MaxiiNet™ Vi22108U/Vi22116U
Operation and Installation Manual

8/16 Port Industrial 802.3bt Managed Midspan

Firmware Version (Version 1.1)
Revision Date (1-2025)

About This Manual

Copyright

Purpose

This guide gives specific information on how to operate and use the management functions of the midspan.

Audience

The guide is intended for use by network administrators who are responsible for operating and maintaining network equipment. Consequently, it assumes a basic working knowledge of general midspan functions, the Internet Protocol (IP), PoE and Syslog.

Conventions

The following conventions are used throughout this guide to show information:

NOTE: Emphasizes important information or calls your attention to related features or instructions.

WARNING: Alerts you to a potential hazard that could cause personal injury.

CAUTION: Alerts you to a potential hazard that could cause loss of data or damage the system or equipment.

Warranty

See the Customer Support/Warranty booklet included with the product. A copy of the specific warranty terms applicable to Vigitron's products and replacement parts can be obtained from Vigitron's Sales and Service Office or authorized dealer.

Disclaimer

Vigitron does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. Vigitron disclaims liability for any inaccuracies or omissions that may have occurred. Information in this user's manual is subject to change without notice and does not represent a commitment on the part of Vigitron. Vigitron assumes no responsibility for any inaccuracies that may be contained in this user's manual. Vigitron makes no commitment to update or keep current the information in this user's manual and reserves the right to make improvements to this user's manual and/or to the products described in this user's manual, at any time without notice.

FCC

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

FCC Caution

To assure continued compliance (example-use only shielded interface cables when connection to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Compliances and Safety Statements

FCC - Class

This equipment has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interferences in which case the user will be required to correct the interferences at his own expense.

CE Mark Declaration of Conformance for EMI and Safety (EEC)

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

You may use unshielded twisted-pair (UTP) for RJ-45 connections - Category 5 or better for 10 Mbps connections, Category 5 or better for 100 Mbps connections, and Category 5, 5e, or 6 for 1000/2500 Mbps connections.

EMC - Compliance

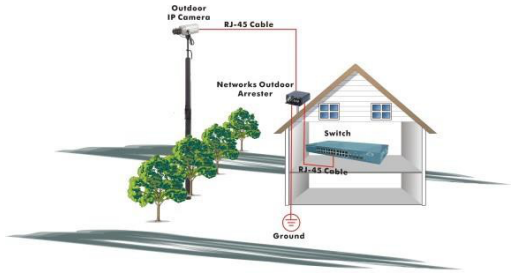
.
This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN61000-3 and the Generic European Immunity Standard EN55024.

EN55022(2006) +A1:2007/CISPR 22:2006+A1:2006	**Class A** **4K V CD, 8KV, AD**
IEC61000-4-2 (2001)	3V/m
IEC61000-4-3(2002)	1KV – (power line), 0.5KV – (signal line)
IEC61000-4-4(2004)	Line to Line: 1KV, Line to Earth: 2KV
IEC61000-4-5 (2001)	130dBuV(3V) Level 2
IEC61000-4-6 (2003)	1A/m
IEC61000-4-8 (2001)	Voltage dips: >95%, 0.5period, 30%, 25periods
IEC61000-4-11(2001)	Voltage interruptions: >95%, 250periods

CAUTION: Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge. To protect your device, always:

Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.

Pick up the device by holding it on the left and right edges only.
If you need to use an outdoor device to connect to this device with a cable, then you need to add an arrester on the cable between the outdoor device and this device.



Add an arrester between the outdoor device and this midspan.

NOTE: The midspan is an indoor device. If it will be used in an outdoor environment or connected with an outdoor device, then a lightning arrester must be used to protect the midspan.

WARNING: Self-demolition on this product is strictly prohibited.
Damages caused by self-demolition will be charged for repair fees.

Do not place products outdoor or in a sandstorm.
Before installation, please make sure input power supply and product.
Specifications are compatible to each other.
To reduce the risk of electric shock. Disconnect all AC or DC power cords 7and RPS cables to completely remove power from the unit.
Before importing/exporting configuration, please make sure the
firmware version is always the same. After the firmware upgrade, the midspan will remove the configuration automatically to latest firmware version.

Introduction

Overview

The Vi22108U/Vi22116U PoE midspan, next generation network solutions, is an affordable managed midspan that provides a reliable infrastructure for your business network allowing for the transition to newer type of high powered 802.3bt PoE. These midspans deliver more intelligent features you need to improve the availability of your critical business applications, protect your sensitive information, and optimize your PoE to deliver information and applications more effectively. Easy to set up and use, it provides the ideal combination of affordability and capabilities for entry level networking, including small business or enterprise applications. It also helps you create a more efficient and better-connected workforce.

The Vi22108U/Vi22116U is an easy to implement managed Ethernet midspan that provides ideal flexibility to design suitable network infrastructure for business requirements. However, unlike other entry-level midspan solutions that provide advanced managed network PoE capabilities only in the most expensive models, all Vigitron's series midspan support the advanced security management capabilities and features to support data, voice, security, and wireless technologies. These midspans are easy to deploy and configure. They provide stable and quality performance network services for your business needs.

Important Note: On PoE Settings

Port PoE power is constantly monitored. Please take care not to exceed the total Poe budget of 730W. To protect the midspan and connected devices if a power surge occurs ports will be disabled starting with the highest number port. IF the unit is connected to the network and the syslog is active a message will be sent out.

When programming port PoE connect the most critical devices starting with Port 1
When selecting port connection start with Port 1 for your most critical devices

To prevent this condition please take care not to exceed the total PoE budget.
If this occurs the port will be disable. To re-enable the port log into the midspan and go to PoE settings re-enable and reprogram the port

To program PoE settings
You must enable the port, or you will not be able program any other ports settings

If a port is disabled for any reason either by user interact or by port monitoring, you must access the GUI and re-activate the port and programming

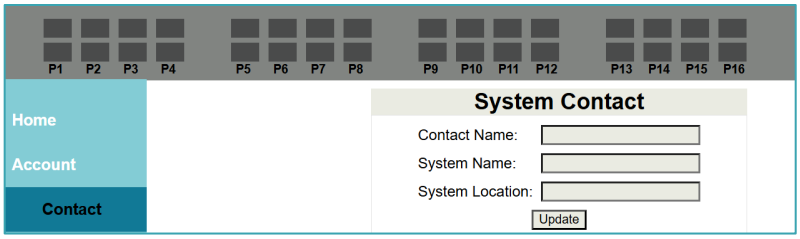
If auto checking is enabled on a port, it will function to monitor the port. In the event a connection and PoE is reinstated the port, and its settings will be retained and previous operation prior to auto checking will be maintained.

If auto checking fails to establish a valid connection the port will be disabled, and the operator will be required to use the GUI to re-enable and re-program the port

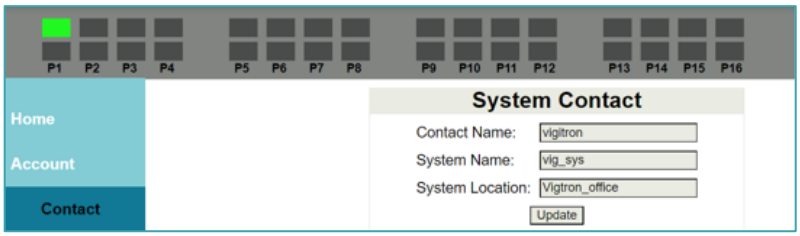
Refreshing the GUI

For screens where you can enter data suggest as system contact and IP address information

1. Enter the information
2. Select update
3. Confirm that new information is updated



Fill in the contact, system names and location to identify the midspan



To confirm the update, Refresh the screen button and it will display the latest information

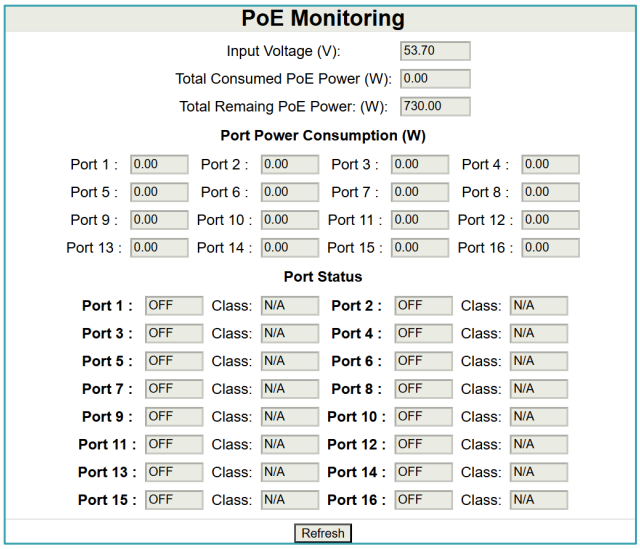


Table of Contents

The Vi22108U/Vi22116U is an 8 or 16 -port network midspan. 8/16 UTP ports provide network connections with PoE and 8 ports for data connections to devices such as switches. 802.3af/af/bt are supported along with major nonstandard PoE versions providing the perfect solution for adding newer cameras to existing switches.

The midspan contains 8/16 100/1000/25000 BASE-T RJ-45 ports. All RJ-45 ports support passing data from sources complying to IEEE transmission standards.

The midspan ports are designed to pass through data on all wire speeds without affecting speed or structure.

The midspan can also be managed over the network with a web browser which also provides the ability to monitor midspan status and errors via System Log (syslog) using port 514.

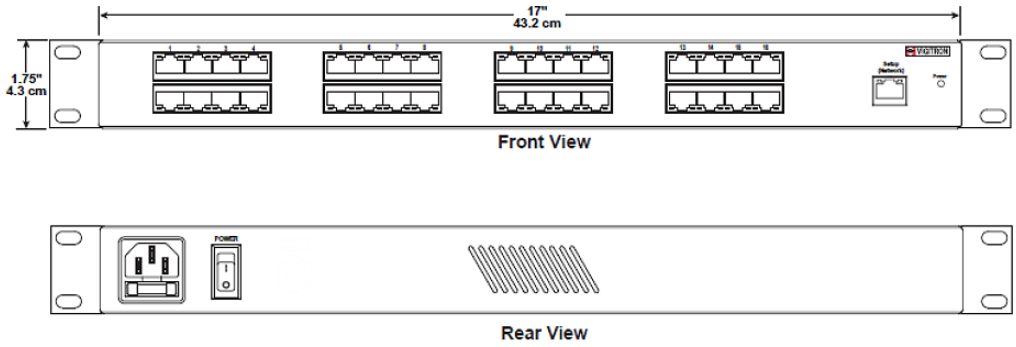
Description of Hardware

The Vi22108U/Vi22116U is an 8 or 16 -port network midspan. 8/16 UTP ports provide network connections with PoE and 8 ports for data connections to devices such as switches. 802.3af/af/bt are supported along with major nonstandard PoE versions providing the perfect solution for adding newer cameras to existing switches.

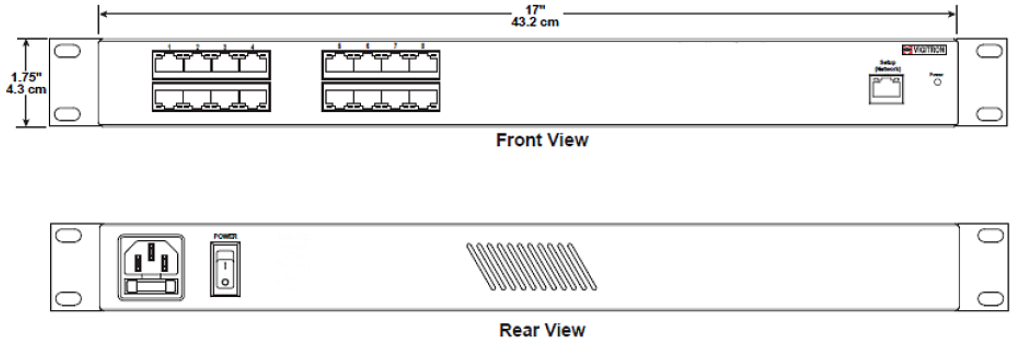
The midspan contains 8/16 100/1000/2500 BASE-T RJ-45 ports. All RJ-45 ports support passing data from sources complying to IEEE transmission standards.

This midspan ports are designed to pass through data on all wire speeds without affecting speed or structure.

The midspan can also be managed over the network with a web browser which also provides the ability to monitor midspan status and errors via System Log (syslog) using port 514. **Front Panel/Rear Panel Vi22116U**



Front Panel/Rear Panel Vi22108U



The following table details the functions and descriptions of various LED indicators:

Model Name	Vi22108U/Vi22116U
Ports	8/16*1G POE Port+ Data ports 8/16*1G Data only ports 1*10/100Mbps Programming/network connection port
Description of Function Slots	Port 1-8/16: 8/16 X RJ45 10/100/1000/2500 Mbps (PoE + Data) Port 1-8/16: 8/16 X RJ45 10/100/1000/2500 Mbps (Data Only) Network Port 1 X RJ45 10/1000/2500 Mbps (uplink)
PoE Ports	1-8/16 port, each port supports af/at/bt, max 90W output
LED Indicator	Port Port #1-8/16 PoE + Data (insert operation) Port # 1-8/16 Data Only
	Power: Green PoE + Data Port Green Data only port-No LED

LED	**State**	**Color**	**Comment**
Power	on	Green	Normally on steady. Note: Firmware can override with 1Hz bink in certain situations
	Off		LED off
Network Port	Link-On	Green	On
	Link- no link		Off
	Traffic - present	Yellow	Flashes with traffic
	Traffic- no Traffic		Off

LED Operation for Auto checking

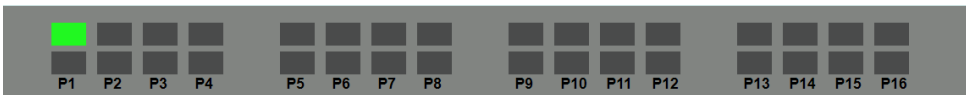
When Auto checking disables a port, the corresponding LED on the GUI panel will turn red.

To re-enable the port, log into the Midspan, go to PoE Settings, under "Power Control, click "Enable" on the appropriate port, and then click "Update". The port will now be operational again.

