Pathway®
Connectivity Solutions

6708 VIA8 Gigabit Ethernet Switch

User Guide and Manual

2/18/2020

1439 17 Ave SE • Calgary, AB • T2G 1J9
Phone +1 (403) 243-8110
www.pathwayconnect.com

Table of Contents

About VIA Ethernet Switches

Pathway VIA Ethernet switches are designed for live entertainment Ethernet systems, including audio and DMX-over-Ethernet networks. This manual covers the 6708 VIA8 model.

The VIA Ethernet Switch is intended specifically for signal routing between Pathport DMX-over-Ethernet nodes, 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 VIA8 is easily configured and upgraded using the freely available software tool, Pathscape.

Installation Instructions

The VIA8 switch is DIN-mountable and intended for use in NEMA enclosures, or to be mounted in a standard 19” equipment rack, using the Pathway 1103 Rack Panel Adapter Kit.

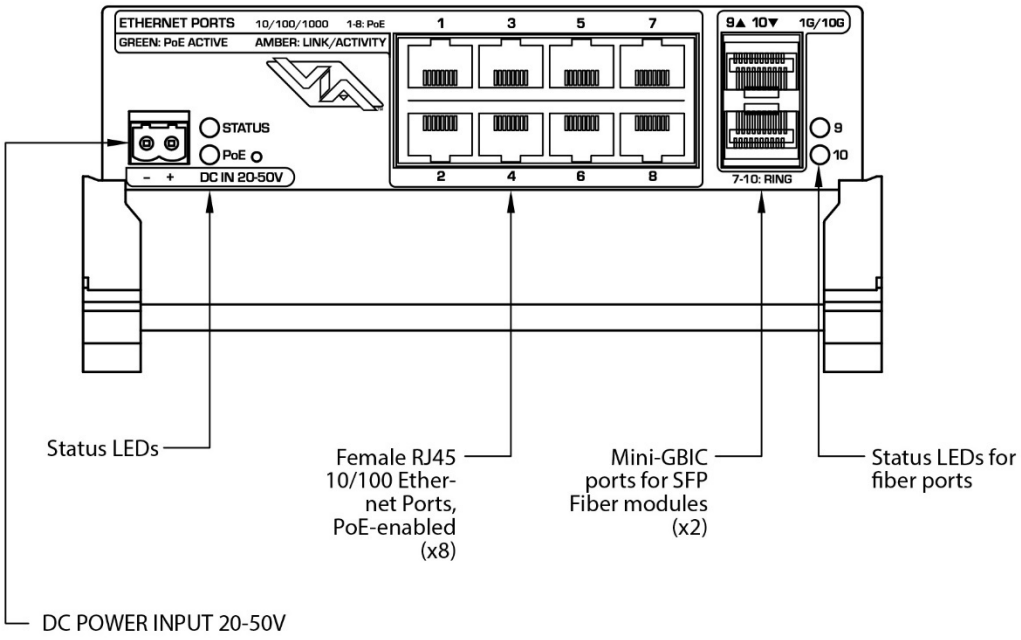
All VIA switches are intended for installation in a dry, indoor location. Operating conditions are 14°F – 118°F (-10°C - 48°C); 5-95% relative humidity, non-condensing.

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

Warning: Except for the terminal block DC power input, all ports on the VIA8 are intended for low voltage and/or data lines only. Attaching anything other than low voltage sources to the data ports may result in severe equipment damage, and personal injury or death.

Panel Layouts

Front Panel – model 6708



The user must provide an SFP (small-form pluggable) or SFP+ fiber adaptor to allow connection of the mini-GBIC ports to fiber optic networks. Use Pathway part number 6798 or 6799, or see Appendix 1 for recommendations on SFP adaptor selection.

The DC IN jack must be connected to an external power supplying at minimum 20 VDC to power the switch. If you are intending to use the VIA8 as a PoE source, the external power supply must provide 48-50 VDC with enough watts to satisfy the draw of connected equipment.

Class 3 PoE (15.4 W) is available on the 8 Ethernet ports. If you intend on using Class 3 devices on all 8 ports, the external supply must be 130 Watts or greater.

If you are using lower-power devices such as Pathport Gateways and Vignette or NSB stations, you may use a smaller supply. For a typical configuration with mostly Class 2 or lower devices, a 100W 48VDC supply (P/N 1001-100-48-DIN) will be sufficient. Always ensure your supply has enough power to supply your connected devices and set the External Power Supply wattage for the VIA8 in Pathscape.

