

VIPA Networking Solutions

PNS | 911-2PNx0 | Manual

HB165 | PNS | 911-2PNx0 | en | 19-28

PROFINET Switches PN5-RD/PN8-RD



VIPA GmbH
Ohmstr. 4
91074 Herzogenaurach
Telephone: +49 9132 744-0
Fax: +49 9132 744-1864
Email: info@vipa.com
Internet: www.vipa.com

Table of contents

1	General	6
	1.1 Copyright © VIPA GmbH	6
	1.2 About this manual.....	7
	1.3 Safety information.....	8
2	Hardware Installation	9
	2.1 Panel Layout.....	9
	2.2 Mounting Dimensions.....	10
	2.3 DIN-Rail Mounting.....	11
	2.4 Wall Mounting (optional).....	11
	2.5 ATEX Information.....	12
	2.6 Wiring Requirements.....	13
	2.7 Grounding the Switch.....	13
	2.8 Wiring the Relay Contact.....	13
	2.9 Wiring the Redundant Power Inputs.....	14
	2.10 Communication Connections.....	14
	2.10.1 10/100BaseT(X) Ethernet Port Connection.....	14
	2.11 Redundant Power Inputs.....	15
	2.12 Relay Contact.....	16
	2.13 Turbo Ring DIP Switch Settings.....	16
	2.14 LED Indicators.....	18
	2.15 Auto MDI/MDI-X Connection.....	18
	2.16 Specifications.....	19
3	Getting Started	21
	3.1 Serial Console Configuration (115200, None, 8, 1, VT100).....	21
	3.2 Configuration by Telnet Console.....	25
	3.3 Configuration by Web Browser.....	27
	3.4 Disabling Telnet and Browser Access.....	29
4	Featured Functions	30
	4.1 Configuring Basic Settings.....	30
	4.1.1 System Identification.....	31
	4.1.2 Password.....	32
	4.1.3 Accessible IP List.....	33
	4.1.4 Port Settings.....	34
	4.1.5 Network Parameters.....	36
	4.1.6 GARP Timer Parameters.....	39
	4.1.7 System Time Settings.....	40
	4.1.8 Turbo Ring DIP Switch.....	42
	4.1.9 System File Update.....	43
	4.1.10 ABC (Auto-Backup Configurator) Configuration.....	45
	4.1.11 Restart.....	45
	4.1.12 Reset to Factory Default.....	46
	4.2 Loop Protection.....	46
	4.3 Configuring SNMP.....	46
	4.3.1 SNMP Read/Write Settings.....	48
	4.3.2 Trap Settings.....	49
	4.3.3 Private MIB Information.....	50
	4.4 Using Traffic Prioritization.....	50

4.4.1	The Traffic Prioritization Concept.....	51
4.4.2	Configuring Traffic Prioritization.....	53
4.5	Using Virtual LAN.....	56
4.5.1	The Virtual LAN (VLAN) Concept.....	56
4.5.2	Sample Applications of VLANs Using VIPA switches.....	58
4.5.3	VLAN Settings.....	59
4.5.4	VLAN Table.....	61
4.6	Using Multicast Filtering.....	62
4.6.1	The Concept of Multicast Filtering.....	62
4.6.2	Configuring IGMP Snooping.....	66
4.6.3	Static Multicast MAC Addresses.....	69
4.6.4	Configuring GMRP.....	69
4.6.5	GMRP Table.....	70
4.7	Using Bandwidth Management.....	71
4.7.1	Configuring Bandwidth Management.....	71
4.8	Using Auto Warning.....	74
4.8.1	Configuring Email Warning.....	75
4.8.2	Configuring Relay Warning.....	78
4.9	Using Line-Swap-Fast-Recovery.....	80
4.9.1	Configuring Line-Swap Fast Recovery.....	80
4.10	Using Set Device IP.....	80
4.10.1	Configuring Set Device IP.....	82
4.10.2	Configuring DHCP Relay Agent.....	82
4.11	Using Diagnosis.....	84
4.11.1	Mirror Port.....	85
4.11.2	Ping.....	85
4.11.3	LLDP Function.....	86
4.12	Using Monitor.....	87
4.12.1	Monitor by Switch.....	87
4.12.2	Monitor by Port.....	88
4.13	Using the MAC Address Table.....	88
4.14	Using Event Log.....	89
4.15	Using Syslog.....	90
5	Communication Redundancy.....	92
5.1	Introduction to Communication Redundancy.....	92
5.2	Turbo Ring.....	93
5.2.1	The Turbo Ring Concept.....	93
5.2.2	Setting up Turbo Ring or Turbo Ring V2.....	94
5.2.3	Configuring Turbo Ring and Turbo Ring V2.....	101
5.3	Turbo Chain.....	108
5.3.1	The Turbo Chain Concept.....	108
5.3.2	Setting Up Turbo Chain.....	109
5.3.3	Configuring Turbo Chain.....	110
5.4	STP/RSTP/MSTP.....	112
5.4.1	The STP/RSTP/MSTP Concept.....	112
5.4.2	STP Example.....	116
5.4.3	Using STP on a Network with Multiple VLANs.....	116
5.4.4	Configuring STP/RSTP.....	117
5.4.5	Configuration Limits of STP/RSTP.....	119

6	Industrial Protocols	121
	6.1 MODBUS/TCP MAP.....	121
	6.1.1 Introduction.....	121
	6.1.2 Data Format and Function Code.....	121
	6.1.3 Configuring MODBUS/TCP on VIPA Switches.....	121
	6.1.4 MODBUS Data Map and Information Interpretation of VIPA Switches.....	122
	6.2 EtherNet/IP.....	131
	6.3 PROFINET I/O.....	132
	6.3.1 Introduction.....	132
	6.3.2 PROFINET Environmental Introductions.....	132
	6.3.3 Configuring PROFINET I/O on VIPA Switches.....	134
	6.3.4 Addressing of I/O Data in PROFINET I/O Based on Slot and Sub-Slots..	134
	6.3.5 PROFINET Attributes.....	135
	6.3.6 Siemens STEP®7 Integration.....	140
	6.3.7 Monitoring the Switch.....	158
	Appendix	166
	A Command Line Interface.....	167

1 General

1.1 Copyright © VIPA GmbH

All Rights Reserved

This document contains proprietary information of VIPA and is not to be disclosed or used except in accordance with applicable agreements.

This material is protected by the copyright laws. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to VIPA), except in accordance with applicable agreements, contracts or licensing, without the express written consent of VIPA and the business management owner of the material.

For permission to reproduce or distribute, please contact: VIPA, Gesellschaft für Visualisierung und Prozessautomatisierung mbH Ohmstraße 4, D-91074 Herzogenaurach, Germany

Tel.: +49 9132 744 -0

Fax.: +49 9132 744-1864

E-Mail: info@vipa.de

<http://www.vipa.com>



Every effort has been made to ensure that the information contained in this document was complete and accurate at the time of publishing. Nevertheless, the authors retain the right to modify the information.

This customer document describes all the hardware units and functions known at the present time. Descriptions may be included for units which are not present at the customer site. The exact scope of delivery is described in the respective purchase contract.

EC Conformity Declaration

Hereby, VIPA GmbH declares that the products and systems are in compliance with the essential requirements and other relevant provisions. Conformity is indicated by the CE marking affixed to the product.

Conformity Information

For more information regarding CE marking and Declaration of Conformity (DoC), please contact your local VIPA customer service organization.

Trademarks

VIPA, SLIO, System 100V, System 200V, System 300V, System 300S, System 400V, System 500S and Commander Compact are registered trademarks of VIPA Gesellschaft für Visualisierung und Prozessautomatisierung mbH.

SPEED7 is a registered trademark of profichip GmbH.

SIMATIC, STEP, SINEC, TIA Portal, S7-300, S7-400 and S7-1500 are registered trademarks of Siemens AG.

Microsoft and Windows are registered trademarks of Microsoft Inc., USA.

Portable Document Format (PDF) and Postscript are registered trademarks of Adobe Systems, Inc.

All other trademarks, logos and service or product marks specified herein are owned by their respective companies.

Information product support Contact your local VIPA Customer Service Organization representative if you wish to report errors or questions regarding the contents of this document. If you are unable to locate a customer service centre, contact VIPA as follows:

VIPA GmbH, Ohmstraße 4, 91074 Herzogenaurach, Germany

Telefax: +49 9132 744-1204

E-Mail: documentation@vipa.de

Technical support Contact your local VIPA Customer Service Organization representative if you encounter problems with the product or have questions regarding the product. If you are unable to locate a customer service centre, contact VIPA as follows:

VIPA GmbH, Ohmstraße 4, 91074 Herzogenaurach, Germany

Tel.: +49 9132 744-1150 (Hotline)

E-Mail: support@vipa.de

1.2 About this manual

Objective and contents This manual describes the Teleservice module 911-2PNx0 from VIPA. It contains a description of the structure, project engineering and deployment.

Product	Order number	as of state:	
		HW	FW
PN5-RD/PN8-RD	911-2PNx0	01	V3.5.4

Target audience The manual is targeted at users who have a background in automation technology.

Structure of the manual The manual consists of chapters. Every chapter provides a self-contained description of a specific topic.

Guide to the document The following guides are available in the manual:

- An overall table of contents at the beginning of the manual
- References with page numbers

Availability The manual is available in:

- printed form, on paper
- in electronic form as PDF-file (Adobe Acrobat Reader)

Icons Headings Important passages in the text are highlighted by following icons and headings:



DANGER!

Immediate or likely danger. Personal injury is possible.

**CAUTION!**

Damages to property is likely if these warnings are not heeded.



Supplementary information and useful tips.

1.3 Safety information

Applications conforming with specifications

The Teleservice module is constructed and produced for:

- communication and process control
- industrial applications
- operation within the environmental conditions specified in the technical data
- installation into a cubicle

**DANGER!**

This device is not certified for applications in

- in explosive environments (EX-zone)

Documentation

The manual must be available to all personnel in the

- project design department
- installation department
- commissioning
- operation

**CAUTION!**

The following conditions must be met before using or commissioning the components described in this manual:

- Hardware modifications to the process control system should only be carried out when the system has been disconnected from power!
- Installation and hardware modifications only by properly trained personnel.
- The national rules and regulations of the respective country must be satisfied (installation, safety, EMC ...)

Disposal

National rules and regulations apply to the disposal of the unit!

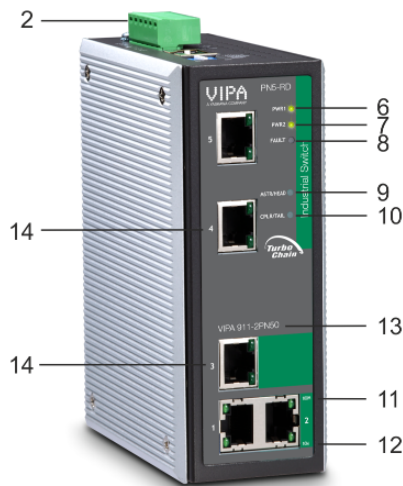
2 Hardware Installation

Overview

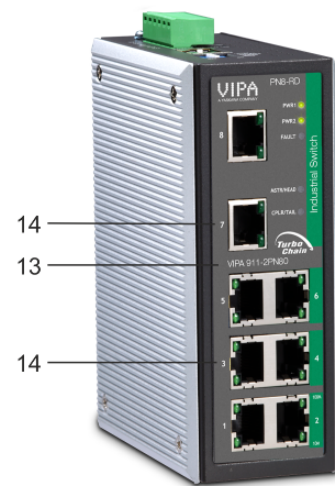
The VIPA Switch PN5-RD/PN8-RD series, which includes both 5- and 8-port smart Ethernet switches, is a cost-effective solution for your Ethernet connections. In addition, the built-in smart alarm function helps system maintainers monitor the health of your Ethernet network.

2.1 Panel Layout

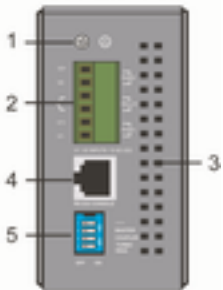
PN5-RD
Front Panel View



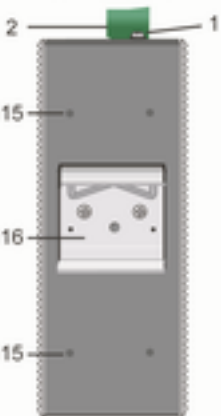
PN8-RD
Front Panel View



Top Panel View

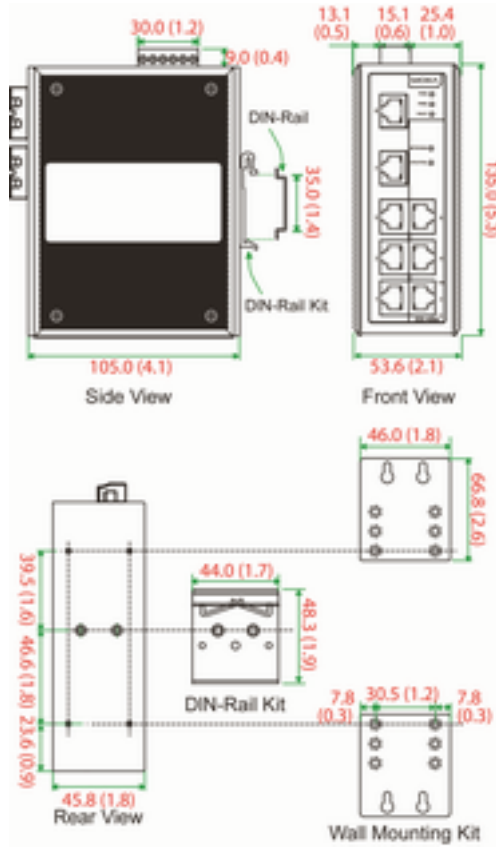


Rear Panel View



- 1 Grounding screw
- 2 Terminal block for power input PWR1/PWR2 and relay output
- 3 Heat dissipation vents
- 4 Console port
- 5 DIP switches
- 6 Power input PWR1 LED
- 7 Power input PWR2 LED
- 8 Fault LED
- 9 MSTR/HEAD: LED indicator
- 10 CPLR/TAIL: LED indicator
- 11 TP port's 100 Mbps LED
- 12 TP port's 10 Mbps LED
- 13 Model Name
- 14 10/100BaseT(X) ports
- 15 Screw hole for wall mounting kit
- 16 DIN-Rail kit

2.2 Mounting Dimensions

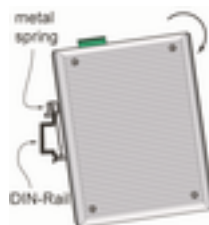


Unit = mm (inch)

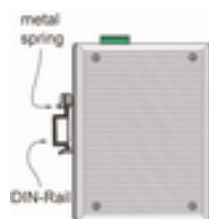
2.3 DIN-Rail Mounting

The aluminum DIN-Rail attachment plate should already be fixed to the back panel of the Switch PN5-RD/PN8-RD when you take it out of the box. If you need to reattach the DIN-Rail attachment plate, make sure the stiff metal spring is situated towards the top, as shown in the following figures.

1. ➤ Insert the top of the DIN-Rail into the slot just below the stiff metal spring.



2. ➤ The DIN-Rail attachment unit will snap into place as shown.

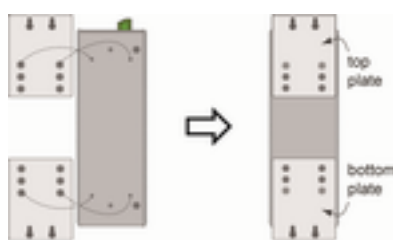


To remove the VIPA Switch from the DIN-Rail, simply reverse Steps 1 and 2.

2.4 Wall Mounting (optional)

For some applications, you will find it convenient to mount the Switch on the wall, as shown in the following figures.

1. ➤ Remove the aluminum DIN-Rail attachment plate from the Switch's rear panel, and then attach the wall mount plates with M3 screws, as shown in the diagram at the right.



2. → Mounting the Switch on the wall requires 4 screws. Use the switch, with wall mount plates attached, as a guide to mark the correct locations of the 4 screws. The heads of the screws should be less than 6.0 mm in diameter, and the shafts should be less than 3.5 mm in diameter, as shown in the figure at the right.



⇒



Before tightening the screws into the wall, make sure the screw head and shank size are suitable by inserting the screw into one of the keyhole-shaped apertures of the wall mounting plates.

Do not screw the screws in completely—leave about 2 mm to allow room for sliding the wall mount panel between the wall and the screws.

3. → Once the screws are fixed in the wall, insert the four screw heads through the large parts of the keyhole-shaped apertures, and then slide the Switch downwards, as indicated. Tighten the four screws for added stability.

2.5 ATEX Information

- Certificate number: DEMKO 08 ATEX 0712961X
- Ambient range ($-40^{\circ}\text{C} \leq T_{\text{amb}} \leq 75^{\circ}\text{C}$)
- Certification string:
 - PN5-RD: EX nA nC IIC T4 Gc
 - PN8-RD: EX nA nC op is IIC T4 Gc
- Standards covered (EN 60079-0:2012, EN 60079-15:2010)
- The conditions of safe usage:
 - These products must be mounted in an IP54 enclosure.
 - Install in an area of pollution degree 2 or less.
 - Use a conductor wire of size 0.2 mm² or greater.
 - Provisions should be made, external to the apparatus, to prevent the rated voltage from being exceeded by transient disturbances of more than 40%.

2.6 Wiring Requirements



WARNING! Safety First!

Be sure to disconnect the power cord before installing and/or wiring your VIPA Switch. Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

Be sure to read and follow these important guidelines:

- Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
- Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
- Use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together.
- Keep input wiring and output wiring separate.
- When necessary, you should label the wiring to all devices in the system.

2.7 Grounding the Switch

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices.

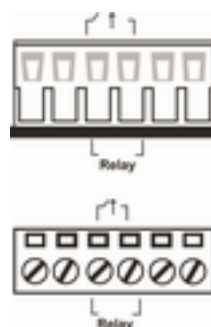


CAUTION!

This product is intended to be mounted to a well-grounded mounting surface, such as a metal panel.

2.8 Wiring the Relay Contact

The Relay Contact consists of the two middle contacts of the terminal block on the PN5-RD/PN8-RD's top panel. Refer to the next section for detailed instructions on how to connect the wires to the terminal block connector and how to attach the terminal block connector to the terminal block receptor. In this section, we explain the meaning of the two contacts used to connect the Alarm Contact.



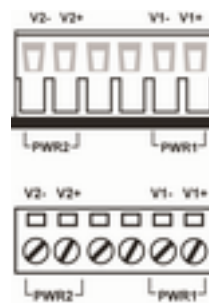
Fault: The two middle contacts of the 6-contact terminal block connector are used to detect both power faults and port faults. The two wires attached to the fault contacts form an open circuit when:

- a relay warning event is triggered.
- the PN5-RD/PN8-RD is the Master of this Turbo Ring and the Turbo Ring is broken.
- there is a start-up failure.

If none of these three conditions is satisfied, the fault circuit will remain closed.

2.9 Wiring the Redundant Power Inputs

The top two contacts and the bottom two contacts of the 6-contact terminal block connector on the PN5-RD/PN8-RD's top panel are used for the PN5-RD/PN8-RD's two DC inputs. Top and front views of one of the terminal block connectors are shown in the following figures:



1. ➤ Insert the negative/positive DC wires into the V-/V+ terminals, respectively.
2. ➤ To keep the DC wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.
3. ➤ Insert the plastic terminal block connector prongs into the terminal block receptor, which is located on the Switch's top panel.



CAUTION!

Before connecting the PN5-RD/PN8-RD to the DC power inputs, make sure the DC power source voltage is stable.

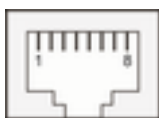
2.10 Communication Connections

PN8-RD models have 5, 6 or 8 10/100BaseT(X) Ethernet ports. PN5-RD models have 3 or 5 10/100BaseT(X) Ethernet ports.

2.10.1 10/100BaseT(X) Ethernet Port Connection

The 10/100BaseT(X) ports located on the Switch's front panel are used to connect to Ethernet-enabled devices. Next, we show pinouts for both MDI (NIC-type) ports and MDI-X (HUB/Switch-type) ports and also show cable wiring diagrams for straight-through and cross-over Ethernet cables.

10/100Base T(x) RJ45 Pin-outs



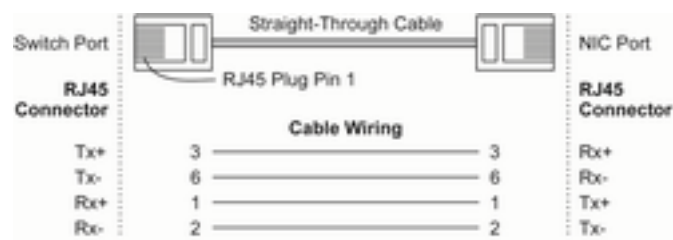
MDI Port Pinouts

Pin	Signal
1	Tx+
2	Tx-
3	Rx+
6	Rx-

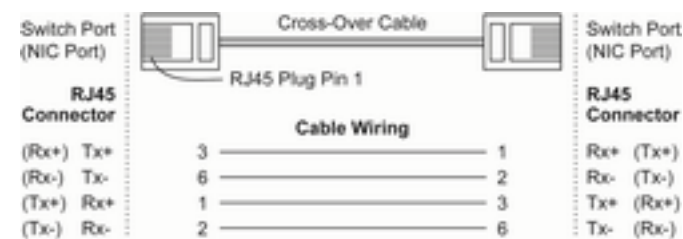
MDI-X Port Pinouts

Pin	Signal
1	Rx+
2	Rx-
3	Tx+
6	Tx-

RJ45 (8-pin) to RJ45 (8-pin) Straight-Through Cable Wiring



RJ45 (8-pin) to RJ45 (8-pin) Cross-Over Cable Wiring



2.11 Redundant Power Inputs

Both power inputs can be connected simultaneously to live DC power sources. If one power source fails, the other live source acts as a backup and automatically supplies the PN5-RD/PN8-RD with power.

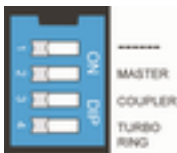
2.12 Relay Contact

The VIPA Switch has one relay contact located on the top panel. For detailed instructions on how to connect the relay contact power wires to the two middle contacts of the 6-contact terminal block connector. [Chap. 2.8 'Wiring the Relay Contact' page 13](#) A typical scenario would be to connect the fault circuit to a warning light located in the control room. The light can be set up to switch on when a fault is detected. The relay contact has two terminals that form a fault circuit for connecting to an alarm system. The two wires attached to the fault contacts form an open circuit when (1) a relay warning event is triggered, (2) the PN5-RD/PN8-RD is the Master of this Turbo Ring, and the Turbo Ring is broken, or (3) there is a start-up failure. If none of these three conditions occur, the fault circuit will be closed.

2.13 Turbo Ring DIP Switch Settings

PN5-RD/PN8-RD series switches are plug-and-play managed redundant Ethernet switches. The proprietary Turbo Ring protocol was developed by VIPA to provide better network reliability and faster recovery time. VIPA Turbo Ring's recovery time is less than 300 ms (*Turbo Ring*) or 20 ms (*Turbo Ring V2*)-compared to a 3 to 5-minute recovery time for commercial switches-decreasing the possible loss caused by network failures in an industrial setting. There are 4 Hardware DIP Switches for Turbo Ring on the top panel of the PN5-RD/PN8-RD that can be used to set up the Turbo Ring easily within seconds. If you do not want to use a hardware DIP switch to set up Turbo Ring, you can use a web browser, Telnet or console to disable this function. [Chap. 5 'Communication Redundancy' page 92](#)

PN5-RD/PN8-RD Series DIP Switches



The default setting for each DIP Switch is OFF. The following table explains the effect of setting the DIP Switch to the ON position.

Turbo Ring DIP Switch Settings

DIP 1	DIP 2	DIP 3	DIP 4
Reserved for future use.	ON: Enables this Switch as the Ring Master.	ON: Enables the default Ring Coupling ports.	ON: Activates DIP switches 1, 2, 3 to configure Turbo Ring settings.
	OFF: This Switch will not be the Ring Master.	OFF: Do not use this as the ring coupler.	OFF: DIP switches 1, 2, 3 will be disabled.

Turbo Ring V2 DIP Switch Settings

DIP 1	DIP 2	DIP 3	DIP 4
ON: Enables the default Ring Coupling (backup) port.	ON: Enables this Switch as the Ring Master.	ON: Enables the default Ring Coupling port.	ON: Activates DIP switches 1, 2, 3 to configure Turbo Ring V2 settings.
OFF: Enables the default Ring Coupling (primary) port.	OFF: This Switch will not be the Ring Master.	OFF: Do not use this Switch as a ring coupler.	OFF: DIP switches 1, 2, 3 will be disabled.










If you do not enable any of the PN5-RD/PN8-RD switches to be the Ring Master, the Turbo Ring protocol will automatically choose the PN5-RD/PN8-RD with the smallest MAC address range to be the Ring Master. If you accidentally enable more than one PN5-RD/PN8-RD to be the Ring Master, these PN5-RD/PN8-RD switches will auto-negotiate to determine which switch will be the Ring Master.



To switch on the Master or Coupler functions of the DIP switch, you need to enable the Turbo Ring Pole first.

2.14 LED Indicators

LED	Color	State	Description
PWR1	 orange	On	Power is being supplied to power input PWR1.
		Off	Power is not being supplied to power input PWR1.
PWR2	 orange	On	Power is being supplied to power input PWR2.
		Off	Power is not being supplied to power input PWR2.
FAULT	 red	On	When (1) a relay warning event is triggered, (2) the Switch is the Master of this Turbo Ring, and the Turbo Ring is broken, or (3) start-up failure.
		Off	When a relay warning event is not triggered.
MSTR/ HEAD	 green	On	When the PN5-RD/PN8-RD is set as the Master of the Turbo Ring, or as the Head of the Turbo Chain.
		Blinking	The PN5-RD/PN8-RD has become the Ring Master of the Turbo Ring, or the Head of the Turbo Chain, after the Turbo Ring or the Turbo Chain is down.
		Off	When the PN5-RD/PN8-RD is not the Master of this Turbo Ring or is set as the Member of the Turbo Chain.
CPLR/TAI L	 green	On	When the PN5-RD/PN8-RD coupling function is enabled to form a back-up path, or when it's set as the Tail of the Turbo Chain.
		Blinking	When the Turbo Chain is down.
		Off	When the PN5-RD/PN8-RD disables the coupling function, or is set as the Member of the Turbo Chain.
10M (TP)	 green	On	TP port's 10 Mbps link is active.
		Blinking	Data is being transmitted at 10 Mbps.
		Off	TP Port's 10 Mbps link is inactive.
100M (TP)	 green	On	TP port's 100 Mbps link is active.
		Blinking	Data is being transmitted at 100 Mbps.
		Off	TP Port's 100 Mbps link is inactive.

2.15 Auto MDI/MDI-X Connection

The Auto MDI/MDI-X function allows users to connect the PN5-RD/PN8-RD's 10/100BaseTX ports to any kind of Ethernet device, without needing to pay attention to the type of Ethernet cable being used for the connection. This means that you can use either a straight-through cable or cross-over cable to connect the PN5-RD/PN8-RD to Ethernet devices.

2.16 Specifications

Technology		
Standards	IEEE802.3, 802.3u, 802.3x, 802.1D, 802.1Q, 802.1w, 802.1p	
Protocols	IGMP V1/V2 device, GMRP, GVRP, SNMPv1/v2c/v3, DHCP Server/Client, TFTP, SNTP, SMTP, RARP, RMON, HTTP, Telnet, Syslog, DHCP Option 66/67/82, BootP, LLDP, Modbus TCP, IPv6	
MIB	MIB-II, Ethernet-Like MIB, P-BRIDGE MIB, RMON MIB Group 1, 2, 3, 9, Bridge MIB, RSTP MIB	
Forwarding and Filtering Rate	148810 pps	
Processing Type	Store and Forward	
Flow Control	IEEE802.3x flow control, back pressure flow control	
Interface		
RJ45 Ports	10/100BaseT(X) auto negotiation speed, F/H duplex mode, and auto MDI/MDI-X connection	
Console	RS232 (RJ45)	
LED Indicators	PWR1, PWR2, FAULT, 10/100M (TP port), 100M (Fiber Port), CPLR/TAIL and MSTR/HEAD	
Relay Contact	One relay output with current carrying capacity of 1A @ 24 VDC	
DIP Switches	Master, Coupler, Turbo Ring, Reserve	
Optical Fiber		
	Multi-mode	Single-mode
Wavelength	1300 nm	1310 nm
Max. Tx	-10 dBm	0 dBm
Min. Tx	-20 dBm	-5 dBm
Rx Sensitivity	-32 dBm	-34 dBm
Link Budget	12 dB	29 dB
Typical Distance	5 km ^a , 4 km ^b	40 km ^c
Saturation	-6 dBm	-3 dBm
a. when using [50/125 μm, 800 MHz*km] cable		
b. when using [62.5/125 μm, 500 MHz*km] cable		
c. when using [9/125 μm, 3.5 PS/(nm*km)] cable		
Power		
Input Voltage	12 to 45 VDC, redundant inputs	
Input Current (@ 24 V)	PN5-RD: Max. 0.24 A PN8-RD: Max. 0.21 A	
Connection	One removable 6-pin terminal block	
Overload Current Protection	Present	
Reverse Polarity Protection	Present	
Physical Characteristics		

Specifications

Technology	
Housing	Metal, IP30 protected
Dimensions	53.6 x 135 x 105 mm
Weight	0.65 kg (PN5-RD models) 0.89 kg (PN8-RD models)
Installation	DIN-Rail, Wall Mounting (optional kit)
Environmental Limits	
Operating Temperature	0 to 60°C (32 to 140°F); -40 to 75°C (-40 to 167°F) for -T models
Storage Temperature	-40 to 85°C (-40 to 185°F)
Ambient Relative Humidity	5% to 95% (non-condensing)
Regulatory Approvals	
Safety	UL 60950-1, UL 508, CSA C22.2 No. 60950-1, EN 60950-1
Hazardous Location	UL/cUL Class I, Division 2, Groups A, B, C and D ATEX Zone 2: PN5-RD: Ex nC nL IIC T4 PN8-RD: EX nA nC op is IIC T4 Gc
EMI	FCC Part 15, CISPR (EN 55022) class A
EMS	EN 61000-4-2 (ESD), Level 3 EN 61000-4-3 (RS), Level 3 EN 61000-4-4 (EFT), Level 3 EN 61000-4-5 (Surge), Level 3 EN 61000-4-6 (CS), Level 3
Shock	IEC 60068-2-27
Free fall	IEC 60068-2-32
Vibration	IEC 60068-2-6
Warranty	5 years

3 Getting Started

In this chapter we explain how to install a VIPA switch for the first time. There are three ways to access the VIPA switch's configuration settings: serial console, Telnet console, or web console. If you do not know the VIPA switch's IP address, you can open the serial console by connecting the VIPA switch to a PC's COM port with a short serial cable. You can open the Telnet or web console over an Ethernet LAN or over the Internet. The following topics are covered in this chapter:

- Serial Console Configuration (115200, None, 8, 1, VT100)
- Configuration by Telnet Console
- Configuration by Web Browser
- Disabling Telnet and Browser Access

3.1 Serial Console Configuration (115200, None, 8, 1, VT100)



- You cannot connect to the serial and Telnet console at the same time.
- You can connect to the web console and another console (serial or Telnet) at the same time. However, we strongly recommend that you do NOT do so. Following this advice will allow you to maintain better control over the VIPA switch's configuration.