Other Front Panel LED responses:

During Firmware and User Configuration upload
Power LED will flash and will to the steady on state when complete

Individual Port PoE Delivery:
When PoE is being delivered the individual RJ45 port will turn Green in the steady on state
If for any reason PoE cannot be delivered the LED will turn off
Note: If you see the individual RJ45 port turn on and then turn off – it is an indication the amount of PoE programmed does not meet the requirement of the connected device and the setting needs to be increased



GUI LED Responses

Condition-Individual Ports	LED Color	Status	Information
No PoE	Gray/Blank	Steady	**No POE is delivering**
PoE Delivering	Green	Steady	**Delivering PoE**
Auto checking in Process	Green / Gray (same as the POE status)	Steady	LED status as Green / Gray (as the PoE status is) until port issue is confirmed the port and shut down, then we will indicate the port LED to be Red
Auto checking Failed port was on but failed	Red	Steady	When Auto Checking disabled the port, LED will be in Red Color

Front Panel LED

Front panel LEDs	LED Condition	Status
Power LED	On	Power Normal
Power LED	Off	No power to unit
Power LED	Flashing	Firmware/Configuration update in progress or PoE disabled on one or more ports
Port PoE LEDs	On	Port is delivering power
Port PoE LEDs	Off	No PoE output

The Vi22108 has a display panel for system and port indications that simplify installation and network troubleshooting. The LEDs are located of the front panel for easy viewing. Details are shown below and described in the following tables.

The green power LED light is used to note normal and trouble states

1) Auto-checking has disabled PoE to one or more ports. The LED will continue to blink until the user uses the GUI to enable the port(s).
2) As the factory default settings are being loaded. When complete, the LED will go back to its ON steady state.
3) When the Vi22108U/Vi22116U is receiving a firmware upgrade.

Network Planning

Introduction to MPoE

A network midspan allows simultaneous provides multiple independent PoE + Data ports and separate network only port. Vigitron's MPoE™ address the most demanding PoE requirements as one of the most important devices for today's networking technology.

A midspan can easily handle data in any Ethernet, Fast Ethernet, or Gigabit Ethernet network to significantly increase PoE while using conventional cabling.

The midspan is suitable for the following applications:

- Network Switches that do not provide PoE.
- Network switches that do not provide required PoE volume.
- Network switches that do not provide newer types of PoE such as 802.3bt.
- Applications that require power both IEEE standard PoE and major nonstandard PoE.
-

NOTE: MPoE™ programming provides the a "Forced Power" mode while maintaining safety in case of wire shorts –Protection is valid to 5% of total port power assigned

---

What is Forced Power:

Under IEEE PoE standards the transmission of PoE from a source (called PSE: Power Source Equipment) to the connect device (called PD: Power Device) is required to confirm a valued connection and the amount of PoE power required. This helps to confirm the connection and PoE transmission safety.

In rare cases, this may not be possible and PoE will not transmit. A Forced Power Mode overrides these safety considerations and will transmit PoE regardless of the connection status. The drawback is in the event of a short power will continue to transmit causing potential damage to the connected devices. The Vi22108U/Vi22116U avoid this by

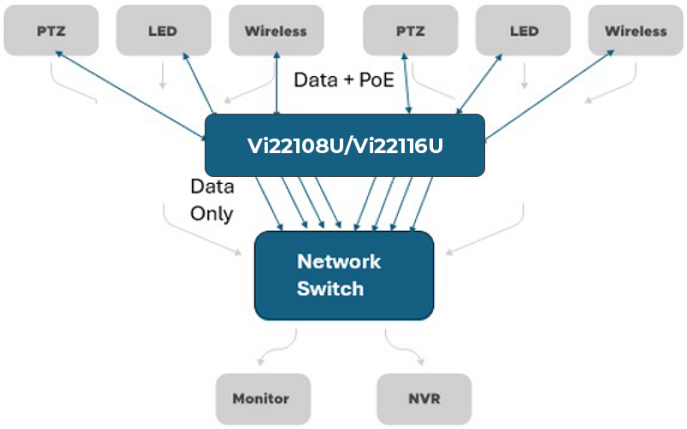
Vigitron's unique MPoE Forced Power mode provides the safety provided by the IEEE standards while allowing for PoE transmission.

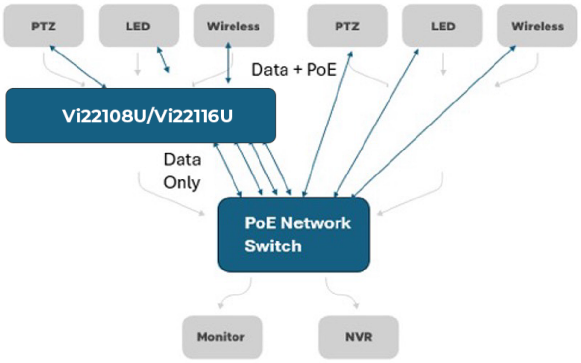
Application Examples

Network Connection between Remote Site and Central Site

This will be replaced with actual product images. (for both Vi22108U and Vi22116U)

Switch to Midspan Configuration





Installing the Midspan

Selecting a Site
The midspan can be mounted using mounts equipment or operated using the rack mount kit or on a flat surface. Be sure to follow the guidelines below when choosing a location.

The site should:
- Be at the center of all the devices that you want to link and near a power outlet.
- Be able to maintain its temperature within 0°C to 40C (32C°F to 104°F) and its humidity within 10% to 90%, non-condensing.
- Be accessible for installing, cabling, and maintaining the devices.
- Allow the status LEDs to be clearly visible.

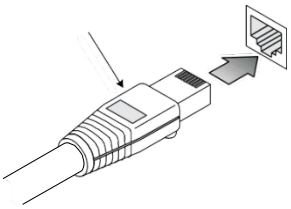
Make sure the twisted-pair Ethernet cable is always routed away from power lines, radios, transmitters, or any other electrical interference.
Make sure that Vi22108U/Vi22116U is connected to a separate grounded power supply that provides 100 to 240 VAC, 50 to 60 Hz.
Make sure the power supply you are using provides the required power for your connected devices.

Ethernet Cabling
To ensure proper operation when installing the midspan into a network, make sure that the current cables are suitable for 100BASE-TX, 1000/2500BASE-T operation.
Check the following criteria against the current installation of your network:

Cable type: Unshielded twisted pair (UTP) or shielded twisted pair (STP) cable with RJ-45 connectors; Category 5 or Category 5e with a maximum length of 100 meters is recommended 100BASE-TX and greater wire speed , and Category 5e or 6 with a maximum length of 100 meters is recommended for 1000/2500BASE-T.
Protection from radio frequency interference emissions.
Electrical surge suppression.
Separation of electrical wires and data-based network wiring.
Safe connections with no damaged cables, connectors, or shields.

Connecting to the Network Port

Rj-45 Connections



The Ethernet port is used to:
Program the Midspan
Connect the Midspan to a network

The Midspan can be secured by first programming the Midspan and inserting it in a network without a network connection.
If you want to monitor the Midspan and receive status and error messages the Midspan must be connected to network.

Package Contents
After unpacking the midspan, please check the contents to make sure you have received all the components. Also, make sure you have all other necessary installation equipment before beginning the installation process.

- Vi22108U/Vi22116U GbE Managed Midspan
- Power cord

NOTE: Please notify your sales representative immediately if any of the aforementioned items are missing or damaged.

WARNING: The mini-GBICs are Class 1 laser devices. Avoid direct eye exposure to the beam coming from the transmit port.

Rack Rail Mounting
Step 1: Attach the mounting brackets to both sides of the chassis. Insert screws and tighten with a screwdriver to secure the brackets.

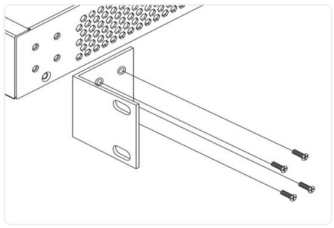
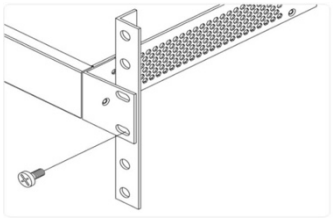


Figure 3: Attaching Brackets to the Switch
Step 2: Place the switch on a rack shelf in the rack. Push it in until the oval holes in the brackets align with the mounting holes in the rack posts.



Step 3: Attach the brackets to the posts. Insert screws and tighten them.
Figure 4: Attaching Brackets to the Rack Post

CAUTION:
While mounting the Midspan in the rack please allow for proper airflow

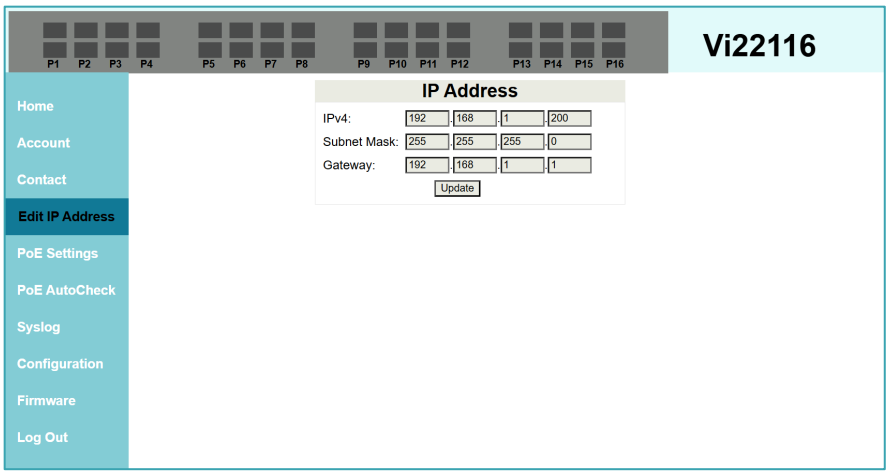
Note:
If this configuration is used without a network connection communication with the Midspan and the use of Syslog messaging is not possible.

The RJ-45 network port on the midspan's front panel is used to connect to the midspan to a network. This connection is also used for programming.

Once the midspan is programmed the midspan can be used to power connected devices with each data only port connected the individual network switch port.

Removing the network port connection isolates the Midspan from the network offering security from hacking but prevents further access to the Midspan

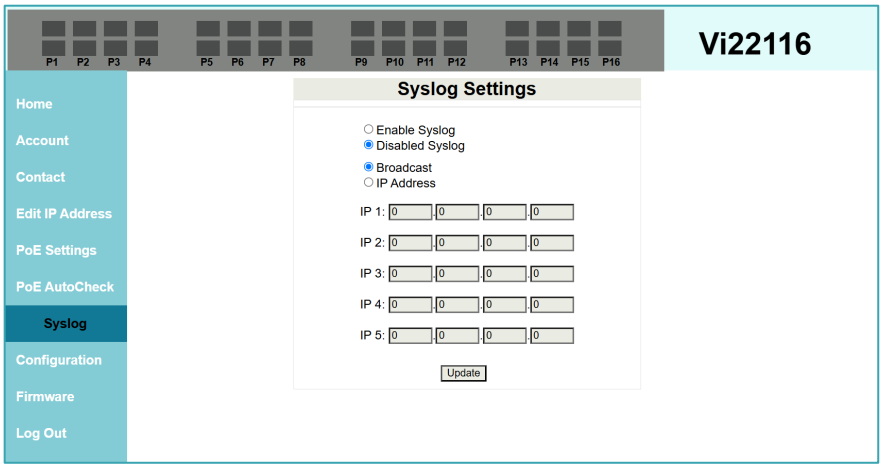
This requires a network connection.



The address to access the switch is the same address used to access the switch. However, this address and its network can be separate from the IP address used for the connected devices.

It can also be different than the address used for other network services such as cameras, and VMS servers. The operating network address used to transmit cameras to the server, access to the Midspan and the ability to receive syslog messages can all have different addresses.

The key is the clients used to receive each type must be on the same network.



Making Network Connections

Connecting Network Devices

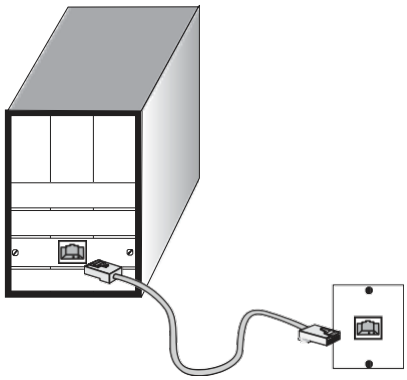
Each device requires an unshielded twisted-pair (UTP) cable with RJ-45 connectors at both ends. Use Category 5e, or 6 cables for 1000BASE-T connections, and Category 5 or better for 100BASE-TX and greater wire speed connections.

Cabling Guidelines- UTP Copper Cabling
The RJ-45 ports on the midspan support automatic MDI/MDI-X pin-out configuration, so you can use standard straight-through or cross twisted-pair cables to connect to any other network device in most cases this will be a network switch

See Appendix B for further information on cabling.

CAUTION: Do not plug a phone jack connector into an RJ-45 port. This will damage the midspan. Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Connecting to PCs, Servers, Hubs and Midspans
Step 1: Attach one end of a twisted-pair cable segment to the device's RJ-45 connector.



Making Twisted-Pair Connections
Step 2: If the device is a network card and the midspan is in the wiring closet, attach the other end of the cable segment to a modular wall outlet that is connected to the wiring closet. See the section "Network Wiring Connections." Otherwise, attach the other end to an available port on the midspan.

NOTE:
Make sure each twisted pair cable does not exceed 100 meters (328 ft) in length.

WARNING

Make certain transmission cables are not positioned next to high power or high signal transmission lines this can result in reduced or non-performance

Connectivity Rules

1000Base-T Cable Requirements
When adding hubs to your network, please note that because midspan break up the path for connected devices into separate collision domains, you should not include the midspan or connected cabling in your calculations for cascade length involving other devices.

The total cable distance from a receiving port and the connected device powered by the Midspan is 328 feet (100m). If longer distances are required, please contact Vigitron to use the appropriate extenders. Distances up to 2,000 feet (606m) are possible depending on the type of cable and PoE requirements of the connected device.

