



# **MaxiiNet™ Vi30018 Operational Manual**

---

**Vi30018**

**Release F30018-SV1.00**

# Section 1: About This Manual

## 1.0 Copyright

Copyright © 2020 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 form by 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 Vi30018.

## 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.

### 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.

### 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



UI 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**



**NOTE:** The switch is an 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 at outdoor or sandstorm.
  - Before installation, please make sure input power supply and product specifications are compatible to each other.
  - To reduce the risk of electric shock, disconnect all AC or DC power 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

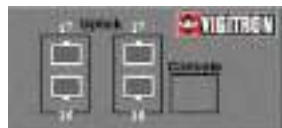
The User's Manual

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

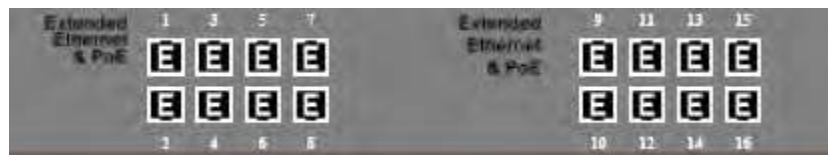
Release	Date	Revision
F30018-SV1.00		

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 17 and 18 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 will show 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*

**PoE: 15.4 Watts, 30 Watts, 36 Watts, 65 Watts**



There are 4 or 8 ports providing 65W PoE on Hybrid Switches as following:

Vi30018	Ports 1-4 (standard)
Vi30126	Ports 1-4 (standard), 17-20 (standard)
Vi31026	Ports 1-4 (extended), 17-20 (standard)
Vi31126	Ports 1-4 (extended), 17-20 (standard)
Vi32026	17-20 (standard)
Vi32126	17-20 (standard)
Vi35126	17-20 (standard)



## Contents

<b>Section 1: About This Manual .....</b>	<b>2</b>
1.0 Copyright.....	2
1.1 Purpose.....	2
1.2 Audience .....	2
1.3 Conventions .....	2
1.4 Warranty.....	2
1.5 Disclaimer .....	3
<b>Section 2: Compliances and Safety Statements .....</b>	<b>4</b>
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
<b>Section 3: Introduction .....</b>	<b>16</b>
3.0 Overview .....	16
3.1 Cabling Guidelines .....	17
3.2 Connecting to PCs, Servers, Hubs and Switches .....	17
3.3 Network Wiring Connection .....	18
3.4 Vi30018 – Front View .....	19
3.5 Vi30018 – Rear View .....	19
<b>Section 4: Description of Hardware .....</b>	<b>20</b>
4.0 1000Base-T Ports .....	20
4.1 SFP Transceivers Slots .....	20
4.2 Ports and System Status LEDs .....	21
4.3 Console Port .....	21
<b>Section 5: Installing the Switch.....</b>	<b>22</b>
5.0 Selecting a Site .....	22
5.1 Ethernet Cabling .....	22
5.2 Equipment Checklist.....	23
5.3 Package Contents .....	23
5.4 Mounting .....	23

5.5 Rack Mounting .....	24
5.6 To Rack-Mount Devices.....	24
5.7 Installing an Optional SFP Transceiver .....	24
5.8 Installing an SFP Transceiver .....	25
5.9 Connecting to a Power Source .....	25
<b>Section 6: Making Network Connections .....</b>	<b>27</b>
6.0 Connecting to a Network Devices.....	27
6.1 Twisted-Pair Devices .....	27
6.2 Cabling Guidelines .....	27
6.3 Connecting to PCs, Servers, Hubs and Switches .....	27
6.4 Network Wiring Connections .....	28
<b>Section 7: Troubleshooting .....</b>	<b>29</b>
7.0 Basic Troubleshooting Tips.....	29
7.1 Table 10: Troubleshooting Chart.....	30
<b>Section 8: Operation of Web-Based Management.....</b>	<b>31</b>
8.0 Initial Configuration.....	31
<b>Section 9: Administration .....</b>	<b>33</b>
9.0 Prior to Logging On .....	33
9.1 Logging On .....	33
9.2 System IP Configuration .....	35
9.3 System Status .....	36
9.4 Load Default.....	37
9.5 Firmware Update.....	38
<b>Section 10: PoE.....</b>	<b>41</b>
10.0 PoE Status .....	41
10.1 PoE Setting .....	42
10.2 PoE Event Counter.....	44
10.3 PoE Power Delay .....	44
10.4 PoE Auto Check .....	46
<b>Section 11: Port Management .....</b>	<b>47</b>
11.0 Port Configuration.....	47
11.1 Port Mirroring.....	53
11.2 Bandwidth Control .....	54
11.3 Broadcast Storm Control .....	56
<b>Section 12: VLAN Settings .....</b>	<b>57</b>
12.0 VLAN Mode.....	57

12.1 VLAN Member (Port Based).....	58
12.2 VLAN Member Settings (Tag Based).....	60
12.3 Multi to 1 Setting .....	62
12.4 Non-Association Port Setting.....	64
<b>Section 13: Per Port Counter .....</b>	<b>65</b>
13.0 Transmit Packet and Receive Packets .....	65
13.1 Drop and Receive Packet.....	66
13.2 CRC error packet and Receive Packet.....	66
13.3 Counter Modes Defined.....	67
<b>Section 14: QoS Settings.....</b>	<b>68</b>
14.0 Priority Mode .....	68
14.1 Setting the Priority Mode .....	68
14.2 Class of Service Configuration .....	69
<b>Section 15: Security.....</b>	<b>74</b>
15.0 MAC Address Binding .....	74
15.1 Scanning MAC Addresses.....	75
15.2 Securing Ports Using Mac Addresses.....	76
15.3 TCP/UDP Filter.....	76
15.4 Secure WAN Port: Select the port to be secured .....	79
<b>Section 16: Spanning Tree .....</b>	<b>80</b>
16.0 STP Bridge Settings .....	80
16.1 STP Port Settings.....	81
16.2 Loopback Detection Settings.....	81
16.3 Trucking .....	83
<b>Section 17: DHCP Relay Agent .....</b>	<b>90</b>
17.1 Relay Agent Configurations .....	90
<b>Section 18: Backup and Recovery.....</b>	<b>93</b>
18.0 Configuration Backup/Recovery .....	93
18.1 Back Up .....	93
18.2 Recovery.....	93
<b>Section 19: Miscellaneous Settings.....</b>	<b>94</b>
19.0 Miscellaneous Settings Defined.....	94
19.1 Output Queue Aging Time .....	94
19.2 VLAN Striding.....	95
19.3 IGMP Snoop V1 & V2.....	95
19.4 VLAN Uplink.....	96

19.5 UDP/TCP Alert Messages .....	96
19.6 SNMP Settings .....	98
19.7 SNMP Trap States .....	99
<b>Section 20: Log Out .....</b>	<b>101</b>
20.0 Log Out Procedure .....	101
<b>Section 21: Glossary .....</b>	<b>102</b>
A .....	102
ACE .....	102
ACL .....	102
AES .....	103
APS .....	103
Aggregation .....	103
ARP .....	103
ARP Inspection .....	103
Auto-Negotiation .....	103
C .....	103
CC .....	103
CCM .....	104
CDP .....	104
D .....	104
DEI .....	104
DES .....	104
DHCP .....	104
DHCP Relay .....	104
DHCP Snooping .....	105
DNS .....	105
DoS .....	105
Dotted Decimal Notation .....	105
DSCP .....	106
E .....	106
EEE .....	106
EPS .....	106
Ethernet Type .....	106
F .....	106
FTP .....	106
Fast Leave .....	106

H .....	106
HTTP .....	106
HTTPS .....	107
I .....	107
ICMP .....	107
IEEE 802.1X .....	107
IGMP .....	107
IGMP Querier .....	108
IP .....	108
L .....	108
LACP .....	108
LLC .....	108
LLDP .....	109
LLDP-MED .....	109
LOC .....	109
M .....	109
MAC Table .....	109
Mirroring .....	109
MLD .....	109
MVR .....	110
N .....	110
NAS .....	110
NetBIOS .....	110
NFS .....	110
NTP .....	110
O .....	111
OUI .....	111
Option 82 .....	111
P .....	111
PCP .....	111
PD .....	111
PHY .....	111
PING .....	111
PoE .....	111
Policer .....	112
Private VLAN .....	112

PTP.....	112
Q.....	112
QCE .....	112
QCL.....	112
QL .....	112
QoS.....	112
R.....	113
RARP .....	113
RADIUS .....	113
RDI.....	113
RSTP .....	113
S.....	113
SHA.....	113
Sharper .....	113
SMTP .....	113
SNAP .....	113
SNMP.....	114
SNTP .....	114
SSID.....	114
SSH.....	114
SSM .....	114
STP.....	114
SyncE.....	114
T.....	115
TACACS+.....	115
Tag Priority .....	115
TCP.....	115
TELNET .....	115
TFTP .....	115
U.....	115
UDP .....	115
User Priority .....	116
V.....	116
VLAN.....	116
VLAN ID .....	116
Voice VLAN.....	117

<b>SFP Interface Guide .....</b>	<b>118</b>
<b>Connecting Vi30018 .....</b>	<b>121</b>
<b>Contact Information .....</b>	<b>122</b>

## Section 3: Introduction

### 3.0 Overview

This user's manual will tell you how to install and connect your network system. Many detailed explanations of hardware and software functions are shown, as well as, the examples of the operation for web-based interface.

The Vi30018 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:

- 18 total Ethernet ports
- 16 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 for ports 5-16
- Up to 72 watts per port for ports 1-4



### 3.1 Cabling Guidelines

Ports 1-16 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 17 and 18 are 10/100/1000Mbps and can also be set to auto sense speeds or forced speeds. Ports 17 and 18 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.