Configuration

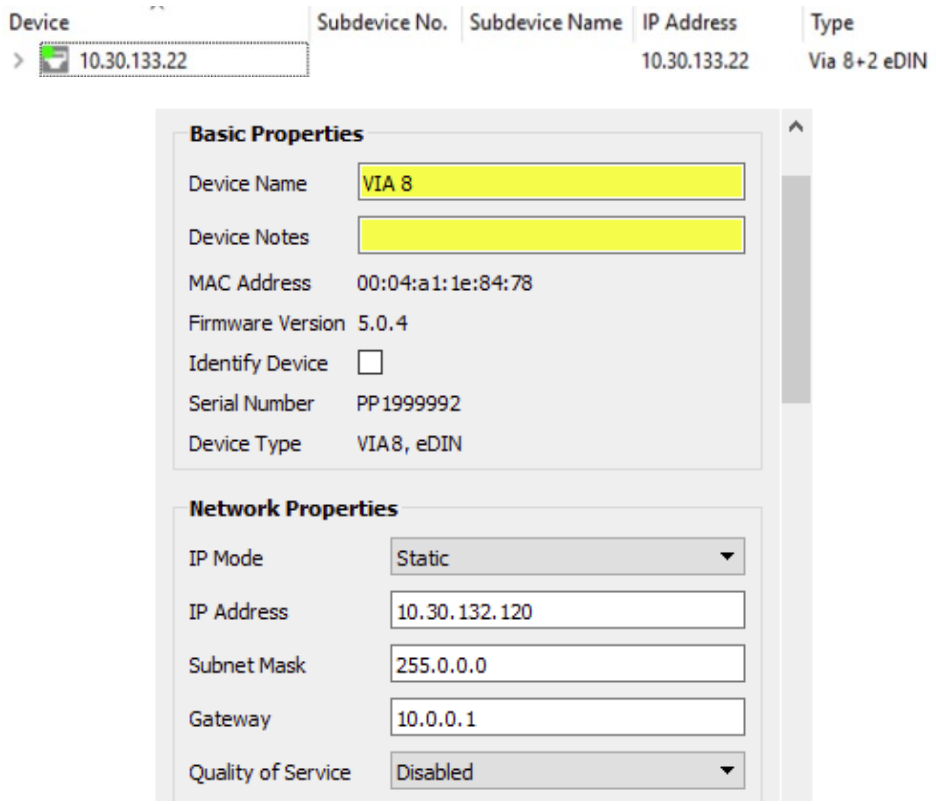
All configuration of the VIA8 must be done through the free software tool, Pathscape. To download Pathscape, go to the Pathway website at http://www.pathwayconnect.com/index.php/products/software/176-pathscape and click the download link.

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

Network Setup

From the factory, the VIA8'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 device's IP address to the same subnet and IP range as the computer and other devices on the lighting network.

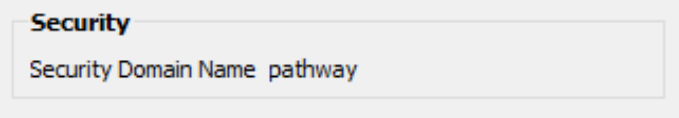
Additionally, the VIA8's name in the device list will be shown as its IP address. Give it a useful name before continuing.



Device Properties

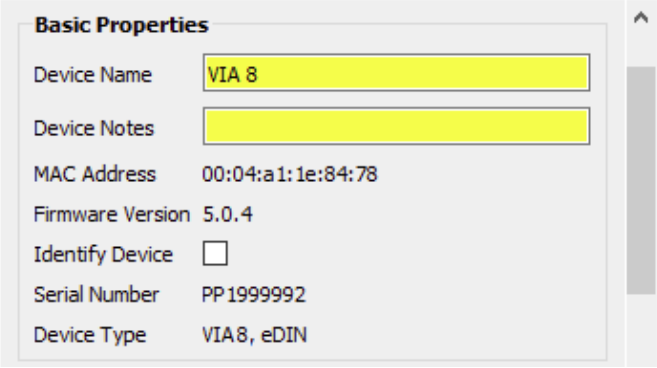
The following fields are shown in the device properties panel. Some are editable, while others are read-only.

Security



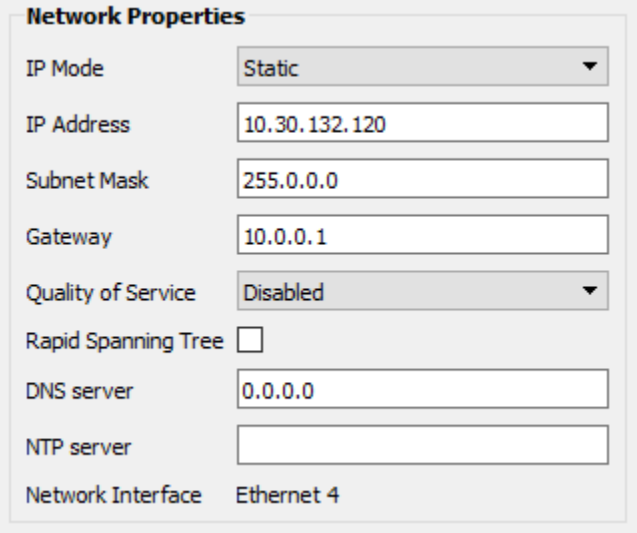
Property	Description
Security Domain	Name of the security domain the device is currently assigned to.

Basic Properties



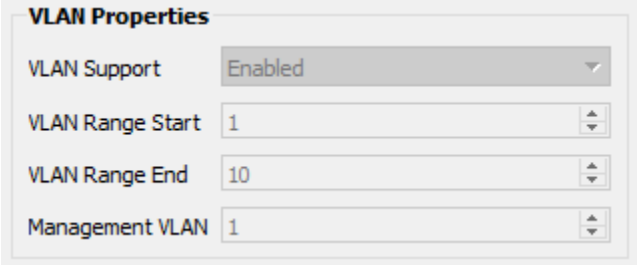
Property	Description
Device Name	Name of the device. User-defined.
Device Notes	Additional notes. User-defined.
MAC Address	Factory-assigned media access control address. Read-only.
Firmware Version	Current operating firmware version. Firmware may be updated using the **Firmware Update** button. Read-only.
Identify Device	This checkbox will show if the device is in Identify mode. You can additionally turn Identify mode on or off using this checkbox by clicking the box and then sending the transaction.
Serial Number	Factory-assigned, Pathway serial number.
Device Type	Factory-assigned, Pathway model number