All Category 5 UTP cables that are used for 100BASE-TX connections should also work for 1000BASE-T, provided that all four wire pairs are connected. However, it is recommended that for all critical connections, or any new cable installations,

Category 5e or Category 6 cable should be used. The Category 5e and 6 specifications include test parameters that are only recommendations for

Category 5. Therefore, the first step in preparing the existing Category 5 cable to run 1000BASE-T is to make sure that it complies with the IEEE 802.3-2005 standards.

Cable Type	Maximum Cable Length	Connector
Category 5, 5e or 6 100-ohm UTP or STP	100.m (328 ft)	RJ-45

100/1000/2500 Mbps Fast Ethernet Collision Domain

Cable Type	Maximum Cable Length	Connector
Category 5, 5e or 6 100-ohm UTP or STP	100.m (328 ft)	RJ-45

Cable Labeling and Connection Records

When planning a network installation, it is essential to label the opposing ends of cables and record where each cable is connected. This will allow the user to easily locate inter-connected devices, isolate faults, and change the topology without the need for unnecessary time consumption.

To best manage the physical implementations of your network, follow these guidelines:

- Clearly label the opposing ends of each cable.
- Use your building's floor plans to draw a map of the locations of all network-connected equipment. For each piece of equipment, identify the devices to which it is connected.
- Note the length of each cable and the maximum cable length supported by the midspan ports.
- For ease of understanding, use a location-based key when assigning prefixes to your cable labeling.
- Use sequential numbers for cables that originate from the same equipment.
- Differentiate between racks by naming accordingly.
- Label each separate piece of equipment.
- Display a copy of your equipment map, including keys to all abbreviations at each equipment rack.

Basic Troubleshooting Tips

Most problems are caused by the following situations. Check for these items first when starting your troubleshoot
Connecting to devices that have a fixed full-duplex configuration.
The RJ-45 ports will pass through data as it is received from external sources.

- If the connected device is also configured to "Auto", the midspan will automatically negotiate both link speed and communication mode.
- If the connected device has a fixed configuration (e.g. 100Mbps at half or full duplex), the midspan will automatically sense the link speed but will default to a communication mode of half-duplex.
- Because the series Vi22108U/Vi22116U behave in this way (in compliance with the IEEE802.3 standard), if a device connected to the midspan has a fixed configuration at full duplex, the device will connect correctly to the external device.
- Make sure all devices connected to the Vi22108U/Vi22116U are configured to pass PoE with wiring configured as per the IEEE standards
- Faulty or lose cables. Look for loose or faulty connections. If they appear to be OK, make sure the connections are snug. If that does not correct the problem, try a different cable.
- Non-standard cables. Non-standard and mis wired cables may cause network collisions and other network problems and can seriously impair network performance. Use a new correctly wired cable for pinouts and correct cable wiring. A category 5, 5e, 6, 6a cable tester is a recommended tool for every 100Base-TX and 1000Base-T network installation.
- Improper Network Topologies. It is important to make sure you have a valid network topology. If you no longer experience the problems, the new topology is probably at fault. In addition, you should make sure that your network topology contains no data path loops.
- Check the port configuration of your network switch and connected device. A port on your midspan may not be operating as you expect because it has been put into a "blocking" state by various switch settings

Basic Troubleshooting Chart

Symptom	Action
POWER LED is Off	o Check connections between the midspan, the power cord, and the wall outlet. o Contact your dealer for assistance.
Link LED is Off-Only on Set Up Port	o Verify that the midspan and attached device are powered on. o Be sure the cable is plugged into the midspan and corresponding device. o If the midspan is installed in a rack, check the o connections to the punch-down block and the patch panel. o Verify that the proper cable type is used, and its length does not exceed specified limits. o Check the adapter on the attached device and cable o connections for possible defects. Replace the defective adapter or cable if necessary.

If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or internal power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses, or surges at the power outlet. If you still cannot isolate the problem, the internal power supply may be defective. Verify that all system components have been properly installed. If one or more components appear to be malfunctioning (e.g. the power cord or network cabling), test them in an alternate environment where you are sure that all the other components are functioning properly.

You can access the management agent in the midspan from anywhere within the attached network using Telnet, a web browser. However, you must first configure the midspan with a valid IP address, subnet mask, and default gateway. If you have trouble establishing a link to the management agent, check to see if you have a valid network connection. Then verify that you've entered the correct IP address. Also, be sure the port that you are connecting to the midspan has not been disabled. If it has not been disabled, then check the network cabling that runs between your remote location and the midspan.

IP Addressing: In order to access the Vi22108U/Vi22116U's GUI, your connected computer must be on the same network as the midspan. As the default IP address is 192.168.1.200, the computer you use can be addressed as 192.168.1.xxx (any number except (200).

Power and Cooling Problems

Installation
The Vi22108U/Vi22116U can operate under temperatures ranging from 0C to 40C. The unit is not weatherproof and requires installation in weatherproof housing. Consideration must be given to the potential internal temperature within the housing that will affect operations. Environmental temperatures higher the 40C (104F) can affect operation and potentially result in damage.

Cables

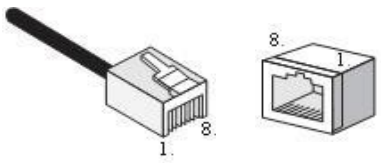
Twisted-Pair Cable and Pin Assignment
For 10/100/1000/2500 BASE-TX connections, the twisted-pair cable must have two pairs of wires. For 1000BASE-T connections, the twisted-pair cable must have four pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be green and the other, green with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

CAUTION: DO NOT plug a phone jack connector into any RJ- 45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

CAUTION: Each wire pair must be attached to the RJ-45 connectors in a specific orientation.

The figure below illustrates how the pins on the RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

Figure 19: RJ-45 Connector Pin Numbers/100BASE-T/1000Base-Tx/2500Base Pin Assignments



Use unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for RJ-45 connections: 100-ohm Category 3 or better cable for 10 Mbps connections, or 100- ohm Category 5 or better cable for 100 Mbps connections. Also, be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

The RJ-45 ports on the midspan base unit support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs or servers, or to other midspans or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3, and 6 at the other end of the cable. When using any RJ-45 port on this midspan, you can use either a straight-through or crossover cable.

Pin	MDI Signal Name	MDI-X Signal Name
1	Transmit Data plus (TD+)	Receive Data plus (RD+)
2	Transmit Data minus (TD-)	Receive Data minus (RD-)
3	Receive Data plus (RD+)	Transmit Data plus (TD+)
6	Receive Data minus (RD-)	Transmit Data minus (TD-)
4,5,7,8	Not used	Not used

NOTE: The "+" and "-" signs represent the polarity of the wires that make up each wire pair.

EIA/TIA 568B RJ-45 Wiring Standard

Straight-Through Wiring

If the twisted-pair cable is to join two ports and only one of the ports has an internal crossover (MDI-X), the two pairs of wires must be straight-through (when auto-negotiation is enabled for any RJ-45 port on this midspan, you can use either straight-through or crossover cable to connect to any device type).

You must connect all four wire pairs as shown in the following diagram to support Gigabit Ethernet.

EIA/TIA 568B RJ-45 Wiring Standard 10/100BASE-TX
Straight-through Cable
Figure 20: Straight-through Wiring

If the twisted-pair cable is to join two ports and either both ports are labeled with an "X" (MDI-X) or neither port is labeled with an "X" (MDI), a crossover must be implemented in the wiring (when auto-negotiation is enabled for any RJ-45 port on this midspan, you can use either straight-through or crossover cable to connect to any device type).

You must connect all four wire pairs as shown in the following diagram to support Gigabit Ethernet

Crossover Wiring

10/100BASE-TX Crossover Cable

Figure 21: Crossover Wiring

1000Base-T Pin Assignments

If your existing Category 5 installation does not meet one of the test parameters for 1000Base-T, there are three measures that can be applied to try and correct the problem:

Replace any Category 5 patch cables with high-performance Category 5e or Category 6 cables.
Reduce the number of connectors used in the link.
Reconnect some of the connectors in the link.

1000BASE-T MDI and MDI-X Port Pin-Out

All 1000BASE-T ports support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs or servers, or to other midspans or hubs.
The table below shows the 1000/2500 BASE-T MDI and MDI-X port pin outs. These ports require that all four pairs of wires be connected. Note that for 1000/2500BASE-T operation, all four pairs of wires are used for both transmit and receive.
Use 100-ohm Category 5, 5e, or 6 unshielded twisted-pair (UTP) or shielded twisted- pair (STP) cable for 1000/2500BASE-T connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 ft).

Pin	MDI Signal Name	MDI-X Signal Name
1	Bi-directional Pair A Plus (BI_DA+)	Bi-directional Pair B Plus (BI_DB+)
2	Bi-directional Pair A Minus (BI_DA-)	Bi-directional Pair B Minus (BI_DB-)
3	Bi-directional Pair B Plus (BI_DB+)	Bi-directional Pair A Plus (BI_DA+)
4	Bi-directional Pair C Plus (BI_DC+)	Bi-directional Pair D Plus (BI_DD+)
5	Bi-directional Pair C Minus (BI_DC-)	Bi-directional Pair D Minus (BI_DD-)
6	Bi-directional Pair B Minus (BI_DB-)	Bi-directional Pair A Minus (BI_DA-)
7	Bi-directional Pair D Plus (BI_DD+)	Bi-directional Pair C Plus (BI_DC+)
8	Bi-directional Pair D Minus (BI_DD-)	Bi-directional Pair C Minus (BI_DC-)

(NEXT), and Far-End Crosstalk (FEXT). This cable testing information is specified in the ANSI/TIA/EIA-TSB-67 standard. Additionally, cables must also pass test parameters for Return Loss and Equal-Level Far-End Crosstalk (ELFEXT). These tests are specified in the ANSI/TIA/EIA-TSB-95 Bulletin, “The Additional Transmission Performance Guidelines for 100 Ohm 4-Pair Category 5 Cabling.

NOTE: That when testing your cable installation, be sure to include all patch cables between midspans and end devices.

Specifications

Physical Characteristics

Ports	8/16 100/1000/2500Mbps UTP Data + PoE ports 8/16 100/1000/25000Mbps UTP Data only ports 1 Network UTP port
Network Interface	Ports 1-8/16: RJ-45 Connector 10BASE-T: RJ-45 (100-ohm, UTP cable; Category 3 or better) 100BASE-TX: RJ-45 (100-ohm, UTP cable; Category 5 or better) 1000/2500BASE-T: RJ-45 (100-ohm, UTP or STP cable; Category 5, 5e or 6) *Maximum Cable Length - 100 m (328 ft)
Weight	11Lb, 5kg-
Size	1.75x17x10.5 in, 4.3x43x26.4 cm (HxWxL)
Temperature	Operating: 0°C to 40°C (32°F to 104°F)
Humidity	Operating: 5% to 90% (non-condensing)
Power Input	120/240VAC 60/50Hz
Power Consumption	70W Resting 813 W when all ports are used to their maximum power levels

Management Features

In-Band Management	Network connection (RJ-45) console port
Software Loading	Upgrading only- Windows™ based

Standards

IEEE 802.3 => 10Base-T Ethernet (Twisted-pair Copper)
IEEE 802.3u => 100Base-TX Ethernet (Twisted-pair Copper)
IEEE 802.3ab => 1000Base-TX Ethernet (Twisted-pair Copper) IEEE 802.3z => 1000Base-X Ethernet
IEEE 802.3bz => 2500Base-T Ethernet (Twisted pair Copper)
IEEE 802.3at/af/bt- common nonstandard forms => Power Over Ethernet (PoE)

Emissions

EN55022 (CISPR 22) Class A EN 61000-3
FCC Class A
CE Mark

Immunity

EN 61000-4-2/3/4/5/6/8/11
EN 55024

Compliances

10Base-T	IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3, 4, or 5 UTP cable.
100Base-T	IEEE 802.3u specification for 100 Mbps Ethernet over two pairs of Category 5 UTP cable.
1000Base-LH	Specification for long-haul Gigabit Ethernet over two strands of 9/125 micron core fiber cable.
1000Base-LX	IEEE 802.3z specification for Gigabit Ethernet over two strands of 50/125, 62.5/125, or 9/125-micron core fiber cable.
1000Base-SX	IEEE 802.3z specification for Gigabit Ethernet over two strands of 50/125 or 62.5/125-micron core fiber cable.
1000Base-T	IEEE 802.3ab specification for Gigabit Ethernet over 100-ohm Category 5e, or 6 twisted-pair cable (using all four wire pairs).
2500Base-T	IEEE 802.3ab specification for Gigabit Ethernet over 100-ohm Category 5e, or 6 twisted-pair cable (using all four wire pairs).
Auto-Negotiation	Signaling method allowing each node to select its optimum operational mode (e.g. speed and duplex mode) based on the capabilities of the node to which it is connected.
Bandwidth	The difference between the highest and lowest frequencies available for network signals. Also synonymous with wire speed, the actual speed of the data transmission along the cable. - as noted by input wire speed
Ethernet	A network communication system developed and standardized by DEC, Intel, and Xerox, were using baseband transmission, CSMA/CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration into the OSI model and extends the physical layer and media with repeaters and implementations that operate on fiber, thin coax, and twisted-pair cable.
Fast Ethernet	A 100 Mbps network communication system based on Ethernet and the CSMA/ CD access method.
Full Duplex	Transmission method that allows two network devices to transmit and receive concurrently, effectively doubling the bandwidth of that link.
Gigabit Ethernet	A 1000 Mbps network communication system based on Ethernet and the CSMA/ CD access method.
IEEE	Institute of Electrical and Electronic Engineers.
IEEE 802.3	Defines carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.
IEEE 802.3AB	Defines CSMA/CD access method and physical layer specifications for 1000BASE-T Gigabit Ethernet (now incorporated in IEEE 802.3- 2005).
IEEE 802.3U	Defines CSMA/CD access method and physical layer specifications for 100BASE- TX Fast Ethernet (now incorporated in IEEE 802.3- 2005).
IEEE 802.3X	Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links (now incorporated in IEEE 802.3-2005).
IEEE 802.3Z	Defines CSMA/CD access method and physical layer specifications for 1000BASE Gigabit Ethernet (now incorporated in IEEE 802.3-2005).
IEEE 802.3at/af/bt	Defines Power Over Ethernet is used to transmit electrical power, PoE IEEE 802.3af (Class 4 PDs limited to 15.4W), IEEE 802.3at (Class 4 PDs limited to 30W). PoE Classes 5-8 conforming to 802.3bt standards. Most used nonstandard high PoE forms
Lan Segment	Separate LAN or collision domain.
LED	Light emitting diode used for monitoring a device or network/PoE condition.
RJ-45 Connector	A connector for twisted-pair wiring.
Mid span Ports	Separation of ports that provide both PoE and Data and those that provide only data connections
TIA	Telecommunications Industry Association.
Transmission Control Protocol/Internet Protocol (TCP/IP)	Protocol suite that includes TCP as the primary transport protocol and IP as the network layer protocol. Applied to network port only
User Datagram Protocol (UDP)	UDP provides a datagram mode for the packet-midspan communications. It uses the IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection- less data grams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.
UTP	Unshielded twisted-pair cable.

