MaxiiNet™ Vi32226
Operational Manual

Vi32226

Release F32226V1.051

© 2019 Vigitron, Inc. All rights reserved. All brand and product names are trademarks or registered trademarks of their respective companies.

Section 1: About This Manual

1.0 Copyright

Copyright © 2019 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 any means by electronic or mechanical. This 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.

1.1 Purpose

This Manual gives specific information on how to operate and use the management functions of the Vi32226.

1.2 Audience

The Manual 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 (IP), and Simple Network Management Protocol (SNMP).

1.3 Conventions

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

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

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

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

1.4 Warranty

See the Customer Support/Warranty booklet included with the product. A copy of the specific warranty terms applicable to your manufacture products and replacement parts can be obtained from Vigitron, Inc.

1.5 Disclaimer

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

Section 2: Compliances and Safety Statements

2.0 FCC Class A

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 interference in which case, the user will be required to correct the interference at the user's own expense.

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 RJ45 connections – Category 3 or better for 10 Mbps connections, Category 5 or better for 100 Mbps connections, Category 5, 5e, or 6 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.

Coax cables should standard RG59 with resistance values near or close to 22K ohms. Aluminum shielded cable cannot be used.

2.1 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.

Coax cables should standard RG59 with resistance values near or close to 22K ohms. Aluminum shielded cable cannot be used.

2.2 CE Mark Warning

This is a Class A device. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

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

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.

2.4 UL Mark

Ul 60950-1 Information Technology Equipment - Safety - Part 1: General Requirements - Edition 2 - Revision Date 2014/05/13

2.5 EMC

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 using outdoor device connect to this device with cable, then you need to add an arrester on the cable between outdoor device and this device.

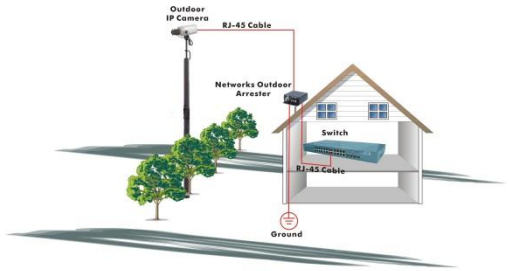


Fig. Addition arrester between outdoor device and this switch

The Vi32226 supports SFP conforming to MSA standards, although differences between manufacturers can affect performance. For best results, use Vigitron SFPS.

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

WARNING:

- Self-demolition on product is strictly prohibited. Damage caused by self-demolition will be charged for repairing fees.
- Do not place product outdoors or during sandstorm.
- Before installation, please make sure that input power supply and product specifications are compatible to each other.
- To reduce the risk of electric shock, disconnect all AC or DC power cord and RPS cables to completely remove power from the unit.
- Before importing/exporting configuration, please make sure the firmware version is always the same.
- After firmware upgrade, the switch will remove the configuration automatically to latest firmware version.

2.6 Related Publications

The following publication gives specific information on how to operate and use the management functions of the switch.

2.7 Revision History

The User's Manual

This section summarizes the changes in each revision of this guide.

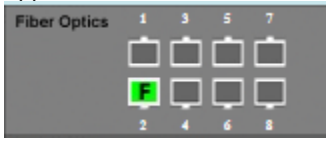
Release	Date	Revision
F32226V1.051		

Updating several functions may require rebooting the switch. Rebooting may take up to several minutes to re-establish a connection from the host to the switch. It is suggested that when rebooting, you exit your browser and enter. Also, if you are using your host for other web access, you periodically clear the browser memory.

1. Ports 24 and 25 are combined ports for either copper (UTP) or fiber connections. If either port is used, both that port and its associated port will show as green indicating they are both in use and prevent connections to both ports.

2. Extended port versions is shown as "E" in both the switch icon and Port Configuration manuals. This indicates they must be connected to an associated extender to operate. The icon itself will not change. However, operation can be verified by viewing several of the monitoring screens such as Port Counter and PoE Settings.

Applies to versions with extended distance ports



Applies to models with fiber port 1-16

Note: When extended "E" ports are linked, they will be displayed as pictured. When activity is present, they will turn Green and flash.

Contents

Section 1: About This Manual 2
1.0 Copyright 2
1.1 Purpose 2
1.2 Audience 2
1.3 Conventions 2
1.4 Warranty 2
1.5 Disclaimer 3
Section 2: Compliances and Safety Statements 4
2.0 FCC Class A 4
2.1 FCC Caution 4
2.2 CE Mark Warning 4
2.3 CE Declaration of Conformance for EMI and Safety (EEC) 5
2.4 UL Mark 5
2.5 EMC 5
2.6 Related Publications 7
2.7 Revision History 7
Section 3: Introduction 15
3.0 Overview 15
3.1 Cabling Guidelines 16
3.2 Connecting to PCs, Servers, Hubs and Switches 16
3.3 Network Wiring Connection 17
3.4 Vi32226 – Front View 18
3.5 Vi32226 – Rear View 18
Section 4: Description of Hardware 19
4.0 1000Base-T Ports 19
4.1 SFP Transceivers Slots 19
4.2 Ports and System Status LEDs 20
4.3 Console Port 20
Section 5: Installing the Switch 21
5.0 Selecting a Site 21
5.1 Ethernet Cabling 21
5.2 Equipment Checklist 22
5.3 Package Contents 22
5.4 Mounting 22
5.5 Rack Mounting 22

5.6 To Rack-Mount Devices....23
5.7 Installing an Optional SFP Transceiver....23
5.8 Installing an SFP Transceiver....24
5.9 Connecting to a Power Source....24
Section 6: Making Network Connections....25
6.0 Connecting to a Network Devices....25
6.1 Twisted-Pair Devices....25
6.2 Cabling Guidelines....25
6.3 Connecting to PCs, Servers, Hubs and Switches....25
6.4 Network Wiring Connections....26
Section 7: Troubleshooting....27
7.0 Basic Troubleshooting Tips....27
7.1 Table 10: Troubleshooting Chart....28
Section 8: Operation of Web-Based Management....29
8.0 Initial Configuration....29
Section 9: Administration....31
9.0 Prior to Logging On....31
9.1 Logging On....31
9.2 System IP Configuration....33
9.3 System Status....34
9.4 Load Default....35
9.5 Firmware Update....36
Section 10: PoE....39
10.0 PoE Status....39
10.1 PoE Setting....40
10.2 PoE Event Counter....42
10.3 PoE Power Delay....43
10.4 PoE Auto Check....43
Section 11: Port Management....45
11.0 Port Configuration....45
11.1 Port Mirroring....50
11.2 Bandwidth Control....51
11.3 Broadcast Storm Control....54
Section 12: VLAN Settings....55
12.0 VLAN Mode....55
12.1 VLAN Member (Port Based)....57

12.2 VLAN Member Settings (Tag Based) 59
12.3 Multi to 1 Setting 60
12.4 Non-Association Port Setting 62
Section 13: Per Port Counter 63
13.0 Transmit Packet and Receive Packets 63
13.1 Drop and Receive Packet 64
13.2 CRC error packet and Receive Packet 64
13.3 Counter Modes Defined 65
Section 14: QoS Settings 66
14.0 Priority Mode 66
14.1 Setting the Priority Mode 66
14.2 Class of Service Configuration 68
Section 15: Security 71
15.0 MAC Address Binding 71
15.1 Scanning MAC Addresses 72
15.2 Securing Ports Using Mac Addresses 73
15.3 TCP/UDP Filter 73
15.4 Secure WAN Port: Select the port to be secured 75
Section 16: Spanning Tree 77
16.0 STP Bridge Settings 77
16.1 STP Port Settings 78
16.2 Loopback Detection Settings 79
Section 17: DHCP Relay Agent 81
17.1 Relay Agent Configurations 81
Section 18: Backup and Recovery 84
18.0 Configuration Backup/Recovery 84
18.1 Back Up 84
18.2 Recovery 84
Section 19: Miscellaneous Settings 85
19.0 Miscellaneous Settings Defined 85
19.1 Output Queue Aging Time 85
19.2 VLAN Striding 86
19.3 IGMP Snoop V1 & V2 86
19.4 VLAN Uplink 87
19.5 UDP/TCP Alert Messages 88
19.6 SNMP Settings 89

19.7 SNMP Trap States....92
Section 20: Log Out....93
20.0 Log Out Procedure....93
Section 21: Glossary....94
A....94
ACE....94
ACL....94
AES....95
APS....95
Aggregation....95
ARP....95
ARP Inspection....95
Auto-Negotiation....95
C....95
CC....95
CCM....96
CDP....96
D....96
DEI....96
DES....96
DHCP....96
DHCP Relay....96
DHCP Snooping....97
DNS....97
DoS....97
Dotted Decimal Notation....97
DSCP....98
E....98
EEE....98
EPS....98
Ethernet Type....98
F....98
FTP....98
Fast Leave....98
H....98
Host Defined Power Limit....98

HTTP....99
HTTPS....99
I....99
ICMP....99
IEEE 802.1X....99
IGMP....100
IGMP Querier....100
Intelligent Power Limit....100
IP....100
L....100
LACP....100
LLC....101
LLDP....101
LLDP-MED....101
LOC....101
M....101
MAC Table....101
Mirroring....101
MLD....102
MVR....102
N....102
NAS....102
NetBIOS....102
NFS....102
NTP....103
O....103
OUI....103
Option 82....103
P....103
PCP....103
PD....103
PHY....103
PING....103
PoE....103
Policer....104
Private VLAN....104

PTP 104
Q 104
QCE 104
QCL 104
QL 104
QoS 105
R 105
RARP 105
RADIUS 105
RDI 105
RSTP 105
S 105
SHA 105
Sharper 106
SMTP 106
SNAP 106
SNMP 106
SNTP 106
SSID 106
SSH 106
SSM 106
STP 106
SyncE 107
T 107
TACACS+ 107
Tag Priority 107
TCP 107
TELNET 107
TFTP 107
U 108
UDP 108
User Priority 108
V 108
VLAN 108
VLAN ID 109
Voice VLAN 109

SFP Interface Guide **110**
Connecting Vi32226 ..... **113**
Contact Information **114**

Section 3: Introduction

3.0 Overview

This user's manual will not only tell you how to install and connect your network system, but how to configure and monitor the Vi32226 through the web by (RJ45) serial interface and Ethernet ports step-by-step. Many detailed explanations of hardware and software functions are shown, as well as, the examples of the operation for web-based interface.

The Vi32226 series, the next generation web managed switches from Vigitron, is a portfolio of affordable managed switches that provides a reliable infrastructure for your business network. These switches deliver intelligent features to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth to deliver information and applications effectively. It provides the ideal combination of affordability and capabilities for entry level networking, including small business or enterprise application to help you create a more efficient and better-connected workforce.

Product description and key bulletin points:

- 24 extended coax ports
- 24 Ports at 10/100 Mbps
- 2 Ports at 1000Mbps
- Layer 2 network switch
- 685 watts total power supply
- 550 watts PoE budget
- Up to 36 watts per port

3.1 Cabling Guidelines

Ports 1-24 are 10/100Mbps and will automatically sense network speeds if set to the auto mode or can be forced set to a either network speed. Ports 25 and 26 are 10/100/1000Mbps and can also be set to auto sense speeds or forced speeds. Ports 25 and 26 can also be connected to optional SFP transceivers and used as either copper or fiber ports, but not at the same time.

Each device requires an unshielded twisted-pair (UTP) cable with RJ45 connectors at both ends. Use Category 5, 5e, or 6 cables for 1000BASE-T connections, Category 5 or better for 100BASE-TX connections.

The RJ45 ports on the switch support automatic MDI/MDI-X pin-out configuration. You can use standard straight-through twisted-pair cables to connect to any other network devices (E.g. PCs, servers, switches, routers, or hubs).

See Appendix B for further information on cabling.

CAUTION: Do not plug a phone jack connector into an RJ45 port. This will damage the switch. Use only twisted-pair cables with RJ45 connectors that conform to FCC standards.

3.2 Connecting to PCs, Servers, Hubs and Switches

Step 1: Attach one end of a twisted-pair cable segment to the device's RJ45 connector.

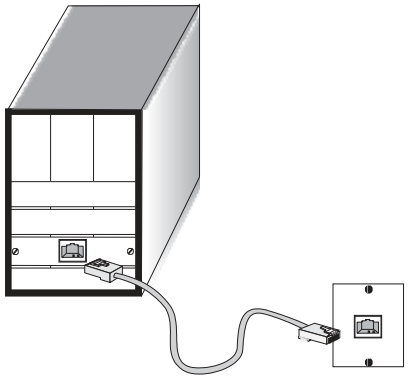


Figure 16: Making Twisted-Pair Connections

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: Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Step 3: As each connection is made, the Link LED (on the switch) corresponding to each port will light yellow (100 Mbps) and (10 Mbps) to indicate that the connection is valid. Will flash when activity if present. Green if PoE is present.

3.3 Network Wiring Connection

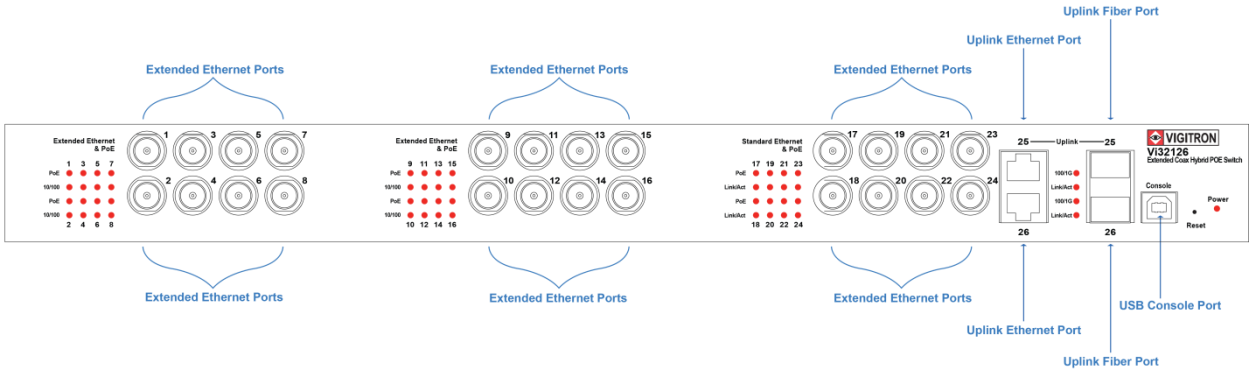
Today, the punch-down block is an integral part of many of the newer equipment racks. It is actually part of the patch panel. Instructions for making connections in the wiring closet with this type of equipment are as follows:

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 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.

3.4 Vi32226 – Front View



3.5 Vi32226 – Rear View

Section 4: Description of Hardware

4.0 1000Base-T Ports

The switch contains 24100BASE-T RJ45 and 2, 1000Mbps ports. All RJ45 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 can be selected automatically.

4.1 SFP Transceivers Slots

Vi32226 supports the Small Form Factor Pluggable (SFP) transceiver slots. The slots are shared with RJ45 port 25 to 26. In the default configuration, if an SFP transceiver (purchased separately) is installed in a slot and has a valid link on the port, the associated RJ45 port is disabled.

The following table shows a list of transceiver types which have been tested with the switch.

Media Standard	Fiber Diameter (microns)	Wavelength (nm)	Maximum Distance*	Transmission Speed
Vi00850MM-H	50/1.25	850nm	300m/500m	1G
Vi01310MM-H	50/1.25	1310nm	2Km	100Mbps
Vi01310SM-H	9/1.25	1310nm	10Km	1G
Vi01000CH	Copper (UTP)		100m	1G

Table 1: Supported SFP Transceivers

NOTE:
* Maximum distance may vary for different SFP vendors.
* Regardless of the SFP speed, ports 1-24 are 100Mbps / Ports 25 & 26 are 1Gbps.
* SFP must be matched at both cable ends.
* For ports 25 and 26, SFP port speed is fixed at 1000Mbps and cannot be changed.

4.2 Ports and System Status LEDs

The Vi32226 includes 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.

LED	Conditions	Status
TP (Link/ACT)	Yellow	Green when the TP link is good. Blinks when any traffic is present.
PoE Port 1-24	Green	Green when the port is delivering PoE power.
Port 25 & 26	Green	On is for 1G Link Slow blink is for 100Mb/s Off with link yellow LED on is for 10Mb/s
SFP (Link/ACT)	Yellow/ Green	Yellow is for activity Green is for link Blinks when any traffic is present.

Table 2: Port Status LEDs

SYSTEM LED	Condition	Status
Power	Green	Lit when powered

Table 3: System Status LED

4.3 Console Port

The console port can be used for direct communications with the switch. If the switch's IP address is lost, it can be recovered without having to reset the switch to its default settings.

To access the console port: Requires running a terminal program on your computer.

Terminal set up:

Baud Rate	19,200
Bit Setting	8 Bit
Parity	No Parity
Stop Bit	1 Stop Bit
Flow Control	No Flow Control (No Hardware)
Log In	Requires User Name and Password

Once log in has been achieved, type “help” (lower case) for a list of accessible functions. The current IP can be displayed along with other functions that can be changed if required.

Section 5: Installing the Switch

5.0 Selecting a Site

The switch can be mounted in a standard 19-inch equipment rack 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 you want to link and near a power outlet.
  - Be able to maintain its temperature within 0°C to 40°C (32°F to 104°F) and its humidity within 10% to 90%, non-condensing.
  - Be accessible for installing, cabling and maintaining the devices.
  - Allow the status LEDs to be clearly visible.
- Make sure the twisted-pair Ethernet cable is always routed away from power lines, radios, transmitters or any other electrical interference.
- Make sure that Vi32226 is connected to a separate grounded power outlet that provides 100 to 240VAC and 50 to 60 Hz.

5.1 Ethernet Cabling

To ensure proper operation when installing the switch into a network, make sure that the current cables are suitable for 100BASE-TX or 1000BASE-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 RJ45 connectors; Category 5 or Category 5e with maximum length of 100 meters is recommend 100BASE-TX, and Category 5e or 6 with maximum length of 100 meters is recommend for 1000BASE-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.

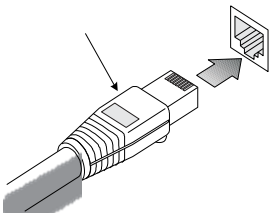


Figure 7: RJ45 Connections

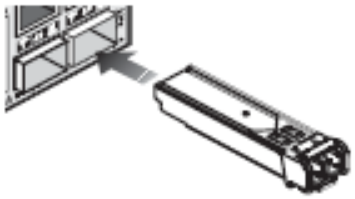


Figure 8: SFP Transceiver

5.2 Equipment Checklist

After unpacking this switch, please make sure you have received all the components. And before beginning the installation process, be sure you have all other necessary installation equipment.

5.3 Package Contents

Contents include:

- Vi32226 16-port extended Coax, 8-port standard PoE network switch, 2 1G uplink ports
- Mounting Accessory (for 19” Rack)
- USB Memory Drive
- AC Power Cord

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

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

5.4 Mounting

The switch can be mounted in a standard 19-inch equipment rack or on a desktop or shelf. Mounting instructions for each type of site as follow.

5.5 Rack Mounting

Before rack mounting the switch, please pay attention to the following factors:

- **Temperature**: Since the temperature within a rack assembly may be higher than the ambient room temperature, check that the rack-environment temperature is within the specified operating temperature range (0 to 40 °C).

- **Mechanical Loading**: Do not place any equipment on top of a rack-mounted unit.
- **Circuit Overloading**: Be sure that the supply circuit to the rack assembly is not overloaded.
- **Grounding**: Rack-mounted equipment should be properly grounded.

5.6 To Rack-Mount Devices

Step 1. Attach the brackets to the device using the screws provided in the Mounting Accessory.

Step 2. Mount the device in the rack using four rack-mounting screws. Be sure to secure the lower rack-mounting screws first to prevent the brackets being bent by the weight of the switch.

Step 3. If installing a single switch only, turn to “Connection to a Power Source” at the end of this chapter.

Step 4. If installing multiple switches, mount them on the rack one below the other, in any order.

5.7 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. Use only Manufacture mini-GBIC.

NOTE:

- 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 compatible issue, and their use may result in product malfunction.

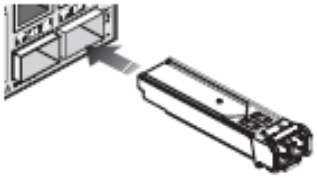


Figure 12: Inserting an SFP Transceiver into a Slot

5.8 Installing an SFP Transceiver

Step 1. Consider network and cabling requirements to select an appropriate SFP transceiver type.

Step 2. Insert the transceiver with the optical connector facing outward and the slot connector facing down. Note that the SFP transceivers are keyed so they can only be installed in one orientation.

Step 3. Slide the SFP transceiver into the slot until it clicks into place.

NOTE: SFP transceivers are not provided in the switch package.

5.9 Connecting to a Power Source

You can plug or remove power cord from AC power socket to switch the power on or off.

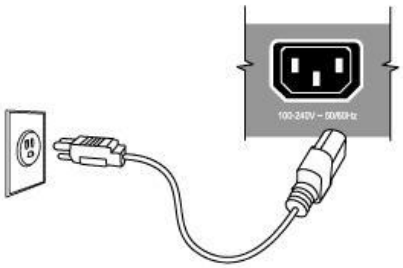


Figure 13: Inserting the Power Cord to AC Power Socket

Step 1. Insert the power cable plug directly into the AC Socket located at the back of the switch.

Step 2. Plug the other end of the cable into a grounded, 3-Pin, AC power source.

Step 3. Check the front-panel LEDs as the device is powered on to be sure the POWER LED is lit. If not, check that the power cable is correctly plugged in.

WARNING: For International use, you may need to change the AC line cord. You must use a line cord set that has been approved for the socket type in your country.

Section 6: Making Network Connections

6.0 Connecting to a 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.

6.1 Twisted-Pair Devices

Each device requires an unshielded twisted-pair (UTP) cable with RJ45 connectors at both ends. Use Category 5, 5e or 6 cables for 1000BASE-T connections, Category 5 or better for 100BASE-TX connections.

6.2 Cabling Guidelines

The RJ45 ports on the switch support automatic MDI/MDI-X pin-out configuration, so you can use standard straight-through 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 RJ45 port. This will damage the switch. Use only twisted-pair cables with RJ45 connectors that conform to FCC standards.

6.3 Connecting to PCs, Servers, Hubs and Switches

Step 1. Attach one end of a twisted-pair cable segment to the device's RJ45 connector.

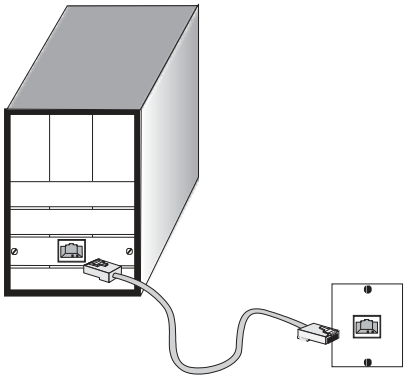


Figure 16: Making Twisted-Pair Connections

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 (328ft) in length.

NOTE: Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise, back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Step 3. As each connection is made, the Link LED (on the switch) corresponding to each port will light green (1000 Mbps) or amber (100 Mbps) to indicate that the connection is valid.

6.4 Network Wiring Connections

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

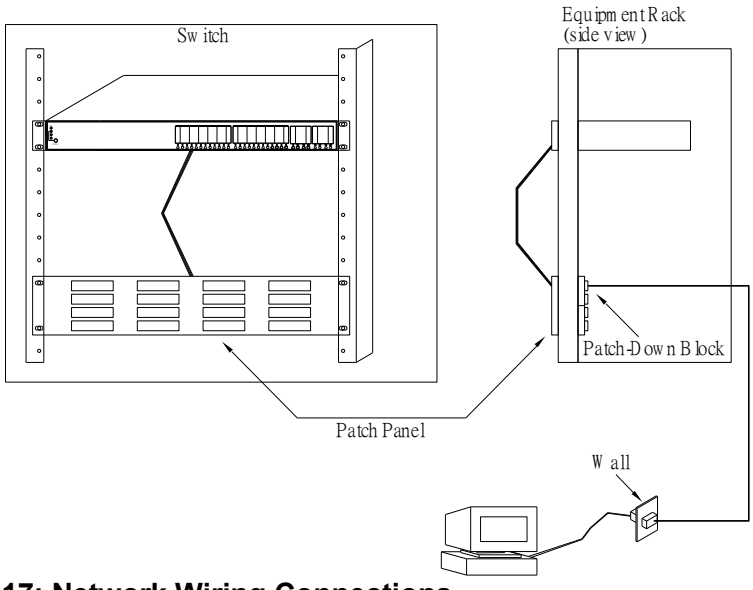


Figure 17: Network Wiring Connections

Section 7: Troubleshooting

7.0 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 RJ45 ports are configured as “Auto”. That is, when connecting to attach 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, for example 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 the Vi32226 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 communications between the switch and the device.

  Make sure all devices connected to the Vi32226 Switch devices are configured to auto negotiate, or are configured to connect at half duplex (all hubs are configured this way, for example).
- **Faulty or loose cables.** Look for loose or obviously 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 pin-outs and correct cable wiring. A category 5 cable tester is a recommended tool for every 100Base-TX and 1000Base-T network installation.
- **Improper Network Topologies.** It is important to make sure you have a valid network topology. If you no longer experience the problems, the new topology is probably at fault. In addition, you should make sure that your network topology contains ***no data path loops.***

- **Check the Port Configuration.** A port on your switch may not be operating as you expect because it has been put into a “blocking” state by Spanning Tree, GVRP (automatic VLANs), or LACP (automatic trunking). (Note that the normal operation of the Spanning Tree, GVRP, and LACP features may put the port in a blocking state.) Or, the port just may have been configured as disabled through software.

7.1 Table 10: Troubleshooting Chart

Symptom	Action
POWER LED is Off	• Check connections between the switch, the power cord and the wall outlet. • Contact your dealer for assistance.
Link LED is Off	• 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 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.

Section 8: Operation of Web-Based Management

8.0 Initial Configuration

This chapter instructs you on how to configure and manage the Vi32226 through the web user interface. With this facility, you can easily access and monitor through any one port of the switch and all the status of the switch, including MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The default values of the Vi32226 are listed in the table below:

IP Address	192.168.1.133
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	system

NOTE: In models where the firmware version ends in 1.03, the switch will default to an IP address of 192.168.1.1.

After the Vi32226 configuration has been finished, you can browse the interface. For instance, if you type **http://192.168.1.133** in the address row in a browser, it will show the following screen and will ask you to input in the username and password in order to login and access authentication.

The default username is **"admin"** and password is **"system"**. For first time use, please enter the default username and password, and then click the **<Update>** button. The login process now is completed. In this login menu, you have to input the complete username and password respectively, the Vi32226 will not give you a shortcut to username automatically. This looks inconvenient, but it's the safer option.

NOTE: When you log into the Switch WEB to manage, you must first type the username of the admin. The default password is “system.” So after you type in the username, please press enter. Management page will enter WEB. When you log into Vi32226 series switch Web UI management, you can use both ipv4 only login to manage. To optimize the display effect, we recommend you use Microsoft Edge above, Firefox, Chrome and OS and have the resolution 1024x768. The switch supported neutral web browser interface. If the UI is not working with any versions of the above browser, it might result from PC security system setting.

NOTE: Updating or refreshing the browser may take several minutes.

Section 9: Administration

9.0 Prior to Logging On

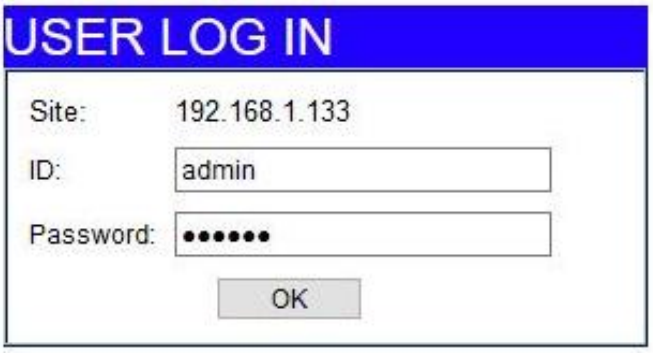
Note the default address for the switch is 192.168.1.133. To access the switch for programming, your computer must be on the same subnet using any final value greater than 1.