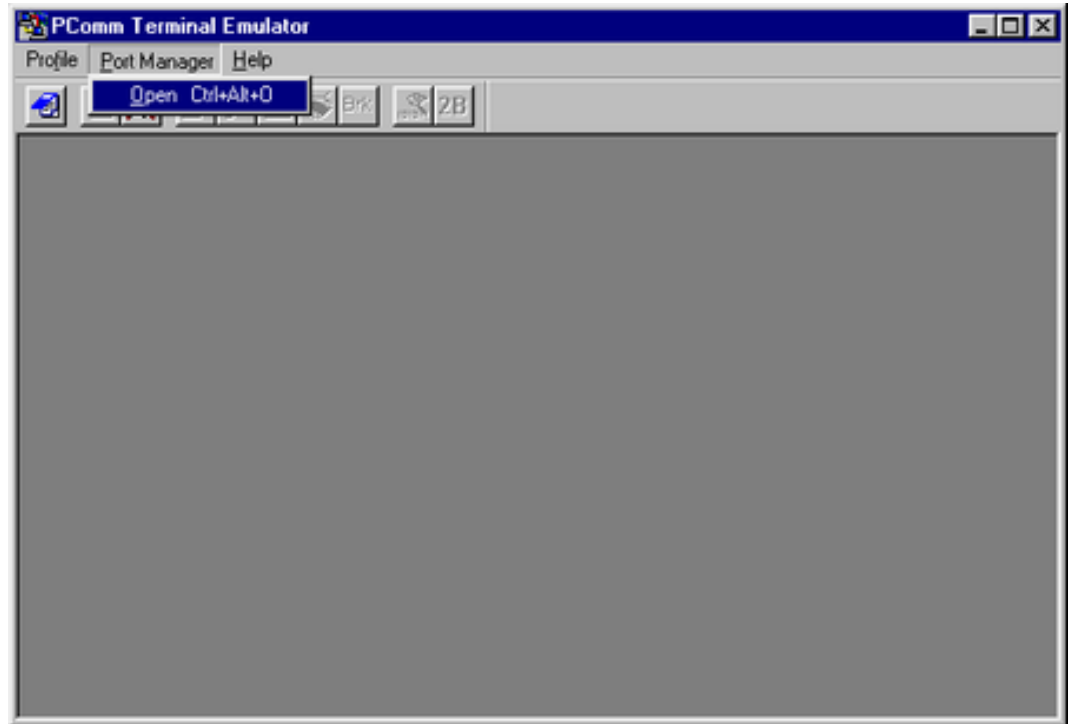


We recommend using PComm "Terminal Emulator" when opening the serial console. This software can be downloaded free of charge from the VIPA website.

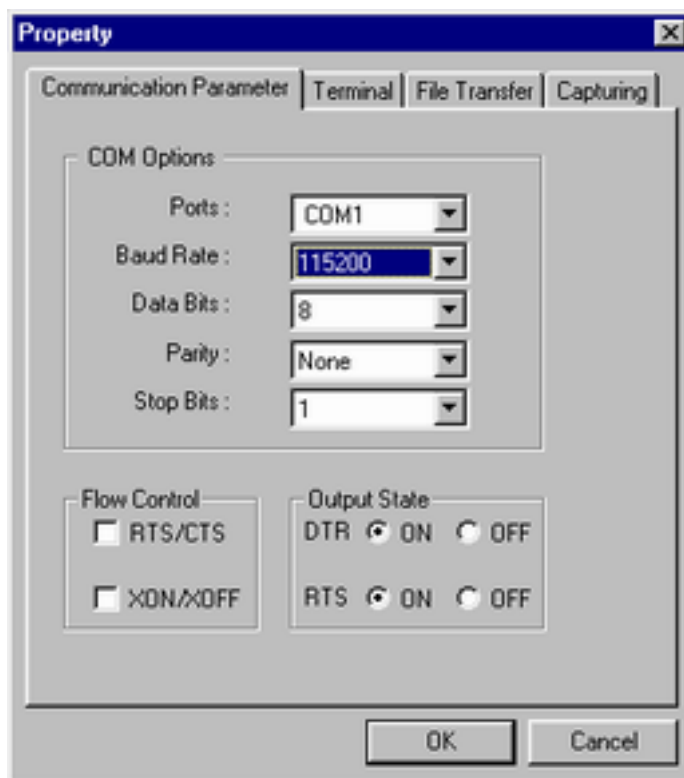
Serial Console Configuration (115200, None, 8, 1, VT100)

Before running "PComm Terminal Emulator", use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the VIPA switch's console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up). After installing "PComm Terminal Emulator", open the VIPA switch's *serial console* as follows:

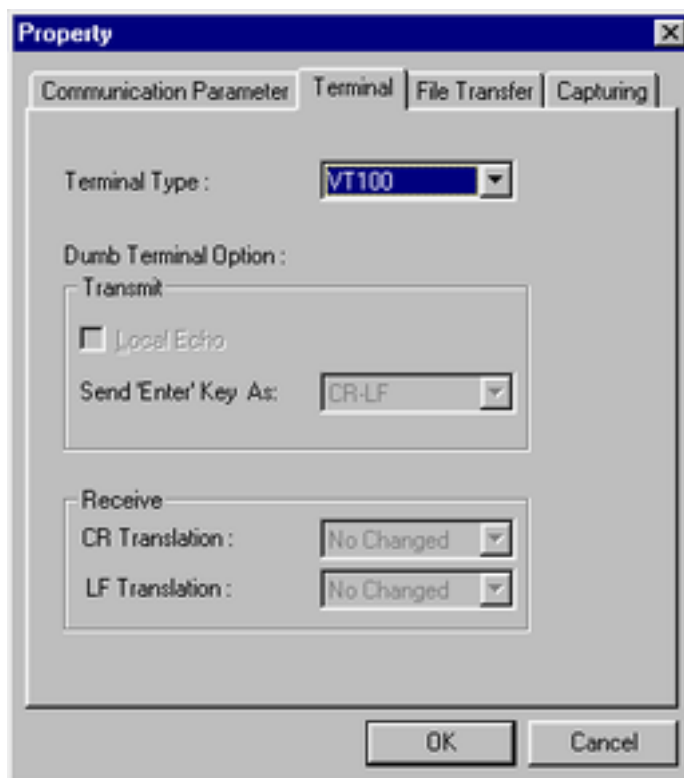
1. From the Windows desktop, click 'Start → VIPA → PComm Lite Ver1.6 → Terminal Emulator'.



2. Select 'Open' under the 'Port Manager' menu to open a new connection.
⇒ The Property window should open.



3. On the 'Communication Parameter' tab for 'Ports', select the COM port that is being used for the console connection. Set the other fields as follows: '115200' for 'Baud Rate', '8' for 'Data Bits', 'None' for 'Parity', and '1' for 'Stop Bits'.



4. On the 'Terminal' tab, select 'VT100' for 'Terminal Type', and then click [OK] to continue.
- ⇒ In the 'Terminal' window, the VIPA switch will prompt you to select a terminal type.

Serial Console Configuration (115200, None, 8, 1, VT100)

5. Enter "1" to select 'ansi/vt100' and then press [Enter].
⇒ The serial console will prompt you to log in.
6. Press [Enter] and select 'admin' or 'user'. Use the down arrow key on your keyboard to select the 'Password' field and enter a password if desired. This password will be required to access any of the consoles (web, serial, Telnet). If you do not wish to create a password, leave the 'Password' field blank and press [Enter].

```

Model :
Name : Managed Redundant Switch 02678
Location : Switch Location

Firmware Version : V2.6
Serial No : 02678
IP : 192.168.127.253
MAC Address : 00-90-E8-1B-55-24

+-----+
| Account : [admin] | user | |
| Password : +-----+ |
+-----+

```

7. The "Main Menu" of the VIPA switch's serial console should appear. (In PComm Terminal Emulator, you can adjust the font by selecting 'Font'... from the 'Edit' menu.)

```

-----
1.Basic Settings - Basic settings for network and system parameter.
2.SNMP Settings - The settings for SNMP.
3.Comm. Redundancy - Establish Ethernet communication redundant path.
4.Traffic Prioritization- Prioritize Ethernet traffic to help determinism.
5.Virtual LAN - Set up a VLAN by IEEE802.1Q VLAN or Port-based VLAN.
6.Multicast Filtering - Enable the multicast filtering capability.
7.Bandwidth Management - Restrict unpredictable network traffic.
8.Auto Warning - Warning email and/or relay output by events.
9.Line Swap - Fast recovery after moving devices to different ports.
a.Set Device IP - Assign IP addresses to connected devices.
b.Diagnosis - Test network integrity and mirroring port.
c.Monitor - Monitor a port and network status.
d.MAC Address Table - The complete table of Ethernet MAC Address List.
e.System log - The setting for System log, and Event log.
f.Exit - Exit
- Use the up/down arrow keys to select a category,
and then press Enter to select. -

```

8. Use the following keys on your keyboard to navigate the VIPA switch's serial console:

Key	Function
Up, down, right, left arrow keys, Tab	Move the onscreen cursor
Enter	Display and select options
Space	Toggle options
Esc	Previous menu

3.2 Configuration by Telnet Console

Opening the VIPA switch's *Telnet* or *web console* over a network requires that the PC host and VIPA switch are on the same logical subnet. You may need to adjust your PC host's IP address and subnet mask. By default, the VIPA switch's IP address is 192.168.127.253 and the VIPA switch's subnet mask is 255.255.255.0 (referred to as a Class B network). Your PC's IP address must be set to 192.168.xxx.xxx if the subnet mask is 255.255.0.0 or to 192.168.127.xxx if the subnet mask is 255.255.255.0.



To connect to the VIPA switch's Telnet or web console, your PC host and the VIPA switch must be on the same logical subnet.



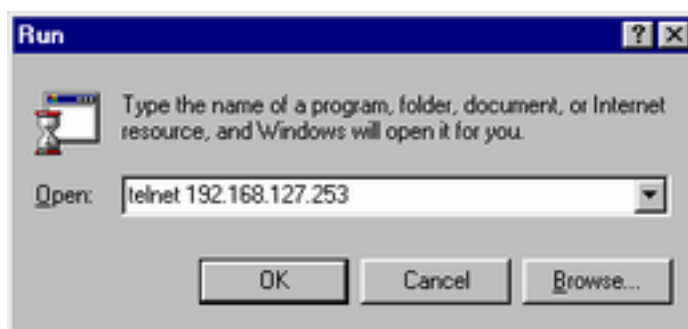
When connecting to the VIPA switch's Telnet or web console, first connect one of the VIPA switch's Ethernet ports to your Ethernet LAN or directly to your PC's Ethernet port. You may use either a straight-through or cross-over Ethernet cable.



The VIPA switch's default IP address is 192.168.127.253.

After making sure that the VIPA switch is connected to the same LAN and logical subnet as your PC, open the VIPA switch's *Telnet console* as follows:

1. Click 'Start → Run' from the Windows Start menu and then Telnet to the VIPA switch's IP address from the Windows Run window. You may also issue the Telnet command from a DOS prompt.



2. In the terminal window, the Telnet console will prompt you to select a terminal type. Type [1] to choose 'ansi/vt100' and then press [Enter].

3. The Telnet console will prompt you to log in. Press *[Enter]* and then select 'admin' or 'user'. Use the down arrow key on your keyboard to select the 'Password' field and enter a password if desired. This password will be required to access any of the consoles (web, serial, Telnet). If you do not wish to create a password, leave the 'Password' field blank and press *[Enter]*.

```

Model :
Name : Managed Redundant Switch 00000
Location : Switch Location

Firmware Version : V1.0
Serial No : 00000
IP : 192.168.127.253
MAC Address : 00-90-E8-00-67-26

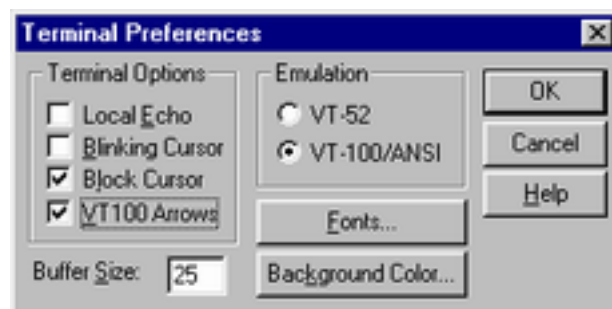
+-----+
+-----+ | admin | +-----+
| Account : [admin] | user | |
| Password : +-----+ |
+-----+
    
```

4. The "Main Menu" of the VIPA switch's *Telnet console* should appear.

```

-----
1.Basic Settings - Basic settings for network and system parameter.
2.SNMP Settings - The settings for SNMP.
3.Comm. Redundancy - Establish Ethernet communication redundant path.
4.Traffic Prioritization- Prioritize Ethernet traffic to help determinism.
5.Virtual LAN - Set up a VLAN by IEEE802.1Q VLAN or Port-based VLAN.
6.Multicast Filtering - Enable the multicast filtering capability.
7.Bandwidth Management - Restrict unpredictable network traffic.
8.Auto Warning - Warning email and/or relay output by events.
9.Line Swap - Fast recovery after moving devices to different ports.
a.Set Device IP - Assign IP addresses to connected devices.
b.Diagnosis - Test network integrity and mirroring port.
c.Monitor - Monitor a port and network status.
d.MAC Address Table - The complete table of Ethernet MAC Address List.
e.System log - The setting for System log, and Event log.
f.Exit - Exit
- Use the up/down arrow keys to select a category,
and then press Enter to select. -
    
```

5. In the terminal window, select 'Preferences'... from the 'Terminal' menu on the menu bar.
6. The 'Terminal Preferences' window should appear. Make sure that 'VT100 Arrows' is checked.



7. Use the following keys on your keyboard to navigate inside the VIPA switch's Telnet console:

Key	Function
Up, down, right, left arrow keys, Tab	Move the onscreen cursor
Enter	Display and select options
Space	Toggle options
Esc	Previous menu



The Telnet console looks and operates in precisely the same manner as the serial console.

3.3 Configuration by Web Browser

The VIPA switch's *web console* is a convenient platform for modifying the configuration and accessing the built-in monitoring and network administration functions. You can open the VIPA switch's *web console* using a standard web browser, such as Internet Explorer.



To connect to the VIPA switch's Telnet or web console, your PC host and the VIPA switch must be on the same logical subnet.



If the VIPA switch is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.



When connecting to the VIPA switch's Telnet or web console, first connect one of the VIPA switch's Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet port. You may use either a straight-through or cross-over Ethernet cable.

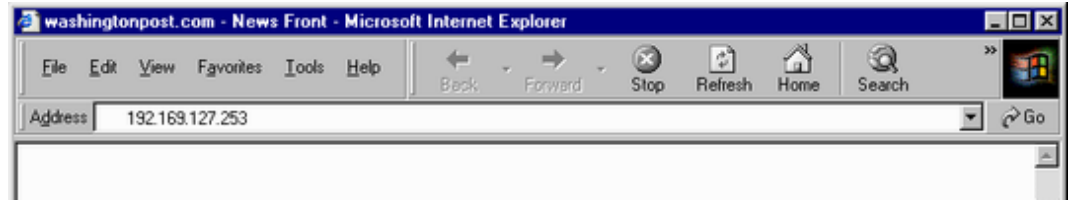


The VIPA switch's default IP address is 192.168.127.253.

Configuration by Web Browser

After making sure that the VIPA switch is connected to the same LAN and logical subnet as your PC, open the VIPA switch's web console as follows:

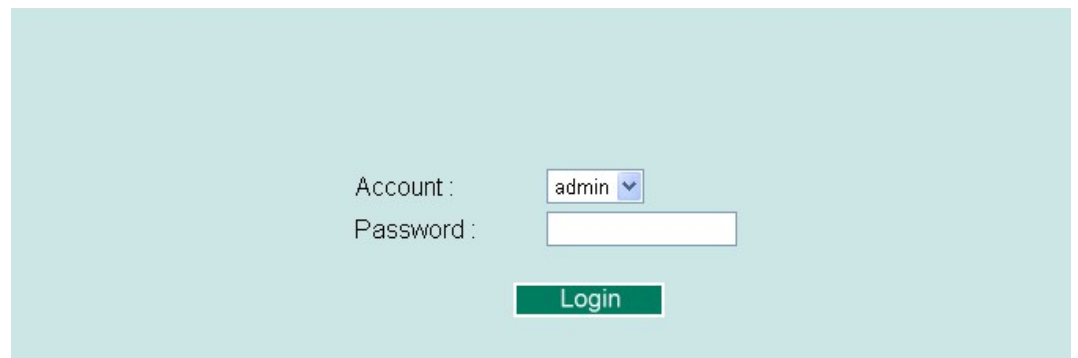
1. ➤ Connect your web browser to the VIPA switch's IP address by entering it in the Address or URL field.



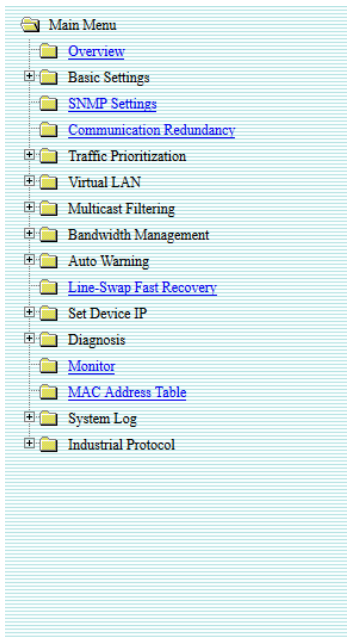
⇒ The VIPA switch's *web console* will open, and you will be prompted to log in.

2. ➤ Select the login account (admin or user) and enter the 'Password'. This password will be required to access any of the consoles (web, serial, Telnet). If you do not wish to create a password, leave the 'Password' field blank and press [Enter].

i *By default, no password is assigned to the VIPA switch's web, serial and Telnet consoles.*



3. ➤ After logging in, you may need to wait a few moments for the *web console* to appear. Use the folders in the left navigation panel to navigate between different pages of configuration options.



Welcome to the Web Console

See below for a brief description of each function groups, and then click on the item in the left pane to access the item.

Basic Settings	- Basic settings for network management parameters and system configurations.
SNMP Settings	- The settings for SNMP.
Communication Redundancy	- Establish Ethernet communication redundant path.
Traffic Prioritization	- Prioritize Ethernet traffic to increase determinism.
Virtual LAN	- Set up a VLAN by IEEE 802.1Q VLAN or Port-based VLAN.
Multicast Filtering	- Enable the multicast filtering capability.
Bandwidth Management	- Restrict unpredictable network traffic.
Auto Warning	- Automatically send warning email and/or trigger relay output by event.
Line-Swap Fast Recovery	- Fast recovery after moving devices to different ports.
Set Device IP	- Assign IP addresses to connected devices.
Diagnosis	- The Settings for Mirror port, LLDP and use Ping command to test network integrity.
Monitor	- Monitor port and network status.
MAC Address Table	- The complete list of Ethernet MAC Addresses.
System log	- The settings for Syslog and Event log.
Industrial Protocol	- The settings for Ethernet/IP, Modbus and PROFINET IO.

3.4 Disabling Telnet and Browser Access

If you are connecting the VIPA switch to a public network but do not intend to manage it over the network, we suggest disabling both the Telnet and web consoles. This is done from the serial console by navigating to 'System Identification' under 'Basic Settings'. Disable or enable the 'Telnet Console' and 'Web Configuration' as shown below:

```

EtherDevice Switch
Basic Settings
[System] [Password] [Accessible IP] [Port] [Network] [Time] [Backup Media]
[Restart] [Factory default] [Upgrade] [Activate] [Main menu]
System Identification
ESC: Previous menu  Enter: Select  Space bar: Toggle

Switch Name           [6726-252                ]
Switch Location       [Switch Location        ]
Switch Description    [                        ]
Maintainer Contact Info [                        ]

Serial NO.            02678
Firmware Version      V2.6
MAC Address           00-90-E8-1B-55-24

Telnet Console        [Enable ]
Web Configuration     [http or https]
Web Auto-logout (s)  [0                ]

```

4 Featured Functions

In this chapter, we explain how to access the VIPA switch's various configuration, monitoring, and administration functions. These functions can be accessed by serial, Telnet, or web console. The serial console can be used if you do not know the VIPA switch's IP address and requires that you connect the VIPA switch to a PC COM port. The Telnet and web consoles can be opened over an Ethernet LAN or the Internet. The web console is the most user-friendly interface for configuring a VIPA switch. In this chapter, we use the *web console* interface to introduce the functions. There are only a few differences between the web console, serial console, and Telnet console.

The following topics are covered in this chapter:

- Configuring Basic Settings
- Loop Protection
- Configuring SNMP
- Using Traffic Prioritization
- Using Virtual LAN
- Using Multicast Filtering
- Using Bandwidth Management
- Using Auto Warning
- Using Line-Swap-Fast-Recovery
- Using Set Device IP
- Using Diagnosis
- Using Monitor
- Using the MAC Address Table
- Using Event Log
- Using Syslog

4.1 Configuring Basic Settings

The *Basic Settings* section includes the most common settings required by administrators to maintain and control a VIPA switch.

4.1.1 System Identification

System Identification items are displayed at the top of the web console and will be included in alarm emails. You can configure the System Identification items to make it easier to identify different switches that are connected to your network.

System Identification

Switch Name	<input type="text" value="Managed Redundant Switch 00000"/>
Switch Location	<input type="text" value="Switch Location"/>
Switch Description	<input type="text"/>
Maintainer Contact Info	<input type="text"/>
Web Auto-logout (s)	<input type="text" value="0"/>
Age Time (s)	<input type="text" value="300"/>
CPU Loading (past 5 seconds)	<input type="text" value="9 %"/>
CPU Loading (past 30 seconds)	<input type="text" value="10 %"/>
CPU Loading (past 5 minutes)	<input type="text" value="10 %"/>
Free Memory	<input type="text" value="60061004"/>

Switch Name

Setting	Description	Factory Default
Max. 30 characters	This option is useful for differentiating between the roles or applications of different units. Example: Factory Switch 1.	Managed Redundant Switch [Serial number of this switch]

Switch Location

Setting	Description	Factory Default
Max. 80 characters	This option is useful for differentiating between the locations of different units. Example: production line 1.	Switch Location

Switch Description

Setting	Description	Factory Default
Max. 30 characters	This option is useful for recording a more detailed description of the unit.	None

Maintainer Contact Info

Setting	Description	Factory Default
Max. 30 characters	This option is useful for providing information about who is responsible for maintaining this unit and how to contact this person.	None

Web Auto-logout (S)

Setting	Description	Factory Default
60 to 86400 (seconds)	Disable or extend the auto-logout time for the web management console.	0 (disabled)

Age Time (S)

Setting	Description	Factory Default
15 to 3825 (seconds)	The length of time that a MAC address entry can remain in the VIPA switch. When an entry reaches its aging time, it "ages out" and is purged from the switch, effectively cancelling frame forwarding to that specific port.	300

CPU Loading

Setting	Description	Factory Default
Read-only	The CPU usage volume in the past 5 seconds, 30 seconds and 5 minutes	None

Free Memory

Setting	Description	Factory Default
Read-only	The immediately free memory of the switch	None

4.1.2 Password

The VIPA switch provides two levels of configuration access. The *'admin'* account has read/write access of all configuration parameters, and the *'user'* account has read access only. A *'user'* account can view the configuration, but will not be able to make modifications.

Password Setting

Account Name :

Old Password :

Type Old Password :

New Password :

Retype Password :

**WARNING!**

By default, a password is not assigned to the VIPA switch's web, Telnet, and serial consoles. If a password is assigned, you will be required to enter the password when you open the serial console, Telnet console or Web console.

Account

Setting	Description	Factory Default
Admin	This account can modify the VIPA switch's configuration.	admin
User	This account can only view the VIPA switch's configurations.	

Password

Setting	Description	Factory Default
Old password (max. 16 characters)	Enter the current password	None
New password (max. 16 characters)	Enter the desired new password. Leave it blank if you want to remove the password.	None
Retype password (max. 16 characters)	Enter the desired new password again. Leave it blank if you want to remove the password.	None

4.1.3 Accessible IP List

The VIPA switch uses an IP address-based filtering method to control access.

Accessible IP List

Enable the accessible IP list ("Disable" will allow all IP's connection)

Index	IP	NetMask
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Activate

You may add or remove IP addresses to limit access to the VIPA switch. When the accessible IP list is enabled, only addresses on the list will be allowed access to the VIPA switch. Each IP address and netmask entry can be tailored for different situations:

- **Grant access to one host with a specific IP address**
For example, enter IP address 192.168.1.1 with netmask 255.255.255.255 to allow access to 192.168.1.1 only.
- **Grant access to any host on a specific subnetwork**
For example, enter IP address 192.168.1.0 with netmask 255.255.255.0 to allow access to all IPs on the subnet defined by this IP address/subnet mask combination.
- **Grant access to all hosts**
Make sure the accessible IP list is not enabled. Remove the checkmark from 'Enable the accessible IP list'.

Additional configuration examples:

Hosts that need access	Input Format
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

4.1.4 Port Settings

Ethernet Port Settings

Port settings are included to give the user control over port access, port transmission speed, flow control and port type (MDI or MDIX).

Port Settings

Port	Enable	Description	Name	Speed	FDX Flow Ctrl	MDI/MDIX
1-1	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto	Disable	Auto
1-2	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto	Disable	Auto
1-3	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto	Disable	Auto
1-4	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto	Disable	Auto
1-5	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto	Disable	Auto
1-6	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto	Disable	Auto
1-7	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto	Disable	Auto
1-8	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto	Disable	Auto
2-1	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto	Disable	Auto
2-2	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto	Disable	Auto
2-3	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto	Disable	Auto
2-4	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto	Disable	Auto

Activate

Enable

Setting	Description	Factory Default
Checked	Allows data transmission through the port.	Enabled
Unchecked	Immediately shuts off port access.	



WARNING!

If a connected device or sub-network is wreaking havoc on the rest of the network, the 'Disable' option under 'Advanced Settings/Port' gives the administrator a quick way to shut off access through this port immediately.

Description

Setting	Description	Factory Default
Media type	Displays the media type for each module's port	N/A

Name

Setting	Description	Factory Default
Max. 63 characters	Specifies an alias for the port to help administrators differentiate between different ports. Example: PLC 1	None

Speed

Setting	Description	Factory Default
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection.	Auto
1G-Full	Choose one of these fixed speed options if the connected Ethernet device has trouble auto-negotiating for line speed.	
100M-Full		
100M-Half		
10M-Full		
10M-Half		

FDX Flow Ctrl

This setting enables or disables flow control for the port when the port's Speed is set to Auto. The final result will be determined by the Auto process between the VIPA switch and connected devices.

Setting	Description	Factory Default
Enable	Enables flow control for this port when the port's Speed is set to Auto.	Disabled
Disable	Disables flow control for this port when the port's Speed is set to Auto.	

MDI/MDIX

Setting	Description	Factory Default
Auto	Allows the port to auto-detect the port type of the connected Ethernet device and change the port type accordingly.	Auto
MDI	Choose MDI or MDIX if the connected Ethernet device has trouble auto-negotiating for port type.	
MDIX		

4.1.5 Network Parameters

Network configuration allows users to configure both IPv4 and IPv6 parameters for management access over the network. The VIPA switch supports both IPv4 and IPv6, and can be managed through either of these address types.

A brief explanation of each configuration item is given below.

Network Parameters

General Settings

IPv4

Auto IP Configuration: Disable

Switch IP Address: 192.168.127.251

Switch Subnet Mask: 255.255.255.0

Default Gateway:

1st DNS Server IP Address:

2nd DNS Server IP Address:

Dhcp Retry Periods: 1 (1-30)

Dhcp Retry Times: 0 (0-65535)

IPv6

Global Unicast Address Prefix:

Global Unicast Address: ::

Link-Local Address: fe80::290:e8ff:fe24:216

Activate

IP4 The IPv4 settings include the switch's IP address and subnet mask, as well as the IP address of the default gateway. In addition, input cells are provided for the IP addresses of a 1st and 2nd DNS server.

Auto IP Configuration

Setting	Description	Factory Default
Disable	The VIPA switch's IP address must be set manually.	Disable
By DHCP	The VIPA switch's IP address will be assigned automatically by the network's DHCP server.	
By BootP	The VIPA switch's IP address will be assigned automatically by the network's BootP server.	

Switch IP Address

Setting	Description	Factory Default
IP address for the VIPA switch	Assigns the VIPA switch's IP address on a TCP/IP network.	192.168.127.253

Switch Subnet Mask

Setting	Description	Factory Default
Subnet mask for the VIPA switch	Identifies the type of network the VIPA switch is connected to (e.g., 255.255.0.0 for a Class B network or 255.255.255.0 for a Class C network).	255.255.255.0

Default Gateway

Setting	Description	Factory Default
IP address for gateway	Specifies the IP address of the router that connects the LAN to an outside network.	None

DNS IP Address

Setting	Description	Factory Default
IP address for 1st DNS server	Specifies the IP address of the DNS server used by your network. After specifying the DNS server's IP address, you can use the VIPA switch's URL to open the web console instead of entering the IP address.	None
IP address for 2nd DNS server	Specifies the IP address of the secondary DNS server used by your network. The VIPA switch will use the secondary DNS server if the first DNS server fails to connect.	None

DHCP Retry Periods

Setting	Description	Factory Default
1 to 30	Users can configure the DHCP retry period manually	1

DHCP Retry Times

Setting	Description	Factory Default
0 to 65535	Users can configure the times of DHCP retry manually	0

IP6

The IPv6 settings include two distinct address types-Link-Local Unicast addresses and Global Unicast addresses. A Link-Local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. To connect to a larger network with multiple segments, the switch must be configured with a Global Unicast address.

Global Unicast Address Prefix (Prefix Length: 64 bits) Default Gateway

Setting	Description	Factory Default
Global Unicast Address Prefix	The prefix value must be formatted according to the RFC 2373 "IPv6 Addressing Architecture" using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.	None

Global Unicast Address

Setting	Description	Factory Default
None	Displays the IPv6 Global Unicast address. The network portion of the Global Unicast address can be configured by specifying the Global Unicast Prefix and using an EUI-64 interface ID in the low order 64 bits. The host portion of the Global Unicast address is automatically generated using the modified EUI-64 form of the interface identifier (Switch's MAC address).	None

Link-Local Address

Setting	Description	Factory Default
None	The network portion of the Link-Local address is FE80 and the host portion of the Link-Local address is automatically generated using the modified EUI-64 form of the interface identifier (Switch's MAC address)	None

Neighbor Cache

Neighbor Cache

IPv6 Address	Link Layer (MAC) Address	State
fe80::290:e8ff:fe0e:e02	00-90-e8-0e-0e-02	Reachable

Setting	Description	Factory Default
None	The information in the neighbor cache that includes the neighboring node's IPv6 address, the corresponding Link-Layer address, and the current state of the entry.	None

4.1.6 GARP Timer Parameters

Generic Attribute Registration Protocol (GARP) was defined by the IEEE 802.1 working group to provide a generic framework. GARP defines the architecture, rules of operation, state machines, and variables for the registration and de-registration of attribute values. The GARP Timer parameters are exchanged by creating the applications via GVRP (GARP VLAN Registration Protocol) to set the attributes of Timer. Note that you need to set the same GARP timer values on all Layer 2 switches to ensure that the system works successfully.

GARP Timer Parameters

Join Time (ms)	<input type="text" value="200"/>
Leave Time (ms)	<input type="text" value="600"/>
Leaveall Time (ms)	<input type="text" value="10000"/>

Join Time

Setting	Description	Factory Default
None	Specifies the period of the join time	200

Leave Time

Setting	Description	Factory Default
None	Specifies the period of leave time	600

Leaveall Time

Setting	Description	Factory Default
None	Specifies the period of leaveall time	10000



Leave Time should be at least two times more than Join Time and Leaveall Time should be larger than Leave Time.

4.1.7 System Time Settings

The VIPA switch has a time calibration function based on information from an NTP server or user specified time and date. Functions such as automatic warning emails can therefore include time and date stamp.



The VIPA switch does not have a real time clock. The user must update the Current Time and Current Date to set the initial time for the VIPA switch after each reboot, especially when there is no NTP server on the LAN or Internet connection.

Current Time

Setting	Description	Factory Default
User-specified time	Allows configuration of the local time in local 24-hour format.	None

Current Date

Setting	Description	Factory Default
User-specified date	Allows configuration of the local date in yyyy-mm-dd format.	None

Daylight Saving Time

The Daylight Saving Time settings are used to automatically set the VIPA switch's time forward according to national standards.