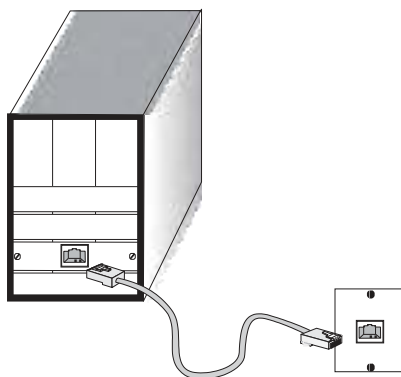
---

**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 is present. Green if PoE is present.

### 3.3 Network Wiring Connection

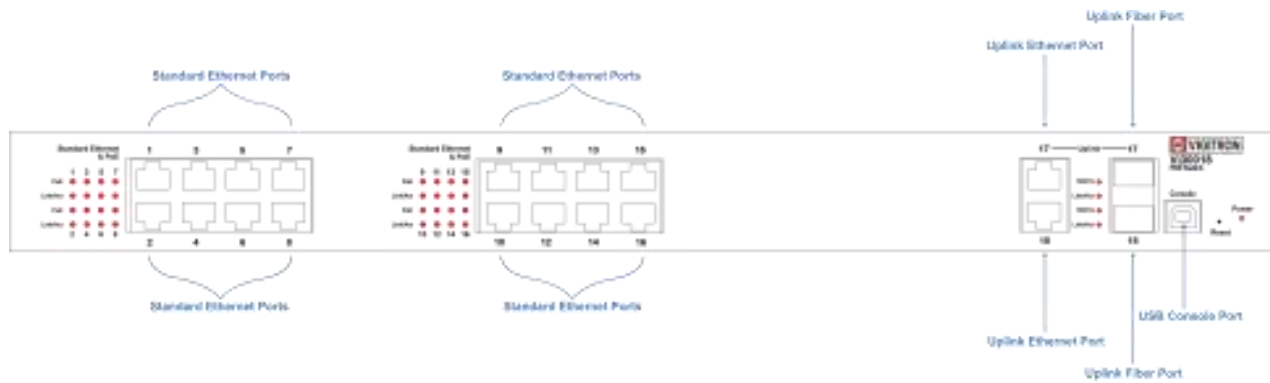
Today, the punch-down block is an integral part of many of the newer equipment racks. It is actually part of the patch panel. Instructions for making connections in the wiring closet with this type of equipment are as follows:

**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 Vi30018 – Front View



### 3.5 Vi30018 – Rear View



## Section 4: Description of Hardware

### 4.0 1000Base-T Ports

The switch contains 16 100BASE-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

Vi30018 supports the Small Form Factor Pluggable (SFP) transceiver slots. The slots are shared with RJ45 port 17-18. 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**

The Vi30018 supports SFP conforming to MSA standards, although differences between manufacturers can affect performance. For best results, use Vigitron SFPS.

---

**NOTE:**

- \* Maximum distance may vary for different SFP vendors.
  - \* Regardless of the SFP speed, ports 1-16 are 100Mbps / Ports 17 & 18 are 1Gbps.
  - \* SFP must be matched at both cable ends.
  - \* For ports 17 and 18, SFP port speed is fixed at 1000Mbps and cannot be changed.
- 



## 4.2 Ports and System Status LEDs

The Vi30018 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 1-16	Green	Green when the port is delivering PoE power.
Port 17 & 18	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 4: 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

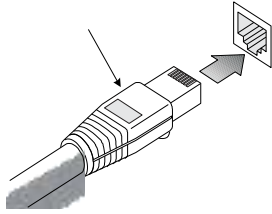
The switch can be mounted in a standard 19-inch equipment rack or on a flat surface. Be sure to follow the guidelines below when choosing a location.

- 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 Vi30018 is connected to a separate grounded power outlet that provides 100 to 240VAC and 50 to 60 Hz.

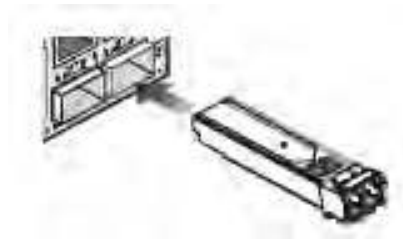
### 5.1 Ethernet Cabling

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:

- Vi30018 100Mbps + 1000Mbps Management Switch
- 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.
- 

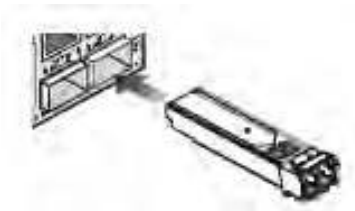


---

**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.



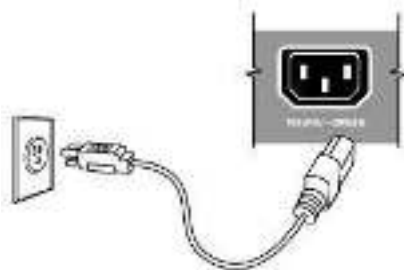
---

**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.



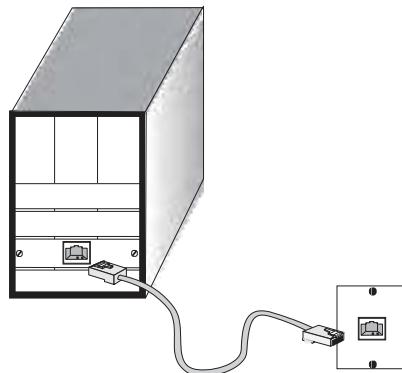
---

**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.

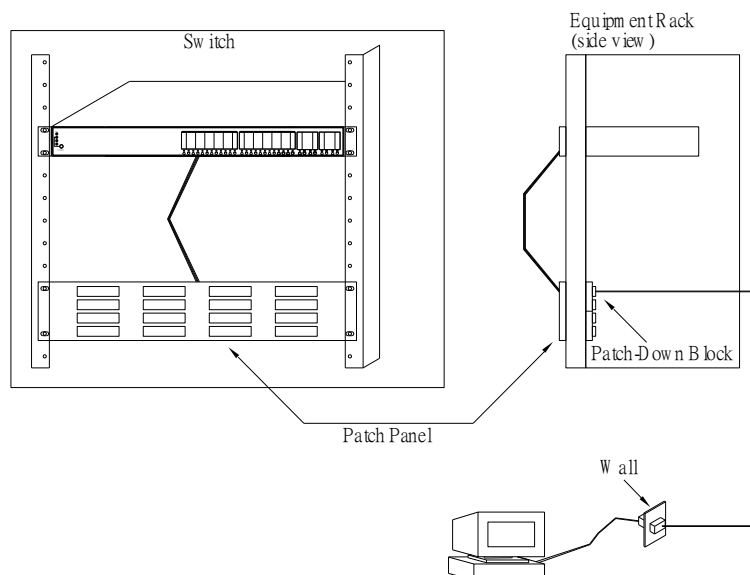
## 6.4 Network Wiring Connections

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 Vi30018 behave 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 Vi30018 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	<ul style="list-style-type: none"> <li>• Check connections between the switch, the power cord and the wall outlet.</li> <li>• Contact your dealer for assistance.</li> </ul>
Link LED is Off	<ul style="list-style-type: none"> <li>• Verify that the switch and attached device are powered on.</li> <li>• Be sure the cable is plugged into the switch and corresponding device.</li> <li>• If the switch is installed in a rack, check the connections to the punch-down block and patch panel.</li> <li>• Verify that the proper cable type is used and its length does not exceed specified limits.</li> <li>• Check the adapter on the attached device and cable connections for possible defects. Replace the defective adapter or cable if necessary.</li> </ul>

## Section 8: Operation of Web-Based Management

### 8.0 Initial Configuration

This chapter instructs you on how to configure and manage the Vi30018 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 Vi30018 are listed in the table below:

<b>IP Address</b>	192.168.1.133
<b>Subnet Mask</b>	255.255.255.0
<b>Default Gateway</b>	192.168.1.254
<b>Username</b>	admin
<b>Password</b>	system

After the Vi30018 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 Vi30018 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, you must first type the user name and password and then press enter. When you log into the Vi32226 switch Web UI management, you can use ipv4 only. To optimize the display effect, we recommend you use either IE, Firefox, or Chrome 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 between 2 and 254, excluding 133.

### 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.



USER LOG IN

Site: 192.168.1.133

ID: admin

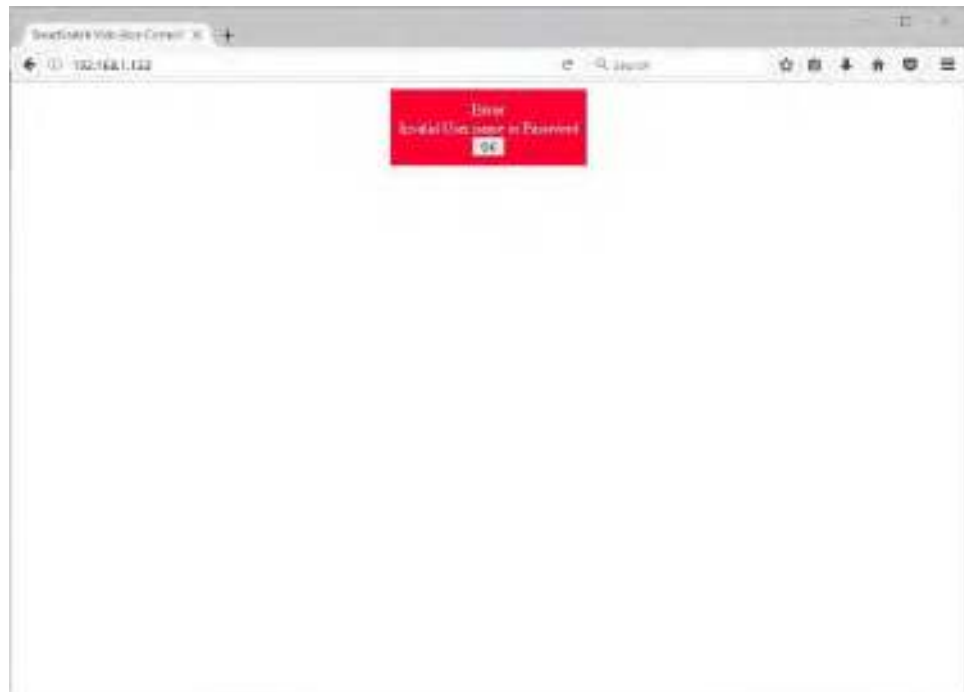
Password: •••••••

OK



**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.

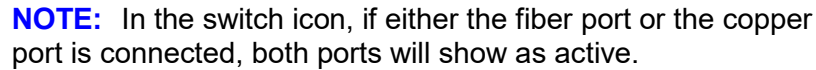
### Full Version




### Lite Version



The Vi30018 provides two separate configuration 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.

[illegible]

- ## 9.2 System IP Configuration



The screenshot shows the 'System IP Configuration' page of the Vigor 2805. The left sidebar contains a navigation menu with the following items: System Overview, System IP Configuration (selected), System Settings, System Status, System Maintenance, System Security, System Logs, and System Tools. The main content area displays a table for System IP Configuration. The table has two columns: 'Setting' and 'Value'. The rows are: IP Address (192.168.1.1), Subnet Mask (255.255.255.0), Gateway (192.168.1.254), and IP Configuration (Static). Below the table is a 'Save' button.