NOTE: The default address for the switch is 192.168.1.133. To access the switch for programming, your computer must be on the same subnet using any final value greater than 1.

In models where the firmware version ends in 1.03, the switch will default to an IP address of 192.168.1.1.

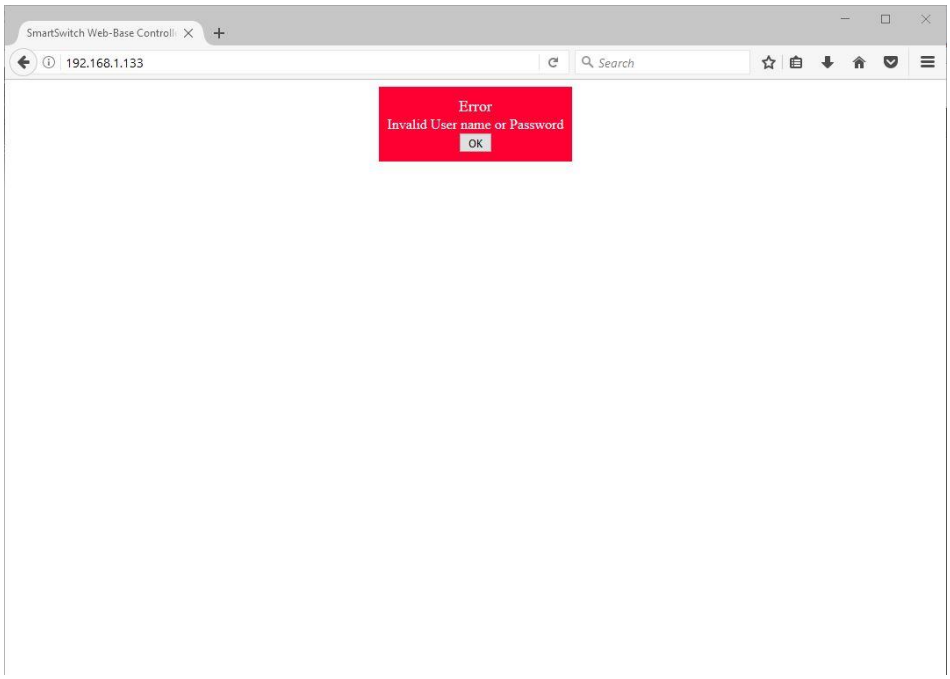
9.1 Logging On

- Enter the correct administrator name and password after the login page shows up.
- Default IP address: 192.168.1.133
- Default administrator name: admin
- Default password: system
- Press “OK” to login.



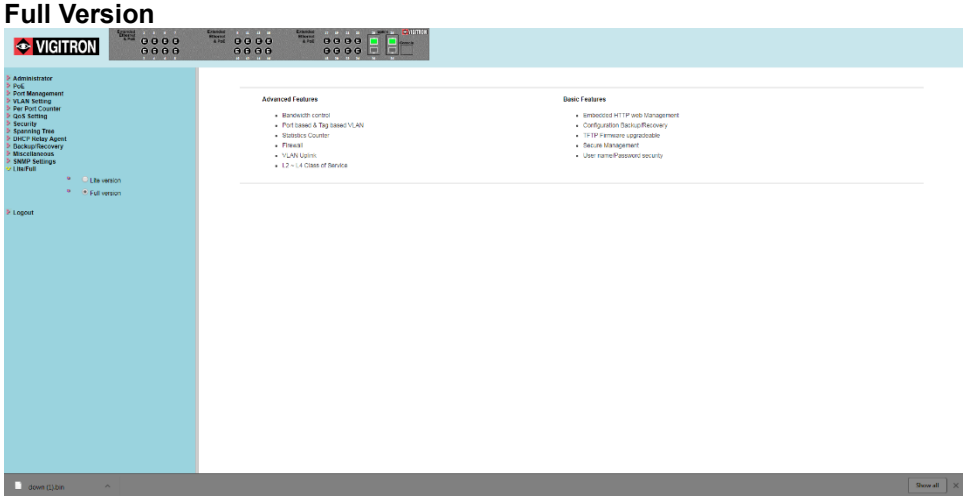
NOTE: The administrator name and password fields are case-sensitive. The higher case characters will be recognized as different characters. For example: “ADMIN” will be recognized as the different character from “admin”.

If you input the incorrect administrator name or password, the following warning message will show up and you must click “OK” to go back to the login page.

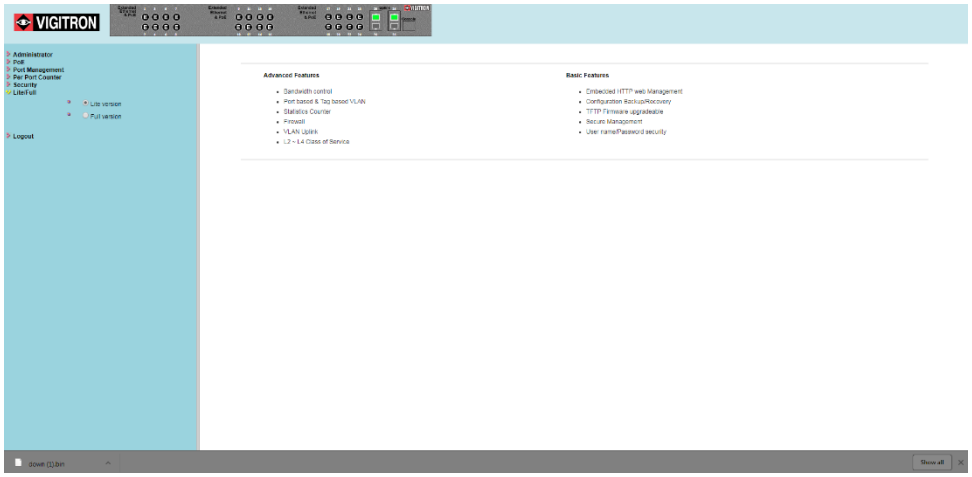


After logging in the following page will appear

Full Version



Lite Version

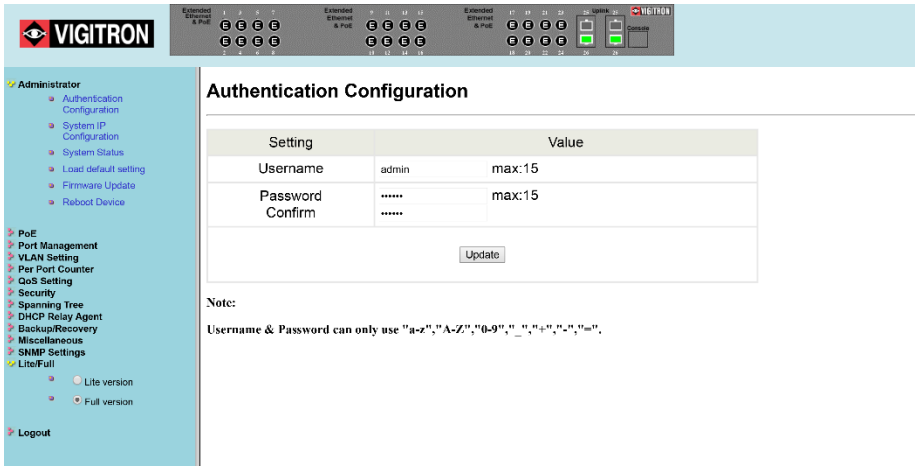


Selecting Operating Mode:

The Vi32226 provides two separate operating modes. The lite version provides set-ups for addressing, PoE and bandwidth, while the full mode provides for all set-ups. These modes can be used to simplify set-ups and operations.

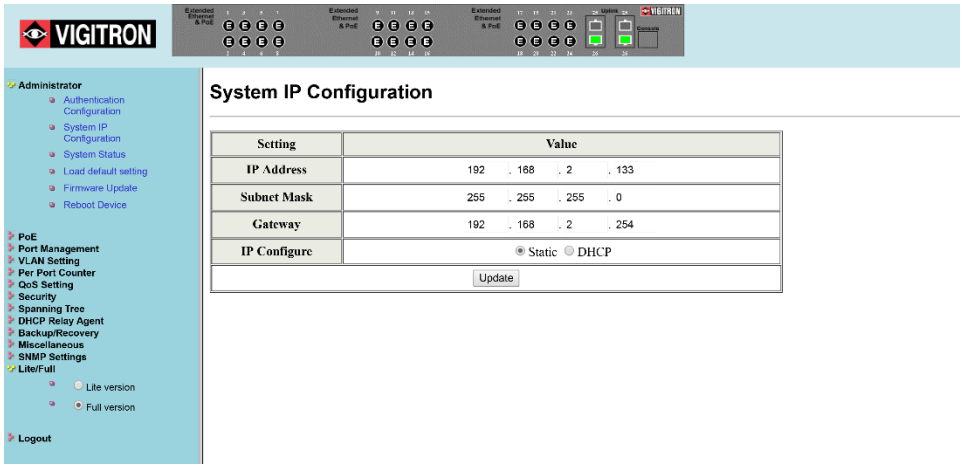
NOTE: In the switch icon, if either the fiber port or the copper port is connected, both ports will show as active.

This switch also supports DHCP allowing dynamic IP addressing as allocated by the DHCP server. If the DHCP server is not used please set the initial address as 192.168.1.133.



- Enter the administrator users name – up to 15 characters.
- Enter a password- up to 15 characters.
- Confirm the password- re-enter the password.
- Click on the update button. The user name and password will now be changed to the entered user name and password.

9.2 System IP Configuration



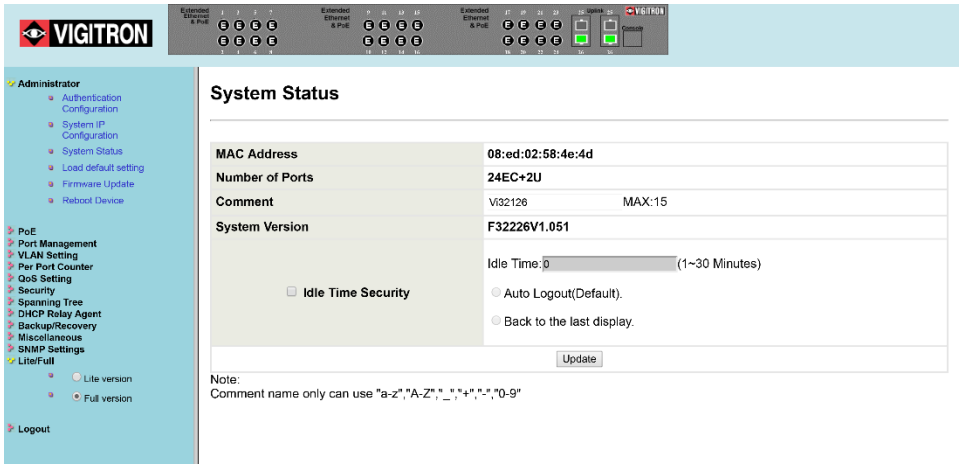
IP Address: Enter a valid IvP4 address.

Subnet Mask: Enter a valid range: 255.255.255.0 will allow for all addresses with in the programmed address.

Gateway: Enter a gateway address making the value is the same as the IP address.

IP Configure: Select Static or DHCP. Select will operate based on the above entries. If DHCP, the switch must be connected to server that will provide an address. In many cases you will not be able to know the IP address from the switch itself.

9.3 System Status



MAC Address: This is fixed and reflects the unique product address

Number of Ports: If the sequence is three numbers:
The first number = number of extended ports
The second number = number of standard ports
The third number = number of uplink ports

Comment: The operator can enter a unique name from the switch. Letters and numbers are restricted as follows “a-z”, “A-Z, “_”, “+”, “-“ and “0-9”

System Version: Is fixed and displays the current firmware version

Enter Idle Time: Enter a value 1-30 = 1to 30 minutes. This is the time a user can stay connected to the switch without any activity. After that time a new log in will be required. Note: This function is only active if the Idle time security button is selected.

Activity Idle Time Security: Click the radio button to activate the IdleTime Security function.

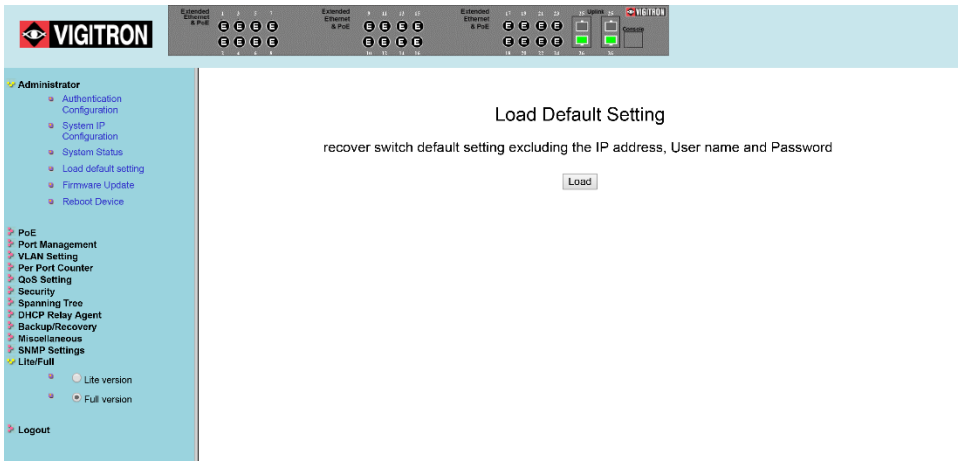
Auto Logout: If the Idle Time Security is selected + the Auto Logout when the non-activity time period is reached, the system will log the user out and return to the log in screen.

NOTE: If only the Idle Time Security function is selected, Auto logout will be the default mode for this function.

Back to last display: If this mode is selected, the screen will return to the last selected screen mode when the Idle time period is reached. A new log in will be required.

Update: After programming is complete, select the Update radio button to confirm.

9.4 Load Default



If you make a mistake in programming switch features, you can return to the original default configuration by pressing the load button. All settings will be reversed with the exception of:

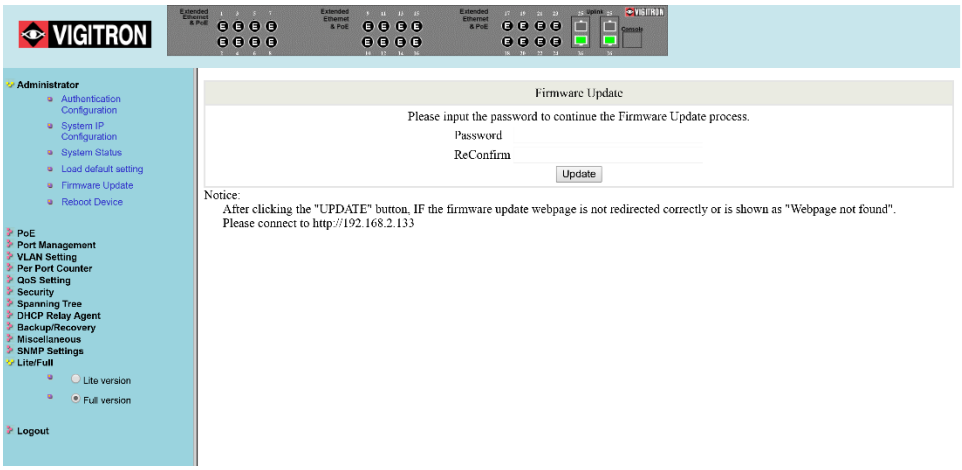
- IP address
- User Name
- Password

NOTE: In models where the firmware version ends in 1.03, the switch will default to an IP address of 192.168.1.1.

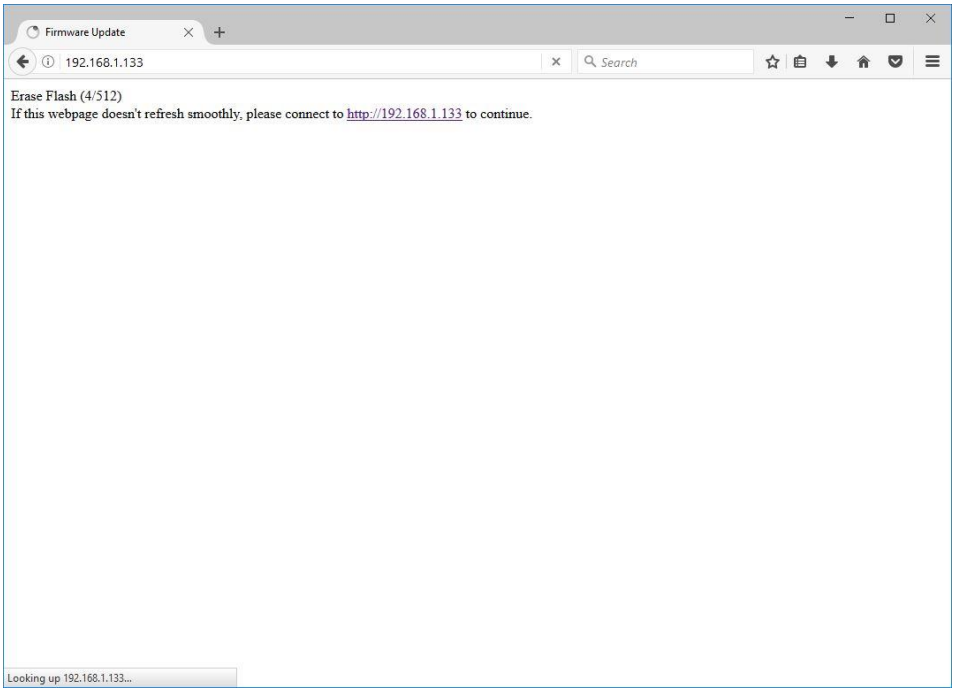
NOTE: Whenever the Switch is set back to the Default settings, the original factory firmware will be installed. If a Firmware upgrade has been performed prior to the Load Default operation, the Switch will again need the Firmware upgrade.

After loading default, you may have to restart your browser.

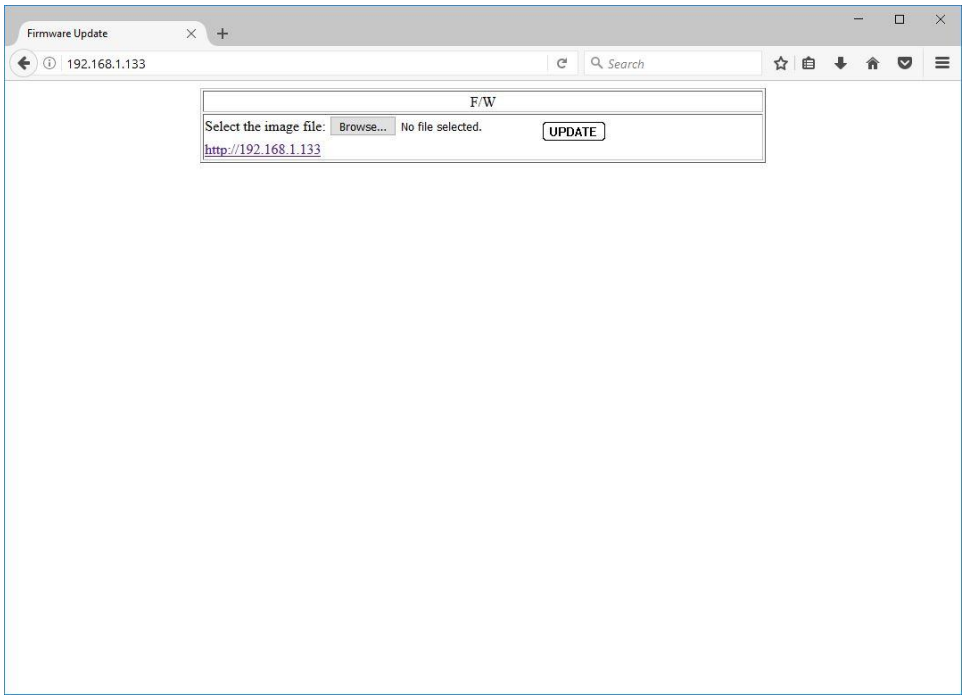
9.5 Firmware Update

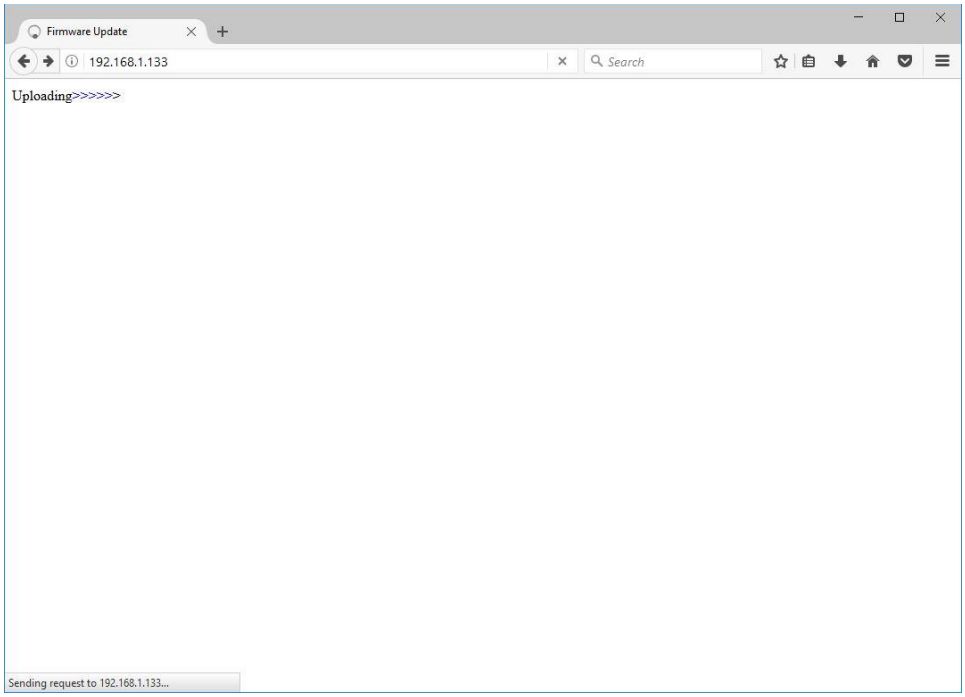


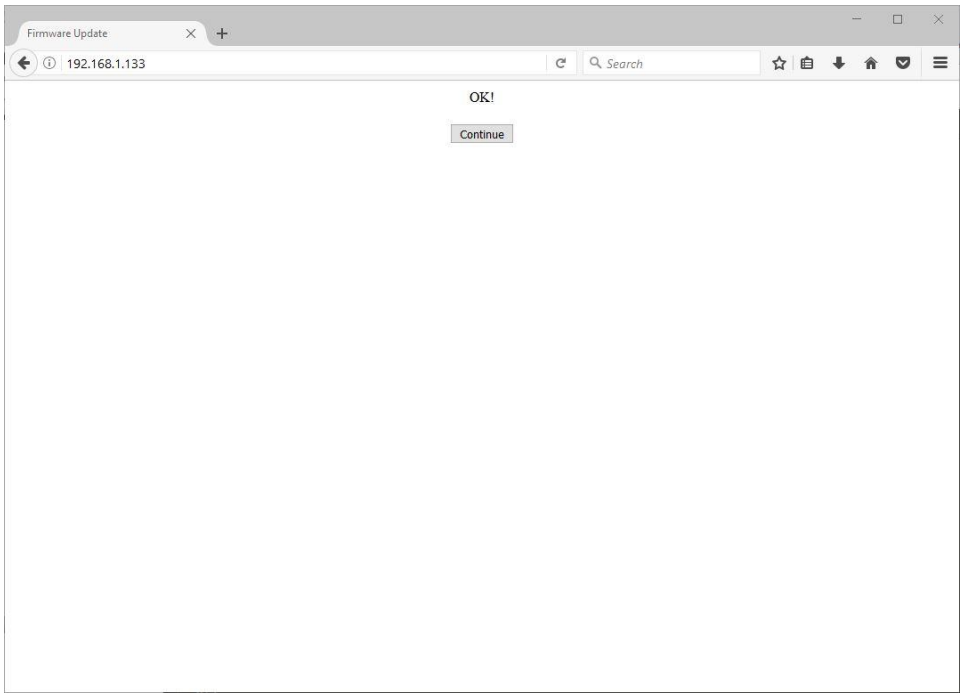
When pressing the update button, it redirects. If the system does not redirect or “webpage not found”, please enter the address http://192.168.1.133.



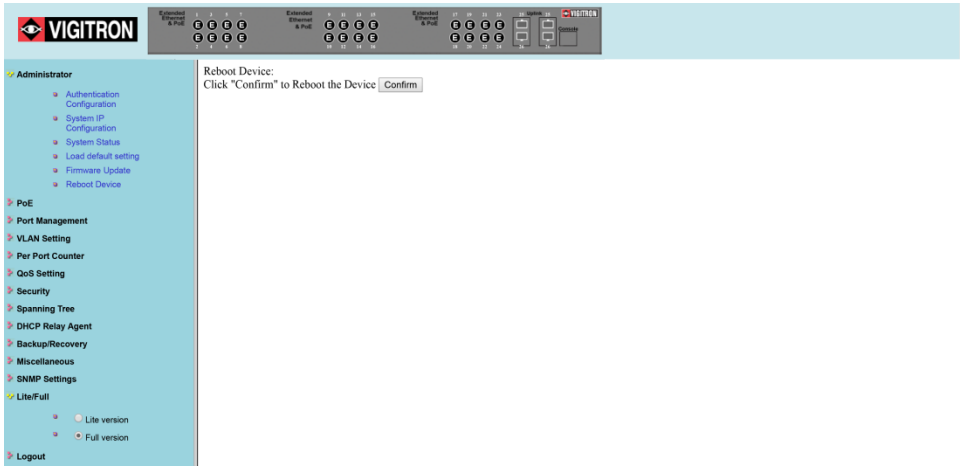
After the “Update” button is pressed, the existing code will be erased. After this is complete, select the new file and press “**Update”.**


Firmware Update
192.168.1.133
Search
F/W
Select the image file:
Browse...
No file selected.
UPDATE
http://192.168.1.133


Firmware Update
192.168.1.133
Search
Uploading>>>>>>
Sending request to 192.168.1.133...

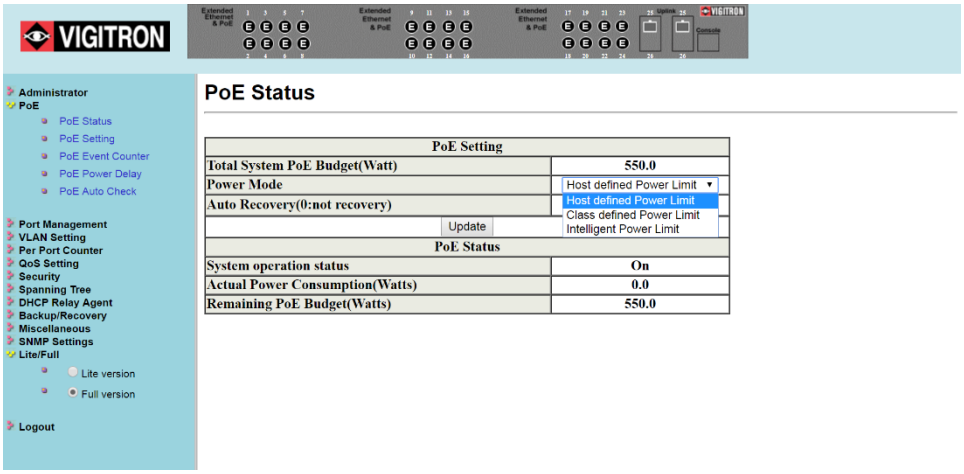


Reboot Device: If operation becomes unstable, select “Reboot Device” and press confirm. Using this function will not reset the hardware.



Section 10: PoE

10.0 PoE Status



Power Mode:

Select Mode by:

Host: Power provided will be determined by connected device.

Class: Power is determined by power class of connected device limited to that power class.

