

MaxiiNet[™] Vi30126 Operational Manual

Vi30126

Release F30126V1.05

Section 1: About This Manual

1.0 Copyright

Copyright © 2017 Vigitron, Inc. All rights reserved. The products and programs described in this User's Manual are licensed products of Vigitron Inc. This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted. No parts of this User's Manual may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable from any means by electronic or mechanical. This includes photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of Vigitron, Inc.

1.1 Purpose

This Manual gives specific information on how to operate and use the management functions of the (insert model(s)).

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 marks 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 RJ-45 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	Class A
22:2006+A1:2006	4K V CD, 8KV, AD
IEC61000-4-2 (2001)	3V/m
IEC61000-4-3(2002)	1KV – (power line), 0.5KV – (signal line)
IEC61000-4-4(2004)	Line to Line: 1KV, Line to Earth: 2KV
IEC61000-4-5 (2001)	130dBuV(3V) Level 2
IEC61000-4-6 (2003)	1A/m
IEC61000-4-8 (2001)	Voltage dips:
	>95%, 0.5period, 30%, 25periods
IEC61000-4-11(2001)	Voltage interruptions:
	>95%, 250periods

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

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.
- If you need using outdoor device connect to this device with cable, then you need to add an arrester on the cable between outdoor device and this device.



Fig. Addition arrester between outdoor device and this switch

The Vi30126 supports SFP conforming to MSA standards, although differences between manufacturers can affect performance. For best results, use Vigitron SFPS.



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

WARNING:

- Self-demolition on product is strictly prohibited. Damage caused by self-demolition will be charged for repairing fees.
- Do not place product 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
F30126V1.00	07-2017	
F30126V1.05	06-2018	

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

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

21 23	25 Uplink 25	VIGITRON
亡亡		
		Console

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

Fiber Optics					
	1 11	1	1	rta I	
		_	_		
	F				
	_	_	_	_	
				8	

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:

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

.

Section 1: About This Manual	2
1.0 Copyright	2
1.1 Purpose	2
1.2 Audience	2
1.3 Conventions	2
1.4 Warranty	2
1.5 Disclaimer	3
Section 2: Compliances and Safety Statements	4
2.0 FCC Class A	4
2.1 FCC Caution	4
2.2 CE Mark Warning	4
2.3 CE Declaration of Conformance for EMI and Safety (EEC)	5
2.4 UL Mark	5
2.5 EMC	5
2.6 Related Publications	7
2.7 Revision History	7
Section 3: Introduction	
3.0 Overview	
3.1 Cabling Guidelines	17
3.2 Connecting to PCs, Servers, Hubs and Switches	
3.3 Network Wiring Connection	
3.4 Vi30126 – Front View	
3.5 Vi30126 – Rear View	19
Section 4: Description of Hardware	20
4.0 1000Base-T Ports	
4.1 SFP Transceivers Slots	20
4.2 Ports and System Status LEDs	
4.3 Console Port	
Section 5: Installing the Switch	22
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
Section 6: Making Network Connections	27
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
Section 7: Troubleshooting	29
7.0 Basic Troubleshooting Tips	29
7.1 Table 10: Troubleshooting Chart	30
Section 8: Operation of Web-Based Management	31
8.0 Initial Configuration	31
Section 9: Administration	33
9.0 Prior to Logging On	33
9.1 Logging On	33
9.2 System IP Configuration	36
9.3 System Status	36
9.4 Load Default	38
9.5 Firmware Update	39
Section 10: PoE	42
10.0 PoE Status	42
10.1 PoE Setting	43
10.2 PoE Event Counter	46
10.3 PoE Power Delay	47
10.4 PoE Auto Check	48
Section 11: Port Management	50
11.0 Port Configuration	50
11.1 Port Mirroring	59
11.2 Bandwidth Control	60
11.3 Broadcast Storm Control	63
Section 12: VLAN Settings	64
12.0 VLAN Mode	64

12.1 VLAN Member (Port Based)	65
12.2 VLAN Member Settings (Tag Based)	67
12.3 Multi to 1 Setting	69
12.4 Non-Association Port Setting	71
Section 13: Per Port Counter	72
13.0 Transmit Packet and Receive Packets	72
13.1 Drop and Receive Packet	73
13.2 CRC error packet and Receive Packet	73
13.3 Counter Modes Defined	74
Section 14: QoS Settings	75
14.0 Priority Mode	75
14.1 Setting the Priority Mode	75
14.2 Class of Service Configuration	76
Section 15: Security	80
15.0 MAC Address Binding	80
15.1 Scanning MAC Addresses	82
15.2 Securing Ports Using Mac Addresses	
15.3 TCP/UDP Filter	83
15.4 Secure WAN Port: Select the port to be secured	85
Section 16: Spanning Tree	86
16.0 STP Bridge Settings	86
16.1 STP Port Settings	87
16.2 Loopback Detection Settings	88
16.3 Trucking	91
Section 17: DHCP Relay Agent	95
17.1 Relay Agent Configurations	95
Section 18: Backup and Recovery	98
18.0 Configuration Backup/Recovery	98
18.1 Back Up	98
18.2 Recovery	98
Section 19: Miscellaneous Settings	99
19.0 Miscellaneous Settings Defined	99
19.1 Output Queue Aging Time	99
19.2 VLAN Striding	100
19.3 IGMP Snoop V1 & V2	101
19.4 VLAN Uplink	102

19.5 UDP/TCP Alert Messages	
19.6 SNMP Settings	
19.7 SNMP Trap States	
Section 20: Log Out	107
20.0 Log Out Procedure	
Section 21: Glossary	
Α	
ACE	
ACL	
AES	
APS	
Aggregation	
ARP	
ARP Inspection	
Auto-Negotiation	
C	
CC	
CCM	
CDP	
D	
DEI	
DES	
DHCP	
DHCP Relay	
DHCP Snooping	
DNS	
DoS	
Dotted Decimal Notation	
DSCP	
E	
EEE	
EPS	
Ethernet Type	
F	
FTP	
Fast Leave	

Н	112
HTTP	112
HTTPS	113
Ι	113
ICMP	
IEEE 802.1X	
IGMP	
IGMP Querier	
IP	
L	
LACP	
LLC	
LLDP	
LLDP-MED	
LOC	
М	
MAC Table	
Mirroring	
MLD	
MVR	
Ν	
NAS	
NetBIOS	
NFS	
NTP	
O	
OUI	
Option 82	
P	
PCP	
PD	
PHY	
PING	
PoE	
Policer	
Private VLAN	

PTP	118
Q	118
QCE	118
QCL	118
QL	
QoS	
R	
RARP	
RADIUS	119
RDI	119
RSTP	119
S	119
SHA	119
Sharper	119
SMTP	119
SNAP	
SNMP	120
SNTP	120
SSID	120
SSH	120
SSM	120
STP	120
SyncE	120
Т	121
TACACS+	121
Tag Priority	121
ТСР	
TELNET	121
TFTP	121
U	121
UDP	121
User Priority	122
V	122
VLAN	122
VLAN ID	122
Voice VLAN	123

SFP Interface Guide	124
Connecting Vi30126	127
Contact Information	

Section 3: Introduction

3.0 Overview

This user's manual will not only tell you how to install and connect your network system, but how to configure and monitor the Vi30126 through the web by (RJ-45) serial interface and Ethernet ports step-by-step. Many detailed explanations of hardware and software functions are shown, as well as, the examples of the operation for web-based interface.

The Vi30126 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:

- 26 total Ethernet ports
- 24 Ports at 10/100 Mbps
- 2 Ports at 1000Mbps
- Layer 2 network switch
- 685 watts total power supply
- 550 watts PoE budget
- Up to 36 watts per port
- Up to 65 watts per port for standard and extended UTP ports

3.1 Cabling Guidelines

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

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

The RJ-45 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 RJ-45 port. This will damage the switch. Use only twisted-pair cables with RJ-45 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 RJ-45 connector.

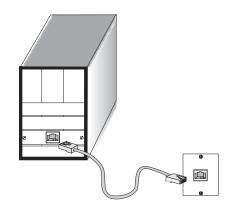


Figure 16: Making Twisted-Pair Connections

Step 2: If the device is a network card and the switch is in the wiring closet, attach the other end of the cable segment to a modular wall outlet that is connected to the wiring closet (see the section "Network Wiring Connections"). Otherwise, attach the other end to an available port on the switch.

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



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

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

3.3 Network Wiring Connection

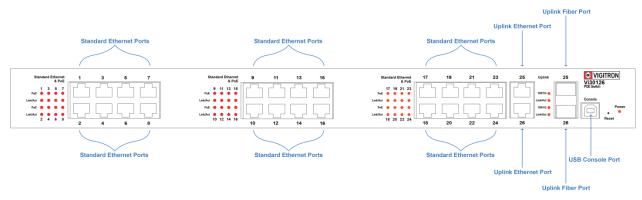
Today, the punch-down block is an integral part of many of the newer equipment racks. It is actually part of the patch panel. Instructions for making connections in the wiring closet with this type of equipment are as follows:

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

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

Step 3: Label the cables to simplify future troubleshooting.

3.4 Vi30126 – Front View



3.5 Vi30126 – Rear View



Section 4: Description of Hardware

4.0 1000Base-T Ports

The switch contains 24100BASE-T RJ-45 and 2, 1000Mbps ports. All RJ-45 ports support automatic MDI/MDI-X operation, auto-negotiation and IEEE 802.3x auto-negotiation of flow control, so the optimum data rate and transmission can be selected automatically.

4.1 SFP Transceivers Slots

Vi30126 supports the Small Form Factor Pluggable (SFP) transceiver slots. The slots are shared with RJ-45 port 25 to 26. In the default configuration, if an SFP transceiver (purchased separately) is installed in a slot and has a valid link on the port, the associated RJ-45 port is disabled.

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

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

Table 1: Supported SFP Transceivers

NOTE:

* Maximum distance may vary for different SFP vendors.

* Regardless of the SFP speed, ports 1-24 are 100Mbps / Ports 25 & 26 are 1Gbps.

* SFP must be matched at both cable ends.

* For ports 25 and 26, SFP port speed is fixed at 1000Mbps and cannot be changed.



4.2 Ports and System Status LEDs

The Vi30126 includes a display panel for system and port indications that simplify installation and network troubleshooting. The LEDs are located on left hand side of the front panel for easy viewing. Details are shown below and described in the following tables.

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

 Table 2: Port Status LEDs

SYSTEM LED	Condition	Status
Power	Green OFF	Lit when power is coming up
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

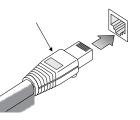
The switch can be mounted in a standard 19-inch equipment rack or on a flat surface. Be sure to follow the guidelines below when choosing a location.

- 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.
 - o 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 Vi30126 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 RJ-45 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.



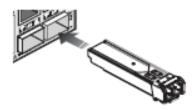


Figure 7: RJ-45 Connections

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:

- Vi30126 100Mbps + 1000Mbps Management Switch
- Mounting Accessory (for 19" Rack Shelf)
- 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.

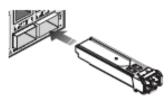


Figure 12: Inserting an SFP Transceiver into a Slot

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.

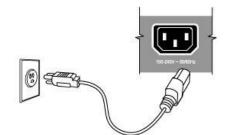


Figure 13: Inserting the Power Cord to AC Power Socket

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 RJ-45 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 RJ-45 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 RJ-45 port. This will damage the switch. Use only twisted-pair cables with RJ-45 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 RJ-45 connector.

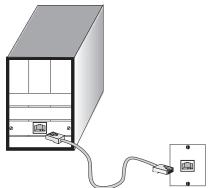


Figure 16: Making Twisted-Pair Connections

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 (100 Mbps) or amber (100 Mbps) to indicate that the connection is valid.

6.4 Network Wiring Connections

i

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.

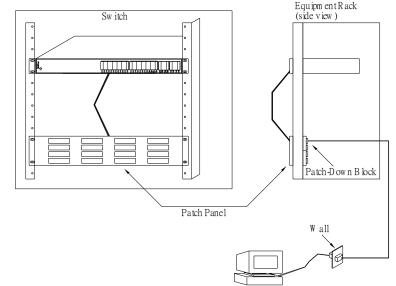


Figure 17: Network Wiring Connections

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 RJ-45 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 Vi30126 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 Vi30126 Switch devices are configured to auto negotiate, or are configured to connect at half duplex (all hubs are configured this way, for example).

- Faulty or loose cables. Look for loose or obviously faulty connections. If they appear to be OK, make sure the connections are snug. If that does not correct the problem, try a different cable.
- Non-standard cables. Non-standard and mis-wired cables may cause network collisions and other network problems, and can seriously impair network performance. Use a new correctly-wired cable for pin-outs and correct cable wiring. A category 5 cable tester is a recommended tool for every 100Base-TX and 1000Base-T network installation.
- Improper Network Topologies. It is important to make sure you have a valid network topology. If you no longer experience the problems, the new topology is probably at fault. In addition, you should make sure that your network topology contains *no data path loops.*

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

7.1 Table 10: Troubleshooting Chart

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

Section 8: Operation of Web-Based Management

8.0 Initial Configuration

This chapter instructs you on how to configure and manage the Vi30126 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.

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

The default values of the Vi30126 are listed in the table below:

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

After the Vi30126 has been finished configuration, you can browse the interface. For instance, if you type <u>http://192.168.1.133</u> 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 Vi30126 will not give you a shortcut to username automatically. This looks inconvenient, but it's the safer option.

The Vi30126 supports a simple user management function to allow only one administrator to configure the system at any one time. *The use of simultaneous administrators could result in unpredictable operation.* Additional users, even with administrator's identity, should only monitor the system. Those who have no administrator's identity can only monitor the system. It is suggested, regardless of security level, that viewing is limited to one client at a time. Also, after accessing the Vi30126 and viewing is complete, log out.



Connections involving the input of routers and use of clients accessing servers, the internet, or other networks can result in *a brief disconnection of client's access to the switch GUI*. It is recommended that after programming or monitoring, clients log out and that users without administrator access be allowed only a minimal access period.

NOTE: When you log into the Switch WEB to manage, you must first type the username of the admin. Password is blank. So after you type in the username, please press enter. Management page will enter WEB. When you log into Vi30126 series switch Web UI management, you can use both ipv4 ipv6 login to manage. To optimize the display effect, we recommend you use Microsoft Edge above, Firefox, Chrome and OS and have the resolution 1024x768. The switch supported neutral web browser interface. If the UI is not working with any versions of the above browser, it might result from PC security system setting.

i

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

Section 9: Administration

9.0 Prior to Logging On

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

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

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

9.1 Logging On

i

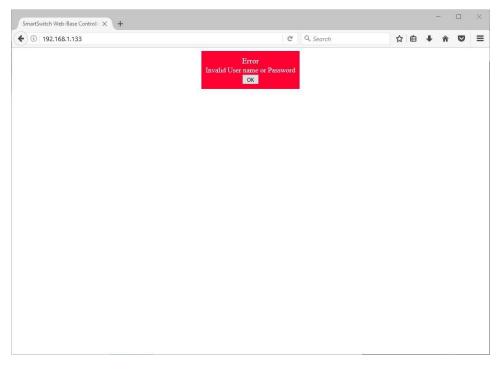
- Enter the correct administrator name and password after the login page shows up.
- Default IP address: 192.168.1.133
- Default administrator name: admin
- Default password: system
- Press "OK" to login.

JSER	LOG IN	
Site:	192.168.1.133	
ID:	admin	
Password:	•••••	
	OK	



NOTE: the administrator name and password fields are casesensitive. 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

	Browned Browned Browned Company Com	
PoE	24-Port	10/100Mbps Plus 2-Port Gigabit Ethernet Switch
Port Management	Advanced Features	Basic Features
Security Lite/Full	Bandwidth control Port based & Tag based VLAN Statistics Counter Firewall VLAN Uplink L2 - L4 Class of Service	Embedded HTTP web Management Configuration Backup/Recovery TFTP Firmware upgradeable Secure Management User name/Password security

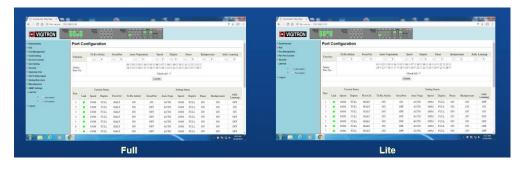
Lite Version

👁 VIGITRON 📃		
Administrator For California Port Management Por Port Counter Security Life Full Clarverson Full version Life version Life version Life version Life version	ort 10/100Mbps Plus 2-Port Gigabit Ethernet Switch Basic Features Etholodidel HTTP web Management - Configuration BiochapRecovery - TTPT Primare logipaloale - Secure Management - User namePassword securty	

Selecting Operating Mode:

i

The Vi30126 provides two separate operating modes. The lite version provides set-ups for addressing, PoE and bandwidth, while the full mode provides for all set-ups. These modes can be used to simplify set-ups and operations.



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

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

VIGITRON		Standard J H H H 15 Ethemet A PoE H H H H H H H H H H H H H H H H H H H	Sport 1 0 2 3 S Optim S C EDenast S Poc B 7 0 2 3 S Optim S C C 0 2 3	
* Administrator	Authentication	Configuratio	on	
 Authentication Configuration 				
 System IP Configuration 	Setting		Value	
System Status	Username	admin	max:15	
Reboot Device PoE	Password Confirm		max:15	
Port Management Per Port Counter			Update	
 Percentroller Security LiteFull Logout 	Note: Username & Password c:	an only use "a-z","A	-Z","0-9","_","+","-","=".	
 Enter t 	he administr	ator user	s name – up to 1	5 characters

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

9.2 System IP Configuration

VIGITRON	Standard 1 3 5 7 Elbernet 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
	System IP Con	figuration
 Authentication Configuration 		
 System IP Configuration 	Setting	Value
System Status	IP Address	192 . 168 . 1 . 133
 Reboot Device PoE 	Subnet Mask	255 . 255 . 0
Port Management	Gateway	192 . 168 . 1 . 254
Per Port Counter	IP Configure	Static DHCP
Security Lite/Full		Update
 Lite version Full version Logout 		
IP Address:	Entor a vali	d IvP4 address.
IF Auuress.		

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

- Gateway: Enter a gateway address making the value is the same as the IP address.
- IP Configure: Select Static or DHCP. Select will operate based on the above entries. If DHCP, the switch must be connected to server that will provide an address. In many cases you will not be able to know the IP address from the switch itself.

9.3 System Status

Authentication Configuration System IP Configuration	MAC Address	08:ed:02:58:13:88
System Status	Number of Ports	24S+2U
	Comment	switch MAX:15
rt Management	System Version	F30126V1.00
Port Counter curity %/Full jout	Idle Time Security	Idle Time: 0 (1~30 Minutes) Auto Logout(Default). Back to the last display.
		Update
	lote: comment name only can use "a-z",	"A-Z","_","+","-","0-9"

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

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

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

System Version: Is fixed and displays the current firmware version

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

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

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

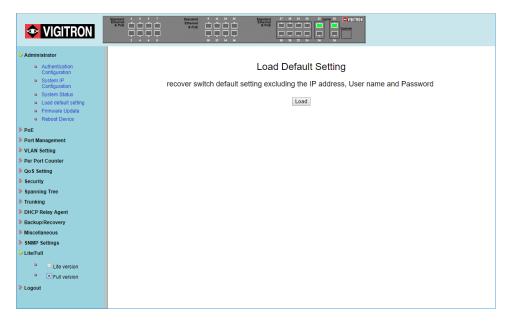


NOTE: If only the Idle Time Security function is selected, Auto logout will be the default mode for this function.