Setting	Value
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
IP Configuration	Static

[Save](#)



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

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

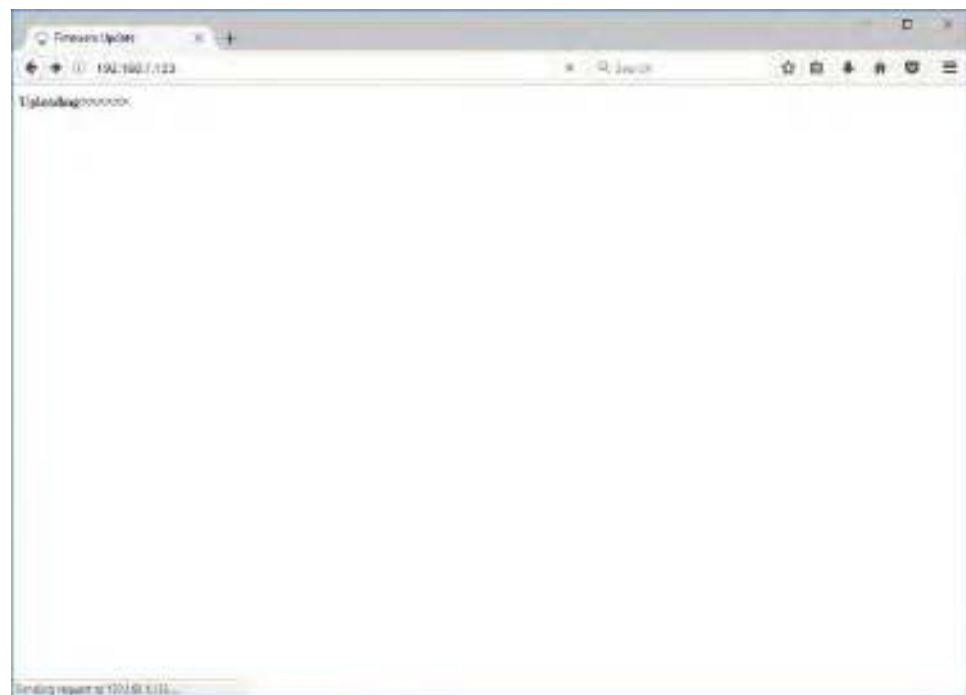
## 9.5 Firmware Update



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”**.

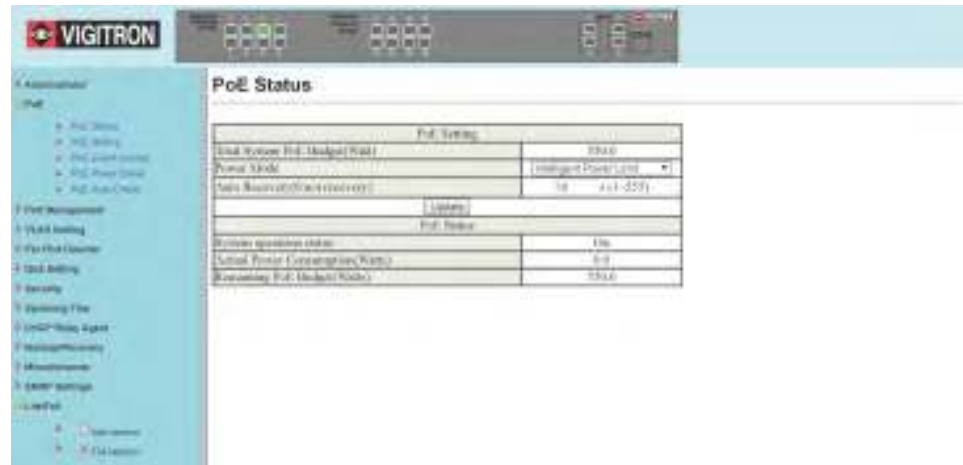






## Section 10: PoE

### 10.0 PoE Status



#### Power Mode:

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

**PoE Setting**

Function	Status	Mode	Available Power (MAX:36 LBS:1 Watt)	Port Priority
Port No.	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16	Check All	Update	

Port	Status	Power	Mode	Class	Voltage(V)	Current(mA)	Temperature(°C)	Power Consumption(W)	Available Power(W)
1	Enable	OFF	0.5 Watt	--	54	--	36.87	0.0	72.0
2	Enable	OFF	0.5 Watt	--	54	--	35.81	0.0	72.0
3	Enable	OFF	0.5 Watt	--	54	--	35.87	0.0	72.0
4	Enable	OFF	0.5 Watt	--	54	--	35.75	0.0	72.0
5	Enable	OFF	0.5 Watt	--	54	--	35.75	0.0	72.0
6	Enable	OFF	0.5 Watt	--	54	--	35.75	0.0	72.0
7	Enable	OFF	0.5 Watt	--	54	--	35.75	0.0	72.0
8	Enable	OFF	0.5 Watt	--	54	--	35.75	0.0	72.0
9	Enable	OFF	0.5 Watt	--	54	--	35.75	0.0	72.0

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.

**PoE Setting**

Function	Status	Mode	Available Power (MAX:36 LBS:1 Watt)	Port Priority
Port No.	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16	Check All	Update	

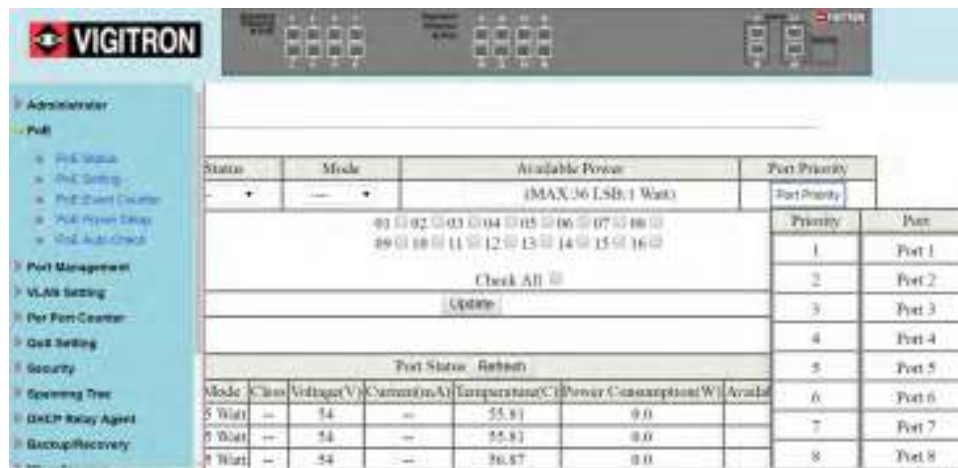
Port	Status	Power	Mode	Class	Voltage(V)	Current(mA)	Temperature(°C)	Power Consumption(W)	Available Power
1	Enable	OFF	0.5 Watt	--	54	--	36.87	0.0	72.0
2	Enable	OFF	0.5 Watt	--	54	--	35.81	0.0	72.0
3	Enable	OFF	0.5 Watt	--	54	--	35.87	0.0	72.0

**PoE Setting**

Function	Status	Mode	Available Power (MAX:36 LBS:1 Watt)	Port Priority
Port No.	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16	Check All	Update	

Port	Status	Power	Mode	Class	Voltage(V)	Current(mA)	Temperature(°C)	Power Consumption(W)	Available Power
1	Enable	OFF	0.5 Watt	--	54	--	35.81	0.0	72.0
2	Enable	OFF	0.5 Watt	--	54	--	35.81	0.0	72.0
3	Enable	OFF	0.5 Watt	--	54	--	36.87	0.0	72.0



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 16 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 16 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.

What does the priority list do? When the switch detects the power usage is above 550 Watts, it will begin disabling ports, until the usage goes down to safe levels again. The switch will start disabling ports with low priority, and move towards the higher priority ports. To re-enable the disabled ports, user will need to log into switch to re-enable the ports in the “PoE settings” page.



**NOTE:** In the default mode, Port 1 is given the highest priority and port 16 the least.

## 10.2 PoE Event Counter

### PoE Event Counter Definitions

Port	E0	E1	E2	E3	E4	E5	E6	E7
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0

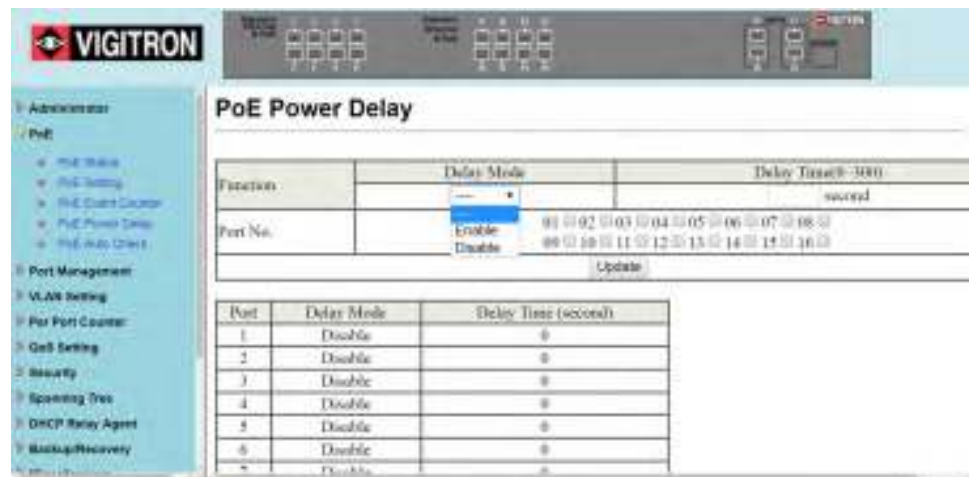
- E0: Port Overload (ICUT) Event
- E1: Port Short Circuit Limit (ILIM) Event
- E2: Port MPS Error (DC Disconnect) Event
- E3: Port Severe Short Circuit Event
- E4: Port Thermal Shutdown Event
- E5: Port Temperature Limit Event
- E6: Main Power Overload Event
- E7: PoE Auto Check Timeout Event

## 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**

Function	Check Interval Time	Wake Up Time
	0 (min) 1 - 240 (min)	0 (s) 1 - 59 (s)
	[Update]	
Enable Port	Port Select	
	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16	
	[Update]	
Function	Port	Check IP Address
	1	0 0 0 0
	[Update]	
Port No.	Enable Status	IP Address
1	Disable	0.0.0.0
2	Disable	0.0.0.0
3	Disable	0.0.0.0
4	Disable	0.0.0.0

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.

**PoE Auto-check**

Function	Check Interval Time	Wake Up Time
	0 (min) 1 - 240 (min)	0 (s) 1 - 59 (s)
	[Update]	
Enable Port	Port Select	
	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16	
	[Update]	
Function	Port	Check IP Address
	1	0 0 0 0
	[Update]	

# Section 11: Port Management

## 11.0 Port Configuration

The screenshot shows the 'Port Configuration' page in the Vigtron management interface. It features a table with columns for Port, Link, Speed, Duplex, FlowCtrl, Tx/Rx Enable, Broadcast, Broadcast Rate, Auto Negotiation, Speed, Duplex, Flow, Backpressure, and Add Learning. The table lists ports 1 through 4, with port 1 selected. Below the table is an 'Update' button.

Select the Port Number: Select the port number 1-18

### NOTE:



For ports 17 and 18, 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.