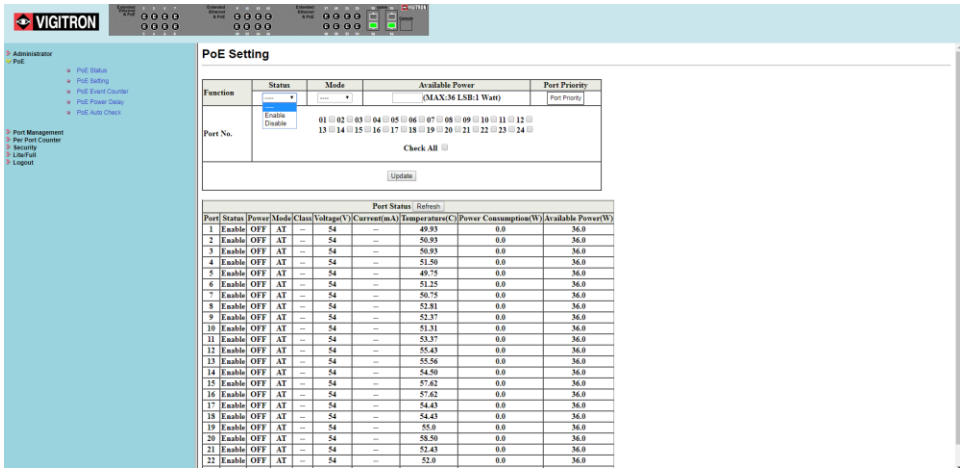
Host defined Power Limit: Power is determined by port setting, which can be any variable within the range of the selected class power.

Class defined Power Limit: Power is defined by the upper limit of the selected class.

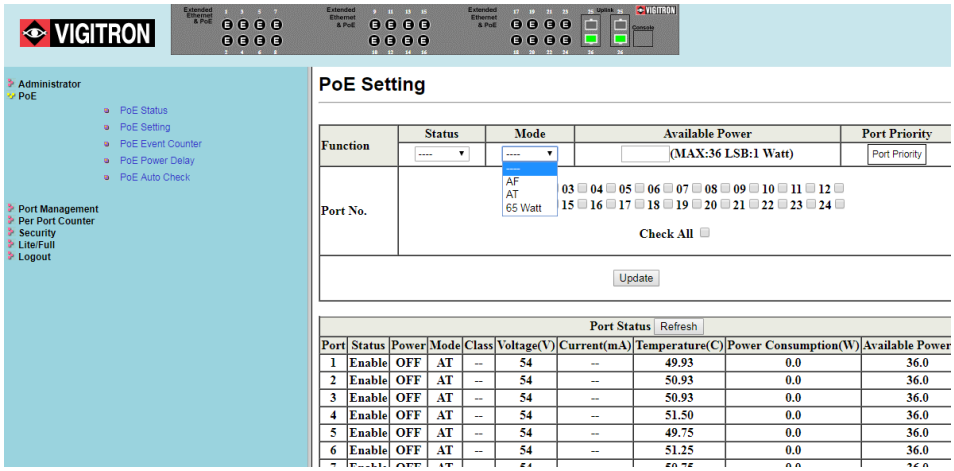
Intelligent Power Limit: Power is determined by the connected device.

Auto Recovery: If PoE is lost, restart will be determined by this setting.

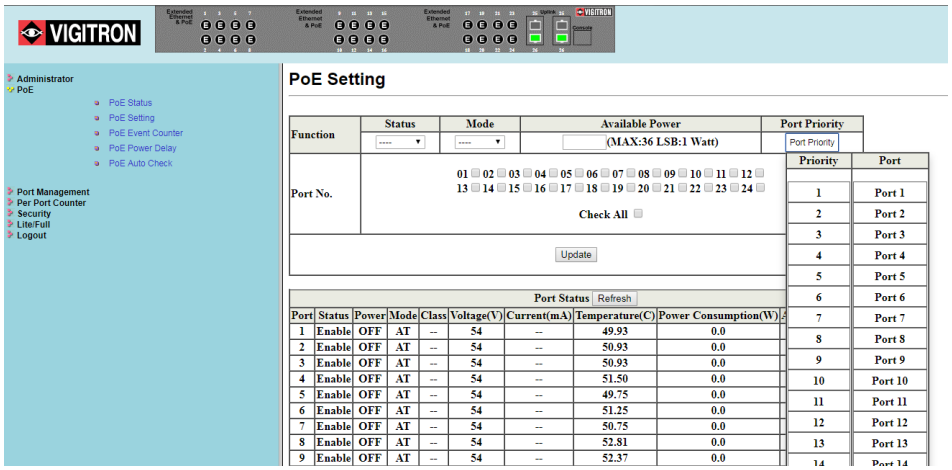
10.1 PoE Setting



1. Select Port.
2. Select Enable/Disable.
3. Select class as Either AF or AT.
4. Input the PoE power level.
5. Select Update: Actual status will be displayed in chart below.



Port	Status	Power	Mode	Class	Voltage(V)	Current(mA)	Temperature(C)	Power Consumption(W)	Available Power
1	Enable	OFF	AT	--	54	--	49.93	0.0	36.0
2	Enable	OFF	AT	--	54	--	50.93	0.0	36.0
3	Enable	OFF	AT	--	54	--	50.93	0.0	36.0
4	Enable	OFF	AT	--	54	--	51.50	0.0	36.0
5	Enable	OFF	AT	--	54	--	49.75	0.0	36.0
6	Enable	OFF	AT	--	54	--	51.25	0.0	36.0



1. In the Port Setting page, click on the “Port Priority” box to display a dropdown list of the current settings. The default is port 1 as the highest priority through port 24 as the lowest.
2. To change the priority of a port, left click on one of the ports in the “Port” column and hold your mouse button down to drag and drop the port to the desired position.
3. When the new port priority placement is finished, click the “Update” button to apply the changes. After the page refreshes, click the “Port Priority” box again to verify the new port priority settings.

Port Priority Setting:
In PoE Settings page, click on the button labeled “Port Priority” in top right segment of page. A new window will appear, showing a list of ports and their respective priorities. As default, the ports will have descending priority, where port 1 has the highest priority, and port 24 has the lowest priority. To change the priority of the ports, drag and drop a specific port into its desired priority position.

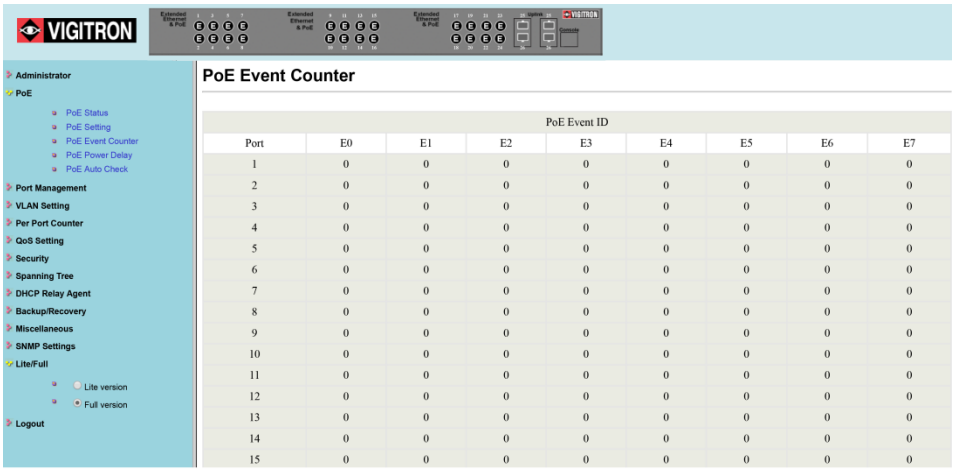
NOTE: When a port is dropped into a priority position, the subsequent ports will be pushed to a lower priority.

Once the priority for the ports has been established, click the “update” button so the changes take effect.

Once the page reloads, note that the priority list has changed by clicking on the “Port Priority” button again.

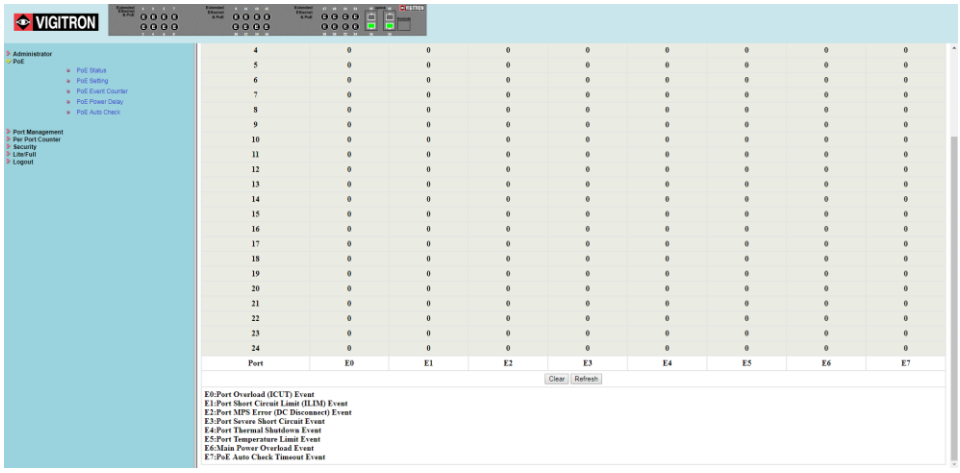
To hide the priority list window, click the “port priority” button again.

10.2 PoE Event Counter



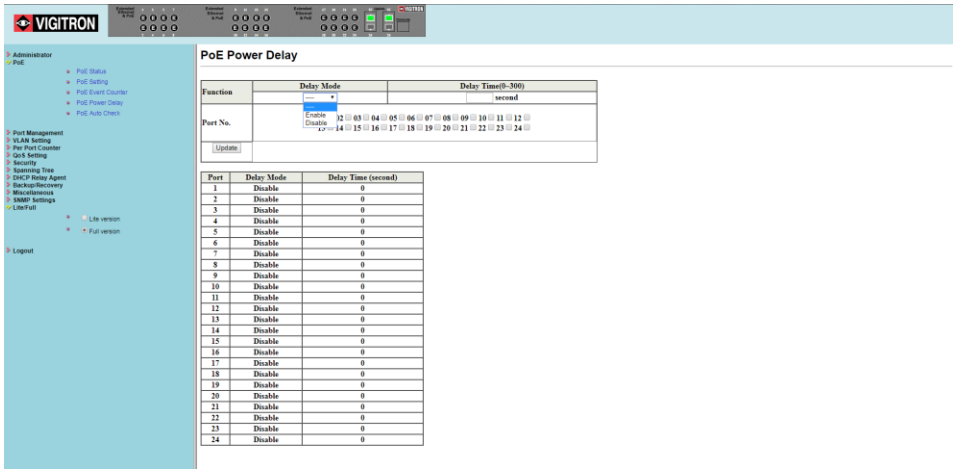
PoE Event Counter Definitions

E0: Port Overload (ICUT) Event
E1: Port Short Circuit Limit (ILIM) Event
E2: Port MPS Error (DC Disconnect) Event
E3: Port Severe Short Circuit Event
E4: Port Thermal Shutdown Event
E5: Port Temperature Limit Event
E6: Main Power Overload Event
E7: PoE Auto Check Timeout Event



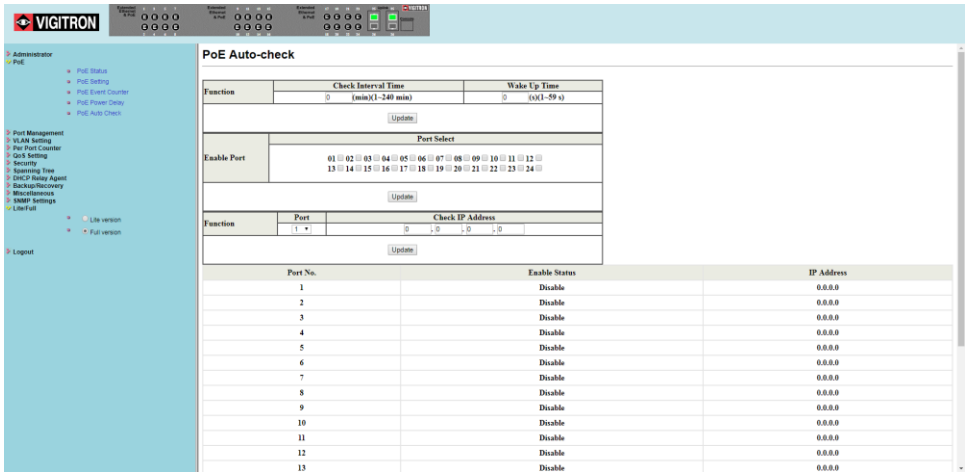
10.3 PoE Power Delay

This setting can be used to delay the application of PoE in cases where a connected device will draw large amounts of power.



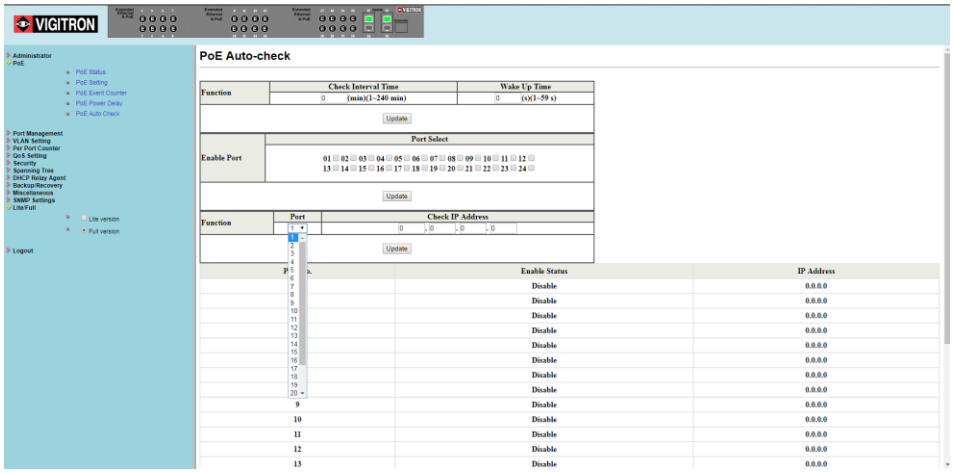
1. Enable the Delay mode. If the Delay mode is already enabled, you can disable it by selecting disable.
2. Enter the delay period between 1-300 seconds, (1 second to 5 minutes). The delay time starts at from the switch boot.
3. The port number to apply the delay to.
4. Click Update.
5. Confirm the setting is correct by seeing if the delay is applied to the selected port.

10.4 PoE Auto Check



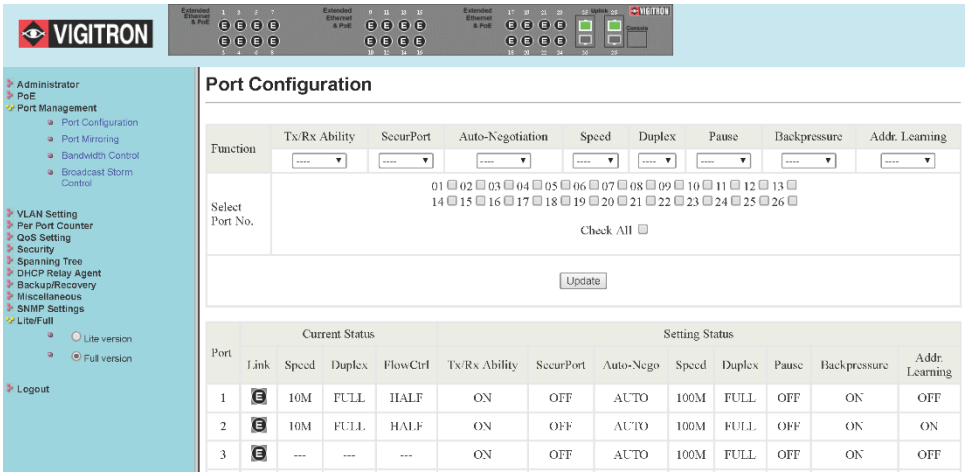
PoE Auto-Check: This setting will check the status of the IP connection, reconnect and reapply PoE.

1. Enter the Interval Time- from 1-240min (1mm- 4 hours). This will define the duration the connected device is ping.
2. Enter the Wake up Time- 1-59 seconds. This will define the time it will take for the connected device will respond and become operational.
3. Enable Port: Select the port- to which the settings and click update.
4. Function: Select the port and enter the connected devices IP address.
5. Click update.
6. Confirm the settings are correct but viewing the “Enable Status” and the IP Address.
7. Make certain the wakeup time is shorter than the check interval duration.



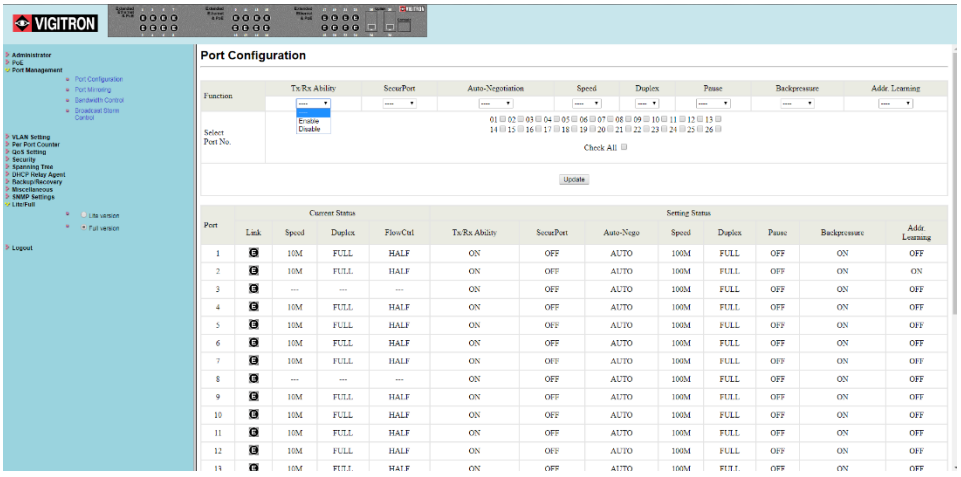
Section 11: Port Management

11.0 Port Configuration



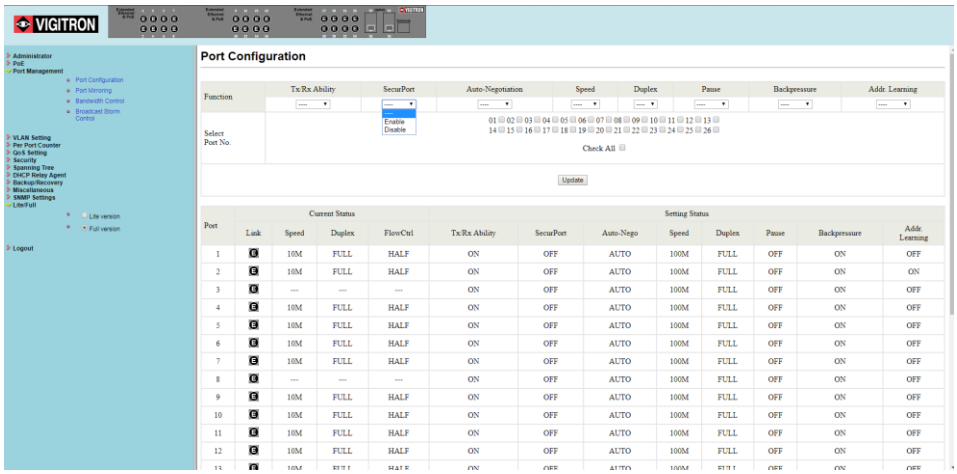
Select the Port Number: Select the port number 1-26.

NOTE:
For ports 25 and 26, port speed is selectable for 100Mbps or 1000Mbps for UTP (copper) connections only. When Fiber STPs are used the port speed will be fixed at 1000Mbps. It cannot be changed and only 1000Mbps SFPs can be used for connected devices.



Tx/Rx:

- Enable for normal operation – this is default setting
- Disable- this will shut down port



1. In the Port Configuration section, click the down arrow under SecurPort. Select either Enable or Disable to turn the feature on or off.
2. Select the desired ports by checking the boxes next to the ports to be set.
3. Click “Update” to apply the new settings.
4. After the page refreshes, verify the correct settings in the table.

SecurPort™

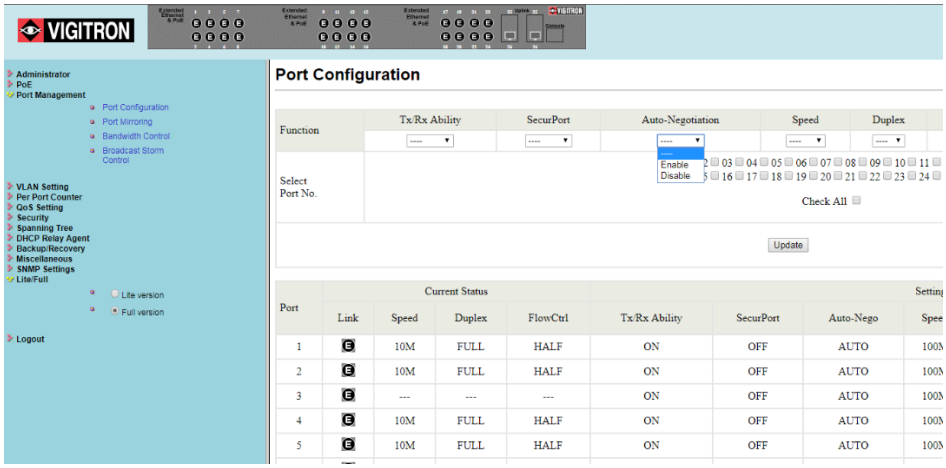
- Click on the dropdown menu for the SecurPort configuration, and select the “Enable” option. Check the checkbox for the ports that will be configured as SecurPort. (Note: For Extended ports and Coax ports, the SecurPort configuration must be enabled only after the port is under stable use, otherwise, the behavior of the ports when nothing is connected will lock the port before the user even starts using the port).

What does SecurPort do?
Once a port has been configured as SecurPort, the transmit/receive ability of the port will be automatically disabled when the switch detects that a physical link to that port goes down.

NOTE: SecurPort only disables the transmit/receive ability of the port. If configured, the port will still provide PoE.

WARNING: Power Loss and SecurPort™ Active
If SecurPort™ is active for any port and a power loss occurs, when power is restored, the switch will remember the setting and deactivate the port. This is to maintain the security of the port and prevent it from being defeated by a power loss.

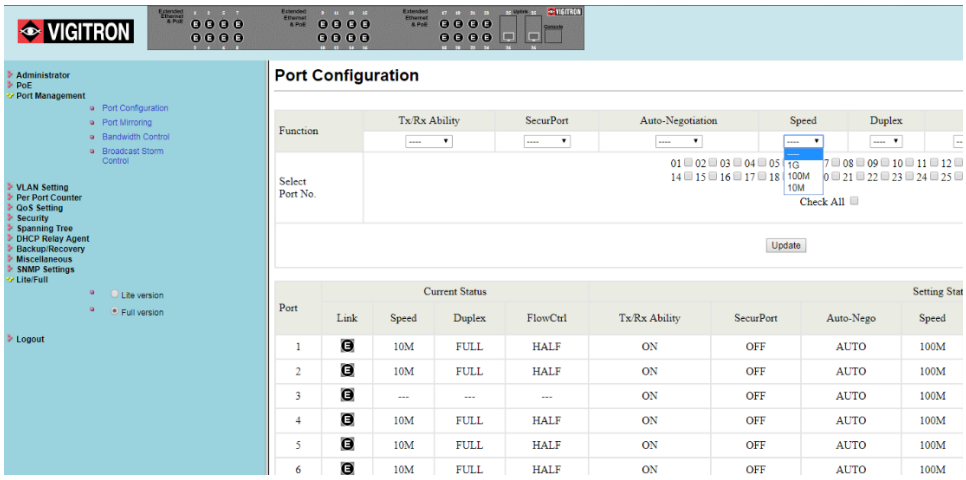
In order to restore the connection, the administrator must log on to the switch and manually enable the port. The Switch will check to see that any ports with SecurPort enabled are linked. If there is no link, the port will be disabled. IP cameras and some other devices go through an initialization process when first powered. During this process the devices will not immediately link up. Since the Switch cannot link to the device during initialization, the port will be disabled.



Auto-Negotiation:

- Enable: Speed will be Auto Negotiate based on the input.
- Disable: Speed will set by the manual setting.

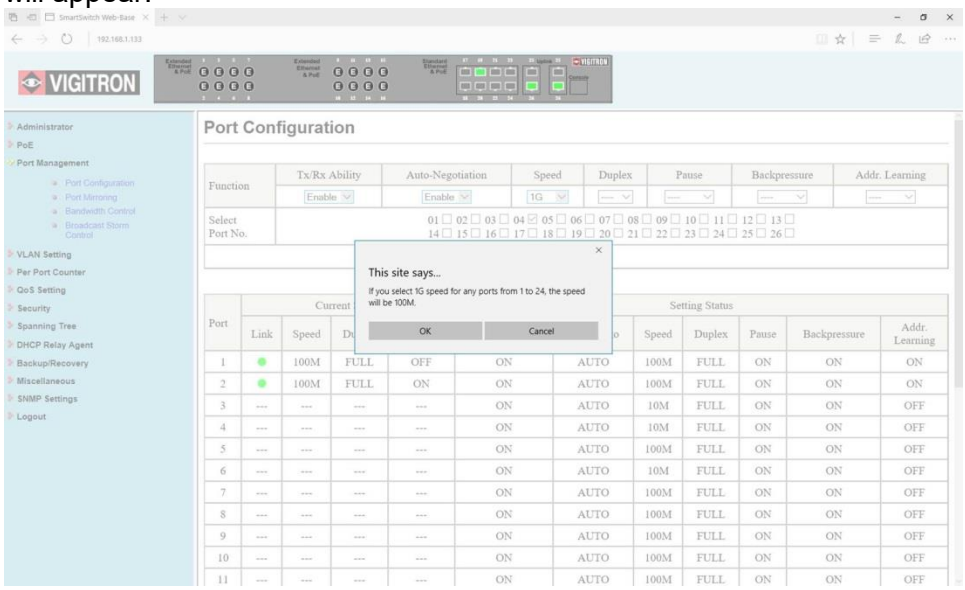
NOTE: If Auto Negotiation is select Speed Selection will not be active.

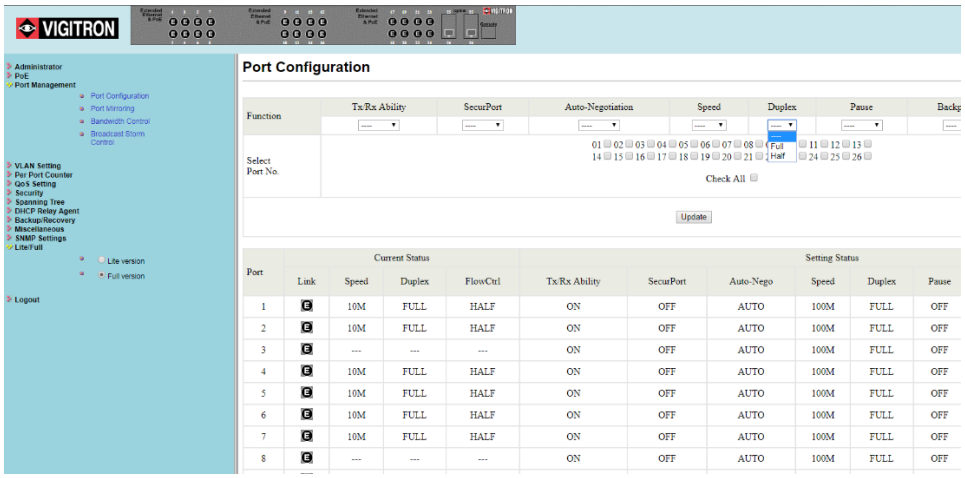


Speed:

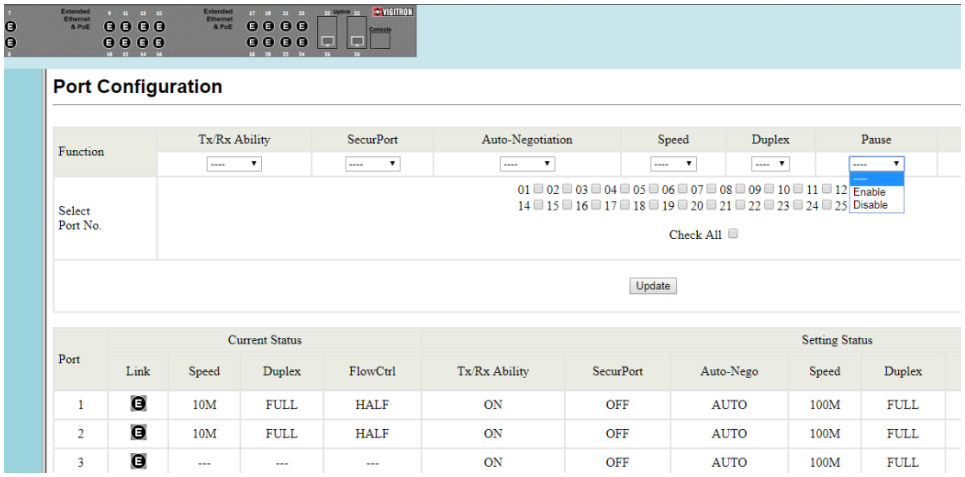
- Select 10Mbps or 100Mbps for ports 1-24.
- Select 10Mbps/100Mbps or 1000Mbps (1Gbps) for ports 25/26
- Note: For ports 25 and 26, copper ports can be set for 10/100/1000Mbps. When using fiber connections, port speed is fixed at 1000Mbps (1G).