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

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

9.4 Load Default



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

- IP address
- User Name
- Password



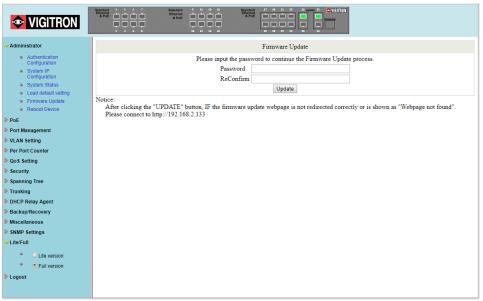
NOTE: In models where the firmware version ends in 1.03, the switch will default to an IP address of 192.168.1.1.

i Se

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

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

9.5 Firmware Update

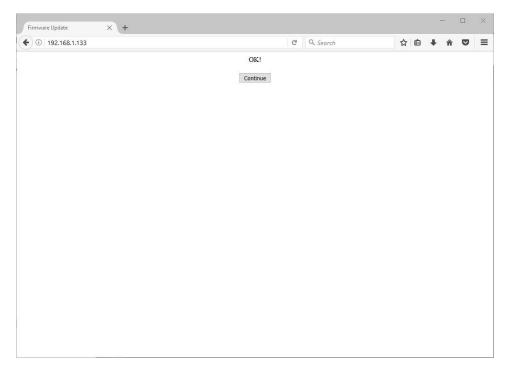


When pressing the update button, it redirects. If the system does not redirect or "webpage not found", please enter the address http://192.168.1.133.

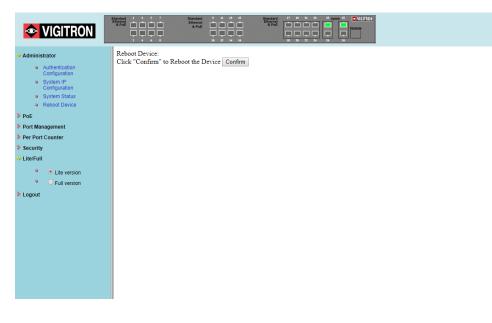
🔿 Firmware Update 🛛 🕹 +						-	-		×
(192.168.1.133		×	Q. Search	☆	Ó	÷	î	◙	≡
Erase Flash (4/512) If this webpage doesn't refresh smoothly	7, please connect to <u>http://192.168.1.133</u> t	o continue.							
Looking up 192.168.1.133									

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

Firmware Update >	< +						_		×
(1) 192.168.1.133			C Q Search		☆ 自	+	Â		≡
		F/W							
	Select the image file: Brow		UPDATE]						
	http://192.168.1.133			53					
G Firmware Update >	< +						_		×
 ↓ Firmware Update ↓ ① 192.168.1.133 	(+		× Q Search		☆ @		Â	•	×
	+		X Q Search		☆ 🖻				
€ € 192.168.1.133	< +		X Q Search		☆□自				
€ € 192.168.1.133	(+		X Q Search		☆│自				
€ € 192.168.1.133	< +		X Q Search		☆ 自				
€ € 192.168.1.133	< +		X Q Search		☆□自				
€ € 192.168.1.133	< +		X Q Search		☆自				
€ € 192.168.1.133	< +		X Q Search	ľ	☆自				
€ € 192.168.1.133	(+		X Q Search		☆ 自				
€ € 192.168.1.133	(+		X Q Search		☆ 自				
€ € 192.168.1.133	< +		X Q Search		☆□自				
€ € 192.168.1.133	< +		X Q Search		☆●自				
€ € 192.168.1.133	< +		X Q Search		☆自				
€ € 192.168.1.133	(+		X Q Search		☆│自				
€ € 192.168.1.133	(+		X Q Search		☆□自				
€ € 192.168.1.133	(+		X Q Search		☆│自				
€ € 192.168.1.133	< +		X Q Search		☆□自				
€ € 192.168.1.133	< +		X Q Search		☆□自				
€ € 192.168.1.133	< +		X Q Search		☆□自				



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



Section 10: PoE

10.0 PoE Status

•	VIGITRO
🖲 Adminis	strator
🥺 PoE	
	PoE Status
	PoE Setting
	PoE Event Counte
	PoE Power Delay
	PoE Auto Check
Port Ma	inagement
Per Por	t Counter
Security	y
Lite/Ful	I
Logout	

J	tinden 1 3 5 7 Stendard 7 B B S Standard Street Barrier Constraint Street Constraint	17 9 21 23 25 Upink 25 CILCITRON 1 1 2 2 24 26 26 26 26 26 26 26 26 26 26 26 26 26
	PoE Status	
	PoE Setting	
	Total System PoE Budget(Watt)	550
	Power Mode	Intelligent Power Limit 🔹
	Auto Recovery(0:not recovery)	10 s (1~255)
	Update	
	PoE Status	
	System operation status	On
	Actual Power Consumption(Watts)	0.0
	Remaining PoE Budget(Watts)	550.0

VIGITRON		Bhennet 8 PoE	E Port	
Administrator	PoE Status			
2 PoE				

dard 1 3 5 7

PoE		
	•	PoE Status
	•	PoE Setting
	•	PoE Event Counter
	•	PoE Power Delay
	•	PoE Auto Check
Port	Mai	nagement
Per	Port	Counter
Secu	irity	
Lite/	Full	
Log	out	

PoE Setting	
Total System PoE Budget(Watt)	550
Power Mode	Intelligent Power Limit •
Auto Recovery(0:not recovery)	Host defined Power Limit Class defined Power Limit
Update	Intelligent Power Limit
PoE Status	
System operation status	On
Actual Power Consumption(Watts)	0.0
Remaining PoE Budget(Watts)	550.0

and 9 II 33 15 Standard 17 19 21 23 25 Upini 25 Third III

Power Mode:

Select Mode by:

Host: Power provided will be determined by connected device.

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

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

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

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

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

10.1 PoE Setting

VIGITRON	Standard Ethernet & PoE		ndard hernet & PoE				Consulta	
dministrator	PoE Set	tina						
ΣE								
PoE Status								
PoE Setting	Function	Status		Mode		Availab	le Power	Port Priority
PoE Event Counter	Gilction		·		'	(MAX	::36 LSB:1 Watt)	Port Priority
PoE Power Delay				01 🗆 02 🛛	03 04 0	5 🗆 06 💷 07 💷 0	8 09 10 11 12)
PoE Auto Check	Port No.			13 🗆 14 🛛	15 🗆 16 🔲 1	7 🗆 18 💷 19 💷 2	0 🗆 21 🗆 22 💷 23 💷 24 🖾)
rt Management						Check All		
Port Counter								
curity					L	Jpdate		
e/Full								
aout					Port Sta	tus Refresh		
gout	Port Status P	ower Mode	Class	Voltage(V)	Current(mA)	Temperature(C)	Power Consumption(W)	Available Power(W)
	1 Enable	OFF 65 Watt		54	/	65.62	0.0	72.0
	2 Enable	OFF 65 Watt		54		65.62	0.0	72.0
	3 Enable	OFF 65 Watt		54		66.18	0.0	72.0
	4 Enable	OFF 65 Watt		54		68.25	0.0	72.0
	5 Enable	OFF AT		54		61.62	0.0	36.0
	6 Enable	OFF AT		54		62.62	0.0	36.0
	7 Enable	OFF AT		54		62.18	0.0	36.0
	8 Enable	OFF AT		54		64.25	0.0	36.0
	9 Enable	OFF AT		54		59.56	0.0	36.0
	10 Enable	OFF AT		54		61.62	0.0	36.0
	11 Enable	OFF AT		54		60.56	0.0	36.0
	12 Enable	OFF AT		54		62.18	0.0	36.0
		OFF AT		54		67.25	0.0	36.0
		OFF AT		54		66.75	0.0	36.0
		OFF AT		54		67.81	0.0	36.0
		OFF AT		54		70.87	0.0	36.0
		OFF 65 Watt		54		65.81	0.0	72.0
		OFF 65 Watt		54		64.81	0.0	72.0
		OFF 65 Watt		54		64.31	0.0	72.0
		OFF 65 Watt		54		67.43	0.0	72.0
		OFF AT		54		66.0	0.0	36.0
		OFF AT		54		66.0	0.0	36.0
		OFF AT		54		68.6	0.0	36.0
	24 Enable	OFF AT		54		69.68	0.0	36.0

- 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.

VIGITRON

Administrator PoE

Standard 9 11 13 15 Ethemet & PoE 18 12 14 16

PoE Setting

us	
ing	
nt Counter	
er Delay	
Check	

	Status	Status Mode Available Power		Port Priority			
Function	v	*	(MAX:36 LSB:1 Watt)	Port Priority			
Port No.	Enable Disable		04 05 06 07 08 09 10 11 12 16 17 18 19 20 21 22 23 24				
	Check All						

Port Managemen Per Port Counter Security 🔰 Lite/Full

PoE Stat
PoE Sett
PoE Eve
PoE Pow
PoE Auto

Logout

						Port Sta	tus Refresh		
Port	Status	Power	Mode	Class	Voltage(V)	Current(mA)	Temperature(C)	Power Consumption(W)	Available Power(W
1	Enable	OFF	65 Watt		54		65.62	0.0	72.0
2	Enable	OFF	65 Watt		54		65.62	0.0	72.0
3	Enable	OFF	65 Watt		54		66.18	0.0	72.0
4	Enable	OFF	65 Watt		54		68.25	0.0	72.0
5	Enable	OFF	AT		54		61.62	0.0	36.0
6	Enable	OFF	AT		54		62.62	0.0	36.0
7	Enable	OFF	AT		54		62.18	0.0	36.0
8	Enable	OFF	AT		54		64.25	0.0	36.0
9	Enable	OFF	AT		54		59.56	0.0	36.0
10	Enable	OFF	AT		54		61.62	0.0	36.0
11	Enable	OFF	AT		54		60.56	0.0	36.0
12	Enable	OFF	AT		54		62.18	0.0	36.0
13	Enable	OFF	AT		54		67.25	0.0	36.0
14	Enable	OFF	AT		54		66.75	0.0	36.0
15	Enable	OFF	AT		54		67.81	0.0	36.0
16	Enable	OFF	AT		54		70.87	0.0	36.0
17	Enable	OFF	65 Watt		54		65.81	0.0	72.0
18	Enable	OFF	65 Watt		54		64.81	0.0	72.0
19	Enable	OFF	65 Watt		54		64.31	0.0	72.0
20	Enable	OFF	65 Watt		54		67.43	0.0	72.0
21	Enable	OFF	AT		54		66.0	0.0	36.0
22	Enable	OFF	AT		54		66.0	0.0	36.0
23	Enable	OFF	AT		54		68.6	0.0	36.0
24	Enable	OFF	AT		54		69.68	0.0	36.0

VIGITRON

PoE Status
PoE Setting
PoE Event Counter
PoE Power Delay
PoE Auto Check

Administrator PoE

Port Management

Per Port Counter Security Lite/Full

Logout

Standard 17 19 21 23 25 Uptin 25 Consele

PoE Setting

Mode Available Power Port Priority Status Function AF 03 04 05 06 07 08 09 10 11 12 AT 15 16 17 18 19 20 21 22 23 24 65 Watt Check All 0 0 0 0 0 0 0 10 11 12 23 24 0 È Port Priority • Port No. Check All 🔲

Update	

						Port Stat	tus Refresh		
Port	Status	Power	Mode	Class	Voltage(V)	Current(mA)	Temperature(C)	Power Consumption(W)	Available Power(W
1	Enable	OFF	65 Watt		54		65.62	0.0	72.0
2	Enable	OFF	65 Watt		54		65.62	0.0	72.0
3	Enable	OFF	65 Watt		54		66.18	0.0	72.0
4	Enable	OFF	65 Watt		54		68.25	0.0	72.0
5	Enable	OFF	AT		54		61.62	0.0	36.0
6	Enable	OFF	AT		54		62.62	0.0	36.0
7	Enable	OFF	AT		54		62.18	0.0	36.0
8	Enable	OFF	AT		54		64.25	0.0	36.0
9	Enable	OFF	AT		54		59.56	0.0	36.0
10	Enable	OFF	AT		54		61.62	0.0	36.0
11	Enable	OFF	AT		54		60.56	0.0	36.0
12	Enable	OFF	AT		54		62.18	0.0	36.0
13	Enable	OFF	AT		54		67.25	0.0	36.0
14	Enable	OFF	AT		54		66.75	0.0	36.0
15	Enable	OFF	AT		54		67.81	0.0	36.0
16	Enable	OFF	AT		54		70.87	0.0	36.0
17	Enable	OFF	65 Watt		54		65.81	0.0	72.0
18	Enable	OFF	65 Watt		54		64.81	0.0	72.0
19	Enable	OFF	65 Watt		54		64.31	0.0	72.0
20	Enable	OFF	65 Watt		54		67.43	0.0	72.0
21	Enable	OFF	AT		54		66.0	0.0	36.0
22	Enable	OFF	AT		54		66.0	0.0	36.0
23	Enable	OFF	AT		54		68.6	0.0	36.0
24	Enable	OFF	AT		54		69.68	0.0	36.0

	Pol	E Set	tina									
Administrator		- 000	ung									
PoE												_
PoE Status	T		St	tatus		Mode		Availat	ole Power	I	Port Priority	
PoE Setting	Func	tion		۲			•	(MA)	(:36 LSB:1 Watt)		Port Priority	1
PoE Event Counter						01 🗆 02	03 04 0	5 06 07 0	8 09 10 11 12	<u> </u>	Priority	Port
PoE Power Delay	Port]	No				13 🗆 14 🛛	15 16 1	7 🗆 18 🗆 19 🗆 2	0 21 22 23 24	i	1	Port 1
 PoE Auto Check 	I OIL .											
Port Management								Check All		_	2	Port 2
Per Port Counter							ι	Jpdate		_	3	Port 3
Security											4	Port 4
Lite/Full							Port Sta	tus Refresh			5	Port 5
Logout	Port	Status P	ower M	lode C	lass	Voltage(V)	Current(mA)	Temperature(C)	Power Consumption(W)	Avai	6	Port 6
	1	Enable	OFF 65	Watt		54		65.62	0.0	_		
	2 1	Enable	OFF 65	Watt		54		65.62	0.0		7	Port 7
	3 1	Enable	OFF 65	Watt		54		66.18	0.0		8	Port 8
	4 1	Enable	OFF 65	Watt		54		68.25	0.0		9	Port 9
						54		61.62	0.0		10	Port 10
						54		62.62	0.0			
						54		62.18	0.0	_	11	Port 11
						54		64.25	0.0	_	12	Port 12
						54		59.56	0.0	_	13	Port 13
						54		61.62	0.0	_	14	Port 14
						54 54		60.56 62.18	0.0	_		
						54		62.18	0.0	_	15	Port 15
						54		67.25	0.0	-	16	Port 16
		Enable		AT		54		67.81	0.0	_	17	Port 17

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

Port Priority Setting:

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



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

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

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

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

What does the priority list do? When the switch detects the power usage is above 550 Watt (400 Watt for Vi35126), 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 reenable 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 24 the least.

10.2 PoE Event Counter

E									
 PoE Status PoE Setting 					PoE Event ID				
 PoE Event Counter PoE Power Delay 	Port	E0	E1	E2	E3	E4	E5	E6	E7
PoE Auto Check	1	0	0	0	0	0	0	0	0
Management	2	0	0	0	0	0	0	0	0
'ort Counter rity	3	0	0	0	0	0	0	0	0
Full	4	0	0	0	0	0	0	0	0
ut	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
	17	0	0	0	0	0	0	0	0
	18	0	0	0	0	0	0	0	0
	19	0	0	0	0	0	0	0	0
	20	0	0	0	0	0	0	0	0
	20	0	0	0	0	0	0	0	0
	22	0	0	0	0	0	0	0	0
	22	0	0	0	0	0	0	0	0
	23	0	0	0	0	0	0	0	0
	Port	E0	El	E2	E3	E4	ES	E6	E
	ron	EU	EI		Clear Refresh	E4	25	E0	E
	E0:Port Overload (ICU E1:Port Short Circuit I E2:Port MPS Error (D E3:Port Severe Short E4:Port Thermal Shut E5:Port Temperature I E6:Main Power Overl	Limit (ILIM) Event C Disconnect) Even Circuit Event Iown Event Limit Event							

PoE Event Counter Definitions

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

10.3 PoE Power Delay

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

	Standard Ethernet	5 7 Stan 1 1 1 1 Eth 8 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		
Administrator	PoE Po	ower Delay		
PoE		-		
PoE Status			Delay Mode	D-1 T(0, 200)
PoE Setting	Function	-	Delay Niode	Delay Time(0~300) second
PoE Event Counter				
 PoE Power Delay PoE Auto Check 	Port No.			05 06 07 08 09 10 11 12 17 18 19 20 21 22 23 24
			13 0 14 0 13 0 10 0	Update
Port Management				opulo
Per Port Counter	Port	Delay Mode	Delay Time (seco	cond)
Security	1	Disable	0	
Lite/Full	2	Disable	0	
Eogout	3	Disable	0	
	4	Disable	0	
	5	Disable	0	
	6	Disable	0	
	7	Disable	0	
	8	Disable	0	
	9	Disable	0	
	10	Disable	0	
	11	Disable	0	
	12	Disable	0	
	13	Disable	0	
	14	Disable	0	
	15	Disable	0	
	16	Disable	0	
	17	Disable	0	
	18	Disable	0	
	19	Disable	0	
	20	Disable	0	
	21	Disable	0	
	22	Disable	0	
	23	Disable	0	
	24	Disable	0	

- 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.

	Standard Ethernet & Pol	5 7 Standi Ethen & P	ard 9 11 13 15 Sta met 1 1 1 15 Sta For 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
Administrator	PoE Po	wer Delay		
✤ PoE				
PoE Status		E	Delay Mode	Delay Time(0~300)
 PoE Setting PoE Event Counter 	Function	[7	second
PoE Power Delay PoE Auto Check	Port No.			05 06 07 08 09 10 11 12 17 18 19 20 21 22 23 24
Port Management			Disable	Update
Per Port Counter				
Security		Delay Mode	Delay Time (seco	cond)
Lite/Full	2	Disable Disable	0	
Logout	3	Disable	0	
-	4	Disable	0	
	5	Disable	0	
	6	Disable	0	
	7	Disable	0	
	8	Disable	0	
	9	Disable	0	
	10	Disable	0	
	11	Disable	i 0	

10.4 PoE Auto Check

		tandard / 11 13 15 Diverset		
ninistrator	PoE Auto-c	heck		
PoE Status	Function		Theck Interval Time Wake Up Ti	
 PoE Setting PoE Event Counter 		5	(min)(1~240 min) 10 (s)(1~	-59 s)
 PoE Power Delay PoE Auto Check 				
Management	Enable Port		Port Select 02 03 04 05 06 07 08 09 10 11 12	
Port Counter	Enable Fort			
urity			Update	
Full out		Port	Check IP Address	
out	Function	1 •	0 . 0 . 0	
			Update	
	Po	rt 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
		5	Disable	0.0.0.0
		6	Disable	0.0.0.0
		7	Disable	0.0.0.0
		8	Disable	0.0.0.0
		9	Disable	0.0.0.0
		10	Disable	0.0.0.0
		11	Disable	0.0.0.0
		12	Disable	0.0.0.0
		13	Disable	0.0.0.0
		14	Disable	0.0.0.0
		15	Disable	0.0.0.0
		15	Disable	0.0.0.0
		17	Disable	0.0.0.0
		18	Disable	0.0.0.0
		19	Disable	0.0.0
		20	Disable	0.0.0.0
		21	Disable	0.0.0.0
		22	Disable	0.0.0.0
		23	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.