Network Properties



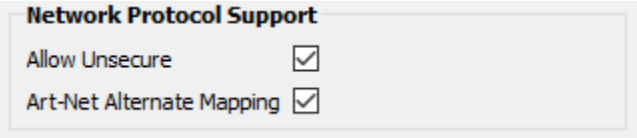
Property	Description
IP Mode	Determines how IP settings will be obtained.
IP Address	Switch IP address.
IP Subnet Mask	Switch subnet mask.
IP Default Gateway	Switch default gateway.
Quality of Service	QoS Settings for determining the relative priority of different data packets.
Rapid Spanning Tree	Turns on or off Rapid Spanning Tree.
DNS Server	Set the device DNS Server here, if applicable.
NTP Server	Set the device Network Time Protocol server here, if applicable.
Network Interface	Shows the Network Interface (NIC) your PC is using to communicate to the device.

VLAN Properties



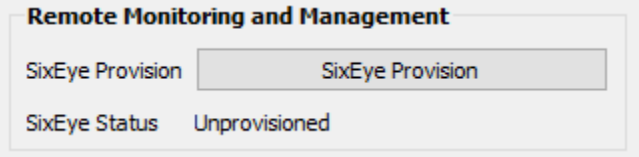
Property	Description
VLAN Support	Shows whether VLANs are Enabled or Disabled. To enable/disable VLANs, use **VLAN Global Configuration** under VLAN Config Tab..
VLAN Range Start	Set the start ID for range of VLAN IDs available to use.
VLAN Range End	Set the end ID for range of VLAN IDs available to use.
Management VLAN	Set the VLAN ID used by Management processor.

Network Protocol Support



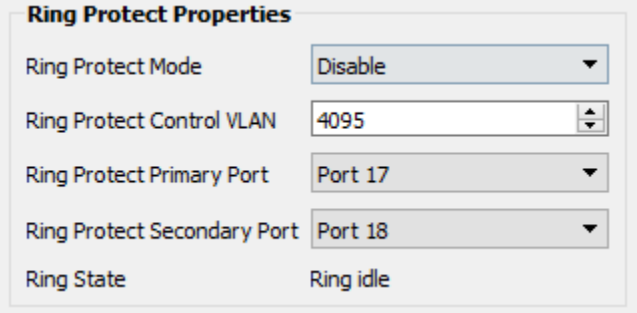
Property	Description
Allow Unsecure	Enable or disable unsecure network protocols.
Art-Net Alternate Mapping	Enable or disable Art-Net Alternate Mapping for Art-Net Trap & Convert feature

Remote Monitoring and Management



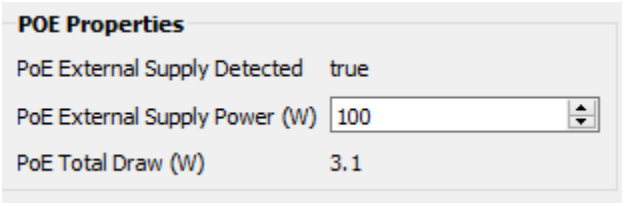
Property	Description
SixEye Provision	If using SixEye, paste the SixEye Provisioning code here.
SixEye Status	Shows status of device with SixEye

Ring Protect Properties



Property	Description
Ring Protect Mode	Set status of Ring Protect Mode.
Ring Protect Control VLAN	Specifies the VLAN ID# used to determine the integrity of the ring. May not be used for any other traffic. Valid ID# is any ID outside the range set in VLAN setup. Default is VLAN 4095.
Ring Protect Primary Port	Designates which port to use as the active uplink port to other switches. Valid range is port 7 through 10.
Ring Protect Secondary Port	Designates which port to use as the fall back link to other switches. Valid range is port 7 through 10.
Ring State	Current state of Ring.

PoE Properties



Property	Description
PoE External Supply Present	Indicates the presence of an external power supply capable of supplying PoE (48VDC). Green PoE LED on VIA8 panel will also indicate this (lit if present, off if not present).
PoE External Supply Power (W)	Enter the power rating of the external supply (in Watts). Default value is 0. The PoE LED on the VIA8 panel will flash green as a reminder if this value is left at 0.
PoE Total Draw (W)	Displays the current power draw from connected PoE devices

NOTE: The PoE External Supply Power must be entered or PoE will not function. All PoE values will be reported as 0.0W.

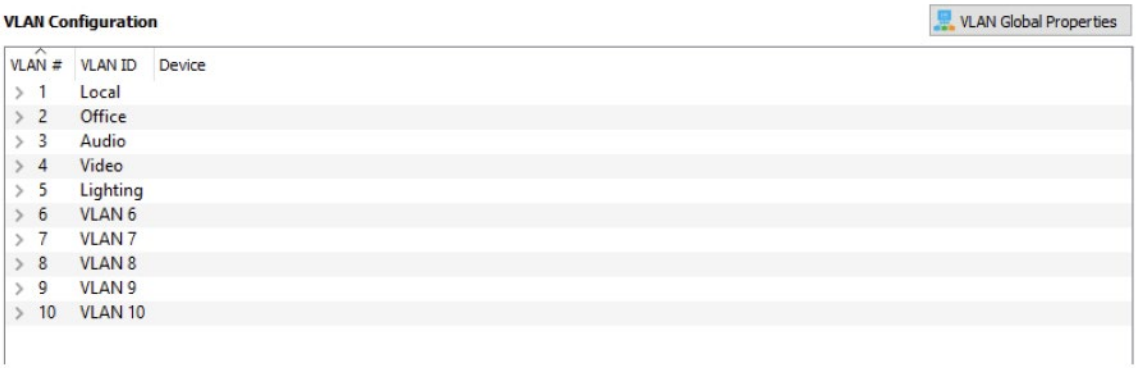
Advanced Properties

Property	Description
User ID	User-defined ID number. If desired, enter a numerical identification number. Default is 0.