RETURN TO DEFAULT

In some cases, it may be necessary to return the Vi22108/Vi22116 to its default settings. **As with the exception of the Default IP address the only method return to the rest of the default setting is download and save them prior to programming.**

If the GUI can be accessed use the system maintenance setting. Remember once activated your computer will lose its connection and you will need to log in using the default IP address

If the GUI cannot be accessed, you can use the front panel button.

To default the Midspan press the front panel reset button.

1) Push and hold the Default button using a small, pointed object like a paper clip.
2) After about 12 seconds of holding the button, the Power LED will begin to blink.
3) Release the button.
4) When the factory values are finished loading, the Power LED will stop blinking and remain on steady. The Midspan will no longer contain any of the previous user configurations.

You will need to log in using the default IP address

Note: Default will reset the IP address back to 192/168.1.200. All previous settings that have been saved will be restored as the saved setting.

To default Midspan press the front panel reset button.

1. Push and hold the Default button using a small, pointed object like a paper clip.
2. After about 12 seconds of holding the button, the Power LED will begin to blink.
3. Release the button.
4. When the factory values are finished loading, the Power LED will stop blinking and remain on steady. The Midspan will no longer contain any of the previous user configurations.

You will need to log in using the default IP address

Note: Default will reset the IP address back to 192/168.1.200. All previous settings that have been saved will be restored as the saved setting. When the front panel reset button is used to return to default the power LED will flash several times indicating defaults are being installed. In this case all previously programmed settings are returned to default and must be re-programmed.

It is suggested once the midspan is programmed to your required settings, download the and save the configuration.

Note the following changes to previously programmed settings when the Front Panel Reset Button is Pressed:

a. The IP address will be changed to 192.168.1.200
b. The subnet mask will be 255.255.255.0
c. The Gateway will be 192.168.1.1
d. The Username will be “admin”
e. The password will be “system”
f. AutoChecking for all ports will be disabled. Note: To restart Autochecking, the Operator will need to be Re-enabled in the AutoChecking portion in the GUI)

Power Loss and Restore

If the Vi22116S loses power and then it is restored: a. Programming is not changed, and all operations will continue as they were prior to the power disruption. b. When power is restored,

Restoring AutoChecking:

If Autochecking disables a port:

a. The Power LED will Flash
b. The power LED will continue to Flash
c. In this case the operator must enable Autochecking
d. The only time AutoChecking will flash the power LED is when it disables a port.

When Autochecking is First Activated:

a. There is no effect on the front panel LEDs.
b. When a port is delivering power, the green port LED will come on regardless to whether AutoChecking is being used or not.

Port Temperature Control

All Ports are continuously monitored for temperature which is based on the connection condition. A short will tend to raise port temperature. The fixed temperature setting is 135C / 266F

1. 1.If auto checking is not active shut down will be temporary. When the temperature returns below 120C/248F the port will return to normal operation.
2. 2.If auto checking is enabled when temperature port shut down occurs, auto checking will remain active and will re-establish the connection when port temperature falls below 120C/248F. If Syslog is active the port condition and Over temperature error will be reported.

Watchdog Timer

In event a lock up occurs which can be the result on mains power surges. The Vi22116S/Vi22108S has a built in watchdog timer. If the lock up is more than 15 seconds, the watchdog will attempt a reset. Messaging will be sent via the Syslog.

sysname at syslocation (192:168:1:200): System Watchdog Restart.

Warranty

Vigitron, Inc. guarantees that all Vigitron products (“Product”), if used in accordance with these instructions, will be free of defects in material and workmanship for a lifetime defined as the duration period of time until product end of life is announced.

After which, Vigitron will continue to provide warranty services for a period of 3 years. The period covering valid warranty will be determined by proof of purchase in the form of an invoice from an authorized Vigitron dealer.

Warranty will only be provided for as long as the original end-user purchaser owns the product. The warranty is not transferrable. At Vigitron's option, the defective product will be repaired, replaced, or substituted with a product of equal value. This warranty does not apply if in the judgment of Vigitron, Inc., the Product fails due to damage from shipment, handling, storage, accident, abuse, or misuse, or if it has been used or maintained not conforming to product manual instructions, has been modified, or serial number removed or defaced. Repair by anyone other than

Vigitron, Inc. or an approved agent will void this warranty. Vigitron, Inc. shall not under any circumstances be liable to any person for any incidental, indirect, or consequential damages, including damages resulting from use or malfunction of the product, loss of profits or revenues, or costs of replacement goods. The maximum liability of Vigitron, Inc. under this warranty is limited to the original purchase price of the product only.

Contact Information

7810 Trade Street, Suite 100 San Diego, CA 92121
Phone: 858-484-5209
Fax: (858) 484-1205
www.vigitron.com
support@vigitron.com

Accessing the Midspan GUI

Network and Non- Network Secure Operations:

For Secure Operations

In some cases, the installation may require the Midspan not to be accessed to avoid hacking. In this case program the Midspan and place it in your system without a network connection. The unit cannot be accessed over the network. If this installation is required to access the Midspan will require connecting a laptop to the network port

In this application Syslog messages will not be able to be recovered

For Network Operations

Connect a network connection to the network port. Using the default address 192.168.1.200 and username: admin, password: system access the midspan. It is recommended you change the Username and Password.

When connected to a network the unit will transmit Syslog messages on port 514.

Defining Network Operating Problems and Solutions

> Web browsers

Do not use web browser standard modes

Standard modes maintain Browser History/Cookies/ and Temporary Internet Files. All of these can prevent you from access your network web-based devices, naming switches

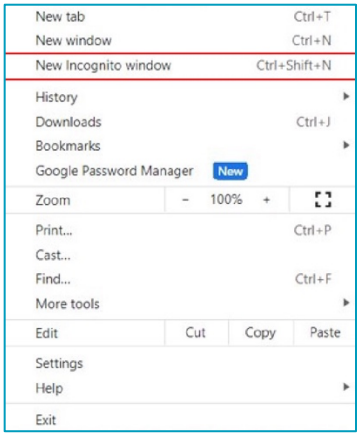
Accessing you Browser's Private Mode

Method one: Keyboard

Browser	Mouse	Keyboard
Chrome	Settings (top right) & New Incognito Window	Ctrl + Shift + N
Edge	Settings (top right) > New InPrivate Window	Ctrl + Shift + P
Firefox	Settings (top right) > New Private Window	Ctrl + Shift + P
Brave	Settings (top right) > New Incognito Window	Ctrl + Shift + N
Safari	Settings (top right) > Private mode	Shift + Command + N

The following Example is Google:

Method Two:



The Midspan can be accessed using most standard network browsers. However, depending on which browser is used, its previous operation and if virus protection software is present access to the Midspan's GUI may be blocked. It is suggested that in accessing the Midspan's GUI use the browser's private mode

GUI Header Controls and Indicators

The icon in the programming GUI displays the status of each port.

Green is normal- the port has a valid connection and is providing PoE
No color- the port is off
Auto checking- Port is disabled during Auto checking and is Red

When completing a programming function press the "Update " button. This will save the function when you exit the mode or if power is lost.

When you use the Update button the individual programmed function will be recorded and maintained. In the event of a power outage the programmed “Saved” function will be loaded.

Use this in the event you what to change the programming. Note all programming with a mode will be reset and require reprogramming.

Some programming functions can have more than one setting mode. Selecting Add allows for programming additional settings. Remember to use the Update functions for each setting you add.

Use the Refresh to update the screen however this may result in having to re-log in.

Home will return you to the Home page

Where active this indicates, the programming selected applies to all ports or actions.

Log out will ask if you want to log out of the website.

Web Browser Configuration Chapter 1: Configuration Preparation

1.1 Access to the Midspan by Web Browser

Important Note: Your choice of Internet browser can affect your ability to access the midspan and/or certain midspan functions. If you experience these problems, please check the browser security settings.

Ensure it is coincident with the following requirements while accessing to the midspan by Web browser.

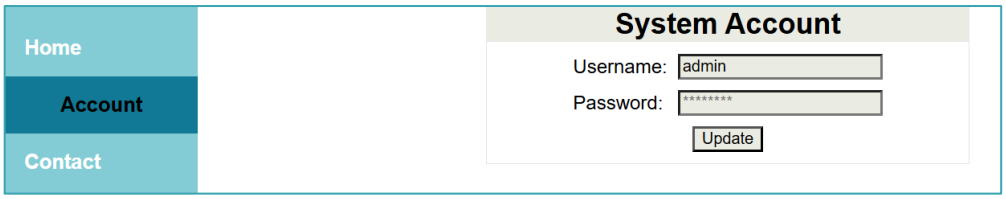
- HTML Version 4.0
- HTTP Version 1.1
- JavaScript™ Version 1.5

Besides, ensure the operation of the main program file supports to access to the midspan, and the computer is connecting to the network of a midspan.

First time access to midspan, you don't need additional configuration but access to midspan directly by using the web browser. If this the first time to use. Revise the IP address of your computer ethernet adapter to"192.168.1. xxx" there the last three digits are different from the Vi22108. The subnet mask is "255.255.255.0".

Open the WEB browser, enter the "192.168.1.200" in the address bar, note that "192.168.1.200" is the defaulted IP address of midspan.

The dialog appears like picture 1 if you use Internet Explorer. Enter the account and passwords in the authenticated dialog, the original username is "admin" and the password is "admin". Please distinguish the capital and small letter.

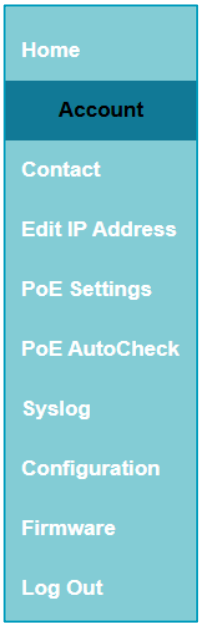


Picture 1: Web Authentication Dialog

Default username: admin
Default password: system

Reset key – default function:

1.2 GUI Guide



Home: Includes system information: Contact Name/System Name/Location/Mac Address/ Software version

Account Page: Contains default Username and Password which can be updated by the operator

Contact page: Provides ability to update Contact person's name/System Name/Location

Edit IP Address Page: Provides the ability to edit: IP Address/ Subnet Mask/Gateway to enable network access

PoE Settings: Provides PoE programming for each port and the ability to confirm if the setting is correct.

PoE Auto Check: Configures individual port to poll connect device and determine if connection is valid and PoE is applied.

Syslog: Assigns IP address or Broadcast for Midspan error and status messages. Midspan must operate on network and client must be able to receive Syslog messages

Configuration: Operator can download and save existing configurations or Upload previously configuration files

Firmware update: used for updating firmware to a new version Please following procedure carefully –

Log out: Removes access to the Midspan and requires a new log in

1.3 Top Control

UPDATE
Note: Up to 5 users can access the Web Browser using the same Username and Password. Access will depend upon the connection and web browser. The access to the Midspans GUI will require a direct connection to the Midpan's IP address. This is done for security reasons and to protect the unit from outside hacking.

The state information and configuration of the device are shown in the Configuration Display. You can change the details by clicking the list items.


Shows Normal Operation


No Link or PoE Present

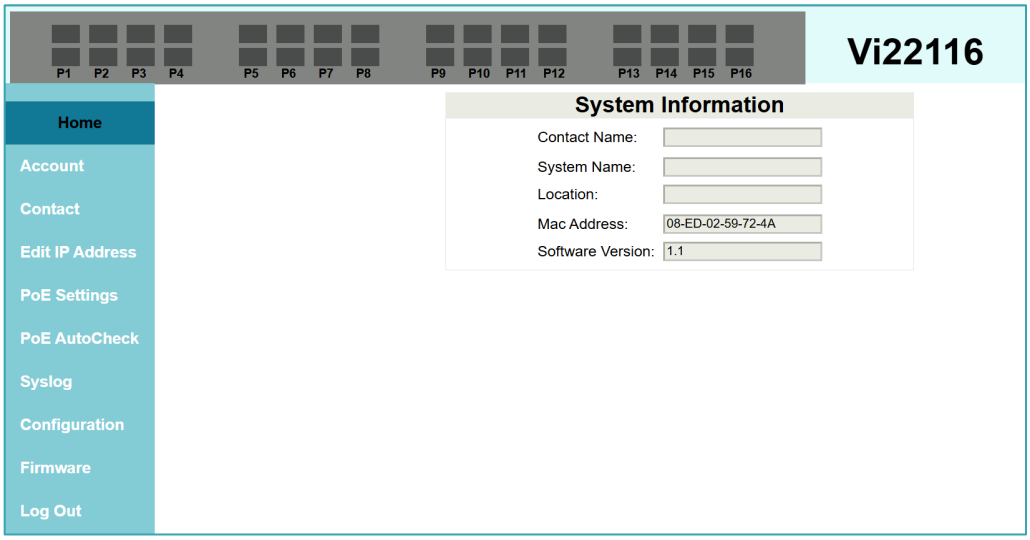
1.4 Login Windows

Default Username: admin
Default Password: system

1.5 Access the GUI

After entering the username and password, the main screen appears as follows.