		& PuE	ååå ÞÞÞ					
ministrator	PoE Auto-		k is is	14	38 28 22 24 26 26			
οE								
PoE Status	Function			C	heck Interval Time	Wake Up Time		
 PoE Setting PoE Event Counter 	Function			5	(min)(1~240 min)	10 (s)(1~59	š)	
PoE Power Delay					Update			
 PoE Auto Check rt Management 					Port Select			
Port Counter	Enable Port				02 03 04 05 06 07 08			
urity				13	14 15 16 17 18 19 20 Update	0 21 22 23 24 2		
Full								
gout	Function		Port			IP Address		
			1 -		0 0	. 0 . 0		
			2		Update			
	1	Port No.	4		Enable Stat	tus	IP Address	
		1	5 6		Disable		0.0.0.0	
		2	7		Disable		0.0.0.0	
		3	8		Disable		0.0.0.0	
		4	10 11		Disable		0.0.0.0	
		5	12		Disable		0.0.0.0	
			13 14					
		6	15		Disable		0.0.0.0	
		7	16 17		Disable		0.0.0.0	
		8	18 19		Disable		0.0.0.0	
		9	20 -		Disable		0.0.0.0	
		10			Disable		0.0.0.0	
		11			Disable		0.0.0.0	
		12			Disable		0.0.0.0	
		13			Disable		0.0.0.0	
		14			Disable		0.0.0.0	
		15			Disable		0.0.0.0	
		16			Disable		0.0.0.0	
		17			Disable		0.0.0.0	
		18			Disable		0.0.0.0	
		19			Disable		0.0.0.0	
		20			Disable		0.0.0.0	
		21			Disable		0.0.0.0	
		22			Disable		0.0.0.0	
		23			Disable		0.0.0.0	
		24			Disable		0.0.0.0	

Section 11: Port Management

11.0 Port Configuration

	Port	Conf	igurat	ion									
nfiguration			Tx/Rx A	bility	SecurPort	Auto-Negotiat	ion Spe	eed Dupl	ex	Pause	Backp	ressure .	Addr. Learning
nnguration	Functio	on		•	···· T	T				T		•	T
	Select Port N	D.					0 17 0 18 0 19 C	07 08 09 20 21 22 heck All					
							Updat	e					
			Cu	rrent Status					Setting St	atus			
	Port	Link	Speed	Duplex	FlowCtrl	Tx/Rx Ability	SecurPort	Auto-Nego	Speed	Duplex	Pause	Backpressure	e Addr. Learning
	1					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	2					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	3					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	4					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	5					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	6					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	7					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	8					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	9					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	10					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	11					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	12					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	13					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	14					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	15					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	16					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	17					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	18					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	19					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	20					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	21					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	22					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	23					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	24					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	25	•	1G	FULL	ON	ON	OFF	AUTO	1G	FULL	ON	ON	ON
	26					ON	OFF	AUTO	1G	FULL	ON	ON	OFF

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

NOTE:



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

ninistrator	Port	Conf	igurat										
t Management			-										
 Port Configuration 	Functi	m	Tx/Rx A	bility	SecurPort	Auto-Negotiat	ion Sp	eed Dupl	ex	Pause	Backp	ressure	Addr. Learning
Port Counter				•	¥	*		▼		•		Y	···· •
urity /Full	Select		Enable Disable					07 08 09 20 21 22					
iruli jout	Port N	D.	DISADR	•					0250240				
								heck All					
							Updat	8					
			Cu	rrent Status					Setting St	atus			
	Port	Link	Speed	Duplex	FlowCtrl	Tx/Rx Ability	SecurPort	Auto-Nego	Speed	Duplex	Pause	Backpressur	e Addr. Learnin
	1					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	2					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	3					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	4					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	5					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	6					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	7					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	8					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	9					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	10					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	11					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	12					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	13					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	14					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	15					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	16					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	17					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	18					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	19					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	20					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	21					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	22					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	23					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	24					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	25	•	1G	FULL	ON	ON	OFF	AUTO	1G	FULL	ON	ON	ON
	26					ON	OFF	AUTO	1G	FULL	ON	ON	OFF

Tx/Rx:

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

					Standard Efferted A Foll								
Administrator PoE Port Management	Port	Conf	igurati	ion									
Port Management Port Configuration Per Port Counter Security Lite/Full	Function		Tx/Rx A	bility ▼	SecurPort			eed Duple 07 08 09 20 21 22	• 10 - 11 -	12 - 13 -	Backp		dr. Learning 🔻
Logout	Port No	0.					Updar	Check All □ te					
			Cu	rrent Status					Setting St	atus			
	Port	Link	Speed	Duplex	FlowCtrl	Tx/Rx Ability	SecurPort	Auto-Nego	Speed	Duplex	Pause	Backpressure	Addr. Learnin
	1					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	2					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	3					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	4					ON	OFF	AUTO	100M	FULL	ON	ON	OFF

- 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.

Po	t Cor	figurat	ion									
		Tx/Rx A	Ability	SecurPort	Auto-Negotiat	ion Sp	eed Dupl	ex	Pause	Backp	ressure .	Addr. Learning
Fund	tion		•	···· ¥	···· •		-		- v		¥	v
Sele Port					01 Enable 14 Disable	0 17 0 18 0 19	07 08 09 20 21 22 heck All					
						Updat	e					
		Cu	urrent Status					Setting St	atus			
Port	Link	Speed	Duplex	FlowCtrl	Tx/Rx Ability	SecurPort	Auto-Nego	Speed	Duplex	Pause	Backpressure	e Addr. Learning
1					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
2					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
3					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
4					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
5					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
6					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
7					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
8					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
9					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
10					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
11					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
12					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
13					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
14					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
15					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
16					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
17					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
18					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
19					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
20					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
21					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
22					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
23					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
24					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
25	•	1G	FULL	ON	ON	OFF	AUTO	1G	FULL	ON	ON	ON
26					ON	OFF	AUTO	1G	FULL	ON	ON	OFF

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.

Po	rt C	onfi	gurati	ion									
			Tx/Rx A	bility	SecurPort	Auto-Negotiat	ion Sp	ed Dupl	ex	Pause	Backp	ressure A	ddr. Learning
Fun	iction			•	•	···· •		▼		T		T	···· •
Sele	ect t No.					01 = 02 = 03 14 = 15 = 16	17 18 1001 10M	a 🗆 21 🗆 22		12 13 25 26			
							Updat	e					
			Cu	rrent Status					Setting St	atus			
Por	t I	Link	Speed	Duplex	FlowCtrl	Tx/Rx Ability	SecurPort	Auto-Nego	Speed	Duplex	Pause	Backpressure	Addr. Learning
1						ON	OFF	AUTO	100M	FULL	ON	ON	OFF
2						ON	OFF	AUTO	100M	FULL	ON	ON	OFF
3						ON	OFF	AUTO	100M	FULL	ON	ON	OFF
4						ON	OFF	AUTO	100M	FULL	ON	ON	OFF
5						ON	OFF	AUTO	100M	FULL	ON	ON	OFF
6	5					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
7						ON	OFF	AUTO	100M	FULL	ON	ON	OFF
8						ON	OFF	AUTO	100M	FULL	ON	ON	OFF
9	•					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
1	0					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
1	1					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
1	2					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
1	3					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
1	4					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
1	5					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
10	6					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
1	7					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
1	8					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
19	9					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
2	0					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
2	1					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
2	2					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
2	3					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
2	4					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
2	5	•	1G	FULL	ON	ON	OFF	AUTO	1G	FULL	ON	ON	ON
2	6					ON	OFF	AUTO	1G	FULL	ON	ON	OFF

Speed:

- Select 10Mbps or 100Mbps for ports 1-24
- Select 10Mbps/100Mbps or 1000Mbps (1Gbps) for ports 25/26

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

Por	t Con	figura	tio			ОК С	ancel					
		Tx/Rx	Ability	SecurPort	Auto-Negotia	tion Sp	eed I	Duplex	Pause	Backpr	essure Add	. Learning
Func	tion		•	*	*	1G	•		•		•	- •
Selec					01 02 03 4 14 15 16	17 🗐 18 🗐 19		22 23 23				
						Updat						
		Cu	rrent Status					Setting	Status			
Port	Link	Speed	Duplex	FlowCtrl	Tx/Rx Ability	SecurPort	Auto-Ne	go Speed	Duplex	Pause	Backpressure	Addr. Learnin
1					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
2			***		ON	OFF	AUTO	100M	FULL	ON	ON	OFF
3		***	***		ON	OFF	AUTO	100M	FULL	ON	ON	OFF
4				***	ON	OFF	AUTO	100M	FULL	ON	ON	OFF
5					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
6					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
7					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
8					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
9					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
10	10000		1222		ON	OFF	AUTO	100M	FULL	ON	ON	OFF
11	1			1000	ON	OFF	AUTO	100M	FULL	ON	ON	OFF
12					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
13			***		ON	OFF	AUTO	100M	FULL	ON	ON	OFF

istrator	Port	Conf	igurat	ion									
Port Configuration			Tx/Rx A	bility.	SecurPort	Auto-Negotiat	ion Sp	eed Dupl	ex	Pause	Backp	ressure .	Addr. Learning
rt Counter	Function	on		•	¥	•		· ·	•	- v		•	V
ty ili t	Select Port N	o.				01 02 03 14 15 16		07 08 Full 20 21 Half		12 13 25 26			
							Updat						
			0	rrent Status					Setting St				
	Port	Link	Speed	Duplex	FlowCtrl	Tx/Rx Ability	SecurPort	Auto-Nego	Speed	Duplex	Pause	Backpressure	Addr. Learnin
	1					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	2					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	3					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	4					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	5					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	6					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	7					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	8					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	9					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	10					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	11					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	12					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	13					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	14					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	15					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	16					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	17					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	18					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	19					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	20					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	21					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	22					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	23					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	24					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	25	•	1G	FULL	ON	ON	OFF	AUTO	1G	FULL	ON	ON	ON
	26					ON	OFF	AUTO	1G	FULL	ON	ON	OFF

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

	2441	_	10 12			2 34 38 28							
Administrator	Port	Conf	igurati	ion									
PoE													
 Port Management Port Configuration 			Tx/Rx A	bility	SecurPort	Auto-Negotiat	ion Sp	ed Dupl	ex	Pause	Backp	ressure A	Addr. Learning
Per Port Counter	Function	on		¥	···· V	···· •		▼	•	T		T	T
Security						01 = 02 = 03	04 05 06	07 08 09	= 10 = 11 E	nable			
Lite/Full	Select Port N					14 🗆 15 🔲 16	0 17 0 18 0 19	20 21 22	■ 23	lisable 🛛			
Logout							С	heck All 💷					
							Updat	e					
			Cu	rrent Status					Setting St	atus			
	Port	Link	Speed	Duplex	FlowCtrl	Tx/Rx Ability	SecurPort	Auto-Nego	Speed	Duplex	Pause	Backpressure	Addr. Learnin
	1					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	2					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	3					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	4					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	5					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	6					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	7					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	8					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	9					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	10					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	11					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	12					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	13					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	14					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	15					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	16					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	17					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	18					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	19					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	20					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	21					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	22					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	23					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	24					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	25	•	1G	FULL	ON	ON	OFF	AUTO	1 G	FULL	ON	ON	ON
	26					ON	OFF	AUTO	1 G	FULL	ON	ON	OFF

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.

				14 16	11 21								
Administrator	Port	Conf	igurati	ion									
PoE Port Management													
Port Management Port Configuration	Functio		Tx/Rx A	bility	SecurPort	Auto-Negotiat	ion Sp	ed Dupl	ex	Pause	Backp	ressure /	ddr. Learning
Per Port Counter	Functi	on		•	¥	¥		T	•	- •		•	···· V
Security	Select							07 08 09			Enab		
Lite/Full Logout	Port N	o.				14 1 15 1 10			25 11 24 1	23 1 20 1	Disat	ble	
Logout								heck All					
							Updat	e					
	Port		Cu	rrent Status					Setting St	atus			
	Port	Link	Speed	Duplex	FlowCtrl	Tx/Rx Ability	SecurPort	Auto-Nego	Speed	Duplex	Pause	Backpressure	Addr. Learnir
	1					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	2					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	3					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	4					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	5					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	6					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	7					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	8					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	9					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	10					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	11					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	12					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	13					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	14					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	15					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	16					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	17					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	18					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	19					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	20					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	21					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	22					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	23					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	24					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	25	•	1G	FULL	ON	ON	OFF	AUTO	1G	FULL	ON	ON	ON
	26					ON	OFF	AUTO	1G	FULL	ON	ON	OFF

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.

					11 20	22 24 26 26							
Administrator	Port	Conf	igurat	ion									
PoE													
Port Management Port Configuration			Tx/Rx A	bility	SecurPort	Auto-Negotiat	ion Sp	ed Dupl	ex	Pause	Backp	ressure .	Addr. Learning
Per Port Counter	Function	on		• •	V	T		▼	v -	V		•	T
Security								07 08 09					Enable
Lite/Full	Select Port N	o.				14 = 15 = 16	0 17 0 18 0 19	20 21 22	23	25 26			Disable
Logout							C	heck All 💷					
							Updat	e					
	Port		Cu	rrent Status					Setting St	atus			
	Port	Link	Speed	Duplex	FlowCtrl	Tx/Rx Ability	SecurPort	Auto-Nego	Speed	Duplex	Pause	Backpressure	e Addr. Learnii
	1					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	2					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	3					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	4					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	5					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	6					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	7					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	8					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	9					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	10					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	11					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	12					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	13					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	14					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	15					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	16					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	17					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	18					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	19					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	20					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	21					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	22					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	23					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	24					ON	OFF	AUTO	100M	FULL	ON	ON	OFF
	25	•	1G	FULL	ON	ON	OFF	AUTO	1 G	FULL	ON	ON	ON
	26					ON	OFF	AUTO	1 G	FULL	ON	ON	OFF

Address Learning

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

Update: Select update to apply your programmed changes

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

11.1 Port Mirroring

	Standard Ebicrott & Poč	Standa Etherr & Pr			Standa Etherr & P			²⁵ Uplink ²⁵]				
 Administrator PoE 	Port Mirrorin	g												
 Port Management Port Configuration Port Mirroring 	Dest	01	02	03	04	05	06	07	08	09	10	11	12	13
 Bandwidth Control Broadcast Storm 	Port	14	15	16	17	18	19	20	21	22	23	24	25	26
Control VLAN Setting	Monitored Packets	Disabl	le 🔻											
 Per Port Counter QoS Setting 	Source	01	02	03	04	05	06	07	08	09	10	11	12	13
 Security Spanning Tree 	Port	14	15	16	17	18	19	20	21	22	23	24	25	26
Trunking DHCP Relay Agent	Multi to Multi Sniffe					. (Update							
Backup/Recovery Miscellaneous	Multi to Multi Sniffe	r function												
SNMP Settings														
 Lite version Eviluation 														
 Full version Logout 														

SmartSwitch Web-Base 🗧 🗙												Θ	-		×
← → C ③ Not secure 192.	168.1.133												7.5	۵	:
	Standard 1 3 5 7 Ethicinet & Poct	Stand: Ether & P	net PoE		51	& PoE	7 19 21		ink 25 Conso Conso 26	IGITRON					
Administrator	Port Mirrorin	g													
Port Management															
 Port Configuration Port Mirroring 	Dest	01	02	03	04	05	06	07	08	09	10	11	12	13	
 Bandwidth Control Broadcast Storm Control 	Port	14	15	16	17	18	19	20	21	22	23	24	25	26	
VLAN Setting	Monitored Packets	Disable Disable													
 Per Port Counter QoS Setting 	Source	Rx Tx Tx & R	x	03	04	05	06	07	08	09	10	11	12	13	
 Security Spanning Tree 	Port	14	15	16	17	18	19	20	21	22	23	24	25	26	
 DHCP Relay Agent Backup/Recovery 	2641-26410-00						Update								
Miscellaneous	Multi to Multi Sniffer	functio	n												
SMMP Settings Lite/Full Cite version Cite version Copout															

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

Select the mirror type:

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

11.2 Bandwidth Control

	4 6 8 10 10 14 16			
Inletrator	Bandwidth Cont	rol		
Management	-			
Port Configuration	Port No	Tx Rate	Pv	Rate
 Port Mirroring Bandwidth Control 	1 7	(0~255) (0:Full Speed)	(0~255)	(0:Full Speed)
 Broadcast Storm Control 		(0-233) (0-1 dii Speed)	(0-233)	(u.i uii Speed)
N Setting		Low:		
Port Counter		(1)32Kbps Tx/Rx bandwidth resolution for port 1~ port 26. Actual Tx/Rx bandwidth =Rate value x 32 kbps. The rate value is 1~255		
Setting		High:		
urity	Speed Base	(1)256Kbps Tx/Rx bandwidth resolution for port 1~ port 24. Actual Tx/Rx bandwidth=Rate value x 256Kbps. The rate value is 1~255	5	
inning Tree		When link speed is 10MB. The rate value is 1~39. (2)the bandwidth resolution is 2048Kbps for port 25, port 26.		
nking CP Relay Agent		Actual Tx/Rx bandwidth=Rate value x 2048Kbps. The rate value is 1~25	55.	
kup/Recoverv		When link speed is 10MB. The rate value is 1~4. When link speed is 100MB. The rate value is 1~48.		
cellaneous		Update LoadE	hafm. (t	
MP Settings	If the link append of a link	d port is lower than the rate that you seting, this system will use the value of lin		
(Full	in the link speed of selection	su porcis iower unan me rate unacyou setting, this system will use the value of in	is speed as your setting rate.	
 O Lite version 				
 Full version 	Port	Tx Rate	Rx Rate	Link
out	No.			Speed
	1	Full Speed	Full Spee	d
	2	Full Speed	Full Spee	d
	3	Full Speed	Full Spee	d
	4	Full Speed	Full Spee	d
	5	Full Speed	Full Spee	d
	6	Full Speed	Full Spee	d
	7	Full Speed	Full Spee	d
	8	Full Speed	Full Spee	d
	9	Full Speed	Full Spee	d
	10	Full Speed	Full Spee	d
	11	Full Speed	Full Spee	d
	12	Full Speed	Full Spee	d
	13	Full Speed	Full Spee	d
	14	Full Speed	Full Spee	d
	15	Full Speed	Full Spee	d
	16	Full Speed	Full Spee	d
	17	Full Speed	Full Spee	d
	18	Full Speed	Full Spee	d
	19	Full Speed	Full Spee	d
	20	Full Speed	Full Spee	d
	21	Full Speed	Full Spee	d
	22	Full Speed	Full Spee	d
	23	Full Speed	Full Spee	d
	24	Full Speed	Full Spee	d
	25	Full Speed	Full Spee	d 1G

