP)** can use any two ports on a switch. Fail-over time when using EAPS on dedicated ports is between 50 and 75 milliseconds, or two to four DMX packets.

Using RSTP, the healing process can take a second or two. Unlike EAPS, 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. PWVIA 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.

REQUIREMENTS AND LIMITATIONS

VLANs must be enabled to use Ring Protection. EAPS uses a dedicated VLAN to monitor the integrity of the ring. By default, VLAN 4094 is used. The Ring Protection VLAN must be outside of the established VLAN range.

Only ports 11 through 14 support this feature.

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

DEFINITIONS FOR EAPS

Master switch monitors the integrity of communications. **Only one switch on the network may be configured as the master.**

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

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.

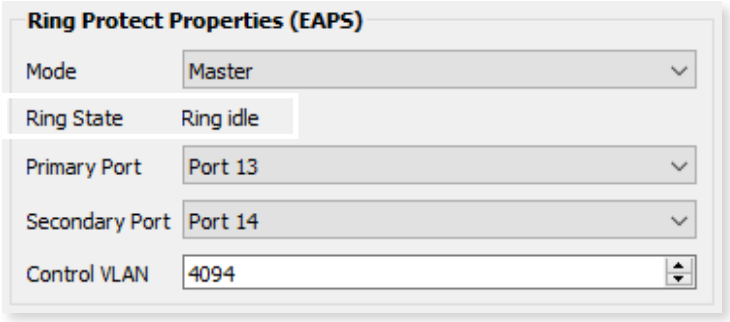
Secondary port is an UPLINK port “ignored” (logically blocked) by the Master switch to break the ring topology. All transit switches also must have one port configured as the secondary port. The secondary port is actively used on transit switches. Only ports 11 through 14 are available to be used as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

Control VLAN is a unique VLAN ID dedicated to monitoring the health of the network. All switches must use the same control VLAN. The default is VLAN ID 4094.

NOTE: Ring Protection wiring topology is not structured. Primary ports can be connected to either the Primary or Secondary port on the next VIA.

SOFTWARE CONFIGURATION OF RING

- Start with the redundant wiring segment unplugged.
- Connect the computer running Pathscape to one of the end switches, in the wiring chain.
- Configure the switch that is physically furthest away on the chain. Work backwards until reaching the closest switch.
- Now plug in the redundant wiring segment. Check the message on the LCD of the switch, which should change within a few seconds from “Ring Protect State: Failed” to Ring Protect State: Complete”. You can also check the **Ring State** property under Ring Protect Properties (EAPS) section in Pathscape.



- If the “Failed” message does not clear, unplug the redundant segment and check the port settings of each switch for misconfiguration.

APPENDIX 5: 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 6: ELECTRICAL AND COMPLIANCE INFORMATION

ELECTRICAL INFORMATION

MODEL PWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] NONPOE

- Power input: 100-240VAC, 50/60Hz
- 25W maximum power consumption

MODEL PWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] POE

- Power input: 100-240VAC, 50/60Hz
- 125W maximum power consumption (25W for switch, Integrated 100W PoE supply for connected PoE devices; Class 3 PoE (15.4W maximum per port)

MODEL PWVIA RM P12 RJ45EC [DUO/QUAD] POE

- Power input: 100-240VAC, 50/60Hz
- 125W maximum power consumption (25W for switch, Integrated 100W PoE supply for connected PoE devices; Class 3 PoE (15.4W maximum per port)
- Additional 10A maximum current draw if using powerCON AC Thru. **Do not connect more than 6 VIA switches together using the THRU connector and one AC input. Do not exceed 10A draw through the first switch.**

COMPLIANCE

- ANSI E1.31 sACN - Streaming ACN
- IEEE 802.3 Ethernet
- IEEE 802.3af Power-over-Ethernet (PoE) (POE Models)
- IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
- IEEE 802.1Q VLAN Support
- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- California Title 1.81.26, Security of Connected Devices
- ETL
- CE
- RoHS 2011/65/EU + A1 2015/863

ENVIRONMENTAL

- Operating Temperature: 14°F to 122°F (-10°C to 50°C)
- Relative Humidity: 5-95%, non-condensing

PHYSICAL

PPWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] NONPOE

- Weight: 4.7 lbs (2.1 kg)
- Dimensions: 17” W x 1.7” H x 7” D (432mm W x 43mm H x 178mm D) [without rack-mounting hardware]

PPWVIA RM P12 RJ45EC [SFPSLOT/1GSFP/10GSFPP] POE

- Weight: 5.2 lbs (2.4 kg)
- Dimensions: 17” W x 1.7” H x 7” D (432mm W x 43mm H x 178mm D) [without rack-mounting hardware]

PPWVIA RM P12 RJ45EC [DUO/QUAD] POE

- Weight: 5.3 lbs (2.4 kg)
- Dimensions: 19” W x 1.7” H x 12” D (483mm W x 43mm H x 305mm D)