If attempts are made to program ports 1-24 for 1G, the following popup will appear:





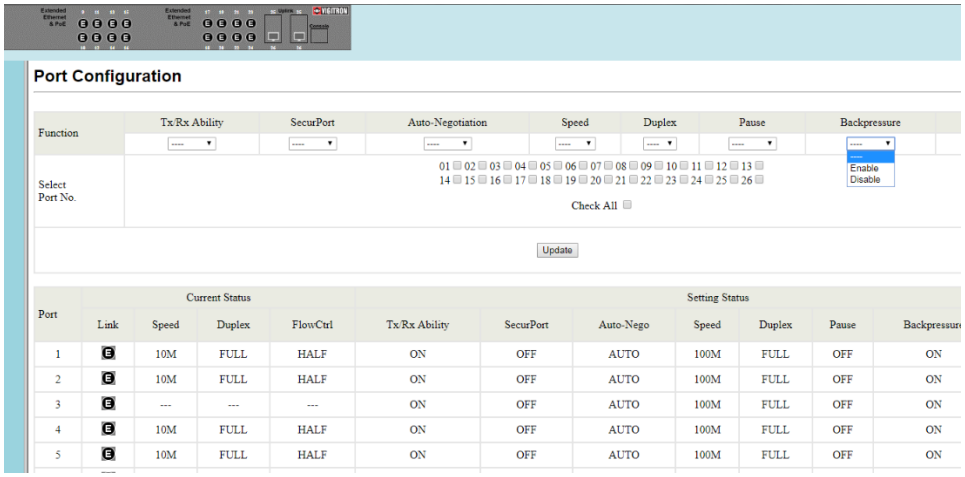
Duplex : Select Full or Half Duplex- for most application select Full.



Pause

- Enable: Responses to pause commands to prevent traffic congestion.
- Disable: disregards pause commands.

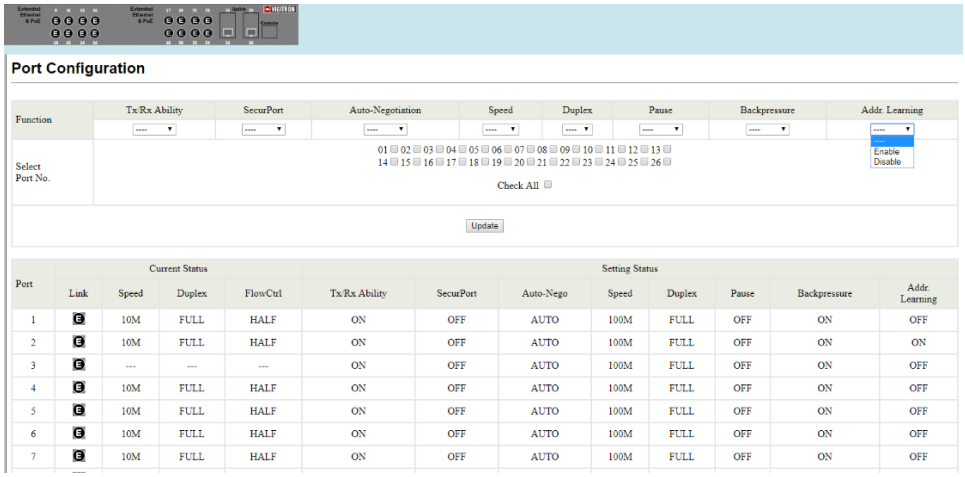
NOTE: The recommended setting is Disable as Enable will slow up traffic and may result in loss or delay of packet transmission.



Backpressure

- Enable: Prevents backpressure in half duplex mode
- Disable: Disables function

NOTE: In most applications the switch will operate in the full duplex mode so this function should be set to Disable.



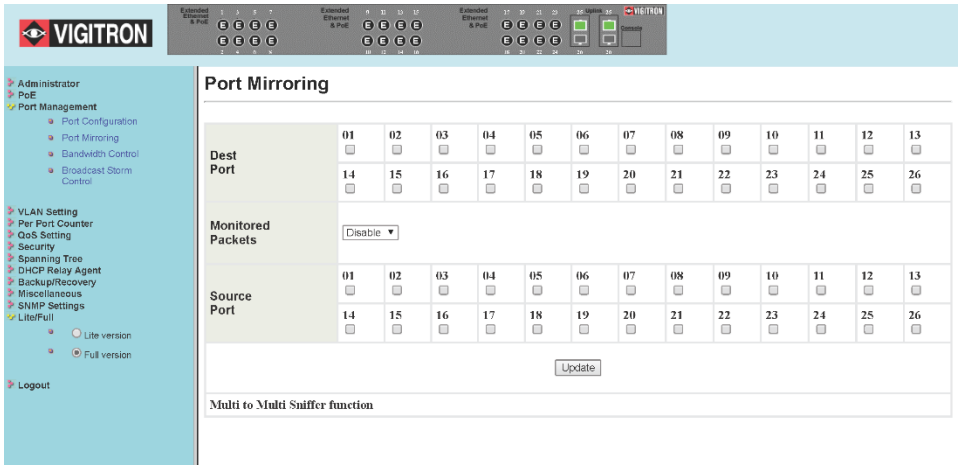
Address Learning

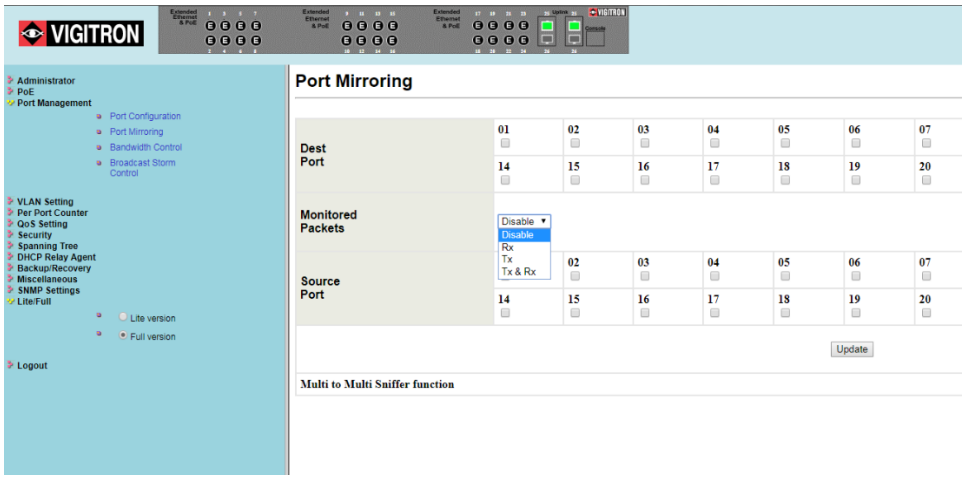
- Enable: Port will learned connected devices MAC – suggested for maintaining security between connected device and switch port.
- Disable: Connected devices MAC address is not learned.

Update: Select update to apply your programmed changes.

Status Screen: After changes are made and Update applied check the status screen to make certain these changes have taken effect.

11.1 Port Mirroring



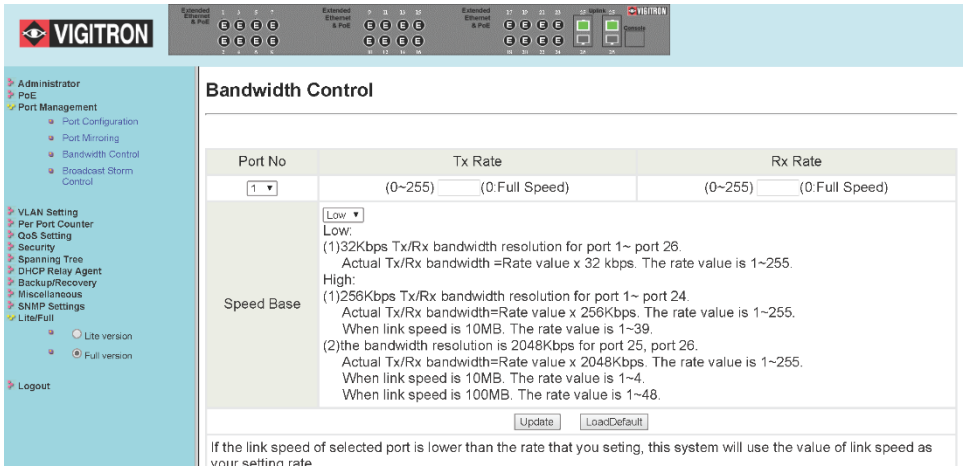


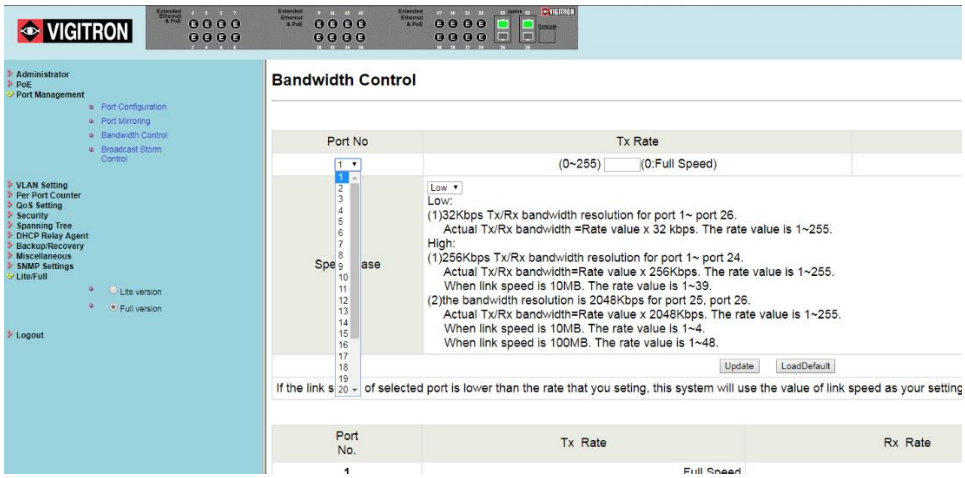
The select of ports to be mirrored is done by port priority by number. For example, if ports 1 and 2 are selected as source ports, and this is followed by ports 23 and 24, Port 1 will be mirrored at port 23 and port 2 will mirrored at port 24.

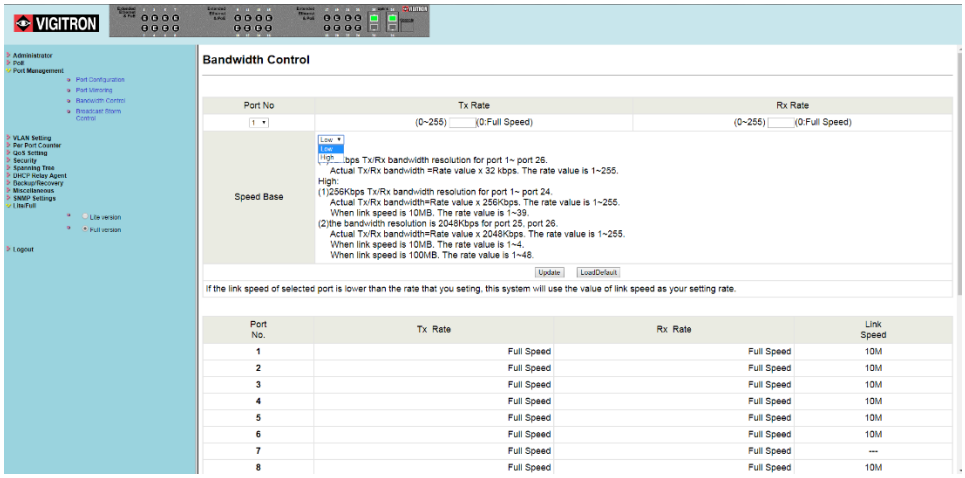
Select the mirror type:

- Disable: Mirroring is disabled on all ports.
- Rx: Only Received packets are mirrored.
- Tx: Only Transmitted packets are mirrored.
- Tx & Rx: Transmitted and Received packets are mirrored.

11.2 Bandwidth Control







NOTE: This is an override setting for the port speed (10/100Mbps for ports 1-24 and 10/100/1000Mbps for ports 25/26). If port speed set in the Bandwidth control is lower than the previous selected speed, the value will revert to that speed.

The Limitation Of The Bandwidth Control

The actual bandwidth should be less than link speed of the port. 100Mbps link speed for port 25 and port 26, the bandwidth setting should be less than 48 if the bandwidth is set to “High”. 10Mbps link speed for port 25 and port 26, the bandwidth setting should be less than 4 if the bandwidth base is set to “High”. 10Mbps link speed for port 1 ~ port 24, the bandwidth setting should be less than 39 if the bandwidth base is set to “High”.

Setting the bandwidth to “0” will make the switch running at the “Full Speed”.

This setting allows the setting of the bandwidth for each port. The Tx rate and Rx rate can be filled with the number ranging from 1 to 255. This number should be multiplied by the selected bandwidth resolution to get the actual bandwidth.

In the “Low” mode, the Tx/Rx bandwidth resolution is 32Kbps for port 1~ port 26. In the “High” mode, the Tx/Rx bandwidth resolution is 256Kbps for port 1 ~ port 24, and 2048Kbps for port 25, port 26.

Low Bandwidth for TX

Example 1: The TX number of the port1~4 is set to 10, 20, 30, 40 respectively, and Speed base is set to “Low”. The real bandwidth comes from the formula of 32Kbps*10, 32Kbps*20, 32Kbps*30 and 32Kbps*40 respectively. After the “Update” button is executed, the real bandwidth will show up in TX fields.

High bandwidth for TX

Example 2: The TX number of the port1~4 is set to 10, 20, 30, 40 respectively, and Speed base is set to “High”. The real bandwidth comes from the formula of 256Kbps*10, 256Kbps*20, 256Kbps*30 and 256Kbps*40 respectively. After the “Update” button is executed, the real bandwidth will show up in TX fields.

Low Bandwidth for RX

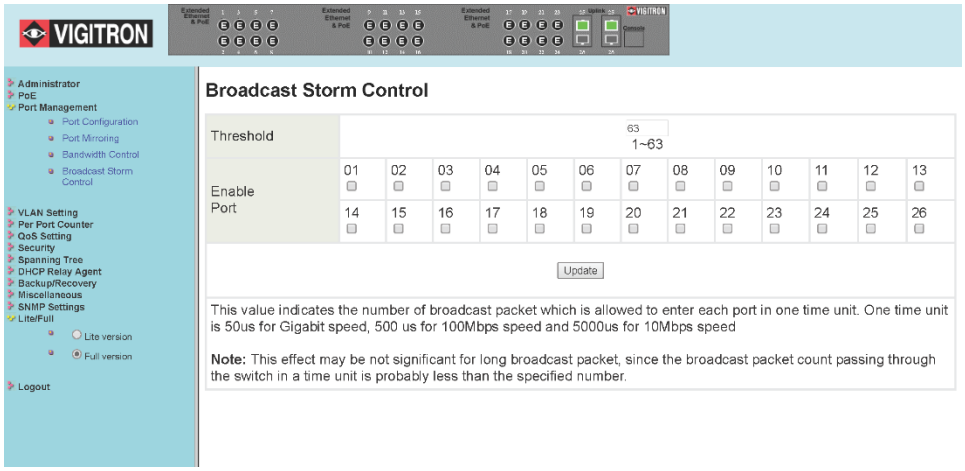
Example 3: The RX bandwidth number of the port 5~ port 8 is set to 50, 60, 70, 80 respectively, and Speed base is set to “Low”. The real bandwidth comes from the formula of 32Kbps*50, 32Kbps*60, 32Kbps*70 and 32Kbps*80 respectively. After the “Update” button is executed, the real bandwidth will show up in RX fields.

High Bandwidth for RX

Example 4: The RX bandwidth number of the port 5~ port 8 is set to 50, 60, 70, 80 respectively, and Speed base is set to “High”. The real bandwidth comes from the formula of 256Kbps*50, 256Kbps*60, 256Kbps*70 and 256Kbps*80 respectively. After the “Update” button is executed, the real bandwidth will show up in RX fields.

11.3 Broadcast Storm Control

The broadcast storm control is used to block the excessive broadcast packets received during the specified time unit. The valid number ranges from 1 to 63. The broadcast packet is only checked at the selected port and the number of broadcast packets is counted in every time unit.



There are 3 options for the selection of the time unit: 50, 500, or 5000 us as the figure shown above. Once the broadcast storm protection is enabled, the excessive broadcast packet will be discarded. For those broadcast packets incoming from the un-selected port, the switch treats it as the normal traffic.

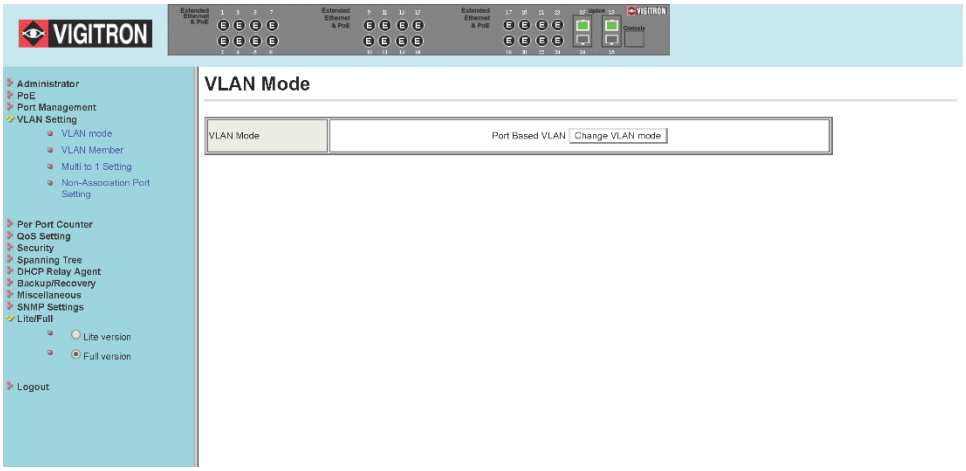
1. Threshold: Indicates the number of packets allowed during the time period based on the selected port bandwidth.
2. Enable: Select the port to apply the packet number limit to.
3. Update: Select update to apply the setting.

NOTE: If function is applied to each port, update must be used prior to setting a program for the next port. Broadcast packets incoming from the un-selected ports will be treated as normal traffic.

Section 12: VLAN Settings

12.0 VLAN Mode

The Vi32226 switch supports two VLAN modes, tag based and port based. Only one VLAN mode can be enabled at one time.



When the tag based VLAN is selected, the administrator can define the handling method of a VLAN tag to the specified port, including “Add Tag”, “don’t care” or “Remove Tag”.

Set Tagging: For each port, define the handling method. One of three methods can be selected. They are -

Add Tag: 802.1Q tag will be inserted into the outgoing packet of the selected port if the packet received by the port does not already contain one. In that case the 802.1Q tag received

Caution: Do add a tag to the port used to configure the switch and in some cases the NIC will not recognize 802.1Q

Don’t Care: The outgoing packet of the selected port will the original packet format of the source port.

Remove Tag: If the outgoing packet of the selected port receives a packet with a 802.1Q tag, it will be removed. No other changes will be made to the packet.

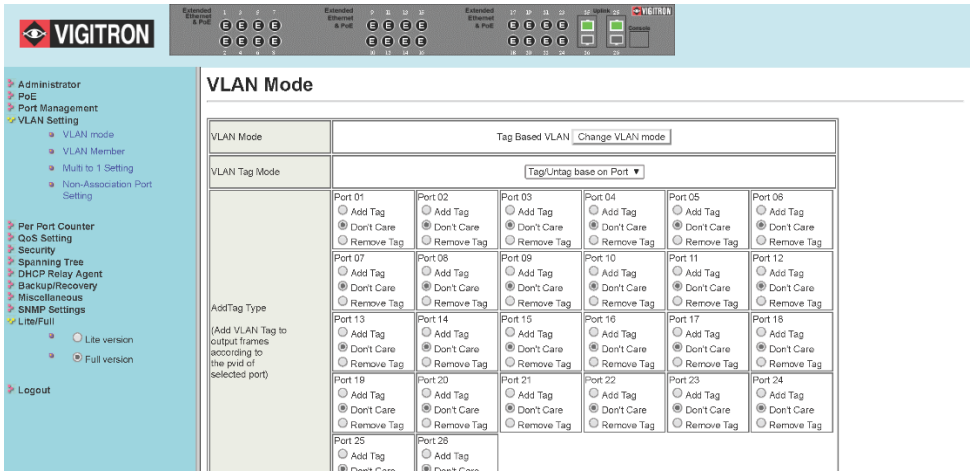
Update: After all the selections are made select “Update” to apply.

Caution: If the port you are using to monitor is not programmed at Rx/Tx or not selected as part of the VLAN, you will lose your connection to the switch and have to return to the default settings.

NOTE: In tag based VLAN mode, adding tag on the port which is used to configure this switch is not allowed, because some NICs cannot recognize 802.1Q tag.

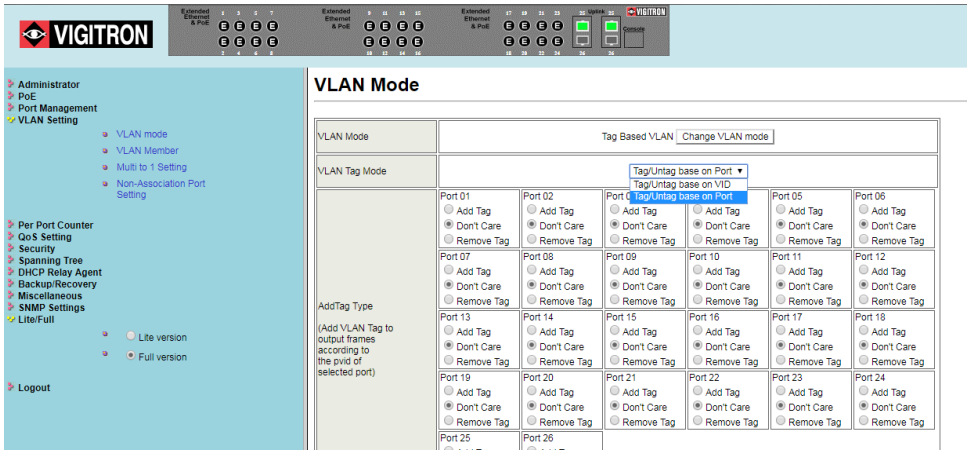
Example:
Port 1: The 802.1Q tag of every packet outgoing from this port will be removed.
Port 4: The 802.1Q tag of every packet outgoing from this port should be included.
Other ports: keep every outgoing packet intact.

12.1 VLAN Member (Port Based)



This setting is designed based on the VLAN member of each port. The following examples illustrate how to configure VLAN in this mode.

The Table is configuring the port-based VLAN member of each port. When the port received the packets allows only forwarded to the VLAN member of this port. The function for each button shown on this page is expressed below.



Name: Enter a name for your VLAN – maximum of 8 characters.

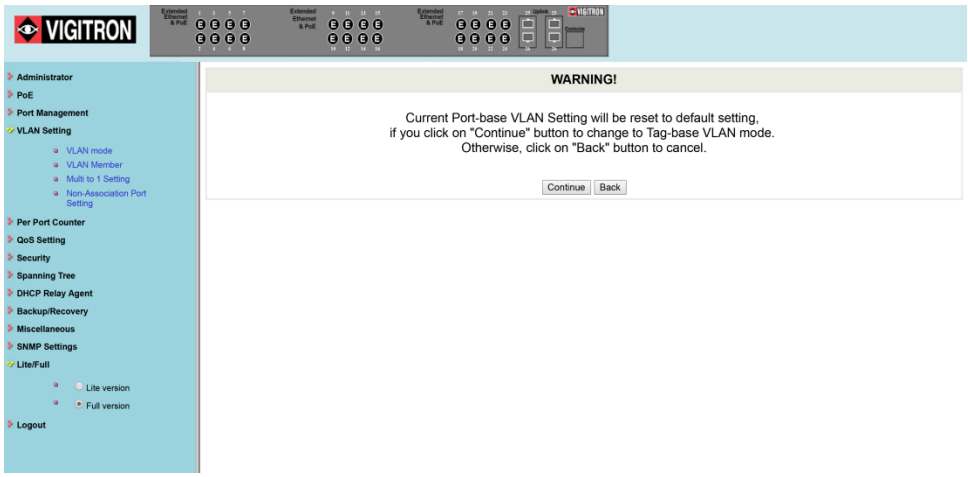
Destination Ports: Select all the port what will be part of the VLAN.

Update: Select Update to confirm your port selections.

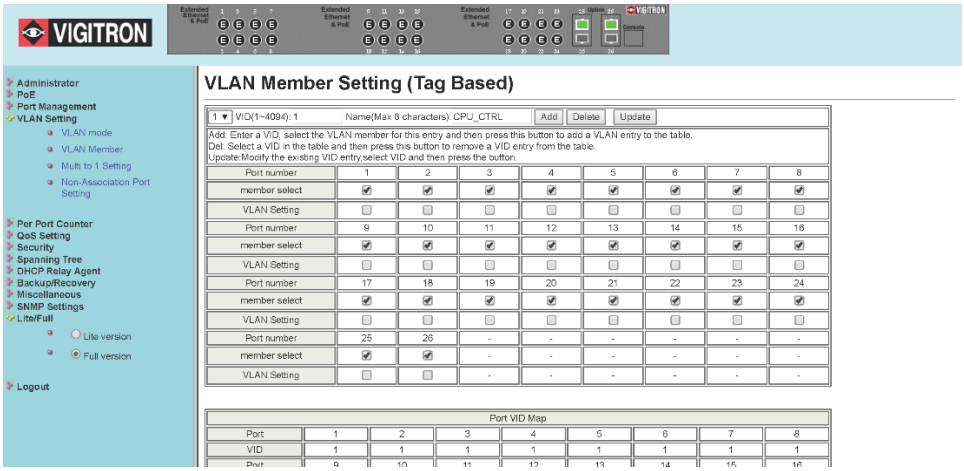
Load Default: If you need to return to the Default setting, select Default.

In the above example:

Port 1 has been selected as the Read Port.
Port 1 received packets can be forward to Ports, 2, 3 and 4.
Port 2 received packets can be forwarded to Ports, 1, 3 and 4.
Port 3 received packets can be forwarded to Ports, 1, 2.



