MPoE MaxiiNet^{TM} Vi30406UU
Operation and Installation Manual

4+2 MPoE Industrial Managed PoE Switch

Firmware Version	(Vi304XX1.0)
Revision Date	(6-28-2025)

© 2025 Vigitron, Inc. All rights reserved. All brand and product names are trademarks or registered trademarks of their respective companies.

About This Manual

Copyright

Copyright © 2025 Vigitron, Inc. All rights reserved. The products and programs described in this user's manual are licensed products of Vigitron, Inc. This user's manual contains proprietary information protected by copyright, and this user's manual and all accompanying hardware, software and documentation are copyrighted. No parts of this user's manual may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable from by any means electronic or mechanical. This also Includes photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of Vigitron, Inc.

Purpose

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

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 switch functions, the Internet Protocol and integrating is required.

Conventions

The following conventions are used throughout this guide to show 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 to 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 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 5e or better for 100 Mbps connections, Category 5e or better for 1000 Mbps connections. For fiber optic connections, you may use 50/125- or 62.5/125-micron multimode fiber or 9/125 micron single- mode fiber.

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.

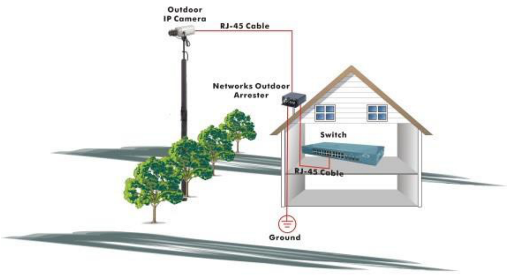
Introduction FCC - Class

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 switch.

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

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

Do not place products outdoors or in a sandstorm.
Before installation, please make sure input power supply and product.
Specifications are compatible with 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 switch will remove the configuration automatically to latest firmware version.

Introduction

Overview

The Vi30406UU PoE switch, is a next generation network solutions using a Unique Vigitron developed MPoE™ firmware providing easy network integration and feature rich PoE programming. It is an affordable managed switch that provides a reliable infrastructure for your business network. These switches deliver more intelligent features you need to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth 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.

Description of Hardware Overview

The Vi30406UU switch is an easy to implement managed Ethernet switch that provides ideal flexibility to design suitable network infrastructure for business requirement. However, unlike other entry-level switching solutions that provide advanced managed network capabilities only in the most expensive models, all Vigitron's series switches support the advanced security management capabilities and network features to support data, voice, security, and wireless technologies. These switches are easy to deploy and configure. They provide stable and quality network services for your business needs.
The switch performs a wire-speed, non-blocking switching fabric. This allows wire- speed transport of multiple packets at low latency on all ports simultaneously. The switch also features full-duplex capability on all ports, which effectively doubles the bandwidth of each connection.

This switch uses store-and-forward technology to ensure maximum data integrity. With this technology, the entire packet must be received into a buffer and checked for validity before being forwarded. This prevents errors from being propagated throughout the network.

The switch can also be managed over the network with a web browser application. Any port can be used to access the switch's GUI for operation and monitoring

Section 1: Description of Hardware

The Vi30406UU is a 4+ 2 network switch. 4 UTP ports provide network connections with PoE. 2 Fiber ports provide network connections. All ports are independent providing the ability to use both sets of UTP and Fiber as uplinks. All UTP and fiber ports at 100Mbps/1G/2.5G. All fiber ports at 1G/2.5G/10G

The switch contains 4/100/ 1000/2500BASE-T RJ-45 ports. All RJ-45 ports support automatic MDI/MDI-X operation, auto- negotiation, and IEEE 802.3x auto-negotiation of flow control, so the optimum data rate, and transmission is selected automatically.

Vi30406UU supports the Small Form Factor Pluggable (SFP) transceiver slots providing 1G/2.5G/10G bandwidth. The SFP transceiver slots are independent from the UTP ports.

The following table shows a list of transceiver types that have been tested with the switch. For an updated list of vendors supplying these transceivers, contact your local dealer. For information on the recommended standards for fiber optic cabling, see “1000 Mbps Gigabit Ethernet Collision Domain”.

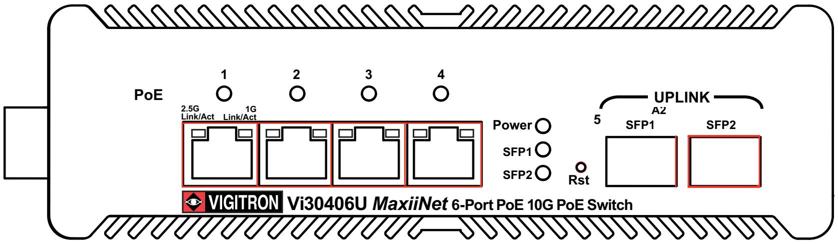
1.1 SFP Interface

Media Standard	**Fiber Diameter** (microns)	**Wavelength (nm)**	**Maximum Distance***
10GBase-LR	9/1.15	1310	10km
2500Base –T	9/1.25		20km
1000BASE-SX	50/125	1310	550 m
	62.5/125	850	275 m
1000BASE-LX/	9/125	1310	10 km
LHX/ XD/ZX	9/125	1550	30.50 km
	9/125	1300	10 km
1000BASE-LX	N/A	TX-1310/RX-1550	20 km
Single Fiber		Tx-1550/RX-1310	20 km
1000BASE-T	N/A	N/A	100 m
100-FX	50/125	850	2 km
	62.5/125	1550	15km

NOTE: Maximum distance may vary for different SFP vendors.

NOTE: The Vi02500CH copper SFP can interface with the Vi30406UU.

1.2 Front LED Status



The following table shows a list of transceiver types that have been tested with the switch. For an updated list of vendors supplying these transceivers, contact your local dealer. For information on the recommended standards for fiber optic cabling, see “1000 Mbps Gigabit Ethernet Collision Domain”.

Front Panel LED Status Description

1. **UTP Port LEDs (Ports 1–4)**

Left LED (Green) – Indicates Link/Activity at 100 Mbps or 1 Gbps
ON (Solid Green) – Link established at 100M/1G
Blinking Green – Data activity at 100M/1G
OFF – No link at 100M/1G

Right LED (Orange) – Indicates Link/Activity at 2.5 Gbps
ON (Solid Orange) – Link established at 2.5G
Blinking Orange – Data activity at 2.5G
OFF – No link at 2.5G

2. **Fiber Port LEDs (Ports 5–6 / SFP1–SFP2)**

Link/Activity LED –
ON (Solid) – Link established
Blinking – Data activity
OFF – No link

3. **PoE LED (per port 1 - 4)**

ON (Green) – PoE is active on that port
OFF – No PoE
(PoE LED status is independent from Link LEDs)

4. **Power LED / Program LED**

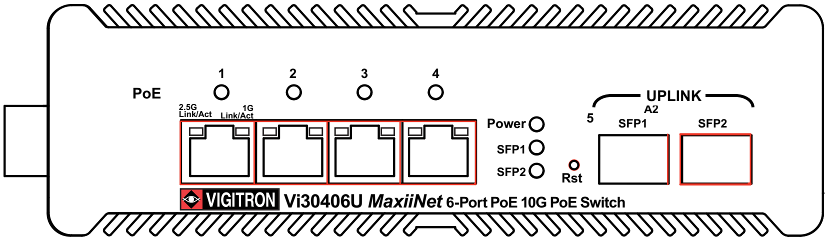
ON (Green) – Device powered and operational
OFF – No power

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

Model Name	Vi30406U
Ports	4* 100Mbps/1G/2.5G POE Port+2*1G/2.5G SFP uplink
Description of Function Slots	Port 1-4: 4 X RJ45 100/1000/2500Mbps (PoE) Port 5-6: 2 X Fiber 1000/2500/10000 Mbps (uplink)
PoE Ports	1-4 port, each port supports af/at/bt, max 90W output
LED Indicator	Pot Port #1-4: **Orange LED – 2.5G Link** **Green LED – 100/1G Link**
	SFP Slot Uplink #5-6 (SFP1) Green LED – Link and activities (SFP2) Green LED – Link and activities
	Power: **GREEEN** System: **N/A**

1.3 Reset Operation

The Vi30406UU has a display panel for system and port indications that simplify installation and network troubleshooting. The LEDs are located on left hand side of the front panel for easy viewing. Details are shown below and described in the following tables.



Reset Button

- Reset the Switch
  - Press and hold reset button for 5 seconds
- Restore the Switch to Factory Defaults
  - Detail procedure to state how to confirm return to default.
    - Press and hold reset button for 10 seconds

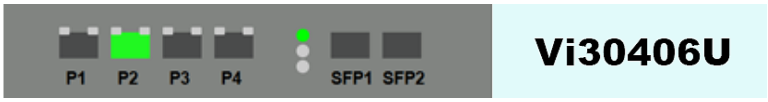
Power LED will be flash, when restoring the switch to Factory defaults, LED will Stop flashing when completed.