This screenshot shows the 'Port Configuration' page with the 'Tx/Rx Enable' dropdown menu open. The menu has two options: 'Enable' and 'Disable'. The 'Enable' option is currently selected. The rest of the interface, including the port settings table and the 'Update' button, remains visible in the background.

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.



To re-enable the transmit/receive ability for a secured port, the user will need to log into the switch GUI and re-enable it from the “Port Configuration” page.



1. In the Port Configuration section, click the down arrow under SecurPort Recovery. 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™ Recovery

Note: For Extended 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 Recovery do?

The SecurPort Recovery configuration determines if a port’s Tx/Rx ability is re-enabled during a reboot. In cases where the switch loses power, any ports configured as SecurPort and are under a “Link Up” state at the time of the shutdown, will be disabled by the SecurPort functionality. In these cases, enabling SecurPort Recovery on a port ensures that its Tx/Rx ability is automatically re-enabled when the switch gets power back. Otherwise, if SecurPort Recovery on a port is disabled, the switch will not automatically re-enable the port’s Tx/Rx ability, instead the user will need to log into the switch’s web interface to manually re-enable the port.



---

**NOTE:** SecurPort only disables the transmit/receive ability of the port. If configured, the port will still provide PoE. The switch does not distinguish between a SecurPort port which was disabled by a loss of Power, and one which was disabled by a physical Link Down event, the SecurPort Recovery configuration will re-enable a disabled port regardless of the circumstances.

---



---

**NOTE:** During the bootup sequence, the SecurPort Recovery will disable the SecurPort configuration for up to 3 minutes to allow any connected devices to undergo their initialization process without triggering the SecurPort functionality through their linking sequence.

---



#### 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 selected, Speed Selection will not be active.



#### Speed:

- Select 10Mbps or 100Mbps for ports 1-16
- Select 10Mbps/100Mbps or 1000Mbps (1Gbps) for ports 17/18

If attempts are made to program ports 1-16 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 learn 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 has taken effect.

## 11.1 Port Mirroring

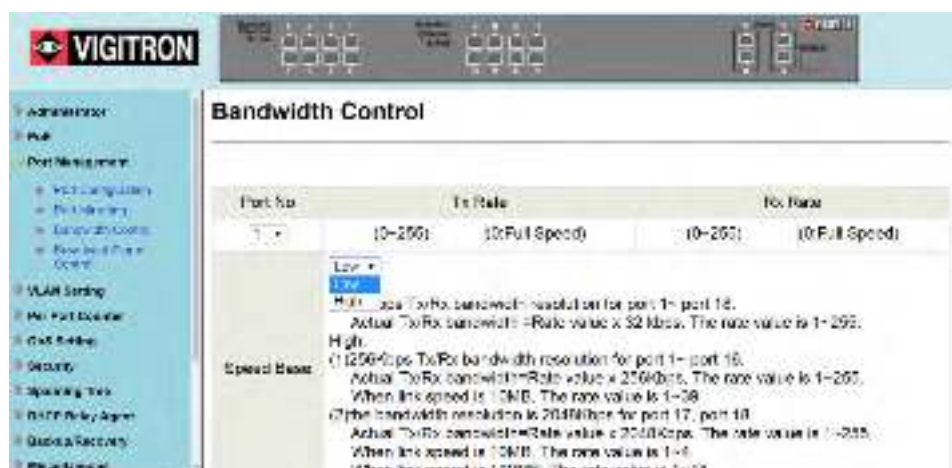
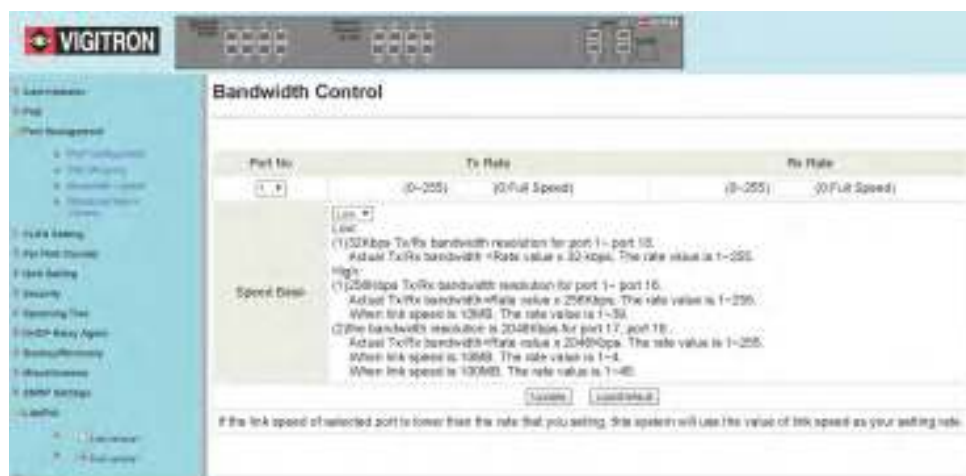


The select of ports to be mirrored is done by port priority by number. For Example; If ports 1 and 2 are selected as source ports and this is followed by ports 17 and 18, Port 1 will be mirrored at port 17 and port 2 will mirrored at port 18.

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 1-16 and 10/100/1000Mbps for ports 17/18). 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 17 and port 18, the bandwidth setting should be less than 48 if the bandwidth is set to “High”. 10Mbps link speed for port 17 and port 18, the bandwidth setting should be less than 4 if the bandwidth base is set to “High”. 10Mbps link speed for port 1 ~ port 16, 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 18. In the “High” mode, the Tx/Rx bandwidth resolution is 256Kbps for port 1 ~ port 16, and 2048Kbps for port 17-18.

#### **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  $32\text{Kbps} \times 10$ ,  $32\text{Kbps} \times 20$ ,  $32\text{Kbps} \times 30$  and  $32\text{Kbps} \times 40$  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  $256\text{Kbps} \times 10$ ,  $256\text{Kbps} \times 20$ ,  $256\text{Kbps} \times 30$  and  $256\text{Kbps} \times 40$  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  $32\text{Kbps} \times 50$ ,  $32\text{Kbps} \times 60$ ,  $32\text{Kbps} \times 70$  and  $32\text{Kbps} \times 80$  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  $256\text{Kbps} \times 50$ ,  $256\text{Kbps} \times 60$ ,  $256\text{Kbps} \times 70$  and  $256\text{Kbps} \times 80$  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 Vi30018 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”.



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.

**VLAN Member Setting (Port Based)**

Name:  (Max 8 characters)

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Destination PORT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Source PORT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Destination PORT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Destination PORT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**VLAN MEMBER**

Portmap	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

**WARNING!**

Current Port-base VLAN Setting will be reset to default setting.  
If you click on "Continue" button to change to Tag-base VLAN mode,  
Otherwise, click on "Back" button to cancel.

## 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.

[illegible]

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

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 2:** Select/De-select VID source corresponding to this VID

### Step 3: Press “Update





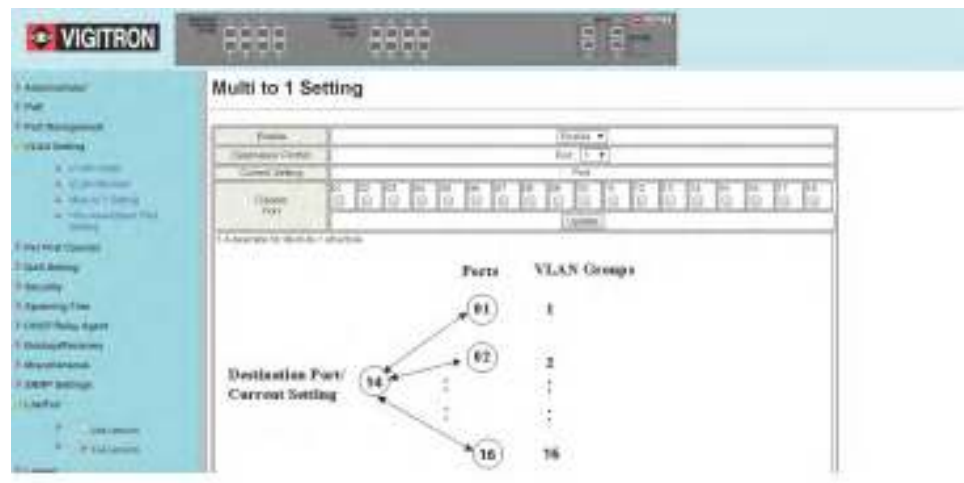
**NOTE:** The CPU control entry cannot be removed.

### 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.

- Administration
- Port Management
- Port Management
  - VLAN Setting
    - VLAN mode
    - VLAN number
    - Multi to 1 Setting
    - Non-Association Port Setting
  - Per Port Counter
  - QoS Setting
  - Security
  - Spanning Tree
  - Dot1P-Rate Agent
  - Backup/Recovery
  - Miscellaneous

### Multi to 1 Setting

Enable

Destination Port

Current Setting

Disable

Port

Update

1.A example for Multi-to-1 structure

Ports	VLAN Groups
01	1
02	2

- Administration
- Port Management
- Port Management
  - VLAN Setting
    - VLAN mode
    - VLAN number
    - Multi to 1 Setting
    - Non-Association Port Setting
  - Per Port Counter
  - QoS Setting
  - Security
  - Spanning Tree
  - Dot1P-Rate Agent
  - Backup/Recovery
  - Miscellaneous

### Multi to 1 Setting

Enable

Destination Port

Current Setting

Disable

Port

Update

1.A example for Multi-to-1 structure

Ports	VLAN	Groups
01	1	
02	2	

## 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



Port	Transmit Packet	Receive Packet
01	0	0
02	0	0
03	0	0
04	0	0
05	0	0
06	0	0
07	0	0
08	0	0
09	0	0
10	0	0
11	0	0
12	0	0
13	0	0



Port	Transmit Packet & Receive Packet	Drop packet & Receive Packet	CRC error packet & Receive Packet
01	0	0	0
02	0	0	0
03	0	0	0
04	0	0	0
05	0	0	0
06	0	0	0
07	0	0	0
08	0	0	0


### 13.1 Drop and Receive Packet



The screenshot shows the VISITRON software interface. On the left is a navigation menu with options like 'Dashboard', 'Hosts', 'Ports', 'Networks', 'Groups', 'Alerts', 'Reports', 'Settings', and 'Help'. The main area is titled 'Counter Category' and displays a table with columns for 'Port', 'Status', and 'Count'. The table lists various ports and their corresponding counts.

Port	Status	Count
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0
27	0	0

### 13.2 CRC error packet and Receive Packet



The screenshot shows the VISITRON software interface. On the left is a navigation menu with options like 'Dashboard', 'Hosts', 'Ports', 'Networks', 'Groups', 'Alerts', 'Reports', 'Settings', and 'Help'. The main area is titled 'Counter Category' and displays a table with columns for 'Port', 'Status', and 'Count'. The table lists various ports and their corresponding counts.