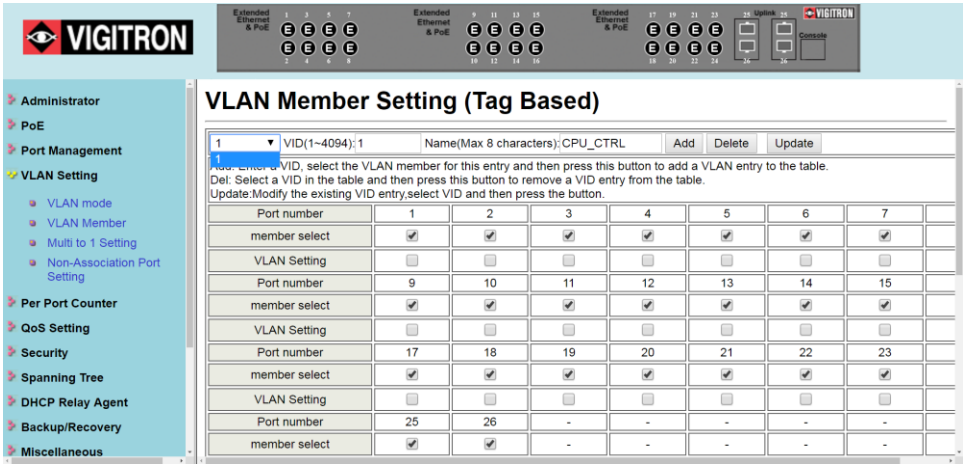
12.2 VLAN Member Settings (Tag Based)



NOTE: This web page allows the administrator configure to Tag-base VLAN member of VID table of 32-entry and Port VID(PVID) source index of each Port.

When a tagged packet is received, the Switch compares the tag in the packet with the one defined in the VID table. The setting will be reflected at VLAN MEMBER window.

When an un-tagged packet is received, the Switch searches for the PVID source index. This PVID will be inserted to the received packet and then it will be forwarded to the destination port according to the VLAN membership corresponding to this PVID. The setting will be reflected at Port VID Map window.



The function for each button shown on this page is expressed below.

Add a VLAN: (Tag Based): Enter a VID (number 1 to 4094) and select a VLAN source port, followed by entering a group name. Select the ADD button to add the VLAN to the list.

Delete a VLAN: Select a VLAN from the Select button and press Delete to remove it.

To add a group: Select more than one port.

Modify a VLAN: Select a VID that you want to modify from the Select drop down. Once the web page is displayed make your modifications and press the “Update” button.

Step 1: Select/De-select the VLAN ID.
Step 2: Select/De-select VID source corresponding to this VID.
Step 3: Press “Update”.

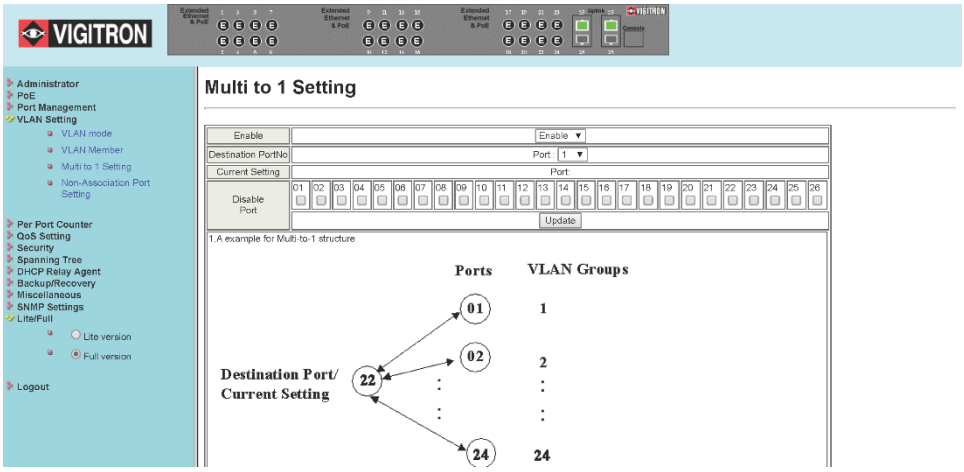
NOTE: The CPU control entry cannot be removed.

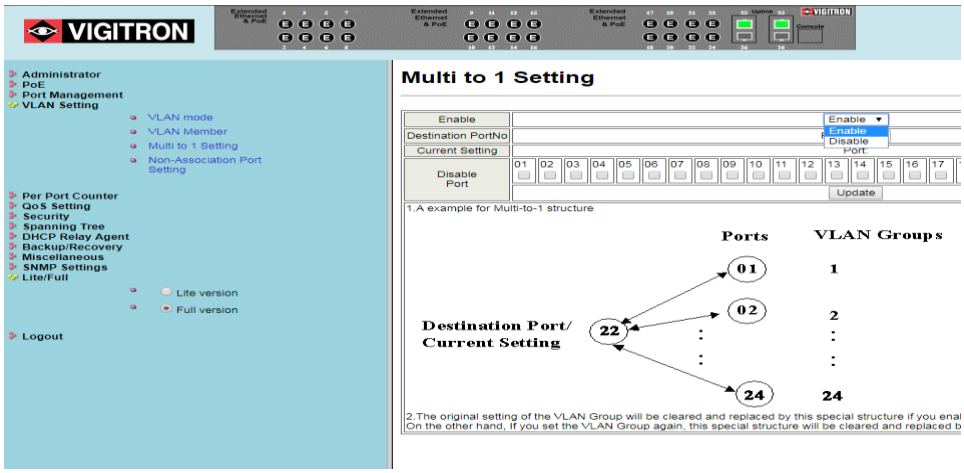
12.3 Multi to 1 Setting

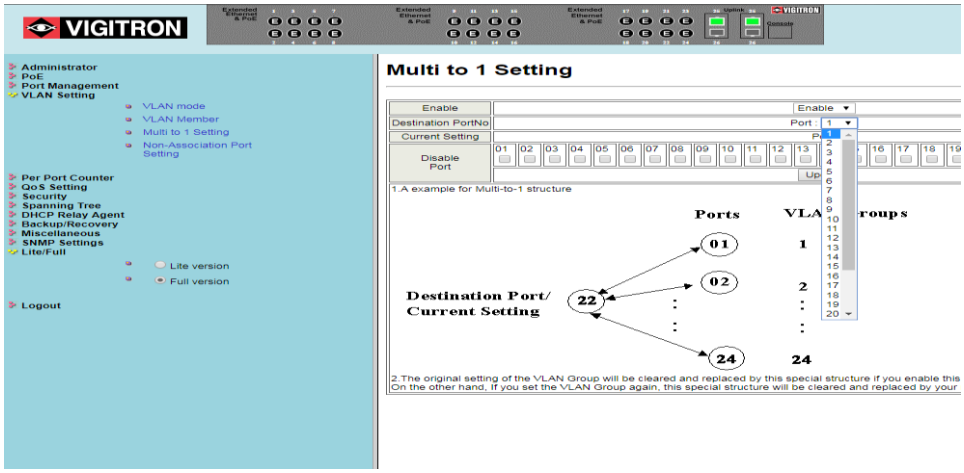
Multi-to-1 VLAN is used in CPE side of Ethernet-to-the-Home and is exclusive to VLAN setting on ”VLAN member setting“. In the other words, once multi-to-1 is set, the previous VLAN setting will be overridden.

The “disable port” means the port which will be excluded in this setting. All ports excluded in this setting are treated as the same VLAN group.

In the following example, port 3, port 4, port 6, port 7, port 8 and port 9 are excluded in this VLAN Furthermore these ports are treated as the member of other VLAN. All ports which are not specified in this table only communicate with port 1.







CAUTION: This setting will over ride other VLAN settings.

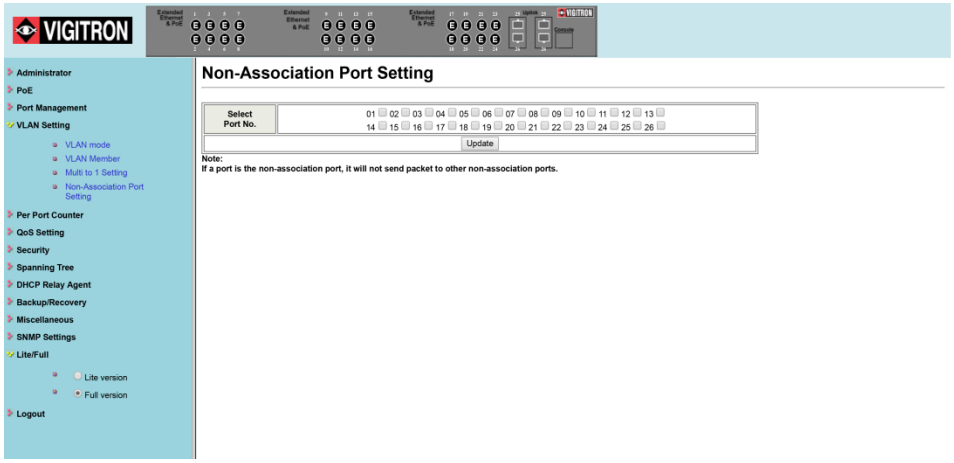
Select the Destination port:

- Select port to be excluded:
- Select the ports excludes them form the VLAN and can be used for other VLANs.
- Select “Update”.

NOTE: All ports which are not excluded will be part of the VLAN.

12.4 Non-Association Port Setting

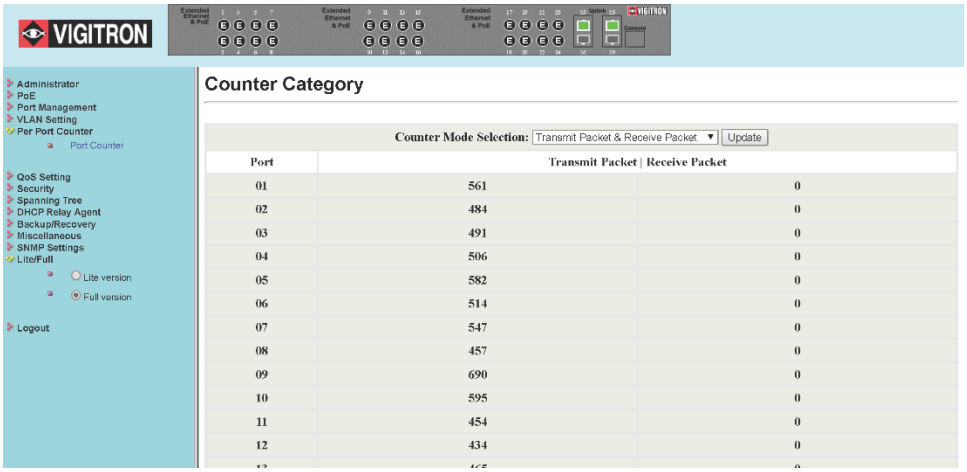
Selecting the non-association Port will not send packets to other non-associated port.

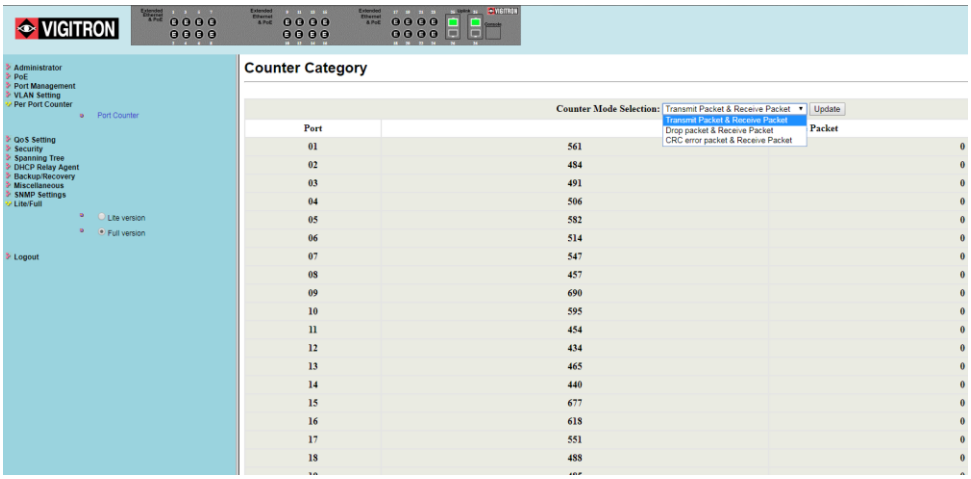


Section 13: Per Port Counter

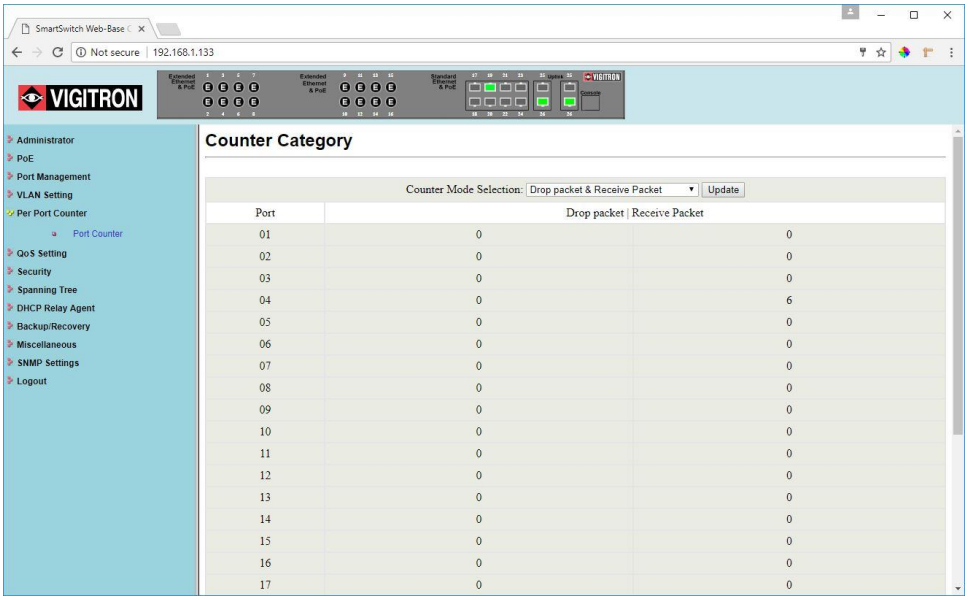
There are three modes. Selecting the mode will display the Transmit and Receive Packets.

13.0 Transmit Packet and Receive Packets

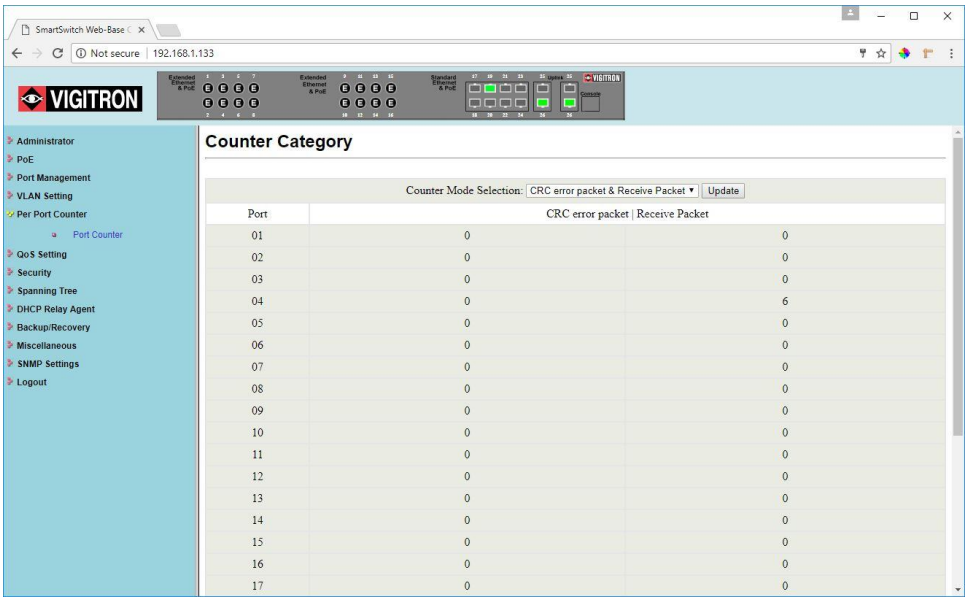




13.1 Drop and Receive Packet



13.2 CRC error packet and Receive Packet



13.3 Counter Modes Defined

The 3 different operational modes are:

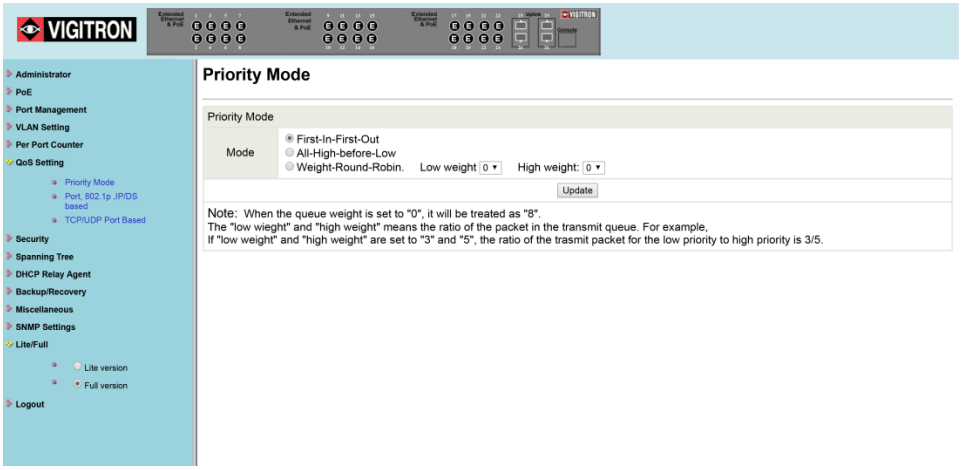
Field	Description
Transmit Packet & Receive Packet	This category shows both the received packet count (excluding the incorrect packet) and the transmitted packet count.
Drop Packet & Receive Packet	This category shows the number of received valid packet and the number of dropped packet.
CRC error Packet & Receive Packet	This category shows the received correct packet and received CRC error.
Refresh	Press “Refresh” button will aggregate the number of the counter for all ports.
Clear	Press “Clear” button will clear all counters.

Switching between modes will clear the previous counter. Entering a mode will update the counter.

Section 14: QoS Settings

14.0 Priority Mode

This setting allows the administrator to set the scheduling mode for the TX packets at each port.



14.1 Setting the Priority Mode

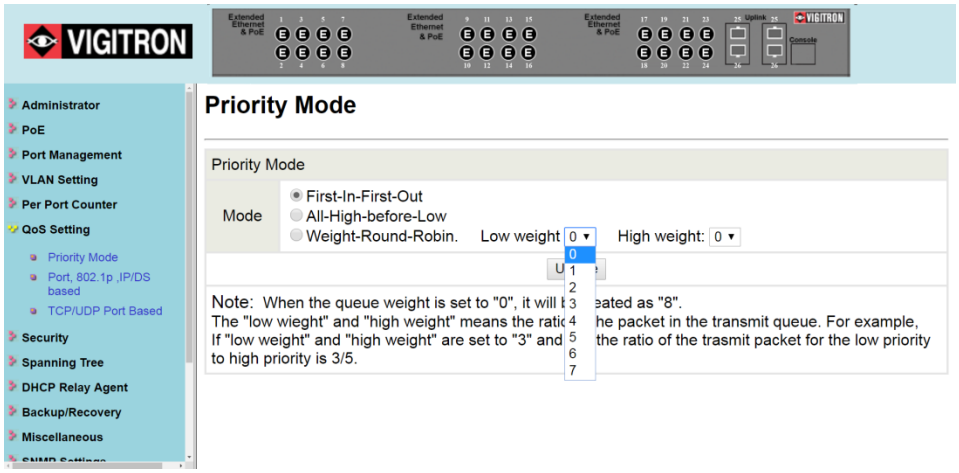
This setting sets the scheduling mode for Transmission packets for each port.

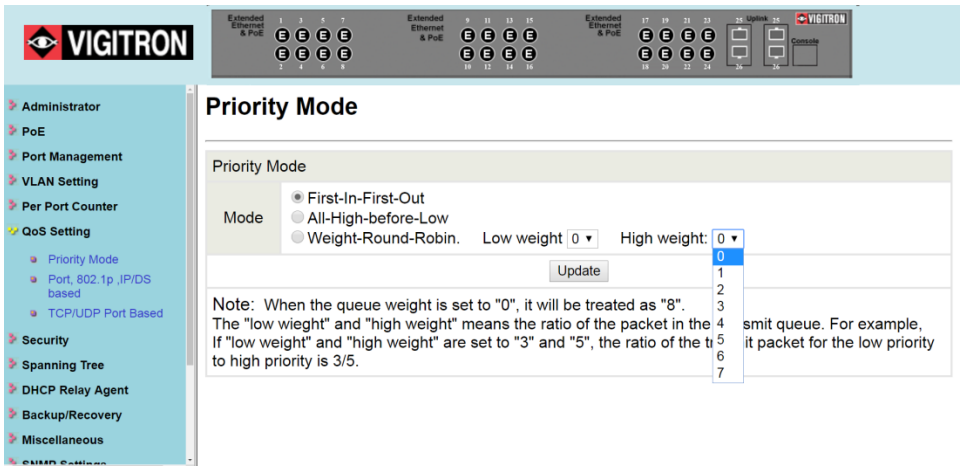
Field	Description
First-In-First-Out (FIFO)	All output packet are queued to one queue, first comes first out.
All-High-before-Low (Strict priority)	All packets will be assigned to either high priority queue or low priority queue. The low priority packet will not forwarded until the high priority queue is empty.
Weight-Round-Robin (WRR)	There are 2 priority queues for Weighted-and-round-robin (WRR) mode. When this mode is selected, the traffic will be forwarded according to the number set in each queue. The queue ID has nothing to do with the priority.

- Selection of the Low and High weight set up ratios of Low/High.
- Selecting “0” will result in a 8 number setting.

The numbers indicate the how packets are treated in sequence at each port so if the ratio is 3 Low/ 5 High, the sequence will be 5 packets will be stored in high followed by 3 packets stored in low, etc.

Example: If High, Low queue are set to 5, 3, then the traffic at the specific port will go out in the following sequence. 5 packets stored in High queue, 3 packets stored in Low queue, 5 packets stored in High queue, 3 packets stored in Low queue.





14.2 Class of Service Configuration

There are 4 types of CoS for this setting; ie, TCP/UDP port number, IP TOS/DS, 802.1p priority tag and physical port. The administrator can select more than one item for each port.

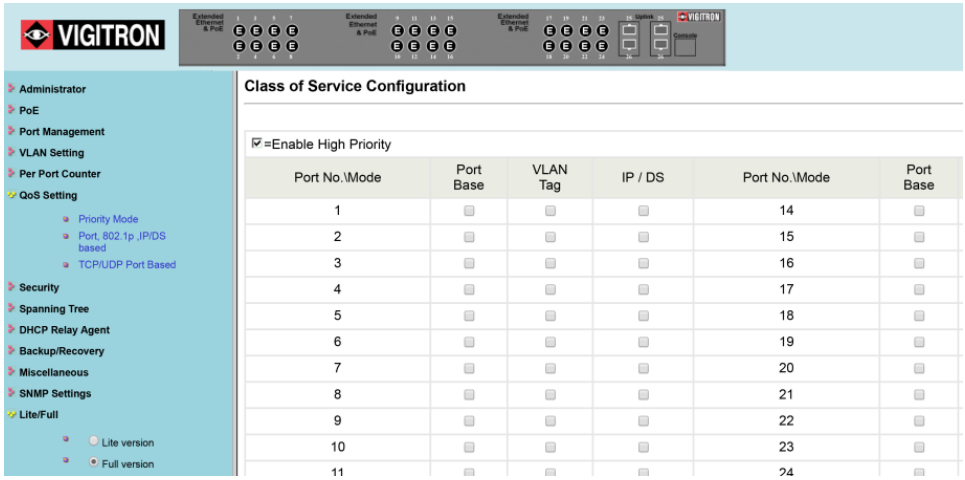
Please note that if more than one type of CoS is selected, the switch will arrange the packet to the assigned queue according the following priority:

1. TCP/UDP port number.
2. IP ToS/DS.
3. 802.1p priority tag the third and physical port the last. This means TCP/UDP port number will override other CoS setting.

The rule is: TCP/UDP > TOS/DS > 802.1p > Physical

For 802.1p priority tag, the following table is used to map the 802.1p field to the priory queue.

Priory Field	Priority Queue
4,5,6,7	High
0,1,2,3	Low

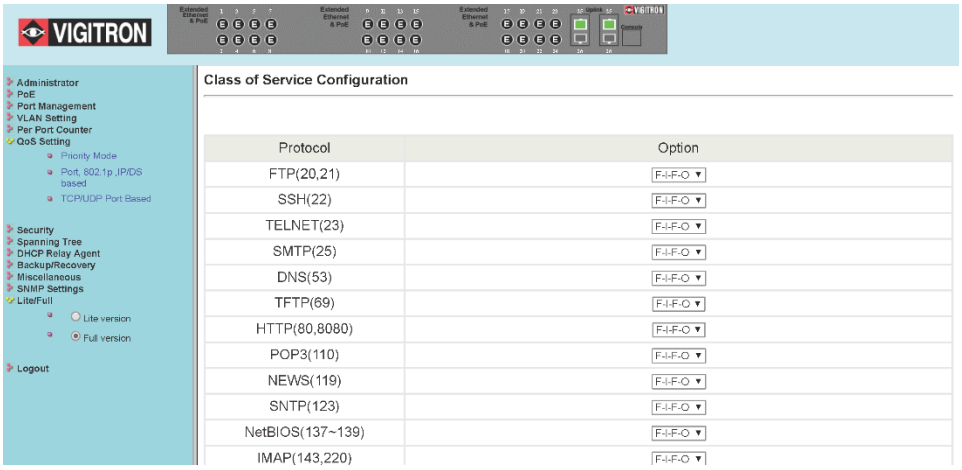


Class of Service Configuration (CoS)
Define CoS:

- TCP or UDP- port number.
- IP TOS/DS.
- 802.1p Priority Tag.
- 802.1p Physical Tag.
- Select the require tag(s) and update.

The administrator can select the protocol that will be forwarded as the specified mode. There are 3 administrator-defined UDP/TCP port groups and many well-known TCP/UDP ports. The administrator-defined port number may be a range or a specific number, depending on the mask.

The operating theory for all 4 CoS types can be illustrated by the following figure and table:



TCP/UDP CoS, IP TOS/DS, 802.1p are global setting for all ports and has no relation with the physical port.

An example of the settings are:

- **Priority Mode:** WRR. High weight=4; Low weight=2
- **TCP/UDP CoS:** P2 FTP =>High queue; P5 SMTP => Low queue
- **TOS/DS setting:** P5 TOS 6'b010010=High queue; P2 TOS 6'b100010=Low queue
- **802.1p:** P2 802.1p = 6(High queue); P5 802.1p =1(Low queue)
- **Physical port:** P5=High queue; P2=Low queue

NOTE: TCP/UDP uses port number 0-65536; however, only the port numbers of 0 to 1024 are used for what are called privilieged services which the most commonly used.