Start Date

Setting	Description	Factory Default
User-specified date	Specifies the date that Daylight Saving Time begins.	None

End Date

Setting	Description	Factory Default
User-specified date	Specifies the date that Daylight Saving Time ends.	None

Offset

Setting	Description	Factory Default
User-specified hour	Specifies the number of hours that the time should be set forward during Daylight Saving Time.	None

System Up Time

Indicates how long the VIPA switch remained up since the last cold start. The up time is indicated in seconds.

Time Zone

Setting	Description	Factory Default
Time zone	Specifies the time zone, which is used to determine the local time offset from GMT (Greenwich Mean Time).	GMT (Greenwich Mean Time)



Changing the time zone will automatically correct the current time. Be sure to set the time zone before setting the time.

Time Server IP/Name

Setting	Description	Factory Default
1st Time Server IP/Name	The IP or domain address (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	None
2nd Time Server IP/Name	The VIPA switch will try to locate the secondary NTP server if the first NTP server fails to connect.	

Time Protocol

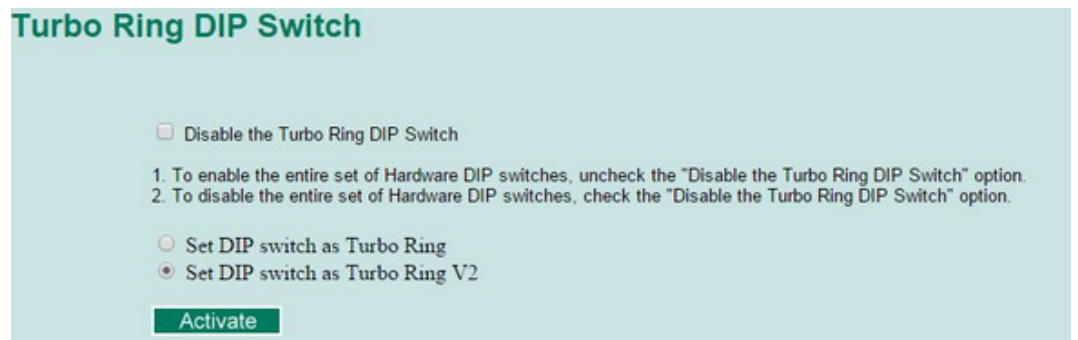
Setting	Description	Factory Default
NTP	NTP (Network Time Protocol) is used to synchronize time with multiple time servers. The time accuracy is up to 50 ms.	-
SNTP	SNTP stands for Simple Network Time Protocol). The synchronization process of SNTP is simpler than NTP. The time accuracy is up to 1 second, which is suitable for low time accuracy requirements.	-

Enable NTP/SNTP Server

Setting	Description	Factory Default
Enable/Disable	Enables SNTP/NTP server functionality for clients	Disabled

4.1.8 Turbo Ring DIP Switch

The *Turbo Ring DIP Switch* page allows users to disable the 4th DIP switch located on the Switch’s outer casing. The default is enabled with Turbo Ring v2 protocol. Once the user changes the 4th hardware DIP switch configuration to ON, the switch will start to initiate the Turbo Ring redundancy protocol based on the configuration. The detailed description is given below:



Setting	Description	Factory Default
Disable the Turbo Ring DIP switch	Unchecked: The Turbo Ring protocol will be activated automatically when the 4th DIP switch is moved to the ON position.	unchecked
	Checked: The Turbo Ring protocol will not be activated automatically, regardless of the position of the 4th DIP switch.	
Set DIP switch as Turbo Ring	If the DIP switch is enabled, Turbo Ring protocol will be enabled when the DIP switch is moved to the ON position.	Set DIP switch as Turbo Ring V2
Set DIP switch as Turbo Ring V2	If the DIP switch is enabled, Turbo Ring V2 protocol will be enabled when the DIP switch is moved to the ON position.	



If the 4th DIP switch (Turbo Ring) is configured to ON, you will not be able to disable the Turbo Ring DIP switch from the web interface, console or Telnet.



If you would like to enable VLAN and/or port trunking on any of the last four ports, do not use the fourth DIP switch to activate Turbo Ring. In this case, you should use the Web, Telnet, or Serial console to activate Turbo Ring.

4.1.9 System File Update

4.1.9.1 Update System Files by Remote TFTP

The VIPA switch supports saving your configuration or log file to a remote TFTP server or local host. Other VIPA switches can also load the configuration at a later time. The VIPA switch also supports loading firmware or configuration files from the TFTP server or a local host.

Update System Files by TFTP

TFTP Server IP/Name	<input type="text"/>	
Configuration Files Path and Name	<input type="text"/>	<input type="button" value="Download"/> <input type="button" value="Upload"/>
Firmware Files Path and Name	<input type="text"/>	<input type="button" value="Download"/>
Log Files Path and Name	<input type="text"/>	<input type="button" value="Upload"/>

TFTP Server IP/Name

Setting	Description	Factory Default
IP address of TFTP server	Specifies the IP address or name of the remote TFTP server. Must be specified before downloading or uploading files.	None

Configuration Files Path and Name

Setting	Description	Factory Default
Max. 40 characters	Specifies the path and file name of the VIPA switch's configuration file on the TFTP server.	None

Firmware Files Path and Name

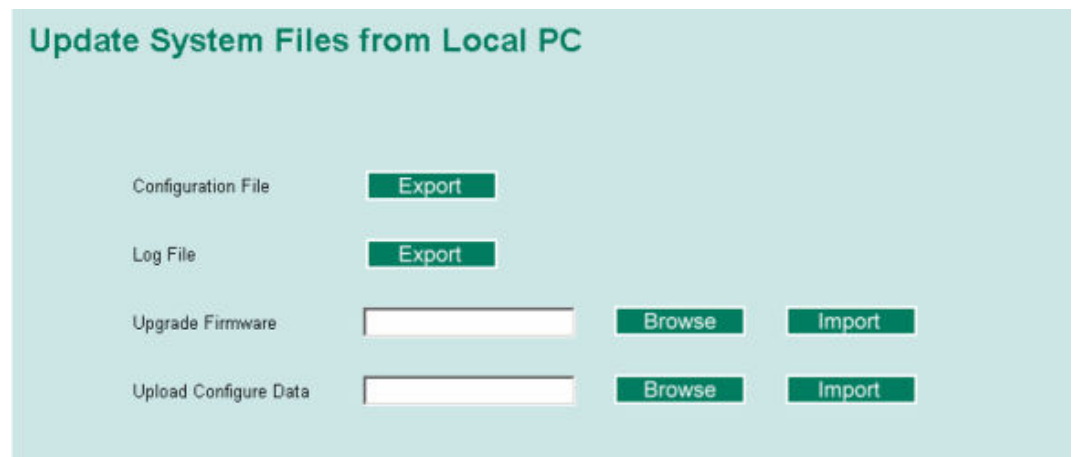
Setting	Description	Factory Default
Max. 40 characters	Specifies the path and file name of the VIPA switch's firmware file.	None

Log Files Path and Name

Setting	Description	Factory Default
Max. 40 characters	Specifies the path and file name of the VIPA switch's log file.	None

➔ After setting the desired paths and file names, click [Download] to download the prepared file from the remote TFTP server or click [Upload] to Upload the desired file to the remote TFTP server.

4.1.9.2 Update System Files from Local PC



Configuration File

➔ Click [Export] to save the VIPA switch's configuration file to the local host.

Log File

➔ Click [Export] to save the VIPA switch's log file to the local host.



Some operating systems will open the configuration file and log file directly in the web page. In such cases, right click the [Export] button to save the file.

Upgrade Firmware

➔ To import a new firmware file into the VIPA switch, click [Browse] to select the firmware file that is saved on your computer. The upgrade procedure will proceed automatically after clicking [Import].

Upload Configure Data

➔ To import a configuration file into the VIPA switch, click [Browse] to select the configuration file already saved on your computer. The upgrade procedure will proceed automatically after clicking [Import].

4.1.10 ABC (Auto-Backup Configurator) Configuration

You can use VIPA's Automatic Backup Configurator to save and load the VIPA switch's configurations through the switch's RS-232 console port.

ABC (Auto-Backup Configurator) Configuration

Auto load ABC's system configurations when system boots up Activate

Save the current configurations to ABC Save

Load the ABC's configurations to Switch Load

4.1.11 Restart

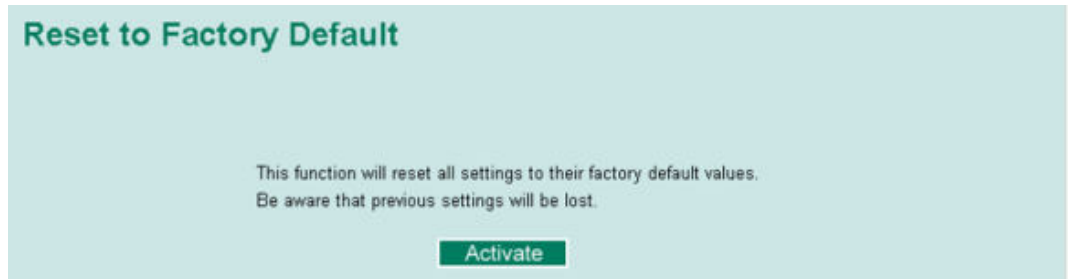
This function provides users with a quick way to restart the system.

Restart

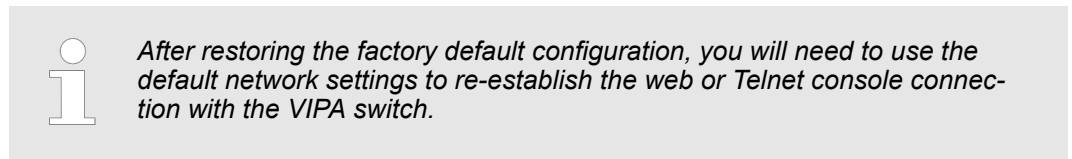
This function will restart the system.

Activate

4.1.12 Reset to Factory Default

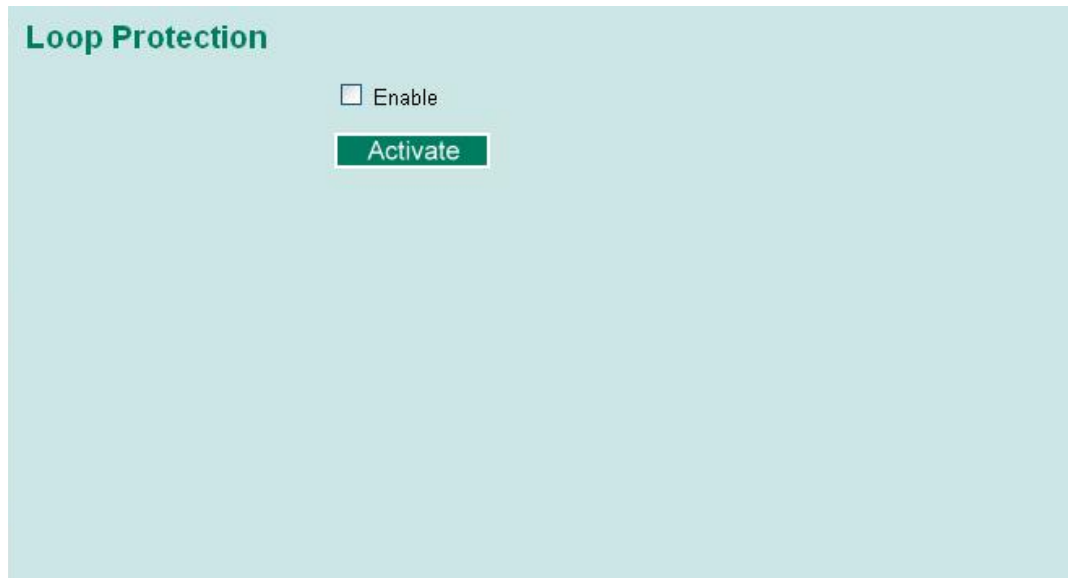


This function provides users with a quick way of restoring the VIPA switch’s configuration to factory defaults. The function is available in the serial, Telnet and web consoles.



4.2 Loop Protection

The switch is designed with a loop checking mechanism: Send a control BPDU from the Ethernet port and check if this control BPDU will be sent back to the switch again. If the looping occurs, the switch will automatically block the Ethernet port to prevent looping.



Check the 'Enable' box and click Activate to enable the Loop protection.

4.3 Configuring SNMP

The VIPA switch supports SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community strings *public* and *private* by default. SNMP V3 requires that you select an authentication level of MD5 or SHA, and is the most secure protocol. You can also enable data encryption to enhance data security. Supported SNMP security modes and levels are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	UI Setting	Authentication	Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Uses a community string match for authentication.
	V1, V2c Write/Read Community	Community string	No	Uses a community string match for authentication.
SNMP V3	No-Auth	No	No	Uses an account with admin or user to access objects
	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

These parameters are configured on the SNMP page. A more detailed explanation of each parameter is given below the figure.

SNMP

SNMP Read/Write Settings

SNMP Versions V1, V2c ▾

V1,V2c Read Community

V1,V2c Write/Read Community

Admin Auth. Type No-Auth ▾

Admin Data Encryption Key

User Auth. Type No-Auth ▾

User Data Encryption Key

Trap Settings

1st Trap Server IP/Name

1st Trap Community

2nd Trap Server IP/Name

2nd Trap Community

Trap Mode

Trap ▾

Retries (1~99)

Timeout (1~300s)

Private MIB information

Switch Object ID enterprise.8691.7.17

Activate

4.3.1 SNMP Read/Write Settings

SNMP Versions

Setting	Description	Factory Default
V1, V2c, V3, or V1, V2c, or V3 only	Specifies the SNMP protocol version used to manage the switch.	V1, V2c

V1, V2c Read Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to authenticate the SNMP agent for read-only access. The SNMP agent will access all objects with read-only permissions using this community string.	Public

V1, V2c Write/Read Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to authenticate the SNMP agent for read/write access. The SNMP server will access all objects with read/write permissions using this community string.	Private

For SNMP V3, two levels of privilege are available accessing the VIPA switch. *Admin* privilege provides access and authorization to read and write the MIB file. *User* privilege allows reading of the MIB file only.

Admin Auth. Type (for SNMP V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
NoAuth	Allows the admin account to access objects without authentication.	No
MD5- Auth	Authentication will be based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Authentication will be based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

Admin Data Encryption Key (for SNMP V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
Enable	Enables data encryption using the specified data encryption key (between 8 and 30 characters).	No
Disable	Specifies that data will not be encrypted.	No

User Auth. Type (for SNMP V1, V2c, V3 and V3 only)

Setting	Description	Factory Default
No-Auth	Allows the admin account and user account to access objects without authentication.	No
MD5-Auth	Authentication will be based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Authentication will be based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

User Data Encryption Key (for SNMP V1, V2c, V3 and V3 only)

Setting	Description	Factory Default
Enable	Enables data encryption using the specified data encryption key (between 8 and 30 characters).	No
Disable	No data encryption	No

4.3.2 Trap Settings

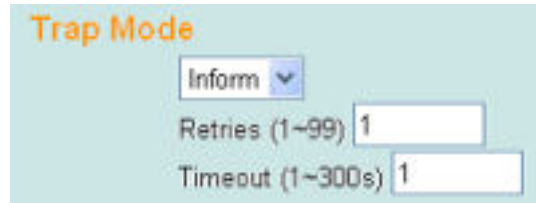
SNMP traps allow an SNMP agent to notify the NMS of a significant event. The switch supports two SNMP modes, *Trap* mode and *Inform* mode.

SNMP Trap Mode - Trap

In Trap mode, the SNMP agent sends an SNMPv1 trap PDU to the NMS. No acknowledgment is sent back from the NMS so the agent has no way of knowing if the trap reached the NMS.

**SNMP Trap Mode - Inform**

SNMPv2 provides an inform mechanism. When an inform message is sent from the SNMP agent to the NMS, the receiver sends a response to the sender acknowledging receipt of the event. This behavior is similar to that of the get and set requests. If the SNMP agent does not receive a response from the NMS for a period of time, the agent will resend the trap to the NMS agent. The maximum timeout time is 300 sec (default is 1 sec), and the maximum number of retries is 99 times (default is 1 time). When the SNMP agent receives acknowledgement from the NMS, it will stop resending the inform messages.



1st Trap Server IP/Name

Setting	Description	Factory Default
IP or name	Specifies the IP address or name of the primary trap server used by your network.	None

1st Trap Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to use for authentication.	Public

2nd Trap Server IP/Name

Setting	Description	Factory Default
IP or name	Specifies the IP address or name of the secondary trap server used by your network.	None

2nd Trap Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to use for authentication.	Public

4.3.3 Private MIB Information

Switch Object ID

Setting	Description	Factory Default
Specific VIPA switch ID	Indicates the VIPA switch’s enterprise value.	Depends on switch model type



The Switch Object ID cannot be changed.

4.4 Using Traffic Prioritization

The VIPA switch’s traffic prioritization capability provides Quality of Service (QoS) to your network by making data delivery more reliable. You can prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay. Traffic can be con-

trolled by a set of rules to obtain the required Quality of Service for your network. The rules define different types of traffic and specify how each type should be treated as it passes through the switch. The VIPA switch can inspect both IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information to provide consistent classification of the entire network. The VIPA switch's QoS capability improves the performance and determinism of industrial networks for mission critical applications.

4.4.1 The Traffic Prioritization Concept

Traffic prioritization allows you to prioritize data so that time-sensitive and system-critical data can be transferred smoothly and with minimal delay over a network. The benefits of using traffic prioritization are:

- Improve network performance by controlling a wide variety of traffic and managing congestion.
- Assign priorities to different categories of traffic. For example, set higher priorities for time-critical or business-critical applications.
- Provide predictable throughput for multimedia applications, such as video conferencing or voice over IP, and minimize traffic delay and jitter.
- Improve network performance as the amount of traffic grows. Doing so will reduce costs since it will not be necessary to keep adding bandwidth to the network.

Traffic prioritization uses the four traffic queues that are present in your VIPA switch to ensure that high priority traffic is forwarded on a different queue from lower priority traffic. Traffic prioritization provides Quality of Service (QoS) to your network.

VIPA switch traffic prioritization depends on two industry-standard methods:

- **IEEE 802.1D**-a layer 2 marking scheme.
- **Differentiated Services (DiffServ)**-a layer 3 marking scheme.

IEEE 802.1D Traffic Marking

- The IEEE Std 802.1D, 1998 Edition marking scheme, which is an enhancement to IEEE Std 802.1D, enables Quality of Service on the LAN. Traffic service levels are defined in the IEEE 802.1Q 4-byte tag, which is used to carry VLAN identification as well as IEEE 802.1p priority information. The 4-byte tag immediately follows the destination MAC address and Source MAC address.
- The IEEE Std 802.1D, 1998 Edition priority marking scheme assigns an IEEE 802.1p priority level between 0 and 7 to each frame. The priority marking scheme determines the level of service that this type of traffic should receive. Refer to the table below for an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

IEEE 802.1p Priority Level	IEEE 802.1D Traffic Type
0	Best Effort (default)
1	Background
2	Standard (spare)
3	Excellent Effort (business critical)
4	Controlled Load (streaming multimedia)
5	Video (interactive media); less than 100 milliseconds of latency and jitter
6	Voice (interactive voice); less than 10 milliseconds of latency and jitter
7	Network Control Reserved traffic

Even though the IEEE 802.1D standard is the most widely used prioritization scheme in the LAN environment, it still has some restrictions:

- It requires an additional 4-byte tag in the frame, which is normally optional for Ethernet networks. Without this tag, the scheme cannot work.
- The tag is part of the IEEE 802.1Q header, so to implement QoS at layer 2, the entire network must implement IEEE 802.1Q VLAN tagging.
- It is only supported on a LAN and not across routed WAN links, since the IEEE 802.1Q tags are removed when the packets pass through a router.

Differentiated Services (DiffServ) Traffic Marking

DiffServ is a Layer 3 marking scheme that uses the DiffServ Code Point (DSCP) field in the IP header to store the packet priority information. DSCP is an advanced intelligent method of traffic marking that allows you to choose how your network prioritizes different types of traffic. DSCP uses 64 values that map to user-defined service levels, allowing you to establish more control over network traffic.

The advantages of DiffServ over IEEE 802.1D are:

- You can configure how you want your switch to treat selected applications and types of traffic by assigning various grades of network service to them.
- No extra tags are required in the packet.
- DSCP uses the IP header of a packet to preserve priority across the Internet.
- DSCP is backwards compatible with IPv4 TOS, which allows operation with existing devices that use a layer 3 TOS enabled prioritization scheme.

Traffic Prioritization

VIPA switches classify traffic based on layer 2 of the OSI 7 layer model, and the switch prioritizes received traffic according to the priority information defined in the received packet. Incoming traffic is classified based upon the IEEE 802.1D frame and is assigned to the appropriate priority queue based on the IEEE 802.1p service level value defined in that packet. Service level markings (values) are defined in the IEEE 802.1Q 4-byte tag, and consequently traffic will only contain 802.1p priority markings if the network is configured with VLANs and VLAN tagging. The traffic flow through the switch is as follows:

- A packet received by the VIPA switch may or may not have an 802.1p tag associated with it. If it does not, then it is given a default 802.1p tag (which is usually 0). Alternatively, the packet may be marked with a new 802.1p value, which will result in all knowledge of the old 802.1p tag being lost.
- Because the 802.1p priority levels are fixed to the traffic queues, the packet will be placed in the appropriate priority queue, ready for transmission through the appropriate egress port. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port is tagged for that VLAN. If it is, then the new 802.1p tag is used in the extended 802.1D header.
- The VIPA switch will check a packet received at the ingress port for IEEE 802.1D traffic classification, and then prioritize it based on the IEEE 802.1p value (service levels) in that tag. It is this 802.1p value that determines which traffic queue the packet is mapped to.

Traffic Queues

The hardware of VIPA switches has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the VIPA switch without being delayed by lower priority traffic. As each packet arrives in the VIPA switch, it passes through any ingress processing (which includes classification, marking/re-marking), and is then sorted into the appropriate queue. The switch then forwards packets from each queue. VIPA switches support two different queuing mechanisms:

- *Weight Fair*. This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, the Weight Fair method gives high priority precedence over low priority, but in the event that high priority traffic does not reach the link capacity, lower priority traffic is not blocked.
- *Strict*. This method services high traffic queues first; low priority queues are delayed until no more high priority data needs to be sent. The Strict method always gives precedence to high priority over low priority.

4.4.2 Configuring Traffic Prioritization

Quality of Service (QoS) provides a traffic prioritization capability to ensure that important data is delivered consistently and predictably. The VIPA switch can inspect IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information, to provide a consistent classification of the entire network. The VIPA switch's QoS capability improves your industrial network's performance and determinism for mission critical applications.

QoS Classification

QoS Classification			
Queuing Mechanism		Weight Fair(8:4:2:1)	
Port	Inspect ToS	Inspect CoS	Port Priority
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▾
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▾
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▾
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▾
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▾
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▾
7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▾
8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3(Normal) ▾

The VIPA switch supports inspection of layer 3 TOS and/or layer 2 CoS tag information to determine how to classify traffic packets.

Queuing Mechanism

Setting	Description	Factory Default
Weight Fair	The VIPA switch has 4 priority queues. In the weight fair scheme, an 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Weight Fair
Strict	In the Strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures that all high priority frames will egress the switch as soon as possible.	

Inspect TOS

Setting	Description	Factory Default
Enable/Disable	Enables or disables the VIPA switch for inspecting Type of Service (TOS) bits in the IPV4 frame to determine the priority of each frame.	Enabled

Inspect COS

Setting	Description	Factory Default
Enable/Disable	Enables or disables the VIPA switch for inspecting 802.1p COS tags in the MAC frame to determine the priority of each frame.	Enabled

Inspect Port Priority

Setting	Description	Factory Default
Port priority	The port priority has 4 priority queues. Low, normal, medium, high priority queue option is applied to each port.	3 (Normal)



The priority of an ingress frame is determined in the following order:

1. Inspect TOS
2. Inspect CoS
3. Port Priority



The designer can enable these classifications individually or in combination. For instance, if a "hot" higher priority port is required for a network design, Inspect TOS and Inspect CoS can be disabled. This setting leaves only port default priority active, which results in all ingress frames being assigned the same priority on that port.

CoS Mapping

Mapping Table of CoS Value and Priority Queues

CoS	Priority Queue
0	Low
1	Low
2	Normal
3	Normal
4	Medium
5	Medium
6	High
7	High

Activate

CoS Value and Priority Queues

Setting	Description	Factory Default
Low/Normal/ Medium/High	Maps different CoS values to 4 different egress queues.	0: Low 1: Low 2: Normal 3: Normal 4: Medium 5: Medium 6: High 7: High

TOS/DiffServ Mapping

Mapping Table of ToS (DSCP) Value and Priority Queues

ToS	Level	ToS	Level	ToS	Level	ToS	Level
0x00(1)	0(Low)	0x04(2)	0(Low)	0x08(3)	0(Low)	0x0C(4)	0(Low)
0x10(5)	0(Low)	0x14(6)	0(Low)	0x18(7)	0(Low)	0x1C(8)	0(Low)
0x20(9)	1(Low)	0x24(10)	1(Low)	0x28(11)	1(Low)	0x2C(12)	1(Low)
0x30(13)	1(Low)	0x34(14)	1(Low)	0x38(15)	1(Low)	0x3C(16)	1(Low)
0x40(17)	2(Normal)	0x44(18)	2(Normal)	0x48(19)	2(Normal)	0x4C(20)	2(Normal)
0x50(21)	2(Normal)	0x54(22)	2(Normal)	0x58(23)	2(Normal)	0x5C(24)	2(Normal)
0x60(25)	3(Normal)	0x64(26)	3(Normal)	0x68(27)	3(Normal)	0x6C(28)	3(Normal)
0x70(29)	3(Normal)	0x74(30)	3(Normal)	0x78(31)	3(Normal)	0x7C(32)	3(Normal)
0x80(33)	4(Medium)	0x84(34)	4(Medium)	0x88(35)	4(Medium)	0x8C(36)	4(Medium)
0x90(37)	4(Medium)	0x94(38)	4(Medium)	0x98(39)	4(Medium)	0x9C(40)	4(Medium)
0xA0(41)	5(Medium)	0xA4(42)	5(Medium)	0xA8(43)	5(Medium)	0xAC(44)	5(Medium)
0xB0(45)	5(Medium)	0xB4(46)	5(Medium)	0xB8(47)	5(Medium)	0xBC(48)	5(Medium)

Activate

ToS (DSCP) Value and Priority Queues

Setting	Description	Factory Default
Low/Normal/ Medium/High	Maps different TOS values to 4 different egress queues.	1 to 16: Low 17 to 32: Normal 33 to 48: Medium 49 to 64: High

4.5 Using Virtual LAN

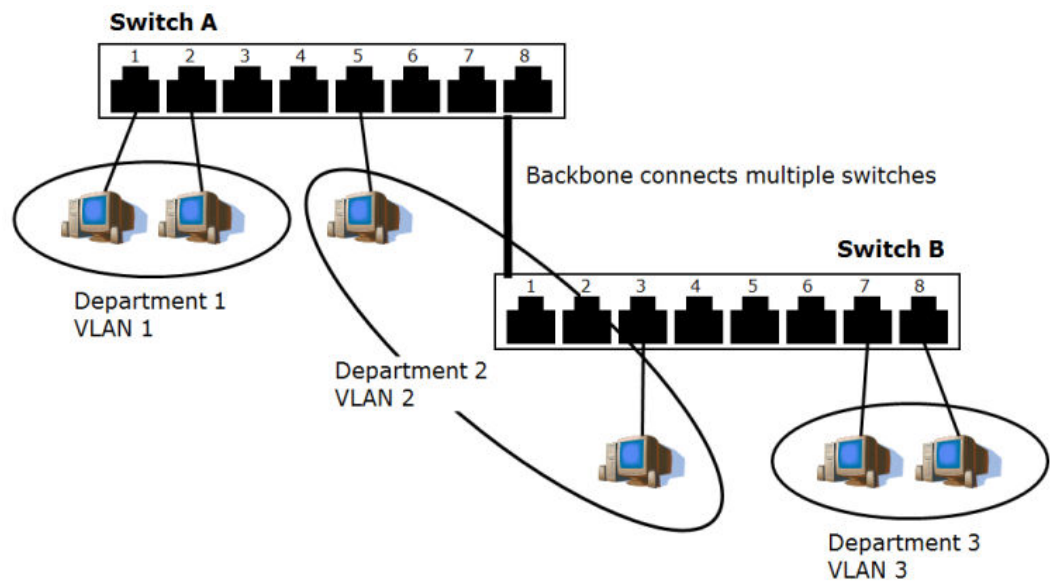
Setting up Virtual LANs (VLANs) on your VIPA switch increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

4.5.1 The Virtual LAN (VLAN) Concept

What is a VLAN?

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections—a limitation of traditional network design. With VLANs you can segment your network according into:

- **Departmental groups:**
You could have one VLAN for the marketing department, another for the finance department, and another for the product development department.
- **Hierarchical groups:**
You could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups:**
You could have one VLAN for email users and another for multimedia users.



Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

■ VLANs ease the relocation of devices on networks:

With traditional networks, network administrators spend much of their time dealing with moves and changes. If users move to a different subnetwork, the addresses of each host must be updated manually. With a VLAN setup, if a host originally on VLAN Marketing, for example, is moved to a port on another part of the network, and retains its original subnet membership, you only need to specify that the new port is on VLAN Marketing. You do not need to do any re-cabling.

■ VLANs provide extra security:

Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on VLAN Marketing needs to communicate with devices on VLAN Finance, the traffic must pass through a routing device or Layer 3 switch.

■ VLANs help control traffic:

With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether or not they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

VLANs and the Rack-mount switch

Your VIPA switch provides support for VLANs using IEEE Std 802.1Q-1998. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-1998 standard allows each port on your VIPA switch to be placed as follows:

- On a single VLAN defined in the VIPA switch
- On several VLANs simultaneously using 802.1Q tagging

The standard requires that you define the 802.1Q VLAN ID for each VLAN on your VIPA switch before the switch can use it to forward traffic:

Managing a VLAN

A new or initialized VIPA switch contains a single VLAN—the Default VLAN. This VLAN has the following definition:

- VLAN Name—Management VLAN
- 802.1Q VLAN ID—1 (if tagging is required)

All the ports are initially placed on this VLAN, and it is the only VLAN that allows you to access the management software of the VIPA switch over the network.

Communication Between VLANs

If devices connected to a VLAN need to communicate to devices on a different VLAN, a router or Layer 3 switching device with connections to both VLANs needs to be installed. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

VLANs: Tagged and Untagged Membership

The VIPA switch supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical link (backbone, trunk). When setting up VLANs you need to understand when to use untagged and tagged membership of VLANs. Simply put, if a port is on a single VLAN it can be an untagged member, but if the port needs to be a member of multiple VLANs, tagged membership must be defined. A typical host (e.g., clients) will be untagged members of one VLAN, defined as an *Access Port* in a VIPA switch, while inter-switch connections will be tagged members of all VLANs, defined as a *Trunk Port* in a VIPA switch. The IEEE Std 802.1Q-1998 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries

additional information that allows a switch to determine which VLAN the port belongs to. If a frame is carrying the additional information, it is known as a tagged frame. To carry multiple VLANs across a single physical link (backbone, trunk), each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong in which VLAN. To communicate between VLANs, a router must be used.

The VIPA switch supports three types of VLAN port settings:

■ **Access Port:**

The port connects to a single device that is not tagged. The user must define the default port PVID that assigns which VLAN the device belongs to. Once the ingress packet of this Access Port egresses to another Trunk Port (the port needs all packets to carry tag information), the VIPA switch will insert this PVID into this packet so the next 802.1Q VLAN switch can recognize it.