This Main Page interface includes mainly 3 parts. Here is the description:



Main Menu

The Web agent displays an image of the Managed Midspan's ports. Different colors mean different states, they are illustrated as follows:

Using the onboard Web agent, you can define system parameters, manage, and control the Managed Midspan, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can set up the managed Midspan by selecting the functions those listed in the Main Menu. Following is short description:

Linked; with PoE No link. Disabled by Auto-Checking Port is Off

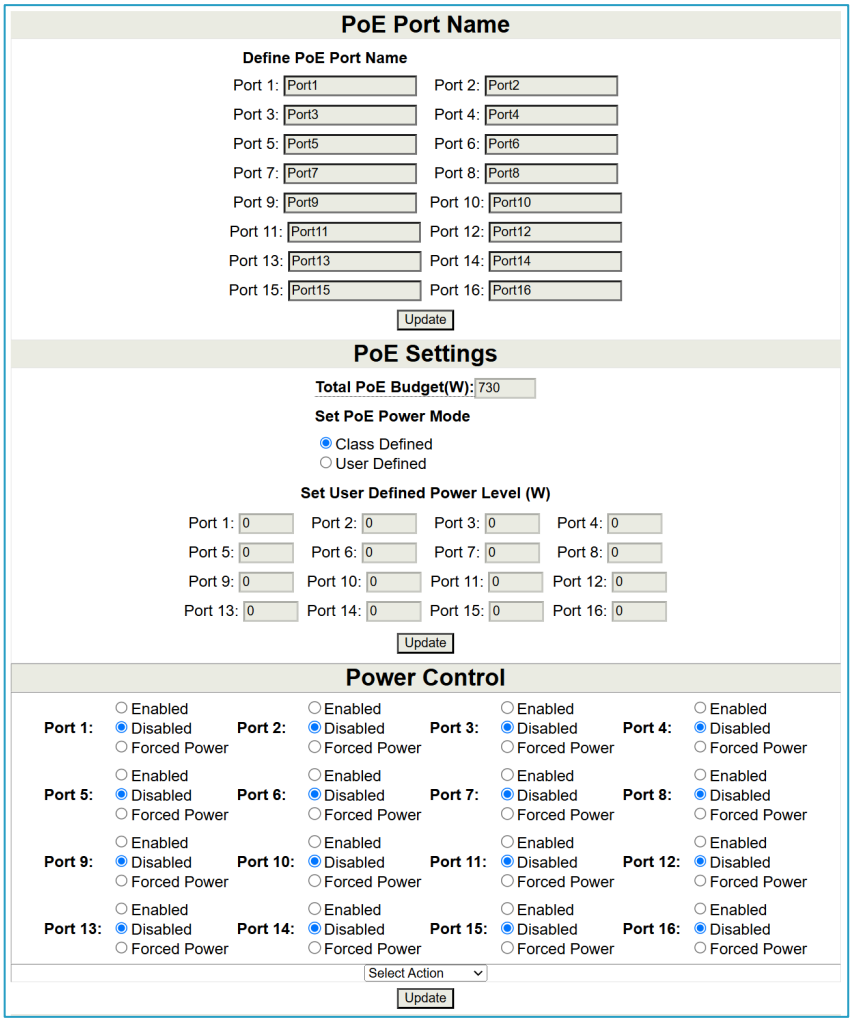
Information & Status – Provides General System Information.
System Name – Name given to the individual model can be any given name.
Location – Where the midspan is located. Location can be any given name.
Mac Address – This is a fixed identifier. It is individual to the unit and cannot be changed.
Software Version – This identifies the current software and is fixed.

Confirming Settings

The Vi22108/Vi22116 has a unique method allowing the operator to verify major settings on a single GUI screen.

PoE Settings
After you complete programming the individual PoE settings for each port select UPDATE

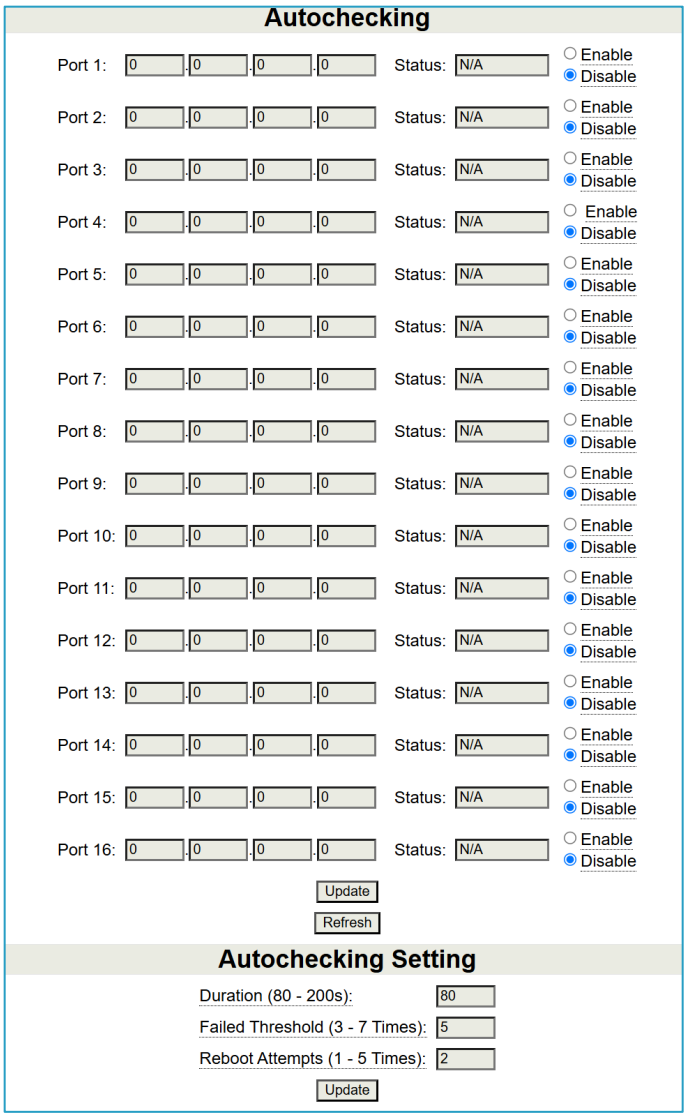
Under PoE Monitoring
Select Refresh and note if the port is showing as on and indicating a Class- if not recheck your settings and repeat the process



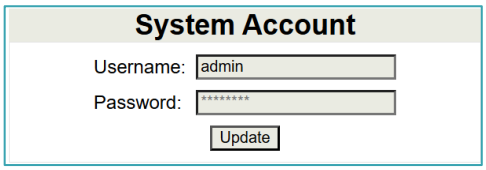
Auto-Checking
Auto-checking ties an individual port to the device connected to that port using that device's IP address.

Program the IP address
Make certain the function for that port is enabled.

Select Update and Refresh
If the connection is valid status will display Good.
If not either the entered IP is incorrect or there is a connection problem.

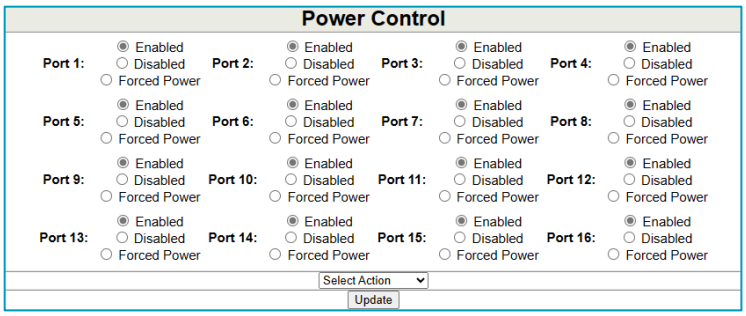


Save settings to Default:



For each setting, pressing the Update will save the setting to memory. It in the event of power loss and restore the save settings will be restored to the previous programmed mode programming.

Extinguishing an alarm condition



An alarm conditions will invoke several reactions on they are:

- GUI LED alarm indicators
- Front panel alarm indicators

The panel program LED will flash if any of the port is shut down by auto checking, this condition require user to login to the GUI to reenable the port(s) to restore the flashing condition.

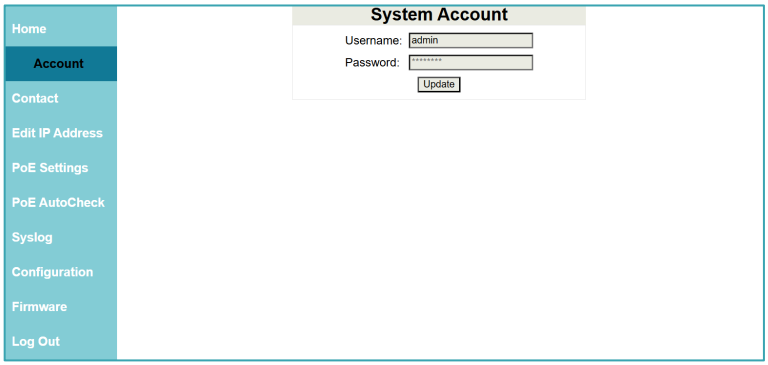
Chapter 2: Account

2.1 Enter a Username and Password or change the existing one.

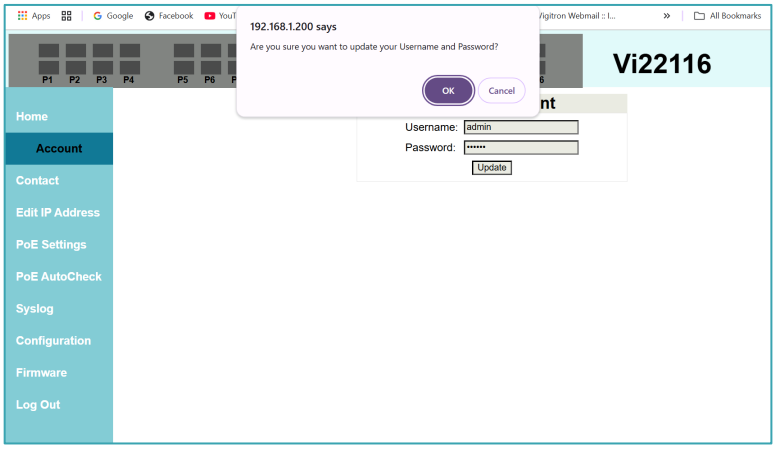
Enter the default IP address 192.168.1.200

The username and password will be required the next time the unit is accessed.

Entries are limited to 15 characters with no spaces allowed.



GUI will send a message to ensure if the user wants to make a change on the username and password.



Chapter 3: System Contact Information

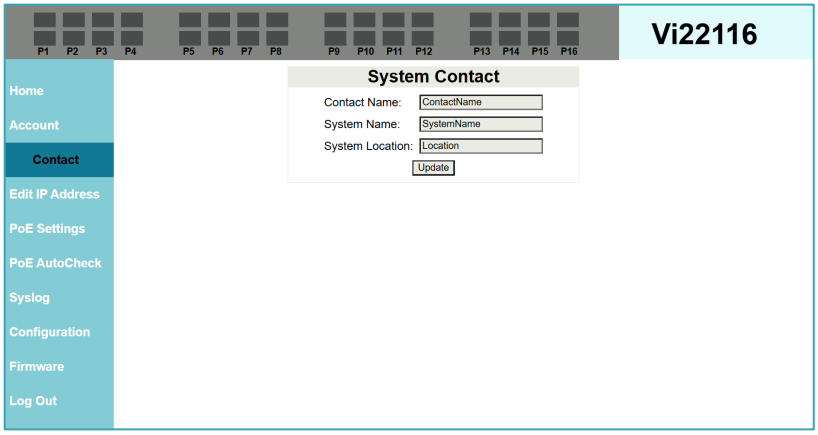
3.1 Enter or Edit

Contact Name
System Name
Location

This information will appear in the home screen and will be contained in the Syslog information.

Entries are limited to 15 characters with no special character allowed except "_".

Press Update



Chapter 4: Enter/Edit IP Address

Syslog IP address: Power Control

4.1 Enter a new or edit the IP address

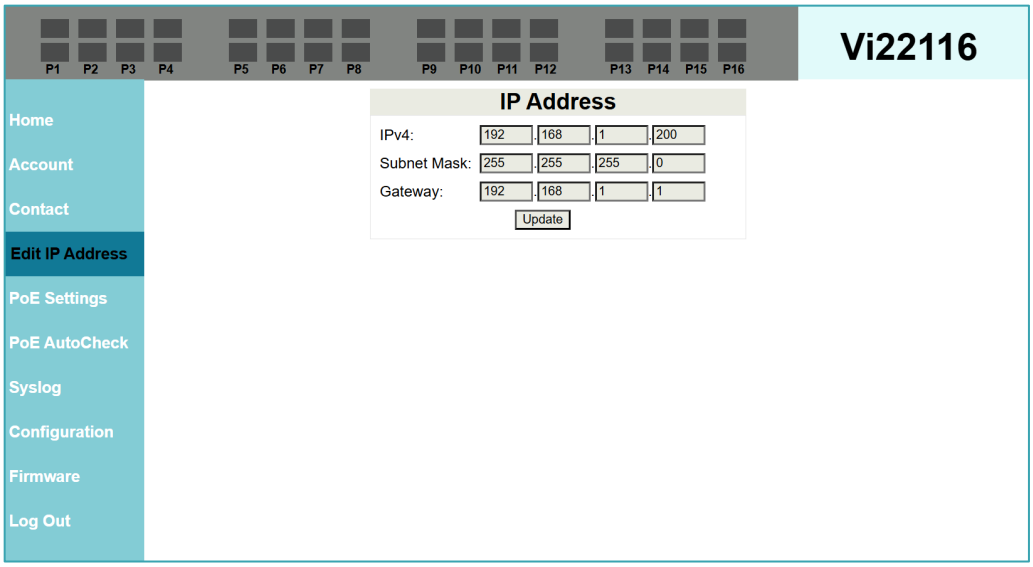
Enter the previous IP address if change or if default enter 192.168.1.200

Enter a new subnet mask – typically will be 255.255.255.0 – which is the default.

Enter a new gateway if required – typically will be to use the default.