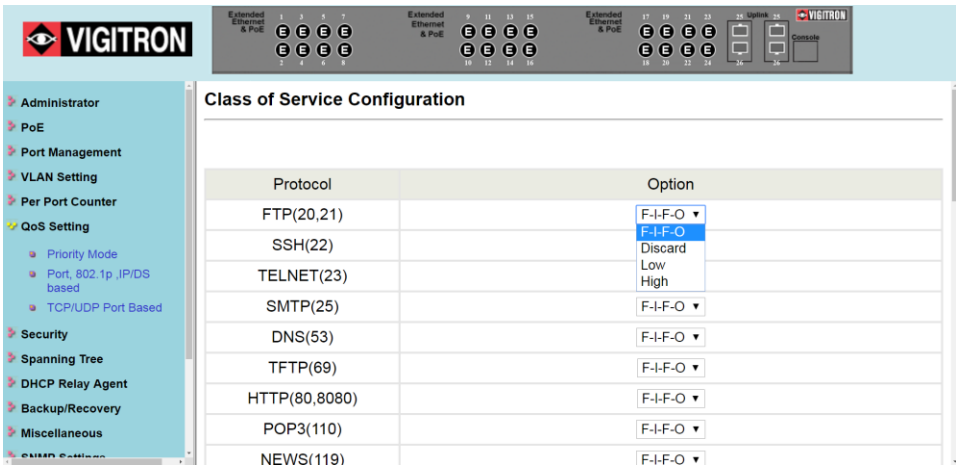
More than one can be selected. In that case the switch will arrange the packet to the assigned queue in the following priority:

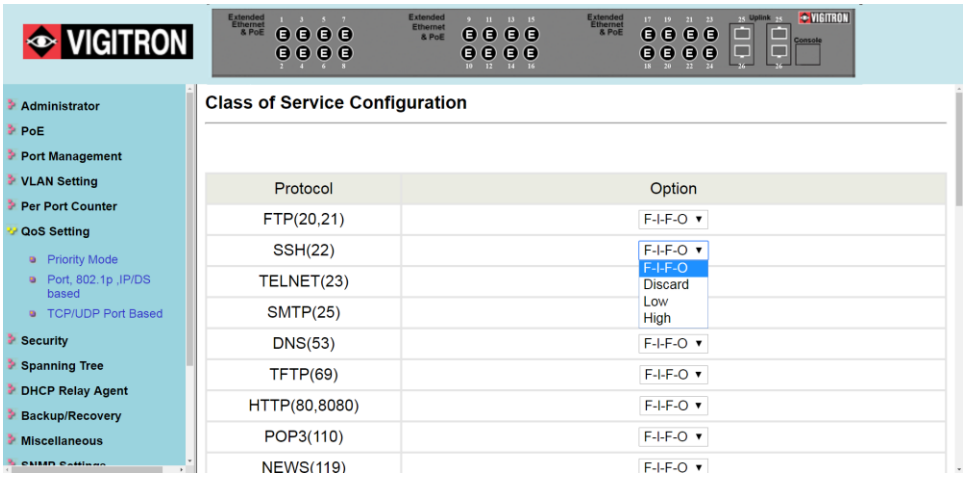
- TCP/UDP port number.
- IP ToS/DS.
- 802.1p priority tag.
- 802.1p physical port.

NOTE: TCP/UDP will over ride all other settings.

If 802.1p priority tag is use the following 802.1 field will be used to set the priority queue:

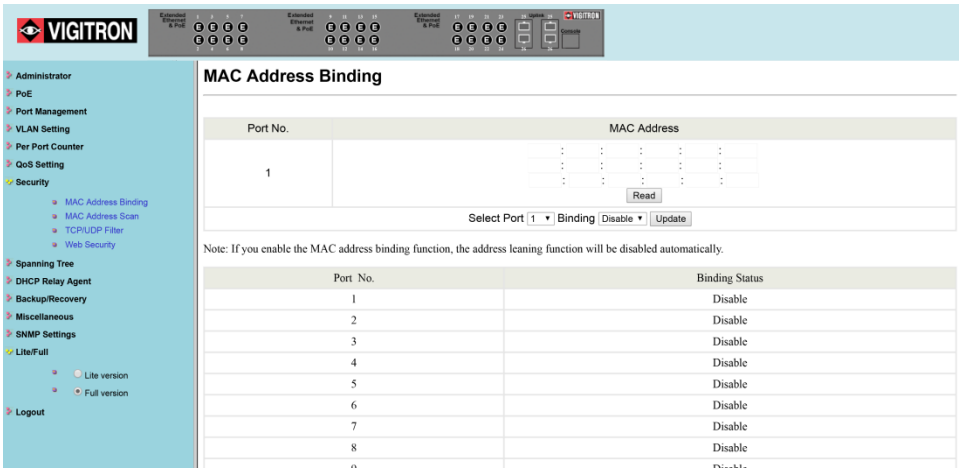
- Priority Fields 4,5,6, and 7 are High Priority.
- Priority Fields 0,1,2, and 3 are Low Priority.
- For IP TOS/DS priority, there are 7 kinds of TOS field can be assigned to High or Low queues. i.e; 6'b101110, 6'b001010, 6'b010010, 6'b011010, 6'b100010, 6'b110000 and 6'b111000.
- Setting each will define the ratios applied, however the order of priority will remain as:
- TCP/UDP>TOS/DS>802.1p>Physical.

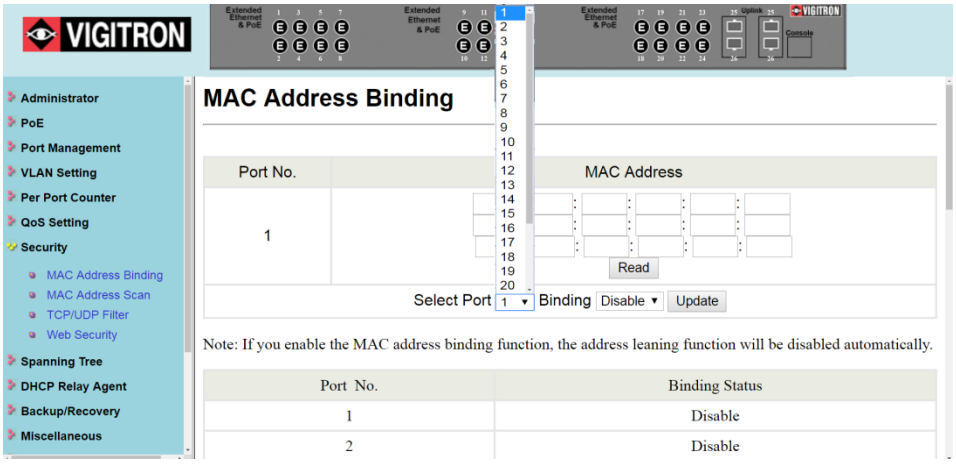


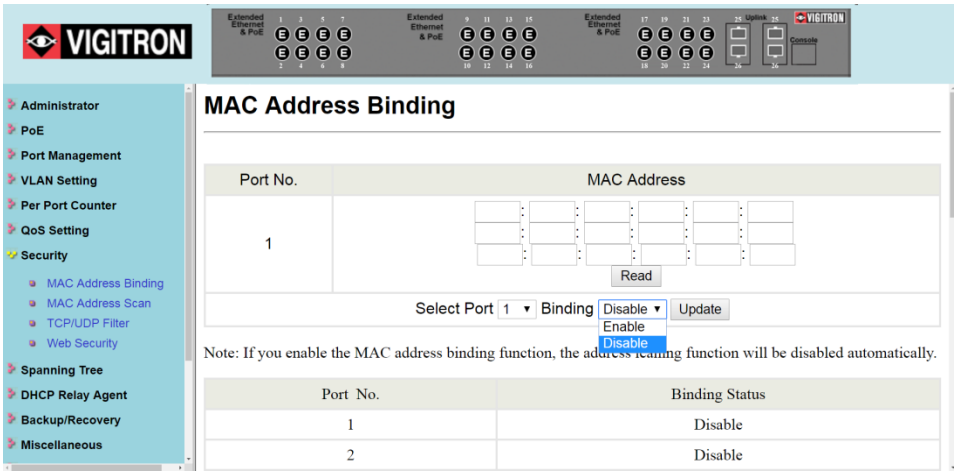


Section 15: Security

15.0 MAC Address Binding







MAC Address Binding: This feature establishes a specific relationship between the switch's physical port and connected device's MAC address. Only the packets from the assigned MAC address can be transmitted to

the connected port. Up to three MAC addresses can be assigned to each port.

- Select the Port.
- Enter up to three MAC addresses.
- Enable Read.
- Enable Binding.
- Select UpDate.

NOTE: If the MAC address binding function is enabled, the address learning function if selected will be disabled.

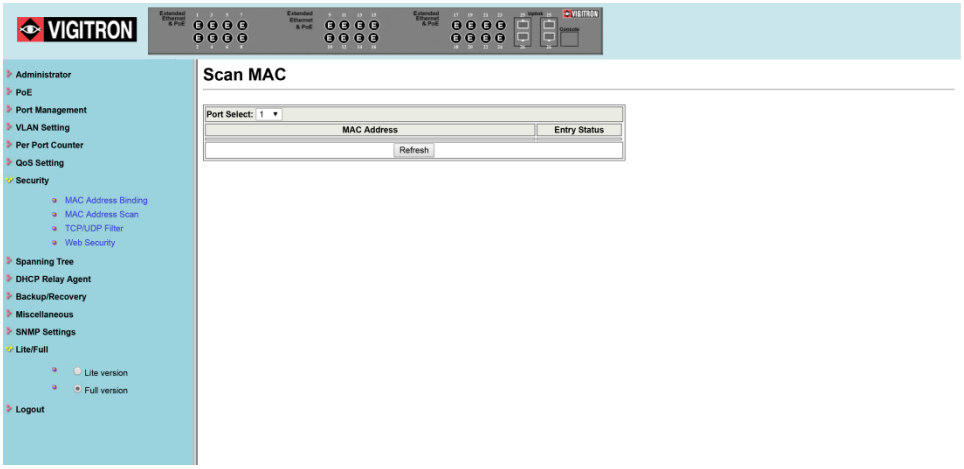
WARNING: Setting multicasting addresses to these fields is not allowed.

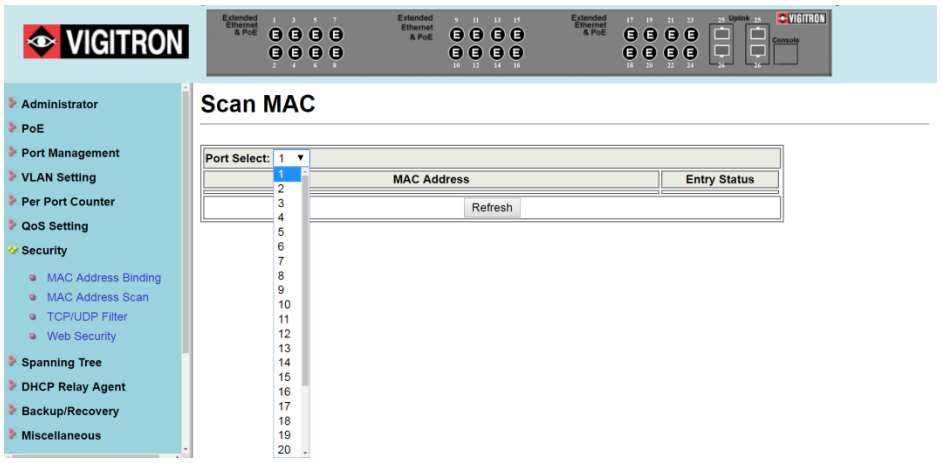
To activate the port binding function, you should enter the correct MAC address, select the port number, and set the port binding to “Enable” and then press “Update”.

Port access will be limit to only those MAC address. It is important that the correct MAC address associated with the port be entered.

Caution: Once you bind a device’s MAC address to a port, only that device will be allowed to connect. If an unbound device is connected to a bound port, the link light will be active but no information will be transmitted.

15.1 Scanning MAC Addresses





15.2 Securing Ports Using Mac Addresses

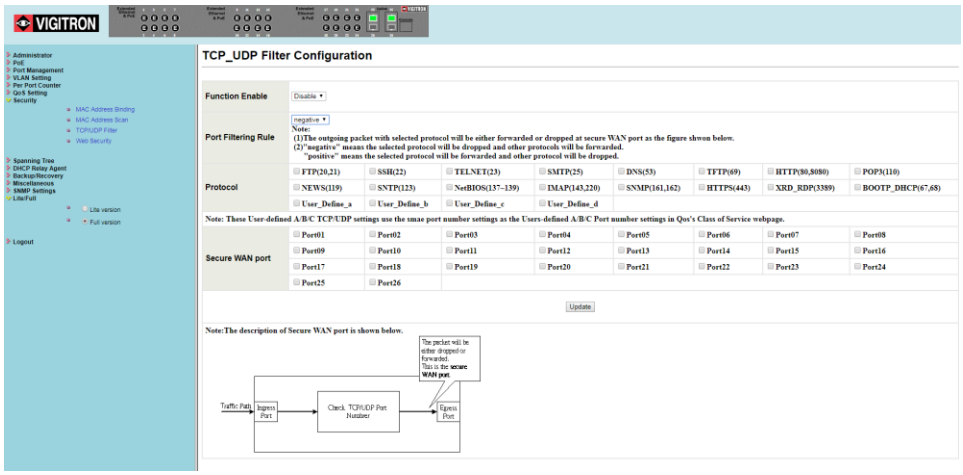
If no MAC address is entered when the scan is peformed, the MAC address of the connected device will be displayed and the “Entry Status” will show “Dynamic” indicating the addres can change, depending on the MAC address of the device.

If you have the “Binding Mode” is active and you have hard coded in a device’s MAC address, no other device will be allowed to connect to that port securing communications between that port and its connected device.

Disabling “Binding” will switch from the static mode to the Dynamic Mode.

15.3 TCP/UDP Filter

By selecting the TCP/UDP port, the network administrator can optionally block some specific applications. There are two kinds of protocol filter functions. The ”positive” function makes the switch forward the selected protocol and drop other protocols. The ”negative” function makes the switch drop the selected protocol and forward other protocols. The protocol is checked at the secure WAN port and it should be set at the server side.



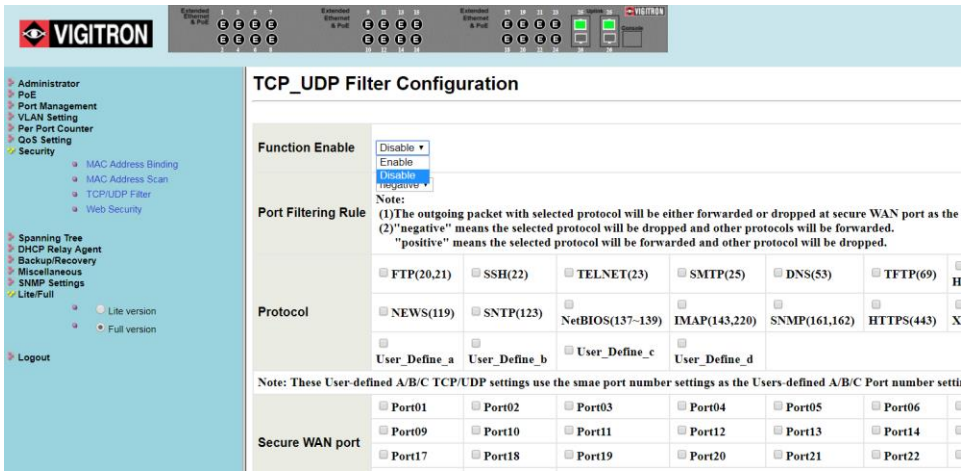
The figure shown below illustrates how this function is applied to the real environment.

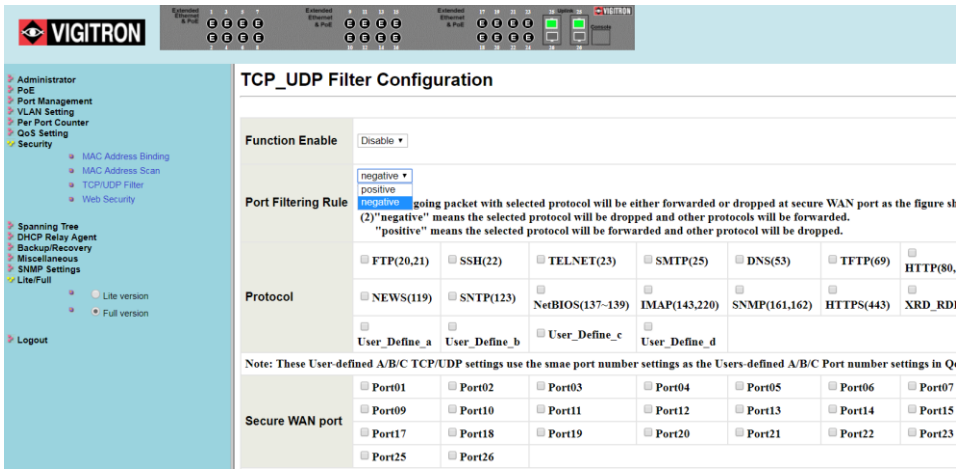
Example:

(a) Enable TCP/UDP Filter function.
(b) Select “positive” rule.
(c) Set port 5 as secure WAN port and select FTP and TELNET as the filtering protocol.
(d) Place the server of the selected protocol at the secure WAN port.

Results

Physical Port	The Behavior of Switch
Port 5	TELNET and FTP will be forwarded. Other protocol will be discarded.
Other ports	All protocol will be forwarded as the normal packet.





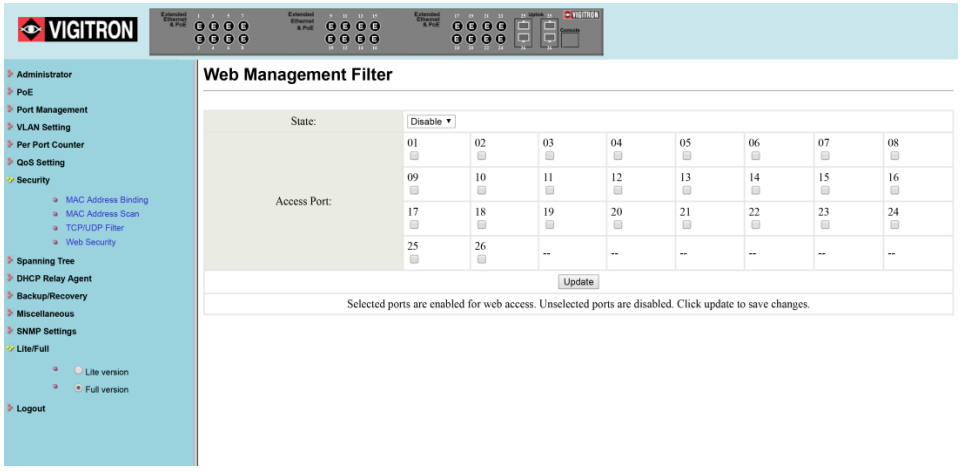
TCP/UDP filter: This feature is used to block specific applications when the switch is connected to a WAN. It is also recommended a similar setting be made at the server side.

Function Enable: Enable/Disable function.

Port Filtering Rule:

- Negative: Select packet(s) will be dropped- others are forwarded.
- Positive: Selected packet(s) are forwarded- others dropped.
- Protocol: Select the protocol(s) (Note there are 4 User Defined).

15.4 Secure WAN Port: Select the port to be secured



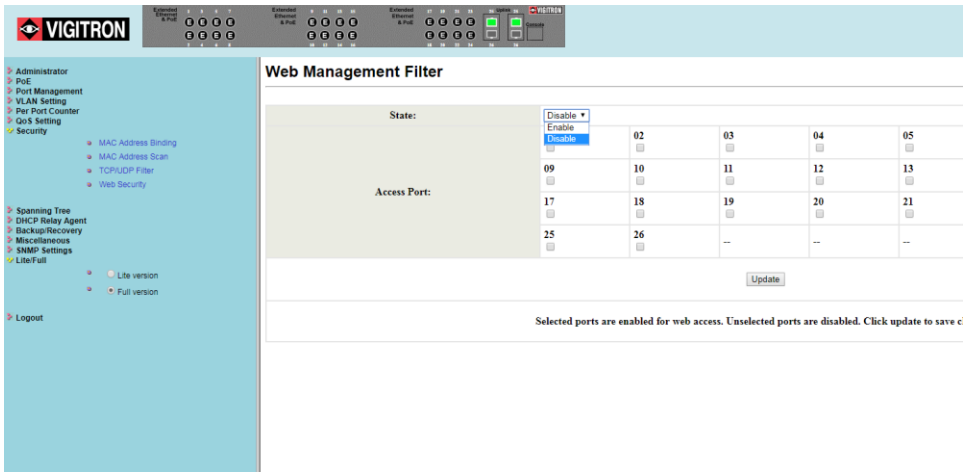
Web Management Filter:

This function blocks access to the switch's GUI preventing the ability to change settings. You will not be able to block the current port which is used to set up and monitor the switch.

Select “Enable” or “Disable the function”.

Select the port that will allow access to the web pages for programming or viewing switch status.

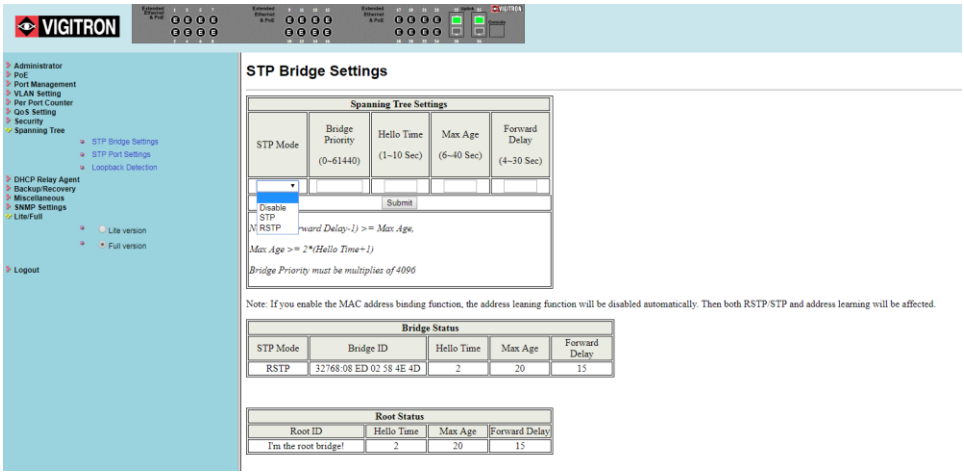
Select “Enable/Disable function”.



Section 16: Spanning Tree

16.0 STP Bridge Settings

The parameters concerning the configuration of RSTP/STP bridge are described below.

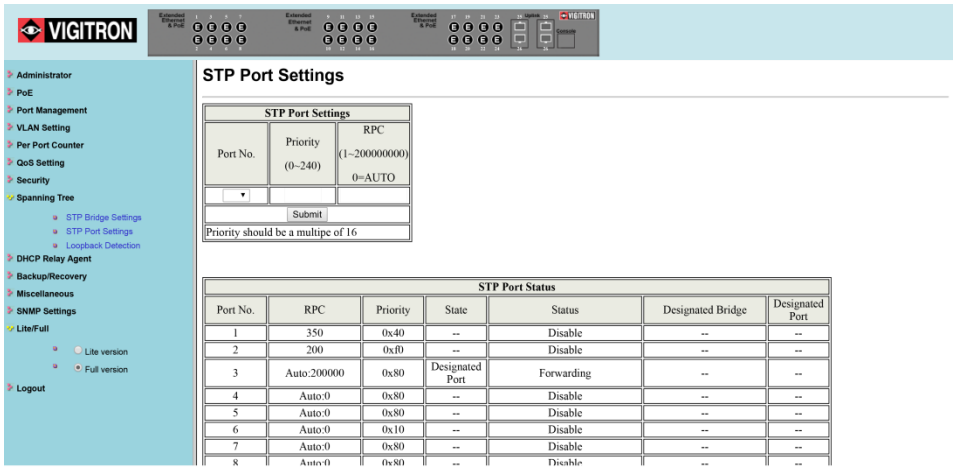


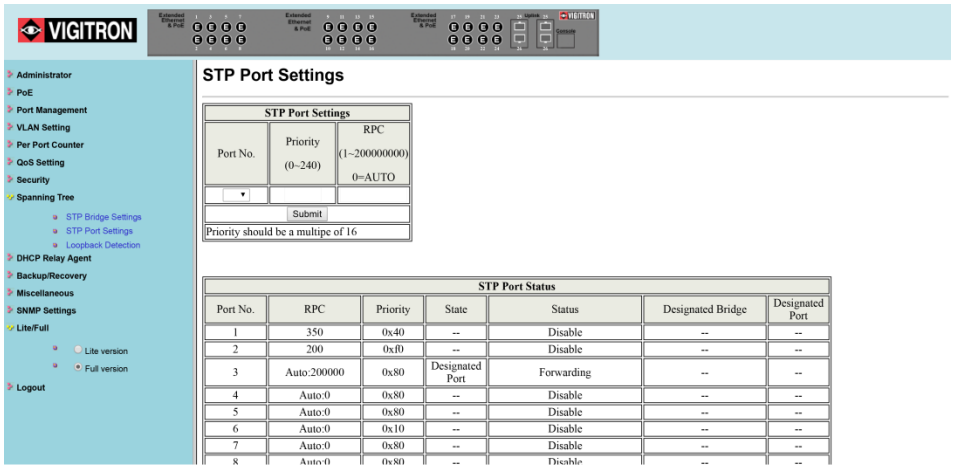
Field	Description
STP Mode	Disable: Disable RSTP/STP. STP: Enable STP function. RSTP: Enable RSTP function, including STP.
Bridge Priority	This field in conjunction with the MAC address forms the Bridge ID. The lowest number of the Bridge ID in a Spanning Tree domain will be selected as the root. Enter a multiple of 4096 this field.
Hello Time, Max Age, and Forwarding Delay	These fields control how this device handles BPDU. The relationship of these fields is listed below.

NOTE: 2*(Forward Delay-1) >= Max Age, Max Age >= 2*(Hello Time+1).

16.1 STP Port Settings

This web page provides an interface for the administrator to set the STP/RSTP port configuration.

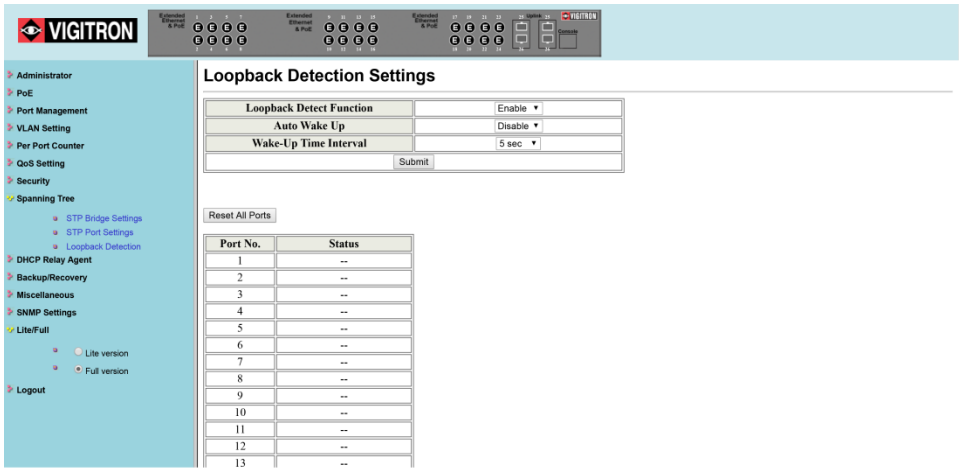


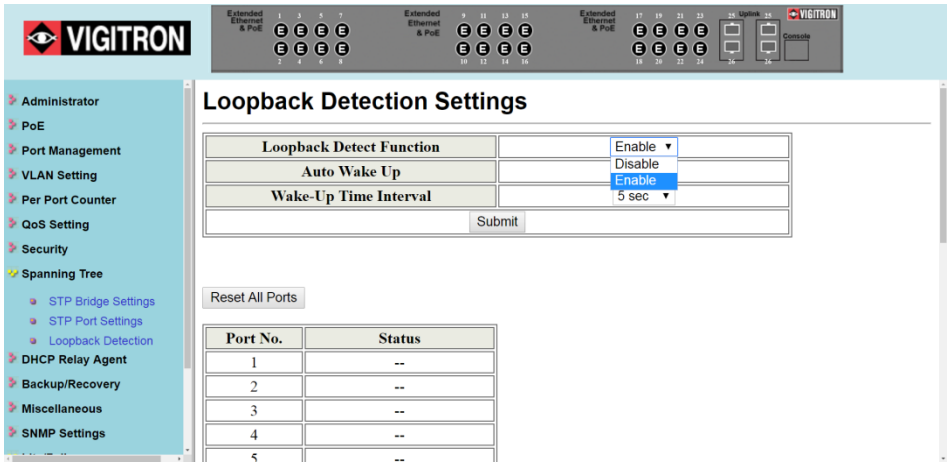


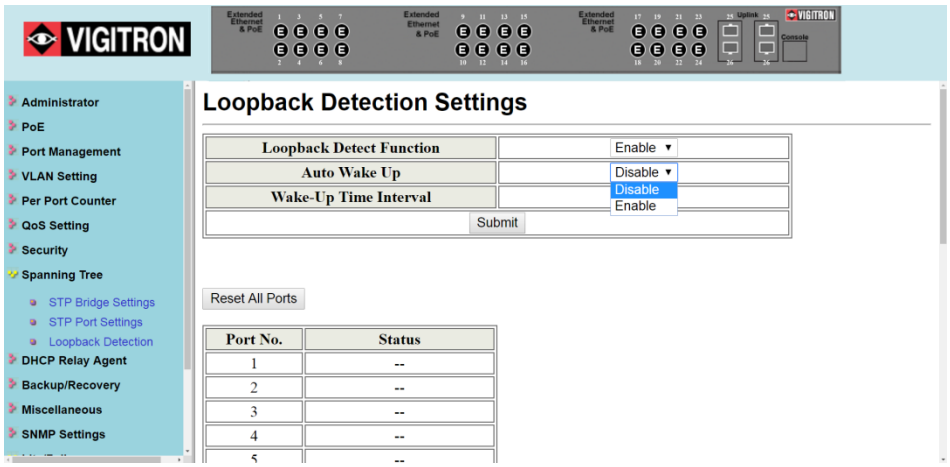
Field	Description
Port No.	To configure the parameters of RSTP/STP port, the administrator should select a physical port number, assign a priory number, enter the RPC and then press “Submit” button.
Priority (0~240)	Priority field defines the priority of the RSTP/STP port. The lower the number is, the higher possibility it will become a root port. There is a default value for each port.
RFC (0~200000000)	RPC stands for “Root Path Cost”. The higher the cost is, the lower possibility it become a root path. In the general case, the physical port with the higher bandwidth will be assigned a lower cost.