■ **Trunk Port:**

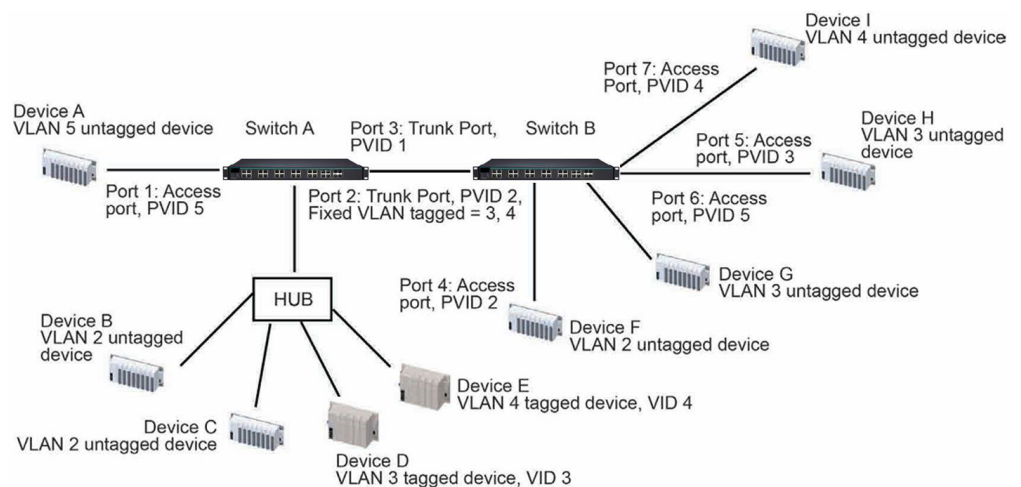
The port connects to a LAN that consists of untagged devices, tagged devices and/or switches and hubs. In general, the traffic of the Trunk Port must have a Tag. Users can also assign a PVID to a Trunk Port. The untagged packet on the Trunk Port will be assigned the port default PVID as its VID.

■ **Hybrid Port:**

The port is similar to a Trunk port, except users can explicitly assign tags to be removed from egress packets.

The following section illustrates how to use these ports to set up different applications.

4.5.2 Sample Applications of VLANs Using VIPA switches



In this application:

- Port 1 connects a single untagged device and assigns it to VLAN 5; it should be configured as Access Port with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2. One tagged device with VID 3 and one tagged device with VID 4. It should be configured as *Trunk Port* with PVID 2 for untagged device and Fixed VLAN (Tagged) with 3 and 4 for tagged device. Since each port can only have one unique PVID, all untagged devices on the same port must belong to the same VLAN.
- Port 3 connects with another switch. It should be configured as *Trunk Port* GVRP protocol will be used through the Trunk Port.
- Port 4 connects a single untagged device and assigns it to VLAN 2; it should be configured as Access Port with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3; it should be configured as Access Port with PVID 3.

- Port 6 connect a single untagged device and assigns it to VLAN 5; it should be configured as Access Port with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4; it should be configured as Access Port with PVID 4.

After the application is properly configured:

- Packets from Device A will travel through *Trunk Port 3* with tagged VID 5. Switch B will recognize its VLAN, pass it to port 6, and then remove tags received successfully by Device G, and vice versa.
- Packets from Devices B and C will travel through *Trunk Port 3* with tagged VID 2. Switch B recognizes its VLAN, passes it to port 4, and then removes tags received successfully by Device F, and vice versa.
- Packets from Device D will travel through *Trunk Port 3* with tagged VID 3. Switch B will recognize its VLAN, pass it to port 5, and then remove tags received successfully by Device H. Packets from Device H will travel through *Trunk Port 3* with PVID 3. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by Device D.
- Packets from Device E will travel through *Trunk Port 3* with tagged VID 4. Switch B will recognize its VLAN, pass it to port 7, and then remove tags received successfully by Device I. Packets from Device I will travel through *Trunk Port 3* with tagged VID 4. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by Device E.

4.5.3 VLAN Settings

To configure 802.1Q VLAN and port-based VLANs on the VIPA switch, use the VLAN Settings page to configure the ports.

VLAN Mode

Setting	Description	Factory Default
802.1Q VLAN	Set VLAN mode to 802.1Q VLAN	802.1Q VLAN
Port-based VLAN	Set VLAN mode to Port-based VLAN	

4.5.3.1 802.1Q VLAN Settings

802.1Q VLAN Settings

VLAN Mode: 802.1Q VLAN

Management VLAN ID: 1

Enable GVRP:

Port	Type	PVID	Fixed VLAN (Tagged)	Fixed VLAN (Untagged)	Forbidden VLAN
1	Access	1			
2	Trunk	1			
3	Hybrid	1			
4	Access	1			
5	Access	1			
6	Access	1			
7	Access	1			
8	Access	1			

Using Virtual LAN > VLAN Settings

Management VLAN ID

Setting	Description	Factory Default
VLAN ID from 1 to 4094	Assigns the VLAN ID of this VIPA switch.	1

Port Type

Setting	Description	Factory Default
Access	Port type is used to connect single devices without tags.	Access
Trunk	Select Trunk port type to connect another 802.1Q VLAN aware switch	
Hybrid	Select Hybrid port to connect another Access 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices and/or other switches/hubs.	



CAUTION!

For communication redundancy in the VLAN environment, set *Redundant Port Coupling Port* and *Coupling Control Port* as *Trunk Port* since these ports act as the backbone to transmit all packets of different VLANs to different VIPA switch units.

Port PVID

Setting	Description	Factory Default
VID ranges from 1 to 4094	Sets the default VLAN ID for untagged devices that connect to the port.	1

Fixed VLAN List (Tagged)

Setting	Description	Factory Default
VID ranges from 1 to 4094	This field will be active only when selecting the Trunk or Hybrid port type. Set the other VLAN ID for tagged devices that connect to the port. Use commas to separate different VIDs.	None

Fixed VLAN List (Untagged)

Setting	Description	Factory Default
VID range from 1 to 4094	This field will be active only when selecting the Hybrid port type. Set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs.	None

Forbidden VLAN List

Setting	Description	Factory Default
VID ranges from 1 to 4094	This field will be active only when selecting the Trunk or Hybrid port type. Set the other VLAN IDs that will not be supported by this port. Use commas to separate different VIDs.	None

4.5.3.2 Port-Based VLAN Settings

Check each specific port to assign its VLAN ID in the table. The maximum VLAN ID is the same as your number of switch ports.

Port-based VLAN Settings

VLAN Mode: Port-based VLAN

VLAN	Port																	
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	G1	G2
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Activate



IGMP Snooping will be disabled when Port-Based VLAN is enabled.

4.5.4 VLAN Table

VLAN Table

VLAN Mode
VLAN Mode: 802.1Q VLAN

Management VLAN
Management VLAN: 1

Current 802.1Q VLAN List

Index	VID	Joined Access Port	Joined Trunk Port	Joined Hybrid Port
1	1	1, 4, 5, 6, 7, 8,	2,	3,

VLAN Table

VLAN Mode

VLAN Mode Port-based VLAN

Current Port-based VLAN List

Index	VLAN	Joined Port
1	1	1, 4, 5, 6, 7, 8,
2	2	2,
3	3	3,

Use the 802.1Q VLAN table to review the VLAN groups that were created, *Joined Access Ports*, *Trunk Ports*, and *Hybrid Ports*, and use the *Port-based VLAN table* to review the VLAN group and *Joined Ports*.



The VIPA managed switches have a maximum of 64 VLAN settings.

4.6 Using Multicast Filtering

Multicast filtering improves the performance of networks that carry multicast traffic. This section explains multicasts, multicast filtering, and how multicast filtering can be implemented on your VIPA switch.

4.6.1 The Concept of Multicast Filtering

What is an IP Multicast?

A multicast is a packet sent by one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. If the network is set up correctly, a multicast can only be sent to an end-station or a subset of end-stations on a LAN or VLAN that belong to the multicast group. Multicast group members can be distributed across multiple subnets, so that multicast transmissions can occur within a campus LAN or over a WAN. In addition, networks that support IP multicast send only one copy of the desired information across the network until the delivery path that reaches group members diverges. To make more efficient use of network bandwidth, it is only at these points that multicast packets are duplicated and forwarded. A multicast packet has a multicast group address in the destination address field of the packet's IP header.

Benefits of Multicast

The benefits of using IP multicast are:

- It uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- It reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- It makes efficient use of network bandwidth and scales well as the number of multicast group members increases.
- Works with other IP protocols and services, such as Quality of Service (QoS).

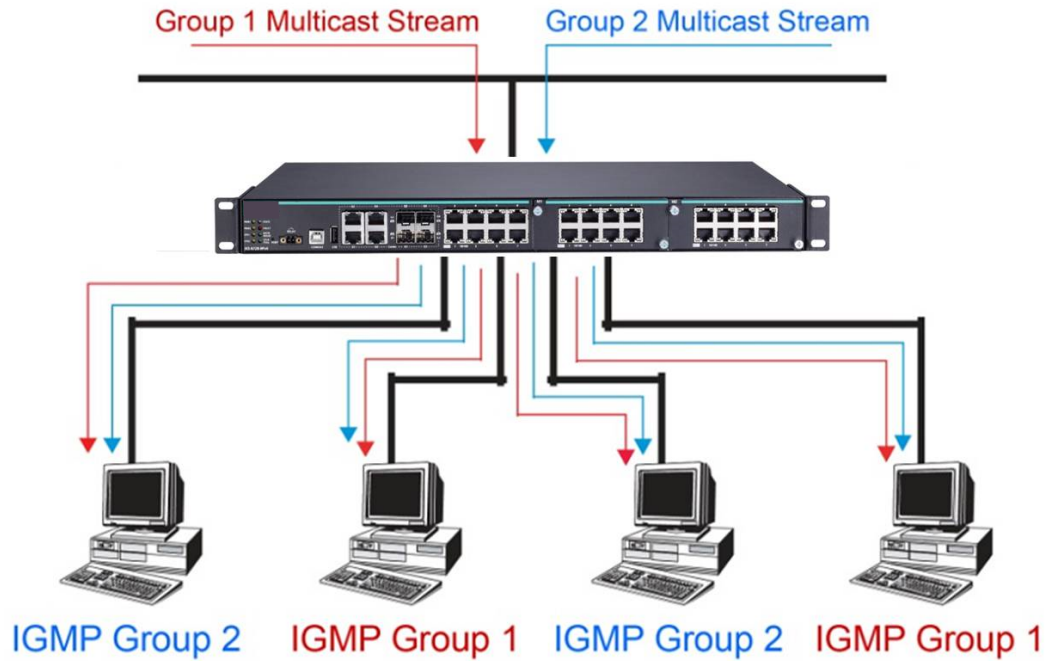
Multicast transmission makes more sense and is more efficient than unicast transmission for some applications. For example, multicasts are often used for video-conferencing, since high volumes of traffic must be sent to several end-stations at the same time, but where broadcasting the traffic to all end-stations would cause a substantial reduction in network performance. Furthermore, several industrial automation protocols, such as Allen-Bradley, EtherNet/IP, Siemens PROFIBUS, and Foundation Fieldbus HSE (High

Speed Ethernet), use multicast. These industrial Ethernet protocols use publisher/subscriber communications models by multicasting packets that could flood a network with heavy traffic. IGMP Snooping is used to prune multicast traffic so that it travels only to those end destinations that require the traffic, reducing the amount of traffic on the Ethernet LAN.

Multicast Filtering

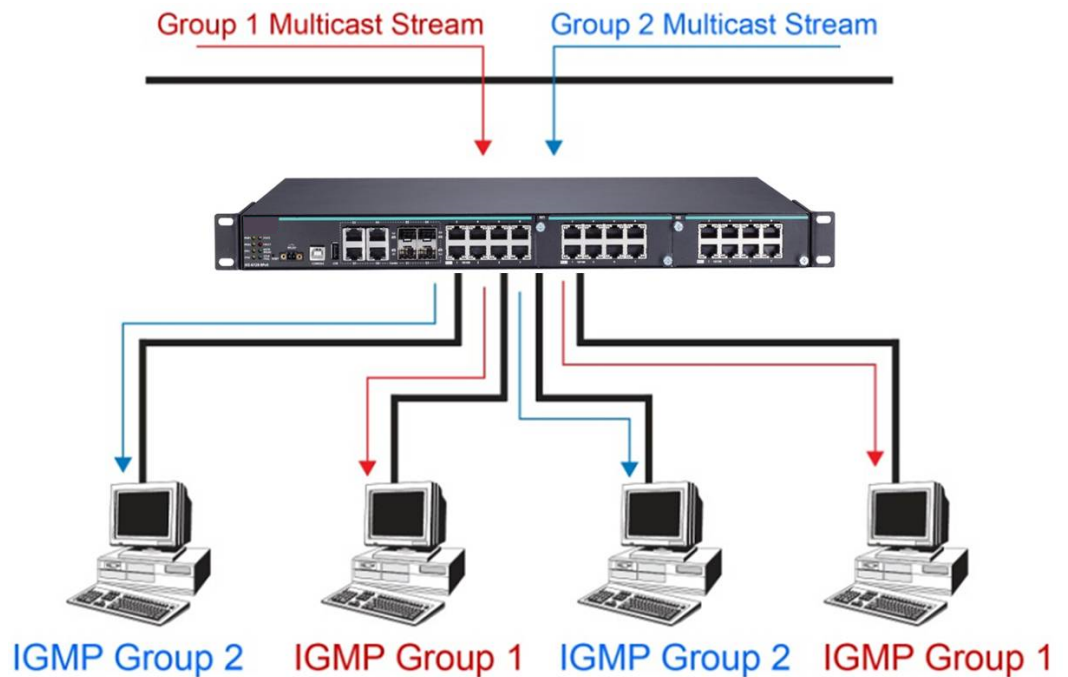
Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves without multicast filtering, and with multicast filtering.

Network without multicast filtering



All hosts receive the multicast traffic, even if they don't need it.

Network with multicast filtering



Hosts only receive dedicated traffic from other hosts belonging to the same group.

Multicast Filtering and VIPA's Industrial Rack-mount Switches

The VIPA switch has three ways to achieve multicast filtering: IGMP (Internet Group Management Protocol) Snooping, GMRP (GARP Multicast Registration Protocol), and adding a static multicast MAC manually to filter multicast traffic automatically.

■ Snooping Mode

Snooping Mode allows your switch to forward multicast packets only to the appropriate ports. The switch snoops on exchanges between hosts and an IGMP device, such as a router, to find those ports that want to join a multicast group, and then configures its filters accordingly.

■ IGMP Snooping Enhanced Mode

Snooping Enhanced Mode allows your switch to forward multicast packets to the VIPA switch's member port only. If you disable Enhanced Mode, data streams will run to the querier port as well as the member port.

■ Query Mode

Query mode allows the VIPA switch to work as the Querier if it has the lowest IP address on the subnetwork to which it belongs.



IGMP Snooping Enhanced mode is only provided in Layer 2 switches.

IGMP querying is enabled by default on the VIPA switch to ensure proceeding query election. Enable query mode to run multicast sessions on a network that does not contain IGMP routers (or queriers). Query mode allows users to enable IGMP snooping by VLAN ID. VIPA switches support IGMP snooping version 1, version 2 and version 3. Version 2 is compatible with version 1. The default setting is IGMP V1/V2.



VIPA Layer 3 switches are compatible with any device that conforms to the IGMP V2 and IGMP V3 device protocols. Layer 2 switches only support IGMP V1/V2.

IGMP Multicast Filtering

IGMP is used by IP-supporting network devices to register hosts with multicast groups. It can be used on all LANs and VLANs that contain a multicast capable IP router, and on other network devices that support multicast filtering. VIPA switches support IGMP version 1, 2 and 3. IGMP version 1 and 2 work as follows:

- The IP router (or querier) periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IP router, the router with the lowest IP address is the querier. A switch with IP address lower than the IP address of any other IGMP queriers connected to the LAN or VLAN can become the IGMP querier.
- When an IP host receives a query packet, it sends a report packet back that identifies the multicast group that the end-station would like to join.
- When the report packet arrives at a port on a switch with IGMP Snooping enabled, the switch knows that the port should forward traffic for the multicast group, and then proceeds to forward the packet to the router.
- When the router receives the report packet, it registers that the LAN or VLAN requires traffic for the multicast groups.
- When the router forwards traffic for the multicast group to the LAN or VLAN, the switches only forward the traffic to ports that received a report packet.

IGMP version comparison

IGMP Version	Main Features	Reference
V1	a. Periodic query	RFC-1112
V2	Compatible with V1 and adds: a. Group-specific query b. Leave group messages c. Resends specific queries to verify leave message was the last one in the group d. Querier election	RFC-2236

GMRP (GARP Multicast Registration Protocol)

VIPA switches support IEEE 802.1D-1998 GMRP (GARP Multicast Registration Protocol), which is different from IGMP (Internet Group Management Protocol). GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or de-register Group membership information dynamically. GMRP functions similarly to GVRP, except that GMRP registers multicast addresses on ports. When a port receives a GMRP-join message, it will register the multicast address to its database if the multicast address is not registered, and all the multicast packets with that multicast address are able to be forwarded from this port. When a port receives a GMRP-leave message, it will de-register the multicast address from its database, and all the multicast packets with this multicast address will not be able to be forwarded from this port.


Static Multicast MAC

Some devices may only support multicast packets, but not support either IGMP Snooping or GMRP. The VIPA switch supports adding multicast groups manually to enable multicast filtering.

Enabling Multicast Filtering

Use the serial console or web interface to enable or disable IGMP Snooping and IGMP querying. If IGMP Snooping is not enabled, then IP multicast traffic is always forwarded, flooding the network.

4.6.2 Configuring IGMP Snooping


IGMP Snooping will be disabled when Port-Based VLAN is enabled.

IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic, thereby reducing the amount of traffic on the Ethernet LAN.

Layer 2 switch setting page

IGMP Snooping Enable

Setting	Description	Factory Default
Enable/Disable	Checkmark the IGMP Snooping Enable checkbox near the top of the window to enable the IGMP Snooping function globally.	Disabled



You should enable IGMP Snooping if the network also uses non-VIPA 3rd party switches.

Query Interval

Setting	Description	Factory Default
Numerical value, input by the user	Sets the query interval of the Querier function globally. Valid settings are from 20 to 600 seconds.	125 seconds

IGMP Snooping Enhanced Mode

Setting	Description	Factory Default
Enable	IGMP Multicast packets will be forwarded to: <ul style="list-style-type: none"> ■ Auto-Learned Multicast Querier Ports ■ Member Ports 	Disable
Disable	IGMP Multicast packets will be forwarded to: <ul style="list-style-type: none"> ■ Auto-Learned Multicast Router Ports ■ Static Multicast Querier Ports ■ Querier Connected Ports ■ Member Ports 	



IGMP Snooping Enhanced Mode in networks composed entirely of VIPA switches

IGMP Snooping

Setting	Description	Factory Default
Enable/Disable	Enables or disables the IGMP Snooping function on that particular VLAN.	Enabled if IGMP Snooping is enabled globally

Querier

Setting	Description	Factory Default
Enable/Disable	Enables or disables the VIPA switch’s querier function.	Enabled if IGMP Snooping is enabled globally

Static Multicast Querier Port

Setting	Description	Factory Default
Select/Deselect	Select the ports that will connect to the multicast routers. These ports will receive all multicast packets from the source. This option is only active when IGMP Snooping is enabled.	Disabled



If a router or layer 3 switch is connected to the network, it will act as the Querier, and consequently this Querier option will be disabled on all VIPA layer 2 switches.

If all switches on the network are VIPA layer 2 switches, then only one layer 2 switch will act as Querier.

IGMP Table

The VIPA switch displays the current active IGMP groups that were detected. View IGMP group setting per VLAN ID on this page.

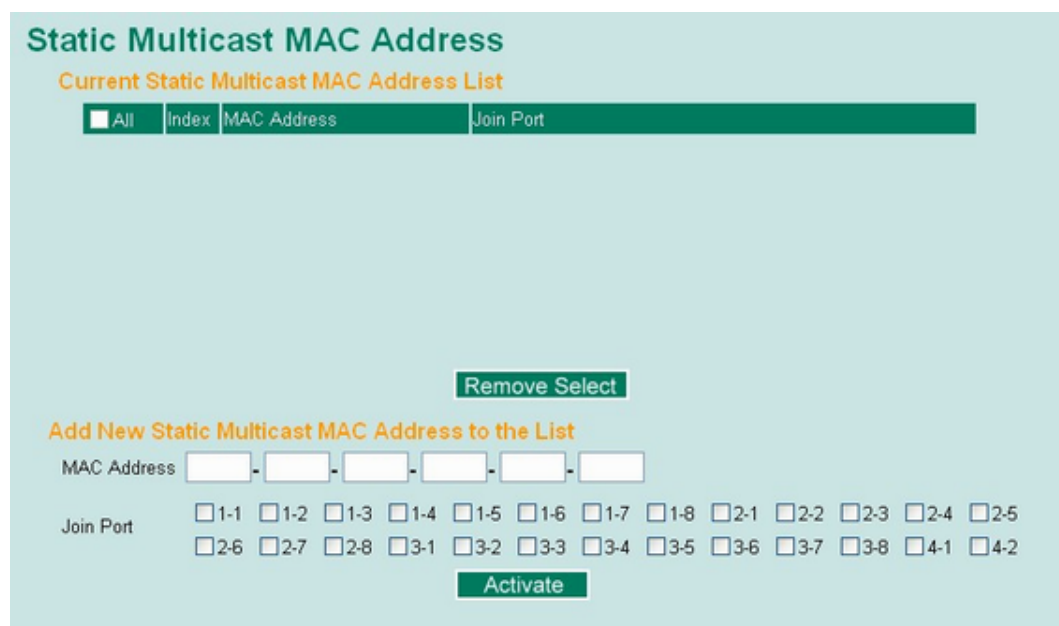
Layer 2 switch page

Current Active IGMP Groups

VID	Auto Learned Multicast Querier Port	Static Multicast Querier Port	Querier Connected Port	Act as Querier	Active IGMP Groups		
					IP	MAC	Members Port

4.6.3 Static Multicast MAC Addresses

Layer 2 switch page



Add New Static Multicast Address to the List

Setting	Description	Factory Default
MAC Address	Input the multicast MAC address of this host.	None

MAC Address

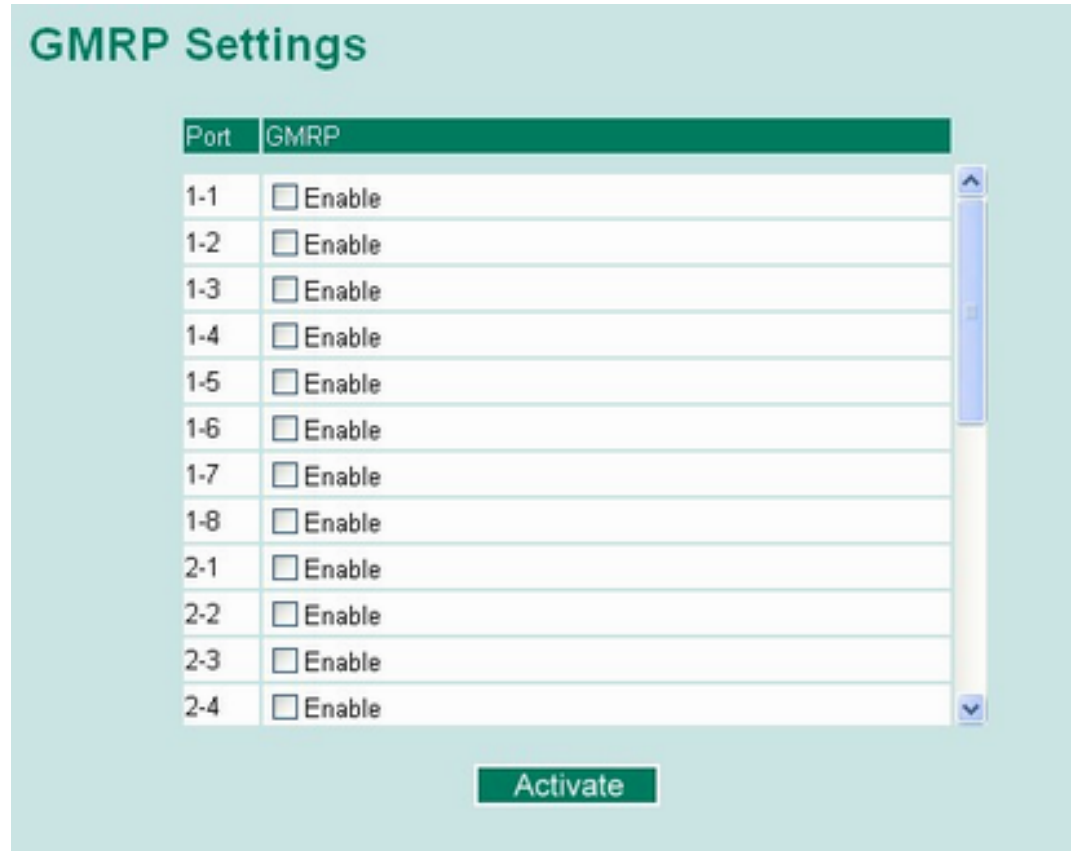
Setting	Description	Factory Default
Integer	Input the number of the VLAN that the host with this MAC address belongs to.	None

Join Port

Setting	Description	Factory Default
Select/Deselect	Checkmark the appropriate check boxes to select the join ports for this multicast group.	None

4.6.4 Configuring GMRP

GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or un-register Group membership information dynamically.

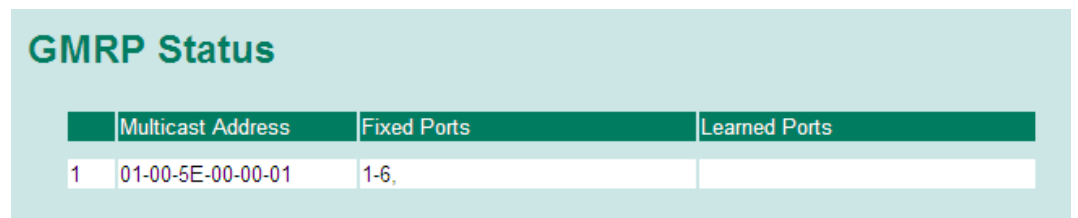


GMRP enable

Setting	Description	Factory Default
Enable/Disable	Enables or disables the GMRP function for the port listed in the Port column	Disable

4.6.5 GMRP Table

The VIPA switch displays the current active GMRP groups that were detected



Setting	Description
Fixed Ports	This multicast address is defined by static multicast.
Learned Ports	This multicast address is learned by GMRP.

4.7 Using Bandwidth Management

In general, one host should not be allowed to occupy unlimited bandwidth, particularly when the device malfunctions. For example, so-called "broadcast storms" could be caused by an incorrectly configured topology, or a malfunctioning device. VIPA industrial Ethernet switches not only prevents broadcast storms, but can also be configured to a different ingress rate for all packets, giving administrators full control of their limited bandwidth to prevent undesirable effects caused by unpredictable faults.

4.7.1 Configuring Bandwidth Management

Please note that two types of bandwidth management settings are available, depending on the specific model of switch.

Traffic Rate Limiting Settings					
Control Mode		Normal			
Port	Policy	Ingress Priority Queue Rate			
		Low	Normal	Medium	High
1	Limit Broadcast	8M	8M	8M	8M
2	Limit Broadcast	8M	8M	8M	8M
3	Limit Broadcast	8M	8M	8M	8M
4	Limit Broadcast	8M	8M	8M	8M
5	Limit Broadcast	8M	8M	8M	8M
6	Limit Broadcast	8M	8M	8M	8M
7	Limit Broadcast	8M	8M	8M	8M
G1	Limit Broadcast	8M	8M	8M	8M
G2	Limit Broadcast	8M	8M	8M	8M

Traffic Rate Limiting Settings

Control Mode	Description	Factory Default
Normal	Set the max. ingress rate limit for different packet types	Normal
Port Disable	When the ingress multicast and broadcast packets exceed the ingress rate limit, the port will be disabled for a certain period. During this period, all packets from this port will be discarded.	

Ingress Rate Limit - Normal

Policy	Description	Factory Default
Limit All	Select the ingress rate limit for different packet types from the following options: Not Limited, 128K, 256K, 512K, 1M, 2M, 4M, 8M	Limit Broadcast 8M
Limit Broadcast, Multicast, Flooded Unicast		
Limit Broadcast, Multicast		
Limit Broadcast		

Traffic Rate Limiting Settings

Control Mode Port Disable ▾

Port Disable Duration (1~65535s) 30

Port	Ingress(fps of multicast and broadcast packets.)
1	Not Limited ▾
2	Not Limited ▾
3	Not Limited ▾
4	Not Limited ▾
5	Not Limited ▾
6	Not Limited ▾

Activate

Ingress Rate Limit – Port Disable

Setting	Description	Factory Default
Port disable duration (1~65535 seconds)	When the ingress multicast and broadcast packets exceed the ingress rate limit, the port will be disabled for this period of time. During this time, all packets from this port will be discarded.	30 second
Ingress (fps)	Select the ingress rate (fps) limit for all packets from the following options: Not Limited, 4464, 7441, 14881, 22322, 37203, 52084, 74405	Not Limited

Egress Rate Limit

Port	Egress
1	Not Limited ▾
2	Not Limited ▾
3	Not Limited ▾
4	Not Limited ▾
5	Not Limited ▾
6	Not Limited ▾
7	Not Limited ▾
G1	Not Limited ▾
G2	Not Limited ▾
G3	Not Limited ▾

Activate

Setting	Description	Factory Default
Egress rate	Select the ingress rate limit (% of max. throughput) for all packets from the following options: Not Limited, 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%	Not Limited

Traffic Rate Limiting Settings

Traffic Rate Limiting Settings

Control Mode Normal ▾

Port	Ingress	Egress
1	Not Limited ▾	Not Limited ▾
2	Not Limited ▾	Not Limited ▾
3	Not Limited ▾	Not Limited ▾
4	Not Limited ▾	Not Limited ▾
5	Not Limited ▾	Not Limited ▾
6	Not Limited ▾	Not Limited ▾
7	Not Limited ▾	Not Limited ▾
8	Not Limited ▾	Not Limited ▾
9	Not Limited ▾	Not Limited ▾
10	Not Limited ▾	Not Limited ▾
11	Not Limited ▾	Not Limited ▾
12	Not Limited ▾	Not Limited ▾
13	Not Limited ▾	Not Limited ▾
14	Not Limited ▾	Not Limited ▾
15	Not Limited ▾	Not Limited ▾
16	Not Limited ▾	Not Limited ▾

Activate

Ingress and Egress Rate Limit - Normal

Setting	Description	Factory Default
Ingress rate	Select the ingress/egress rate limit (% of max. throughput) for all packets from the following options: Not Limited, 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%	Not Limited
Egress rate		

Traffic Rate Limiting Settings

Control Mode Port Disable ▾
 Period (1~65535s) 30

Port	Ingress
1	Not Limited ▾
2	Not Limited ▾
3	Not Limited ▾
4	Not Limited ▾
5	Not Limited ▾
6	Not Limited ▾
7	Not Limited ▾
8	Not Limited ▾
9	Not Limited ▾
10	Not Limited ▾
11	Not Limited ▾
12	Not Limited ▾
15	Not Limited ▾
16	Not Limited ▾

Activate

Ingress Rate Limit – Port Disable

Setting	Description	Factory Default
Period (1~65535 seconds)	When the ingress packets exceed the ingress rate limit, the port will be disabled for a certain period.	30 seconds
Ingress (frame per second)	Select the ingress rate (fps) limit for all packets from the following options: Not Limited, 4464, 7441, 14881, 22322, 37203, 52084, 74405	Not Limited

4.8 Using Auto Warning

Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that an industrial Ethernet switch that connects to these devices must provide system maintainers with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur. The VIPA switch supports different approaches to warn engineers automatically, such as email and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

4.8.1 Configuring Email Warning

The Auto Email Warning function uses e-mail to alert the user when certain user-configured events take place. Three basic steps are required to set up the Auto Warning function:

1. Configure Email Event Types

Select the desired *Event types* from the Console or Web Browser Event type page (a description of each event type is given later in the Email Alarm Events setting subsection).

2. Configure Email Settings

To configure a VIPA switch's email setup from the serial, Telnet, or web console, enter your Mail Server IP/Name (IP address or name), Account Name, Account Password, Retype New Password, and the email address to which warning messages will be sent.