Port	Status	Count
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0
27	0	0
28	0	0
29	0	0
30	0	0
31	0	0
32	0	0
33	0	0
34	0	0
35	0	0
36	0	0
37	0	0
38	0	0
39	0	0
40	0	0
41	0	0
42	0	0
43	0	0
44	0	0
45	0	0
46	0	0
47	0	0
48	0	0
49	0	0
50	0	0
51	0	0
52	0	0
53	0	0
54	0	0
55	0	0
56	0	0
57	0	0
58	0	0
59	0	0
60	0	0
61	0	0
62	0	0
63	0	0
64	0	0
65	0	0
66	0	0
67	0	0
68	0	0
69	0	0
70	0	0
71	0	0
72	0	0
73	0	0
74	0	0
75	0	0
76	0	0
77	0	0
78	0	0
79	0	0
80	0	0
81	0	0
82	0	0
83	0	0
84	0	0
85	0	0
86	0	0
87	0	0
88	0	0
89	0	0
90	0	0
91	0	0
92	0	0
93	0	0
94	0	0
95	0	0
96	0	0
97	0	0
98	0	0
99	0	0
100	0	0

### 13.3 Counter Modes Defined

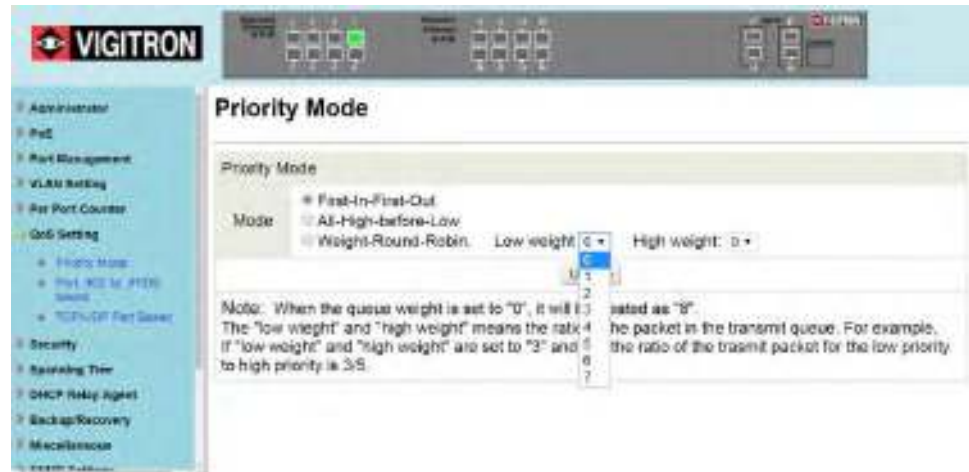
The 3 different operational modes are:

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.

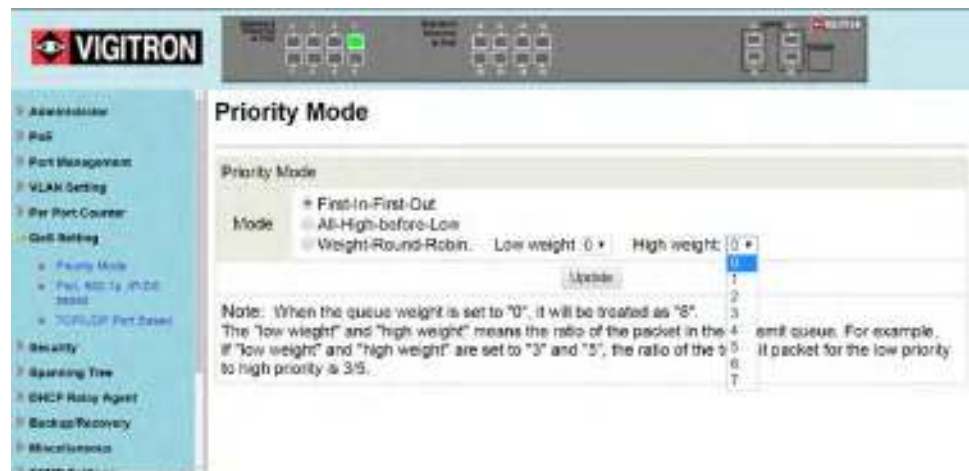
Switching between modes will clear the previous counter. Entering a mode will update the counter.



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.



gh, LLow 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: TCP/UDP port number the first, IP ToS/DS the second, 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 priority queue.

Priority 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 use for what are called privileged 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

**VIGITRON**

Class of Service Configuration

Protocol	Option
FTP(20,21)	F-I-F-Q *
SSH(22)	F-I-F-Q *
TELNET(23)	Discard
SMTP(25)	Low
DNS(53)	High
TFTP(69)	F-I-F-Q *
HTTP(80,8080)	F-I-F-Q *
POP3(110)	F-I-F-Q *
IMAP4(143)	F-I-F-Q *

**VIGITRON**

Port number (1-65535) Mask(0-255)

Port: Mask: Port: Mask: Port: Mask: Port: Mask:

Note: The mask defines which bit is ignored within the IP address bit 0 - bit 7. For example, UDP/TCP port = 65535 and mask = 5, this means 65530, 65531, 65534 and 65535 are all taken into account. UDP/TCP port = 65535 and mask=0, this means only 65535 is taken into account.

TCP/UDP port QoS function: Not Override \*

Note: When the "override" item is selected, the Port\_based, Tag\_based, User\_Defined, CoS listed above will be ignored.

Update

The Class of Service for TCP/UDP port number allows the network administrator to assign the specific application to a priority queue.

F-I-F-Q: The incoming packet will be forwarded in first-in-first-out scheme.  
Discard: The incoming packet will be discarded at the source port.  
High: The incoming packet will be forwarded with the high priority.  
Low: The incoming packet will be forwarded with the Low priority.

**VIGITRON**

MSN(1883)	F-I-F-Q *
XRD_RDP(3389)	F-I-F-Q *
QQ(4000,6000)	F-I-F-Q *
ICQ(5190)	F-I-F-Q *
Yahoo(5050)	F-I-F-Q *
BOOTP_DHCP(67,68)	Low *
User_Define_a	Low
User_Define_b	High
User_Define_c	F-I-F-Q *
User_Define_d	F-I-F-Q *

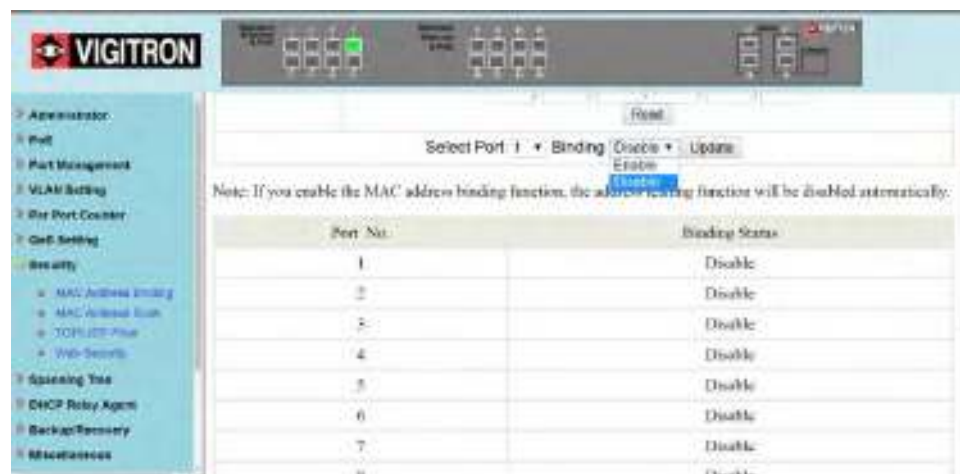
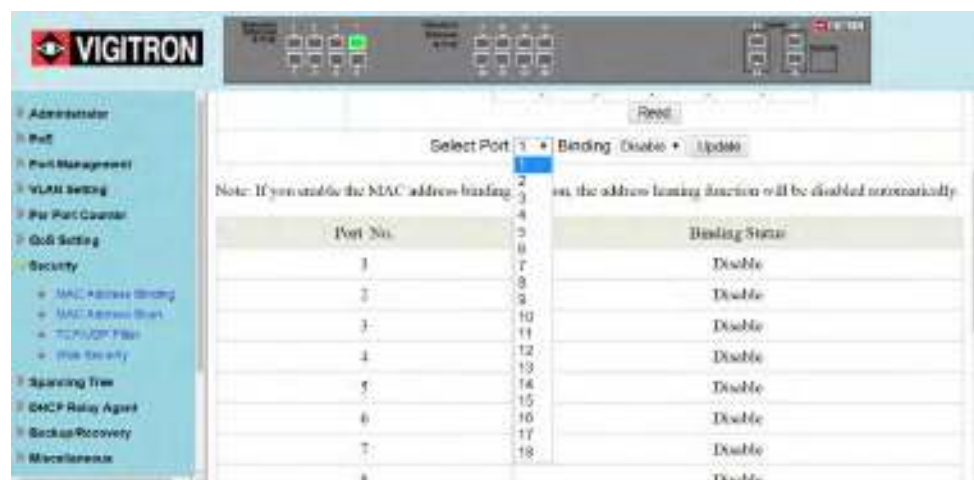
User\_Define Port number (1-65535) Mask(0-255)

User\_Define\_a Port: Mask: User\_Define\_b Port: Mask: User\_Define\_c Port: Mask: User\_Define\_d Port: Mask:





### 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.

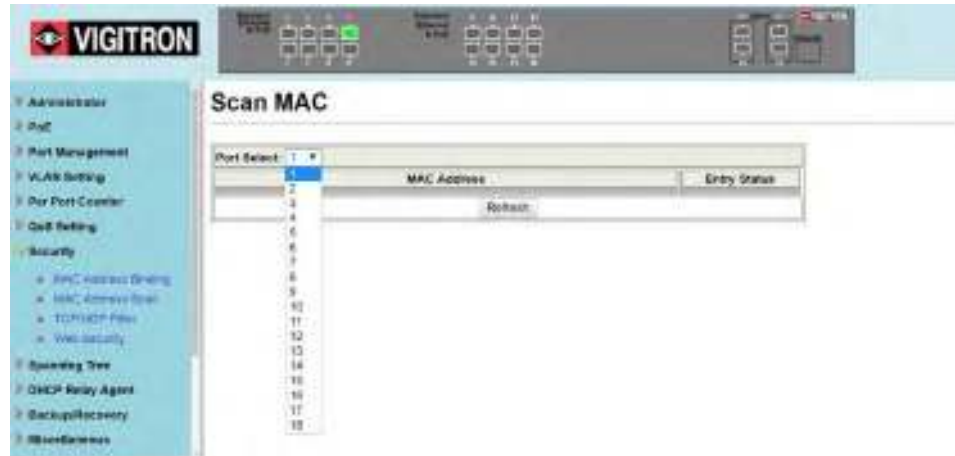
To activate the port binding function, you should enter the correct MAC address, select the port number, and set the port binding to “Enable” and then press “Update”.