Note: the IP address and gateway need to be on the same network as the host

Press Update



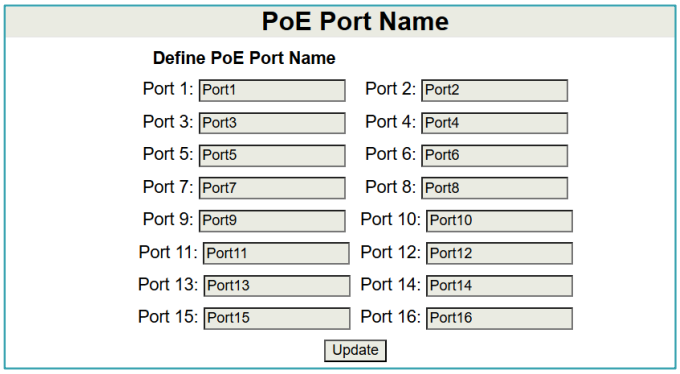
Chapter 5: PoE Settings

5.1 Define PoE Port Name

Enter the PoE port name limited to 15 characters.
The Port name will appear in the Syslog.

Maximum text is limited to 15 characters with no special character allowed except "_".

Press Update to confirm



5.2 PoE Settings

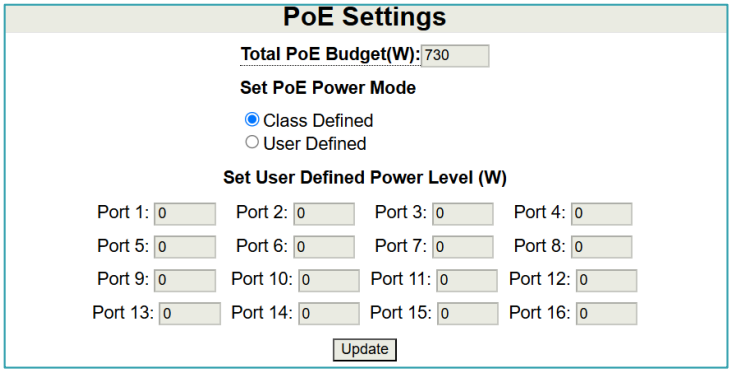
The PoE budget of 730W is fixed by the internal power supply.

Define the PoE Mode:

Class is defined by the maximum power as determined by the PoE Class 0-8.

User Defined is defined by the individual value for each port. The total values cannot exceed more than 730W.

Press Update to apply



Note: You must Enable or Select Forced Power in order to continue with Port PoE programming

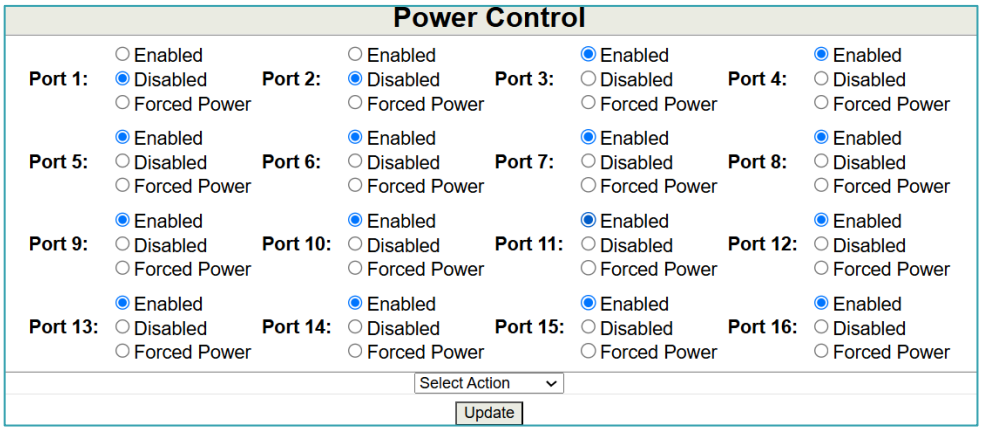
5.3 PoE Power Control

Enable PoE or Disable PoE for each port. If PoE is disabled, the port will still transmit data, but the connected device will not be powered by the port.

Forced Power: This mode provides PoE to the connected device without the need to confirm if the connection is valid or the specific PoE required by the connected device. When using this device safety to prevent damage from shorts or overpower is still in effect.

Select Action: Enables PoE, Disable PoE or Forced Power and can be applied to all ports if this mode is selected. If not then the individual settings for each port will be applied.

Press Update: This applies the settings are programmed



5.4 PoE Monitoring

PoE Monitoring is used to confirm the PoE settings

Refresh: Press the Reset Button: PoE Monitoring will read the settings and the connections to the individual ports showing their status.

Input Voltage: Displays the input volage

For PoE Classes 0-3 the input voltage should be 48V or greater

For PoE Classes 4-8 the input voltage should be 54V or greater

Allocated PoE Power: This is 730W fixed by the internal power supply

Port Power Consumption (w)

This will display the individual the individual power consumption as defined by the connected device. This amount will not necessarily be the same as the programmed PoE.

Port Status:

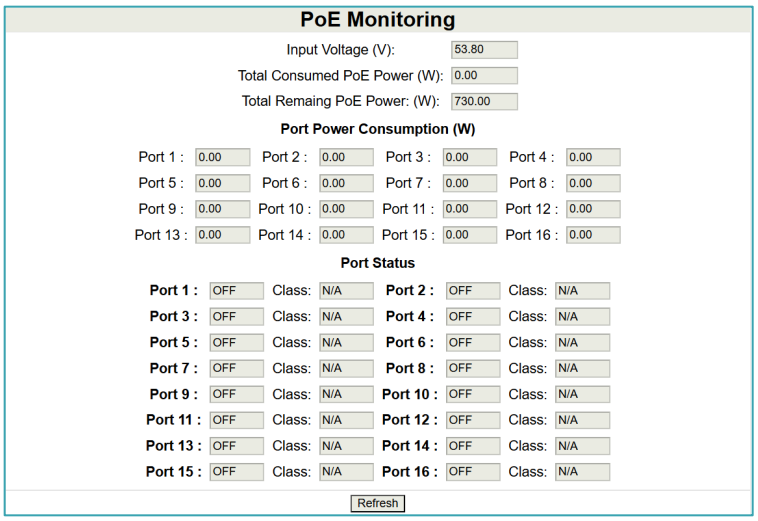
On/Off:

On: The port is active, PoE is being applied to the connected device and the connected device is powered.

Off: The port is not active, PoE is not being applied to the connected device and the connected device is not powered.

Class: If PoE is being applied and the connection is valid the actual PoE class as determined by the connected device will be displayed

Press Refresh



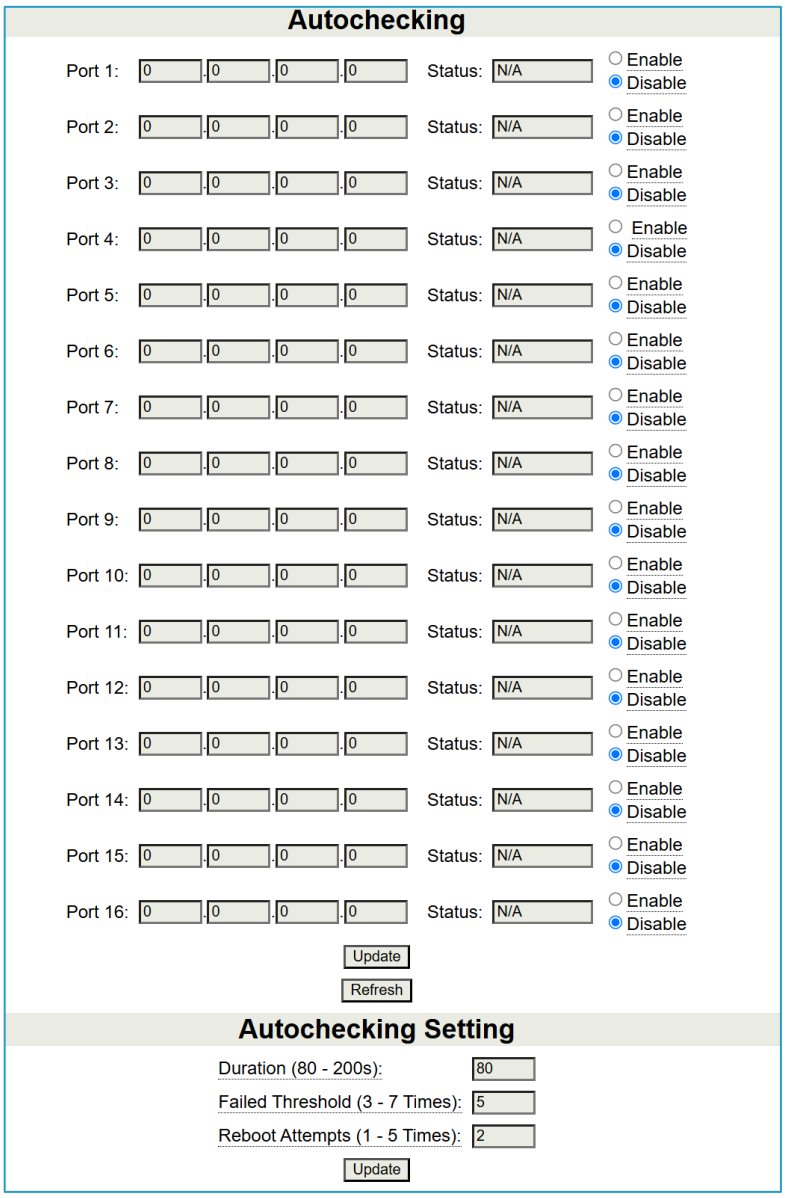
PoE monitoring will confirm if the PoE settings are valid for powering the connected device. If programming for an individual port displays as off, recheck your settings and change the programmed values.

Note on PoE Settings:
When programming PoE take care not to exceed the total PoE budget of 730W. If they figure is exceed, which can be due to connected device power surges, individual ports will automatically be disabled starting with the high number port.

When programming port PoE connected the most critical devices starting with Port 1.

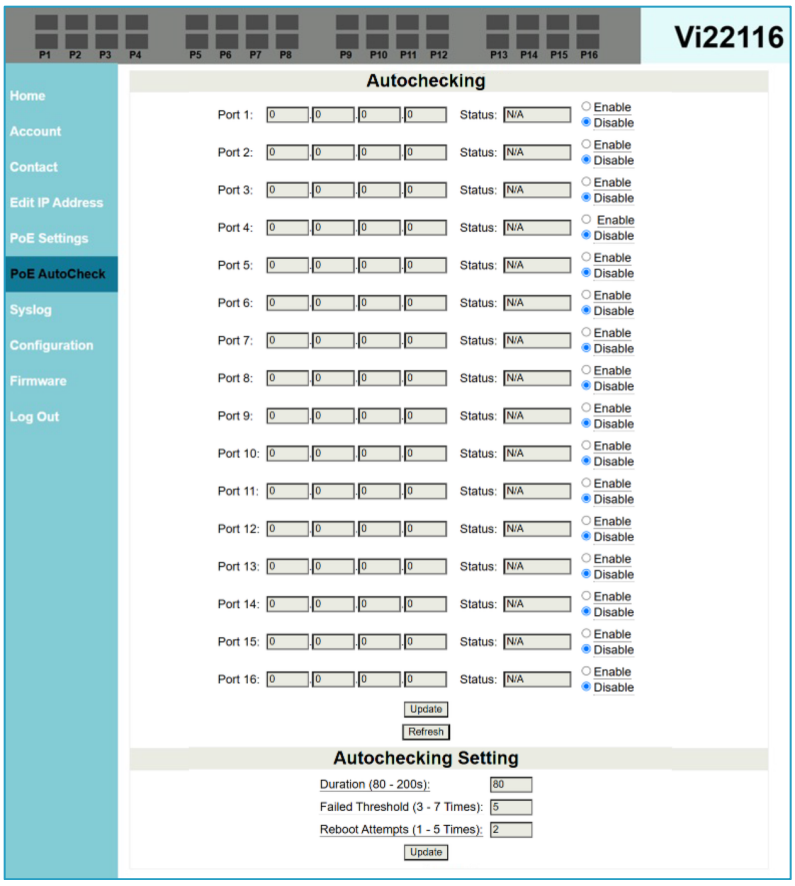
If this occurs you must log into the midspan and manually re-enable the ports.
If the midspan is connected to a network and syslog is active a syslog message will be transmitted.

Chapter 6: PoE Auto-checking



Important Note:

When Auto-checking is activated the GUI Port affected will turn Red and remain Red until the port is re-abled.
If a power cycle occurs during auto checking, when power is restored, the port will no longer be displayed as red as auto-checking will no longer be enabled for that port
The operator will be required to manually -re-enable auto-checking for that port



PoE Checking monitors the connection to a port by pinging the IP address of the connected device. If the connection is lost, the port will attempt to apply PoE and then reconnect eliminating the need for service calls.

Individual connected devices, even those from the same manufacturer with the same model numbers can experience different time to power up which is required first to reconnect. To assure adequate time for power up, the duration is 10 minutes.

If auto checking is enabled on a port, it will function to monitor the port. In the event a connection and PoE is reinstated the port and its settings will be retained and previous operation prior to auto check will be maintained.

The following Syslog messages are available

1. sysname at syslocation (192:168:1:200): System Cold Start.
2. sysname at syslocation (192:168:1:200): Authorized User Logged in.
3. sysname at syslocation (192:168:1:200): Someone tried to log in with wrong credentials.
4. sysname at syslocation (192:168:1:200): Port x (port_name) PoE is ON.
5. sysname at syslocation (192:168:1:200): Port x (port_name) PoE is OFF.
6. sysname at syslocation (192:168:1:200): Port x (port_name) Autocheck Ping Failed.
7. sysname at syslocation (192:168:1:200): Port x (port_name) Autocheck Rebooting.
8. sysname at syslocation (192:168:1:200): Port x (port_name) Autocheck Rebooted.
9. sysname at syslocation (192:168:1:200): Port x (port_name) Autocheck TURN OFF.
10. sysname at syslocation (192:168:1:200): Port x (port_name) is overheated.
11. sysname at syslocation (192:168:1:200): Port x (port_name) shut down due to exceeding PoE budget, system overloaded.
12. sysname at syslocation (192:168:1:200): System Watchdog Restart.

6.1 Enter IP Address

Enter the IP address of the connected device

Enable/Disable: Enable will start the ping and reapplication process.
Disable will disable Auto checking for the port.