Advanced Configuration

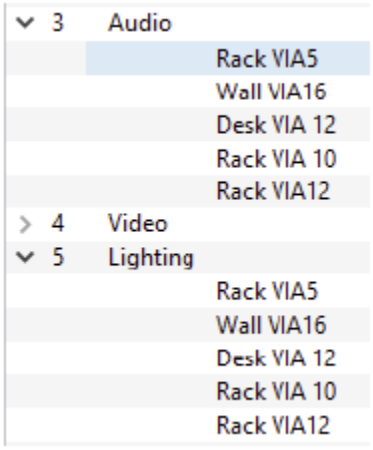
VLAN Configuration

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



In the VLAN Configuration window, there are three columns: VLAN #, VLAN ID and Device. By default, the VLAN ID will likely not have unique names (as in the screenshot above) but simply labeled “VLAN 1”, “VLAN 2”, etc.

Click on the arrow next to each VLAN to the 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.

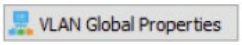
VLAN Properties such as IP Address, DHCP and IGMP settings are configured per VLAN per switch. For example, to configure VLAN 3 (Audio) on the “Rack VIA5” above, expand VLAN

3 and click on the Rack VIA5 device, then edit its properties in the Properties Pane. To edit VLAN 5 on the same switch, expand VLAN 5 and click on the Rack VIA5 to edit VLAN 5 on that device.

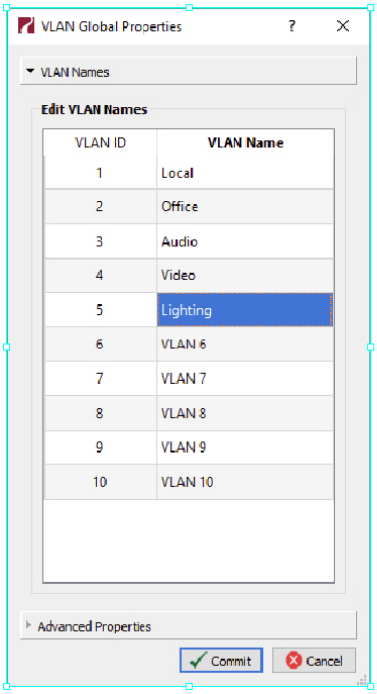
VLAN Global Properties

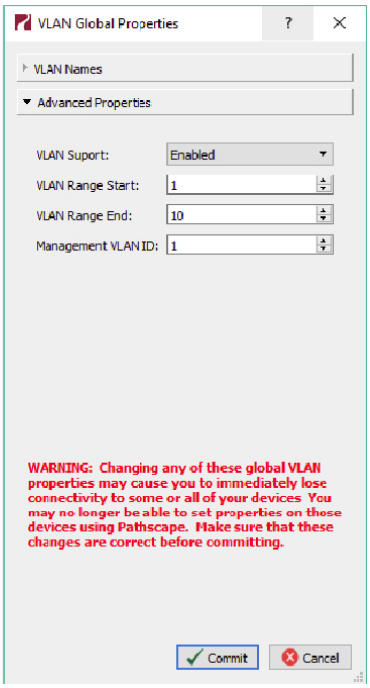
Plan your VLAN layout before attempting configuration. The creation of a map of the network, showing which devices and which ports to associate with a given VLAN, is strongly recommended prior to configuration.

EXTREMELY IMPORTANT NOTE: When configuring one or multiple VIA switches using Pathway's software-based configuration tools, be certain all switches are set to the same Management VLAN ID#. Be certain that the port connected to your computer is also on the same VLAN ID#, and is not on a tagged port. Failure to observe this rule will result in what appears to be a broken network, and embarrassment upon realizing the operator error.

In order to use VLANs, VLAN Support must be enabled in VLAN Global Properties, which is access by clicking the 

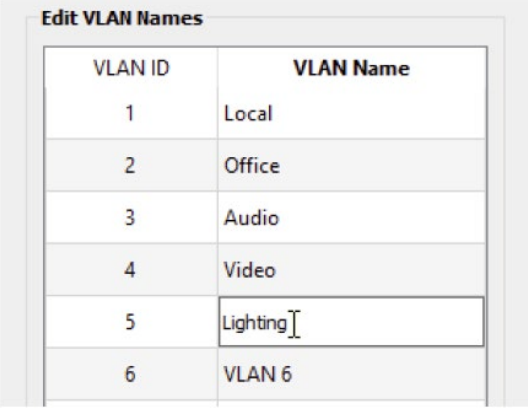
button in the top-right corner of the window.





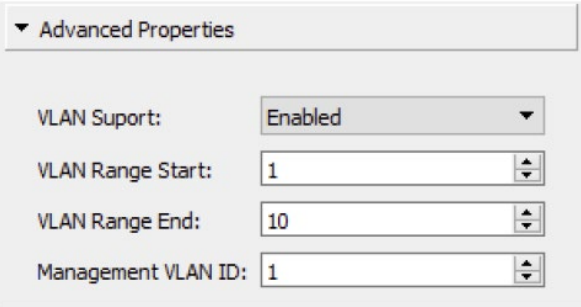
There are two sections to the VLAN Global Properties window: the VLAN Names panel, and the Advanced Properties panel.