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

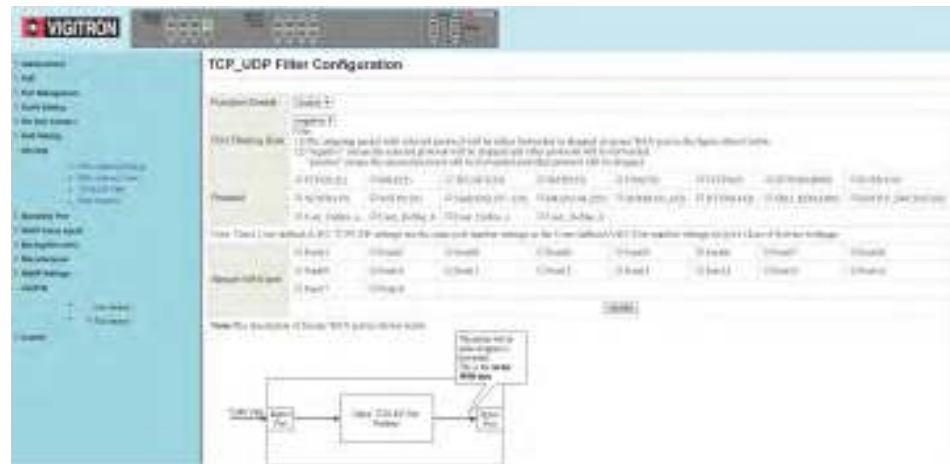
If no MAC address is entered when the scan is performed the MAC address of the connected device will be displayed and the “Entry Status” will show “Dynamic” indicating the address can change depending on the MAC address of the device.

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.



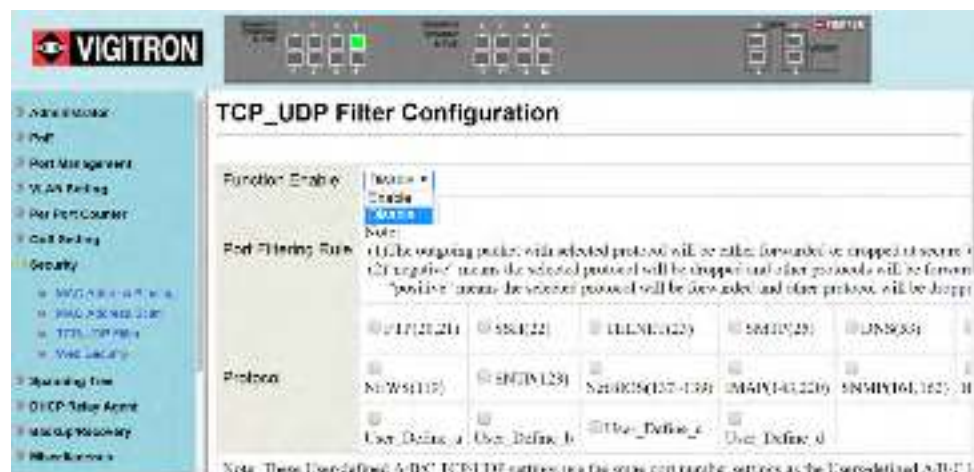
The figure shown below illustrates how this function is applied to the real environment.

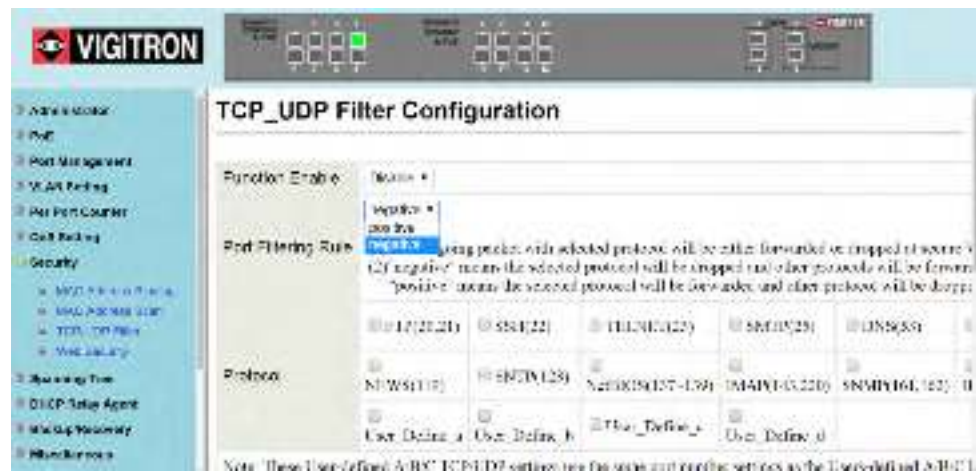
Example:

- Enable TCP/UDP Filter function.
- Select “positive” rule.
- Set port 5 as secure WAN port and select FTP and TELNET as the filtering protocol.
- 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.

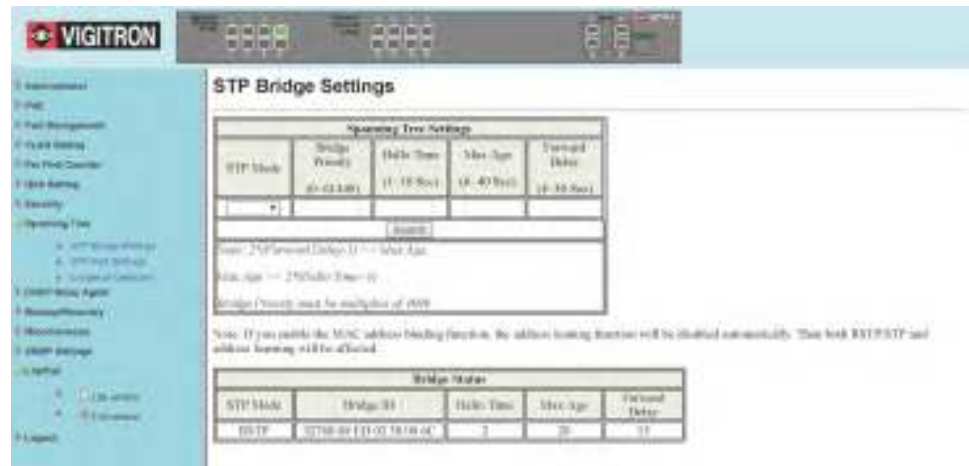




## Section 16: Spanning Tree

### 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:**  $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$ ,  $\text{Max Age} \geq 2 * (\text{Hello Time} + 1)$



## 16.1 STP Port Settings

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

Port No.	RPC	Priority	Status	Designated Port
1	100	100	Enable	---
2	100	100	Enable	---
3	100000000	1000	Enable	---
4	100000000	1000	Enable	---
5	100000000	1000	Enable	---
6	100000000	1000	Enable	---
7	100000000	1000	Enable	---
8	100000000	1000	Enable	---
9	100000000	1000	Enable	---
10	100000000	1000	Enable	---
11	100000000	1000	Enable	---
12	100000000	1000	Enable	---
13	100000000	1000	Enable	---
14	100000000	1000	Enable	---
15	100000000	1000	Enable	---
16	100000000	1000	Enable	---
17	100000000	1000	Enable	---
18	100000000	1000	Enable	---
19	100000000	1000	Enable	---
20	100000000	1000	Enable	---
21	100000000	1000	Enable	---
22	100000000	1000	Enable	---
23	100000000	1000	Enable	---
24	100000000	1000	Enable	---
25	100000000	1000	Enable	---
26	100000000	1000	Enable	---
27	100000000	1000	Enable	---
28	100000000	1000	Enable	---
29	100000000	1000	Enable	---
30	100000000	1000	Enable	---
31	100000000	1000	Enable	---
32	100000000	1000	Enable	---
33	100000000	1000	Enable	---
34	100000000	1000	Enable	---
35	100000000	1000	Enable	---
36	100000000	1000	Enable	---
37	100000000	1000	Enable	---
38	100000000	1000	Enable	---
39	100000000	1000	Enable	---
40	100000000	1000	Enable	---
41	100000000	1000	Enable	---
42	100000000	1000	Enable	---
43	100000000	1000	Enable	---
44	100000000	1000	Enable	---
45	100000000	1000	Enable	---
46	100000000	1000	Enable	---
47	100000000	1000	Enable	---
48	100000000	1000	Enable	---
49	100000000	1000	Enable	---
50	100000000	1000	Enable	---
51	100000000	1000	Enable	---
52	100000000	1000	Enable	---
53	100000000	1000	Enable	---
54	100000000	1000	Enable	---
55	100000000	1000	Enable	---
56	100000000	1000	Enable	---
57	100000000	1000	Enable	---
58	100000000	1000	Enable	---
59	100000000	1000	Enable	---
60	100000000	1000	Enable	---
61	100000000	1000	Enable	---
62	100000000	1000	Enable	---
63	100000000	1000	Enable	---
64	100000000	1000	Enable	---
65	100000000	1000	Enable	---
66	100000000	1000	Enable	---
67	100000000	1000	Enable	---
68	100000000	1000	Enable	---
69	100000000	1000	Enable	---
70	100000000	1000	Enable	---
71	100000000	1000	Enable	---
72	100000000	1000	Enable	---
73	100000000	1000	Enable	---
74	100000000	1000	Enable	---
75	100000000	1000	Enable	---
76	100000000	1000	Enable	---
77	100000000	1000	Enable	---
78	100000000	1000	Enable	---
79	100000000	1000	Enable	---
80	100000000	1000	Enable	---
81	100000000	1000	Enable	---
82	100000000	1000	Enable	---
83	100000000	1000	Enable	---
84	100000000	1000	Enable	---
85	100000000	1000	Enable	---
86	100000000	1000	Enable	---
87	100000000	1000	Enable	---
88	100000000	1000	Enable	---
89	100000000	1000	Enable	---
90	100000000	1000	Enable	---
91	100000000	1000	Enable	---
92	100000000	1000	Enable	---
93	100000000	1000	Enable	---
94	100000000	1000	Enable	---
95	100000000	1000	Enable	---
96	100000000	1000	Enable	---
97	100000000	1000	Enable	---
98	100000000	1000	Enable	---
99	100000000	1000	Enable	---
100	100000000	1000	Enable	---

Field	Description
Port No.	To configure the parameters of RSTP/STP port, the administrator should select a physical port number, assign a priority 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.
RPC (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.