Status: Checking: PoE is being applied, but the connected device is not yet powered.
Good: The connection is valid. The connected device is properly powered.
Port Shut Down by Auto checking: Port will show as disabled.
Failed: System attempt to connect and failed.

Update: Press Update to show status

Note: The auto checking process will start after 10 minutes to allow the connected device to power up

6.2 Auto checking Settings

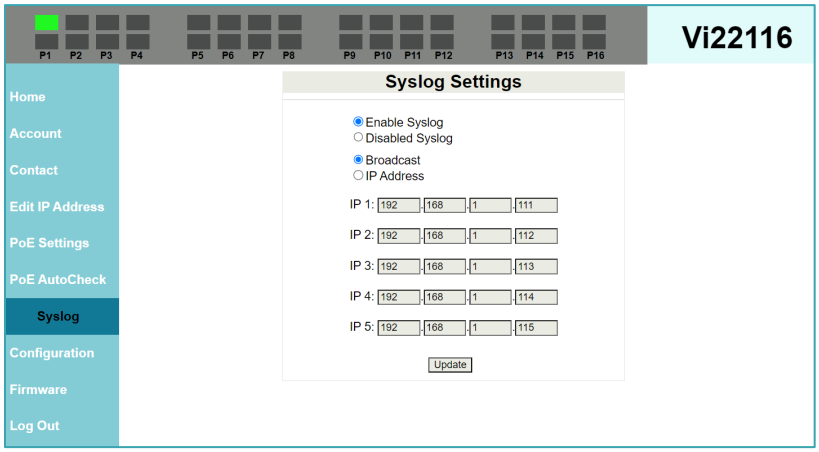
Duration: This sets the duration between pings.

Failed Threshold: This sets this number the system will attempt to connect prior to attempting a reboot. When that number is reached without connecting a reboot will be performed.

Reboot Attempts: The number of attempts prior to stopping the process.

Upon each application the system will wait 10 minutes to assure PoE has been applied to the connected device.

Chapter 7: Syslog Settings

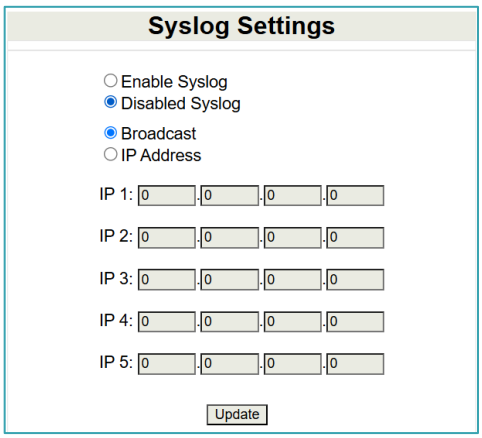


7.1 Syslog

Syslog is a method of status and error messaging. It is transmitted on Port 514. To be received the Midspan must be connected to the network and the midspan has to be on the same network as the client receiving the message. The client must have port opened and software required to receive the messages.

Vigitron provides free software, SysCap™ which can be used to receive and retain syslog messages.

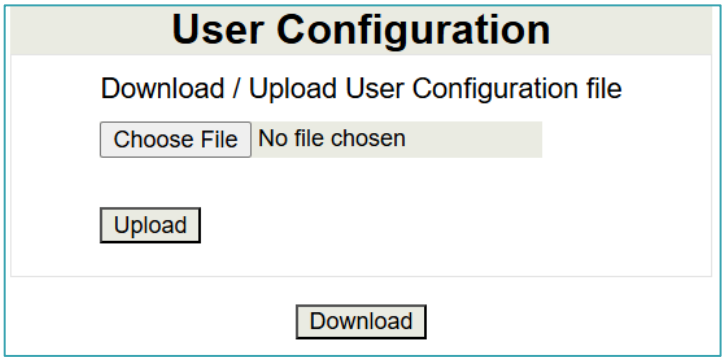
Enable Syslog: The Midspan will transmit syslog messages.
Disable Syslog: The Midspan will not transmit syslog messages.
Broadcast (Syslog needs to be active): Syslog messages will be received by all clients on the network with open port 514 and capable of receiving syslog messages.
IP Address: Syslog messages are only transmitted to the addresses listed. Note: The receiving client must be on the same network as the Midspan.



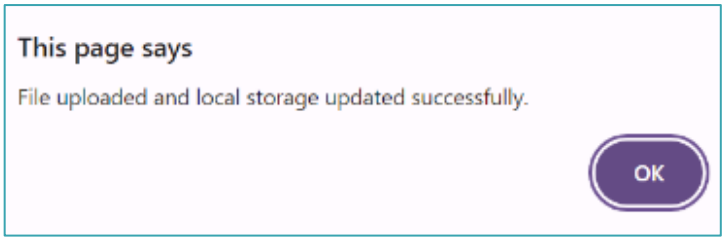
Chapter 8: User Configuration

8.1 Configuration

User Configurations are used to download or upload programmed configurations. Once downloaded they can be uploaded to additional midspans with the same model number reducing programming time – to operate this you must be connected to client.



When the file update is complete the following message will appear

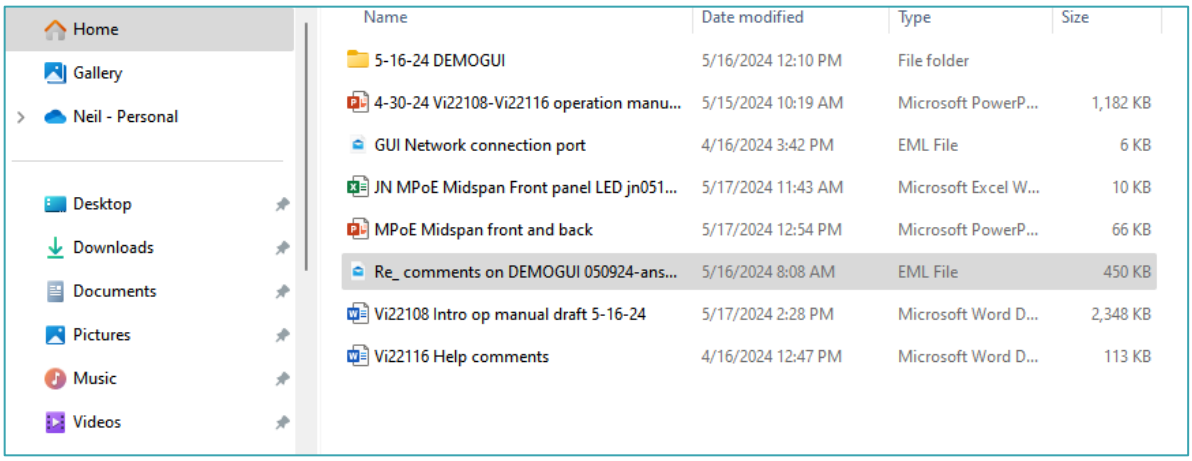


Download:
Choose file: Choose location on your computer where you want to save the configuration. By pressing Choose File, the screen will display the Windows™ based data storage locations. You can provide a custom name to the file.
Download: Press download to save the file.

Upload:
Press Upload: the screen will display the Windows™ based file locations. The file selected must be compatible to the Midspan. It can be one downloaded from the same or same model number midspan.

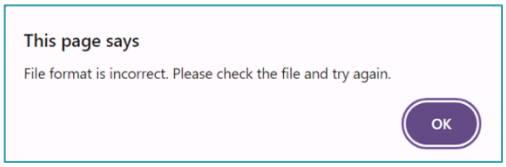
When no file is selected, the screen will display “No File Chosen”.

When Download is selected, the screen will show available spaces on the client computer to save the file.
When Upload is selected the screen will show files on the client computer – a compatible file must be used.



The following message will appear if no file is selected

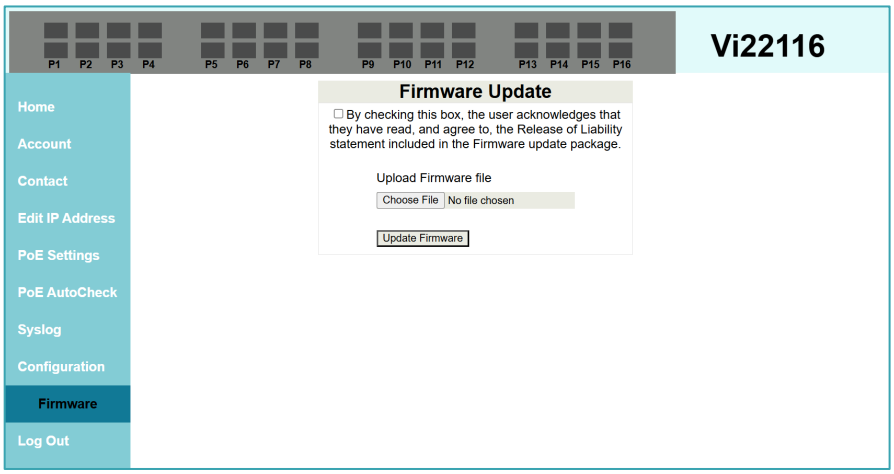
The following message will appear if the wrong file type is selected



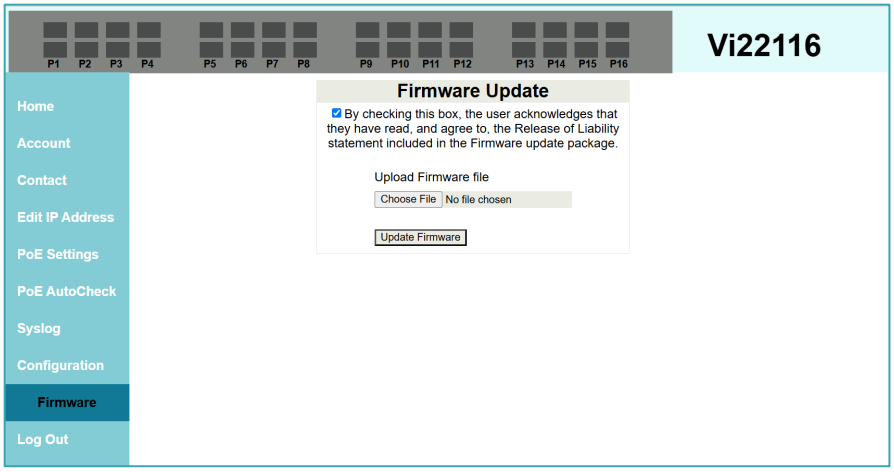
Chapter 9: Firmware Updating

Note: Updating firmware should only be done after consulting with Vigitron. Prior to attempting to update firmware contact Vigitron at support@vigitron.com.
Under normal circumstances if an update becomes necessary you will be contacted by Vigitron.

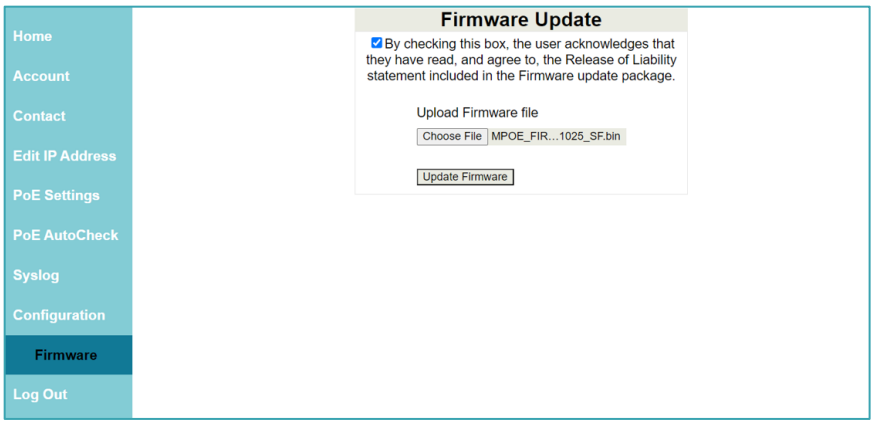
9.1 Firmware Update Procedure



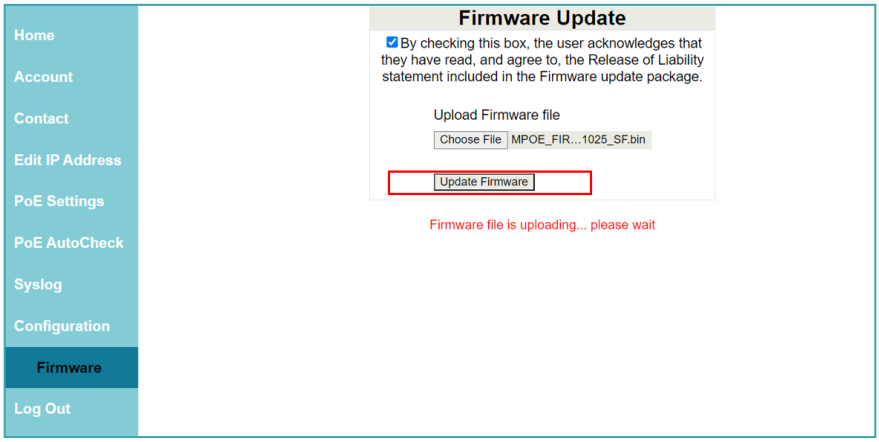
1. Login to the Vi22116U firmware GUI
2. Go to “Firmware” Page



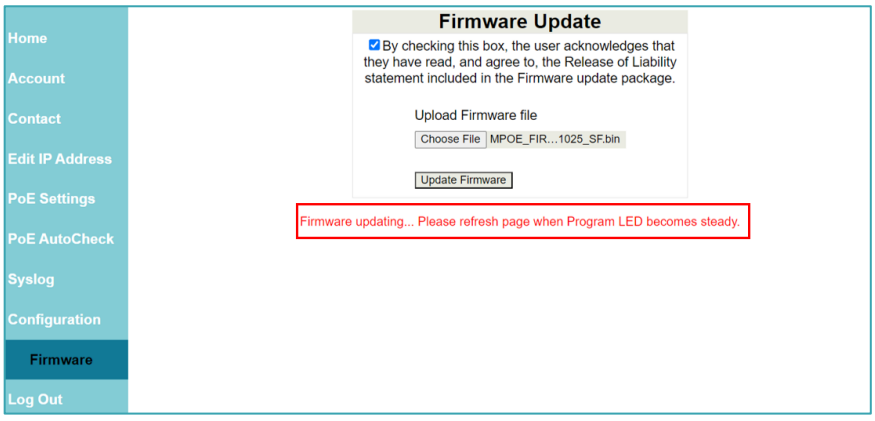
3. Click on Check box to acknowledge the Release of Liability Statement



4. Click on “Choose File” Button to browse and select valid Vigitron Firmware for Vi22116U.
   Note please be certain it is a valid firmware file



5. After firmware file is selected, Click on “Update Firmware” Button
6. Firmware validation process will be run automatically after “Update Firmware” Button is clicked (Red text will show current validation process progress concurrently)
7. After firmware validation process is completed with no error, a Prompt message will be show to confirm the firmware update process
8. Click “OK” to proceed



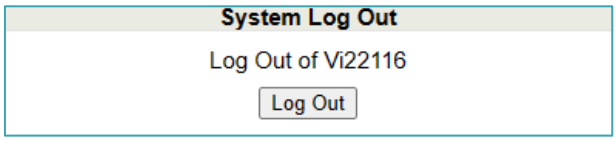
9. Red text will show up to indicate firmware update is in process.
   Observe the Program LED on the unit, when Program LED steps flashing and LED becomes steady, refresh the GUI page to enter the Updated Firmware GUI.