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



You will then see several transactions 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.



Property	Description
VLAN Support	Enable or disable VLANs. Note this is a Global setting and will enable or disable VLANs across the entire network.
VLAN Range Start: <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 ID:<x>	Specifies the VLAN ID# used by the management processor. Default is 1. This value MUST be within the range specified by the range start and end set above, or you will not be able to configure the switch.

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

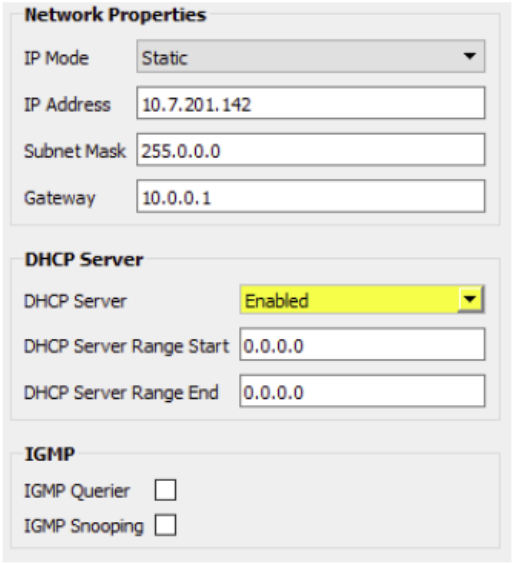
If the Management VLAN is accidentally set to a value outside the VLAN range, it may be necessary to use the Factory Reset button to restore communication with the management processor and allow further configuration.

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

The VLAN ID# is assigned to individual ports in the VLAN Patch tab.

VLAN Network Properties

VLANs must be enabled prior to configuring these properties.



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

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

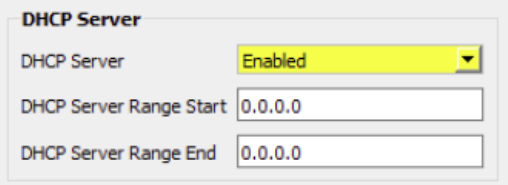
Default gateway addresses are not typically required on most entertainment installations, as these systems do not typically connect to the Internet. Any Internet access will be through a proxy or NAT gateway, in which case the default gateway IP should point to this device.

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.

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

VLAN DHCP Properties



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

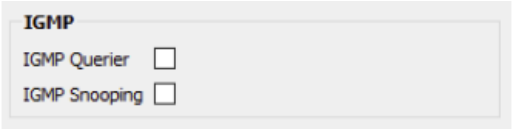
Important: Only one DHCP server may be active on any given VLAN at one time. Running multiple DHCP servers will cause network reliability problems.

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

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

Property	Description
DHCP Server Enable	**Disabled (default):** DHCP service is turned off. Use this setting for all static (manually-set) IP systems, and for all switches other than the VLAN's designated DHCP server host. **Enabled:** Enables DHCP server.
DHCP Server Range Start	Set the first available IP address. 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.
DHCP Server Range End	Set the last available IP address.

VLAN IGMP Properties



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

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

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

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

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

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

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

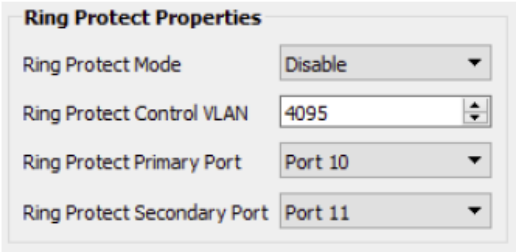
https://www.youtube.com/watch?v=0MVE22JCIt4

And the following video for a real-world example.

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

Ring Protect Configuration

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



Property	Description
Ring Protect Mode	Status of Ring Protect Mode. Disabled (default): Ring Protection feature is turned off Master: Only one switch may be set as the Master. Transit: All other switches must be set as Transit.
Ring Protect Control VLAN	Specifies the VLAN ID# used to determine the integrity of the ring. May not be used for any other traffic. Valid ID# is any ID outside the range set in VLAN setup. Default is VLAN 4095.
Ring Protect Primary Port	Designates which port to use as the active uplink port to other switches. Valid range is port 7 through 10.
Ring Protect Secondary Port	Designates which port to use as the fall back link to other switches. Valid range is port 7 through 10.

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

During the setup and configuration of the Ring Protection feature, communication between devices may be erratic or broken. We strongly recommend that all switches be configured 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.

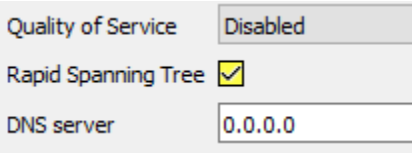
Prior to setup, determine which switch will be the master. Generally, the least busy switch in a position with the most stable power (i.e., not on a roving platform) is the best choice. All other switches must be configured as transit switches.

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

passed through the ports. Tagged ports must be connected to other tagged ports on other switches. Do not connect gateways or computers to tagged ports.

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

Rapid Spanning Tree



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

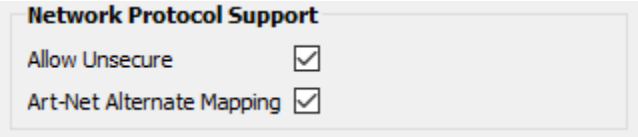
The Rapid Spanning Tree algorithm detects and prevents network loops. Networks with loops could have very poor performance.