Important

a) Reset will reload all previously saved programming
b) b. Reset button will only disable all auto checking, set login username and password to default, change IP address to default; These must be reset after using the front panel reset
c) b. After performing a reset make certain to re- assign the Vi30206U to the address required for your network.

1.4 GUI Status

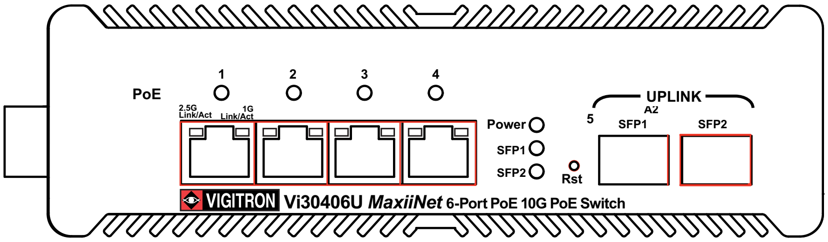
Front Panel Description and Operation



GUI LED Responses

Condition	LED Color	Status	Information
No PoE	Dark Gray	OFF	No PoE is present
PoE Delivering	Green	POE ON	Delivering PoE
2.5G	N/A	N/A	N/A
100/1G	N/A	N/A	N/A
SFP communication	Green	N/A	N/A
Auto checking in Process	N/A	N/A	N/A
Power LED	RED	POE Disabled	Auto check failed
Power LED	Green	Power on	Unit is Powered Up
SFP LED1	N/A	N/A	N/A
SFP LED2	N/A	N/A	N/A

1.5 Panel Status

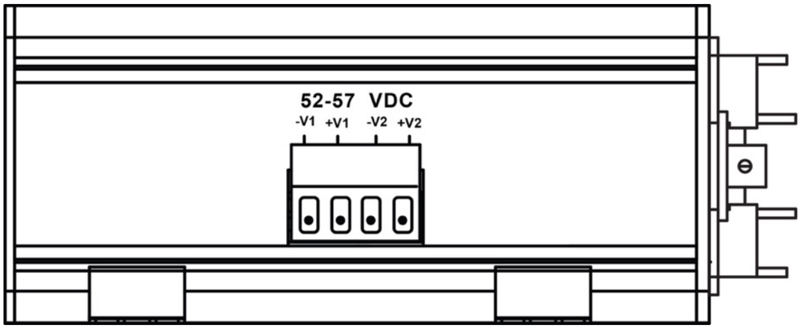


Power LED	Green On	Unit is ON
Power LED	OFF	Unit is OFF
Power LED	Green Flashing	System Programming / Auto checking –Warning
UTP Ports		
Port LED	PoE	Green On Solid PoE is Active
		Off no PoE present
Port LED	100/1G	Green solid – Link it valid
		Green Blinking- activity
Port LED	2.5G	Orange solid- Link is valid
		Orange Blinking -activity
SFP 1 and 2	On	Green SFP connection Link up
	Blinking	Green Activity

1.6 External power connections

Front Panel Description and Operation

The Vi30406UU DC power inputs. The maximum power input for limited to 480W. The power supply used must conform to the IEEE standard, requiring a DC voltage input between 52-57VDC.
Vigitron suggests using one three power supplies: Vi10120 (120 watts), Vi10240 (240 watts), and Vi10480 (480 watts). Please match the required input power to the requirements of your connected devices. The input DC will determine your available PoE budget and should be entered as part of your PoE setup. At least 360W @56VDC is required to have all 4 UTP ports provide 802.3bt @ 90W.



The Vi30406U has two independent power inputs. Each serve as a backup to each other in the event the one fails. Note the total power consumption is 366W. It is not required to have both power inputs connected.

1.7 Introduction of Switch Application and installation

A network switch allows simultaneous transmission of multiple packets. Therefore, the switch has been recognized as one of the most important devices for today's networking technology. The Vi30406UU uses fixed managed complying to L2 functions with the ability to integrate into existing networks.

When performance bottlenecks are caused by congestion at the network access point such as file server, the device can be connected directly to a switched port. By using the full-duplex mode, the bandwidth of the dedicated segment can be doubled to maximize throughput.

When networks are based on repeater (hub) technology, the distance between end stations is limited by a maximum hop count This switch will automatically be configured in any Ethernet, Fast Ethernet, or Gigabit Ethernet network to significantly increase bandwidth while using conventional cabling and network cards. Jumbo frame transmission up to 10.4Kbytes can be transmitted.

The Vi30406U as auto MDIX and 2 slots for the removable SFP module which support comprehensive types of fiber connection, such as LC and BiDi-LC modules. It is not only designed to segment your network, but also to provide a wide range of options in setting up network connections. Some typical applications are described below.

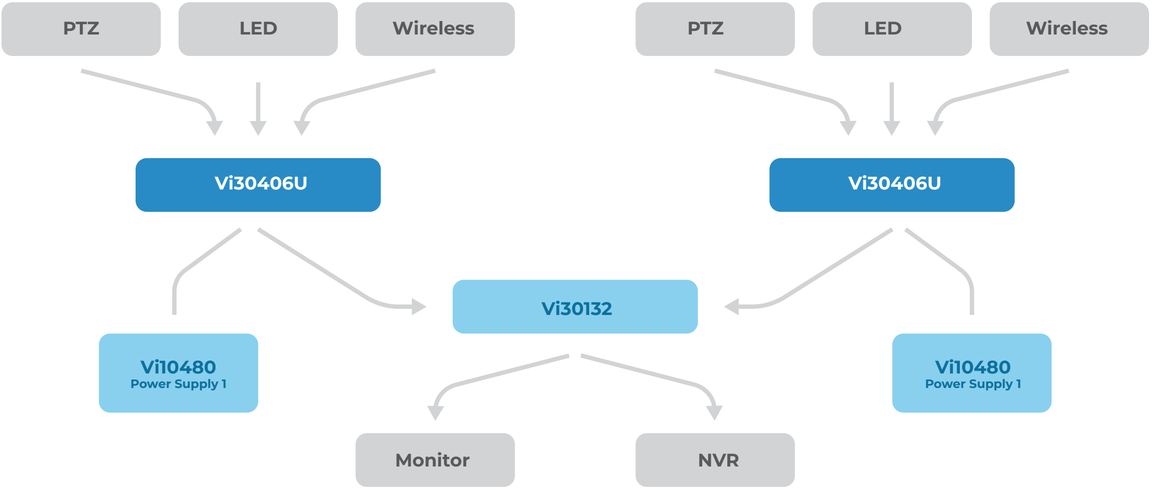
The switch is suitable for the following applications:

- Remote site applications are used in enterprise or SMB.
- Peer-to-peer application is used in two remote offices. Office network.
- High-performance requirement environment.
- Advance security for network safety applications.
- Suitable for data/voice and video conference applications.

NOTE: Fiber ports are labeled as Ports 5 and 6.

Application Examples
Network Connection between Remote Site and Central Site
Installing the Switch Application Examples

This will be replaced with actual product images.
Peer to Peer
IDF to MDF Configuration



Installing the Switch

Selecting a Site
Both switches can be mounted using DIN Rail 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.

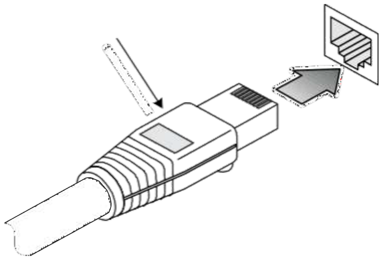
The site should:

- 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 -40°C to 70C (-40C°F to 158°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.

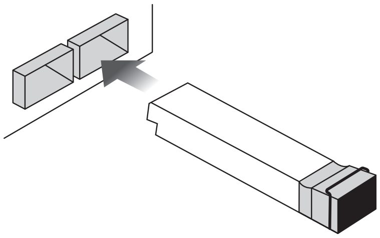
Make sure the twisted-pair Ethernet cable is always routed away from power lines, radios, transmitters, or any other electrical interference.
Make sure that Vi30406UU is connected to a separate grounded power supply that provides the necessary power for the connected cameras.
Make sure the power supply you are using provides the required power for your connected devices.

Ethernet Cabling
To ensure proper operation when installing the switch 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 5e with a maximum length of 100 meters 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.

Equipment Checklist
Rj-45 Connections



SFP Transceiver



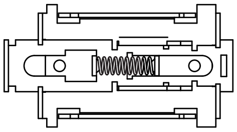
Package Contents
After unpacking the switch, please check the contents to make sure you have received all of the components. Also, make sure you have all other necessary installation equipment before beginning the installation process.