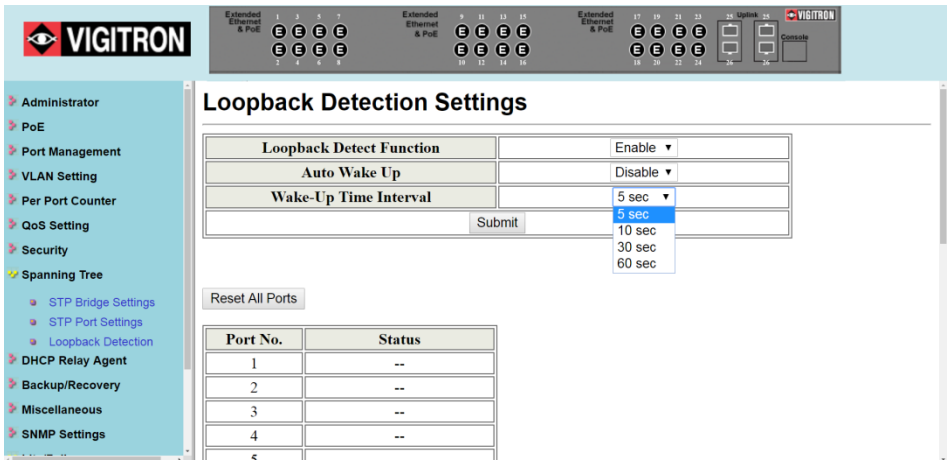
16.2 Loopback Detection Settings

This web page provides loopback detection function. When loopback detection function is enabled and a port received its own BPDU, the detection agent drops the loopback BPDU and places the interface in discarding mode. This loopback status can be released automatically, if auto wake up function is enabled.







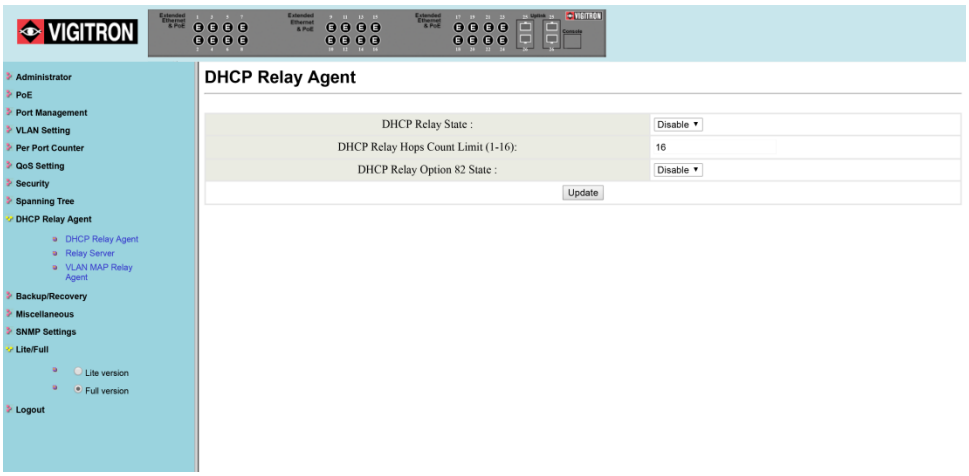


Field	Description
Loopback Detect Function	Enable/Disable the loopback detect function.
Auto Wake Up	Enable/Disable auto wake up for loopback detection of each ports.
Wake-Up Time Interval	Set auto wake up time value.

Section 17: DHCP Relay Agent

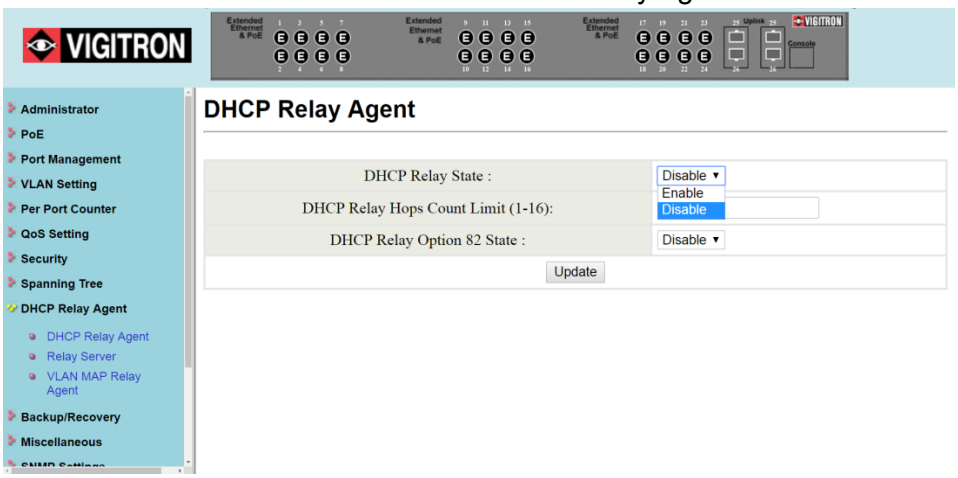
17.1 Relay Agent Configurations

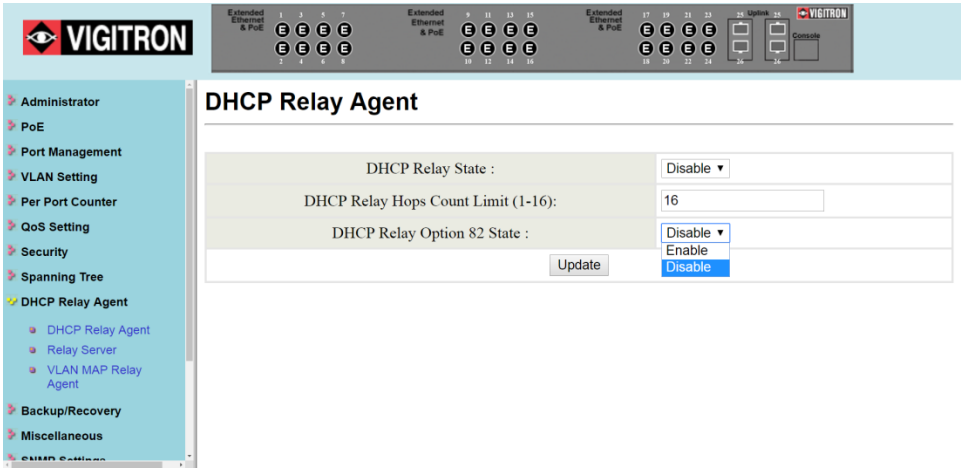
This web page allows the administrator to enable/disable DHCP Relay Agent function. In addition, option 82 message is selectable by setting.



Field	Description
DHCP Relay State	Allow the administrator to enable/disable Relay Agent function.
DHCP Relay Hops Count Limit	Specify the maximum number of Relay Agent traveling from DHCP agent to DHCP server.
DHCP Relay Option 82 State	The pre-condition for enabling/disabling this function is that DHCP Relay State is set to “enable”. Once the Relay State is set to “enable”, the administrator can enable/disable Option 82, depending on whether the Option 82 information is required.

This function sets the enable/disable DHCP Relay Agent.





Select Update

NOTE: On Relay Option 82: This has two components the Circuit ID and the Remote ID. In the case of the Circuit ID a network switch the identifier will be the switch port. In the case of the Remote ID the information relates to the host and is usually the MAC address of the destination.

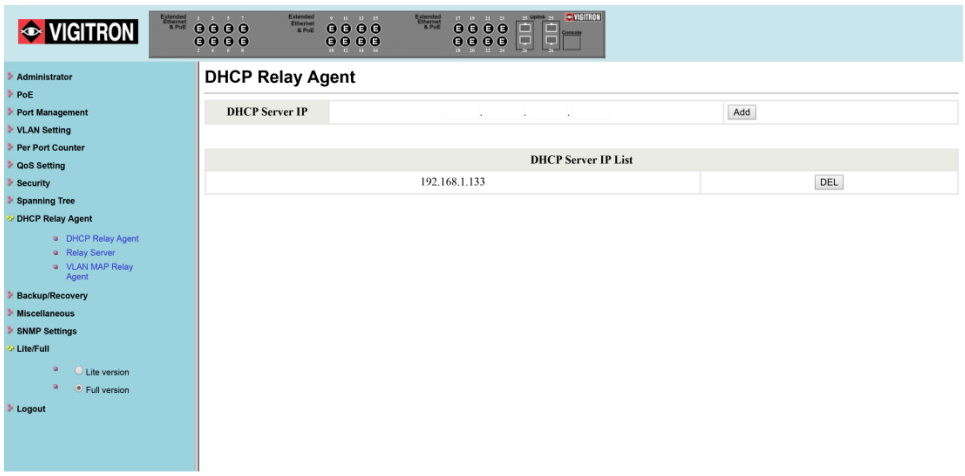
Server IP List: The IP address of DHCP server, which can be relayed by this Relay Agent should be specified on this web page.

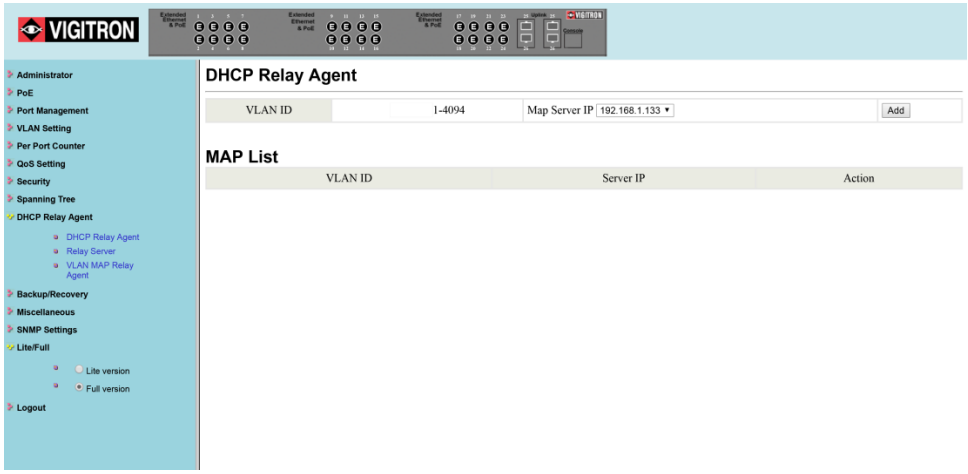
VLAN to Server IP Map: This functions defines the relationship between the VLAN group and the server IP address.

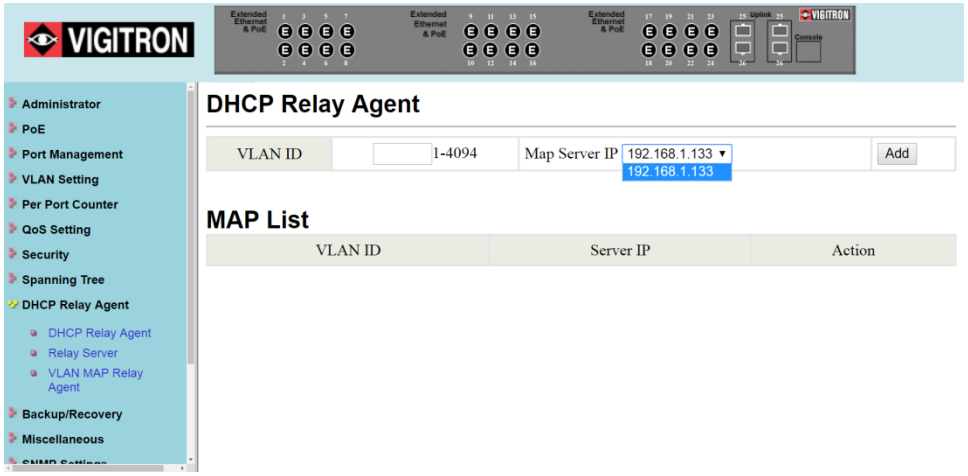
Enter VLAN ID: 1-4094

Select the Map Server IP Address: Use the drop down.
Select Add: Adds the IP address.

NOTE: Only one server can belong to one VLAN ID. If the same server is set to different VLANs, a warning message will show up. You can program more than one server IP address to the same VLAN.

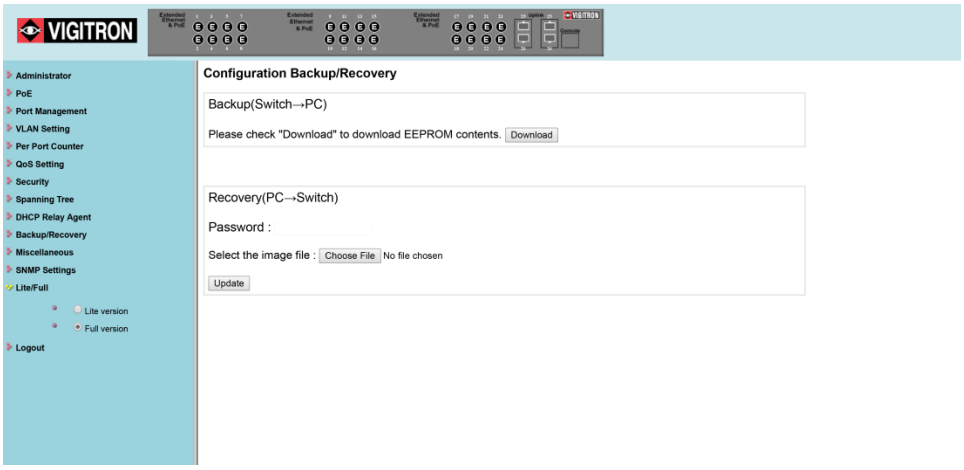

VIGITRON
Administrator
PoE
Port Management
VLAN Setting
Per Port Counter
QoS Setting
Security
Spanning Tree
DHCP Relay Agent
DHCP Relay Agent
Relay Server
VLAN MAP Relay Agent
Backup/Recovery
Miscellaneous
SNMP Settings
Lite/Full
Lite version
Full version
Logout
DHCP Relay Agent
DHCP Server IP
Add
DHCP Server IP List
192.168.1.133
DEL


VIGITRON
Administrator
PoE
Port Management
VLAN Setting
Per Port Counter
QoS Setting
Security
Spanning Tree
DHCP Relay Agent
DHCP Relay Agent
Relay Server
VLAN MAP Relay Agent
Backup/Recovery
Miscellaneous
SNMP Settings
Lite/Full
Lite version
Full version
Logout
DHCP Relay Agent
VLAN ID
1-4094
Map Server IP
192.168.1.133
Add
MAP List
VLAN ID
Server IP
Action


VIGITRON
Administrator
PoE
Port Management
VLAN Setting
Per Port Counter
QoS Setting
Security
Spanning Tree
DHCP Relay Agent
DHCP Relay Agent
Relay Server
VLAN MAP Relay Agent
Backup/Recovery
Miscellaneous
DHCP Relay Agent
VLAN ID
1-4094
Map Server IP
192.168.1.133
192.168.1.133
Add
MAP List
VLAN ID
Server IP
Action

Section 18: Backup and Recovery

18.0 Configuration Backup/Recovery

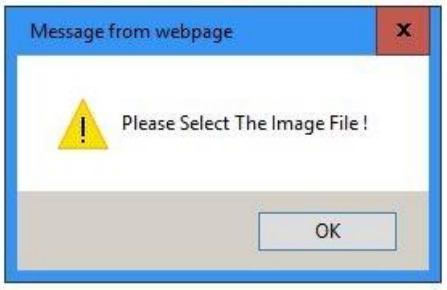


18.1 Back Up

This function will download the contents of the EEPROM to the client computer file

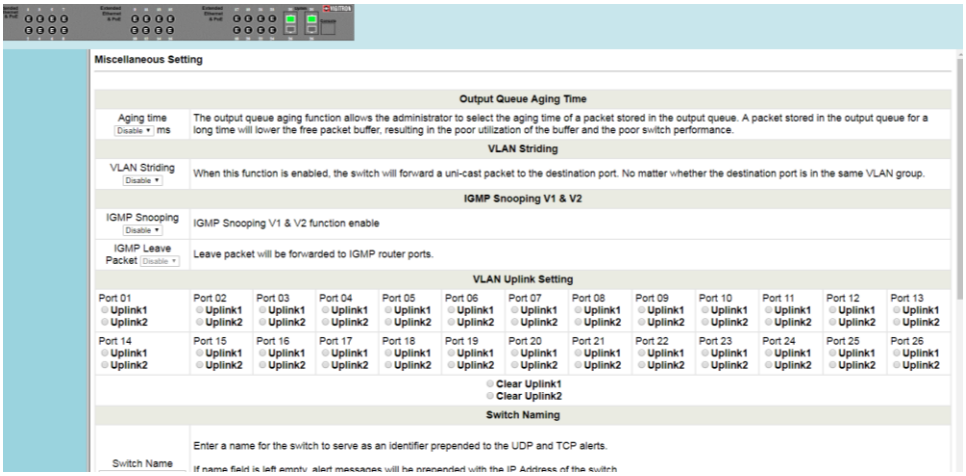
18.2 Recovery

To upload new firmware, first select the file on your client computer. Enter the switch password and select “Update”. If the image file is not selected or the wrong file is selected, the following image will appear.



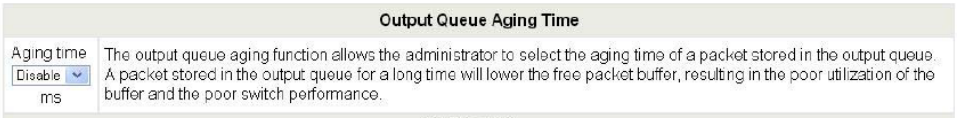
Section 19: Miscellaneous Settings

19.0 Miscellaneous Settings Defined

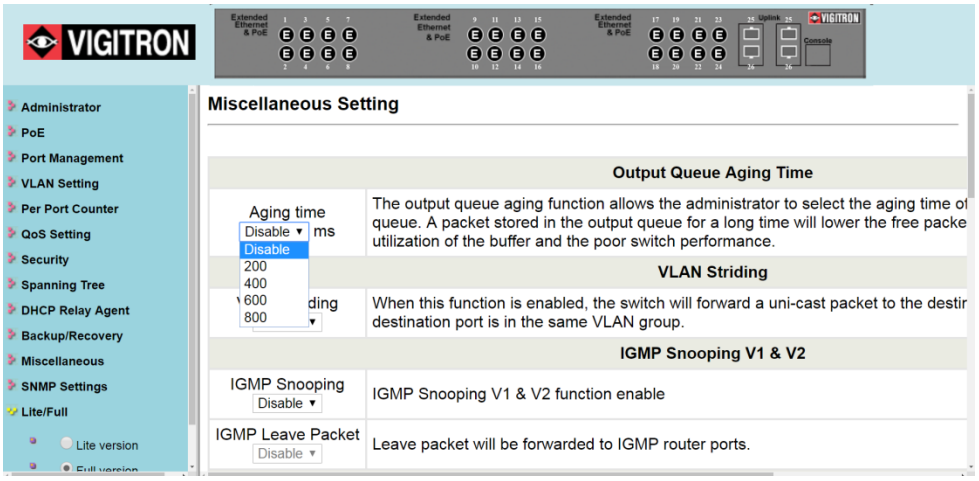


Miscellaneous setting is used to configure Output Queue Aging Time, VLAN Striding, IGMP Snooping and VLAN Uplink.

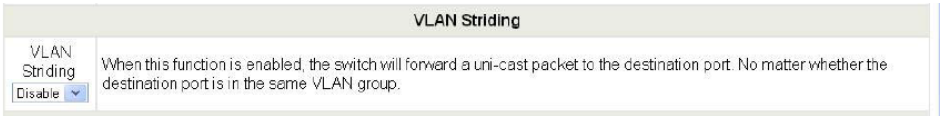
19.1 Output Queue Aging Time



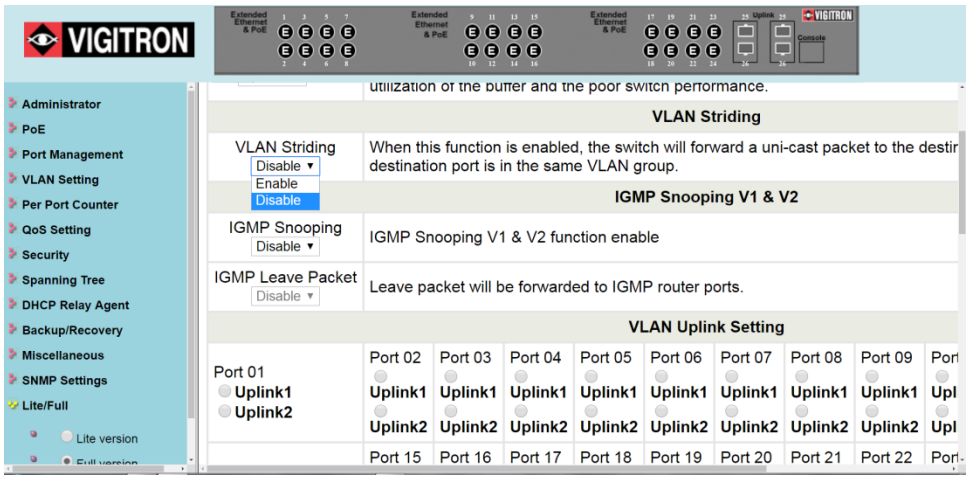
This function is used to avoid the poor utilization of the switch. When a packet is stored in a switch for a long time, the time slot defined by the protocol will expire and this packet becomes useless. To prevent these useless packets from wasting the bandwidth, this switch provides an option to enable the queue aging function. Once enabled, the switch will monitor the aging timer for each packet before it is sent out. The packet which stays inside a queue for a long time will be discarded.



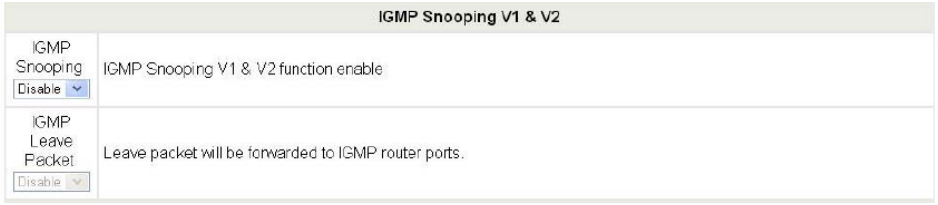
19.2 VLAN Striding



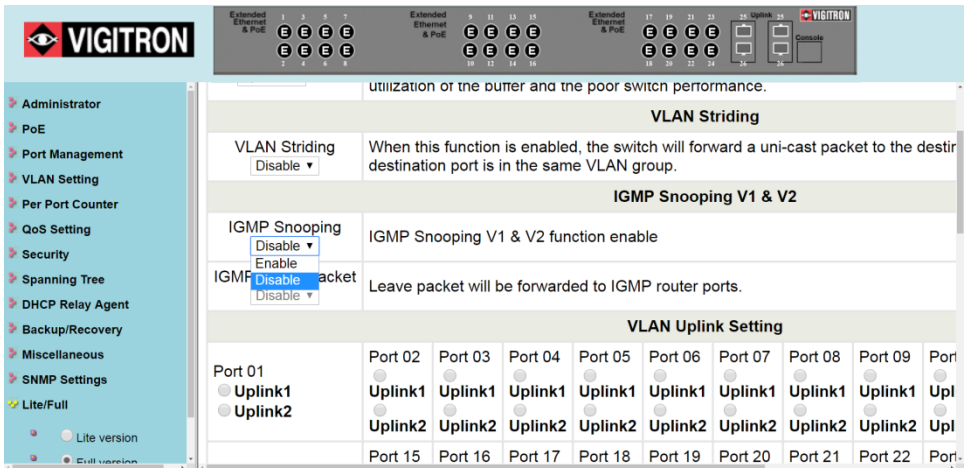
By selecting this function, the switch will forward uni-cast packets to the destination port, no matter whether destination port is in the same VLAN.



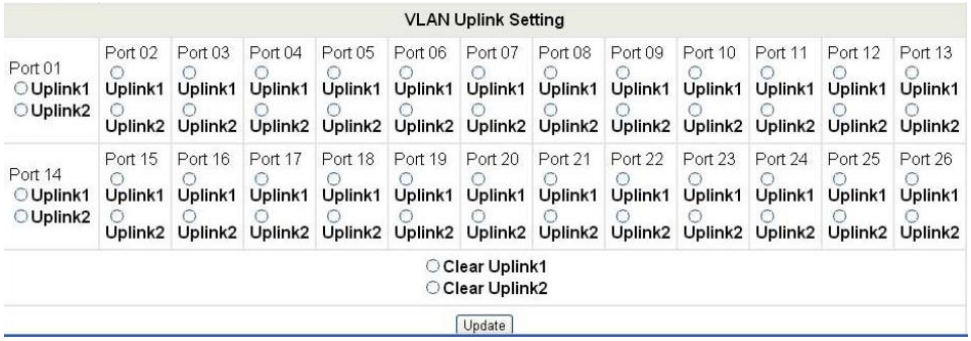
19.3 IGMP Snoop V1 & V2



When this function is enabled, the switch will execute IGMP snooping version 1 and version 2 without the intervention of CPU. The IGMP report packets are automatically handled by the switch when the user enables the “Leave packet will be forwarded to IGMP router ports” function. If members want to leave this multicast group, the IGMP leave packet will be forwarded to the router ports.



19.4 VLAN Uplink



In the VLAN, the user can define the “Uplink port”. This is normally the port that attached to the uplink router. This feature is similar to the “Router port”. After that is set. Any frame transferred to the other VLAN member is forwarded only out the uplink port.

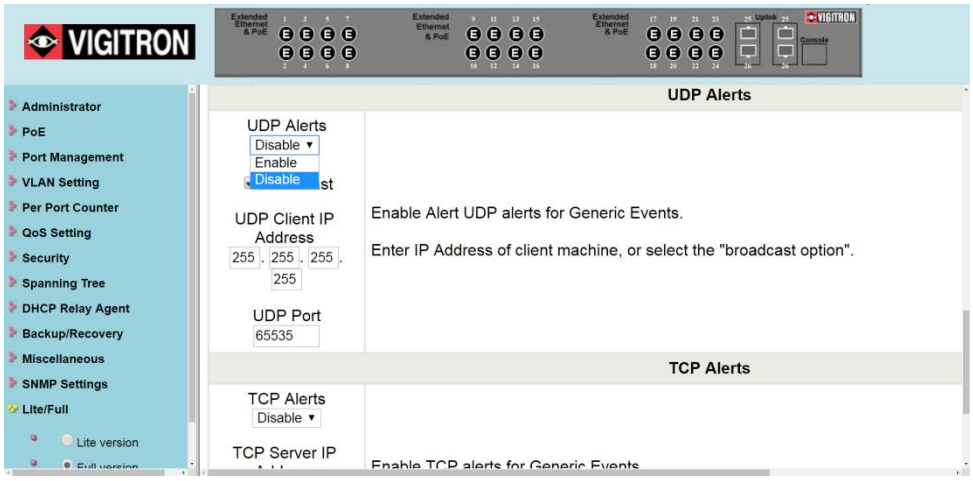
For example:

Step 1: set port 1, 2 and 3 are the same VLAN; set port 4, 5 and 6 are the same VLAN.