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

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

For more information, please refer to the Appendix.

Art-Net Alternate Mapping



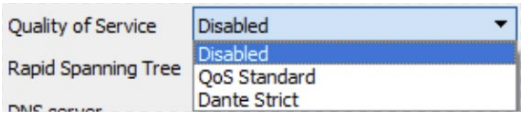
This feature is used in conjunction with the “Art-Net Trap-and-Convert to sACN”, feature. It does not affect unicast Art-Net packets.

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

However, most other common protocols, including sACN, do not have a universe 'zero'. The issue is compounded because some 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.

Quality of Service (QoS)



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

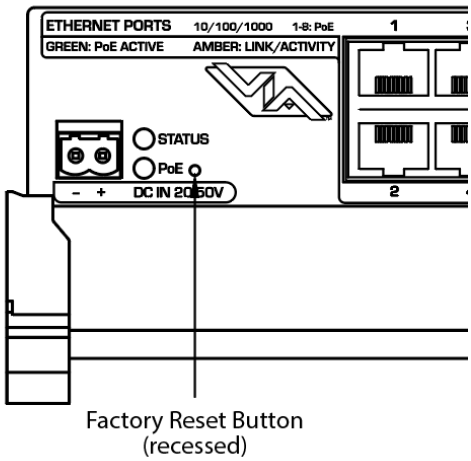
Property	Description
Quality of Service	**Disabled (default):** Disables QoS-based routing. All traffic is treated equally. **Standard:** Traffic priority is observed using a weighted algorithm to ensure timely delivery of high priority traffic and eventual delivery of lower priority packets. **Dante 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.

For more information, please refer to the Appendix.

Factory Default

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

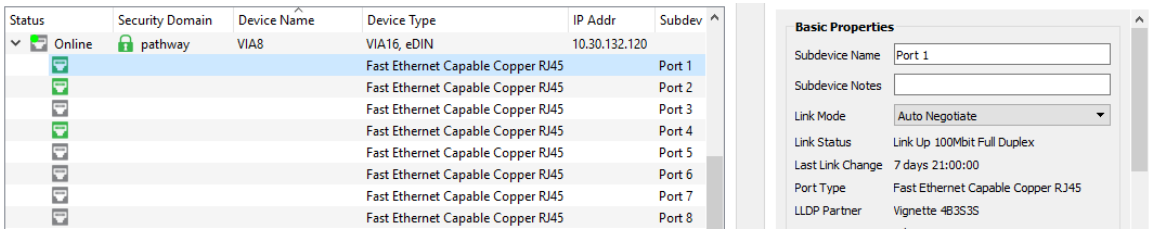
While powered, insert the tip of a pen or paperclip into the small hole in the front panel next to the PoE LED and press and hold the reset button for 5 seconds.



The switch will then reboot with the default configuration from the factory.

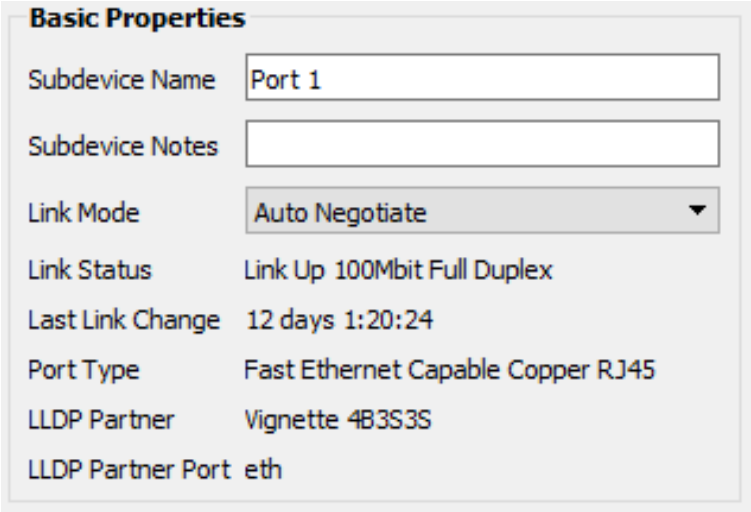
Port Properties and Configuration

Port Status and properties may be reviewed by expanding the device in the device tree, and clicking on a subdevice, or port. The properties for that port will then be shown in the properties panel.



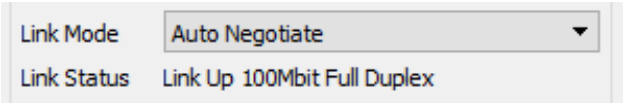
The following fields are shown in the subdevice/port properties panel. Some are editable, while others are read-only.

Basic Properties



Property	Description
Subdevice Name	Name of the port. Default is the port number. User-defined.
Subdevice Notes	Additional notes. User-defined.
Link Mode	**Disable:** Disables the port. **Auto Negotiate (default, recommended):** Allows the switch and the connected device to determine the fastest mutually supported connection speed. Read-only. 10Mbit Half Duplex 10Mbit Full Duplex 100Mbit Half Duplex 100Mbit Full Duplex 1Gbit Full Duplex (Fiber Ports Only) 10Gbit Full Duplex (Fiber Ports Only)
Link Status	Shows the status of the link (up or down) and the link 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).
Port Type	Shows the type of port currently selected (Copper RJ45 or Gigabit Capable Fiber). Read-only.
LLDP Partner	If the connected device supports Link Layer Discovery Protocol (LLDP), such as Pathway Pathport gateways and VIA switches, the connected device's name will appear here. Read-only.
LLDP 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 does not support LLDP, this will simply show "Eth", denoting an Ethernet device is connected.