VIGITRON				
inietrator	Bandwidth Contr	ol		
itanagement				
 Port Configuration Port Mirroring 	Port No	Tx Rate	Rx Rate	
Bandwidth Control	1 1	(0~255) (0:Full Speed)	(0~255) (0:Full	Speed)
 Broadcast Storm Centrol 	2344	Low T		
N Setting	3	Low:		
Port Counter	4	(1)32Kbps Tx/Rx bandwidth resolution for port 1~ port 26. Actual Tx/Rx bandwidth =Rate value x 32 kbps. The rate value is 1~255		
Setting	5	High: (1)256Kbps Tx/Rx bandwidth resolution for port 1~ port 24.		
urity Inning Tree	Sp 7 se	Actual Tx/Rx bandwidth=Rate value x 256Kbps. The rate value is 1~255		
nning tree Iking	9	When link speed is 10MB. The rate value is 1~39. (2)the bandwidth resolution is 2048Kbps for port 25, port 26.		
CP Relay Agent	11	Actual Tx/Rx bandwidth=Rate value x 2048Kbps. The rate value is 1~25	5.	
ckup/Recovery	12	When link speed is 10MB. The rate value is 1~4. When link speed is 100MB. The rate value is 1~48.		
acellaneous	14	Update LoadD	efault	
IMP Settings	Kilka Kalka 10 Kaalaataa	port is lower than the rate that you seting, this system will use the value of lin		
eFull	17 18	por a construction of the face that you accurg, and system will use the value of in	n opere us year acturing tate.	
 O Lite version 	19			
 Full version gout 	20 -	Tx Rate	Rx Rate	Link
lout	No.			Speed
	1	Full Speed	Full Speed	
	2	Full Speed	Full Speed	
	3	Full Speed	Full Speed	
	4	Full Speed	Full Speed	
	5	Full Speed	Full Speed	
	6	Full Speed	Full Speed	
	7	Full Speed	Full Speed	
	8	Full Speed	Full Speed	
	9	Full Speed	Full Speed	
	10	Full Speed	Full Speed	-
	11	Full Speed	Full Speed	
	12	Full Speed	Full Speed	
	13	Full Speed	Full Speed	
	14	Full Speed	Full Speed	
	15	Full Speed	Full Speed	
	16	Full Speed	Full Speed	
	17	Full Speed	Full Speed	
	18	Full Speed	Full Speed	
	19	Full Speed	Full Speed	
	20	Full Speed	Full Speed	
	21	Full Speed	Full Speed	-
	22	Full Speed	Full Speed	
	23	Full Speed	Full Speed	
	24	Full Speed	Full Speed	
	25	Full Speed	Full Speed	1G
	26	Full Speed	Full Speed	

🖞 SmartSwitch Web-Base 🗆 🗙				Θ – □
> C 🛈 Not secure	192.168.1.133			୧ 🕈 🛧 🐵
ministrator	Bandwidth Contr	rol		
E	· · · · · · · · · · · · · · · · · · ·			
rt Management Port Configuration				
Port Mirroring	Port No	Tx Rate	Rx Rate	
 Bandwidth Control Broadcast Storm 	1 🔻	(0~255) (0:Full Speed)	(0~255) (0:F	full Speed)
Control AN Setting Port Counter 5 setting curity anning Tree CP Reay Agent ckup/Recovery colaraoous	Speed Base	The second secon	255.	
IP Settings		Update LoadDe	Paul I	
NFUI	If the link speed of selects	d port is lower than the rate that you seting, this system will use the value		
 O Lite version 	If the link speed of selecte	a port is tower than the rate that you seeing, this system will use the value	or mix apoon as your actuing rule.	
 Full version 				
	Port No.	Tx Rate	Rx Rate	Link Speed
	1	Full Speed	Full Speed	
	2	Full Speed	Full Speed	
	3	Full Speed	Full Speed	
	4	Full Speed	Full Speed	
	5	Full Speed	Full Speed	
	6	Full Speed	Full Speed	
	7	Full Speed	Full Speed	
	8			
		Full Speed	Full Speed	
	9	Full Speed	Full Speed	
	10	Full Speed Full Speed	Full Speed Full Speed	
	10 11	Full Speed Full Speed Full Speed	Full Speed Full Speed Full Speed	
	10 11 12	Full Speed Full Speed Full Speed Full Speed	Full Speed Full Speed Full Speed Full Speed	
	10 11 12 13	Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed	Full Speed Full Speed Full Speed Full Speed Full Speed	
	10 11 12 13 14	Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed	Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed	
	10 11 12 13 14 15	Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed	Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed	
	10 11 12 13 14 15 16	Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed	Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed	
	10 11 12 13 14 16 16 17	Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed Ful Speed	Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed	••• ••• ••• ••• ••• •••
	10 11 12 13 14 15 16 17 18	Ful Speed Ful Speed	Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed	
	10 11 12 13 14 15 16 17 18 18 19	Ful Speed	Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed Full Speed	
	10 11 12 13 14 15 16 17 18 19 20	Full Speed	Full Speed Full Speed	
	10 11 12 13 14 15 16 17 18 19 20 21	Full Speed	Full Speed Full Speed	
	10 11 12 13 14 15 16 17 18 19 20 21 22	Ful Speed	Full Speed Full Speed	
	10 11 12 13 14 15 16 17 16 17 18 19 20 21 22 22 23	Full Speed	Full Speed Full Speed	
	10 11 12 13 14 15 16 17 18 19 20 21 22 23 24	Ful Speed	Full Speed Full Speed	
	10 11 12 13 14 15 16 17 16 17 18 19 20 21 22 22 23	Full Speed	Full Speed Full Speed	

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

The Limitation Of The Bandwidth Control

i

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

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

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

	In the "Low" mode, the Tx/Rx bandwidth resolution is 32Kbps for port 1~ port 26. In the "High" mode, the Tx/Rx bandwidth resolution is 256Kbps for port 1 ~ port 24, and 2048Kbps for port 25, port 26.
Low Bandwidth for TX	
	Example 1: The TX number of the port1~4 is set to 10, 20, 30, 40 respectively, and Speed base is set to "Low". The real bandwidth comes from the formula of 32Kbps*10, 32Kbps*20, 32Kbps*30 and 32Kbps*40 respectively. After the "Update" button is executed, the real bandwidth will show up in TX fields.
High bandwidth for TX	
Low Bandwidth	Example 2: The TX number of the port1~4 is set to 10, 20, 30, 40 respectively, and Speed base is set to "High". The real bandwidth comes from the formula of 256Kbps*10, 256Kbps*20, 256Kbps*30 and 256Kbps*40 respectively. After the "Update" button is executed, the real bandwidth will show up in TX fields.
for RX	Example 2: The DV handwidth number of the part 5 part 9 is not to 50
	Example 3: The RX bandwidth number of the port 5~ port 8 is set to 50, 60, 70, 80 respectively, and Speed base is set to "Low". The real bandwidth comes from the formula of 32Kbps*50, 32Kbps*60, 32Kbps*70 and 32Kbps*80 respectively. After the "Update" button is executed, the real bandwidth will show up in RX fields.
High Bandwidth for RX	
	Example 4: The RX bandwidth number of the port 5~ port 8 is set to 50, 60, 70, 80 respectively, and Speed base is set to "High". The real bandwidth comes from the formula of 256Kbps*50, 256Kbps*60, 256Kbps*70 and 256Kbps*80 respectively. After the "Update" button is executed, the real bandwidth will show up in RX fields.

11.3 Broadcast Storm Control

i.

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.

	2 4 6 2													
Administrator	Broadcast S	Storm	Cont	rol										
PoE								63	-					
Port Management	Threshold							1~63	5					
 Port Configuration Port Mirroring 		01	02	03	04	05	06	07	08	09	10	11	12	13
Bandwidth Control	Enable													
 Broadcast Storm Control 	Port	14	15	16	17	18	19	20	21	22	23	24	25	26
VLAN Setting														
Per Port Counter							Update							
QoS Setting	This value indicate	es the nu	mber of b	proadcas	t packet	which is	allowed	to enter	each po	ort in one	e time ur	nit. One ti	ime unit i	s 50us
Security	Gigabit speed, 50	0 us for 1	00Mbps	speed ar	nd 5000i	us for 10	Mbps sp	eed						
security														
	Note: This effect	may be n					icket, sin	ce the b	roadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree	Note: This effect r a time unit is prob	may be n					icket, sin	ce the b	oadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree Trunking DHCP Relay Agent		may be n					icket, sin	ce the b	oadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree Trunking DHCP Relay Agent Backup/Recovery		may be n					icket, sin	ce the b	oadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree Trunking DHCP Relay Agent Backup/Recovery Miscellaneous		may be n					icket, sin	ce the b	oadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree Trunking DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings		may be n					icket, sini	ce the b	roadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree Trunking DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings Lite/Full		may be n					icket, sin	ce the b	roadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree Trunking DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings Lite/Full © Lite version		may be n					icket, sin	ce the b	roadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree Trunking DHCP Relay Agent Backup/Recovery Miscellaneous SMMP Settings Lite/Full		may be n					icket, sin	ce the b	roadcas	t packet	count pa	assing th	rough the	ə switch
Spanning Tree Trunking DHCP Relay Agent Backup/Recovery Miscellaneous SMMP Settings Litle:Full		may be n					icket, sini	ce the b	roadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree Trunking DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings Lite/Full Lite/Full		may be n					icket, sini	ce the b	roadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree Trunking DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings Lite/Full Lite/Full		may be n					icket, sin	ce the bi	roadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree frunking UHCP Relay Agent Jackup Recovery Ulscellaneous SUMP Settings LiterFull Ule Version Full version		may be n					icket, sin	ce the b	roadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree frunking UHCP Relay Agent Jackup Recovery Ulscellaneous SUMP Settings LiterFull Ule Version Full version		may be n					icket, sini	ce the b	roadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree Trunking DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings Lite/Full Lite/Full		may be n					icket, sini	ce the b	roadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree Trunking DHCP Relay Agent Backup/Recovery Miscellaneous SMMP Settings Lite/Full		may be n					icket, sini	ce the b	roadcas	t packet	count pa	assing th	rough the	e switch
Spanning Tree Trunking DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings Lite/Full © Lite version		may be n					icket, sini	ce the b	roadcas	t packet	count pa	assing th	rough the	e switch

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 Vi30126 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".

	Standard 1 3 5 7 Ethernet & PoE 2 4 6 1	Standard Ethemet & PoE		-		uplink ²² CVIGTRO	N	
Administrator	VLAN Mod	e						
PoE								
Port Management	VLAN Mode			Port Base	ed VLAN Change	VLAN mode		
VLAN Setting								
VLAN mode								
VLAN Member								
 Multi to 1 Setting Non-Association Port Setting 								
Per Port Counter								
QoS Setting								
Security								
Spanning Tree								
Trunking								
DHCP Relay Agent								
Backup/Recovery								
Miscellaneous								
SNMP Settings								
2 Lite/Full								
Lite version								
Full version								
> Logout								
	Standard 1 3 5 7 Ethemat 8 POE 2 4 6 1			andard 17 19 21 themet 10 10 10 10 10 10 10 10 10 10 10 10 10	💼 💼 💼 _{Con}	VIGITRON		
 Administrator PoE 	VLAN Mode							
Port Management	VLAN Mode			Tag Based VLAN	Change VLAN mode	e		1
VLAN Setting	VLAN Tag Mode			Tag/Untag t	base on Port 🔻			
VLAN mode		Port 01	Port 02	Port 03	Port 04	Port 05	Port 06	
 VLAN Member Multi to 1 Setting 		 Add Tag Don't Care 	 Add Tag Don't Care 	 Add Tag Don't Care 	 Add Tag Don't Care 	 Add Tag Don't Care 	 Add Tag Don't Care 	
 Non-Association Port Setting 		Remove Tag	Remove Tag	Remove Tag	Remove Tag	Remove Tag	Remove Tag	
Per Port Counter		Port 07 Add Tag	Port 08 Add Tag	Port 09 Add Tag	Port 10 Add Tag	Port 11 Add Tag	Port 12 Add Tag	
V QoS Setting		Don't Care	Don't Care	Don't Care	Don't Care	Don't Care	Don't Care	
Security	AddTag Type	Remove Tag Port 13	Remove Tag Port 14	Remove Tag Port 15	Remove Tag Port 16	Remove Tag Port 17	Remove Tag Port 18	
Spanning Tree	(Add VLAN Tag to output frames	O Add Tag	Add Tag	Add Tag	Add Tag	Add Tag	O Add Tag	
> Trunking	according to the pvid of	Don't Care Remove Tag	Don't Care Remove Tag	Don't Care Remove Tag	Don't Care Remove Tag	Don't Care Remove Tag	Don't Care Remove Tag	
DHCP Relay Agent	selected port)	Port 19	Port 20	Port 21	Port 22	Port 23	Port 24	
Backup/Recovery Miscellaneous		 Add Tag Don't Care 	 Add Tag Don't Care 	 Add Tag Don't Care 	 Add Tag Don't Care 	 Add Tag Don't Care 	 Add Tag Don't Care 	
SNMP Settings		Remove Tag	Remove Tag	Remove Tag	Remove Tag	Remove Tag	Remove Tag	
V Lite/Full		Port 25 Add Tag	Port 26 Add Tag					
		Don't Care	Don't Care					
O Lite version								1
 Lite version Full version 		Remove Tag	Remove Tag	Undate				
			Remove Tag	Update				
• Full version	Note: If the link partner is a networ	Remove Tag	obably cannot reco	gnize the VLAN tag.	In this case, it is stro	ongly recommended	the	
• Full version		Remove Tag	obably cannot reco	gnize the VLAN tag.	In this case, it is stro	ongly recommended	the	
• Full version	If the link partner is a networ	Remove Tag	obably cannot reco	gnize the VLAN tag.	In this case, it is stro	ongly recommended	the	

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

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

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

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

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

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

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

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



Example:

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

Other ports: keep every outgoing packet intact.

12.1 VLAN Member (Port Based)

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

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

	Standard 1 3 5 7 Ethernet 8 PoE	Ethernet & PoE		Standard Ethernet & PoE					
VIGHTKON									
dministrator	VLAN Member	Setting	ı (Port	Based)					
PoE		•	• •	,					
ort Management	Name	(may 9 ch	aracters) Add	Rename					
AN Setting		adDefault	aracters) Aud	Ivename					
VLAN mode	Delete Opdate Lo Destination PORT	01	02	03	04	05	06	07	08
VLAN Member	Select	01		03		05			08
Multi to 1 Setting	Destination PORT	09	10	11		13	14	15	16
Non-Association Port	Select	09	10		12	13	14	15	10
Setting	Destination PORT	17	18	19	20	21	22	23	24
Port Counter	Select		18	19	20	21	- 22		24
S Setting	Destination PORT	25	26						
urity	Select	25	20					<u> </u>	· ·
ining Tree	Select						-		
king									
ICP Relay Agent				VLAN M					1
kup/Recovery	Port Num 01	02 03 04 0	5 06 07 08	09 10 11	12 13 14	15 16 17	18 19 20	21 22 23	24 25 26
allaneous									
P Settings									
-									
e/Full									
Lite version									
• Full version									
gout									
your									

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

VIGITRON	
Administrator	WARNING!
PoE Pot Management VLAN Setting VLAN mode VLAN mode VLAN Member Mutit to 1 Setting Non-Association Port Setting	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. Continue Back
Per Port Counter	
QoS Setting	
Security	
Spanning Tree	
Trunking	
DHCP Relay Agent	
Backup/Recovery	
Miscellaneous	
SNMP Settings	
🥺 Lite/Full	
 Lite version Full version Logout 	

12.2 VLAN Member Settings (Tag Based)

Administrator	VLAN Member	Settin	ng (Ta	g Based	I)				
PoE									
Port Management	1 VID(1~4094):1			haracters): CPU	-	Add Delete	Update		
VLAN Setting	Add: Enter a VID, select the V Del: Select a VID in the table a Update:Modify the existing VII	and then pres	s this buttor	n to remove a VI	D entry from th	add a VLAN en ne table.	ry to the table.		
 VLAN mode VLAN Member 	Port number	1	2	3	4	5	6	7	8
 Multi to 1 Setting 	member select								
 Non-Association Port 	VLAN Setting								
Setting	Port number	9	10	11	12	13	14	15	16
Per Port Counter	member select								
QoS Setting	VLAN Setting								
Security	Port number	17	18	19	20	21	22	23	24
Spanning Tree	member select				1	Image: A start and a start			
Trunking	VLAN Setting								
DHCP Relay Agent	Port number	25	26	- 1	- 1	-	- 1	- 1	1 -
Backup/Recovery	member select	1		-	-	-	•	-	-
Miscellaneous	VLAN Setting			-				-	
SNMP Settings	t <u>e</u>								
🥺 Lite/Full				Por	t VID Map				
Lite version	Port	1	2	3	4	5	6	7	8
• Full version		1	1	1	1	1	1	1	1
Elogout		9	10	11	12	13	14	15	16
r Logoul		1	1	1	1	1	1 22	1	1
		1	18	19	20	21	1	23	24
		25	26			· ·	-		
		1	1	-	-	-	-	-	-
				I					
				VLA	N MEMBER				
	Name(VID) 01	02 03 04	05 06 0	7 08 09 10	11 12 13	14 15 16	17 18 19 2	0 21 22 23	24 25 26
	CPU_CTRL(1) V	v v v	v v v	v v v	v v v	V V V V	v v v	v v v	V V V

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



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

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

Iministrator VLAN Mode	e					
DE						
rt Management			Tag Based VI AN	Change VLAN mod	1	
N Setting VLAN Tag Mode				ase on Port V	<u>.</u>	
VI AN mode	Port 01	Port 02	Port 0 Tag/Untag t	base on VID	Port 05	Port 06
VLAN Member	Add Tag	Add Tag	AGO Tag/Untag t	base on Port	Add Tag	Add Tag
Multi to 1 Setting	Don't Care	Don't Care	Don't Care	Don't Care	Don't Care	Don't Care
Non-Association Port	Remove Tag	Remove Tag	Remove Tag	Remove Tag	Remove Tag	Remove Tag
Setting	Port 07	Port 08	Port 09	Port 10	Port 11	Port 12
r Port Counter	Add Tag	Add Tag	Add Tag	Add Tag	Add Tag	Add Tag
C. Cattler	Don't Care	Don't Care	Don't Care	Don't Care	Don't Care	Don't Care
S Setting AddTag Type	Remove Tag	Remove Tag	Remove Tag	Remove Tag	Remove Tag	Remove Tag
surity	Port 13	Port 14	Port 15	Port 16	Port 17	Port 18
nning Tree (Add VLAN Tag to output frames	Add Tag	Add Tag	Add Tag	Add Tag	Add Tag	Add Tag
king according to	Don't Care	Don't Care	Don't Care	Don't Care	Don't Care	Don't Care
the pvid of	Remove Tag	Remove Tag	Remove Tag	Remove Tag	Remove Tag	Remove Tag
P Relay Agent selected port)	Port 19	Port 20	Port 21	Port 22	Port 23	Port 24
up/Recovery	Add Tag	Add Tag	Add Tag	Add Tag	Add Tag	O Add Tag
ellaneous	Don't Care	Don't Care	Don't Care	Don't Care	Don't Care	Don't Care
Settings	Remove Tag	Remove Tag	Remove Tag	Remove Tag	Remove Tag	Remove Tag
•	Port 25	Port 26				
Full	Add Tag	Add Tag				
Lite version	Don't Care	Don't Care				
Full version	Remove Tag	Remove Tag				
			Update			
ut						

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

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

To add a group: Select more than one port

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

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

Administrator	WARNING!
PoE Pot Management VLAN Setting VLAN Member VLAN Member Multi to 1 Setting Nort-Association Port Setting	Current Tag-base VLAN Setting will be reset to default setting, if you click on "Continue" button to change to Port-base VLAN mode. Otherwise, click on "Back" button to cancel. Continue Back
 Per Port Counter QoS Setting 	
 Security Spanning Tree Trunking 	
 DHCP Relay Agent Backup/Recovery 	
 Miscellaneous SNMP Settings Lite/Full 	
 Lite version Full version 	
Logout	

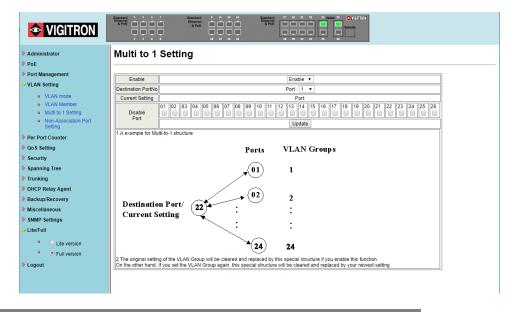


12.3 Multi to 1 Setting

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

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

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



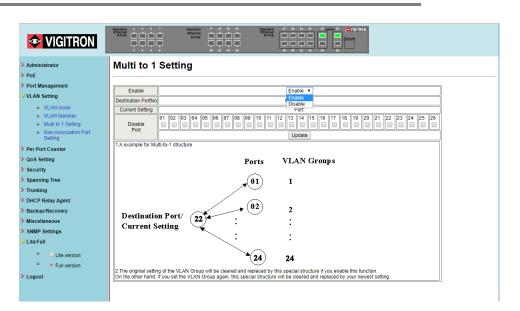
CAUTION: This setting will over ride other VLAN settings.