Vi30406UU GbE Management Switch
DIN Rail/Wall Adaptor

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.

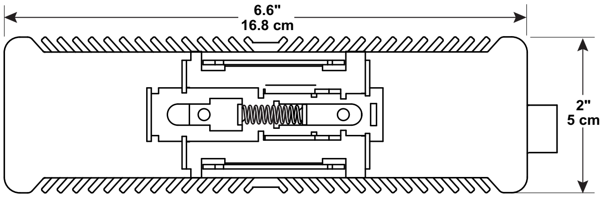
DIN Rail Mounting

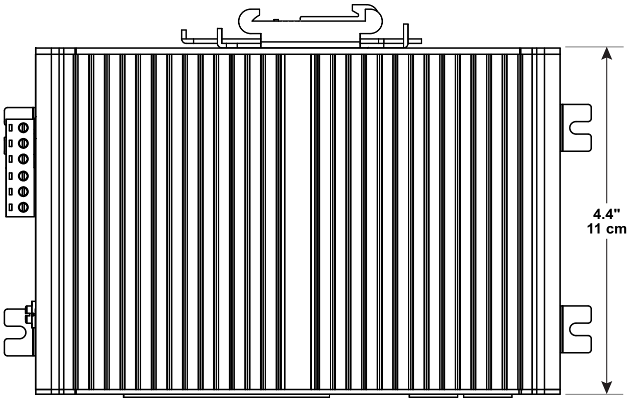


Locate the mounting holds on the rear of the cabinet.

Desktop Mounting

Insert the four tabs as shown. Secure the Vi30406UU a flat surface. DIN Rail Mounting





Installing an Optional SFP Transceiver

You can install or remove a mini-GBIC SFP from a mini-GBIC slot without having to power off the switch.

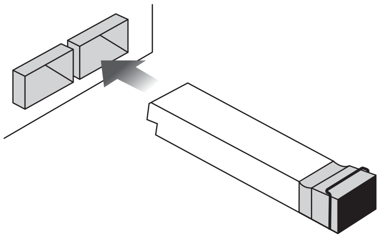
NOTE:

- The mini-GBIC slots are shared with the two 10/ 100/ 1000Base-T RJ-45 ports.
- If a mini-GBIC is installed in a slot, the associated RJ-45 port is disabled and cannot be used.
- The mini-GBIC ports operate only at full duplex.
- Half-duplex operation is not supported. Ensure the network cable is NOT connected when you install or remove a mini-GBIC.

CAUTION:

Use only supported genuine manufacture mini- GBICs with your switch. Non-manufacture mini-GBIC might have compatibility issues and may result in product malfunction. SFPs should conform to the MSA standards.

Inserting an SFP Transceiver into a Slot



SFP Slots Support the following SFPs- SFPs must match the Fiber Cable
1000Base-SX GE SFP Fiber Module, LC Multi-Mode 850nm
1000Base-SX GE SFP Fiber Module, LC Multi-Mode 1310nm 2km
1000Base-LX GE SFP Fiber Module, LC Single-Mode 10km
1000Base-LX GE SFP Fiber Module, LC Single-Mode 30km
1000Base-LX GE SFP Fiber Module, LC Single-Mode 50km
1000Base-LX GE SFP Fiber Module, LC Single-Mode 50km
1000Base-LX GE SFP Fiber Module, Bidi LC Single-Mode 10km, 1310nm
1000Base-LX GE SFP Fiber Module, Bidi LC Single-Mode 10km, 1550nm
1000Base-LX GE SFP Fiber Module, Bidi LC Single-Mode 20km, 1550nm
1000Base-LX GE SFP Fiber Module, Bidi LC Single-Mode 20km, 1310nm
100Base-FX FE SFP Fiber Module, LC Multi-Mode, 850nm
100Base-FX FE SFP Fiber Module, LC Single-Mode 20km, 1310nm
2500Base-LX SFP Fiber Module, LC – Single Mode 20Km, 1310nm
10000Base-LR SPF Fiber Module LC-Single Mode 10km 1310nm

CAUTION:

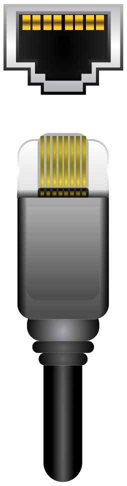
Differences in manufacturers may result in different performance and reporting statuses.

To Install an SFP Transceiver, Do the Following:
Step1: Consider the network and cabling requirements to select an appropriate SFP transceiver type.
Step2: Insert the transceiver with the optical connector facing outward and the slot connector facing down. Note that SFP transceivers are keyed so they can only be installed in one orientation.
Step3: Slide the SFP transceiver into the slot until it clicks into place.

NOTE:

- SFP transceivers are not provided in the switch package.
- **To access the switch GUI for programming and status checking connect to any UTP port.**

Connecting to UTP Port



1.8 Network Connections

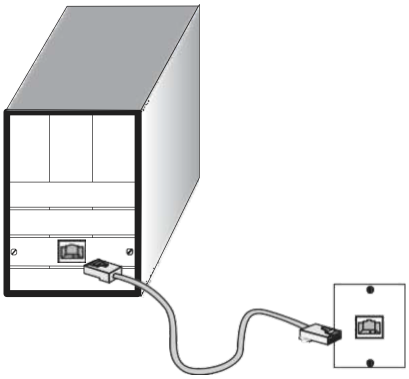
Connecting Network Devices
The switch is designed to be connected to 10, 100, or 1000Mbps network cards in PCs and servers, as well as to other switches and hubs. It may also be connected to remote devices using optional SFP transceivers.
Each device requires an unshielded twisted-pair (UTP) cable with RJ-45 connectors at both ends. Use Category 5e, or 6 cables for 100/1000/2500BASE-T connections.
Cabling Guidelines- UTP Copper Cabling
The RJ-45 ports on the switch 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 (PCs, servers, switches, routers, or hubs).

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 switch. Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Connecting to PCs, Servers, Hubs and Switches
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 switch 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 switch.

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

NOTE:
Only CAT 5e,6,6a, cables should be used. SFP must be MSA compactible and selected with regards to the proper fiber cable.

Step 3: The **Orange and Green** LED notes both link and activity. When the link is 10M / 1G the Green LED will be shown.

Network Wiring Connections

Today, the punch-down block is an integral part of many of the newer equipment racks. It is part of the patch panel. Instructions for making connections in the wiring closet with this type of equipment are as follows.

Step 1: Attach one end of a patch cable to an available port on the switch, and the other end to the patch panel.

Step 2: If it's not already in place, attach one end of a cable segment to the back of the patch panel where the punch-down block is located and the other end to a modular wall outlet.

Step 3: Label the cables to simplify future troubleshooting. See **"Cable Labeling and Connection Records"** on page 29.

Making Fiber Port Connections

An optional Gigabit SFP transceiver can be used as a backbone connection between switches, or as a connection to a high-speed server.

Each single-mode fiber port requires 9/125 micron single-mode fiber optic cable with an LC connector at both ends. Each multimode fiber optic port requires 50/125- or 62.5/125-micron multimode fiber optic cabling with an LC connector at both ends.

WARNING: This switch uses lasers to transmit signals over a fiber optic cable. The lasers are inherently eye-safe in normal operation. However, the user should never look directly at a transmit port when it is powered on.

WARNING: Considering safety, when selecting a fiber SFP device, please make sure that it can function at a temperature that is not less than the recommended maximum operating temperature of the product. You must also use an approved laser SFP transceiver.

Step 1: Remove and keep the LC port's rubber plug. When it's not connected to a fiber cable, the rubber plug
should be replaced to protect the optics.

Step 2: Check that the fiber terminators are clean. You can clean the cable plugs by wiping them gently with a clean tissue or cotton ball moistened with a little ethanol. Dirty fiber terminators on fiber optic cables will impair the quality of the light transmitted through the cable and lead to degraded performance on the port.

Step 3: Connect one end of the cable to the LC port on the switch and the other end to the LC port on the other device. Since LC connectors are keyed, the cable can be attached in only one orientation.

Step 4: As a connection is made, check the Link LED on the switch corresponding to the port to be sure that the connection is valid.

The fiber optic ports operate at 1G/2.5/10 Gbps. The maximum length for fiber optic cable operating at Gigabit speed will depend on the fiber type as listed under "Gigabit Ethernet Collision Domain" on page xx.

Connectivity Rules

1000/2500Base-T Cable Requirements

When adding hubs to your network, please note that because switches break up the path for connected devices into separate collision domains, you should not include the switch or connected cabling in your calculations for cascade length involving other devices.