Link Mode



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

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

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

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

For fiber ports, the Link Mode has only two options: Enable or Disable the port.

LLDP Partner

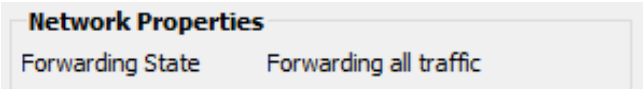
Link Layer Discovery Protocol (LLDP) is an industry-standard method for device announcement and reporting described in the IEEE 802.1AB standard. Any Ethernet-aware device may announce itself using LLDP, not just switches.

For Pathway devices supporting LLDP, the name shown in the LLDP Partner field will be the device's name, as configured in Pathscape. Other LLDP-enabled devices may return different information. This property is only shown when a device is connected to the port in question.

Network Properties

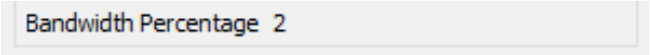
Property	Description
Forwarding State	Traffic forwarding state of the port: Forwarding all traffic or Blocked by RSTP detecting a loop. RSTP must be active. Read-only.
Bandwidth Percentage	Shows the bandwidth used on the selected port. Bandwidth is relative to the port speed as negotiated with the link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

Forwarding State



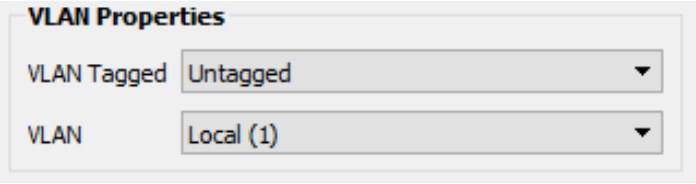
Shows the forwarding state for the selected Port. Typically, this will show “Forwarding all traffic”. If RSTP is enabled and a network loop is detected, RSTP will block the port that is creating the loop. In this case, the Forwarding State will be shown as “Blocked by RSTP”.

Bandwidth Percentage



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

VLAN Properties



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

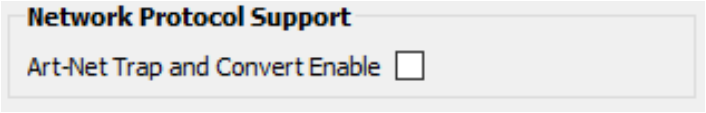
Once VLANs are enabled and the VLAN range is set, by default a port is set as Untagged (Normal) with a VLAN ID# of 1, or the lowest ID# of the VLAN range.

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 should only be connected to other tagged ports, typically on other switches. Do not connect Pathport gateways or other devices like computers unless you have specifically configured your Ethernet port to receive tagged data (advanced network setup only).

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

Network Protocol Support



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

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. 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.

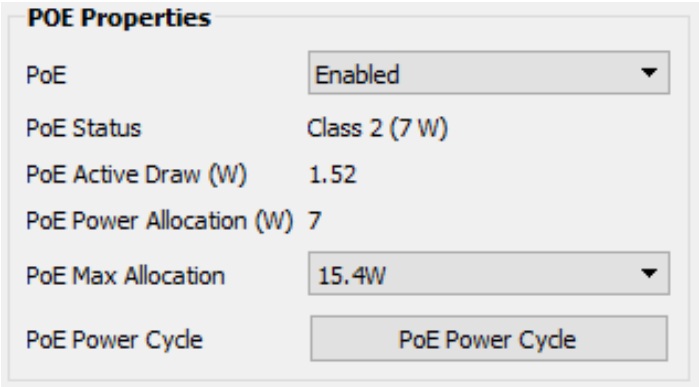
The Art-Net packet will be converted to the analogous sACN universe. Due to how Art-Net universes are numbered, there is the possibility of an off-by-one error. Change the “Art-Net Alternate Mapping” option should the universe mapping seem incorrect.

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

Currently, there is no method of converting the sACN back to Art-Net. This feature assumes the DMX gateways can receive sACN instead of Art-Net.

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

PoE Properties



Property	Description
PoE	Enabled by default, this option allows the user to completely disable PoE on a given port. Any PoE allocation set with the following parameter will be ignored. Ports 1-8 only.
PoE Status	The PoE class as reported by device. Read-only. Not Detected: not a PoE device Class 0: No class reported, 15.4W draw assumed Class 1: Uses up to 4W Class 2: Uses up to 7W Class 3: Uses up to 15.4W
PoE Active Draw (W)	Consumption as reported by the PoE controller, in watts.
PoE Power Allocation (W)	Reports the maximum draw, in watts, allowed by the PoE class, or the limit set by the user, whichever is less.
PoE Max Allocation	Sets the PoE allocation for the port. Default is 15.4W, regardless of the size of the power supply. Allocation options range from 0.9W to 15.4W, in 900mW increments.
PoE Power Cycle	Pressing this button will disable and then re-enable PoE on the given port, in order to power cycle the end device.

PoE Max Allocation

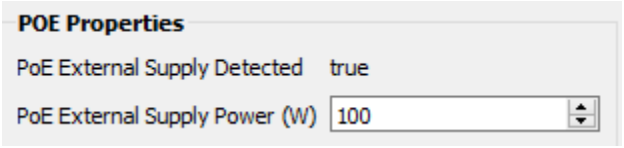
Allows you to set an upper limit to the power available to a connected device, such as a Pathport gateway or Vignette wall station. Use Max Allocation to ensure critical devices will have power. Also use Max Allocation to compensate for Class 0 device power allocation. Many older PoE devices cannot report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

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

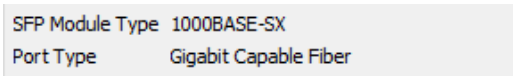
Troubleshooting tip: If the green PoE LED on the front panel is blinking, the maximum allocation is too low for the connected device, the PoE power supply has not been set up (see note below) or all available power is already allocated.