**VIGITRON**

Loopback Detection Settings

Loopback Detect Function:

Auto Wake Up:

Wake-Up Time Interval:

Reset All Ports

Port No.	Status
1	---
2	---
3	---
4	---
5	---
6	---
7	---
8	---
9	---
10	---
11	---
12	---
13	---
14	---
15	---

**VIGITRON**

Loopback Detection Settings

Loopback Detect Function:

Auto Wake Up:

Wake-Up Time Interval:

Reset All Ports

Port No.	Status
1	---
2	---
3	---
4	---
5	---

**VIGITRON**

Loopback Detection Settings

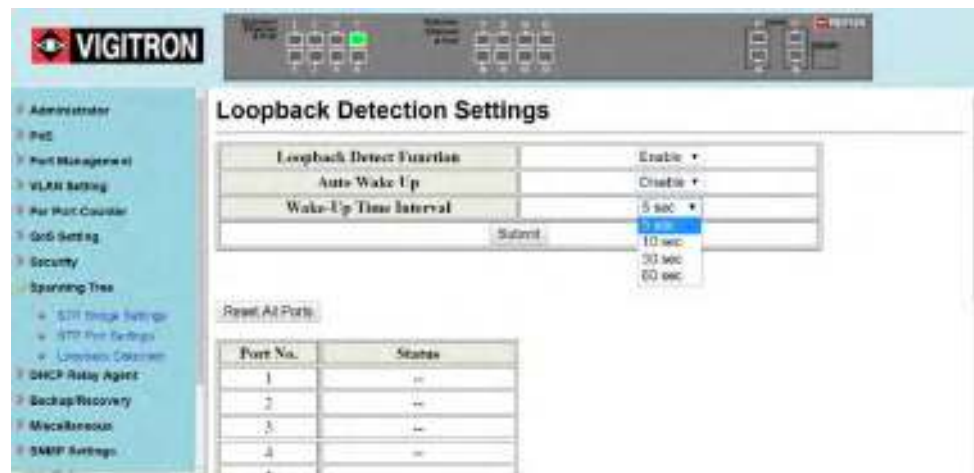
Loopback Detect Function:

Auto Wake Up:

Wake-Up Time Interval:

Reset All Ports

Port No.	Status
1	---
2	---
3	---
4	---
5	---



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.

## 16.3 Trunking



This page is used to set trunk group for load balance and cable link auto-backup. There are 2 methods to set a trunk; i.e. Static and LACP.

The meaning of each field shown in the following table is explained as following.

The switch supports three trunk groups, which can set port 1 ~ port 8, port 17 and port 18, and trunk 1 consists of port 1 ~ port 4, trunk 2 consists of port 5 ~ port 8, trunk 3 consists of port 17, port 18. Trunk hash algorithm can be selected according to 2 different methods.

Link Aggregation Algorithm	Description
SA	Among the trunk member ports, the packet will be distributed based on the source MAC address.
DA XOR SA	Among the trunk member ports, the packet will be distributed based on the XOR calculation result of the source MAC address and the destination MAC address

If Binding has been activated on the port, you cannot use Link Aggregation.





VLAN 1

VLAN 2

VLAN 3

VLAN 4

VLAN 5

- Administrator
- Port
- Port Management
- VLAN Setting
  - VLAN Mode
  - VLAN Member
  - VLAN to 1 Setting
  - Non-Associated Port Setting
- Per Port Counter
- QoS Setting
- Security
- Spanning Tree
- Trunking
  - Link Aggregation Settings

Refresh

	Link Group 1				Link Group 2				Link Group 3	
Member	P1	P2	P3	P4	P5	P6	P7	P8	P17	P18
	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇
	--	--	--	--	--	--	--	--	--	--
State	Disable ▾				Disable ▾				Disable ▾	
Type	LACP ▾				LACP ▾				LACP ▾	
Operation Key	1 (1-65535)				2 (1-65535)				3 (1-65535)	
Time Out	Short Time Out ▾				Short Time Out ▾				Short Time Out ▾	
Activity	Passive ▾				Passive ▾				Passive ▾	
Submit										

Note: If you enable LACP on some specified ports and their link partners are normal port without LACP, these specified ports cannot transmit packet to receive packet from the link partner.

VLAN 1

VLAN 2

VLAN 3

VLAN 4

VLAN 5

- Administrator
- Port
- Port Management
- Per Port Counter
- Link
- Security
- Logout

Refresh

	Link Group 1				Link Group 2				Link Group 3	
Member	P1	P2	P3	P4	P5	P6	P7	P8	P17	P18
	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇
	--	--	--	--	--	--	--	--	--	--
State	Disable ▾				Disable ▾				Disable ▾	
Type	LACP ▾				LACP ▾				LACP ▾	
Operation Key	1 (1-65535)				2 (1-65535)				3 (1-65535)	
Time Out	Short Time Out ▾				Short Time Out ▾				Short Time Out ▾	
Activity	Passive ▾				Passive ▾				Passive ▾	
Submit										

Note: If you enable LACP on some specified ports and their link partners are normal port without LACP, these specified ports cannot transmit packet to receive packet from the link partner.

VLAN 1

VLAN 2

VLAN 3

VLAN 4

VLAN 5

- Administrator
- Port
- Port Management
- VLAN Setting
  - VLAN Mode
  - VLAN Member
  - VLAN to 1 Setting
  - Non-Associated Port Setting
- Per Port Counter
- QoS Setting
- Security
- Spanning Tree
- Trunking
  - Link Aggregation Settings

Refresh

	Link Group 1				Link Group 2				Link Group 3	
Member	P1	P2	P3	P4	P5	P6	P7	P8	P17	P18
	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇
	--	--	--	--	--	--	--	--	--	--
State	Disable ▾				Disable ▾				Disable ▾	
Type	LACP ▾				LACP ▾				LACP ▾	
Operation Key	1 (1-65535)				2 (1-65535)				3 (1-65535)	
Time Out	Short Time Out ▾				Short Time Out ▾				Short Time Out ▾	
Activity	Passive ▾				Long Time Out ▾				Passive ▾	
Submit										

Note: If you enable LACP on some specified ports and their link partners are normal port without LACP, these specified ports cannot transmit packet to receive packet from the link partner.

- Administrator
- Port Management
- VLAN Setting
  - VLAN Enable
  - VLAN Member
  - VLAN Trunk Setting
  - VLAN Access/Trunk Port Setting
- Per Port Counter
- QoS Setting
- Security
- Spanning Tree
  - STP Aggregation Setting
- Link Aggregation

Refresh

	Link Group 1				Link Group 2				Link Group 3	
Member	P1	P2	P3	P4	P5	P6	P7	P8	P17	P18
	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇
State	Disable ▾				Disable ▾				Disable ▾	
Type	LACP ▾				LACP ▾				LACP ▾	
Operation Key	1 (1-65535)				2 (1-65535)				3 (1-65535)	
Time Out	Short Time Out ▾				Short Time Out ▾				Short Time Out ▾	
Activity	Passive ▾				Passive ▾				Passive ▾	
<div>Submit</div> <div>Passive ▾</div> <div>Active</div>										

Note: If you enable LACP on some specified ports and their link partners are normal port without LACP, these specified ports cannot transmit packet to receive packet from the link partner.

- Administrator
- Port Management
- Per Port Counter
- Security
- Link Aggregation
- Logout

Refresh

	Link Group 1				Link Group 2				Link Group 3	
Member	P1	P2	P3	P4	P5	P6	P7	P8	P17	P18
	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇
State	Disable ▾				Disable ▾				Disable ▾	
Type	LACP ▾				LACP ▾				LACP ▾	
Operation Key	1 (1-65535)				2 (1-65535)				3 (1-65535)	
Time Out	Short Time Out ▾				Short Time Out ▾				Short Time Out ▾	
Activity	Passive ▾				Passive ▾				Passive ▾	
<div>Submit</div> <div>Passive ▾</div> <div>Active</div>										

Note: If you enable LACP on some specified ports and their link partners are normal port without LACP, these specified ports cannot transmit packet to receive packet from the link partner.

- Administrator
- Port Management
- Per Port Counter
- Security
- Link Aggregation
- Logout

Refresh

	Link Group 1				Link Group 2				Link Group 3	
Member	P1	P2	P3	P4	P5	P6	P7	P8	P17	P18
	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇	⬇
State	Disable ▾				Disable ▾				Disable ▾	
Type	LACP ▾				LACP ▾				LACP ▾	
Operation Key	1 (1-65535)				2 (1-65535)				3 (1-65535)	
Time Out	Short Time Out ▾				Short Time Out ▾				Short Time Out ▾	
Activity	Passive ▾				Passive ▾				Passive ▾	
<div>Submit</div> <div>Passive ▾</div> <div>Active</div>										

Note: If you enable LACP on some specified ports and their link partners are normal port without LACP, these specified ports cannot transmit packet to receive packet from the link partner.


**VIGITRON**




**VIGITRON**

- Administrator
- Pub
- Port Management
- Per-Port Config
- Security
- Link/Port
- Logout

Switch

Member	Link Group 1				Link Group 2				Link Group 3	
	P1	P2	P3	P4	P5	P6	P7	P8	P17	P18
	off	off	off	off	off	off	off	off	off	off
	on	on	on	on	on	on	on	on	on	on
State	Disable +				Disable +				Disable +	
Type	LACP +				LACP +				LACP +	
Operation Key	1 (1-65535)				2 (1-65535)				3 (1-65535)	
Time Out	Short Time Out +				Short Time Out +				Short Time Out +	
Activity	Passive +				Passive +				Passive +	
<input type="button" value="Submit"/>										

If you enable LACP on some specified ports and their link partners are normal port without LACP, these

Page | 88





Member	Link Group 1				Link Group 2				Link Group 3	
	P1	P2	P3	P4	P5	P6	P7	P8	P17	P18
	A	A	A	A	A	A	A	A	A	A
State	Disable				Disable				Disable	
Type	LACP				LACP				LACP	
Operation Key	1 (1-65535)				2 (1-65535)				3 (1-65535)	
Time Out	Short Time Out				Short Time Out				Short Time Out	
Activity	Passive				Passive				Passive	

Submit

If you enable LACP on some specified ports and their link partners are normal port without LACP, these specified ports cannot transmit packet to/receive packet from the link partner.

Field	Description
Member	There are three configurable trunk groups. “--” means the trunk has not been built on the corresponding port. “A” means trunk has been built on the corresponding port.
State	Administrator can enable/disable the function of this trunk.
Type	Static: Static setting by manual. LACP: Setting by ACP.
Operation Key	Assign an operation key for this device
Time out	Short Time Out: Re-configure LACP trunk every 1 second. Long Time Out: Re-configure LACP trunk every 30 second.
Activity	You should set at least one side of each trunk to “Active” state. If both sides of a trunk are all set to “Passive”, LACP trunk will never be built up.