All Category 5e and above UTP cables that are used for 100BASE-TX connections should also work for 1000/25000BASE-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 5e 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 5e or 6/6a 100-ohm UTP or STP	100.m (328 ft)	RJ-45

Fiber Size	Fiber Bandwidth	Maximum Cable Length	Connector
62.5/125-micron	160 MHz/km	220 m (722 ft)	LC
multimode fiber	200 MHz/km	275 m (902 ft)	LC
50/125-micron	400 MHz/km	500 m (1641 ft)	LC
multimode fiber	500 MHz/km	550 m (1805 ft)	LC

Table 6: Maximum 1000BASE-SX Gigabit Fiber Cable Lengths

Fiber Size	Fiber Bandwidth	Maximum Cable Length	Connector
9/125 micron single-	N/A	10km (6.2 miles)	LC
mode fiber 1310nm			
9/125 micron single-	N/A	30km (18.64 miles)	LC
mode fiber 1550nm		50km (31.06 miles)	LC

Maximum 1000BASE-LX/LHX/XD/ZX Gigabit Fiber Cable Length

Fiber Size	Fiber Bandwidth	Maximum Cable Length	Connector
Single-mode TX-	N/A	20km (12.42miles)	BIDI
1310nm RX-1550nm			LC
Single-mode TX-	N/A	20km (12.42miles)	BIDI
1550nm RX-1310nm			LC

Maximum 1000BASE-LX Single Fiber Gigabit Fiber Cable Length

100 Mbps Fast Ethernet Collision Domain

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

Maximum Fast Ethernet Cable Lengths

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 switch 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.

1.9 Troubleshooting

Basic Troubleshooting Tips

Most problems are caused by the following situations. Check for these items first when starting your troubleshooting:
Connecting to devices that have a fixed full-duplex configuration.
The RJ-45 ports are configured as "Auto". When connecting to the attached devices, the switch will operate in one of two ways to determine the link speed and the communication mode (half-duplex or full duplex):

- If the connected device is also configured to "Auto", the switch 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 switch will automatically sense the link speed but will default to a communication mode of half-duplex.
- Because Vi30406UU behaves in this way (in compliance with the IEEE802.3 standard), if a device connected to the switch has a fixed configuration at full duplex, the device will not connect correctly to the switch. The result will be high error rates and very inefficient communication between the switch and the device.
- Make sure all devices connected to the Vi30406UU are configured to auto-negotiate or are configured to connect at half-duplex (e.g. all hubs are configured this way).
- 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 5/6 cable tester is a recommended tool for every 100Base- TX and 1000/2500Base-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. A port on your switch may not be operating as you expect because it has been put into a "blocking" state by the settings or connection.

Important note:
If the Vi30406UU's IP address needs to be restored to the default address, username and password you must use the front panel reset button. When doing so please note the other programing: Auto checking settings will have to be reprogrammed

Basic Troubleshooting Chart

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

If the power indicator does not turn on when the connected to the power source, you may have a problem with the power outlet, power cord, or 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 switch from anywhere within the attached network using a web browser. However, you must first configure the switch 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 switch has not been disabled. If it has not been disabled, then check the network cabling that runs between your remote location and the switch.

IP Address:
To access the Vi30406UU’s GUI, your connected computer must be on the same network as the switch. 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 (1).

1.10 Saving Programming

Power and Cooling Problems

Installation
The Vi30406UU can operate at high temperatures ranging from -40C to 70C. 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. It is recommended these settings do not exceed 70 C.

After confirming individual settings, the switch will automatically save those settings. In the event of power loss, these settings will be saved including the programmed IP Address. If Power loss happens, all setting will be restored as programmed when power is restored.

1.11 Watch Dog Timer

The Vi30208U contains a watchdog timer which is always active. It will sense the system condition every 15 seconds. The watchdog senses input power and in the event of power loss will reboot the switch once power is restored.

1.12 Cabling

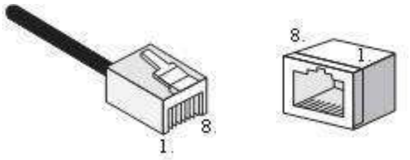
Twisted-Pair Cable and Pin Assignment

For 100/1000/2500BASE-TX connections, the twisted-pair cable must have two pairs of wires. For 1000/2500BASE-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.



The **Figure 19: RJ-45 Connector Pin Numbers**

100BASE-T/1000/2500Base-Tx 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 switch 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 switches 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 switch, 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

IP Address:
The “+” and “-” signs represent the polarity of the wires that make up each wire pair.

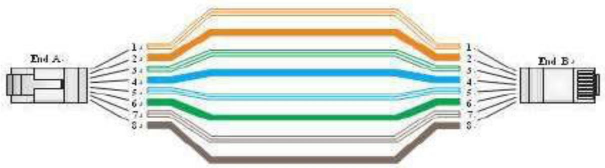
EIA/TIA 568B RJ-45 Wiring Standard

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 switch, 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 switch, 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

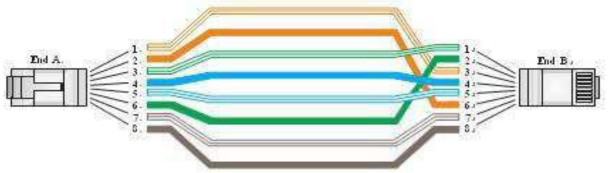


Figure 21: Crossover Wiring
1000/2500Base-T Pin Assignments

If your existing Category 5 installation does not meet one of the test parameters for 1000/2500Base-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.

1000/2500BASE-T MDI and MDI-X Port Pin-Out

All 1000/2500BASE-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 switches or hubs.
The table below shows the 1000/2500BASE-T MDI and MDI-X port pin outs. These ports require that all four pairs of wires be connected. Note that for 1000BASE-T operation, all four pairs of wires are used for both transmitting and receiving.
Use 100-ohm Category 5e, or 6/6a unshielded twisted-pair (UTP) or shielded twisted- pair (STP) cable for 1000BASE- 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:
When testing your cable installation, be sure to include all patch cables between switches and end devices.

Fiber Standards
Important Note: Fiber SFPs have no standards regarding interface with network switches with the exception of the Multi standard Agreement (MSA) with is limited to the physical interface between the SFP and a switch port. Data transmission may require adjusting port bandwidth settings on your switch.

When installing SFP matches certain the SFP matches the installed fiber and are the same on both ends of the cable
The International Telecommunication Union (ITU-T) has standardized various fiber types for data networks. These are summarized in the following table.

Fiber Standards

ITU-T Standard	Description	Application
G.651	Multimode Fiber 50/125-micron core	Short-reach connections in the 1300- nm or 850-nm band.
G.652	Non-Dispersion-Shifted Fiber Single-mode, 9/125- micron core	Longer spans and extended reach. Optimized for operation in the 1310- nm band, but can also be used in the 1550-nm band.
G.652.C	Low Water Peak Non- Dispersion- Shifted Fiber Single-mode, 9/125- micron core	Longer spans and extended reach. Optimized for wavelength-division multiplexing (WDM) transmission across wavelengths from 1285 to 1625 nm. The zero-dispersion wavelength is in the 1310-nm region.
G.653	Dispersion-Shifted Fiber Single-mode, 9/125- micron core	Longer spans and extended reach. Optimized for operation in the region from 1500 to 1600- nm.
G.654	1550-nm Loss- Minimized Fiber Single-mode, 9/125- micron core	Extended long-haul applications. Optimized for high-power transmission in 1500 to 1600-nm region, with low loss in the 1550-nm band.
G.655	Non-Zero Dispersion- Shifted Fiber Single-mode, 9/125- micron core	Extended long-haul applications. Optimized for high-power dense wavelength-division multiplexing (DWDM) operation in the region from 1500 to 1600-nm.