Chapter 10: Log Out

10.1 Log Out

Log out is used to exit programming functions. Once activated, the operator will be required to re-enter the username and password in order to access the program functions.

Press the log out button in order to Log out the programming functions.



Addendum A: Syslog Messages

All **Syslog messaging** include message example:
Sysname at locations (192:168:1:200): System Cold Start.
(Note: Time and Date will be inserted by the Client Computer receiving the Syslog Message)

1. sysname at syslocation (192:168:1:200): System Cold Start.
2. sysname at syslocation (192:168:1:200): Authorized User Logged in.
3. sysname at syslocation (192:168:1:200): Someone tried to log in with wrong credentials.
4. sysname at syslocation (192:168:1:200): Port x (port_name) PoE is ON.
5. sysname at syslocation (192:168:1:200): Port x (port_name) PoE is OFF.
6. sysname at syslocation (192:168:1:200): Port x (port_name) Autocheck Ping Failed.
7. sysname at syslocation (192:168:1:200): Port x (port_name) Autocheck Rebooting.
8. sysname at syslocation (192:168:1:200): Port x (port_name) Autocheck Rebooted.
9. sysname at syslocation (192:168:1:200): Port x (port_name) Autocheck TURN OFF.
10. sysname at syslocation (192:168:1:200): Port x (port_name) is overheated.

To receive Syslog messages:

The client computer must be on the same network as the address
Port 514 must be open (it usually will not require any additional settings)
Your client must have the ability to receive and decode Syslog messages.

Vigitron provides a free Syslog capture software called SysCap™. The software can receive messages from multiple midspans or any network device capable of transmitting Syslog messages.

SysCap can be downloaded from the website at:
https://vigitron.com/product/vi30012/

When SysCap is used, the software will insert the Time and Data as determined by the client.

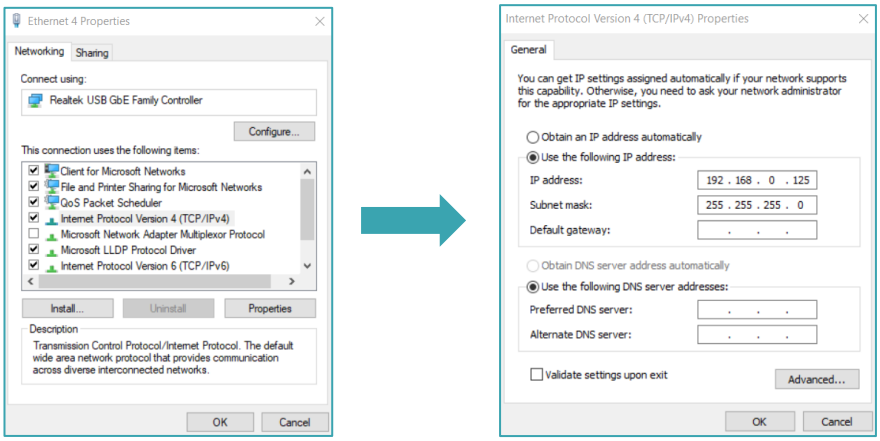
Addendum B: Troubleshooting

I cannot access the Midspan

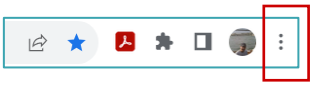
Your midspan must be on the same network as the client you are using to access it.

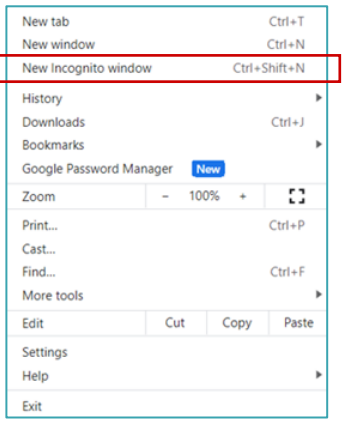
Use your client network settings to put your client on the same network as the Midspan.

As the Midspan default address is: 192.168.1.200
Your client address needs to be: 192.168.1.XXX (any number other than 200)



Do not use the standard browser mode – use the private or incognito mode – depending on the browser
Depending on the browser you will find either three dots or lines in the upper right-hand corner





Select the mode, the screen will show the mode – enter the IP address

Addendum C: Default Settings

The following are Default settings. Many settings still require programming and the ones that are defaulted may not apply to your specific system requirements.

- The following are a readable format for the default settings:
- Username: admin
- Password: system
- Contact name: '' ''
- System Name: '' ''
- System Location: '' ''
- Ip address: 192.168.1.200
- Subnet: 255.255.255.0
- Gateway: 192.168.1.1
- Port name: Port1 - Port16
- Total PoE Budget: 730
- PoE Power Mode: Class Defined
- Defined Power Level: 0W (for Port1 to Port16)
- Power Control: ALL DISABLED
- Auto-checking: ALL PORT IP ADDRESS: 0.0.0.0
- Auto-checking Duration: 80
- Auto-checking Failed Threshold: 5
- Auto-checking Reboot attempts: 2
- Syslog Enable: Disabled
- Syslog Mode: Broadcast
- Syslog IP address: ALL IP ADDRESS: 0.0.0.0

Is the Port Transmitting PoE?

There are several methods to see if PoE is being transmitted from the port:

Look at the GUI unit image

GUI Port Status Color:
Grey: Port is off
Green: PoE Port is connecting and outputting Power
Red: PoE Port is disabled by auto checking
If Port is shut down by auto checking, it will show Red for a short time (3 seconds), then it will become gray to indicate the port is OFF.

If a port is shut down by Auto checking, the GUI LED Indicator will be in Red Color
And User need to re-enable the port to get the red LED condition back to normal

Method 3: Look at Port PoE Monitoring under PoE Settings.

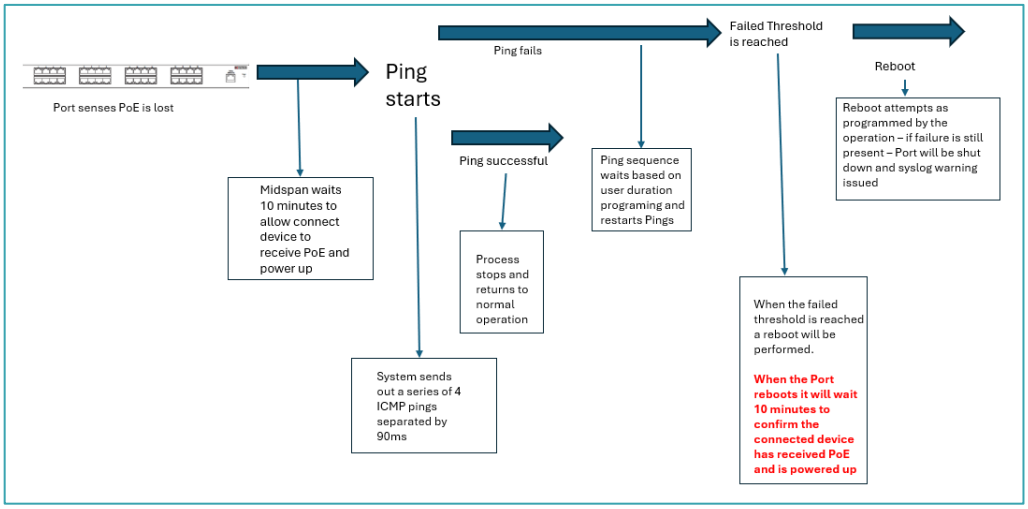
Is my Midspan connected to the network?

Start by: Confirming you are properly addressed. Is the client on the same network as the Midspan?
Check Cables.

Method 1: Look at the units front panel RJ45 network connection. (John what define the RJ45 status of the network connection.)

Method 2: Check the end connected to the computer or server to confirm its LED status
Most managed network switches provide GUI port monitoring.

How does Auto Checking Work?



Important Note:

For licensing information regarding the libraries used in this firmware, please contact Vigitron technical support.

Appendix 5 Glossary

ACE
ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.
ACL
ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights. ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.
AES
AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.
AMS
AMS is an acronym for Auto Media Select. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and cu cables are inserted, the port will select the preferred media.
APS
APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.
ARP
ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.
ARP Inspection
ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.
CC
CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.
CCM
CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to it's peer MEP and used to implement CC functionality.
CDP
CDP is an acronym for Cisco Discovery Protocol.
DEI
DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.
DES
DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.
DHCP
DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.
DHCP Relay
DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.
DHCP Snooping
DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.
DNS
DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.
DoS
DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.
DSCP
DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.
EEE
EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS
EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.
Ethernet Type
Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.
FTP
FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.
Fast Leave
Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.
HTTP
HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW). HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested.
WEB
Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.
Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.
HTTPS
HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection. HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logins. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is no longer considered an adequate degree of encryption for commercial exchange.
ICMP
ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as timestamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.
IEEE 802.1X
IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection, or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.
IGMP
IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming and allows more efficient use of resources when supporting these uses.
IGMP Querier
A router sends IGMP Query messages onto a particular link. This router is called the Querier. There will be only one IGMP Querier that wins Querier election on a particular link.
IMAP
IMAP is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server. IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server. The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.
IP
IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network. IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.
The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new
version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC
IPMC is an acronym for IP MultiCast. IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.
IPMC Profile
IPMC Profile is an acronym for IP MultiCast Profile. IPMC Profile is used to deploy the access control on IP multicast streams.
IP Source Guard
IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.
LACP
LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.
LLC
The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1-byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.
LLDP
LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).
LLDP-MED
LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).
LLQI
LLQI (Last Listener Query Interval) is the maximum response time used to calculate the Maximum Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).
LOC
LOC is an acronym for Loss of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as switch criteria by EPS
MAC Table
Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.
The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC
addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.
MEP
MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).
MD5
MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.
Mirroring
For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)
Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.
MLD
MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.
MLD Querier
A router sends MLD Query messages onto a particular link. This router is called the Querier. There will be only one MLD Querier that wins Querier election on a particular link.
MSTP
In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.
MVR
Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them (Wikipedia).

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

OAM

OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.

Optional TLVs.

A LLDP frame contains multiple TLVs For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for Powered Device. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implements the Ethernet physical layer (IEEE-802.3).

PING

Ping (Packet Internet Grouper) is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

Ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

PoE is an acronym for Power Over Ethernet. Power over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN Access Points (AP), IP cameras and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for Point-to-Point Protocol over Ethernet. It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a private VLAN, PVLANs provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

PTP

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

QCE
QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.
There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.
QCI
QCI is an acronym for QoS Class Identifier. This is a special identifier defining the quality of packet communication provided by LTE (Long Term Evolution, marketed as 4G LTE).
QCL
QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.
Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.
QL
QL In Synced this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.
QoS
QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.
A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.
Achieving the required QoS becomes the secret to a successful end-to-end business solution.
Therefore, QoS is the set of techniques to manage network resources.
QoS class
Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one-to-one mapping between QoS class, queue, and priority. A QoS class of 0 (zero) has the lowest priority.
Querier Election
Querier election is used to dedicate the Querier, the only one router sends Query messages, on a particular link. Querier election rule defines that IGMP Querier or MLD Querier with the lowest IPv4/IPv6 address wins the election.
RARP
RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.
RADIUS
RADIUS is an acronym for Remote Authentication Dial in User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.
RDI
RDI is an acronym for Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP.
Router Port
A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.
RSTP
In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.
SAMBA
Samba is a program running under UNIX-like operating systems (not the Brazilian dance) that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.
Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2. Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".
sFlow
sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.
Additional information can be found at http://sflow.org.
SHA
SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.
Shaper
A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.
SMTP
SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack Protocol using ROUting Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to base on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

Switch ID

Switch IDs (1-1) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

TACACS+

TACACS+ is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame. The 3-bits provide 8 priority levels (0~7).

TCP

TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS

ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP
TKIP is an acronym for Temporal Key Integrity Protocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.
UDP
UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.
UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.
UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.
Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).
UPnP
UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.
User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.
VLAN
Virtual LAN.A method to restrict communication between switch ports. VLANs can be used for the following applications:
VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.
VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.
Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.
VLAN ID
VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.
Voice VLAN
Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.
WEP
WEP is an acronym for Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio and are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).
WiFi
WiFi is an acronym for Wireless Fidelity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual band, etc. The term is promulgated by the Wi-Fi Alliance.
WPA
WPA is an acronym for Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard but will not work with some older network cards (Wikipedia).
WPA-PSK
WPA-PSK is an acronym for Wi-Fi Protected Access - Pre-Shared Key. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)
WPA-Radius
WPA-Radius is an acronym for Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode
security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia).
WPS
WPS is an acronym for Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WRED

WRED is an acronym for Weighted Random Early Detection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame result in a higher probability that the frame is dropped during times of congestion.

WTR

WTR is an acronym for Wait to Restore. This is the time a failure on a resource must be 'not active' before restoration back to this (previously failing) resource is done.