## 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.





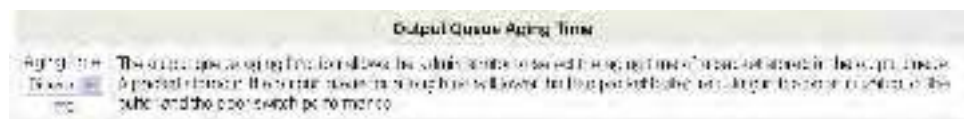
## Section 19: Miscellaneous Settings

### 19.0 Miscellaneous Settings Defined

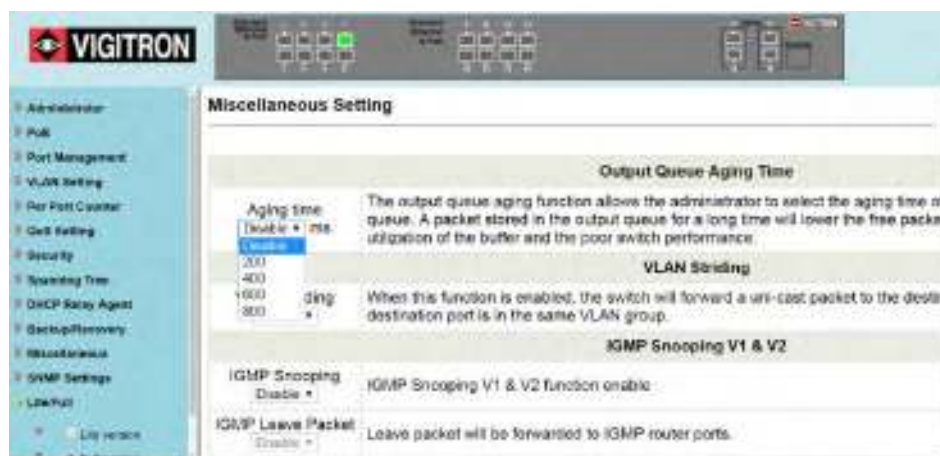


Miscellaneous setting is used to configure Output Queue Aging Time, VLAN Striding, IGMP Snooping and VLAN Uplink.

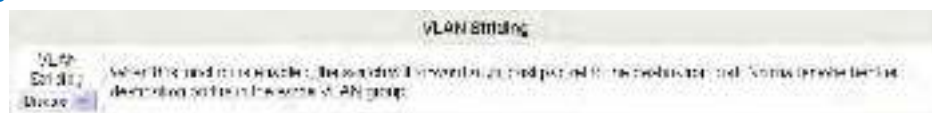
### 19.1 Output Queue Aging Time



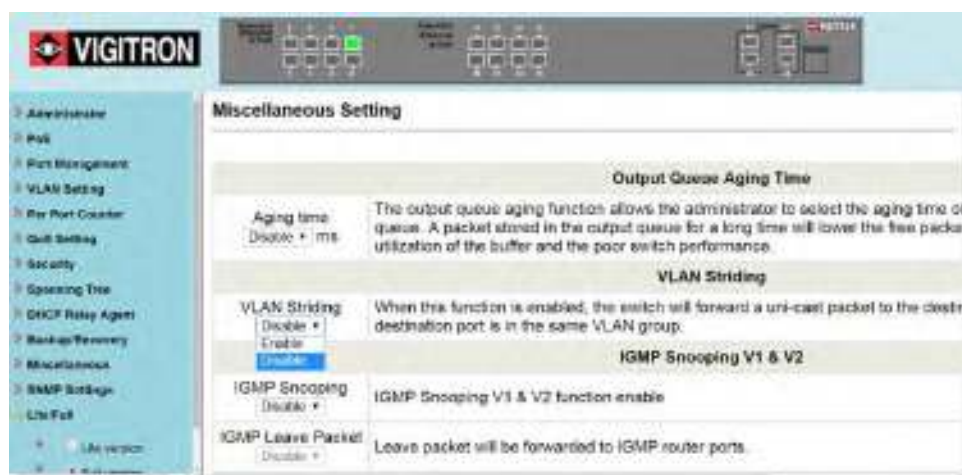
This function is used to avoid the poor utilization of the switch. When a packet is stored in a switch for a long time, the time slot defined by the protocol will expire and this packet becomes useless. To prevent these useless packets from wasting the bandwidth, this switch provides an option to enable 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 enable “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-cast 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 field 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.

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 192.18.1.133. 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”

“Loss of Traffic Detected Port xx”

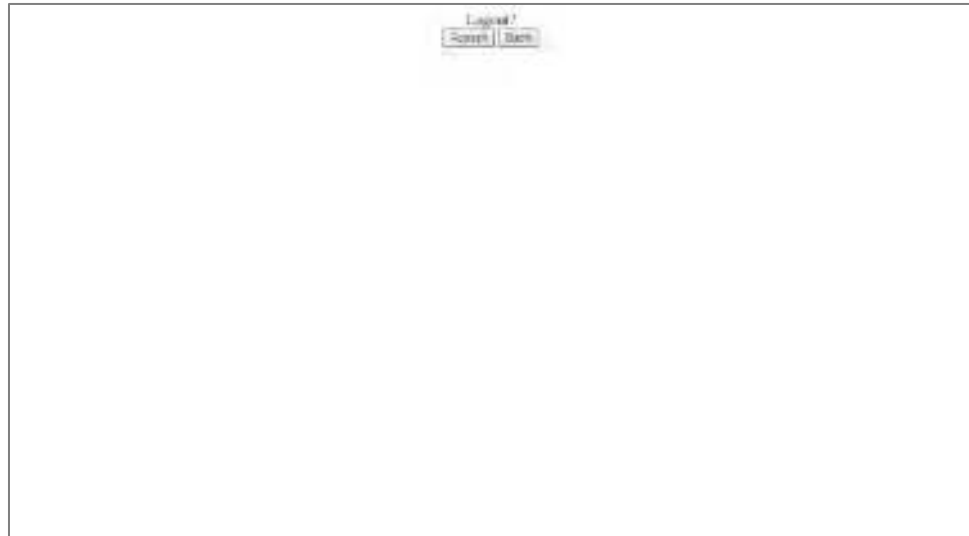
“Authentication Failure: This message is sent when someone tries to login with incorrect information.”

“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 from 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.

## 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 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**

CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

## **CCM**

CCM is an acronym for Continuity Check Message. It is 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**

DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

## **DES**

DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

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**

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP 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**

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

## **DNS**

DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

## **DoS**

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

## **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**

DSCP is an acronym for Differentiated Services Code Point. It 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**

FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

## **Fast Leave**

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

## **H**

## **HTTP**

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

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

/

## **ICMP**

ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as 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**

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

## **IGMP Querier**

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

## **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

LOC is an acronym for Loss of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as 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

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

## **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**

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

### **NetBIOS**

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

The NetBIOS 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**

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

## 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 then 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

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

### PD

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

### PHY

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

### PING

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

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

### PoE

PoE is an acronym for Power over Ethernet. Power over Ethernet is used to transmit electrical power to remote devices over standard Ethernet cable. It could 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**

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

## **Q**

## **QCE**

QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID. There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

## **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**

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

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

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



## R

### RARP

RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

### RADIUS

RADIUS is an acronym for Remote Authentication Dial in User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

### RDI

RDI is an acronym for Remote Defect Indication. It is 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

SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

### 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**

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

## **SNTP**

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

## **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**

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

## **SSM**

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

## **STP**

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

## **SyncE**

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

## T

### TACACS+

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

### Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

### TCP

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

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

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

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

### TELNET

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

### TFTP

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

## U

### UDP

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

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

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

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

### 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.

# SFP Interface Guide

	Bandwidth	(Vi30018), Vi30126, Vi31026, Vi31126, Vi32026, Vi32126, Vi35126	Vi3010 / Vi3026	Compatible
		SFP port 25-26 (Vi30018 ports 17-18)	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	(Vi30018), Vi30126, Vi31026, Vi31126, Vi32026, Vi32126, Vi35126	Vi5001	Compatible
		SFP port 25-26 (Vi30018 ports 17-18)	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	(Vi30018), Vi30126, Vi31026, Vi31126, Vi32026, Vi32126, Vi35126	Vi50001	Compatible
		SFP port 25-26 (Vi30018 ports 17-18)	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	(Vi30018), Vi30126, Vi31026, Vi31126, Vi32026, Vi32126, Vi35126	Vi3005	Compatible
		SFP port 25-26 (Vi30018 ports 17-18)	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	(Vi30018), Vi30126, Vi31026, Vi31126, Vi32026, Vi32126, Vi35126	Vi30005	Compatible
		SFP port 25-26 (Vi30018 ports 17-18)	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

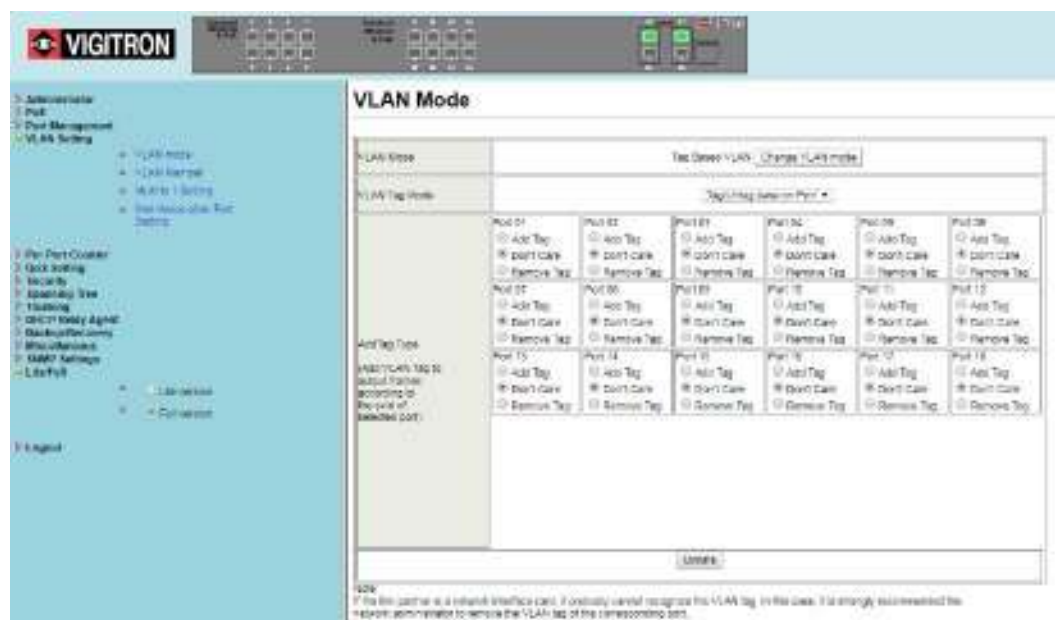


# Connecting Vi30018

When connecting the Vi30018 to other model Switches, it is sometimes 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 17



## Contact Information

**Vigitron, Inc.**

7810 Trade Street, Suite 100

San Diego, CA 92121

[support@vigitron.com](mailto:support@vigitron.com)

Tel: (858) 484-5209

Fax: (858) 484-1205

[www.vigitron.com](http://www.vigitron.com)