Step 2: set port 1 is uplink port of Uplink 1, set port 4 is uplink port of Uplink 2, and press “Update” button.

Step 3: If port 2 want to send a uni-case packet to port 5. The packet will be transferred to the port 1.

19.5 UDP/TCP Alert Messages



Sending Out UDP/TCP Alert Messages:
This function can be used to integrate alert messages generated by the Switch to various “Health Monitoring” software packages. For a complete list of messages that can be sent out by the Switch see the “SNMP Trap States” section of this manual.

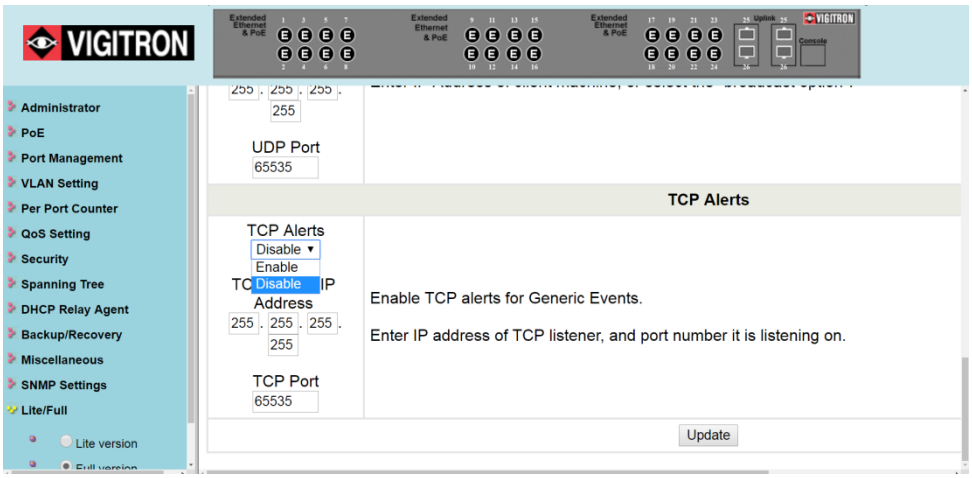
Switch Name:
The Switch can be named by entering the text into this box. This name will be sent out in the alert messages and can be used to identify the specific unit where the alert originated. If the box is blank, the IP address of the Switch will be sent for identification.

UDP Alerts:
To enable or disable this function, click the down arrow located under “UDP Alerts” and select the appropriate option.

To broadcast the alert messages, check the box next to “Broadcast”.

To send alerts to a specific IP address, type the address into the “UDP Client IP Address” text boxes. The same Subnet mask that is used when setting up the IP address of the Switch will also be used in the UDP messaging. Be sure to un-check the “Broadcast” check box prior to inputting the IP Address.

Finally input the port to be used and click the “Update” button.



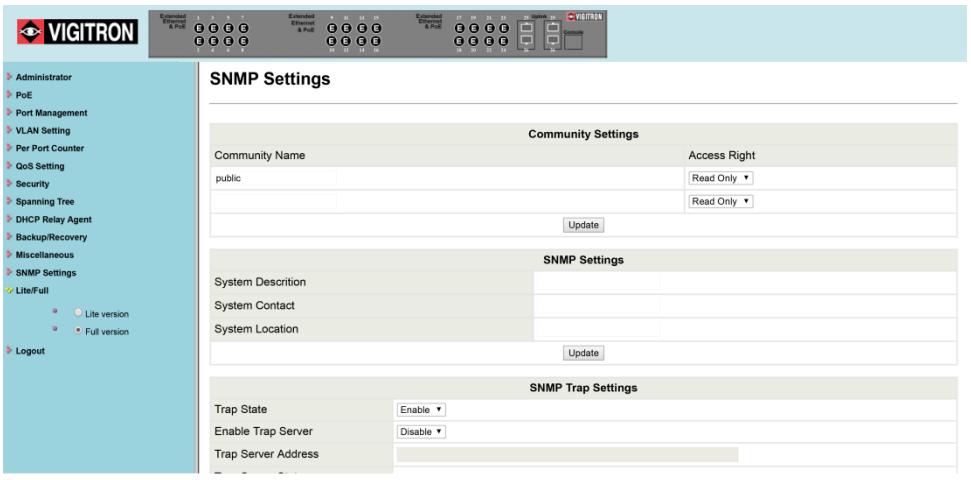
TCP Alerts:
To enable or disable this function, click the down arrow located under "TCP Alerts" and select the appropriate option.

Type the IP Address of the server into the "TCP Server IP Address" text boxes. The same Subnet mask that is used when setting up the IP address of the Switch will also be used in the TCP messaging.

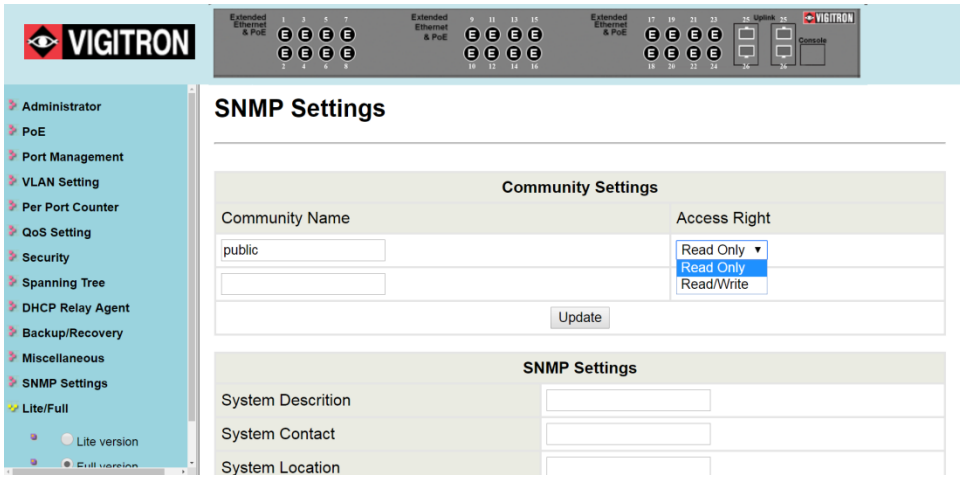
Next input the port to be used and click the "Update" button.

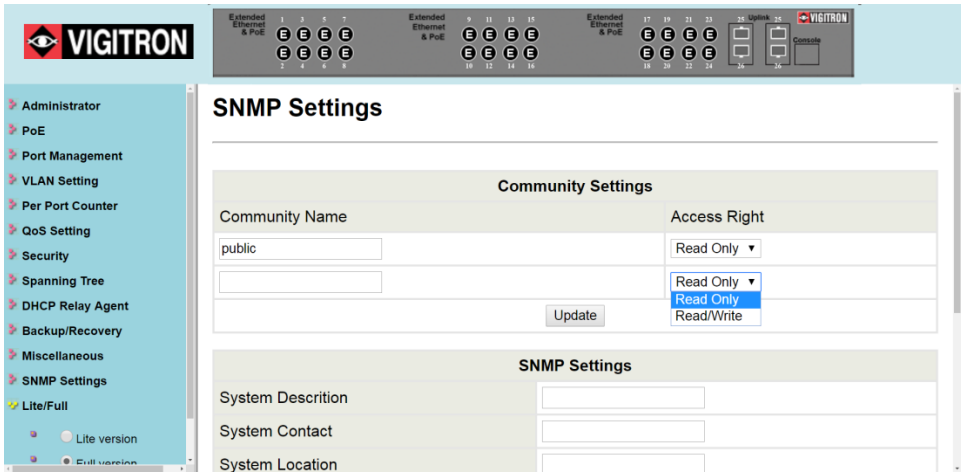
Update:
To apply any changes that are made to the messaging setup the "Update" button must be clicked on the bottom of the page.

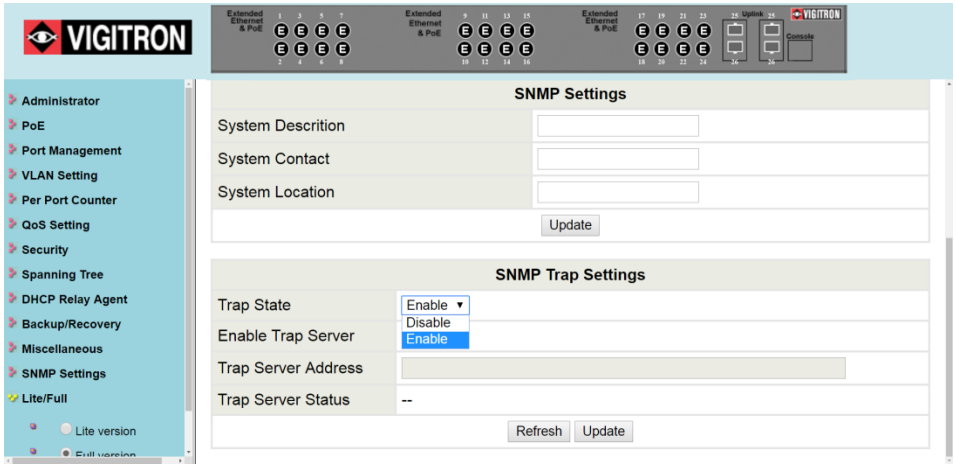
19.6 SNMP Settings

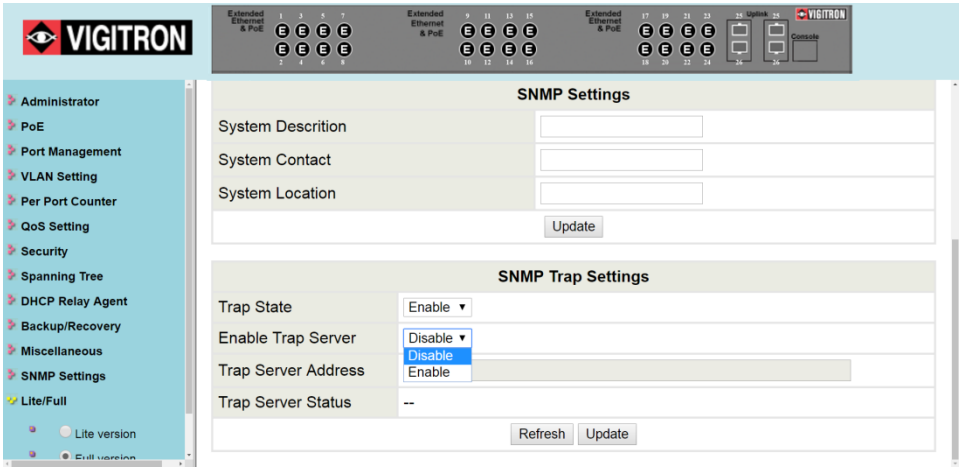


Field	Description
Community Name	This field allows the administrator to enter the community name.
Access Right	This filed defines the access attribute. "Read only" means the administrator can view this community only. "Read/Write" means the administrator can view and modify this community.


VIGITRON
Administrator
PoE
Port Management
VLAN Setting
Per Port Counter
QoS Setting
Security
Spanning Tree
DHCP Relay Agent
Backup/Recovery
Miscellaneous
SNMP Settings
Lite/Full
Lite version
SNMP Settings
Community Settings
Community Name
Access Right
public
Read Only
Read Only
Read/Write
Update
SNMP Settings
System Descrition
System Contact
System Location

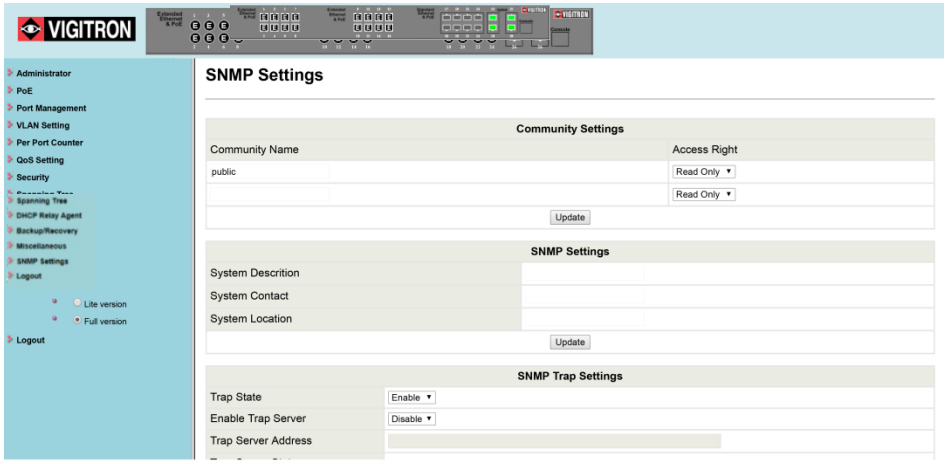

VIGITRON
Administrator
PoE
Port Management
VLAN Setting
Per Port Counter
QoS Setting
Security
Spanning Tree
DHCP Relay Agent
Backup/Recovery
Miscellaneous
SNMP Settings
Lite/Full
Lite version
SNMP Settings
Community Settings
Community Name
Access Right
public
Read Only
Read Only
Read/Write
Update
SNMP Settings
System Descrition
System Contact
System Location


VIGITRON
Administrator
PoE
Port Management
VLAN Setting
Per Port Counter
QoS Setting
Security
Spanning Tree
DHCP Relay Agent
Backup/Recovery
Miscellaneous
SNMP Settings
Lite/Full
Lite version
SNMP Settings
System Descrition
System Contact
System Location
Update
SNMP Trap Settings
Trap State
Enable
Disable
Enable
Enable Trap Server
Trap Server Address
Trap Server Status
--
Refresh
Update



Field	Description
System Description	The administrator can enter a device name for the identification in the network.
System Contact	The contact person responsible for maintaining network.
System Location	The location of this device.
Trap State	Enable/Disable trapped event. The trapped event are: Power up event. Physical port status change event.

19.7 SNMP Trap States



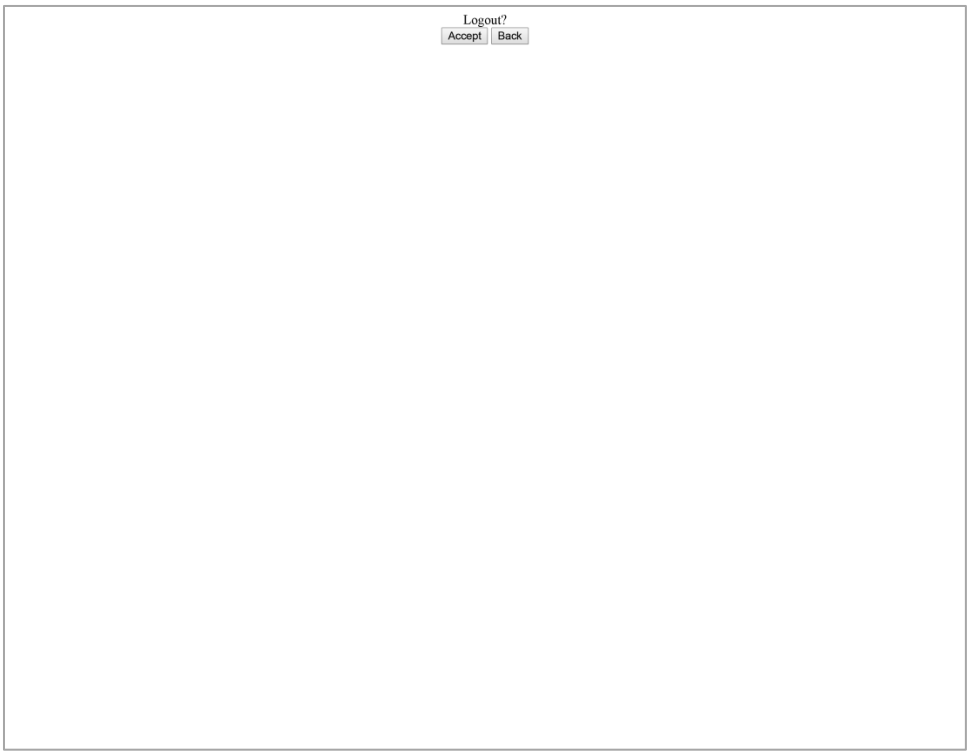
This screenshot shows how the switch was configured and on the right side of the screen, how the trap messages are display. The switch IP address is 192.168.1.133. The switch uses SNMPv1. The time and date displayed are from the host computer.

SNMP will deliver the following messages:

“PoE_On Port xx”
“PoE_Off Port xx”
“SecurPort: TxRx Disabled Port xx”
“E0: Port Overload (ICUT) Event on Port xx“
“E1: Port Short Circuit Limit (ILIM) Event on Port xx”
“E3: Port Severe Short Circuit Event on Port xx”
“E4: Port Thermal Shutdown Event on Port xx”
“E5: Port Temperature Limit Event on Port xx”
“E6: Main Power Overload Event on Port xx”
“E7: PoE Auto Check Timeout Event on Port xx”
“Power Budget: Budget Exceeded, disabled Port xx”
“PSE Overload Protection: Disabled Port xx”
“Traffic Detected Port xx” (Exception: Vi30126, Vi35126)
“Loss of Traffic Detected Port xx” (Exception: Vi30126, Vi35126)
“Authentication Failure: This message is sent when someone tries to login with incorrect information.”
“Cold Start: This message is sent when the PoE Switch is powered up.”
“Warm Start: This message is sent when the PoE Switch is rebooted form the GUI.”

Section 20: Log Out

20.0 Log Out Procedure



Select: Accept to logout.

Back: Returns to the previous page.

Hardware Based Loading Default settings: The purpose of this function is to provide a method for the network administrator to restore all configurations to the default value.

(a) To activate this function, the administrator should follow the following procedures. Press the “Load Default” button for 3 seconds until you see the “LoadDefault” LED blinking.
(b) When LED starts blinking, it means the CPU is executing the “load default” procedure. You can release the button now.

After completing this procedure, all the factory default value will be restored. This includes the IP address, the administrator name, the password and all switch configurations.

In models where the firmware version ends in 1.03, the switch will default to an IP address of 192.168.1.1.

Section 21: Glossary

A

ACE

ACE is an acronym for Access Control Entry. It describes the 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 and 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.

For example, the ACL implementations can be quite complex when the ACEs are prioritized for the 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 to use the service. ACL can generally be configured to control inbound traffic and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc.) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the “Web page help” text for each specific port property.

ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

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.

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.

Aggregation

Use multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability (also Port Aggregation and Link Aggregation).

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.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

Continuity Check (CC) is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

Continuity Check Message (CCM) is an OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for Cisco Discovery Protocol.

D

DEI

Drop Eligible Indicator (DEI) is a 1-bit field in the VLAN tag.

DES

Data encryption standard (DES) is a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations, which are based on a binary number called a key.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

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.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

Domain Name System (DNS) 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

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.

An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

DSCP

Differentiated Services Code Point (DSCP) is a field in the header of IP packets for packet classification purposes.

E

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.

F

FTP

File Transfer Protocol (FTP) 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.

H

Host Defined Power Limit

Host defined power limit allows for specific power level setting.

HTTP

Hypertext Transfer Protocol (HTTP) is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. 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 log-ons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sub-layer 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 considered an adequate degree of encryption for commercial exchange.

I

ICMP

Internet Control Message Protocol (ICMP) is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions.

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

Internet Group Management Protocol (IGMP) 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.

Intelligent Power Limit

Intelligent power limit is power as required from the device.

IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

L

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 is an IEEE 802.1ab standard protocol.

LLDP

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).

LOC

Loss of Connectivity (LOC) is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS.

M

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 has been seen after a configurable age time.

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

Multicast Listener Discovery(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.

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).

N

NAS

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

NetBIOS

Network Basic Input/Output System (NetBIOS) 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 gives each computer in the network both a NetBIOS name and an IP address corresponding to a different host name. It 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. This means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

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

O

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.

Option 82

Option 82 provides information about the DHCP client network location. The DHCP server than uses this information to implement the IP address and other client information. Option 82 supports RFC 3046 which is the DHCP Relay Agent Information Option. Its use helps in protection the spoofing (forging) of IP and MAC addresses.

P

PCP

Priority Code Point (PCP) 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

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

PING

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

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

PoE

Power over Ethernet (PoE) is used to transmit electrical power to remote devices over standard Ethernet cable. It could be used for powering IP telephones,

wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

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

Private VLAN

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

PTP

Precision Time Protocol (PTP) a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QoS Control Entry (QCE) 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.

QCL

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects. Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL in SyncE; this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

Quality of Service (QoS) is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

R

RARP

Reverse Address Resolution Protocol (RARP) 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

Remote Defect Indication (RDI) is an OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP while being backwards-compatible with STP.

S

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.

Sharper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

Simple Mail Transfer Protocol (STMP) 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.

SNAP

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

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

SNTP

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

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, based on pre-configuration or by displaying a list of SSIDs in range and asking the user to select one (Wikipedia).

SSH

Secure Shell (SSH) 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

Synchronization Status Message (SSM) 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.

SyncE

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

T

TACACS+

Terminal Access Controller Access Control System Plus (TACACS+) 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.

TCP

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

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

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

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

TELNET

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

TFTP

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

U

UDP

User Datagram Protocol (UDP) is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

User Priority

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

V

VLAN

Virtual LAN is 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.

	Bandwidth	Vi30126, Vi31026, Vi31126, Vi32026, Vi32226, Vi35126	Vi3010 / Vi3026	Compatible
		SFP port 25-26	Setting	Result
VI00850MM-H	1G	Fixed 1G	Auto	Yes
		Fixed 1G	Fixed 1G	Yes
VI01310MM-H	100 MB	Fixed 1G	Auto	No
		Fixed 1G	Fixed 1G	No
VI01310 SM-H	1G	Fixed 1G	Auto	Yes
		Fixed 1G	Fixed 1G	Yes

	Bandwidth	Vi30126, Vi31026, Vi31126, Vi32026, Vi32226, Vi35126	Vi5001	Compatible
		SFP port 25-26	Setting	Result
VI00850MM-H	1G	Fixed 1G	Fixed 100MB	No
VI01310MM-H	100 MB	Fixed 1G	Fixed 100MB	No
VI01310SM-H	1G	Fixed 1G	Fixed 100MB	No

	Bandwidth	Vi30126, Vi31026, Vi31126, Vi32026, Vi32226, Vi35126	Vi50001	Compatible
		SFP port 25-26	Setting	Result
Vi00850MM-H	1G	Fixed 1G	Fixed 1G	Yes
Vi01310MM-H	100 MB	Fixed 1G	Fixed 1G	Yes
Vi01310SM-H	1G	Fixed 1G	Fixed 1G	Yes

	Bandwidth	Vi30126, Vi31026, Vi31126, Vi32026, Vi32226, Vi35126	Vi3005	Compatible
		SFP port 25-26	Setting	Result
Vi00850 MM-H	1G	Fixed 1G	Fixed 100MB	No
Vi01310MM-H	100 MB	Fixed 1G	Fixed 100MB	No
Vi01310SM-H	1G	Fixed 1G	Fixed 100MB	No

	Bandwidth	Vi30126, Vi31026, Vi31126, Vi32026, Vi32226, Vi35126	Vi30005	Compatible
		SFP port 25-26	Setting	Result
Vi00850MM-H	1G	Fixed 1G	Fixed 1G	Yes
Vi01310MM-H	100 MB	Fixed 1G	Fixed 1G	Yes
VI01310SM-H	1G	Fixed 1G	Fixed 1G	Yes

	Bandwidth	VI35126	Vi3010/Vi3026	Compatible
		SFP port 1-16	Setting	Result
VI00850MM-H	1G	Fixed 100MB	Auto	Yes
		Fixed 100MB	Fixed 100MB	Yes
VI01310MM-H	100 MB	Fixed 100MB	Auto	Yes
		Fixed 100MB	Fixed 100MB	Yes
VI01310 SM-H	1G	Fixed 100MB	Auto	Yes
		Fixed 100MB	Fixed 100MB	Yes

	Bandwidth	VI35126	Vi5001	Compatible
		SFP port 1-16	Setting	Result
VI00850MM-H	1G	Fixed 100MB	Fixed 100MB	Yes
VI01310MM-H	100 MB	Fixed 100MB	Fixed 100MB	Yes
VI01310SM-H	1G	Fixed 100MB	Fixed 100MB	Yes

	Bandwidth	VI35126	Vi50001	Compatible
		SFP port 1-16	Setting	Result
Vi00850MM-H	1G	Fixed 100MB	Fixed 1G	No
Vi01310MM-H	100 MB	Fixed 100MB	Fixed 1G	No
Vi01310SM-H	1G	Fixed 100MB	Fixed 1G	No

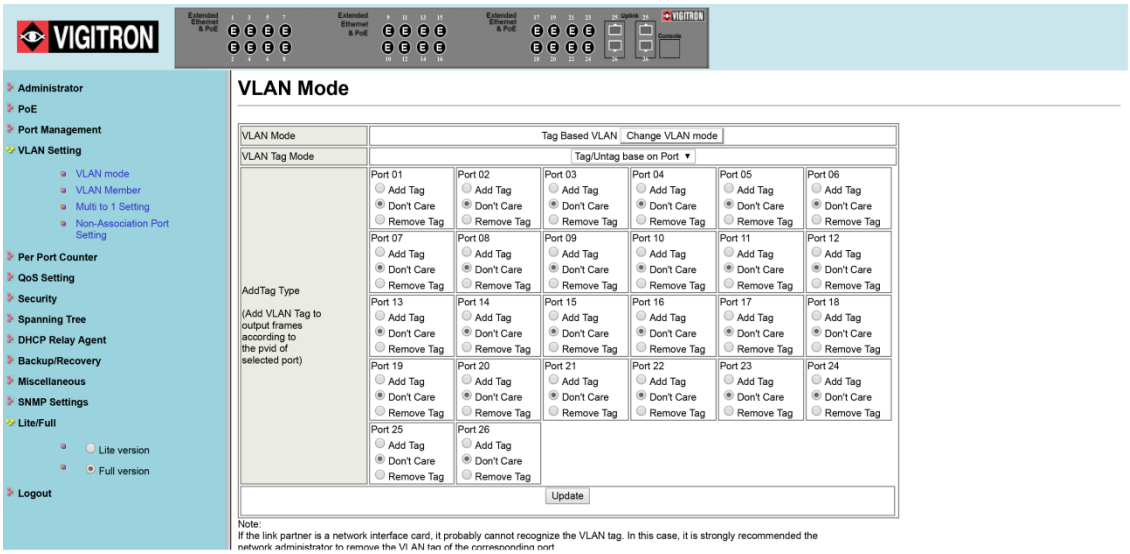
	Bandwidth	VI35126	Vi3005	Compatible
		SFP port 1-16	Setting	Result
Vi00850 MM-H	1G	Fixed 100MB	Fixed 100MB	Yes
Vi01310MM-H	100 MB	Fixed 100MB	Fixed 100MB	Yes
Vi01310SM-H	1G	Fixed 100MB	Fixed 100MB	Yes

	Bandwidth	VI35126	Vi30005	Compatible
		SFP port 1-16	Setting	Result
Vi 00850MM-H	1G	Fixed 100MB	Fixed 1G	No
Vi01310MM-H	100 MB	Fixed 100MB	Fixed 1G	No
VI01310SM-H	1G	Fixed 100MB	Fixed 1G	No

When connecting the Vi32226 to other model Switches, it is necessary to add a Tag to the gigabit port to get the Switches to communicate.

To add a Tag to the gigabit port, Click on “VLAN Setting” then “VLAN mode”. Select “Add Tag” to the port used to connect to the other Switch and then click “Update”.

Note: port 25



Contact Information

Vigitron, Inc.
7810 Trade Street, Suite 100
San Diego, CA 921
Tel: (858) 484-5209
Fax: (858) 484-1205
www.vigitron.com