1.13 Product specifications

Specifications Vi30406U/Vi30410

Ports	2 1000/2500010000Mbps SFP ports 4 GbE (100/1000,2500Mbps) UTP Ports-Vi30406U
Network Interface	Ports 1-4: RJ-45 Connector-Vi30406U 100BASE-T to 2500Base-T: RJ-45 (100-ohm, UTP cable; Category 5e or better) (100-ohm, UTP or STP cable; Category 5, 5e or 6) *Maximum Cable Length - 100 m (328 ft) Ports 5/6 Vi30406U SFP Fiber MSA Compatible 1G/2.5G/10G
Switching Database LEDs	POWER TP Port: status (LINK/ACT), 10/100/1000M/2500M SFP Port: status (LINK/ACT/SPD), 100/1000M/2500
Weight	1.03 lb (470g)
Size	1.8 x 4.8 x 2 in (4.5 x 122 x 10.6cm (HXW/xL)
Temperature	Operating: -40°C to 70°C (-40°F to 158°F)
Humidity	Operating: 5% to 90% (non-condensing)
Power Input	Not to exceed 480 watts 57VDC
Power Supply	External DC Input
Switch Fabric	Vi30406UU 65Gbps
Power Consumption	4W (standby)
Jambo Frame	10K
In-Band Management	Via GUI
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-Tx Ethernet (Twisted – pair copper IEEE 802.3z=> 1G Fiber IEEE 803.3bz => 2.5G/10G fiber IEEE 802.3x => Flow Control Capability ANSI/IEEE 802.3 => Auto-negotiation
Emissions	IEEE 802.3at/af/bt => Power Over Ethernet (PoE)
Immunity	EN55022 (CISPR 22) Class A EN 61000-3 FCC Class A CE Mark
Compliances Standards	EN 61000-4-2/3/4/5/6/8/11 EN 55024

1.14 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 5, 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 data transmission along the cable.
Collision Domain	Single CSMA/CD LAN segment.
CSMA/CD	CSMA/CD (Carrier Sense Multiple Access/Collision Detect) is the communication method employed by Ethernet, Fast Ethernet, and Gigabit Ethernet.
End Station	A workstation, server, or other device that does not forward traffic.
Ethernet	A network communication system developed and standardized by DEC, Intel, and Xerox used 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 1000-10000 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), PoE++ IEEE 802.3at (Class 4 PDs limited to 30W). – Class 5-8 to 90W
Lan Segment	Separate LAN or collision domain.
LED	Light emitting diode is used for monitoring a device or network condition.
Local Area Network (LAN)	A group of interconnected computer and support devices.
Media Access Control (MAC)	A portion of the networking protocol that governs access to the transmission medium, facilitating the exchange of data between network nodes.

MIB	An acronym for Management Information Base. It is a set of database objects that contain information about the device.
Modal Bandwidth	Bandwidth for multimode fiber is referred to as modal bandwidth because it varies with the modal field (or core diameter) of the fiber. Modal bandwidth is specified in units of MHz per km, which indicates the amount of bandwidth supported by the fiber for a one km distance.
Network Diameter	Wire distance between two end stations in the same collision domain.
RJ-45 Connector	A connector for twisted-pair wiring.
Switched Ports	Ports that are on separate collision domains or LAN segments.

1.15 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 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 transferable. 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. Repairs 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 damage, including damage 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.

1.16 Contact Information

Vigitron, Inc.

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

Section 2: Accessing and Controlling the Vi30406UU

2.1 Accessing the Switch GUI

After programming a function use the UPDATE button to apply the programming changes

1. After applying programming changes REFRESH the screen to confirm the changes.
2. To see status changes press the REFRESH button

Accessing the Switch GUI
Network and Non- Network Secure Operations:

For Secure Operations
In some cases, the installation may require the switch not to be accessed to avoid hacking. In this case program the switch 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 switch will require connecting a laptop to the network port Without a network connection Syslog message will **not be able to be recovered**

For Network Operations
Connect a network connection to any UTP (RJ45) or Fiber port. Using the default address 192.168.1.200 and username: admin, password: system access the switch. It is recommended you change the Username and Password.
When connected to a network the unit will transmit Syslog messages on port 514.

2.2 Using a Web Browser

Defining Network Operating Problems and Solutions

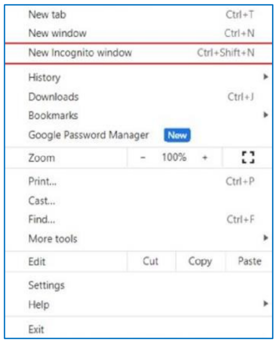
> Web browsers
Do not use web browser standard modes
Standard modes maintain Browser History/Cookies/ and Temporary Internet Files. All of these can prevent you from access your network web-based devices, naming switches
Accessing you Browser's Private Mode

Method one: Keyboard

Browser	**Mouse**	**Keyboard**
Chrome	Settings (top right) & New Incognito Window	Ctrl + Shift + N
Edge	Settings (top right) > New InPrivate Window	Ctri + Shift + P
Firefox	Settings (top right) > New Private Window	Ctrl + Shift + P
Brave	Settings (top right) > New Incognito Window	Ctrl + Shift 35 N
Safari	Settings (top right) > Private mode	Shift + Command + N

The following Example is Google:

Method Two:



The switch 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 Switch's GUI may be blocked. It is suggested that in accessing the switch's GUI use the browser's private mode

2.3 Accessing the Switch by Web

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

Ensure it coincides with the following requirements while accessing the switch by Web browser.

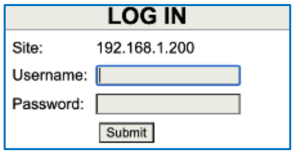
- HTML Version 4.0
- HTTP Version 1.1
- JavaScript™ Version 1.5

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

First time access to switch, you don’t need additional configuration but access to switch directly by WEB if this is 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 Vi30210U. The subnet mask is “255.255.255.0”.

Open the WEB browser, enter the “(192.168.1. xxx” in the address bar, note that 192.168.1.200 is the defaulted IP
address of switch.

The dialog appeared 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.



LOG IN

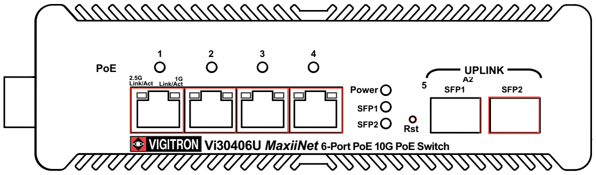
Site: 192.168.1.200

Username:

Password:

WEB Authentication Dialog.

Default username: admin
Default password: system
Reset key – default function:



Steps for Resetting the Vi30406UU

The browser will display the system information page if it’s authenticated successfully.
After Reset is complete, recheck your programming as some setting may need to be reprogrammed.
After Reset is complete, recheck your programming as some setting may need to be reprogrammed.

2.4 GUI 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.

2.5 Updating and programming saved functions

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 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.

Section 3: Web Configuration

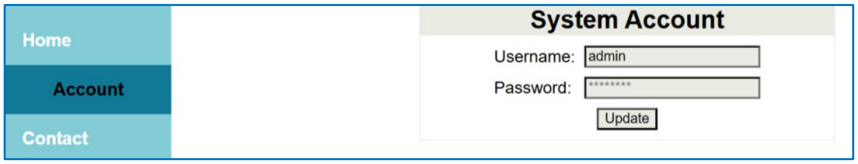
3.1 Accessing Using Defaults

Accessing the Switches by Web Browser.

Important Note: Your choice of Internet browser can affect your ability to access switch and/or certain switch functions. If you experience these problems, please check the browser security settings.
Ensure it is coincident with the following requirements while accessing the switch 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 access to the switch, and the computer is connecting to the network of a switch.
First time access to switch, you don't need additional configuration but access to the switch 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 Vi30406UU. 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 switch. 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.



System Account

Username: admin
Password: ********

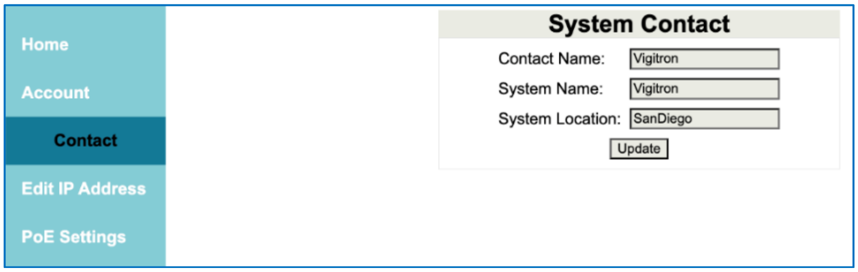
Web Authentication Dialog

3.2 Adding Contact information

Program System Contact Information.

Program the:
- Contact name
- System name
- System Location

Select Update

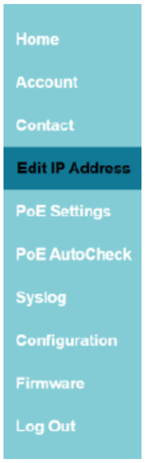


System Contact

Contact Name: Vigitron
System Name: Vigitron
System Location: SanDiego

The Maximum input character is 14 characters.
The **Contact Name**, **System Name**, and **System Location** fields accept only letters (A–Z or a–z), digits (0–9), and the underscore (_).
Spaces are not allowed

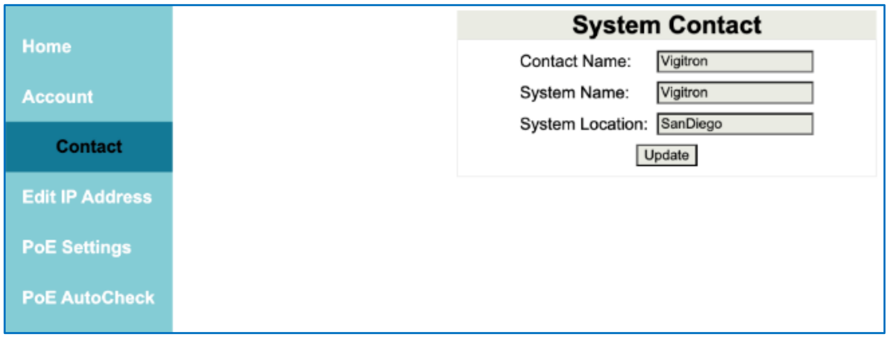
3.3 Operating the program menu



First time access to switch, you don’t need additional configuration but access to the switch directly by using the web browser. If this is 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 Vi30406UU. The subnet mask is “255.255.255.0”.