IMPORTANT NOTE: The VIA8 ships with hardware support for IEEE 802.3af Power-over-Ethernet standard (PoE). To make use of this hardware, an external 48VDC auxiliary power supply, such as Pathway P/N 1001-100-48-DIN, must be connected to the VIA12.

Once the power supply is connected, the VIA must be configured with the size – in watts – of the PoE supply.



SFP Module (Fiber Ports Only)



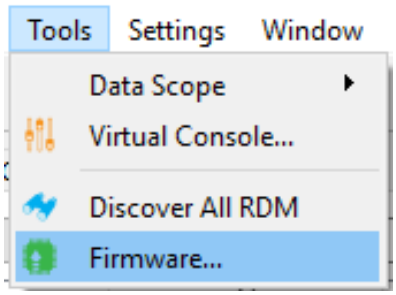
Property	Description
Not Detected	No module inserted
Not Support	Module is not compatible/supported
1000Base-SX	Module is recognized as type noted
1000Base-LX	Module is recognized as type noted
10GBase-SR	Module is recognized as type noted
10GBase-SW	Module is recognized as type noted

Firmware Upgrades

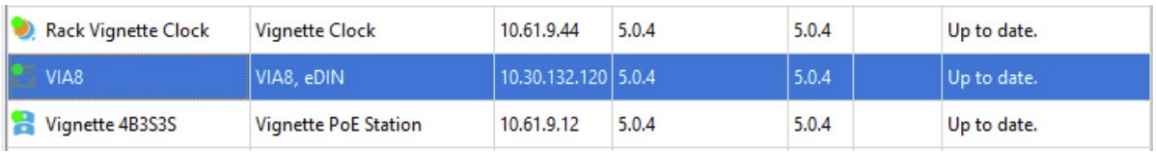
Firmware upgrades may only be done using Pathscape.

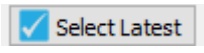
The most recently released firmware is bundled with the most recent version of Pathscape. To ensure you have the most up-to-date firmware available for upgrading, ensure you have downloaded the most recent version of Pathscape from the Pathway site, http://www.pathwayconnect.com.

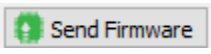
To upgrade a VIA switch, ensure the device's IP address is configured correctly and is on the same subnet and IP range as the computer. Open Pathscape, click the **Tools** menu, then select **Firmware…**



This will bring up the Firmware Update window.



Select the VIA8 and click the 

button at the bottom of the window. The latest firmware version will be shown in the table next to "Current". Click the 

button and wait for the progress bar to finish. After the device reboots, the firmware is updated.

.

Appendix 1: SFP Fiber Adapter Selection

The VIA8 allows the end user to provide a fiber adaptor. The adaptors are typically referred to as an SFP (Small Form Pluggable transceiver) or mini-GBIC (gigabit interface converter).

Pathway part number 6799 is an SFP 850nm Ethernet Optical Transceiver that is compatible with VIA12, VIA16 and VIA8, capable of 1Gbps. Part number 6798 is an SFP+ 850nm Ethernet Optical Transceiver capable of 10Gbps, compatible with the VIA8 and VIA12 model 675X. 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-SW)
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 corresponding Link/Activity LED will light up green. If an incompatible module is detected, the 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 VIA8 will only work with 1000BASE-SX, 1000BASE-LX (1Gbps) and 10GBase-SR and 10GBase-SW (10Gbps) fiber modules.

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 the network does not get flooded with redundant data.

Definitions

VLAN naming practices can be confusing. 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 with Pathscape. Refer to software documentation for complete configuration instructions.

When configuring 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.

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

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

It is strongly recommended that the ports used to connect separate VIA switches should be set to matching configurations.

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 tab to configure the desired IP settings for each VLAN.

VLAN ID#	1	2	3	4	5	6	7	8
Label								
IP Address								
Subnet Mask								
Default Gateway								
IGMP Snooping								
IGMP Querier								
DHCP Server								
Art-Net Alternate Mapping								
QoS Level								

Switch Label:										
Port	1	2	3	4	5	6	7	8	9	10
Connected Device										
Normal/Uplink										
VLAN ID#										
ArtNet to sACN										
PoE Max										
Link Mode										
SFP Type										

Appendix 3: Ring Protection

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

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

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

Requirements and Limitations

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

Only ports 15 thru 18 may be used with this feature.

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

Definitions

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

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

Note: Ring Protection wiring topology is not structured. No care need be taken when connecting primary and secondary ports together – any arrangement is acceptable.

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 15 through 18 are available to be used as the primary port. If using copper, typically port 15 will be primary and 16 will be secondary. If using fiber, port 17 is primary and port 18 is secondary.

Secondary port is an UPLINK port 'ignored' (logically blocked) by the Master switch to break the ring topology. All transit switches also must have one port configured as the secondary port. The secondary port is actively used on transit switches. Only ports 15 through 18 are available to be used as the secondary port.

Appendix 4: Rapid Spanning Tree Protocol

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

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 Queues 3 and 4 are handled by strict priority, while the two lower queues are handled by the weighted algorithm.