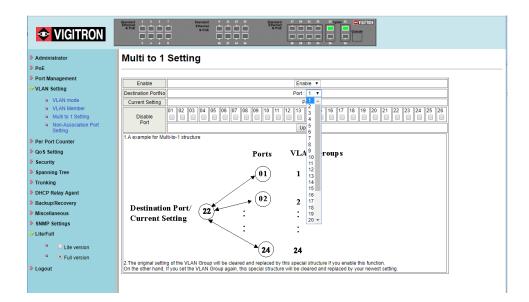
Select the Destination port:

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



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





12.4 Non-Association Port Setting

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

> Administrator > PoE	Non-Association Port Setting
Port Management VLAN Setting VLAN mode	Select 01 02 03 04 05 06 07 08 09 10 11 12 13 Port No. 14 15 16 17 18 19 20 21 22 23 24 25 26 Update
VLAN Mode VLAN Member Multi to 1 Setting Non-Association Port Setting	Note: If a port is the non-association port, it will not send packet to other non-association ports.
Per Port Counter	
 QoS Setting Security 	
Spanning Tree Trunking	
DHCP Relay Agent	
Backup/Recovery Miscellaneous	
SNMP Settings	
 Lite version Full version 	
 Full version Logout 	
	a

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

Counter Catego	исин инжин	
	• 9	
	Counter Mode Selection: Transmit Packet & Red	eive Packet
Port		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
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	6196	5716
26	0	0

VIGITRON			
Administrator PoE	Counter Category		
Port Management			
Per Port Counter		Counter Mode Selection: Transmit Packet & Receive Packet Upda Transmit Packet & Receive Packet	ite
Port Counter	Port	Drop packet & Receive Packet et	
Security	01	0 CRC error packet & Receive Packet	0
ite/Full	02	0	0
Logout	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
	14	0	0

13.1 Drop and Receive Packet

	Banders Brees		
Administrator	Counter Category		
οE			
ort Management		Counter Mode Selection: Drop packet & Receive P.	acket V Update
LAN Setting			
er Port Counter	Port	Drop packet 1	
 Port Counter 	01	0	0
S Setting	02	0	0
curity	03	0	0
anning Tree	04	0	0
inking ICP Relay Agent	05	0	0
ckup/Recovery	06	0	0
scellaneous	07	0	0
MP Settings	08	0	
e/Full			0
gout	09	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

13.2 CRC error packet and Receive Packet

fministrator	Counter Category		
E irt Management	-		
AN Setting		Counter Mode Selection: CRC error packet & Rece	ive Packet V Update
r Port Counter	Port	CRC error packet	Receive Packet
Port Counter	01	0	0
S Setting	02	0	0
curity	03	0	0
anning Tree	04	0	0
unking	05	0	0
CP Relay Agent	-		
ickup/Recovery scellaneous	06	0	0
MP Settings	07	0	0
e/Full	08	0	0
gout	09	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

13.3 Counter Modes Defined

The 3 different operational modes are:

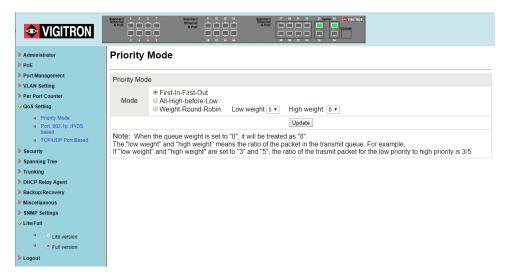
Field	Description
Transmit Packet & Receive Packet	This category shows both the received packet count (excluding the incorrect packet) and the transmitted packet count.
Drop Packet & Receive Packet	This category shows the number of received valid packet and the number of dropped packet.
CRC error Packet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

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

Section 14: QoS Settings

14.0 Priority Mode

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



14.1 Setting the Priority Mode

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

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

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

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

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

Administrator POE	Priority Mode
 PoE Port Management VLAN Setting Port Your Counter VLAS Setting Prorty Mode Prorty Mode Port, 802.1p.JPDS based Security Spanning Tree Trunking DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings Litte/Full Lite Version Full version Full version 	Priority Mode First-In-First-Out All-High-before-Low Weight-Round-Robin. Low weight or High weight or Update ed as "8". Interview weight and "high weight" are set to "3" and "5 6 7 ratio of the trasmit packet for the low priority to high priority is 3/5.
VIGITRON	
 Administrator PoE 	Priority Mode
Port Management	Priority Mode
 VLAN Setting Per Port Counter QoS Setting Priority Mode 	Mode
Port 802 tp JP/DS based TCP/UDP Port Based Security Spanning Tree Trunking DHCP Relay Agent	Update 1 2 Note: When the queue weight is set to "0", it will be treated as "8". 3 3 The "low weight" and "high weight" means the ratio of the packet in the trat. it queue. For example, acket for the low priority to high priority is 3/5. If "low weight" and "high weight" are set to "3" and "5", the ratio of the trats 5 it queue. For example, acket for the low priority to high priority is 3/5.
BackupiRecovery Miscellaneous SNMP Settings Lite/Full Lite/Full Lite version Full version Logout	

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 priory queue.

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

Administrator	Class of Service Conf	iguration						
PoE								
Port Management								
VLAN Setting Per Port Counter		Port	VLAN			Port	VLAN	
Per Port Counter	Port No.\Mode	Base	Tag	IP / DS	Port No.\Mode	Base	Tag	IP / DS
 Priority Mode 	1				14			
Port, 802.1p ,IP/DS	2				15			
 based TCP/UDP Port Based 	3				16			
ecurity	4				17			
panning Tree	5				18			
runking	6				19			
HCP Relay Agent	7				20			
Backup/Recovery Aiscellaneous	8				20			
SNMP Settings	9				21			
ite/Full	-							
Lite version	10				23			
• Full version	11				24			
.ogout	12				25			
	13				26			
				Upo	date			

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:

dministrator	Class of Service Configuration						
)E							
ort Management							
LAN Setting	Protocol		Opt	tion			
er Port Counter	FTP(20.21)		F-I-F-	0 •			
oS Setting	SSH(22)		F-1-F-	0 •			
 Priority Mode Port, 802.1p ,IP/DS 	TELNET(23)		F-1-F-	0 •			
based TCP/UDP Port Based	SMTP(25)		F-I-F-	0 •			
eourity	DNS(53)		F-I-F-	0 🔻			
panning Tree	TFTP(69)		F-I-F-				
runking	HTTP(80,8080)		F-I-F-				
HCP Relay Agent	POP3(110)		F-I-F-				
ackup/Recovery			F-I-F-				
liscellaneous NMP Settings	NEWS(119)		F-1-F-				
ite/Full	SNTP(123)		F-I-F-				
 O Lite version 	NetBIOS(137~139)		F-1-F-				
 Elle version Full version 	IMAP(143,220)						
Logout	SNMP(161,162)	F-I-F-O V F-I-F-O V					
	HTTPS(443)						
	MSN(1863)	F.J.F.O T					
	XRD_RDP(3389)	F-LF-Q V					
	QQ(4000,8000)						
	ICQ(5190)		F-I-F-				
	Yahoo(5050)	F-I-F-O V					
	BOOTP_DHCP(67,68)	Low V					
	User_Define_a		F-I-F-	0 🔻			
	User_Define_b		F-1-F-	0 🔻			
	User_Define_c		F-1-F-	0 🔻			
	User_Define_d		F-I-F-	0 🔻			
	User_Define Port number (1~65535) Mask(0~255)	User_Define_a Port: Mask:o	User_Define_b Port: Mask:0	User_Define_c Port: Mask:0	User_Define_d Port Mask:0		
	Note:The mask defines which bit is ignore For example, UDP/TCP port = 65535 and UDP/TCP port =65535 and mask=0, this m TCP Note:When the "override" item is selected	mask = 5,this means 65530, 6553 neans only 65535 is taken into ac P/UDP port QoS function Not Ovi	1, 65534 and 65535 are all take count. erride V				
			Update				
	The Class of Service for TCP/UDP port nu F-I-F-O: The incoming packet will be forwar Discard: The incoming packet will be disc High: The incoming packet will be forward	rded in first-in-first-out scheme. arded at the source port.	rator to assign the specific applic	ation to a priotity queue.			

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

j)

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

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

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

Section 15: Security

15.0 MAC Address Binding

ministrator E		
	MAC Address Binding	
: t Management		
Port Counter	Port No.	MAC Address
MAC Address Binding MAC Address Scan TOP/UDP Filter Web Security	1	
/Full		Select Port 1 V Binding Disable V Update
jout	Note: If you enable the MAC address bindi	ng function, the address leaning function will be disabled automatically.
	Port No.	Binding Status
	1	Disable
	2	Disable
	3	Disable
	4	Disable
	5	Disable
	6	Disable
	7	Disable
	8	Disable
	9	Disable
	10	Disable
	11	Disable
	12	Disable
	13	Disable
	14	Disable
	15	Disable
	16	Disable
	17	Disable
	18	Disable
	19	Disable
	20	Disable
	21	Disable
	22	Disable
	23	Disable
	24	Disable
	25	Disable

	A Pole			
Administrator PoE Port Management	MAC Address B	inding		
Per Port Counter	Port No.			MAC Address
 Security MAC Address Binding MAC Address Scan TCP/UDP Filter Web Security 	1			
Lite/Full		Select F	Port 1 🔻	Binding Disable V Update
Logout	Note: If you enable the MA	C address binding function, the addre		unction will be disabled automatically.
	1	Port No.	4	Binding Status
		1	6	Disable
		2	8	Disable
		3	10	Disable
		4	11 12	Disable
		5	13 14	Disable
		6	15	Disable
		7	17	Disable
		8	19	Disable
		9	20 🔻	Disable
		10		Disable
		11		Disable
		12		Disable

VIGITRON	ndard 1 3 5 7 Blandard triang				
 Administrator PoE Port Management 	MAC Address B	inding			
Per Port Counter	Port No.		MAC Address		
Security MAC Address Binding MAC Address Scan TCP/UDP Filter Web Security	1				
Lite/Full		Select	Port 1 V Binding Disable V Update		
Logout	Note: If you enable the MAC address binding function, the address leaning function w				
	1	Port No.	Binding Status		
		1	Disable		
		2	Disable		
		3	Disable		
		4	Disable		
		5	Disable		
		6	Disable		
		7	Disable		
		8	Disable		
		9	Disable		
		10	Disable		
		11	Disable		
		12	Disable		

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

	Sender 1 3 1 3 Sender 2 1 3 1 3 Sender 3 1 3 1 3 1 3 1 3 1 3 1 3 1 3 1 3 1 3	
Administrator	Scan MAC	
PoE		_
Port Management	Port Select: 1 V	
Per Port Counter	MAC Address Entry Status	
Security	Refresh	
 MAC Address Binding MAC Address Scan 		
 TCP/UDP Filter 		
Web Security		
Lite/Full		
Logout		
	л 	
	Sjandard 4 5 5 ? Slandard 9 66 85 Sjandard 87 89 28 28 26 uptine 26 🚭 WGIIROD	
VIGITRON	Bandard Benda	
Administrator	Scan MAC	
≯ PoE		
Port Management	Port Select: 1 V	
Per Port Counter	1 A MAC Address Entry Status	
💀 Security	2 3 Refresh	
MAC Address Binding	4 5	
MAC Address Scan	6 7	
 TCP/UDP Filter Web Security 	8	
Lite/Full	9 10	
> Logout	11 12	
Logour	13	
	14 15	
	16 17	
	18	
	19 20 -	

15.2 Securing Ports Using Mac Addresses

If no MAC address is entered when the scan is peformed the MAC address of the connected device will be displayed and the "Entry Status" will show "Dynamic" indicating the 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.

Functi	ion Enable	Disable •									
Port Counter urity		Unable T mightle T Note: (1)The outgoing packet with selected protocol will be either forwarded or dropped at secure WAX port as the figure shwon below: (2)The outgoing packet with selected protocol will be forwarded or dropped at deter protocols will be forwarded. "positive" means the selected protocol will be forwarded on deter protocols will be dropped.									
		■ FTP(20,21)	SSH(22)	I TELNET(23)	□ SMTP(25)	■ DNS(53)	TFTP(69)	BHTTP(80,8080)	POP3(110)		
Protoc	loc	NEWS(119)	SNTP(123)	NetBIOS(137~139)	IMAP(143,220)	© SNMP(161,162)	HTTPS(443)	© XRD_RDP(3389)	BOOTP_DHCP(67,68		
		User_Define_a	User_Define_b	User_Define_c	II User_Define_d						
Note: 1	Note: These User-defined A/B/C TCP/UDP settings use the smae port number settings as the Users-defined A/B/C Port number settings in Qos's Class of Service webpage.										
	Secure WAN port	B Port01	Port02	Port03	E Port04	Dort05	Port06	E Port07	Port08		
		E Port09	Port10	Port11	El Port12	DPort13	Port14	III Port15	Dert16		
Secur	e wan port	E Port17	Port18	Port19	E Port20	Dert21	Port22	Dort23	III Port24		
		Port25	Port26								
	Uodate										
	affic Path Port	s of Secure WAN po	eck. TCP/UDP Part Nutaber	The packet will be either adopted or forwards. This is the secure WAN port Egress Port							

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

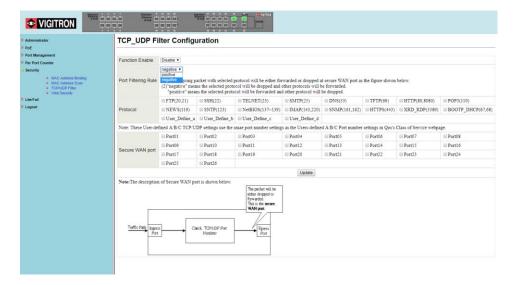
Example:

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

Results

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

Administrator PoE	TCP_UDP Fi	Iter Configu	uration									
Port Management Per Port Counter	Function Enable	Disable ¥ Enable										
Security MAC Address Binding MAC Address Scat TCP/UDP Filter Web Security	Port Filtering Rule	(2)"negative" mea	ns the selected proto	protocol will be either for col will be dropped and col will be forwarded an	other protocols will b	e forwarded.	the figure shwon	below.				
Lite/Full		@ FTP(20,21)	SSH(22)	I TELNET(23)	SMTP(25)	BDNS(53)	BTFTP(69)	BHTTP(80,8080)	B POP3(110)			
Logout	Protocol	NEWS(119)	SNTP(123)	@ NetBIOS(137~139)	IMAP(143,220)	■ SNMP(161,162)	HTTPS(443)	IN XRD_RDP(3389)	BOOTP_DHCP(67,6)			
		User_Define_a	User_Define_b	User_Define_c	User_Define_d							
	Note: These User-del	Note: These User-defined A/B/C TCP/UDP settings use the smae port number settings as the Users-defined A/B/C Port number settings in Qoi's Class of Service webpage.										
		E Port01	Dert02	Dort03	Dert04	Dert05	E Port06	Port07	Port08			
	0	E Port09	Port10	III Port11	III Port12	D Port13	E Port14	III Port15	Port16			
	Secure WAN port	E Port17	Port18	III Port19	Port20	Dert21	Port22	III Port23	Port24			
		Port25	Port26									
		Update										
	Note: The description	ī .	eck TCP/UDP Port Number	The packet will be entry dopped or florwardst. This is the secure WAN port. Egress Port								



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

VIGITRON	Standard 1 3 5 7 Ethernet A Pol	Standard Ethernet & PoE			ndard 17 11 hernet 8 Poe 1	21 23 2 21 23 2 2 2 24 2	Suplink 25 Conse		
 Administrator PoE Port Management 	Web Manageme	ent Filte	er						
Per Port Counter	State:	Disabl	e 🔻						
 Security MAC Address Binding 		01	02	03	04	05	06	07	08
 MAC Address Scan TCP/UDP Filter 	Access Port:	09	10	11	12	13	14	15	16
 Web Security Lite/Full 	Access Fort.	17	18	19	20	21	22	23	24
Logout		25	26						
				Upda	ate				
	Selected ports are e	enabled for	web access	Unselecte	d ports are	disabled. C	lick update	to save ch	anges.
	· ·				-		•		-

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.

VIGITRON	Standard 1 3 5 7 Ethernet 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Standard Ethernet & PoE		Star Eth 8	ndard 17 19 k POE		Uplink 25 Consc Consc 26		
 Administrator PoE Port Management 	Web Manageme								
 Per Port Counter Security MAC Address Binding MAC Address Scan TCP/UDP Filter Web Security Lter/Full 	State: Access Port:	Disable Enable Disable	02 10 18	03 11 19	04 12 20	05 13 21	06 14 22	07 15 23	08 16 24
₽ Logout	Selected ports are e	25 nabled for we	26	 Upda Unselected		 disabled. C	 lick update	 to save cha	 anges.