3.4 Logging Out.

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

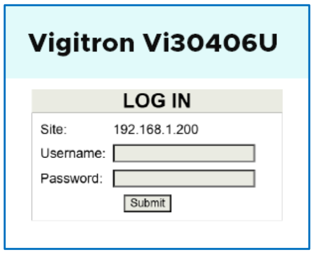


System Contact

Contact Name: Vigitron
System Name: Vigitron
System Location: SanDiego

Section 4: Operator Programming

4.1 Logging in



Vigitron Vi30406U

LOG IN

Site: 192.168.1.200

Username:

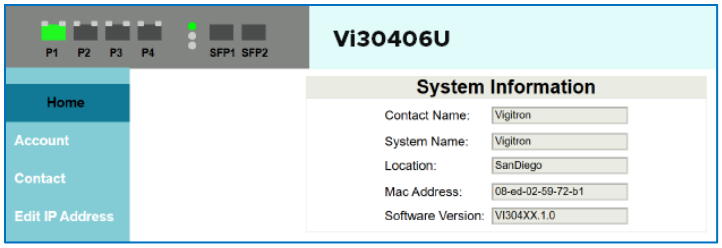
Password:

Vigitron Login in page for Vi30406UU
Username input and Password input.

Default username is admin, and default password is system
If the Username and password have been previously changed, you must use the last one.

Press submit will log into the Vi30406UU GUI Home Page.

4.2 System Information



Vi30406U

System Information

Contact Name: Vigitron

System Name: Vigitron

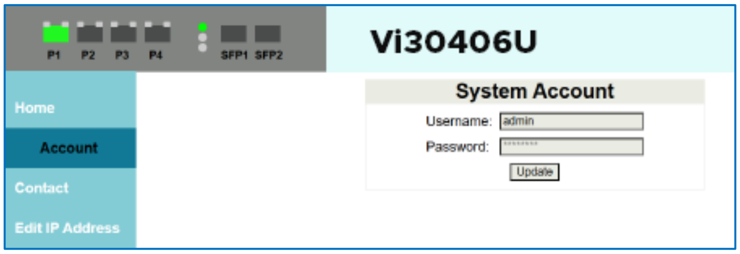
Location: SanDiego

Mac Address: 08-ed-02-59-72-b1

Software Version: VI304XX.1.0

Homepage contains System information, including user defined System contact name, system name, location, Mac address, and Current Software Version.

4.3 System Account



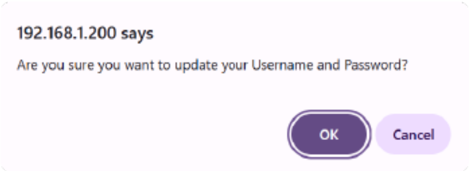
Vi30406U

System Account

Username: admin

Password: ********

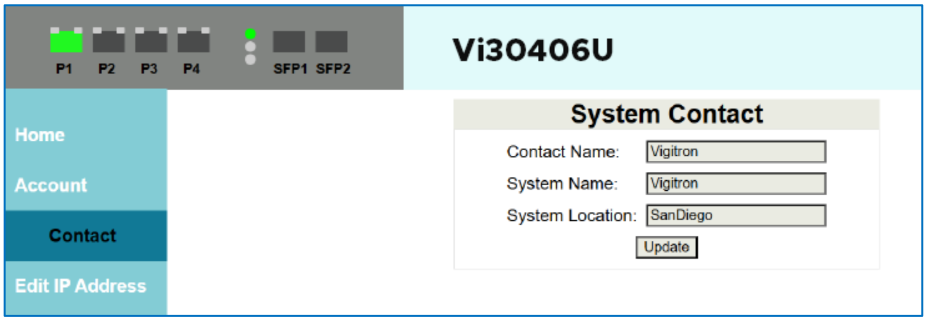
The system Account page is where the user can update the username and password for this Vi30406UU device.
Enter new username or Password, then press Update
GUI will send messages to ensure if the user wants to make change on the username and password.



192.168.1.200 says

Are you sure you want to update your Username and Password?

4.4 System Contact



Vi30406U

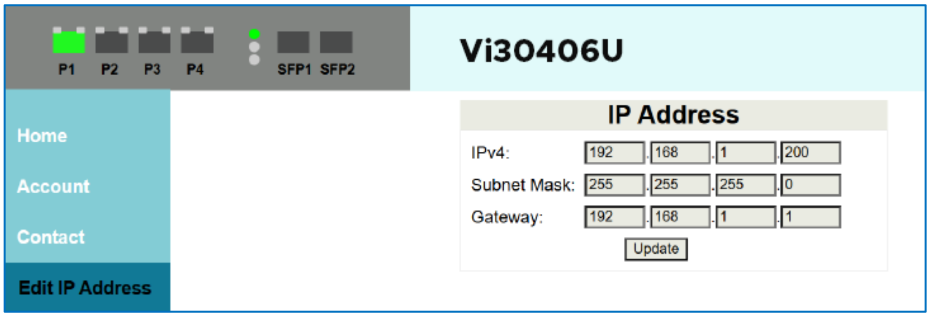
System Contact

Contact Name: Vigitron
System Name: Vigitron
System Location: SanDiego

The system Contact page is where the user can update the System contact name, system name, location for this Vi30406UU device.
Enter new System contact name, system name, location, then press Update
The updated information will appear in the Account Screen

The Maximum input character is 14 characters.
The **Contact Name**, **System Name**, and **System Location** fields accept only letters (A–Z or a–z), digits (0–9), and the underscore (_).
Spaces are not allowed

4.5 Programming the IP Address



Vi30406U

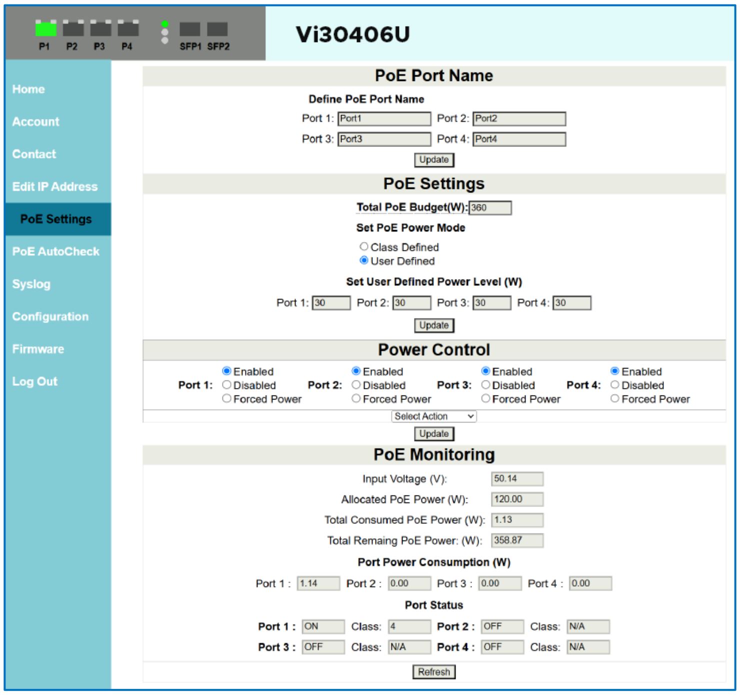
IP Address

IPv4: 192 . 168 . 1 . 200
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 192 . 168 . 1 . 1

The system IP Address page is where the user can update the System IP Address for this Vi30406U device.

Users can enter new desired IP address, Subnet, and Gateway for this Vi30406U, then press Update to update IP Address setting of the Vi30406UU.
After and pressing upgrade. the previous connection to the switch will be lost. The connecting device, laptop must be reset to the same network as the switch to access the Vi3046U.