3. Activate your settings and if necessary, test the email

After configuring and activating your VIPA switch's Event Types and Email Setup, you can use the *Test Email* function to see if your e-mail addresses and mail server address have been properly configured.

Configuring Event Types

Event Types can be divided into two basic groups: *System Events* and *Port Events*. System Events are related to the overall function of the switch, whereas Port Events are related to the activity of a specific port.

System Events	Warning e-mail is sent when...
Switch Cold Start	Power is cut off and then reconnected.
Switch Warm Start	VIPA switch is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Power Transition (On→Off)	VIPA switch is powered down.
Power Transition (Off→On)	VIPA switch is powered up.
DI1/DI2 (On→Off)	Digital Input 1/2 is triggered by on to off transition

Using Auto Warning > Configuring Email Warning

System Events	Warning e-mail is sent when...
DI1/DI2 (Off→On)	Digital Input 1/2 is triggered by off to on transition
Configuration Change Activated	Any configuration item has been changed.
Authentication Failure	An incorrect password was entered.
Comm. Redundancy Topology Changed	If any Spanning Tree Protocol switches have changed their position (applies only to the root of the tree). If the Master of the Turbo Ring has changed or the backup path is activated.

Port Events	Warning e-mail is sent when...
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%)	Enter a nonzero number if the port's Traffic-Overload item is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every Traffic-Duration seconds if the average Traffic-Threshold is surpassed during that time period.



The Traffic-Overload, Traffic-Threshold (%), and Traffic-Duration (sec.) Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a nonzero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.



The sender of warning e-mail messages will have the following form:

Managed-Redundant-Switch-00000@Switch_Location

where Managed-Redundant-Switch-00000 is the default Switch Name, 00000 is the VIPA switch's serial number, and Switch_Location is the default Server Location. ↪ Chap. 4.1 'Configuring Basic Settings' page 30

Configuring Email Settings

Mail Server IP/Name

Setting	Description	Factory Default
IP address	The IP Address of your email server.	None

SMTP Port

Setting	Description	Factory Default
SMTP port	Display the SMTP port number	25

Account Name

Setting	Description	Factory Default
Max. 45 of characters	Your email account.	None

Password Setting

Setting	Description	Factory Default
Disable/Enable to change password	To reset the password from the Web Browser interface, click the Change password check-box, type the Old password, type the New password, retype the New password, and then click [Activate] (Max. of 45 characters).	Disable
Old password	Type the current password when changing the password	None
New password	Type new password when enabled to change password; Max. 45 characters.	None
Retype password	If you type a new password in the Password field, you will be required to retype the password in the Retype new password field before updating the new password.	None

Email Address

Setting	Description	Factory Default
Max. of 30 characters	You can set up to 4 email addresses to receive alarm emails from the VIPA switch.	None

Send Test Email

After you complete the email settings, you should first click [Activate] to activate those settings, and then press the [Send Test Email] button to verify that the settings are correct.



Auto warning e-mail messages will be sent through an authentication protected SMTP server that supports the CRAM-MD5, LOGIN, and PAIN methods of SASL (Simple Authentication and Security Layer) authentication mechanism.

We strongly recommend not entering your Account Name and Account Password if auto warning e-mail messages can be delivered without using an authentication mechanism.

4.8.2 Configuring Relay Warning

The Auto Relay Warning function uses relay output to alert the user when certain user-configured events take place. There are two basic steps required to set up the Relay Warning function:

1. Configure Relay Event Types

Select the desired Event types from the Console or Web Browser Event type page (a description of each event type is given later in the Relay Alarm Events setting subsection).

2. Activate your settings

After completing the configuration procedure, you will need to activate your VIPA switch's Relay Event Types.

Configuring Event Types

Relay Warning Events Settings

System Events

Override Relay 1 Warning Settings
 Power Input 1 failure(On->Off) Disable
 DI 1 (Off) Disable DI 1 (On) Disable
 Turbo Ring Break Disable

Override Relay 2 Warning Settings
 Power Input 2 failure(On->Off) Disable
 DI 2 (Off) Disable DI 2 (On) Disable

Port Events

Port	Link	Traffic-Overload	Rx-Threshold(%)	Traffic-Duration(s)
1	Ignore	Disable	1	1
2	Ignore	Disable	1	1
3	Ignore	Disable	1	1
4	Ignore	Disable	1	1
5	Ignore	Disable	1	1
6	Ignore	Disable	1	1
7	Ignore	Disable	1	1
8	Ignore	Disable	1	1

Activate

Event Types can be divided into two basic groups: *System Events* and *'Port Events'*. System Events are related to the overall function of the switch, whereas Port Events are related to the activity of a specific port. The VIPA switch supports two relay outputs. You can configure which relay output is related to which events, which helps administrators identify the importance of the different events.

System Events	Warning Relay output is triggered when...
Power Transition (On→Off)	VIPA switch is powered down
Power Transition (Off→On)	VIPA switch is powered up
DI1/DI2 (On→Off)	Digital Input 1/2 is triggered by on to off transition
DI1/DI2 (Off→On)	Digital Input 1/2 is triggered by off to on transition
Turbo Ring Break	The Turbo Ring is broken. Only the MASTER switch of Turbo Ring will output warning relay.

Port Events	Warning e-mail is sent when...
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%)	Enter a nonzero number if the port's Traffic-Overload item is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every Traffic-Duration seconds if the average Traffic-Threshold is surpassed during that time period.

Override relay alarm settings

Check the checkbox to override the relay warning setting temporarily. Releasing the relay output will allow administrators to fix any problems with the warning condition



The Traffic-Overload, Traffic-Threshold (%), and Traffic-Duration (sec) Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a nonzero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

Warning List

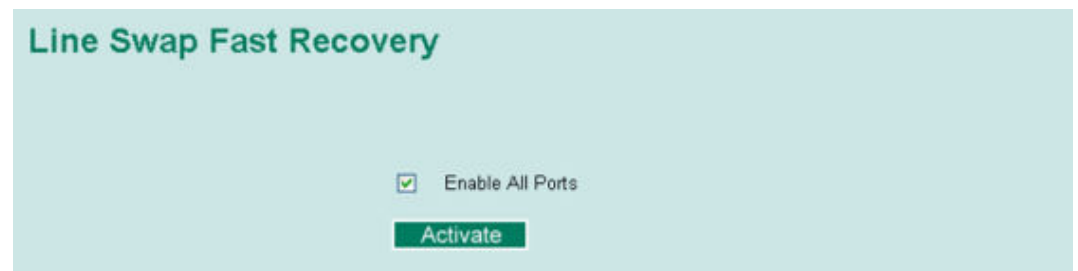
Use this table to see if any relay alarms have been issued.

Current Warning List	
Index	Event

4.9 Using Line-Swap-Fast-Recovery

The Line-Swap Fast Recovery function, which is enabled by default, allows the VIPA switch to return to normal operation extremely quickly after devices are unplugged and then re-plugged into different ports. The recovery time is on the order of a few milliseconds (compare this with standard commercial switches for which the recovery time could be on the order of several minutes). To disable the Line-Swap Fast Recovery function, or to re-enable the function after it has already been disabled, access either the Console utility's "Line-Swap recovery" page, or the Web Browser interface's "Line-Swap fast recovery" page, as shown below.

4.9.1 Configuring Line-Swap Fast Recovery



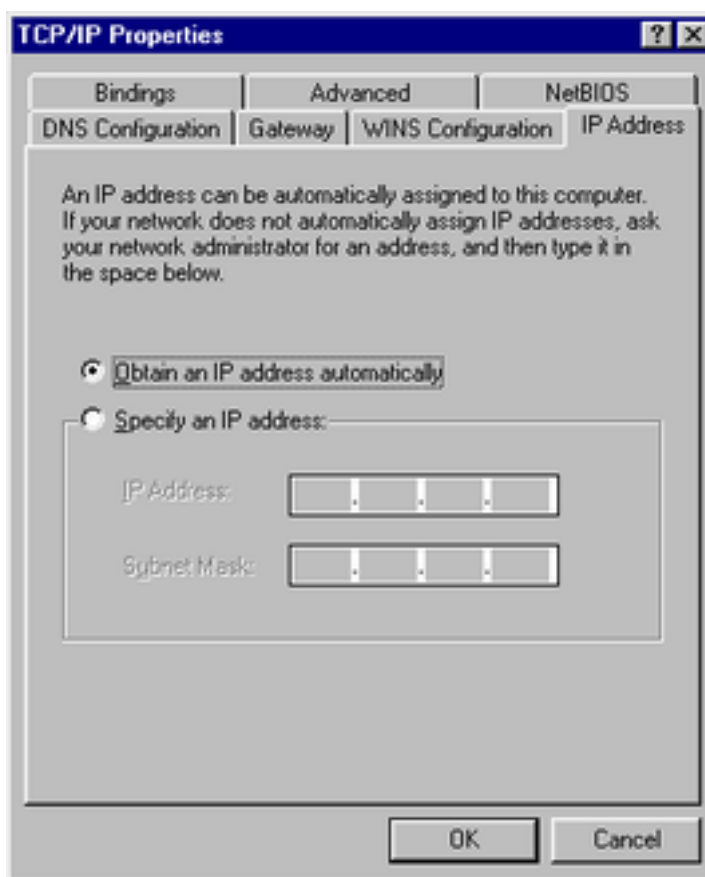
Enable Line-Swap-Fast-Recovery

Setting	Description	Factory Default
Enable/Disable	Checkmark the checkbox to enable the Line-Swap-Fast-Recovery function	Enable

4.10 Using Set Device IP

To reduce the effort required to set up IP addresses, the VIPA switch comes equipped with DHCP/BootP server and RARP protocol to set up IP addresses of Ethernet-enabled devices automatically. When enabled, the Set device IP function allows the VIPA switch to assign specific IP addresses automatically to connected devices that are equipped with DHCP Client or RARP protocol. In effect, the VIPA switch acts as a DHCP server by assigning a connected device with a specific IP address stored in its internal memory. Each time the connected device is switched on or rebooted, the VIPA switch sends the device the desired IP address. Take the following steps to use the Set device IP function:

Take the following steps to use the Set device IP function:



1. ➤ Set up the connected devices
 - Set up those Ethernet-enabled devices connected to the VIPA switch for which you would like IP addresses to be assigned automatically. The devices must be configured to obtain their IP address automatically.
 - The devices' configuration utility should include a setup page that allows you to choose an option similar to the *Obtain an IP address automatically* option.
 - For example, Windows' TCP/IP Properties window is shown at the right. Although your device's configuration utility may look quite a bit different, this figure should give you some idea of what to look for.
 - You also need to decide which of the VIPA switch's ports your Ethernet-enabled devices will be connected to. You will need to set up each of these ports separately, as described in the following step.
2. ➤ Configure the VIPA switch's *Set device IP* function, either from the Console utility or from the Web Browser interface. In either case, you simply need to enter the *Desired IP* for each port that needs to be configured.
3. ➤ Be sure to activate your settings before exiting.
 - When using the Web Browser interface, activate by clicking on the Activate button.
 - When using the Console utility, activate by first highlighting the [Activate] menu option, and then press [Enter]. You should receive the "Set device IP settings are now active! (Press any key to continue)" message.

4.10.1 Configuring Set Device IP

Automatic Set Device IP by DHCP/BootP/RARP

Automatic Set Device IP by DHCP/BootP/RARP

Port	Device's current IP	Active function	Desired IP address
1-1	NA	--	<input type="text"/>
1-2	NA	--	<input type="text"/>
1-3	NA	--	<input type="text"/>
1-4	NA	--	<input type="text"/>
1-5	NA	--	<input type="text"/>
1-6	NA	--	<input type="text"/>
1-7	NA	--	<input type="text"/>
1-8	NA	--	<input type="text"/>
2-1	NA	--	<input type="text"/>
2-2	NA	--	<input type="text"/>
2-3	NA	--	<input type="text"/>
2-4	NA	--	<input type="text"/>

Desired IP Address

Setting	Description	Factory Default
IP Address	Set the desired IP of connected devices.	None

4.10.2 Configuring DHCP Relay Agent

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers. The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP sever on a remote subnet, or those that are not located on the local subnet.

DHCP Relay Agent (Option 82)

Option 82 is used by the relay agent to insert additional information into the client's DHCP request. The Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers can recognize the Relay Agent Information option and use the information to implement IP addresses to Clients. When Option 82 is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified. The Option 82 information contains 2 sub-options, Circuit ID and Remote ID, which define the relationship between the end device IP and the DHCP Option 82 server. The Circuit ID is a 4-byte number generated by the Ethernet switch—a combination of physical port number and VLAN ID. The format of the Circuit ID is shown below:

FF-VV-VV-PP

This is where the first byte FF is fixed to "01", the second and the third byte VV-VV is formed by the port VLAN ID in hex, and the last byte PP is formed by the port number in hex. For example:

01-00-0F-03 is the *Circuit ID* of port number 3 with port VLAN ID 15.

The *Remote ID* identifies the relay agent itself and can be one of the following:

- The IP address of the relay agent.
- The MAC address of the relay agent.
- A combination of IP address and MAC address of the relay agent.
- A user-defined string.

DHCP Relay Agent

Server IP Address

1st Server

2nd Server

3rd Server

4th Server

DHCP Option 82

Enable Option 82

Type IP

Value 192.168.127.253

Display C0A87FFD

DHCP Function Table

Port	Circuit-ID	Option 82
1-1	01000101	<input type="checkbox"/> Enable
1-2	01000102	<input type="checkbox"/> Enable
1-3	01000103	<input type="checkbox"/> Enable
1-4	01000104	<input type="checkbox"/> Enable
1-5	01000105	<input type="checkbox"/> Enable
1-6	01000106	<input type="checkbox"/> Enable
1-7	01000107	<input type="checkbox"/> Enable

Activate

Server IP Address

1st Server

Setting	Description	Factory Default
IP address for the 1st DHCP server	Assigns the IP address of the 1st DHCP server that the switch tries to access.	None

2nd Server

Setting	Description	Factory Default
IP address for the 2nd DHCP server	Assigns the IP address of the 2nd DHCP server that the switch tries to access.	None

3rd Server

Setting	Description	Factory Default
IP address for the 3rd DHCP server	Assigns the IP address of the 3rd DHCP server that the switch tries to access.	None

Using Diagnosis

4th Server

Setting	Description	Factory Default
IP address for the 4th DHCP server	Assigns the IP address of the 4th DHCP server that the switch tries to access.	None

DHCP Option 82

Enable Option 82

Setting	Description	Factory Default
Enable or Disable	Enable or disable the DHCP Option 82 function.	Disable

Type

Setting	Description	Factory Default
IP	Uses the switch's IP address as the remote ID sub.	IP
MAC	Uses the switch's MAC address as the remote ID sub.	IP
Client-ID	Uses a combination of the switch's MAC address and IP address as the remote ID sub.	IP
Other	Uses the user-designated ID sub.	IP

Value

Setting	Description	Factory Default
Max. 12 characters	Displays the value that was set. Complete this field if type is set to Other.	Switch IP address

Display

Setting	Description	Factory Default
read-only	The actual hexadecimal value configured in the DHCP server for the Remote-ID. This value is automatically generated according to the Value field. Users cannot modify it.	COA87FFD

DHCP Function Table

Enable

Setting	Description	Factory Default
Enable or Disable	Enable or disable the DHCP Option 82 function for this port.	Disable

4.11 Using Diagnosis

The VIPA switch provides three important tools for administrators to diagnose network systems.

4.11.1 Mirror Port

The *Mirror Port* function can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation. Using a mirror port allows the network administrator to *sniff* the observed port to keep tabs on network activity.

Mirror Port Settings

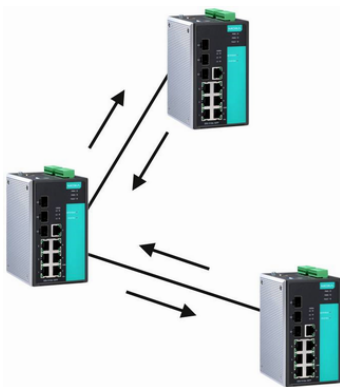
Setting	Description
Monitored Port	Select the number of one port whose network activity will be monitored.
Watch Direction	Select one of the following two watch direction options: <ul style="list-style-type: none"> ■ <i>Input data stream:</i> Select this option to monitor only those data packets coming into the VIPA switch's port. ■ <i>Output data stream:</i> Select this option to monitor only those data packets being sent out through the VIPA switch's port. ■ <i>Bi-directional:</i> Select this option to monitor data packets both coming into, and being sent out through, the VIPA switch's port.
Mirror Port	Select the number of the port that will be used to monitor the activity of the monitored port.

4.11.2 Ping

The *Ping* function uses the ping command to give users a simple but powerful tool for troubleshooting network problems. The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the VIPA switch itself. In this way, the user can essentially sit on top of the VIPA switch and send ping commands out through its ports. To use the Ping function, type in the desired IP address, and then press [Enter] from the Console utility, or click [Ping] when using the Web Browser interface.

4.11.3 LLDP Function

Overview



LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a VIPA managed switch, to periodically send its system and configuration information to its neighbours. Because of this, all LLDP devices are kept informed of each other's status and configuration and with SNMP, this information can be transferred to VIPA's MXview for auto-topology and network visualization. From the switch's web interface, you can enable or disable LLDP, and set the LLDP transmit interval. In addition, you can view each switch's neighbour-list, which is reported by its network neighbours. Most importantly, enabling the LLDP function allows VIPA's MXview to automatically display the network's topology and system setup details, such as VLAN and Trunking, for the entire network.

Configuring LLDP Settings



General Settings

LLDP

Setting	Description	Factory Default
Enable or Disable	Enables or disables the LLDP function.	Enable

Message Transmit Interval

Setting	Description	Factory Default
5 to 32768 sec.	Sets the transmit interval of LLDP messages, in seconds.	30 (seconds)

LLDP Table

The LLDP Table displays the following information:

Port	The port number that connects to the neighbor device.
Neighbor ID	A unique entity (typically the MAC address) that identifies a neighbor device.

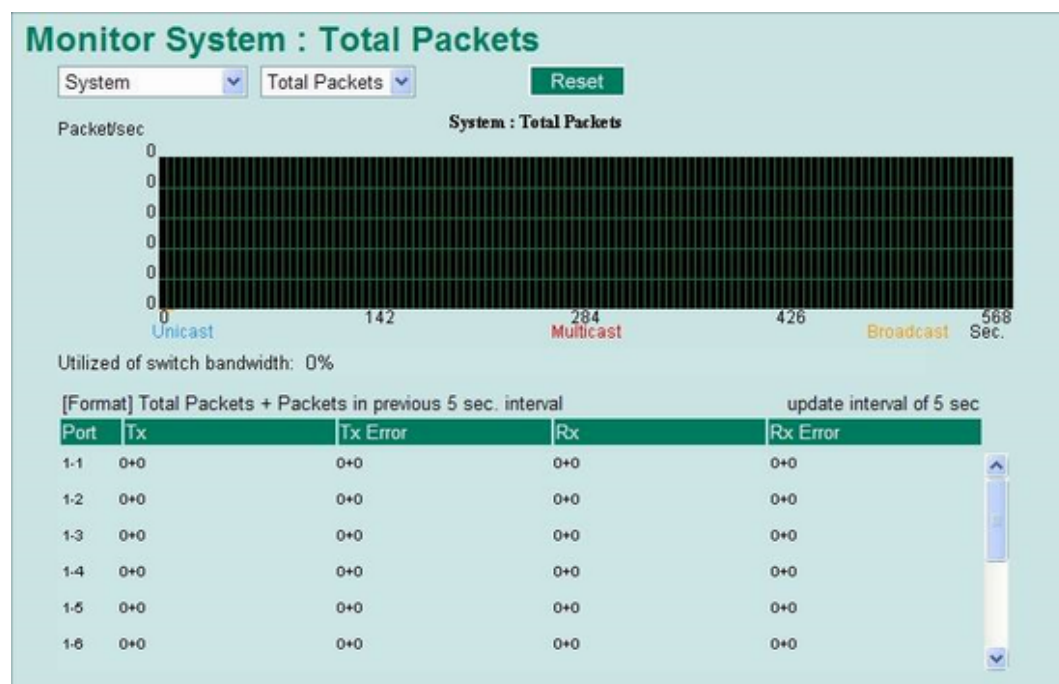
Neighbor Port	The port number of the neighbor device.
Neighbor Port Description	A textual description of the neighbor device's interface.
Neighbor System	Hostname of the neighbor device.

4.12 Using Monitor

You can monitor statistics in real time from the VIPA switch's web console and serial console.

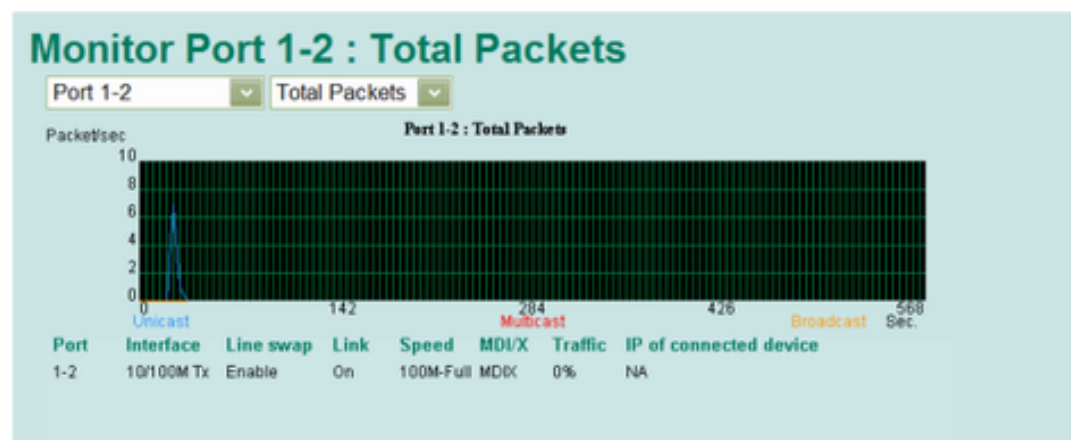
4.12.1 Monitor by Switch

- Access the Monitor by selecting 'System' from the left selection bar.
 - ⇒ Monitor by System allows the user to view a graph that shows the combined data transmission activity of all of the VIPA switch's 18 ports.
- Click one of the four options, 'Total Packets', 'TX Packets', 'RX Packets' or 'Error Packets', to view transmission activity of specific types of packets.
 - ⇒ Recall that TX Packets are packets sent out from the VIPA switch, RX Packets are packets received from connected devices, and Error Packets are packets that did not pass TCP/IP's error checking algorithm. The Total Packets option displays a graph that combines TX, RX, and TX Error, RX Error Packets activity. The graph displays data transmission activity by showing 'Packets/s' (i.e., packets per second, or pps) versus 'sec.' (seconds). In fact, three curves are displayed on the same graph: Uni-cast packets (in red color), 'Multi-cast' packets (in green color), and 'Broad-cast' packets (in blue color). The graph is updated every few seconds, allowing the user to analyse data transmission activity in real-time.



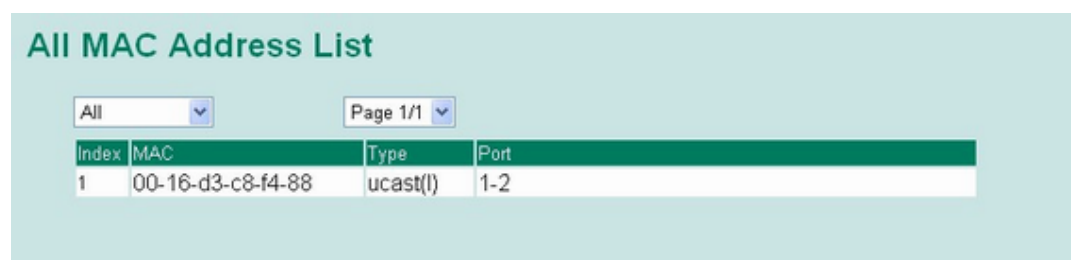
4.12.2 Monitor by Port

- ➔ Access the Monitor by Port function by selecting ' ALL 10/100M or 1G Ports' or 'Port i', in which 'i = 1, 2, ..., G2', from the left pull-down list.
 - ⇒ The 'Port i' options are identical to the Monitor by System function discussed above, in that users can view graphs that show All Packets, TX Packets, RX Packets, or Error Packets activity, but in this case, only for an individual port. The 'All Ports' option is essentially a graphical display of the individual port activity that can be viewed with the Console Monitor function discussed above. The All Ports option shows three vertical bars for each port. The height of the bar represents 'Packets/s' for the type of packet, at the instant the bar is being viewed. That is, as time progresses, the height of the bar moves up or down so that the user can view the change in the rate of packet transmission. The blue colored bar shows 'Uni-cast' packets, the red colored bar shows 'Multi-cast' packets, and the orange colored bar shows 'Broad-cast' packets. The graph is updated every few seconds, allowing the user to analyse data transmission activity in real-time.



4.13 Using the MAC Address Table

This section explains the information provided by the VIPA switch's MAC address table.



The MAC Address table can be configured to display the following VIPA switch MAC address groups, which are selected from the drop-down list:

ALL	Select this item to show all of the VIPA switch's MAC addresses.
ALL Learned	Select this item to show all of the VIPA switch's Learned MAC addresses.
ALL Static Lock	Select this item to show all of the VIPA switch's Static Lock MAC addresses.
ALL Static	Select this item to show all of the VIPA switch's Static, Static Lock, and Static Multicast MAC addresses.

ALL Static Multicast	Select this item to show all of the VIPA switch's Static Multicast MAC addresses.
Port x	Select this item to show all of the MAC addresses dedicated ports.

The table displays the following information:

MAC	This field shows the MAC address.
Type	This field shows the type of this MAC address.
Port	This field shows the port that this MAC address belongs to.

4.14 Using Event Log

Event Log Table

Page 67/67

Index	Bootup	Date	Time	System Startup Time	Event
991	419	--	--	0d0h42m37s	Port 1-2 link off
992	420	--	--	0d0h0m1s	Cold start
993	420	--	--	0d0h0m3s	Port 3-8 link on
994	420	--	--	0d0h1m14s	192.168.127.1 admin Auth. ok
995	420	--	--	0d0h1m54s	Port 3-8 link off
996	421	--	--	0d0h0m1s	Cold start
997	421	--	--	0d0h0m4s	Port 1-2 link on
998	421	--	--	0d0h0m12s	192.168.127.1 admin Auth. ok
999	421	--	--	0d0h53m26s	Configuration change activated
1000	421	--	--	0d0h53m33s	192.168.127.1 admin Auth. ok

Clear

Event Log Table

Setting	Description
Bootup	This field shows how many times the VIPA switch has been rebooted or cold started.
Date	The date is updated based on how the current date is set in the Basic Setting page.
Time	The time is updated based on how the current time is set in the Basic Setting page.
System Startup Time	The system startup time related to this event.
Events	Events that have occurred.



The following events will be recorded into the VIPA switch's Event Log Table:

- Cold start
- Warm start
- Configuration change activated
- Power 1/2 transition (Off (On), Power 1/2 transition (On (Off))
- Authentication fail
- Topology changed
- Master setting is mismatched
- Port traffic overload
- dot1x Auth Fail
- Port link off/on

4.15 Using Syslog

The Syslog function provides the event logs for the syslog server. The function supports 3 configurable syslog servers and syslog server UDP port numbers. When an event occurs, the event will be sent as a syslog UDP packet to the specified syslog servers.

Syslog Settings

Syslog Server 1	<input style="width: 90%;" type="text"/>	
Port Destination	<input style="width: 80%;" type="text" value="514"/> (1~65535)	
Syslog Server 2	<input style="width: 90%;" type="text"/>	
Port Destination	<input style="width: 80%;" type="text" value="514"/> (1~65535)	
Syslog Server 3	<input style="width: 90%;" type="text"/>	
Port Destination	<input style="width: 80%;" type="text" value="514"/> (1~65535)	

Syslog Server 1/2/3

Setting	Description	Factory Default
IP Address	Enter the IP address of Syslog server 1/2/3, used by your network.	None
Port Destination (1 to 65535)	Enter the UDP port of Syslog server 1/2/3.	514



The following events will be recorded into the VIPA switch's Event Log table, and will then be sent to the specified Syslog Server:

- Cold start*
- Warm start*
- Configuration change activated*
- Power 1/2 transition (Off (On), Power 1/2 transition (On (Off))*
- Authentication fail*
- Topology changed*
- Master setting is mismatched*
- Port traffic overload*
- dot1x Auth Fail*
- Port link off/on*

5 Communication Redundancy

5.1 Introduction to Communication Redundancy

Setting up Communication Redundancy on your network helps protect critical links against failure, protects against network loops, and keeps network downtime at a minimum.

Communication Redundancy allows you to set up redundant loops in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged. This is a particularly important feature for industrial applications, since it could take several minutes to locate the disconnected or severed cable. For example, if the VIPA switch is used as a key communications component of a production line, several minutes of downtime could cause a big loss in production and revenue. The VIPA switch supports three different protocols to support this communication redundancy function:

- Turbo Ring and Turbo Ring V2
- Turbo Chain
- Rapid Spanning Tree and Spanning Tree Protocols (IEEE 802.1W/802.1D-2004)

When configuring a redundant ring, all switches on the same ring must be configured to use the same redundancy protocol. You cannot mix the Turbo Ring, Turbo Ring V2, and STP/RSTP protocols on the same ring. The following table lists the key differences between the features of each protocol. Use this information to evaluate the benefits of each, and then determine which features are most suitable for your network.

	Turbo Ring	Turbo Ring V2	Turbo Chain	STP	RSTP
Topology	Ring	Ring	Chain	Ring, Mesh	Ring, Mesh
Fast Ethernet Recovery Time	< 300 ms	< 20 ms	< 20 ms	Up to 30 sec.	Up to 5 sec.
Gigabit Ethernet Recovery Time		< 50 ms	< 50 ms		



All of VIPA's managed switches now support three proprietary Turbo Ring protocols:

- Turbo Ring refers to the original version of VIPA's proprietary redundant ring protocol, which has a recovery time of under 300 ms.
- Turbo Ring V2 refers to the new generation Turbo Ring, which has a recovery time of under 20 ms for Fast Ethernet ports and under 50 ms for Gigabit Ethernet ports.
- Turbo Chain is a new VIPA proprietary protocol with unlimited flexibility that allows you to construct any type of redundant network topology. The recovery time is under 20 ms for Fast Ethernet ports and under 50 ms for Gigabit Ethernet ports. To achieve a recovery time under 50 ms in a Gigabit Turbo Chain, we recommend using a Gigabit fiber port as Head port.

In this manual, we use the terminology Turbo Ring and Turbo Ring V2 to differentiate between rings configured for one or the other of these protocols.

Gigabit Ethernet Redundant Ring Capability (< 50 ms)



Ethernet has become the default data communications medium for industrial automation applications. In fact, Ethernet is often used to integrate video, voice, and high-rate industrial application data transfers into one network. VIPA switches come equipped with a redundant Gigabit Ethernet protocol called Gigabit Turbo Ring. With Gigabit Turbo Ring, if any segment of the network gets disconnected, your automation system will be back to normal in less than 300 ms (Turbo Ring) or 50 ms (Turbo Ring V2).