Section 16: Spanning Tree

16.0 STP Bridge Settings

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

Administrator	STP Bridge Settings										
> PoE											
Port Management	Spanning Tree Settings										
VLAN Setting	Bridge True Forward										
Per Port Counter	STP Mode Priority Hello Time Max Age Delay										
QoS Setting	(0~61440) (1~10 Sec) (6~40 Sec) (4~30 Sec)										
Security											
Spanning Tree	Submit										
 STP Bridge Settings STP Port Settings 	Note: 2*(Forward Delay-1) >= Max Age,										
 Loopback Detection 	Max Age >= 2*(Hello Time+1)										
Trunking											
DHCP Relay Agent	Bridge Priority must be multiplies of 4096										
Backup/Recovery	Note: If you enable the MAC address binding function, the address leaning function will be disabled automatically. Then both RSTP/STP and										
Miscellaneous	ddress learning will be affected.										
SNMP Settings	Bridge Status										
✓ Lite/Full	Forward										
Lite version	STP Mode Bridge ID Hello Time Max Age Delay										
 Full version 	RSTP 32768:10 F0 13 F0 18 26 2 20 15										
Logout											
	Root Status										
	Root ID Hello Time Max Age Forward Delay										
	I'm the root bridge! 2 20 15										

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



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

	Standard Ethernet & Poe		ndard 9 11 13 iermet 1 11 11 2 POE 1 11 11 11 11 11 11 11 11 11 11 11 11 11 11	Ethernet & PoE		25 Uptink 25 Console Console 26 24 24	1800				
 Administrator PoE 	STP Brid	ge Settii	ngs								
Port Management		Sna	anning Tree Set	tings		1					
VLAN Setting		Bridge	1		Forward						
Per Port Counter	STP Mode	Priority	Hello Time	Max Age	Delay						
QoS Setting		(0~61440)	(1~10 Sec)	(6~40 Sec)	(4~30 Sec)						
Security	· ·										
💀 Spanning Tree	Dischla										
STP Bridge Settings	M STP m										
STP Port Settings		$\begin{array}{l} \begin{array}{l} \begin{array}{l} \begin{array}{l} \begin{array}{l} \begin{array}{l} \begin{array}{l} \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{l} \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{l} \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{l} \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{l} \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{l} \end{array} \\ \end{array} $									
Loopback Detection Trunking	Max Age >= 2	*(Hello Ilme+	-1)								
DHCP Relay Agent	Bridge Priority	v must be multi	plies of 4096								
Backup/Recovery	Note: If you en	able the MAC	address binding	function the a	ldress leaning fu	nction will be d	lisabled automatically. Then both RSTP/STP and				
Miscellaneous	address learning										
SNMP Settings			Duida	e Status			ח				
😵 Lite/Full						Forward					
Lite version	STP Mode	Brid	lge ID	Hello Time	Max Age	Delay					
• Full version	RSTP	32768:10 F	0 13 F0 18 26	2	20	15					
Logout							_				
_											
			Root Status								
	Roo		Hello Time		Forward Delay						
	I'm the ro	ot bridge!	2	20	15						

16.1 STP Port Settings

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

	Standard 1 8 5 7	Standard	11 12 13	Standard 17 19	21 22 25 U ^{ga} nk 💽 VIGTRON		
	A PoE	8 PoE		& PoE			
			چيا ليونا ليونا 12 14 14	نيانيا ه ه	ана а ана а		
Administrator	STP Por	t Settings					
PoE							
Port Management	5	TP Port Settings	RPC				
VLAN Setting		Priority	RPC				
Per Port Counter	Port No.	(1~)	200000000)				
QoS Setting Security		(0~240)	AUTO				
Spanning Tree		Submit					
 STP Bridge Settings STP Port Settings 	Priority should	be a multipe of 16					
Loopback Detection							
Trunking							
DHCP Relay Agent Backup/Recovery				S	TP Port Status		
Miscellaneous	Port No.	RPC	Priority	State	Status	Designated Bridge	Designated Port
SNMP Settings	1	Auto:0	0x80		Disable		
Lite/Full	2	Auto:0	0x80		Disable		
Lite version	3	Auto:0	0x80		Disable		
• Full version	4	Auto:0	0x80		Disable		
Logout	5	Auto:0 Auto:0	0x80 0x80		Disable Disable		
	7	Auto:0	0x80 0x80		Disable		
	8	Auto:0	0x80		Disable		
	9	Auto:0	0x80		Disable		
	10	Auto:0	0x80		Disable		
	11	Auto:0	0x80		Disable		
	12	Auto:0	0x80		Disable		
	13	Auto:0	0x80		Disable		
	14	Auto:0 Auto:0	0x80 0x80		Disable		
	15	Auto:0	0x80 0x80		Disable		
	10	Auto:0	0x80		Disable		
	18	Auto:0	0x80		Disable		
	19	Auto:0	0x80		Disable		j
	20	Auto:0	0x80		Disable		
	21	Auto:0	0x80		Disable		
	22	Auto:0	0x80		Disable		
	23	Auto:0 Auto:0	0x80 0x80		Disable Disable		
	24	Auto:20000	0x80	Designated	Forwarding		
	26	Auto:0	0x80	Port	Disable		
	20	Auto:0	0880		Disable		

	forestand 1 1 1 5	Standard	11 13 15	Remote 17 18	21 23 25 U <mark>šiek Ch</mark> istrok		
		Etherret A PoE		& PoE			
Administrator	STP Po	rt Settings					
PoE		it oottingo					
Port Management		CTD Dant Cattings					
VLAN Setting		STP Port Settings	RPC				
Per Port Counter		Priority	ICI C				
	Port No.		200000000)				
QoS Setting		(0~240)	-AUTO				
Security	The second secon		ACIO				
Spanning Tree		Submit					
 STP Bridge Settings STP Port Settings 	Prio 2 ou	ld be a multipe of 16					
 Loopback Detection 	3	no oc a monipe of ro					
Trunking	4						
DHCP Relay Agent	5 -			S	TP Port Status		
Backup/Recovery	7	DDC.	Detecto	1	1	Destant 1D 11	Designated
Miscellaneous	P 8 .	RPC	Priority	State	Status	Designated Bridge	Port
SNMP Settings	10	Auto:0	0x80		Disable		
ite/Full		Auto:0	0x80		Disable		
Lite version	12	Auto:0	0x80		Disable		
• Full version	14	Auto:0	0x80		Disable		
ogout	15	Auto:0	0x80		Disable		
	17	Auto:0	0x80		Disable		
		Auto:0	0x80		Disable		
	19 -	Auto:0	0x80		Disable		
	9	Auto:0	0x80		Disable		
	10	Auto:0	0x80		Disable		
	11	Auto:0	0x80		Disable		
	12	Auto:0	0x80		Disable		
	13	Auto:0	0x80		Disable		
	14	Auto:0 Auto:0	0x80 0x80		Disable Disable		
	15	Auto:0	0x80 0x80		Disable		
	10	Auto:0	0x80 0x80		Disable		
	18	Auto:0	0x80		Disable		
	19	Auto:0	0x80		Disable		
	20	Auto:0	0x80		Disable		
	21	Auto:0	0x80		Disable		
	22	Auto:0	0x80		Disable		
	23	Auto:0	0x80		Disable		
	24	Auto:0	0x80		Disable		
	25	Auto:20000	0x80	Designated Port	Forwarding		
	26	Auto:0	0x80		Disable		

Field	Description
Port No.	To configure the parameters of RSTP/STP port, the administrator should select a physical port number, assign a priory number, enter the RPC and then press "Submit" button.
Priority (0~240)	Priority field defines the priority of the RSTP/STP port. The lower the number is, the higher possibility it will become a root port. There is a default value for each port.
RFC (0~20000000)	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

stP Bridge Settings
 STP Port Settings
 Loopback Detection
 Trunking

Lite version
 Full version

DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings Lite/Full

Logout

Standard 17 U 21 23 25 UHm CVGITRON 8 Protein Control Control

Administrator
PoE
Port Management

VLAN Setting Per Port Counter QoS Setting Security

Loopback Detection Settings

Loopback Detect Function		Disable •	
Auto Wake Up		Disable •	
Wake-Up Time Interval		10 sec 🔻	
	Subm		

Reset All Ports

Standard Elternet & PoE

Port No.	Status
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	

VIGITRON	
Administrator PoE	Loopback Detection Settings
Port Management	Auto Wake Up Disable
VLAN Setting	Wake-Up Time Interval
Per Port Counter	Submit
QoS Setting	Gustine
Security	
 Spanning Tree STP Bridge Settings 	Reset All Ports
 STP Port Settings Loopback Detection 	Port No. Status
Trunking	1
DHCP Relay Agent	2
Backup/Recovery	3
Miscellaneous	4
SNMP Settings	5
V Lite/Full	6
Lite version	
Elle version Full version	9
Logout	10
	13

Administrator	Loopback Detection Settings
PoE	
Port Management	Loopback Detect Function Disable V
VLAN Setting	Auto Wake Up Disable Wake Up Time Internal Disable
Per Port Counter	Finable
QoS Setting	Submit
Security	
🥺 Spanning Tree	Reset All Ports
STP Bridge Settings	Reset All Ports
STP Port Settings	Port No. Status
Loopback Detection Frunking	1
DHCP Relay Agent	2
Backup/Recovery	3
Miscellaneous	4
SNMP Settings	5
-	6
2 Lite/Full	7
Lite version	8
• Full version	9
Logout	10
	12
	13

VIGITRON Enter		
Administrator PoE Port Management	Loopback Detection Settin	gs
 VLAN Setting Per Port Counter 	Auto Wake Up Wake-Up Time Interval Sub	Disable V 10 sec V nit 5 sec
QoS Setting Security		10 sec 30 sec 60 sec
 Spanning Tree STP Bridge Settings STP Port Settings Loopback Detection 	Reset All Ports Port No. Status	
 Trunking DHCP Relay Agent 	1 2 3	
Backup/Recovery Miscellaneous SNMP Settings	4 5 6	
 Lite/Full C Lite version 	7	
 Full version Logout 	9 10 11	
	12 13 14	
	14	

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 Trucking

Member Ø <th></th> <th>Standard Ethernet & PoE</th> <th>Standard Ethernet & PoE</th> <th></th> <th>" " "</th> <th>Standard Ethemet & PoE</th> <th>л и ССС ССС и и</th> <th></th> <th>25 Upink 25</th> <th></th> <th>11</th> <th></th> <th></th>		Standard Ethernet & PoE	Standard Ethernet & PoE		" " "	Standard Ethemet & PoE	л и ССС ССС и и		25 Upink 25		11		
 PoE Port Kanagement VLAN Setting VLAN Setting Per Port Counter Gos Setting Security Spanning Tree Chick Aggregation Settings Link Aggregation Settings Settings Link Aggregation State Disable ▼ Di	Administrator	-	Trunkina										
> VLAN Setting Link Aggregation Algorithm MAC Src&Dst ▼ > Per Port Counter Submit Submit > Go S Setting Submit Submit > Security Sanning Tree Refresh > Trunking Ink Aggregation Bit Mac Src&Dst ▼ > Dick Aggregation P1 P2 P3 > Dick Relay Agent Member Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø	PoE												
 Per Port Counter Go S setting Security Spanning Tree Trunking Submit DtCP Relay Agent Backup/Recovery Miscellaneous State Disable ▼ D	Port Management		System Prie	ority			1		(1~6	5535)			
 Cos Setting Security Spanning Tree Trunking Link Aggregation Settings DHCP Reby Agent Backup/Recovery State DISAR Disable ▼ Disable ▼ Disable ▼ Disable ▼ Disable ▼ Disable ▼ Disable ▼ Deration Key 1 (1-65535) 2 (1-65535) 3 (1-655) Time Out Short Time Out ▼ Short Time Out ▼ Short Time Out ▼ Short Time Out ▼ Passive ▼ Passive ▼ Passive ▼ Passive ▼ Passive ▼ 	VLAN Setting	Ì	Link Aggregation	Algorith	m			MAC S	rc&Dst •	·			
 Security Spanning Tree Tunking Link Aggregation Settings DHC Relay Agent Backup/Recovery Mscellaneous State Disable ▼ Dis	Per Port Counter				S	ubmit							
 Spanning Tree Tunking Link Aggregation settings Hick Aggregation Settings Backup/Recovery Miscelianeous SNMP Settings LiteFull Subsettings LiteFull State Disable ▼ Disable ▼<	QoS Setting											1	
Tunking Link Group 1 Link Group 2 Link Group 3 > DtCP Relay Agent P1 P2 P3 P4 P5 P6 P7 P8 P2.5 P2 > DtCP Relay Agent Ø <th>Security</th> <th></th>	Security												
Ink Aggregation Settings Link Group 1 Link Group 2 Link Group 3 PI CP Relay Agent P1 P2 P3 P4 P5 P6 P7 P8 P25 P2 P Backup Recovery Image: Covery	Spanning Tree		Refresh										
• Link Aggregation Settings P1 P2 P3 P4 P5 P6 P7 P8 P25 P2 • DHCP Relay Agent ● </th <th>7 Trunking</th> <th></th> <th></th> <th>1</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	7 Trunking			1									
Member Image: Constraint of the section o										-	1		-
Backup/Recovery Interfect								<u> </u>					P26
Miscellaneous State Disable ▼ Disable ₹ Disable ₹ Disable ₹ Disable ₹ Disable ₹ Disable ₹ Disable ₹ <t< th=""><th></th><th></th><th>Member</th><th></th><th></th><th></th><th></th><th></th><th></th><th>1</th><th></th><th></th><th></th></t<>			Member							1			
SMMP Setting Date Date <thdate< th=""> Date Date</thdate<>	Backup/Recovery												
LtterFull	Miscellaneous		State		Disal	ole 🔻			Disa	ble 🔻		Dis	able 🔻
Operation accy (* 00000) (* 0000) (* 0000) (* 00000) (* 0000) (* 0000)) (* 0000)	SNMP Settings		Type		LAC	ΡV			LAC	P 🔹		L	ACP V
• • Full version Logout	Lite/Full		Operation Key	1		(1~65	535)	2		(1~65	535)	3	(1~65535)
Logout	Lite version		Time Out		Short Tin	ne Out 🔻		[Short Tir	ne Out 🔻	·	Short	lime Out ▼
	• Full version		Activity		Pass	ve •			Pass	ive 🔻		Pa	ssive 🔻
	Logout						S	ubmit					
Note: If you enable LACP on some specified ports and their link partners are normal port without LACP these specific													
concent transmit packet to/receive packet from the link partner.									mers are	normal	port wit	hout LACP,th	ese specified por

Administrator PoE	Trunking										
Port Management	System Pri	ority			1		(1~65	535)]	
VLAN Setting	Link Aggregation	•	m			MAC S	irc&Dst V				
Per Port Counter				ubmit		MAC S					
QoS Setting						MAC S	irc&Dst]	
Security											
Spanning Tree	Refresh										
opunning rice	TKelleon										
Trunking											
			Link G	roup 1			Link G	roup 2		Link	Group 3
Trunking Link Aggregation Settings		P1	Link G	P3	P4	P5	Link G	roup 2	P8	Link P25	Group 3 P26
 Link Aggregation Settings 	Member	P1			₽4	P5			P8		-
Link Aggregation Settings DHCP Relay Agent	Member		P 2	P3			P6	P 7		P25	P26
 Link Aggregation Settings DHCP Relay Agent Backup/Recovery 	Member		₽2 ✓	P3 ✓	1		P6 	P7 	1	P25 	P26
			P2	P3 ✓	1		P6	P7	1	P25	P26
Link Aggregation Settings DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings	State		P2	P3			P6	P7		P25	P26
 Link Aggregation Settings DHCP Relay Agent Backup/Recovery Miscellaneous 	State Type	 ✓ ✓	P2	P3 	535)		P6	P7 	535)	P25	P26
Link Aggregation Settings DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings LiterFull	State Type Operation Key	 ✓ ✓	P2	P3 ✓ ble ▼ (1~65 ne Out ▼	535)		P6 Disat	P7 	535)	P25 ✓ Disa [] [] [] [] [] [] [] [] [] []	P26 ✓ able ▼ CP ▼ (1~65535)

This page is used to set trunk group for load balance and cable link autobackup. 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 $1 \sim \text{port } 8$, port 25 and port 26, and trunk 1 consists of port $1 \sim \text{port } 4$, trunk 2 consists of port 5 $\sim \text{port } 8$, trunk 3 consists of port 25, port 26. 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

 Administrator PoE 	Note The port has been set MAC bunding()
 Port Management VLAN Setting 	
 Per Port Counter QoS Setting 	
 Security 	
Spanning Tree V Trunking	
 Link Aggregation Settings 	
 DHCP Relay Agent Backup/Recovery 	
Miscellaneous	
SNMP Settings	
> Logout	

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

PoE										1	
Port Management	System Prie				1	-	(1~6				
VLAN Setting	Link Aggregation	Algorith				MAC S	rc&Dst •				
Per Port Counter			S	ubmit							
QoS Setting											
Security											
Spanning Tree	Refresh										
Trunking			Link G	roun 1			Link G	roup ?		L ink (Group 3
 Link Aggregation Settings 		P1	P2	P3	P4	P5	P6	P7	P8	P25	P26
DHCP Relay Agent	Member										
Backup/Recovery											
Miscellaneous	State		Disa	ble 🔻	·		Disa	ble 🔻		Disa	ible 🔻
SNMP Settings	Туре		Disal				LAC	P 🔹		LAC	CP V
Lite/Full	Operation Key	1	Lildu	(1~65	535)	2		(1~65	535)	3	(1~65535)
Lite version	Time Out		Short Tir	ne Out 🔻			Short Tir	ne Out 🔻		Short Ti	me Out 🔻
• Full version	Activity		Pass	ive 🔻			Pass	ive 🔻		Pass	sive 🔻
Logout					S	ubmit					
	Note: If you enable LACP cannot transmit packet to/re						ners are	normal	port wit	hout LACP,thes	se specified po