4.6 PoE Port Name



PoE Port Name

Define PoE Port Name

Port 1: Port1 Port 2: Port2
Port 3: Port3 Port 4: Port4

PoE Settings

Total PoE Budget(W): 360

Set PoE Power Mode

○ Class Defined
● User Defined

Set User Defined Power Level (W)

Port 1: 30 Port 2: 30 Port 3: 30 Port 4: 30

Power Control

Port 1: ● Enabled ○ Disabled ○ Forced Power
Port 2: ● Enabled ○ Disabled ○ Forced Power
Port 3: ● Enabled ○ Disabled ○ Forced Power
Port 4: ● Enabled ○ Disabled ○ Forced Power

PoE Monitoring

Input Voltage (V): 50.14
Allocated PoE Power (W): 120.00
Total Consumed PoE Power (W): 1.13
Total Remaing PoE Power: (W): 358.87

Port Power Consumption (W)

Port 1 : 1.14 Port 2 : 0.00 Port 3 : 0.00 Port 4 : 0.00

Port Status

Port 1 : ON Class: 4 Port 2 : OFF Class: N/A
Port 3 : OFF Class: N/A Port 4 : OFF Class: N/A

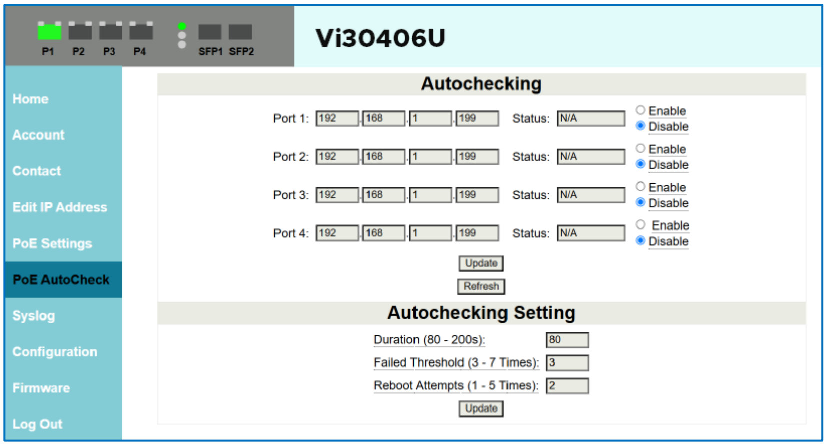
This page contains 4 sections: PoE Port Name, PoE Settings, Power Control, PoE Monitoring

PoE Port Name: sets up PoE Port Names. Port naming is important in identifying the ports in both the GUI and Syslog messaging
PoE Settings: sets up total PoE Budget, PoE Mode, and Power level for each port.

Power Control: can Switch On / OFF (using Enable, Disable, or Forced Power) for each PoE port on this Vi30406U device.
PoE Monitoring monitors all the Power consumption, and status of each port on this Vi30406U.

Press the Refresh to confirm the setting you entered. The port status will show if the settings are correct by indicating if the port is in the On or OFF stage. If the ports show off recheck your settings

4.7 Auto-checking



Autochecking

Port 1: 192 . 168 . 1 . 199 Status: N/A ○ Enable ● Disable
Port 2: 192 . 168 . 1 . 199 Status: N/A ○ Enable ● Disable
Port 3: 192 . 168 . 1 . 199 Status: N/A ○ Enable ● Disable
Port 4: 192 . 168 . 1 . 199 Status: N/A ○ Enable ● Disable

Autochecking Setting

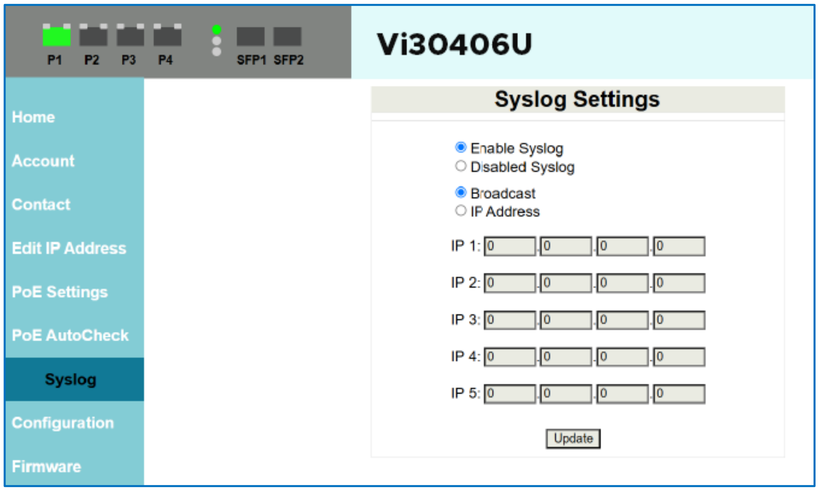
Duration (80 - 200s): 80
Failed Threshold (3 - 7 Times): 3
Reboot Attempts (1 - 5 Times): 2

This page will set up the Auto Checking ability on the Vi30406U (Port 1 – Port 4), based on the setting, system will ping to each enabled port automatically to check if the Port can be linked, if the port fails to response for specified attempts, the Vi30406U will automatically try to reboot the PoE Port.
After entering the IP address of the current device, enable the function and when programming is complete update and refresh.

Status will show if the entered IP address is current. If N/A appears recheck the IP address.
This page also shows status of the Auto-checking for each port.

White auto-checking is in process the Green Power light will flash. When complete it will return to the steady on state   -- NOT RIGHT, Power LED will not flash, when auto-checking in process, the only thing change is the Status output will become from “N/A” to “Checking”

4.8 Syslog



Syslog Settings

● Enable Syslog
○ Disabled Syslog

● Broadcast
○ IP Address

IP 1: 0 . 0 . 0 . 0
IP 2: 0 . 0 . 0 . 0
IP 3: 0 . 0 . 0 . 0
IP 4: 0 . 0 . 0 . 0
IP 5: 0 . 0 . 0 . 0

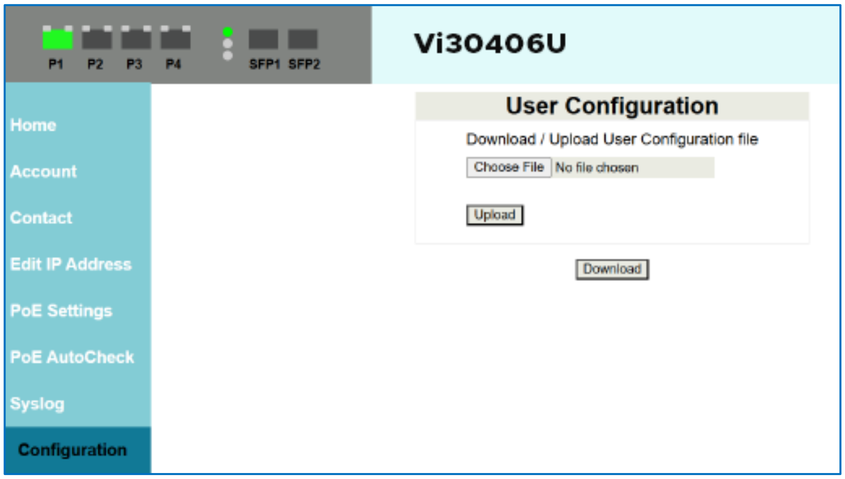
This page enables users to enable or disable the Syslog function.

When enabled, system will send Syslog message when specific event occurs.

Syslog transmits on port 514. The receiving device must be able to receive Syslog messages and display them. This requires the receiving device have the required software such as Vigitron’s SysCap™- see addendum.

Syslog messages can be programmed as “broadcast” allowing reception on any network device that can receive Syslog or up to 5 individual connected devices by programming their individual IP addresses

4.9 User Configuration



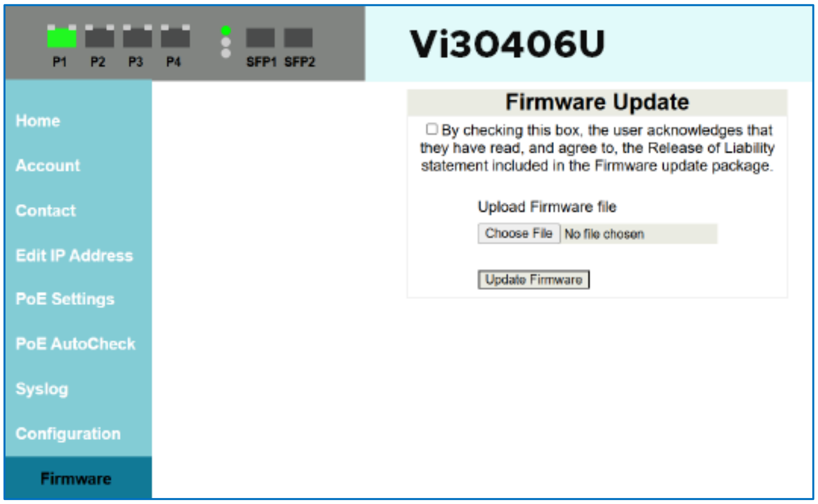
User Configuration

Download / Upload User Configuration file

No file chosen

Users can use this page to download or upload their setting for the Vi30406U.
The operator can save programming and either download from and switch or once downloaded uploaded to another switch.
Be aware: Downloaded programming also includes a switch’s IP address. If programming is uploaded from a switch, make certain the IP address is changed prior to integrating it into a network

4.10 User Configuration



□ By checking this box, the user acknowledges that they have read, and agree to, the Release of Liability statement included in the Firmware update package.