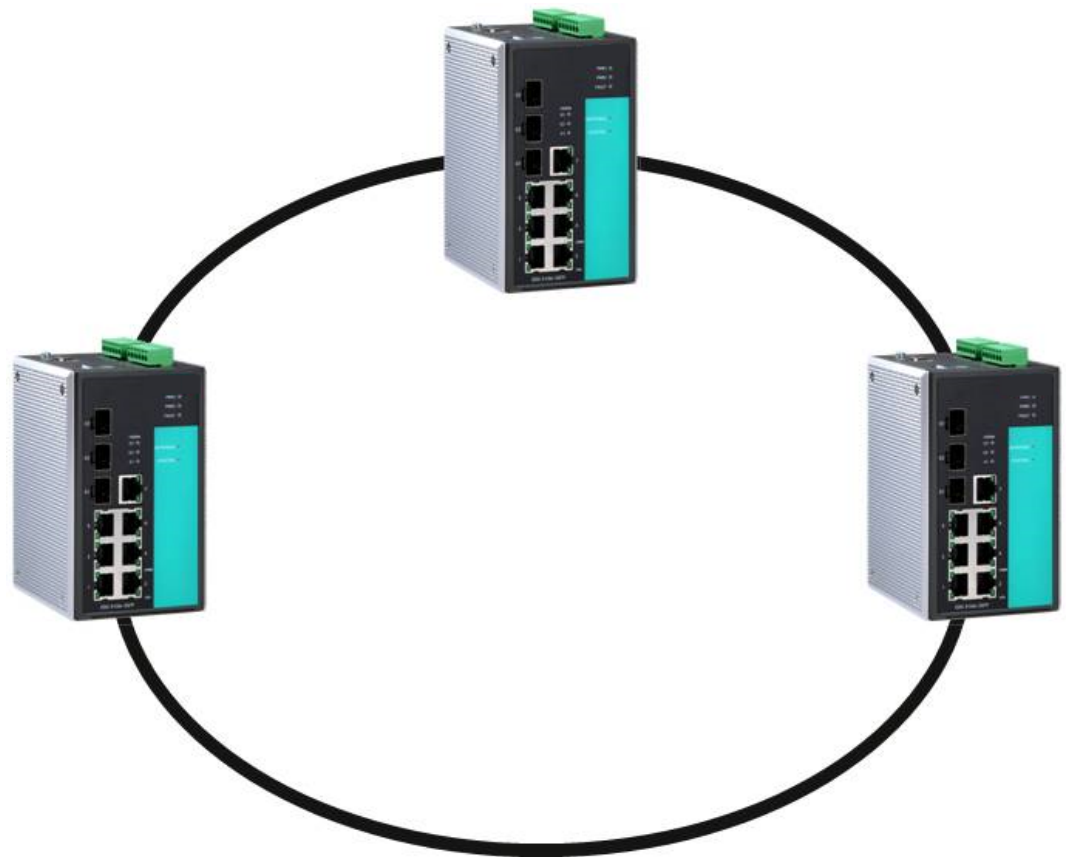
Port trunking and Turbo Ring can be enabled simultaneously to form a backbone. Doing so will increase the bandwidth of the backbone, and also provide redundancy. For example, suppose that two physical ports, 1 and 2, are trunked to form trunk group Trk1, and then Trk1 is set as one Turbo Ring path. If port 1 gets disconnected, the remaining trunked port, port 2, will share the traffic. If ports 1 and 2 are both disconnected, the Turbo Ring will create a backup path within 300 ms.

5.2 Turbo Ring

5.2.1 The Turbo Ring Concept

VIPA developed the proprietary Turbo Ring protocol to optimize communication redundancy and achieve a faster recovery time on the network. The Turbo Ring and Turbo Ring V2 protocols identify one switch as the master of the network, and then automatically block packets from travelling through any of the network's redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network.

5.2.2 Setting up Turbo Ring or Turbo Ring V2



1. Select any two ports as redundant ports.
2. Connect the redundant ports to form the Turbo Ring.

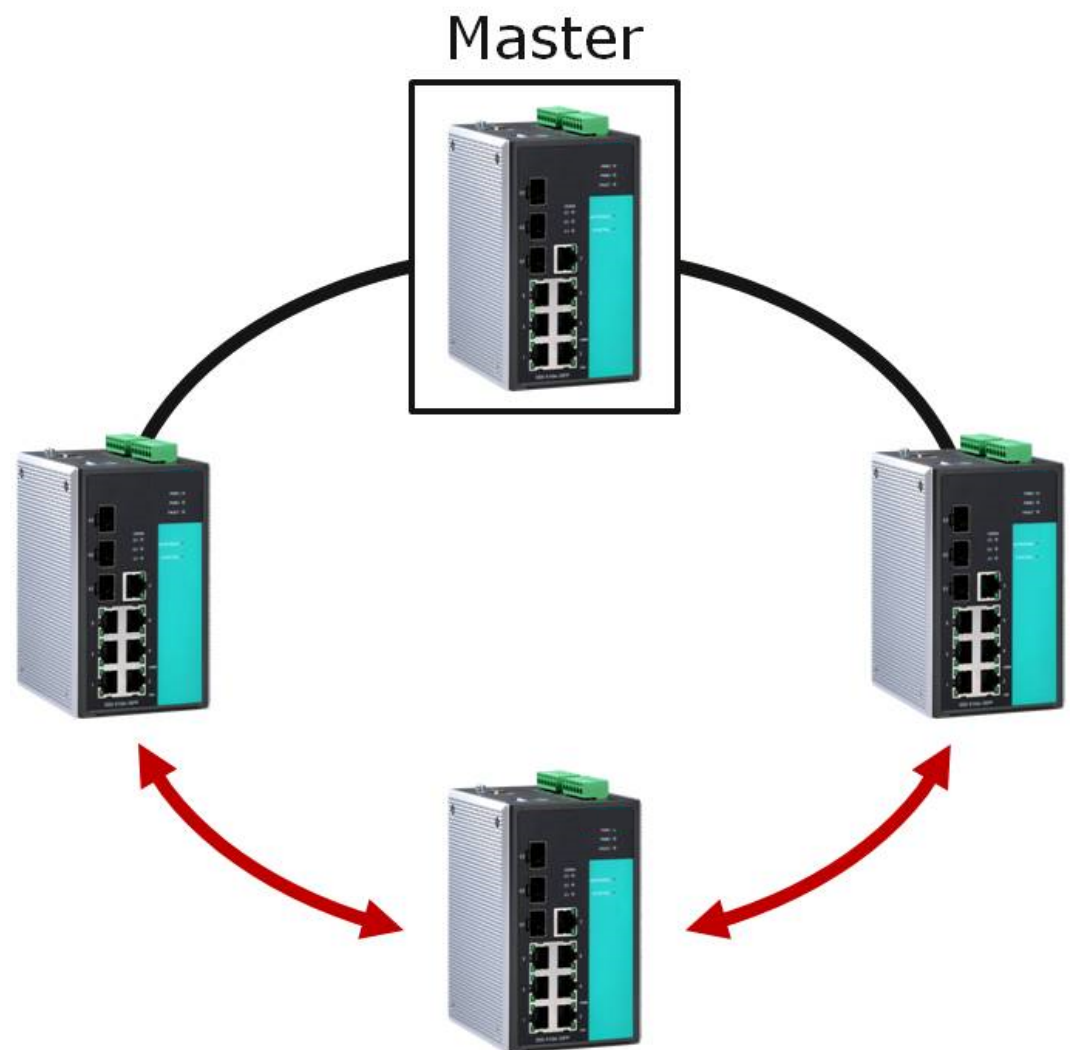
The user does not need to configure any of the switches as the master to use Turbo Ring or Turbo Ring V2. If none of the switches in the ring is configured as the **master**, then the protocol will automatically assign master status to one of the switches. In fact, the master is only used to identify which segment in the redundant ring acts as the backup path. In the following subsections, we explain how the redundant path is selected for rings configured for Turbo Ring, and Turbo Ring V2.

Determining the Redundant Path of a "Turbo Ring" Ring

In this case, the redundant segment (i.e., the segment that will be blocked during normal operation) is determined by the number of switches in the ring, and where the ring master is located.

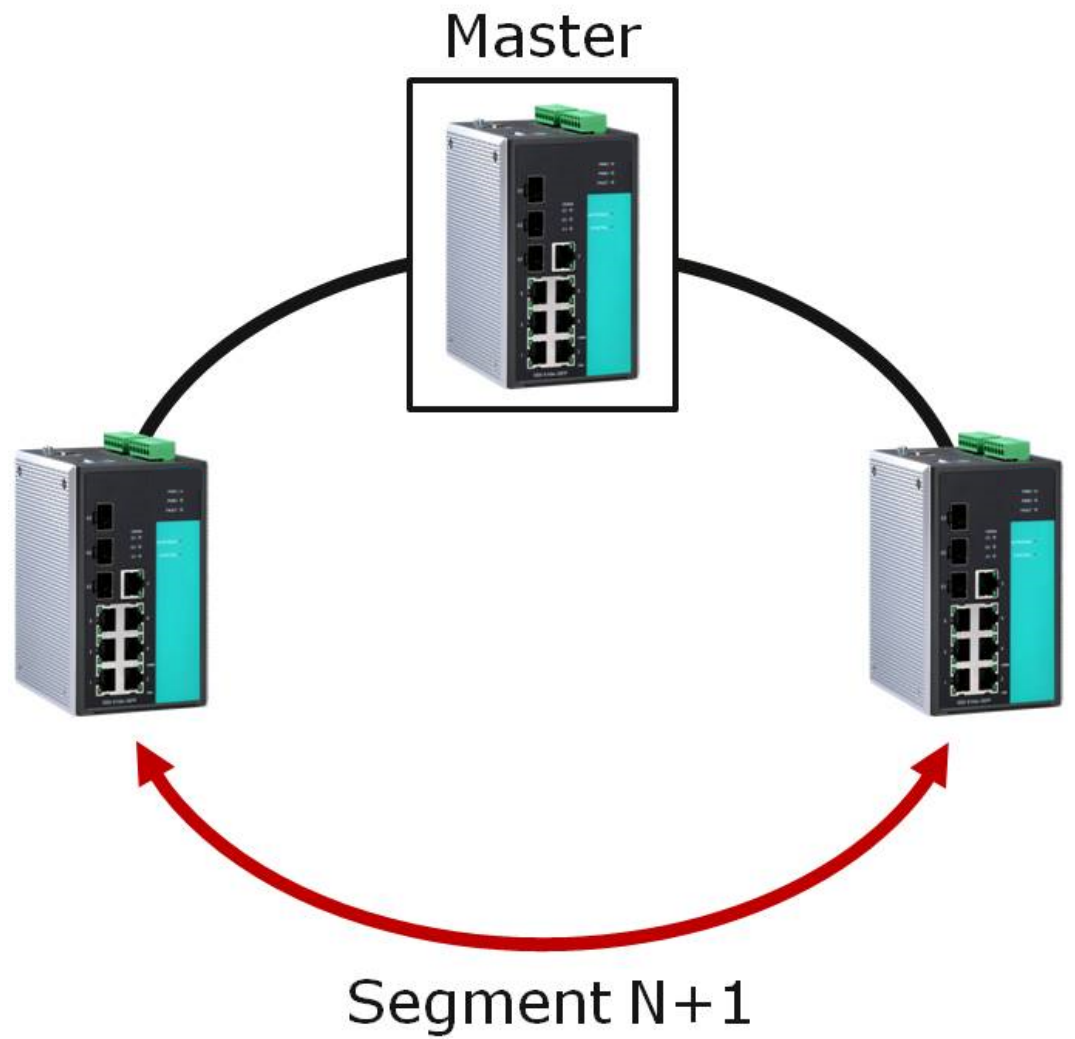
■ When the Number of Switches in the Turbo Ring is Even

If there are $2N$ switches (an even number) in the "Turbo Ring" ring, then the backup segment is one of the two segments connected to the $(N+1)$ st switch (i.e., the switch directly opposite the master).



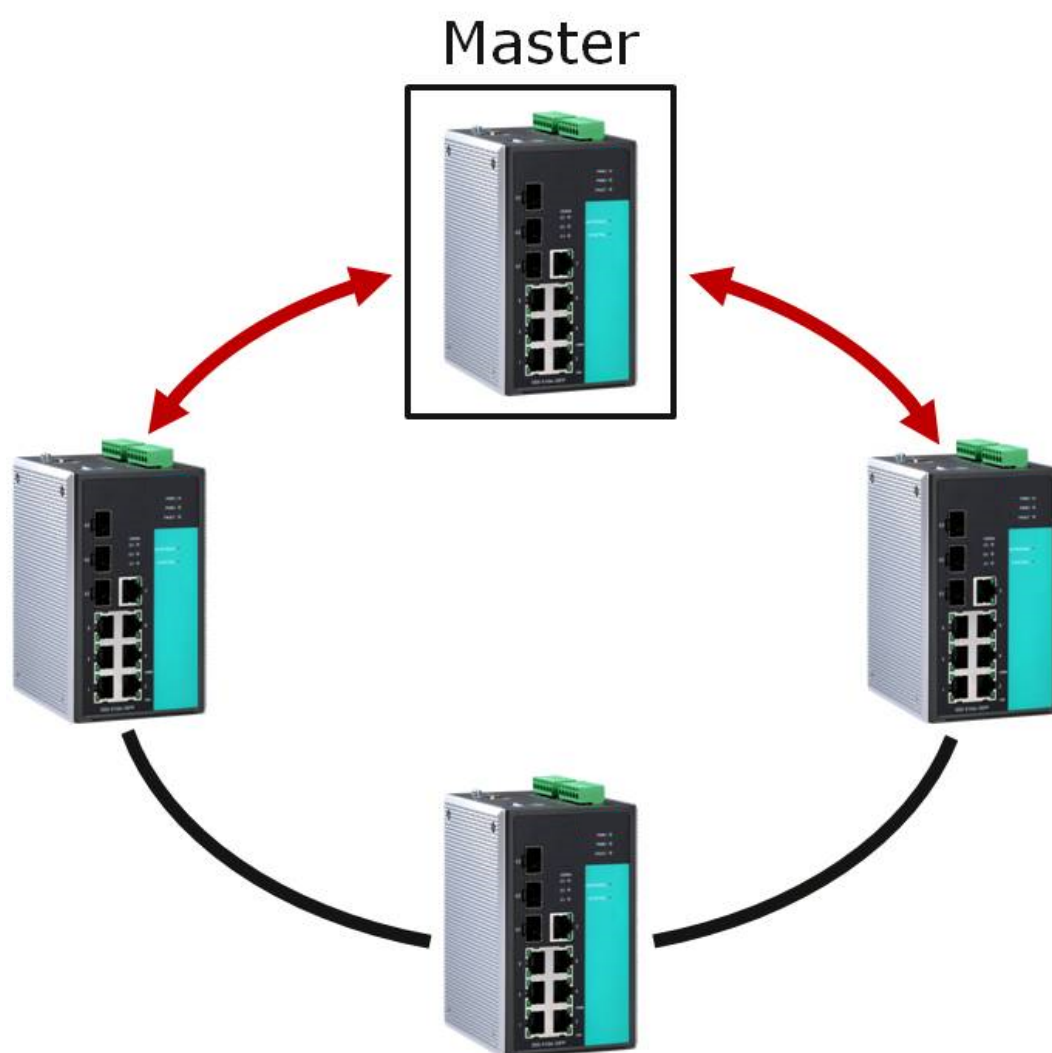
■ **When the Number of Switches in the Turbo Ring is Odd**

If there are $2N+1$ switches (an odd number) in the "Turbo Ring" ring, with switches and segments labeled counterclockwise, then segment $N+1$ will serve as the backup path. For the example shown here, $N=1$, so that $N+1=2$.



Determining the Redundant Path of a "Turbo Ring V2" Ring

For a Turbo Ring V2 ring, the backup segment is the segment connected to the 2nd redundant port on the master. See Configuring Turbo Ring V2 in the Configuring Turbo Ring and Turbo Ring V2 section below.



Ring Coupling Configuration

For some systems, it may not be convenient to connect all devices in the system to create one BIG redundant ring, since some devices could be located in a remote area. For these systems, *Ring Coupling* can be used to separate the devices into different smaller redundant rings, but in such a way that they can still communicate with each other.

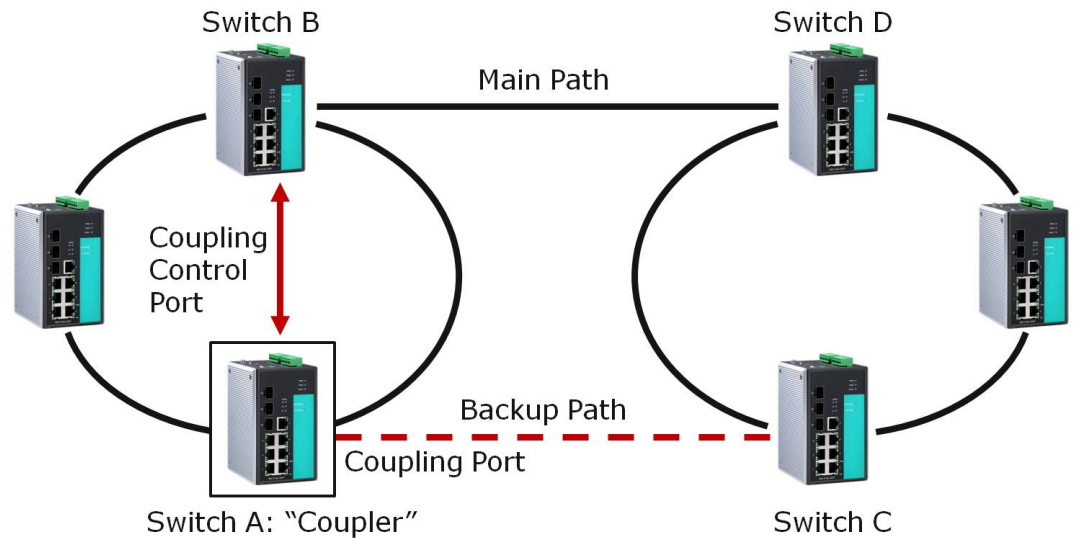


CAUTION!

In a VLAN environment, the user must set *Redundant Port*, *Coupling Port* and *Coupling Control Port* to join all VLANs, since these ports act as the backbone to transmit all packets of different VLANs to different switches.

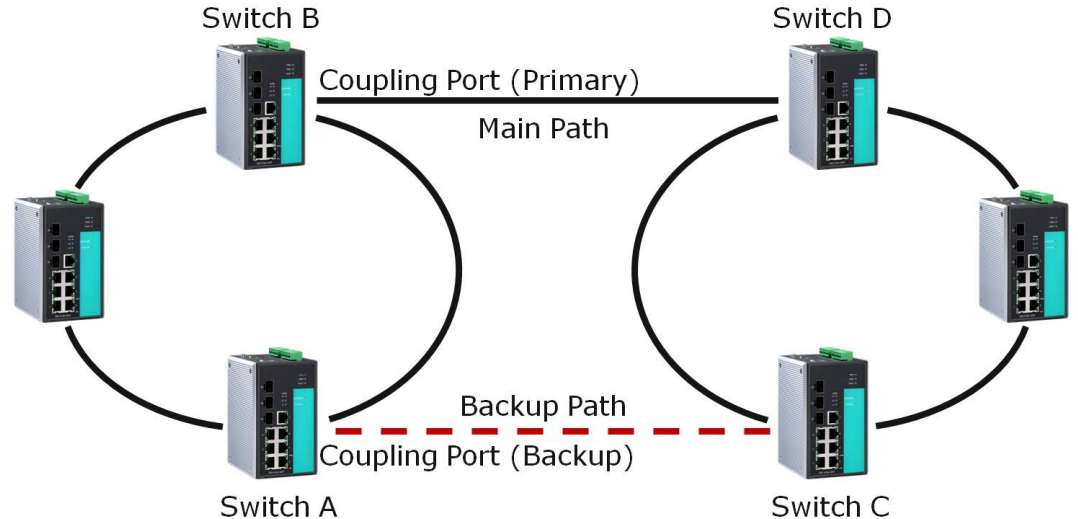
■ Ring Coupling for a "Turbo Ring" Ring


To configure the Ring Coupling function for a "Turbo Ring" ring, select two switches (e.g., Switch A and B in the above figure) in the ring, and another two switches in the adjacent ring (e.g., Switch C and D). Decide which two ports in each switch are appropriate to be used as coupling ports, and then link them together. Next, assign one switch (e.g., Switch A) to be the *coupler* and connect the coupler's coupling control port with Switch B (for this example). The coupler switch (i.e., Switch A) will monitor switch B through the coupling control port to determine whether or not the coupling port's backup path should be recovered.




■ **Ring Coupling for a "Turbo Ring V2" Ring**

Note that the ring coupling settings for a Turbo Ring V2 ring are different from a Turbo Ring ring. For Turbo Ring V2, Ring Coupling is enabled by configuring the *Coupling Port (Primary)* on Switch B, and the *Coupling Port (Backup)* on Switch A only. You do not need to set up a coupling control port, so that a Turbo Ring V2 ring does not use a coupling control line. The *Coupling Port (Backup)* on Switch A is used for the backup path, and connects directly to an extra network port on Switch C. The *Coupling Port (Primary)* on Switch B monitors the status of the main path, and connects directly to an extra network port on Switch D. With ring coupling established, Switch A can activate the backup path as soon as it detects a problem with the main path.

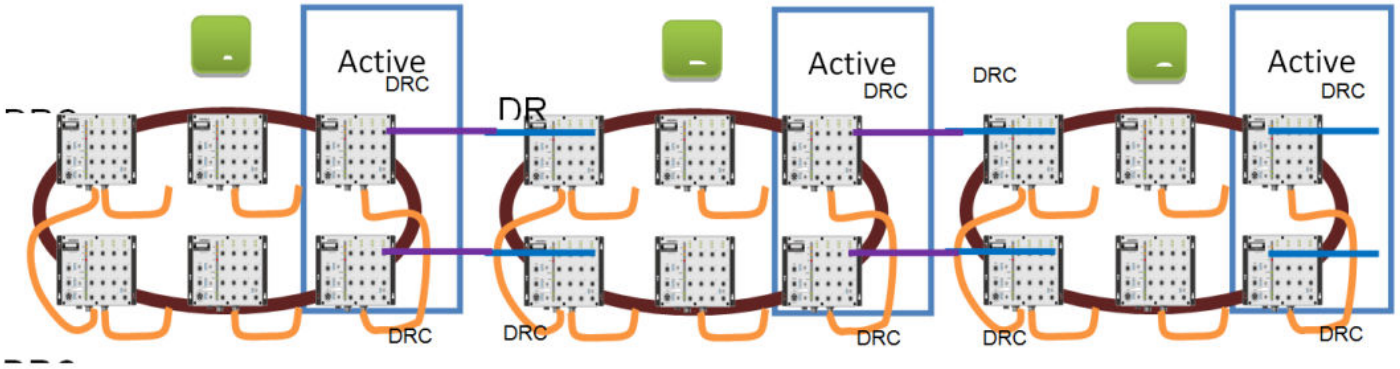


CAUTION!  Ring Coupling only needs to be enabled on one of the switches serving as the Ring Coupler. The Coupler must designate different ports as the two Turbo Ring ports and the coupling port.

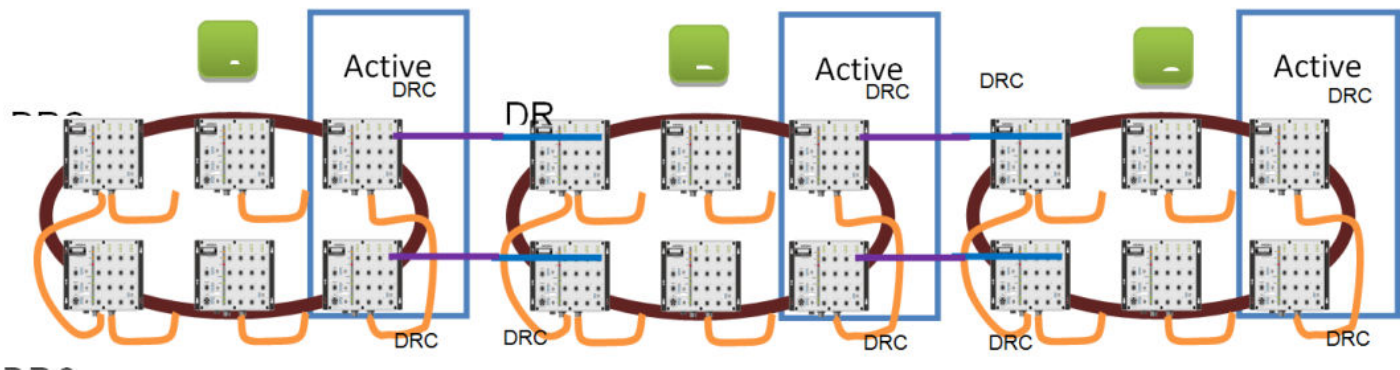
 You do not need to use the same switch for both Ring Coupling and Ring Master.

Dynamic Ring Coupling (DRC) Configuration (applies only to Turbo Ring V2)

VIPA’s switch supports Turbo Ring V2 with Dynamic Ring Coupling (DRC), which is an innovative inter-consist network redundancy technology. It not only supports Ring Coupling (RC), which enables fast network recovery during link failures, but also automatically assigns the active coupler switch on each train consist when train consist sequences are changed, added, or removed. This not only prevents looping and broadcast storms, but also reduces additional configuration time and possible errors caused by user configuration, enhancing network communication reliability and efficiency.



Turbo Ring V2 with DRC Diagram 1



Turbo Ring V2 with DRC Diagram 2



Note that the dynamic ring coupling settings are only supported by Turbo Ring V2.

Turbo Ring V2 with DRC (Dynamic Ring Coupling)

- DRC Group 1 requires one or two switches as members of a ring (Diagram 1: Left side of ring A, B, C; or Diagram 2: Left side of ring A, C, and right side of ring B).
- DRC Group 2 requires one or two switches as members of a ring (Diagram 1: Right side of ring A, B, C; or Diagram 2: Right side of ring A, C and left side of ring B).
- Ring Coupler – Scenario 1:
Linking all members of DRC group 1 to the member of the another ring DRC group 2 (Diagram 1: The left side DRC group 1 of ring C coupled to right side DRC group 2 of ring B); or linking all members of DRC group 1 to the member of the another ring DRC group 1 (Diagram 2: The right side of DRC group 1 of ring B coupled to the left side of DRC group 1 of ring C); or no connection to DRC group 1 (Diagram 1: The left side DRC group 1 of ring A).

- (4) Ring Coupler – Scenario 2:
By linking all members of DRC group 2 to the member of the another ring DRC group 1 (Diagram 1: The right side DRC group 2 of ring A coupler to left side DRC group 1 of ring B) or by linking all members of DRC group 2 to the member of the another ring DRC group 2 (Diagram 2: The right side DRC group 2 of ring A coupler to left side DRC group 2 of ring B) or no connection of the DRC group 2 (Diagram 2: The right side DRC group 2 of ring C)
- After all cable connections complete, the DRC protocol will start convergence and automatically assign one DRC group of the ring as Active DRC group.



CAUTION!

The ports which support bypass function cannot be used in redundant protocol like STP, RSTP, MSTP, Turbo Ring, Turbo Ring v2, Turbo Ring V2 with DRC (Dynamic Ring Coupling) and Turbo Chain.

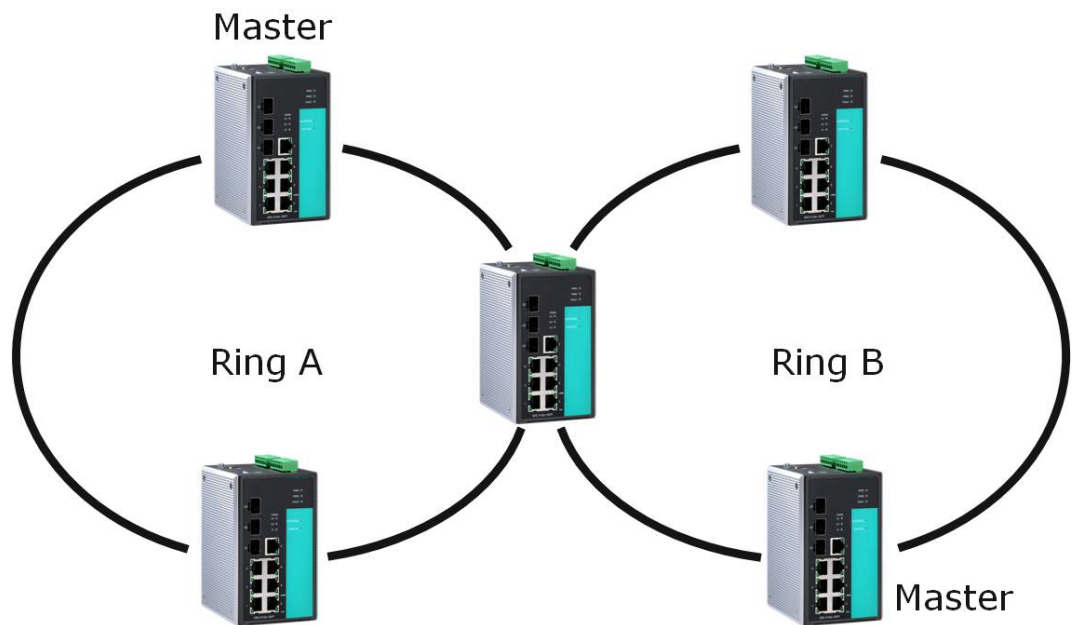


Bypass function is used to apply on linear topology only.

Dual-Ring Configuration (applies only to Turbo Ring V2)

The *dual-ring* option provides another ring coupling configuration, in which two adjacent rings share one switch. This type of configuration is ideal for applications that have inherent cabling difficulties.

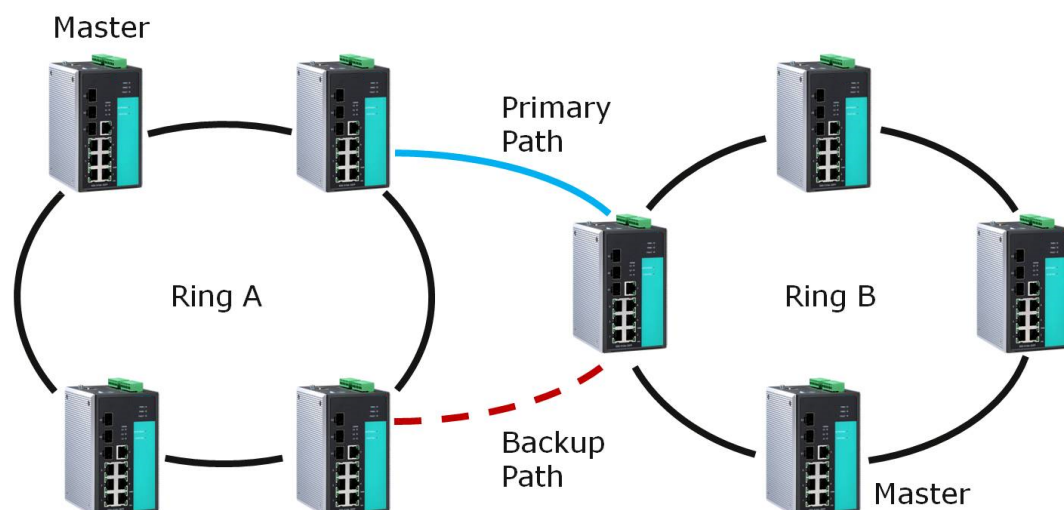
- **Dual-Ring for a Turbo Ring V2 Ring**



Dual-Homing Configuration (applies only to Turbo Ring V2)

The *dual-homing* option uses a single Ethernet switch to connect two networks. The primary path is the operating connection, and the backup path is a back-up connection that is activated in the event that the primary path connection fails.

- **Dual-Homing for a Turbo Ring V2 Ring**



5.2.3 Configuring Turbo Ring and Turbo Ring V2

Use the *Communication Redundancy* page to select Turbo Ring, Turbo Ring V2, or Turbo Chain. Note that configuration pages for these three protocols are different.

Configuring Turbo Ring

Communication Redundancy

Current Status

Now Active	None		
Master/Slave	---		
Redundant Ports Status	1st Port	---	
	2nd Port	---	
Ring Coupling Ports Status	---		
Coupling Port	---		
Coupling Control Port	---		

Settings

Redundancy Protocol		Turbo Ring	▼
<input type="checkbox"/> Set as Master			
Redundant Ports	1st Port	2-3	▼
	2nd Port	2-4	▼
<input type="checkbox"/> Enable Ring Coupling			
Coupling Port		2-2	▼
Coupling Control Port		2-1	▼

Activate

Explanation of Current Status Items

- **Now Active**
It shows which communication protocol is in use: Turbo Ring, Turbo Ring V2, RSTP, or none.
- **Master/Slave**
It indicates whether or not this switch is the Master of the Turbo Ring. (This field appears only when Turbo Ring or Turbo Ring V2 modes are selected.)