	ADE & POE	الیالیال ۱۱ ۱۲ ۱۹	16		18 20		26 26		_		
Administrator	Trunking										
PoE											
Port Management	System Pr	iority			1		(1~6	5535)			
VLAN Setting	Link Aggregation	n Algorith	m			MAC S	rc&Dst •	-			
Per Port Counter			S	ubmit							
QoS Setting											
Security											
Spanning Tree	Refresh										
r Trunking	(received)										
-			Link G	roup 1			Link G	roup 2		Link	Group 3
 Trunking Link Aggregation Settings 		P1	Link G	roup 1 P3	P4	P5	Link G	P7	P8	Link P25	Group 3 P26
 Link Aggregation Settings 	Member	P1			₽4 ✓	₽5 ♥			P8		-
 Link Aggregation Settings DHCP Relay Agent 	Member		P2	P3		<u> </u>	P6	P7		P25	P26
 Link Aggregation Settings DHCP Relay Agent Backup/Recovery 	Member		₽2 Ø	P3		1	P6 	P7 ✓		₽25 ✓	P26
 Link Aggregation Settings DHCP Relay Agent Backup/Recovery Miscellaneous 			P2 ✓	P3		1	P6 	P7 ✓ ble ▼		P25	P26
Link Aggregation Settings DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings	State		P2 Disat	P3 ple V P V C 65		1	P6 Disal	P7 ✓ ble ▼		P25	P26
Link Aggregation Settings DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings	State Type	···	P2 Disat	P3 ble V P V c -65		 	P6 Disal	P7 ♥7 ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■		P25	P26
Link Aggregation Settings DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings Lite/Full	State Type Operation Key	···	P2 Disat LAC Stati LAC	P3 ble P c -65 P -65 P -65		 	P6 Disal	P7 ✓ DIE ▼ (1~65 ne Out ▼		P25 ✓ Dis 3 Short	P26 ■ sable ▼ ACP ▼ (1~65535)
Settings DHCP Relay Agent Backup/Recovery Miscellaneous SMMP Settings LiterFull Ute version	State Type Operation Key Time Out	···	P2 Disat LAC Stati LAC Short Tin	P3 ble P c -65 P -65 P -65	535)	 	P6 Disal LAC Short Tin	P7 ✓ DIE ▼ (1~65 ne Out ▼		P25 ✓ Dis 3 Short	P26 → sable ▼ ACP ▼ (1~65535) Time Out ▼

	Trunking										
PoE	System Pri	ovite			1		(1-6	5535)			
Port Management	· · · · · · · · · · · · · · · · · · ·						×				
VLAN Setting	Link Aggregation	Link Aggregation Algorithm MAC Src&Dst V									
Per Port Counter		Submit									
QoS Setting											
Security											
Spanning Tree	Refresh										
Trunking											
Link Aggregation		_	Link G					Froup 2	-		Group 3
Settings		P1	P2	P3	P4	P5	P6	P7	P8	P25	P26
					1	1	Image: A start and a start	v	Image: A start and a start	a	
DHCP Relay Agent	Member					•					
DHCP Relay Agent	Member										
DHCP Relay Agent Backup/Recovery	Member										able V
DHCP Relay Agent Backup/Recovery Miscellaneous				 ble •			 Disa			Dis	
DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings	State		 Disa	 ble •			 Disa	 ble ▼		Dis	able 🔻
DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings	State Type		 Disa LAC Short Tir	 ble ▼ P ▼ (1~65) ne Out ▼			 Disa	 ble • :P • (1~65	535)	LA	able CP
DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings Lite/Full	State Type Operation Key		 Disa LAC	 Die V P V (1~65 ne Out V ie Out			Disa LAC	 ble • :P • (1~65	535)	Dis. LA 3 Short T	able CP (1~65535)

			Ş.	Standard Ethernet & PoE			25 upink 25				
Administrator	Trunking										
PoE				1						1	
Port Management	System Priority 1 (1~65535)										
VLAN Setting	Link Aggregation	Link Aggregation Algorithm MAC Src&Dst V									
Per Port Counter	Submit										
QoS Setting											
Security											
Spanning Tree	Refresh										
Trunking		Link Group 1 Link Group 2 Link Group 3									a
 Link Aggregation 		P1	P2	P3	P4	P5	P6	P7	P8	P25	P26
Settings DHCP Relay Agent	Member	P1	P2	P5	P4	PS	PO	P/	Po	P25	P20
Backup/Recovery	Memoer										
Miscellaneous	State		Disat					ble 🔻			able V
SNMP Settings	Type		LAC				LAC			LACP V	
Lite/Full	Operation Key	1	2110	(1~65	535)	2	2710	(1~65	(535)	3	(1~65535)
Lite version	Time Out		Short Tin				Short Tir				(1-05555)
Elle version Elle version	Activity		Passi				_	ive V			ssive V
e Puli Version	Activity		Pass	ive	0	ubmit	1 835	. 911		1 44	Salve .
Logout			Active	e	3	aonnt					
	Note: If you enable LACP cannot transmit packet to re						mers are	normal	port wit	hout LACP,the	ese specified port

Description

Field

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.
Туре	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.

VIGITRON		Consele
Administrator	DHCP Relay Agent	
> PoE		
Port Management	DHCP Relay State :	Disable V
VLAN Setting		
Per Port Counter	DHCP Relay Hops Count Limit (1-16):	16
QoS Setting	DHCP Relay Option 82 State :	Disable •
Security	Update	
Spanning Tree		
Trunking		
V DHCP Relay Agent		
 DHCP Relay Agent 		
 Relay Server VLAN MAP Relay 		
Agent		
Backup/Recovery		
Miscellaneous		
SNMP Settings		
💀 Lite/Full		
Lite version		
• Full version		
Logout		

Field	Description
DHCP Relay State	Allow the administrator to enable/disable Relay Agent function.
	°
DHCP Relay Hops	Specify the maximum number of Relay Agent
Count Limit	traveling from DHCP agent to DHCP server.
DHCP Relay	The pre-condition for enabling/disabling this function
Option 82 State	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.

VIGITRON	
Administrator	DHCP Relay Agent
PoE	
Port Management	DHCP Relay State : Disable •
VLAN Setting	Enable
Per Port Counter	DHCP Relay Hops Count Limit (1-16): Disable
 QoS Setting Security 	DHCP Relay Option 82 State : Disable •
 Spanning Tree 	Update
> Spanning Tree	
DHCP Relay Agent	
 DHCP Relay Agent 	
 Relay Server 	
 VLAN MAP Relay Agent 	
Backup/Recovery	
Miscellaneous	
SNMP Settings	
v Lite/Full	
 Lite version Full version 	
Logout	
Standard	сэ 5 7 Standard 9 6 8 6 Standard 9 8 8 8 Standard 9 8 8 8 Standard 9 8 8 8 Standard 8 (Ст. 1993) Эндэ дэгдээ Боннов суулар дээ (Ст. 1992) (Ст. 1993) (Ст. 1993)
	արիարիարիարի հանրիարիարի հանրիարիարիարի 2 4 6 8 39 22 14 36 38 38 38 38
Administrator	DHCP Relay Agent
PoE	
Port Management	DHCP Relay State : Disable V
VLAN Setting	
Per Port Counter	DHCP Relay Hops Count Limit (1-16): 16
QoS Setting	DHCP Relay Option 82 State : Disable
> Security	Update Disable
 Spanning Tree Trunking 	
DHCP Relay Agent	
 DHCP Relay Agent Relay Server 	
VLAN MAP Relay	
Agent	
Backup/Recovery Miscellaneous	
SNMP Settings	
V Lite/Full	
 Lite version Eull version 	
- C Full version	
Logout	

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

i

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

VIGITRON				
Administrator	DHCP Relay Age	ent		
PoE				
ort Management	DHCP Server IP			Add
AN Setting				
er Port Counter		DHCP	Server IP List	
oS Setting		DIICI	Server II List	
ecurity				
anning Tree				
unking				
HCP Relay Agent				
 DHCP Relay Agent 				
 Relay Server VLAN MAP Relay 				
Agent				
ackup/Recovery				
scellaneous				
MP Settings				
te/Full				
Lite version				
 Elleversion Full version 				
Stards	et Ethernet Ethernet			
ogout			Console	
VIGITRON	DHCP Relay Age	ent		[A44]
TIGITRON Construction dministrator oE ort Management			Console	Add
dministrator oE ot Management LAN Setting	DHCP Relay Age	ent		Add
CONTRACTORY AND A SETTING Aministrator DE OT Management LAN Setting er Port Counter	DHCP Relay Age	ent		Add
CURCETRON dministrator Se brt Management AN setting pr Port Counter os Setting	DHCP Relay Age	ent		Add
CONCEPTION dministrator oE ort Management LAN Setting er POrt Counter o S Setting ecurity	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	
dministrator oE or Management LAN Setting er Port Counter os Setting currity panning Tree	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	
CALL AND	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	
Content of the second s	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	
CALL AND	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	
CONTRIBUTION Administrator of ort Management LAN setting er Port Counter os Setting county panning Tree uniking HCP Relay Agent DHCP Relay Agent DHCP Relay Agent Control	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	
CONTROLOGY dministrator oc or transgement LAN Setting er Port Counter os Setting ser Jort Counter os Setting panning Tree unking HCP Relay Agent - Relay Savar - Relay Savar - KLAN MAP Relay Agent	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	
EVIGITRON diministrator SE or Management LAN Setting or Port Counter os Setting serunty manning Tree surking HCP Relay Agent = DHCP Relay Agent = DHCP Relay Agent = VLAN MAP Relay Agent = VLAN MAP Relay Agent	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	
CONTROLOGY Aministrator DE or Management LAN Setting er Port Counter S Setting ecurity panning Tree unking HCP Relay Agent = DHCP Relay Agent = DHCP Relay Agent = DHCP Relay Agent = VLAN MAP Relay Agent ackup/Recovery iscellaneous	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	
Content of the second s	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	
CONCEPTION dministrator oE ort Management LAN Setting er Port Counter so Setting ecurity panning Tree surking HCP Relay Agent • DHCP Relay Agent • DHCP Relay Agent • DHCP Relay Agent • DHCP Relay Agent • ULAN MAP Relay Agent actup/Recovery lascellaneous NMP Settings terFull	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	
CONCRETERON dministrator og or Management LAN Setting er Port Counter os Setting er Port Counter so Setting county panning Tree curity panning Tree curity panning Tree curity panneng Tree setting to POPC Relay Agent a Reay Saver b MAM ARP Relay actup/Recovery liscellancous huff Setting tareful * Other version	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	
CONCECTERON dministrator oE or Management LAN Setting er Port Counter to's Setting er Port Counter so Setting curity panning Tree curity panning Tree curity panning Tree curity panning Tree Counter to Relay Server B Colle Relay Magnet B Colle R	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	
CONTRACTORY dministrator og or Management LAN Setting er Port Counter os Setting ser Soft Counter os Setting ser Soft Counter os Setting panning Tree unking HCP Relay Agent 0 DCP Relay Agen	DHCP Relay Age VLAN ID MAP List	ent	Map Server IP V	

Section 18: Backup and Recovery

18.0 Configuration Backup/Recovery

VIGITRON Bread	
Administrator Administrator PoE Vulan Setting Por Port Counter Os Setting Security Spanning Tree Trunking	Configuration Backup/Recovery Backup(Switch→PC) Please check "Download" to download EEPROM contents. Download Recovery(PC—Switch) Decovery(PC
 DHCP Relay Agent Backup/Recovery Miscellaneous SNMP Settings Lite/Full Lite version 	Password : Select the image file : Choose File No file chosen Update
 Full version Logout 	

18.1 Back Up

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

18.2 Recovery

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



Section 19: Miscellaneous Settings

19.0 Miscellaneous Settings Defined

Administrator	Miscellaneous S	etting											
PoF													
Port Management													
VLAN Setting						Output	Queue Aging	Time					
Per Port Counter	Aging time		e output queue aging function allows the administrator to select the aging time of a packet stored in the output queue. A packet stored in the output queue for a long time lower the free packet buffer, resulting in the poor utilization of the buffer and the poor switch performance.										
QoS Setting	Disable • ms	will lower the	free packet b	uffer, resulting	in the poor utili	zation of the b	uffer and the p	por switch perf	ormance.				
Security			VLAN Striding										
Spanning Tree	VLAN Striding	When this fu	action is anabl	lod the switch	will forward a r	ini cast packet	to the dectinat	ion port. No m	atter whether ti	he destination	out is in the es	mo VI AN arou	10
Trunking	Disable *	when ans to	en this function is enabled, the switch will forward a uni-cast packet to the destination port. No matter whether the destination port is in the same VLAN group.										
DHCP Relay Agent			IGMP Snooping V1 & V2										
Backup/Recovery	IGMP Snooping	10110 0111	ina V1 & V2 fu	and an an able									
Miscellaneous	Disable *	IGMP Shoop	ang v1 & v2 tu	Inction enable									
SNMP Settings	IGMP Leave	Logue packs	t will be forwar	relation ICMD	autor ports								
Lite/Full	Packet Disable *	Leave packs	L WIII DE IOIWAR	ded to rowie i	outer ports.								
 O Lite version 						VLA	N Uplink Setti	ng					
 Full version 	Port 01	Port 02	Port 03	Port 04	Port 05	Port 06	Port 07	Port 08	Port 09	Port 10	Port 11	Port 12	Port 13
Logout	O Uplink1	Uplink1	Uplink1	O Uplink1	O Uplink1	O Uplink1	Uplink1	O Uplink1	Uplink1	O Uplink1	Uplink1	O Uplink1	Uplink
Logour	© Uplink2	Uplink2	O Uplink2	O Uplink2	O Uplink2	O Uplink2	O Uplink2	OUplink2	Uplink2	© Uplink2	O Uplink2	O Uplink2	Oplink
	Port 14	Port 15	Port 16	Port 17	Port 18	Port 19	Port 20	Port 21	Port 22	Port 23	Port 24	Port 25	Port 26
	Uplink1 Uplink2	Uplink1 Uplink2	Uplink1 Uplink2	Uplink1	Uplink1	Uplink1	Uplink1 Uplink2	Uplink1	Uplink1	 Uplink1 Uplink2 	Uplink1	Uplink1	Uplink
	opinikz	Opinikz	Opinikz	Opinikz	Opinikz		10 10 10 10 10 10 10 10 10 10 10 10 10 1	1 - REPARTS AND	Opinikz	Opinikz	Opinikz	opinikz	Opinik
							Clear Uplink1						
							Clear Uplink2						
							Update						

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

19.1 Output Queue Aging Time

Output Queue Aging Time

Aging time Disable ms
The output queue aging function allows the administrator to select the aging time of a packet stored in the output queue A packet stored in the output queue for a long time will lower the free packet buffer, resulting in the poor utilization of the buffer and the poor switch performance.

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.

Disable • ms will	he output queue a											
Disable • ms will												
Disable • ms will												
Disable • ms will		100			Output	Queue Aging	Time					
	e output queue aging function allows the administrator to select the aging time of a packet stored in the output queue. A packet stored in the output queue for a long tim Il lower the free packet buffer, resulting in the poor utilization of the buffer and the poor switch performance.											
					V	LAN Striding						
200		the strang.										
600 ding Wt	/hen this function	en this function is enabled, the switch will forward a uni-cast packet to the destination port. No matter whether the destination port is in the same VLAN group.										
800												
					IGMP	Snooping V1	1 V2					
IGMP Snooping	3MP Snooping V1	& V2 fu	inction enable									
Disable *	sin chooping vi	G V2 10	inction enable									
IGMP Leave Packet Disable *	eave packet will b	e forwar	ded to IGMP re	outer ports.								
					VLA	N Uplink Setti	ng					
OUplink1 O		plink1	Port 04	Port 05	Port 06 Uplink1	Port 07 Uplink1	Port 08 Ouplink1	Port 09 Oplink1	Port 10 Uplink1	Port 11 Ouplink1	Port 12 Uplink1	Port 13
OUplink2	Uplink2 0U	plink2	O Uplink2	Uplink2	© Uplink2	© Uplink2	O Uplink2	OUplink2	Uplink2	Oplink2	© Uplink2	© Uplin
		plink1	Port 17	Port 18 Uplink1	Port 19 Oplink1	Port 20 Uplink1	Port 21 Uplink1	Port 22 Uplink1	Port 23 Uplink1	Port 24	Port 25 OUplink1	Port 26 Uplin Uplin
OUplink1 0		plink2	O Uplink2	Uplink2	Uplink2	Uplink2						
© Uplink2	P	OUplink2 OU Port 15 Port OUplink1 OU	Ouplink2 Uplink2 Port 15 Port 16 Uplink1 Uplink1	Ouplink2 Ouplink2 Ouplink2 Ouplink2 Port 15 Port 16 Port 17 Ouplink1 Ouplink1 Ouplink1	Uplink2 Uplink2 Uplink2 Uplink2 Uplink2 Port 15 Port 16 Port 17 Port 18 Uplink1 Uplink1 Uplink1 Uplink1	Opplink2 Opplink2 Opplink2 Opplink2 Opplink2 Opplink2 Port 15 Port 16 Port 17 Port 18 Port 19 Opplink1 Opplink1 Opplink1 Opplink1 Opplink1	Oplink2 Oplink1 Oplink1 <t< td=""><td>Oplink2 Oplink2 Oplink1 <t< td=""><td>Oplink2 Oplink2 <t< td=""><td>Oplink2 Oplink2 <t< td=""><td>Oplink2 Oplink2 <t< td=""><td>Uplink2 Uplink2 <t< td=""></t<></td></t<></td></t<></td></t<></td></t<></td></t<>	Oplink2 Oplink1 Oplink1 <t< td=""><td>Oplink2 Oplink2 <t< td=""><td>Oplink2 Oplink2 <t< td=""><td>Oplink2 Oplink2 <t< td=""><td>Uplink2 Uplink2 <t< td=""></t<></td></t<></td></t<></td></t<></td></t<>	Oplink2 Oplink2 <t< td=""><td>Oplink2 Oplink2 <t< td=""><td>Oplink2 Oplink2 <t< td=""><td>Uplink2 Uplink2 <t< td=""></t<></td></t<></td></t<></td></t<>	Oplink2 Oplink2 <t< td=""><td>Oplink2 Oplink2 <t< td=""><td>Uplink2 Uplink2 <t< td=""></t<></td></t<></td></t<>	Oplink2 Oplink2 <t< td=""><td>Uplink2 Uplink2 <t< td=""></t<></td></t<>	Uplink2 Uplink2 <t< td=""></t<>

19.2 VLAN Striding

VLAN Striding

VLAN Striding Disable V When this function is enabled, the switch will forward a uni-cast packet to the destination port. No matter whether the destination port is in the same VLAN group.

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.

		ATUE III I		APSE IN IN IN										
Administrator PoE Port Management	Miscellaneous S	etting												
VLAN Setting VLAN Setting VLAN Setting VLAN Setting Social Setting Social Setting Social Setting Decomposition De	Aging time Disable • ms													
	VLAN Striding VLAN Striding When this function is enabled, the switch will forward a uni-cast packet to the destination port. No matter whether the destination port is in the same VLAN group													
	Catalon IGMP Snooping V1 & V2 IGMP Snooping V1 & V2 IGMP Snooping V1 & V2 Inction enable Deater *													
SNMP Settings	IGMP Leave Packet [Instite +] VLAN Uplink Setting													
C Lite version Full version Logout	Port 01 Ouplink1 Ouplink2	Port 02 Uplink1 Uplink2	Port 03 © Uplink1 © Uplink2	Port 04 Uplink1 Uplink2	Port 05 Uplink1 Uplink2	Port 06 Uplink1 Uplink2	Port 07 Uplink1 Uplink2	Port 08 Uplink1 Uplink2	Port 09 Uplink1 Uplink2	Port 10 Uplink1 Uplink2	Port 11 Uplink1 Uplink2	Port 12 Uplink1 Uplink2	Port 13 Uplink1 Uplink2	
	Port 14 OUplink1 Uplink2	Port 15 Uplink1 Uplink2	Port 16 © Uplink1 © Uplink2	Port 17 Uplink1 Uplink2	Port 18 Uplink1 Uplink2	Port 19 Uplink1 Uplink2	Port 20 O Uplink1 Uplink2	Port 21 © Uplink1 © Uplink2	Port 22 Uplink1 Uplink2	Port 23 O Uplink1 O Uplink2	Port 24 Ouplink1 Ouplink2	Port 25 O Uplink1 O Uplink2	Port 26 Uplink1 Uplink2	
	-						Clear Uplink1 Clear Uplink2							
							Update							

19.3 IGMP Snoop V1 & V2

	IGMP Snooping V1 & V2
IGMP Snooping Disable 💙	IGMP Snooping V1 & V2 function enable
IGMP Leave Packet Disable	Leave packet will be forwarded to IGMP router ports.