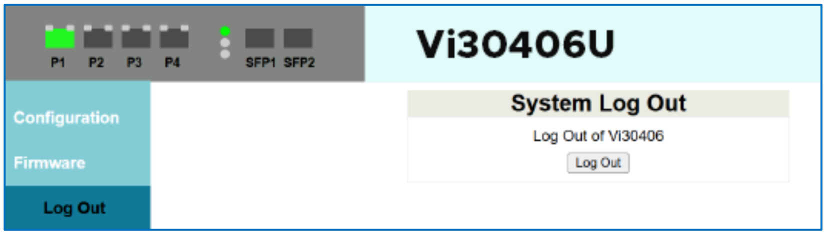
Upload Firmware file

This page is used to update firmware for the Switch.
Vigitron or notify you or you can ask if any firmware upgrades.
Prior to upgrading, make certain the new firmware on the computer connected to the switch
To upgrade firmware:

1. Select the “Update Firmware” button
2. The screen will open to computer’s hone page
3. Select the location where the new firmware is located and select it.
4. Press Enter to update.

The GUI will send Prompt message to confirm if user wants to update firmware, once confirmed, Power LED (on front panel) will start to flash. When Firmware update is complete, Flash LED will be Combe steady, User will require to refresh the GUI page to re-enter the GUI.

4.11 System Log Out



Log Out of Vi30406

Press the “log out” button
To access the switch a log in will be required

Section 5: Addendums

5.1 Syslog Messages

Addendum A: Syslog Messages

All **Syslog messaging** includes 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.
11. sysname at syslocation (192:168:1:200): System Watchdog Restart.

To receive Syslog messages:

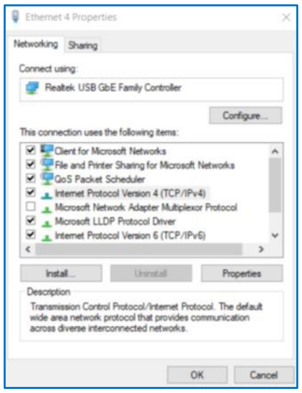
The client computer must be on the same network as the address
Port 514 must be open (it usually will not require any additional settings) Your client must have the ability to receive and decode Syslog messages.
Vigitron provides free Syslog capture software called SysCapTM. The software can receive messages from multiple switchs 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.

5.2 Trouble Shooting

Addendum B: Troubleshooting

Switch cannot be accessed
Your switch 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 switch. As the switch default address is: 192.168.1.200
Your client address needs to be: 192.168.1.XXX (any number other than 200)

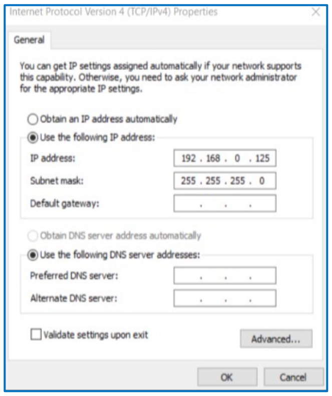

Ethernet 4 Properties

Connect using:
Realtek USB GbE Family Controller

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.


Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

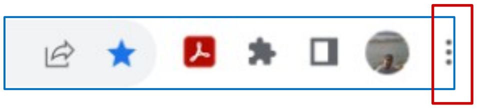
IP address: 192 . 168 . 0 . 125
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

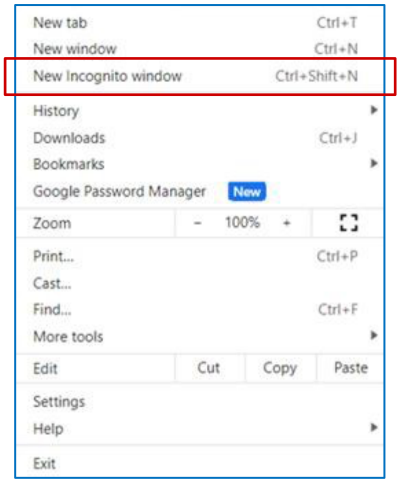
○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

☐ Validate settings upon exit

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

5.4 Default Setting

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 – Port6 (Vi30406U)- Port 1-10 (Vi40410)
- Total PoE Budget: 730
- PoE Power Mode: Class Defined
- Defined Power Level: 0W
- 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

5.4 Syslog Messages

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 Switch connected to the network?

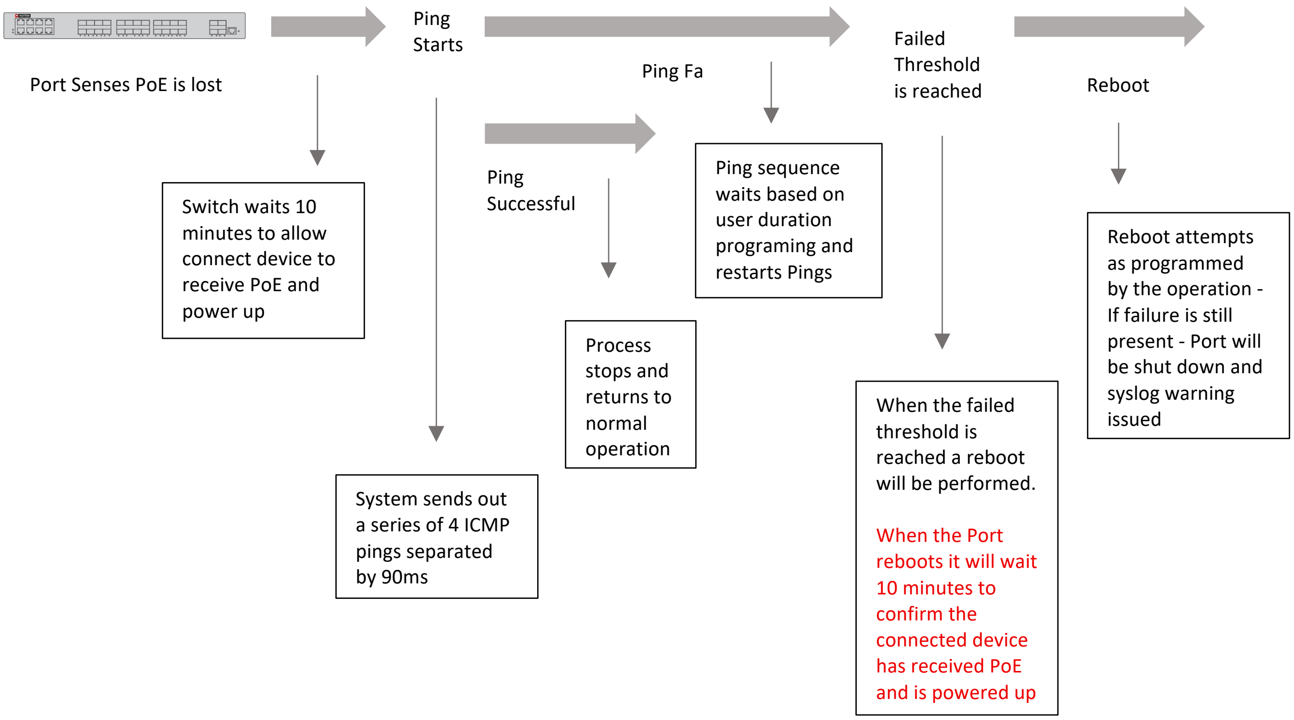
Start by: Confirming you are properly addressed. Is the client on the same network as the Switch?

Check Cables.

Method 1: Look at the unit's front panel RJ45 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?



Port Senses PoE is lost

Switch waits 10 minutes to allow connect device to receive PoE and power up

Ping Starts

System sends out a series of 4 ICMP pings separated by 90ms

Ping Successful

Process stops and returns to normal operation

Ping Fa

Ping sequence waits based on user duration programing and restarts Pings

Failed Threshold is reached

When the failed threshold is reached a reboot will be performed.

When the Port reboots it will wait 10 minutes to confirm the connected device has received PoE and is powered up

Reboot

Reboot attempts as programmed by the operation - If failure is still present - Port will be shut down and syslog warning issued

Important Note:

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

5.5 Definitions

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 various situations. 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 using the service. ACL can generally be configured to control inbound traffic, and in this context, they are like 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 can 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 into 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 connections, 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 is 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 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 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 generates 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 like 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 more than 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 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 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 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 original 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 remove 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 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. 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 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 SyncE this is the Quality Level of a given clock source. This is received on a port in an 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 a 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 obsolete 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 allows diverse network objects to participate in network management architecture. It enables network management systems to learn about 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 contains 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 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 transferring 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 is 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 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 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.