The user does not need to set the master to use Turbo Ring. If master is not set, the Turbo Ring protocol will assign master status to one of the switches in the ring. The master is only used to determine which segment serves as the backup path.

- **Redundant Ports Status (1st Port, 2nd Port)**
- **Ring Coupling Ports Status (Coupling Port, Coupling Control Port)**
The "Ports Status" indicators show *Forwarding* for normal transmission, *Blocking* if this port is connected to a backup path and the path is blocked, and *Link down* if there is no connection.

Explanation of Settings Items

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
Turbo Ring V2 with DRC (Dynamic Ring Coupling)	Select this item to change to the Turbo Ring V2 with DRC configuration page.	
Turbo Chain	Select this item to change to the Turbo Chain configuration page.	
RSTP (IEEE 802.1W/802.1D-2004)	Select this item to change to the RSTP configuration page.	
None	Ring redundancy is not active	

Set as Master

Setting	Description	Factory Default
Enabled	Select this switch as Master	Not checked
Disabled	Do not select this switch as Master	

Redundant Ports

Setting	Description	Factory Default
1st Port	Select any port of the switch to be one of the redundant ports.	The second from the last port
2nd Port	Select any port of the switch to be one of the redundant ports.	The last port

Enable Ring Coupling

Setting	Description	Factory Default
Enable	Select this switch as Coupler	Not checked
Disable	Do not select this switch as Coupler	

Coupling Port

Setting	Description	Factory Default
Coupling Port	Select any port of the switch to be the coupling port	The fourth from the last port

Coupling Control Port

Setting	Description	Factory Default
Coupling Control Port	Select any port of the Switch to be the coupling control port	The third from the last port

Configuring Turbo Ring V2

Communication Redundancy

Current Status

Now Active None	
Ring 1	Ring 2
Status	Status
Master/Slave	Master/Slave
1st Ring Port Status	1st Ring Port Status
2nd Ring Port Status	2nd Ring Port Status
Coupling	
Mode	
Coupling Port status	Primary Port -- Backup Port --

Settings

Redundancy Protocol Turbo Ring V2

Enable Ring 1

Set as Master

Redundant Ports 1st Port 2-3

2nd Port 2-4

Enable Ring Coupling

Coupling Mode Dual Homing

Primary Port 1-1 Backup Port 1-2

Enable Ring 2

Set as Master

Redundant Ports 1st Port 2-2

2nd Port 2-1


Activate



When using the Dual-Ring architecture, users must configure settings for both Ring 1 and Ring 2. In this case, the status of both rings will appear under 'Current Status'.

Explanation of Current Status Items

- **Now Active**
It shows which communication protocol is in use: ‘Turbo Ring’, ‘Turbo Ring V2’, ‘Turbo Chain’, ‘RSTP’ or ‘None’.
- **Ring 1/2-Status**
It shows ‘Healthy’ if the ring is operating normally and shows ‘Break’ if the ring’s backup link is active.
- **Ring 1/2-Master/Slave**
It indicates whether or not this Switch is the Master of the Turbo Ring. (This field appears only when Turbo Ring or Turbo Ring V2 modes are selected.)

 The user does not need to set the master to use Turbo Ring. If master is not set, the Turbo Ring protocol will assign master status to one of the Switch units in the ring. The master is only used to determine which segment serves as the backup path.

- **Ring 1/2-1st Ring Port Status**
- **Ring 1/2-2nd Ring Port Status**
The *Ports Status* indicators show *Forwarding* for normal transmission, *Blocking* if this port is connected to a backup path and the path is blocked, and *Link down* if there is no connection.
- **Coupling-Mode**
It indicates either ‘None’, ‘Dual Homing’ or ‘Ring Coupling’.
- **Coupling-Coupling Port status**
It indicates either *Primary* or *Backup*.

Explanation of Settings Items

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
Turbo Ring V2 with DRC (Dynamic Ring Coupling)	Select this item to change to the Turbo Ring V2 with DRC configuration page.	
Turbo Chain	Select this item to change to the Turbo Chain configuration page.	
RSTP (IEEE 802.1W/ 802.1D-2004)	Select this item to change to the RSTP configuration page.	
None	Ring redundancy is not active	

Enable Ring 1

Setting	Description	Factory Default
Enabled	Enable the Ring 1 settings	Not checked
Disabled	Disable the Ring 1 settings	

Enable Ring 2*

Setting	Description	Factory Default
Enabled	Enable the Ring 2 settings	Not checked
Disabled	Disable the Ring 2 settings	



You should enable both Ring 1 and Ring 2 when using the Dual-Ring architecture.

Set as Master

Setting	Description	Factory Default
Enabled	Select this Switch as Master	Not checked
Disabled	Do not select this Switch as Master	

Redundant Ports

Setting	Description	Factory Default
1st Port	Select any port of the Switch to be one of the redundant ports.	The second from the last port
2nd Port	Select any port of the Switch to be one of the redundant ports.	The last port

Enable Ring Coupling

Setting	Description	Factory Default
Enable	Select this Switch as Coupler	Not checked
Disable	Do not select this Switch as Coupler	

Coupling Mode

Setting	Description	Factory Default
Dual Homing	Select this item to change to the Dual Homing configuration page	See the following table
Ring Coupling (backup)	Select this item to change to the Ring Coupling (backup) configuration page	See the following table
Ring Coupling (primary)	Select this item to change to the Ring Coupling (primary) configuration page	See the following table

Default Dual Homing Ports

Default Dual Homing (Primary)	Default Dual Homing (Backup)
The fourth from the last port	The third from the last port



The Turbo Ring DIP Switches located on the outer casing of switches can be used to configure the switches' Turbo Ring protocols (Turbo Ring or Turbo Ring V2). If the Turbo Ring DIP Switch is enabled from any access interface (web-based UI, console, or Telnet), and the 4th DIP Switch on the switch outer casing is set to ON, the Redundancy Protocol will be set automatically to the Turbo Ring protocol based on the version configured in the Turbo Ring DIP Switch page and the corresponding Redundant Ports, Coupling Ports, and Coupling Control Port will be fixed to the assigned factory default port number automatically. In this case, you will not be able to use the web-based UI, console, or Telnet interface to change the status of the DIP Switch and the Communication Redundancy settings will be grayed out in the web browser as shown in the following figure:

Communication Redundancy

Current Status

Now Active: **Turbo Ring V2**

Ring 1		Ring 2	
Status	Break	Status	--
Master/Slave	Master	Master/Slave	--
1st Ring Port Status	Link down	1st Ring Port Status	--
2nd Ring Port Status	Link down	2nd Ring Port Status	--

Coupling

Mode: **none**

Coupling Port status: Primary Port -- Backup Port --

Settings

Redundancy Protocol: Turbo Ring V2

Enable Ring 1 Enable Ring 2

Set as Master Set as Master

Redundant Ports 1st Port: G8 2nd Port: G9

Redundant Ports 1st Port: G7 2nd Port: G6

Enable Ring Coupling

Coupling Mode: Dual Homing

Primary Port: G7 Backup Port: G6

Activate

In addition, those default Redundant Ports, Coupling Ports, and Coupling Control Port will be added automatically to all VLANs (i.e., to act as Trunk Ports) if you set the 4th DIP Switch to the ON position when the Turbo Ring DIP Switch is enabled. Once you flip the 4th DIP Switch from ON to OFF when the Turbo Ring DIP Switch is enabled, such default Redundant Ports, Coupling Ports, and Coupling Control Port that were added to all VLANs will be restored to their previous software settings.



If you would like to enable VLAN and/or port trunking on any of the last four ports, do not use the fourth DIP switch to activate Turbo Ring. In this case, you should use the Web, Telnet, or Serial console to activate Turbo Ring.

Configuring Turbo Ring V2 with Dynamic Ring Coupling (DRC)

Communication Redundancy

Ring Status

Now Active Turbo Ring V2 with DRC (Dynamic Ring Coupling)
 Ring Master ID 00:90:E8:30:90:27
 Status Healthy
 Master/Slave Master
 1st Ring Port Status Forwarding
 2nd Ring Port Status Blocked

DRC Status

Coupling Group	Coupling port status
Group 1 (Inactive)	1 <00:90:E8:30:90:31> 15 Link down 2 16 Link down
Group 2 (Inactive)	1 <00:90:E8:30:90:31> 16 Link down 2 <00:90:E8:30:90:2D> 15 Link down

Ring Settings

Redundancy Protocol Turbo Ring V2 with DRC (Dynamic Ring Coupling) ▼
 Set as Master
 Redundant Ports 1st Port 17 ▼
 2nd Port 18 ▼

DRC Settings

Coupling Group	Coupling Ports
Group 1	1 16 ▼ Auto ▼ 2 -- ▼ Auto ▼
Group 2	1 -- ▼ Auto ▼ 2 -- ▼ Auto ▼

Activate

Explanation of Ring Status Items

- **Now Active**
It shows which redundant protocol is in use: 'Turbo Ring', 'Turbo Ring V2', 'RSTP', 'MSTP', 'Turbo Ring V2 with DRC (Dynamic Ring Coupling)' or 'none'.
- **Ring Master ID**
It indicates the smallest MAC address of the device in the ring.
- **Status**
The Status indicator shows 'Healthy' for normal transmission of a ring, 'Break' if the ring is incomplete or there is no connection.
- **Master/Slave**
It indicates whether or not this switch is the Master of the Turbo Ring V2 with DRC. (This field appears only when Turbo Ring, Turbo Ring V2 or Turbo Ring V2 with DRC modes are selected.)
- **1st Ring Port Status**
The Ring Ports Status indicators show 'Forwarding' for normal transmission, 'Blocked' if this port is connected to a backup path and the path is blocked, and 'Link down' if there is no connection.
- **2nd Ring Port Status**
The Ports Status indicators show 'Forwarding' for normal transmission, 'Blocked' if this port is connected to a backup path and the path is blocked, and 'Link down' if there is no connection.

Explanation of DRC Status Items

- **Coupling Group**
The Coupling Group indicators show 'Active' for taking the responsibility to maintain the coupling links, 'Inactive' if the other group of the ring is Active status already.
- **Coupling Port Status**
The Coupling Ports Status indicators show 'Port number + Forwarding' for normal transmission. If the switch is the ring master, it will show the status of two coupling groups using 'MAC address + Port number + Link up'. If the coupling port has no connection, it shows 'MAC address + Port number + Link down'.

Explanation of *Ring Settings* Items

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
Turbo Ring V2 with DRC (Dynamic Ring Coupling)	Select this item to change to the Turbo Ring V2 with DRC configuration page.	
Turbo Chain	Select this item to change to the Turbo Chain configuration page.	
RSTP (IEEE 802.1W/802.1D-2004)	Select this item to change to the RSTP configuration page.	

Set as Master

Setting	Description	Factory Default
Enabled	Select this switch as Master	Disabled
Disabled	Select this switch as Slave or if no master in the ring, it may choose the switch with smallest MAC address as Master (Candidate Master)	

DRC Settings

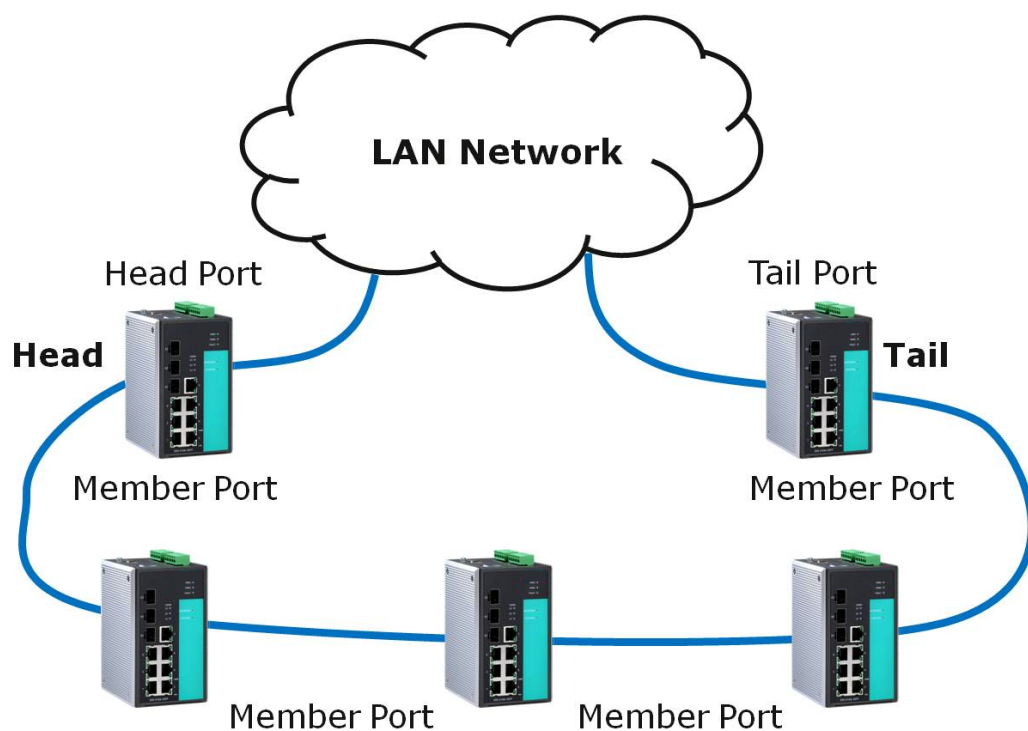
Setting	Description	Factory Default
Group1/Coupling Ports	Select any port of the switch to be one of the coupling group 1 port and choose auto, primary, backup as the port role	Port number: None Role: Auto
Group2/Coupling Ports	Select any port of the switch to be one of the coupling group 2 port and choose auto, primary, backup as the port role	Port number: None Role: Auto

5.3 Turbo Chain

5.3.1 The Turbo Chain Concept

VIPA's Turbo Chain is an advanced software-technology that gives network administrators the flexibility of constructing any type of redundant network topology. When using the chain concept, you first connect the Ethernet switches in a chain and then simply link the two ends of the chain to an Ethernet network, as illustrated in the following figure. Turbo Chain can be used on industrial networks that have a complex topology. If the industrial network uses a multi-ring architecture, Turbo Chain can be used to create flexible and scalable topologies with a fast media-recovery time.

5.3.2 Setting Up Turbo Chain



1. Select the Head switch, Tail switch, and Member switches.
2. Configure one port as the Head port and one port as the Member port in the Head switch, configure one port as the Tail port and one port as the Member port in the Tail switch, and configure two ports as Member ports in each of the Member switches.
3. Connect the Head switch, Tail switch, and Member switches as shown in the above diagram.

The path connecting to the Head port is the main path, and the path connecting to the Tail port is the backup path of the Turbo Chain. Under normal conditions, packets are transmitted through the Head Port to the LAN network. If any Turbo Chain path is disconnected, the Tail Port will be activated so that packet transmission can continue.

5.3.3 Configuring Turbo Chain

Head Switch Configuration

Communication Redundancy

Current Status
Now Active **Turbo Chain**

Settings

Redundancy Protocol

Role

Port Role	Port Num	Port Status
Head Port	<input type="text" value="1-1"/>	Forwarding
Member Port	<input type="text" value="1-2"/>	Forwarding

Member Switch Configuration

Communication Redundancy

Current Status
Now Active **Turbo Chain**

Settings

Redundancy Protocol

Role

Port Role	Port Num	Port Status
1st Member Port	<input type="text" value="1-1"/>	Forwarding
2nd Member Port	<input type="text" value="1-2"/>	Forwarding

Tail Switch Configuration

Communication Redundancy

Current Status
Now Active **Turbo Chain**

Settings

Redundancy Protocol

Role

Port Role	Port Num	Port Status
Tail Port	<input type="text" value="1-1"/>	Blocked
Member Port	<input type="text" value="1-2"/>	Forwarding

Explanation of Current Status Items■ **Now Active**

It shows which communication protocol is in use: *'Turbo Ring'*, *'Turbo Ring V2'*, *'RSTP'*, *'Turbo Chain'* or *'None'*. The Ports Status indicators show *'Forwarding'* for normal transmission, *'Blocked'* if this port is connected to the Tail port as a backup path and the path is blocked, and *'Link down'* if there is no connection.

Explanation of Settings Items**Redundancy Protocol**

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
Turbo Chain	Select this item to change to the Turbo Chain configuration page	
RSTP	Select this item to change to the RSTP configuration page.	
None	Ring redundancy is not active	

Role

Setting	Description	Factory Default
Head	Select this Switch as Head Switch	Member
Member	Select this Switch as Member Switch	
Tail	Select this Switch as Tail Switch	

Head Role

Setting	Description	Factory Default
Head Port	Select any port of the Switch to be the head port.	The second from the last port
Member Port	Select any port of the Switch to be the member port.	The last port

Member Role

Setting	Description	Factory Default
1st Member port	Select any port of the Switch to be the 1st member port	The second from the last port
2nd Member port	Select any port of the Switch to be the 2nd member port	The last port

Tail Role

Setting	Description	Factory Default
Tail Port	Select any port of the Switch to be the tail port.	The second from the last port
Member Port	Select any port of the Switch to be the member port.	The last port

5.4 STP/RSTP/MSTP**5.4.1 The STP/RSTP/MSTP Concept**

Spanning Tree Protocol (STP) was designed to help reduce link failures on a network, and provide an automatic means of avoiding loops. This is particularly important for networks that have a complicated architecture, since unintended loops in the network can cause broadcast storms. VIPA switches' STP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every VIPA switch connected to your network.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by IEEE 802.1D-2004. RSTP provides the following benefits:

- The topology of a bridged network will be determined much more quickly compared to STP.
- RSTP is backward compatible with STP, making it relatively easy to deploy. For example:
 - Defaults to sending 802.1D style BPDUs if packets with this format are received.
 - STP (802.1D) and RSTP (802.1w) can operate on different ports of the same switch, which is particularly helpful when switch ports connect to older equipment such as legacy switches.

You get essentially the same functionality with RSTP and STP. To see how the two systems differ, see the Differences between STP and RSTP section in this chapter.



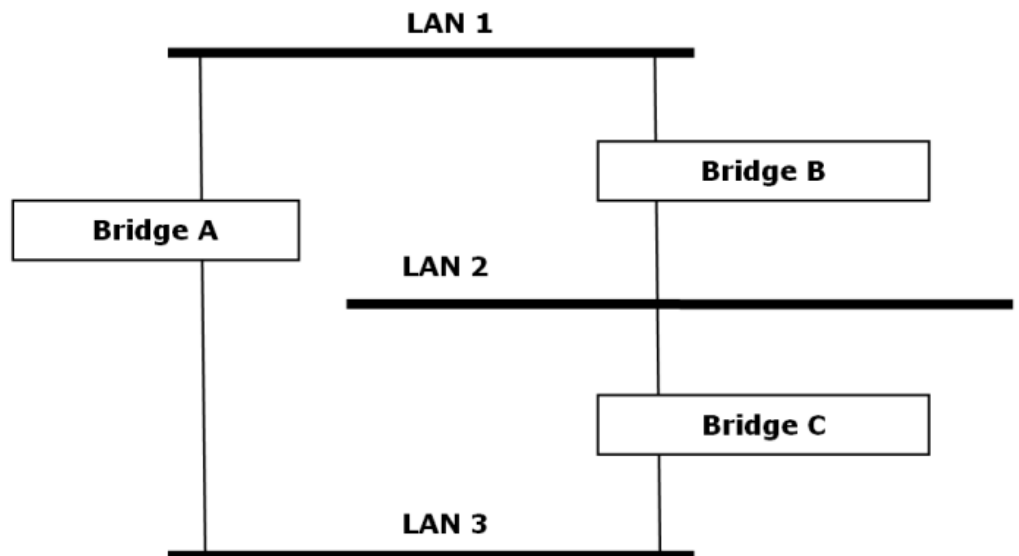
The STP protocol is part of the IEEE Std 802.1D, 2004 Edition bridge specification. The following explanation uses bridge instead of switch.

What is STP?

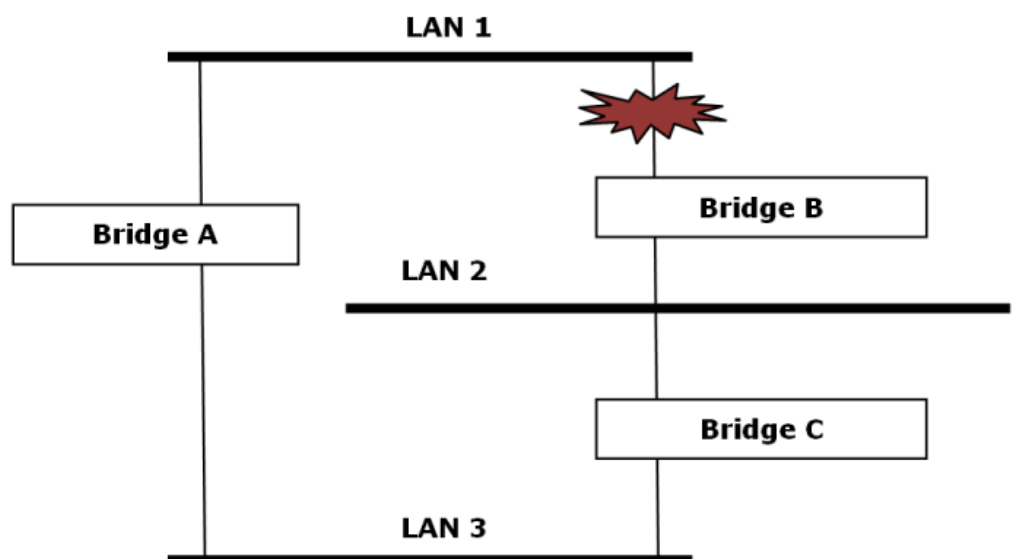
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

- Locate and then disable less efficient paths (i.e., paths that have a lower bandwidth).
- Enable one of the less efficient paths if a more efficient path fails.

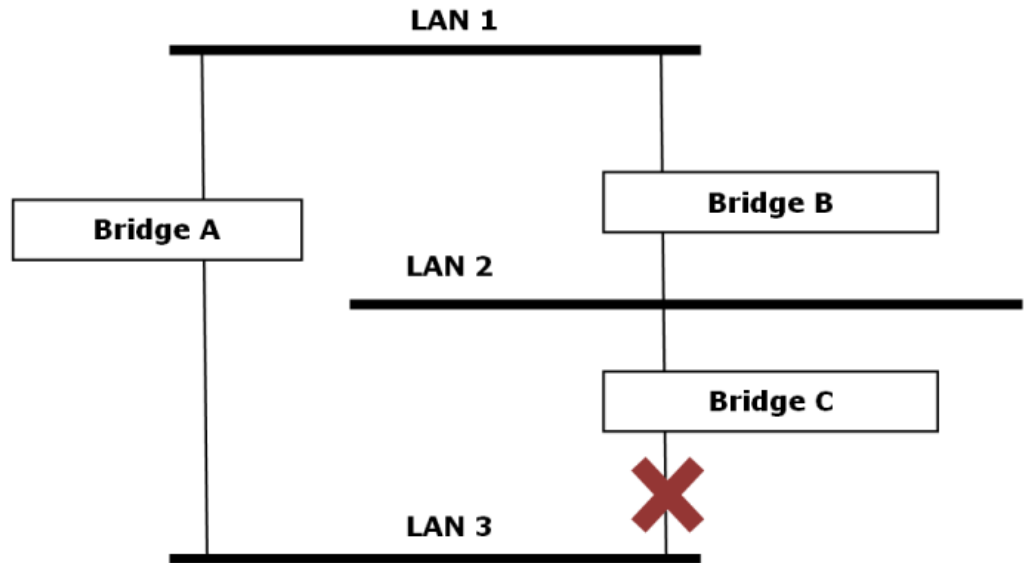
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



If STP is enabled, it will detect duplicate paths and prevent, or block, one of the paths from forwarding traffic. In the following example, STP determined that traffic from LAN segment 2 to LAN segment 1 should flow through bridges C and A since this path has a greater bandwidth and is therefore more efficient.



What happens if a link failure is detected? As shown in next figure, the STP process reconfigures the network so that traffic from LAN segment 2 flows through bridge B.



STP will determine which path between each bridged segment is most efficient, and then assign a specific reference point on the network. When the most efficient path has been identified, the other paths are blocked. In the previous 3 figures, STP first determined that the path through bridge C was the most efficient, and as a result, blocked the path through bridge B. After the failure of bridge C, STP re-evaluated the situation and opened the path through Bridge B.

How STP Works

When enabled, STP determines the most appropriate path for traffic through a network. The way it does this is outlined in the sections below.

■ STP Requirements

When enabled, STP determines the most appropriate path for traffic through a network. The way it does this is outlined in the sections below.

- All bridges must be able to communicate with each other. The communication is carried out using Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address.
- Each bridge must have a Bridge Identifier that specifies which bridge acts as the central reference point, or Root Bridge, for the STP system—bridges with a lower Bridge Identifier are more likely to be designated as the Root Bridge. The Bridge Identifier is calculated using the MAC address of the bridge and a priority defined for the bridge. For example, the default priority setting of VIPA switches is 32768.
- Each port has a cost that specifies the efficiency of each link. The efficiency cost is usually determined by the bandwidth of the link, with less efficient links assigned a higher cost.

■ STP Calculation

The first step of the STP process is to perform calculations. During this stage, each bridge on the network transmits BPDUs. The following items will be calculated:

- Which bridge should be the *Root Bridge*. The Root Bridge is the central reference point from which the network is configured.
- The *Root Path Costs* for each bridge. This is the cost of the paths from each bridge to the Root Bridge.
- The identity of each bridge's *Root Port*. The Root Port is the port on the bridge that connects to the Root Bridge via the most efficient path. In other words, the port connected to the Root Bridge via the path with the lowest Root Path Cost. The Root Bridge, however, does not have a Root Port.
- The identity of the *Designated Bridge* for each LAN segment. The Designated Bridge is the bridge with the lowest Root Path Cost from that segment. If several bridges have the same Root Path Cost, the one with the lowest Bridge Identifier becomes the Designated Bridge. Traffic transmitted in the direction of the Root Bridge will flow through the Designated Bridge. The port on this bridge that connects to the segment is called the *Designated Bridge Port*.

■ STP Configuration

After all of the bridges on the network agree on the identity of the Root Bridge, and all other relevant parameters have been established, each bridge is configured to forward traffic only between its Root Port and the Designated Bridge Ports for the respective network segments. All other ports are blocked, which means that they will not be allowed to receive or forward traffic.

■ STP Reconfiguration

Once the network topology has stabilized, each bridge listens for Hello BPDUs transmitted from the Root Bridge at regular intervals. If a bridge does not receive a Hello BPDUs after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, has ceased to function. This will trigger the bridge to reconfigure the network to account for the change. If you have configured an SNMP trap destination, when the topology of your network changes, the first bridge to detect the change will send out an SNMP trap.

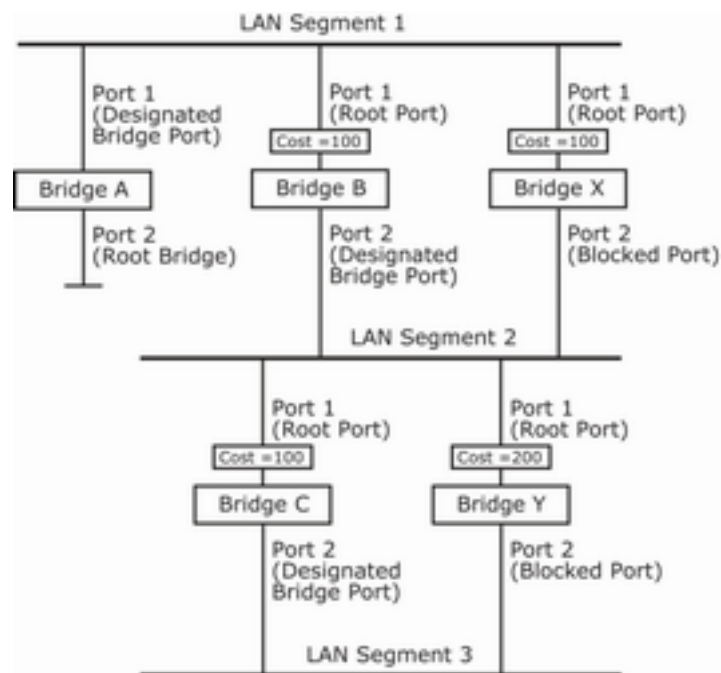
Differences between STP, RSTP and MSTP

RSTP is similar to STP, but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighbouring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP. STP and RSTP spanning tree protocols

operate without regard to a network's VLAN configuration, and maintain one common spanning tree throughout a bridged network. Thus, these protocols map one loop-free, logical topology on a given physical topology. MSTP uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

5.4.2 STP Example

The LAN shown in the following figure has three segments, with adjacent segments connected using two possible links. The various STP factors, such as Cost, Root Port, Designated Bridge Port, and Blocked Port are shown in the figure.

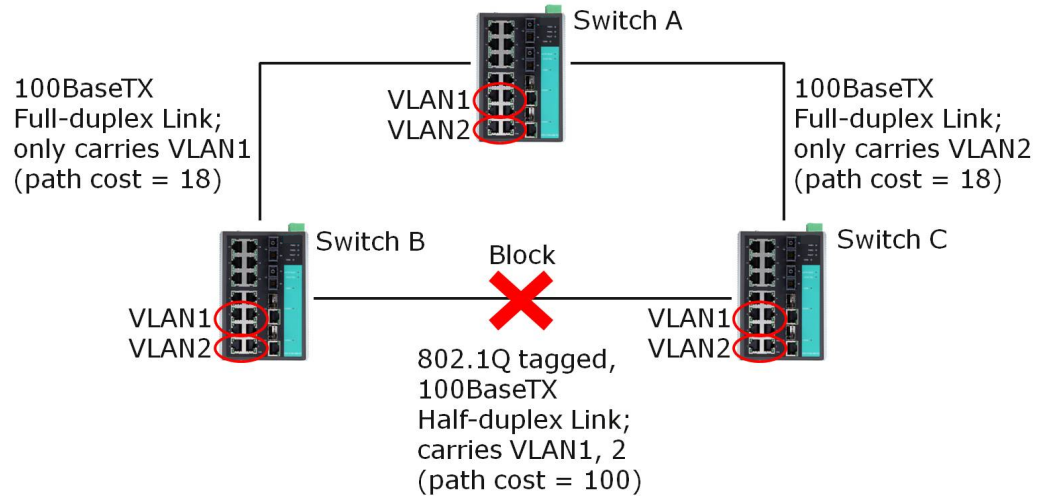


- Bridge A has been selected as the Root Bridge, since it was determined to have the lowest Bridge Identifier on the network.
- Since Bridge A is the Root Bridge, it is also the Designated Bridge for LAN segment 1. Port 1 on Bridge A is selected as the Designated Bridge Port for LAN Segment 1.
- Ports 1 of Bridges B, C, X, and Y are all Root Ports since they are nearest to the Root Bridge, and therefore have the most efficient path.
- Bridges B and X offer the same Root Path Cost for LAN segment 2. However, Bridge B was selected as the Designated Bridge for that segment since it has a lower Bridge Identifier. Port 2 on Bridge B is selected as the Designated Bridge Port for LAN Segment 2.
- Bridge C is the Designated Bridge for LAN segment 3, because it has the lowest Root Path Cost for LAN Segment 3:
 - The route through bridges C and B costs 200 (C to B=100, B to A=100)
 - The route through bridges Y and B costs 300 (Y to B=200, B to A=100)
- The Designated Bridge Port for LAN Segment 3 is port 2 on bridge C.