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.

Administrator	Miscellaneous S	etting											
PoE													
ort Management						Output	Queue Aging	Time					
AN Setting In Port Counter	Aging time Disable • mS	The output q will lower the	ueue aging fur free packet b	nction allows th uffer, resulting	e administrato in the poor util	r to select the zation of the b	aging time of a uffer and the p	packet stored oor switch perf	in the output q ormance.	ueue. A packet	stored in the o	output queue fo	r a long tim
curity						v	LAN Striding						
anning Tree	VLAN Striding Disable •	When this fu	nction is enabl	ed, the switch	will forward a	uni-cast packet	to the destinat	ion port. No m	atter whether t	he destination (port is in the sa	ime VLAN grou	ip.
DHCP Relay Agent Backup/Recovery Miscellaneous						IGMP	Snooping V1	& V2					
	IGMP Snooping												
IMP Settings teiFull	Packet Usable *	Leave packe	t will be forwar	ded to IGMP r	outer ports.								
Ute version						VLA	N Uplink Setti	ng					
 Full version gout 	Port 01 Uplink1 Uplink2	Port 02 Uplink1 Uplink2	Port 03 Uplink1 Uplink2	Port 04 Uplink1 Uplink2	Port 05 Uplink1 Uplink2	Port 06 Uplink1 Uplink2	Port 07 Uplink1 Uplink2	Port 08 Uplink1 Uplink2	Port 09 Uplink1 Uplink2	Port 10 Uplink1 Uplink2	Port 11 Uplink1 Uplink2	Port 12 Uplink1 Uplink2	Port 13 Uplink Uplink
	Port 14 © Uplink1 © Uplink2	Port 15 Uplink1 Uplink2	Port 16 Uplink1 Uplink2	Port 17 © Uplink1 © Uplink2	Port 18 Ouplink1 Ouplink2	Port 19 Uplink1 Uplink2	Port 20 Uplink1 Uplink2	Port 21 Uplink1 Uplink2	Port 22 © Uplink1 © Uplink2	Port 23 Uplink1 Uplink2	Port 24 © Uplink1 © Uplink2	Port 25 © Uplink1 © Uplink2	Port 26 Uplink Uplink
							Clear Uplink1 Clear Uplink2						
							Update						

Administrator	Miscellaneous S	etting											
PoE													
ort Management						Output	Queue Aging	Time					
VLAN Setting Per Port Counter Gos Setting Security	Aging time Disable • ms	Aging time The output queue aging function allows the administrator to select the aging time of a packet stored in the output queue. A packet stored in the output queue of a long time											
		VLAN Striding											
panning Tree unking	VLAN Striding Disable •	When this fu	nction is enabl	ed, the switch	will forward a u	ini-cast packet	to the destinat	tion port. No mi	atter whether ti	he destination (port is in the sa	me VLA <mark>N grou</mark>	ip.
DHCP Relay Agent Backup/Recovery Miscellaneous						IGMP	Snooping V1	& V2					
	IGMP Snooping Enable •	IGMP Snoop	ing V1 & V2 fu	inction enable									
NMP Settings Ite/Full	IGMP Leave Packet Disable •	Leave packe	eave packet will be forwarded to IGMP router ports.										
 Othe version 	Disable					VLA	N Uplink Setti	ng					
• Full version opout	Port 01 Uplink1 Uplink2	Port 02 Uplink1 Uplink2	Port 03 Uplink1 Uplink2	Port 04 Uplink1 Uplink2	Port 05 Uplink1 Uplink2	Port 06 Uplink1 Uplink2	Port 07 Uplink1 Uplink2	Port 08 Uplink1 Uplink2	Port 09 Uplink1 Uplink2	Port 10 Uplink1 Uplink2	Port 11 Uplink1 Uplink2	Port 12 Uplink1 Uplink2	Port 13 Uplink Uplink
	Port 14 © Uplink1 © Uplink2	Port 15 Uplink1 Uplink2	Port 16 Uplink1 Uplink2	Port 17 Uplink1 Uplink2	Port 18 Uplink1 Uplink2	Port 19 Uplink1 Uplink2	Port 20 Uplink1 Uplink2	Port 21 Uplink1 Uplink2	Port 22 Uplink1 Uplink2	Port 23 Uplink1 Uplink2	Port 24 Uplink1 Uplink2	Port 25 Uplink1 Uplink2	Port 26 Uplink Uplink
							Clear Uplink1 Clear Uplink2						
	-						Update						

19.4 VLAN Uplink

					VLAN	Jplink Se	tting					
Port 01 OUplink1 OUplink2	Port 02 Uplink1 Uplink2	Port 03 Uplink1 Uplink2	Port 04 O Uplink1 O Uplink2	Port 05 Uplink1 Uplink2	Ó	Port 07 O Uplink1 O Uplink2	Port 08 O Uplink1 O Uplink2	Port 09 O Uplink1 O Uplink2	Ó	Port 11 O Uplink1 O Uplink2	Port 12 O Uplink1 O Uplink2	Port 13 O Uplink1 O Uplink2
Port 14 OUplink1 OUplink2	Port 15 O Uplink1 O Uplink2	Port 16 O Uplink1 O Uplink2	0	Port 18 O Uplink1 O Uplink2	Ó	Port 20 Uplink1	Port 21 O Uplink1 O Uplink2	Ó	Ó	Port 24 O Uplink1 O Uplink2	Port 25 O Uplink1 O Uplink2	Port 26 Uplink1
						ear Uplin ear Uplin						

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

For example:

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

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

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

Administrator	Miscellaneous Setting	9											
PoE Port Management													
VLAN Setting			Output Queue Aging Time										
Per Port Counter © Go3 Setting	Aging time Disable V ms	The output qu buffer, resultin	It queue aging function allows the administrator to select the aging time of a packet stored in the output queue. A packet stored in the output queue for a long time will lower the free packet utiling in the poor utilization of the buffer and the poor switch performance.										
> security			VLAN Striding										
Spanning Tree	VLAN Striding Disable V	When this fun	is function is enabled, the switch will forward a uni-cast packet to the destination port. No matter whether the destination port is in the same VLAN group.										
Trunking DHCP Relay Agent		-	IGMP Snooping V1 & V2										
Backup/Recovery	IGMP Snooping Disable V	IGMP Snoopi	coping V1 & V2 function enable										
> Miscellaneous > SNMP Settings	IGMP Leave Packet	Leave packet	will be forwarded	to IGMP router p	iorts.								
/ Lite/Full						VLAN	Uplink Setting	G					
Clite version Generation Generation Logout	Port 01 O Uplink1 O Uplink2	Port 02 OUplink1 OUplink2	link1 OUplink1								Port 13 OUplink1 OUplink2		
	Port 14 OUplink1 OUplink2									Port 25 O Uplink1 O Uplink2	Port 26 OUplink1 OUplink2		
	- opmax	opinit	- Opining	- Opinia	- opinike	0	Clear Uplink1	- opining	oopiink	- opinic	o opining	o opinike	Copinite
						Sw	ritch Naming						
	Switch Name					the UDP and TC the IP Address of							
							JDP Alerts						
	UDP Alerts Disable V												
	Broadcast												
	UDP Client IP Address [255] [255] [255] [255]		able UDP alerts for Generic Events. ler IP Address of client machine, or select the "Broadcast" option.										
	UDP Port 55000												
						1	TCP Alerts						
	TCP Alerts Disable V												
	TCP Server IP Address 192. 168. 1	and announce	lerts for Generic		er it is listening o	0.							
	TCP Port 53001												
							Update						

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

VIGITRON				
Administrator PoE Port Management	SNMP Settings			
VLAN Setting		Community	Settings	
Per Port Counter QoS Setting	Community Name	ooninaniy (Access Right	
Security	public		Read Only •	
Spanning Tree			Read Only •	
Trunking		Update		
DHCP Relay Agent Backup/Recovery		SNMP Set		
Miscellaneous	System Descrition	SNMP Set	ungs	
SNMP Settings				
Lite/Full	System Contact			
 Lite version 	System Location			
 Full version Logout 		Update		
Logon		SNMP Trap S	lettings	
	Trap State	Enable •		
	Enable Trap Server	Disable •		
	Trap Server Address			
	Trap Server Status			
		Refresh U	padte	

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

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.

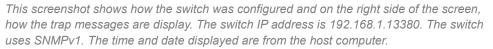
istrator					
trator	SNMP Settings				
lanagement					
Setting			Community Settings		
Counter	Community Name			Access Right	
ting	public			Read Only *	
r 1g Tree				Read Only Read/Wite	
ng				Readivitie	
Relay Agent			Update		
Recovery			SNMP Settings		
llaneous	System Descrition				
9 Settings	System Contact				
	System Location				
Lite version Eul version	System Location				
ut			Update		
			SNMP Trap Settings		
	Trap State	Enable •			
	Enable Trap Server	Disable *			
	Trap Server Address				
	Trap Server Status	-			
			Refresh Upadte		

VIGITRON				
Administrator PoE Port Management	SNMP Settings			
VLAN Setting			Community Settings	
Per Port Counter QoS Setting	Community Name			Access Right
Security	public			Read Only ·
Spanning Tree				Read Only *
Trunking			Update	
DHCP Relay Agent Backup/Recovery			01000 0-000-00	
Miscellaneous			SNMP Settings	
SNMP Settings	System Descrition			
Lite/Full	System Contact			
Lite version	System Location			
Full version			Update	
Logout			SNMP Trap Settings	
	Trap State	Enable *		
	Enable Trap Server	Disable Enable		
	Trap Server Address	Linue		
	Trap Server Status			
			Refresh Upadte	

	Binned Street Street			
> Administrator > PoE	SNMP Settings			
Port Management				
VLAN Setting Per Port Counter			Community Settings	
QoS Setting	Community Name			Access Right
Security	public			Read Only
Spanning Tree				Read Only *
Trunking			Update	
DHCP Relay Agent				
Backup/Recovery			SNMP Settings	
Miscellaneous SNMP Settings	System Descrition			
V Lite/Full	System Contact			
 Lite version 	System Location			
• Full version			Update	
Logout			Openne	
			SNMP Trap Settings	
	Trap State	Enable •		
	Enable Trap Server	Disable *		
	Trap Server Address	Disable		
	Trap Server Status			
			Refresh Upadte	
			Contract Capital Contract	

19.7 SNMP Trap States

	Tenning I I I I I I I I I I I I I I I I I I I			Ÿ	\$ 0	1	© 10:58:06 © 10:57:59	Date 7/28/2017	Source 192.168.2.213 192.168.2.213 192.168.2.213 Local	Description Link Up physical port 21 Link Up physical port 23 Celd Start ColdStart Trave Watcher Startet - Listening on UDP port 162.
Administrator PoE Port Management	SNMP Settings									
VLAN Setting		Community Settings								
 Per Port Counter GoS Setting 	Community Name		Access Right							
 Security 	public		Read Only *							
Spanning Tree			Read Only *							
Trunking DHCP Relay Agent		Update								
Backup/Recovery		SNMP Settings					0000 30	6E 02 01	00 04 06 7	0 75 62 6C 69 63 A4 61 06 0n
Miscellaneous SNMP Settings	System Description	F30126V1.00					0020 02 0030 06	01 03 02 0A 2B 06	01 03 43 0	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
Logout	System Contact	Vigitron					0040 1E 0050 68 0060 0F	06 0A 2E 79 73 69 06 0A 2E	06 01 02 0 63 61 6C 2 06 01 02 0	1 02 02 01 02 15 04 10 70 + p 0 70 6F 72 74 20 32 31 30 hysical port 210 1 02 02 01 03 15 02 01 06 +
S. STREET	System Location	Vigitron						noth: 112		
		Update					Communit	y: public 3 6 1 4 1	30970.3	
		SNMP Trap Settings					sysUpTin Generic	192.168 e: 0 days 3 - Link	2 213 . 00 00 07 . 0p	
	Trap State	Enable *					Specific OID: 1	36121	2.2.1.1.21 r32 0x02 (2	
	Enable Trap Server	Disable *								
	Trap Server Address								2 2 1 2 21 String 0x04 ort 21 2 2 1 3 21	
-	Trap Server Status	2 I					ASN1 Typ Value: 6	e: Intege	r32 0x02 (2	1
		Refresh Update								
								1.2		137149



SNMP will deliver the following messages:

"PoE_On Port xx"

"PoE_Off Port xx"

"SecurPort: TxRx Disabled Port xx"

"E0: Port Overload (ICUT) Event on Port xx"

"E1: Port Short Circuit Limit (ILIM) Event on Port xx"

"E3: Port Severe Short Circuit Event on Port xx"

"E4: Port Thermal Shutdown Event on Port xx"

"E5: Port Temperature Limit Event on Port xx"

"E6: Main Power Overload Event on Port xx"

"E7: PoE Auto Check Timeout Event on Port xx"

"Power Budget: Budget Exceeded, disabled Port xx"

"PSE Overload Protection: Disabled Port xx"

"Traffic Detected Port xx" (Exception: Vi30126, Vi35126)

"Loss of Traffic Detected Port xx" (Exception: Vi30126, Vi35126)

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

"Cold Start: This message is sent when the PoE Switch is powered up." "Warm Start: This message is sent when the PoE Switch is rebooted form the GUI."

Section 20: Log Out

20.0 Log Out Procedure

192.168.1.133/logout.htm ×		± - D
→ C ③ 192.168.1.133/logout.htm		x 💠 🏲
	Logout?	

Select: Accept to logout

Back: Returns to the previous page

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

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

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

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

Section 21: Glossary

A

ACE

ACE is an acronym for Access Control Entry. It describes the access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed and different parameter options that are available for individual application.

ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

For example, the ACL implementations can be quite complex when the ACEs are prioritized for the various situations. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic and in this context, they are similar to firewalls.

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

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

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

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

AES

AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

APS

APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation

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

ARP

ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-

Negotiation

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

С

СС

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.

ССМ	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 is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

Ε

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.

Η

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 sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is 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.

М

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.

Μ	V	R
		••

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).

Ν

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.

0	
ουι	
	OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.
Option 82	
	Option 82 provides information about the DHCP client network location. The DHCP server than uses this information to implement the IP address and other client information. Option 82 supports RFC 3046 which is the DHCP Relay Agent Information Option. Its use helps in protection the spoofing (forging) of IP and MAC addresses.
Ρ	
РСР	
	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.
ΡοΕ	
	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	N
	In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.
РТР	
	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	Vi30126, Vi31026, Vi31126, Vi32026, Vi32126, Vi35126	Vi3010 / Vi3026	Compatible
		SFP port 25-26	Setting	Result
VI00850MM-H	1G	Fixed 1G	Auto	Yes
V1008501VIIVI-H		Fixed 1G	Fixed 1G	Yes
VI01310MM-H	100 MB	Fixed 1G	Auto	No
		Fixed 1G	Fixed 1G	No
VI01310 SM-H	1G	Fixed 1G	Auto	Yes
		Fixed 1G	Fixed 1G	Yes

	Bandwidth	Vi30126, Vi31026, Vi31126, Vi32026, Vi32126, Vi35126	Vi5001	Compatible
		SFP port 25-26	Setting	Result
VI00850MM-H	1G	Fixed 1G	Fixed 100MB	No
VI01310MM-H	100 MB	Fixed 1G	Fixed 100MB	No
VI01310SM-H	1G	Fixed 1G	Fixed 100MB	No

	Bandwidth	Vi30126, Vi31026, Vi31126, Vi32026, Vi32126, Vi35126	Vi50001	Compatible
		SFP port 25-26	Setting	Result
Vi00850MM-H	1G	Fixed 1G	Fixed 1G	Yes
Vi01310MM-H	100 MB	Fixed 1G	Fixed 1G	Yes
Vi01310SM-H	1G	Fixed 1G	Fixed 1G	Yes

	Bandwidth	Vi30126, Vi31026, Vi31126, Vi32026, Vi32126, Vi35126	Vi3005	Compatible
		SFP port 25-26	Setting	Result
Vi00850 MM-H	1G	Fixed 1G	Fixed 100MB	No
Vi01310MM-H	100 MB	Fixed 1G	Fixed 100MB	No
Vi01310SM-H	1G	Fixed 1G	Fixed 100MB	No

	Bandwidth	Vi30126, Vi31026, Vi31126, Vi32026, Vi32126, Vi35126	Vi30005	Compatible
		SFP port 25-26	Setting	Result
Vi00850MM-H	1G	Fixed 1G	Fixed 1G	Yes
Vi01310MM-H	100 MB	Fixed 1G	Fixed 1G	Yes
VI01310SM-H	1G	Fixed 1G	Fixed 1G	Yes

	Bandwidth	VI35126	Vi3010/Vi3026	Compatible
	Banuwiuth	SFP port 1-16	Setting	Result
VI00850MM-H	1G	Fixed 100MB	Auto	Yes
V1008501VIIVI-H		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	
	Banuwiuth	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	
	Bandwidth	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
	Danuwiuth	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
	Banuwiuth	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 Vi30126

When connecting the Vi30126 to other model Switches, it is necessary to add a Tag to the gigabit port to get the Switches to communicate.

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

Note: port 25

Administrator	VLAN Mode							
POE								
Port Management		1				-]	
	VLAN Mode			Tag Based VLAN	Change VLAN mod	e		
/LAN Setting	VLAN Tag Mode			Tag/Untag I	base on Port 🔻			
VLAN mode		Port 01		Port 03	Port 04	Port 05	Port 06	
 VLAN Member 		Add Tag						
 Multi to 1 Setting 		Don't Care						
Non-Association Port		Remove Tag						
Setting		Port 07	Port 08	Port 09	Port 10	Port 11	Port 12	
Per Port Counter		Add Tag	O Add Tag					
Do S Setting		Don't Care						
Security	AddTag Type	Remove Tag						
	(Add VLAN Tag to	Port 13	Port 14	Port 15	Port 16	Port 17	Port 18	
spanning Tree	output frames	Add Tag						
runking	according to the pvid of	Don't Care Remove Tag						
HCP Relay Agent	selected port)	Port 19	Port 20	Port 21	Port 22	Port 23	Port 24	
Backup/Recovery		Add Tag						
		Don't Care						
liscellaneous		Remove Tag						
NMP Settings		Port 25	Port 26		- risilore hug	- risinore lug	- remove lug	
.ite/Full		Add Tag	Add Tag					
		Opn't Care	Don't Care					
Lite version		Remove Tag	Remove Tag					
				1				

Contact Information

Vigitron, Inc.

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