5.4.3 Using STP on a Network with Multiple VLANs

IEEE Std 802.1D, 1998 Edition, does not take into account VLANs when calculating STP information-the calculations only depend on the physical connections. Consequently, some network configurations will result in VLANs being subdivided into a number of isolated sections by the STP system. You must ensure that every VLAN configuration on your network takes into account the expected STP topology and alternative topologies

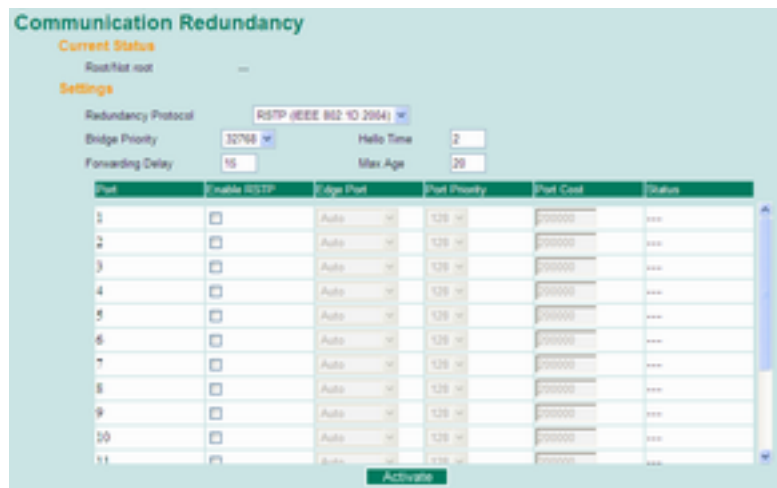
that may result from link failures. The following figure shows an example of a network that contains VLANs 1 and 2. The VLANs are connected using the 802.1Q-tagged link between switch B and Switch C. By default, this link has a port cost of 100 and is automatically blocked because the other switch-to-switch connections have a port cost of 36 (18+18). This means that both VLANs are now subdivided-VLAN 1 on switches A and B cannot communicate with VLAN 1 on switch C, and VLAN 2 on switches A and C cannot communicate with VLAN 2 on switch B.



To avoid subdividing VLANs, all inter-switch connections should be made members of all available 802.1Q VLANs. This will ensure connectivity at all times. For example, the connections between switches A and B, and between switches A and C, should be 802.1Q tagged and carrying VLANs 1 and 2 to ensure connectivity.

5.4.4 Configuring STP/RSTP

The following figures indicate which Spanning Tree Protocol parameters can be configured. A more detailed explanation of each parameter follows.



At the top of this page, the user can check the *Current Status* of this function. For RSTP, you will see:

Now Active

It shows which communication protocol is being used *'Turbo Ring'*, *'RSTP'* or *'neither'*.

Root/Not Root

This field only appears when RSTP mode is selected. The field indicates whether or not this switch is the Root of the Spanning Tree (the root is determined automatically).

At the bottom of this page, the user can configure the *Settings* of this function. For RSTP, you can configure:

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	None

Bridge priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Forwarding Delay (sec.)

Setting	Description	Factory Default
Numerical value input by user	The amount of time this device waits before checking to see if it should change to a different state.	15

Hello time (sec.)

Setting	Description	Factory Default
Numerical value input by user	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. The "hello time" is the amount of time the root waits between sending hello messages.	2

Max. Age (sec.)

Setting	Description	Factory Default
Numerical value input by user	If this device is not the root, and it has not received a "hello" message from the root in an amount of time equal to <i>Max. Age</i> , then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate to set up a new Spanning Tree topology.	20

Enable STP per Port

Setting	Description	Factory Default
Enable/Disable	Select to enable the port as a node on the Spanning Tree topology.	Disabled



We suggest not enabling the Spanning Tree Protocol once the port is connected to a device (PLC, RTU, etc.) as opposed to network equipment. The reason is that it will cause unnecessary negotiation.

Setting	Description	Factory Default
Auto	1. If the port does not receive a BPDU within 3 seconds, the port will be in the forwarding state. 2. Once the port receives a BPDU, it will start the RSTP negotiation process.	Auto
Force Edge	The port is fixed as an edge port and will always be in the forwarding state	
False	The port is set as the normal RSTP port	

Port Priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this port's priority as a node on the Spanning Tree topology by entering a lower number.	128

Port Cost

Setting	Description	Factory Default
Numerical value input by user	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology.	200000

Port Status

It indicates the current Spanning Tree status of this port. Forwarding for normal transmission or Blocking to block transmission.

5.4.5 Configuration Limits of STP/RSTP

The Spanning Tree Algorithm places limits on three of the configuration items described previously:

[Eq. 1]: $1 \text{ sec} \leq \text{Hello Time} \leq 10 \text{ sec}$

[Eq. 2]: $6 \text{ sec} \leq \text{Max. Age} \leq 40 \text{ sec}$

[Eq. 3]: $4 \text{ sec} \leq \text{Forwarding Delay} \leq 30 \text{ sec}$

These three variables are further restricted by the following two inequalities:

[Eq. 4]: $2 \times (\text{Hello Time} + 1 \text{ sec}) \leq \text{Max. Age} \leq 2 \times (\text{Forwarding Delay} - 1 \text{ sec})$

For example, setting

Hello Time = 5 sec, Max. Age = 20 sec, and Forwarding Delay = 4 sec does not violate Eqs. 1 through 3, but does violate Eq. 4, since in this case, $2 \times (\text{Hello Time} + 1 \text{ sec}) = 12 \text{ sec}$, and $2 \times (\text{Forwarding Delay} - 1 \text{ sec}) = 6 \text{ sec}$.

You can remedy the situation in many ways. One solution is simply to increase the Forwarding Delay value to at least 11 sec.

Perform the following steps to avoid guessing:

1. ➤ Assign a value to Hello Time and then calculate the left most part of Eq. 4 to get the lower limit of *Max. Age*.
2. ➤ Assign a value to Forwarding Delay and then calculate the right most part of Eq. 4 to get the upper limit for *Max. Age*.
3. ➤ Assign a value to Forwarding Delay that satisfies the conditions.

6 Industrial Protocols

6.1 MODBUS/TCP MAP

6.1.1 Introduction

MODBUS TCP is a protocol commonly used for the integration of a SCADA system. It is also a vendor-neutral communication protocol used to monitor and control industrial automation equipment such as PLCs, sensors, and meters. In order to be fully integrated into industrial systems, VIPA's switches support Modbus TCP/IP protocol for real-time monitoring in a SCADA system.

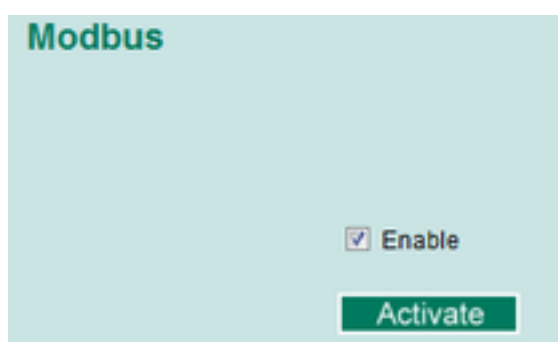
6.1.2 Data Format and Function Code

MODBUS TCP supports different types of data format for reading. The primary four types of them are:

Data Access Type		Function Code	Function Name	Note
Bit access	Physical Discrete Inputs	2	Read Discrete Inputs	
	Internal Bits or Physical Coils	1	Read Coils	
Wordaccess (16-bit access)	Physical Input Registers	4	Read Input Registers	VIPA Support
	Physical Output Registers	3	Read Holding Registers	

6.1.3 Configuring MODBUS/TCP on VIPA Switches

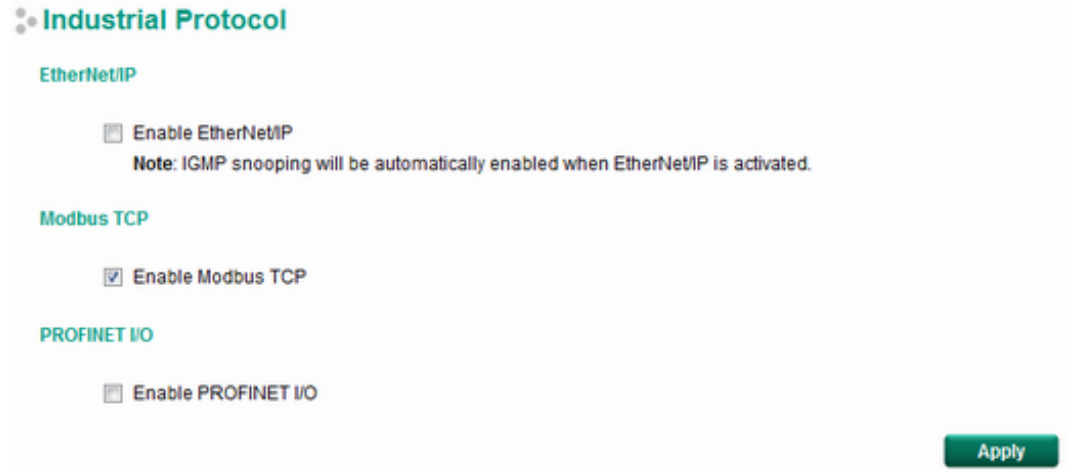
Type 1



Select the checkbox and click [Activate] to enable the Modbus TCP.

Type 2: New UI 2.0

Modbus TCP is enabled by default. To disable Modbus TCP, uncheck 'Enable Modbus TCP' then click [Apply].



6.1.4 MODBUS Data Map and Information Interpretation of VIPA Switches

The data map addresses of VIPA switches shown in the following table start from *MODBUS address 30001* for Function Code 4. For example, the address offset 0x0000 (hex) equals MODBUS address 30001, and the address offset 0x0010 (hex) equals MODBUS address 30017. Note that all the information read from VIPA switches are in hex mode. To interpret the information, refer to the ASCII table for the translation (e.g. 0x4D = 'M', 0x6F = 'o').

Address Offset	Data Type	Interpretation	Description
System Information			
0x0000	1 word	HEX	Vendor ID = 0x1393
0x0001	1 word		Unit ID (Ethernet = 1)
0x0002	1 word	HEX	Product Code = 0x0003
0x0010	20 words	ASCII	Vendor Name = "VIPA" Word 0 Hi byte = 'V' Word 0 Lo byte = 'I' Word 1 Hi byte = 'P' Word 1 Lo byte = 'A' Word 2 Hi byte = '\0' Word 2 Lo byte = '\0'

Address Offset	Data Type	Interpretation	Description
0x0030	20 words	ASCII	Product Name = "PN8-RD" Word 0 Hi byte = 'P' Word 0 Lo byte = 'N' Word 1 Hi byte = '8' Word 1 Lo byte = '-' Word 2 Hi byte = 'R' Word 2 Lo byte = 'D' Word 3 Hi byte = '\0' Word 3 Lo byte = '\0' Word 4 Hi byte = '\0' Word 4 Lo byte = '\0'
0x0050	1 word		Product Serial Number
0x0051	2 words		Firmware Version Word 0 Hi byte = major (A) Word 0 Lo byte = minor (B) Word 1 Hi byte = release (C) Word 1 Lo byte = build (D)
0x0053	2 words	HEX	Firmware Release Date For example: Word 0 = 0x0609 Word 1 = 0x0705 Firmware was released on 2007-05-06 at 09 o'clock
0x0055	3 words	HEX	Ethernet MAC Address Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0x00 Word 0 Lo byte = 0x01 Word 1 Hi byte = 0x02 Word 1 Lo byte = 0x03 Word 2 Hi byte = 0x04 Word 2 Lo byte = 0x05
0x0058	1 word	HEX	Power 1 0x0000: Off 0x0001: On
0x0059	1 word	HEX	Power 2 0x0000: Off 0x0001: On

MODBUS/TCP MAP > MODBUS Data Map and Information Interpretation of VIPA Switches

Address Offset	Data Type	Interpretation	Description
0x005A	1 word	HEX	Fault LED Status 0x0000: No 0x0001: Yes
0x0080	1 word	HEX	DI1 0x0000: Off 0x0001: On
0x0081	1 word	HEX	DI2 0x0000: Off 0x0001: On
0x0082	1 word	HEX	DO1 0x0000: Off 0x0001: On
0x0083	1 word	HEX	DO2 0x0000: Off 0x0001: On
Port Information			
0x1000 to 0x1011	1 word	HEX	Port 1 to 8 Status 0x0000: Link down 0x0001: Link up 0x0002: Disable 0xFFFF: No port
0x1100 to 0x1111	1 word	HEX	Port 1 to 8 Speed 0x0000: 10M-Half 0x0001: 10M-Full 0x0002: 100M-Half 0x0003: 100M-Full 0xFFFF: No port
0x1200 to 0x1211	1 word	HEX	Port 1 to 8 Flow Ctrl 0x0000: Off 0x0001: On 0xFFFF: No port
0x1300 to 0x1311	1 word	HEX	Port 1 to 8 MDI/MDIX 0x0000: MDI 0x0001: MDIX 0xFFFF: No port

Address Offset	Data Type	Interpretation	Description
0x1400 to 0x1413 (Port 1) 0x1414 to 0x1427 (Port 2)	20 words	ASCII	Port 1 to 8 Description Port Description = "100TX,RJ45." Word 0 Hi byte = '1' Word 0 Lo byte = '0' Word 1 Hi byte = '0' Word 1 Lo byte = 'T' ... Word 4 Hi byte = '4' Word 4 Lo byte = '5' Word 5 Hi byte = '.' Word 5 Lo byte = '\0'
Packets Information			
0x2000 to 0x2023	2 words	HEX	Port 1 to 8 Tx Packets Ex: port 1 Tx Packet Amount = 44332211 Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211
0x2100 to 0x2123	2 words	HEX	Port 1 to 8 Rx Packets Ex: port 1 Rx Packet Amount = 44332211 Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211
0x2200 to 0x2223	2 words	HEX	port 1 to 8 Tx Error Packets Ex: port 1 Tx Error Packet Amount = 44332211 Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211
0x2300 to 0x2323	2 words	HEX	port 1 to 8 Rx Error Packets Ex: port 1 Rx Error Packet Amount = 44332211 Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211
Redundancy Information			

MODBUS/TCP MAP > MODBUS Data Map and Information Interpretation of VIPA Switches

Address Offset	Data Type	Interpretation	Description
0x3000	1 word	HEX	Redundancy Protocol 0x0000: None 0x0001: RSTP 0x0002: Turbo Ring 0x0003: Turbo Ring V2 0x0004: Turbo Chain 0x0005: MSTP
0x3100	1 word	HEX	RSTP Root 0x0000: Not Root 0x0001: Root 0xFFFF: RSTP Not Enable
0x3200 to 0x3211	1 word	HEX	RSTP Port 1 to 8 Status 0x0000: Port Disabled 0x0001: Not RSTP Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: RSTP Not Enable
0x3300	1 word	HEX	TurboRing Master/Slave 0x0000: Slave 0x0001: Master 0xFFFF: Turbo Ring Not Enable
0x3301	1 word	HEX	TurboRing 1st Port status 0x0000: Port Disabled 0x0001: Not Redundant Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding
0x3302	1 word	HEX	TurboRing 2nd Port status 0x0000: Port Disabled 0x0001: Not Redundant Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding

Address Offset	Data Type	Interpretation	Description
0x3303	1 word	HEX	TurboRing Coupling 0x0000: Off 0x0001: On 0xFFFF: Turbo Ring is Not Enabled
0x3304	1 word	HEX	TurboRing Coupling Port Status 0x0000: Port Disabled 0x0001: Not Coupling Port 0x0002: Link Down 0x0003: Blocked 0x0005: Forwarding 0xFFFF: Turbo Ring is Not Enabled
0x3305	1 word	HEX	TurboRing Coupling Control Port Status 0x0000: Port Disabled 0x0001: Not Coupling Port 0x0002: Link Down 0x0003: Blocked 0x0005: Forwarding 0x0006: Inactive 0x0007: Active 0xFFFF: Turbo Ring is Not Enabled
0x3500	1 word	HEX	TurboRing V2 Coupling Mode 0x0000: None 0x0001: Dual Homing 0x0002: Coupling Backup 0x0003: Coupling Primary 0 xFFFF: Turbo Ring V2 is not Enabled
0x3501	1 word	HEX	TurboRing V2 Coupling Port Primary Status (Used in Dual Homing, Coupling Backup, and Coupling Primary) 0x0000: Port Disabled 0x0001: Not Coupling Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: Turbo Ring V2 is not Enabled

Address Offset	Data Type	Interpretation	Description
0x3502	1 word	HEX	TurboRing V2 Coupling Port Backup Status (Only using in Dual Homing) 0x0000: Port Disabled 0x0001: Not Coupling Port 0 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: Turbo Ring V2 Not Enable
0x3600	1 word	HEX	TurboRing V2 Ring 1 status 0x0000: Healthy 0x0001: Break 0xFFFF: Turbo Ring V2 not Enable
0x3601	1 word	HEX	TurboRing V2 Ring 1 Master/Slave 0x0000: Slave 0x0001: Master 0xFFFF: Turbo Ring V2 Ring 1 not Enable
0x3602	1 word	HEX	TurboRing V2 Ring 1 1st Port Status 0x0000: Port Disabled 0x0001: Not Redundant Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: Turbo Ring V2 Ring 1 is not Enabled
0x3603	1 word	HEX	TurboRing V2 Ring 1's 2nd Port Status 0x0000: Port Disabled 0x0001: Not Redundant Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: Turbo Ring V2 Ring 1 is not Enabled
0x3680	1 word	HEX	TurboRing V2 Ring 2 Status 0x0000: Healthy 0x0001: Break 0xFFFF: Turbo Ring V2 Ring 2 is not Enabled

Address Offset	Data Type	Interpretation	Description
0x3681	1 word	HEX	TurboRing V2 Ring 2 Status 0x0000: Healthy 0x0001: Break 0xFFFF: Turbo Ring V2 Ring 2 is not Enabled
0x3682	1 word	HEX	TurboRing V2 Ring 2's 1st Port Status 0x0000: Port Disabled 0x0001: Not Redundant 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: Turbo Ring V2 Ring 2 is Not Enabled
0x3683	1 word	HEX	TurboRing V2 Ring 2's 2nd Port Status 0x0000: Port Disabled 0x0001: Not Redundant 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFF: Turbo Ring V2 Ring 2 is not Enabled
0x3700	1 word	HEX	Turbo Chain Switch Roles 0x0000: Head 0x0001: Member 0x0002: Tail 0xFFFF: Turbo Chain is not Enabled
0x3701	1 word	HEX	Turbo Chain 1st Port status 0x0000: Link Down 0x0001: Blocking 0x0002: Blocked 0x0003: Forwarding 0xFFFF: Turbo Ring V2 Ring 2 not Enable
0x3702	1 word	HEX	Turbo Chain 2nd Port status 0x0000: Link Down 0x0001: Blocking 0x0002: Blocked 0x0003: Forwarding 0xFFFF: Turbo Ring V2 Ring 2 not Enable
MSTP Register			

Address Offset	Data Type	Interpretation	Description
0x4000 ~ 0x407F	1 word, 0x0103 => port role = DesignatedPort port state = Forwarding	HEX	MSTP CIST Port Role / Port State 0x00: DisabledPort / 0x00 Port Disabled 0x01: DesignatedPort / 0x01 Discarding 0x02: RootPort / 0x02 Learning 0x03: AlternatePort / 0x03 Forwarding 0x04: BackupPort 0x06: Not MSTP Port / 0x06 not MSTP Port 0xFFFF: MSTP not Enable
0x4080 ~ 0x40FF	1 word, 0x0103 => port role = DesignatedPort port state = Forwarding	HEX	MSTP MSTI1 Port Role / Port State 0x00: DisabledPort / 0x00 Port Disabled 0x01: DesignatedPort / 0x01 Discarding 0x02: RootPort / 0x02 Learning 0x03: AlternatePort / 0x03 Forwarding 0x04: BackupPort 0x05: MasterPort 0x06: Not MSTP Port / 0x06 not MSTP Port 0xFFFF: MSTP not Enable
0x4100 ~ 0x417F	1 word, 0x0103 => port role = DesignatedPort port state = Forwarding	HEX	MSTP MSTI2 Port Role / Port State 0x00: DisabledPort / 0x00 Port Disabled 0x01: DesignatedPort / 0x01 Discarding 0x02: RootPort / 0x02 Learning 0x03: AlternatePort / 0x03 Forwarding 0x04: BackupPort 0x05: MasterPort 0x06: Not MSTP Port / 0x06 not MSTP Port 0xFFFF: MSTP not Enable
0x4180 ~ 0x41FF	1 word, 0x0103 => port role = DesignatedPort port state = Forwarding	HEX	MSTP MSTI3 Port Role / Port State 0x00: DisabledPort / 0x00 Port Disabled 0x01: DesignatedPort / 0x01 Discarding 0x02: RootPort / 0x02 Learning 0x03: AlternatePort / 0x03 Forwarding 0x04: BackupPort 0x05: MasterPort 0x06: Not MSTP Port / 0x06 not MSTP Port 0xFFFF: MSTP not Enable

Address Offset	Data Type	Interpretation	Description
0x4200 ~ 0x427F	1 word, 0x0103 => port role = DesignatedPort port state = Forwarding	HEX	MSTP MSTI4 Port Role / Port State 0x00: DisabledPort / 0x00 Port Disabled 0x01: DesignatedPort / 0x01 Discarding 0x02: RootPort / 0x02 Learning 0x03: AlternatePort / 0x03 Forwarding 0x04: BackupPort 0x05: MasterPort 0x06: Not MSTP Port / 0x06 not MSTP Port 0xFFFF: MSTP not Enable
0x4280 ~ 0x42FF	1 word, 0x0103 => port role = DesignatedPort port state = Forwarding	HEX	MSTP MSTI5 Port Role / Port State 0x00: DisabledPort / 0x00 Port Disabled 0x01: DesignatedPort / 0x01 Discarding 0x02: RootPort / 0x02 Learning 0x03: AlternatePort / 0x03 Forwarding 0x04: BackupPort 0x05: MasterPort 0x06: Not MSTP Port / 0x06 not MSTP Port 0xFFFF: MSTP not Enable
0x4300 ~ 0x437F	1 word, 0x0103 => port role = DesignatedPort port state = Forwarding	HEX	MSTP MSTI6 Port Role / Port State 0x00: DisabledPort / 0x00 Port Disabled 0x01: DesignatedPort / 0x01 Discarding 0x02: RootPort / 0x02 Learning 0x03: AlternatePort / 0x03 Forwarding 0x04: BackupPort 0x05: MasterPort 0x06: Not MSTP Port / 0x06 not MSTP Port 0xFFFF: MSTP not Enable
0x4380 ~ 0x43FF	1 word, 0x0103 => port role = DesignatedPort port state = Forwarding	HEX	MSTP MSTI7 Port Role / Port State 0x00: DisabledPort / 0x00 Port Disabled 0x01: DesignatedPort / 0x01 Discarding 0x02: RootPort / 0x02 Learning 0x03: AlternatePort / 0x03 Forwarding 0x04: BackupPort 0x05: MasterPort 0x06: Not MSTP Port / 0x06 not MSTP Port 0xFFFF: MSTP not Enable

6.2 EtherNet/IP

This chapter is under preparation!

6.3 PROFINET I/O

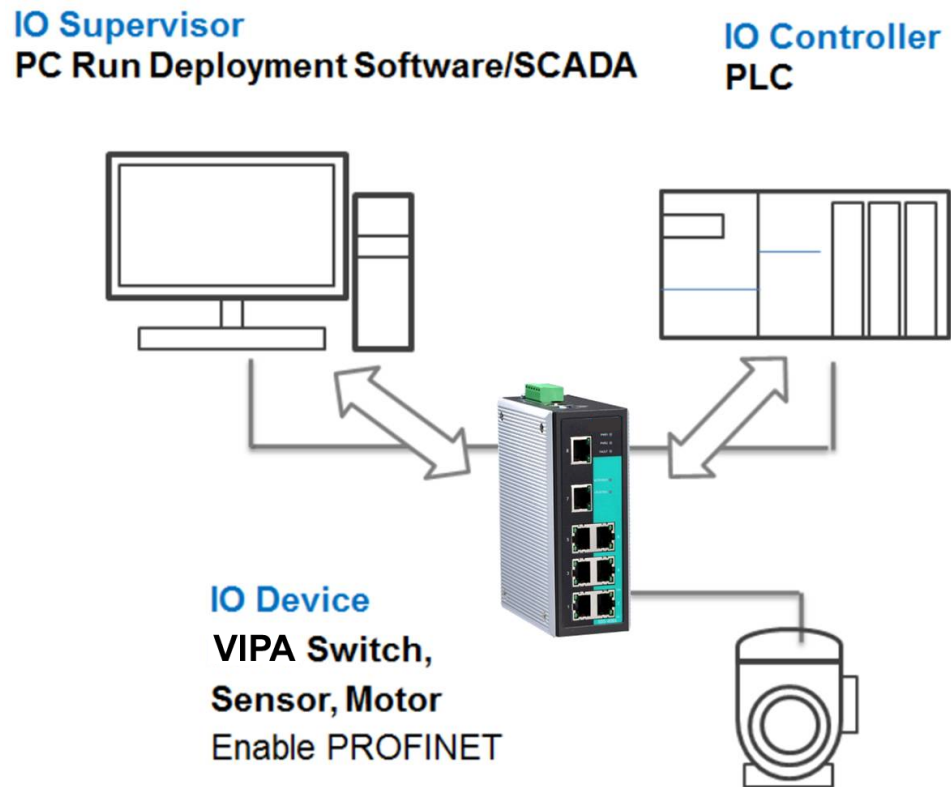
6.3.1 Introduction

PROFINET is a communication standard for automation of PROFIBUS & PROFINET International (PI). It is 100% Ethernet-compatible as defined in IEEE standards. With PROFINET, applications can be implemented for production and process automation, safety applications, and the entire range of drive technology. With its integrated Ethernet-based communication, PROFINET satisfies a wide range of requirements, from data-intensive parameter assignment to extremely fast I/O data transmission. PROFINET I/O is used for data exchange between I/O controllers (PLC, etc.) and I/O devices (field devices). This specification defines a protocol and an application interface for exchanging I/O data, alarms, and diagnostics. And its real-time (RT) solution allows response time in the range of 5 ms, which corresponds to today's PROFIBUS DP applications.

6.3.2 PROFINET Environmental Introductions

PROFINET Networking Structure

PROFINET I/O follows the Provider/Consumer model for data exchange. PROFINET forms logical link relationships between network character types. They are shown below.



There are 3 major character types defined by PROFINET I/O, including I/O controller, I/O supervisor, and I/O devices. Switches are considered I/O devices.

- I/O Controller
 - This is typically the programmable logic controller (PLC) on which the automation program runs. The I/O controller provides output data to the configured I/O-devices in its role as provider and is the consumer of input data of I/O devices.
- I/O Supervisor
 - This can be a programming device, personal computer (PC), or human machine interface (HMI) device for commissioning or diagnostic purposes.
- I/O Device
 - An I/O device is a distributed I/O field device that is connected to one or more I/O controllers via PROFINET I/O. The I/O device is the provider of input data and the consumer of output data.

An I/O device is a distributed I/O field device that is connected to one or more I/O controllers via PROFINET I/O. The I/O device is the provider of input data and the consumer of output data.

PROFINET I/O Devices

The VIPA switch is a PROFINET I/O device. A device model describes all field devices in terms of their possible technical and functional features. It is specified by the DAP (Device Access Point) and the defined modules for a particular device family. A DAP is the access point for communication with the Ethernet interface and the processing program.

PROFINET Protocols

- DCP
 - In PROFINET I/O, each field device has a symbolic name that uniquely identifies the field device within a PROFINET I/O system. This name is used for assigning the IP address and the MAC address. The DCP protocol (Dynamic Configuration Protocol) integrated in every I/O device is used for this purpose.
- DHCP
 - Because DHCP (Dynamic Host Configuration Protocol) is in widespread use internationally, PROFINET has provided for optional address setting via DHCP or via manufacturer-specific mechanisms.
- PROFINET Type LLDP
 - Automation systems can be configured flexibly in a line, star, or tree structure. To compare the specified and actual topologies, to determine which field devices are connected to which switch port, and to identify the respective port neighbour, LLDP according to IEEE 802.1AB was applied in PROFINET I/O. PROFINET filed bus exchange existing addressing information with connected neighbour devices via each switch port. The neighbour devices are thereby unambiguously identified and their physical location is determined.

Device descriptions

- GSD file
 - The GSD files (General Station Description) of the field devices to be configured are required for system engineering. This XML-based GSD describes the properties and functions of the PROFINET I/O field devices. It contains all data relevant for engineering as well as for data exchange with the device. Find your field device GSD file in the CD or download the GSD file from the VIPA web site.

6.3.3 Configuring PROFINET I/O on VIPA Switches

Enable PROFINET in WEB UI



- ➔ Select the 'Enable' option and click [Activate] to enable PROFINET I/O.
 - ⇒ With PROFINET I/O enabled, PROFINET type LLDP will be enabled automatically.
- ➔ Select the 'Disable' option and click [Activate] to disable PROFINET I/O.
 - ⇒ The switch will disable PROFINET type LLDP and use standard LLDP.

CLI

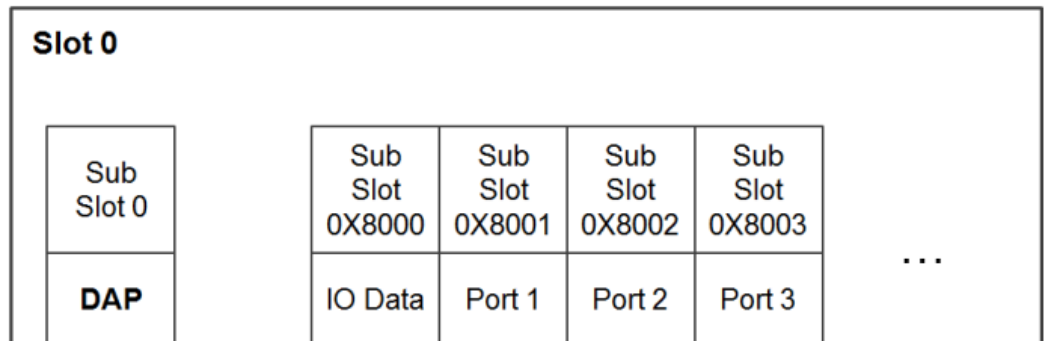
The CLI (command line interface) can be used to enable or disable PROFINET for the switch.

Command List:

- profinetio to enable PROFINET I/O.
- no profinetio to disable PROFINET I/O.

6.3.4 Addressing of I/O Data in PROFINET I/O Based on Slot and Sub-Slots

The concept of the VIPA PROFINET switch with GSD version 2 is shown the table below. In this structure, each switch port represents one sub-slot.



Manufacturer Information

Each PROFINET device is addressed based on a MAC address. This address is unique worldwide. The company code (bits 47 to 24) can be obtained from the IEEE Standards Department free of charge. This part is called the OUI (organizationally unique identifier).

Table of VIPA OUI

Bit Value 47..24						Bit Value 23..0					
0	0	0	2	2	9	x	x	x	x	x	x
Company Code (OUI)						Consecutive Number					

6.3.5 PROFINET Attributes

The PROFINET I/O connection can be configured for both cyclic I/O data and I/O parameters. I/O parameters are acyclic I/O data. These are major setup and monitor attributes in PROFINET.

- **Cyclic I/O Data**
Cyclic I/O data are always sent between the PLC and Switches at the specified periodic time. These data are transmitted almost real time. For example, status information from the Switches, and variables to be written to the Switch would typically be part of the cyclic data.
- **I/O Parameters**
PROFINET I/O parameters are defined for device configuration and status monitoring. These data are useful for infrequent data transfers, or for very large data transfers. Only transfer when needed
- **Alarm**
Alarms are mainly PROFINET I/O transmitted high-priority events. Alarm data are exchanged between an I/O device and an I/O controller. Once an event triggers it, the switch will send the alarm to the PLC immediately. Enable or disable these alarms by setting I/O parameters.

PROFINET Cyclic I/O Data

The VIPA PROFINET switch provides PROFINET I/O cyclic data and includes the following items:



The default transfer frequency of PROFINET Cyclic I/O data is 128 ms. There are 3 options available in Siemens SIMATIC STEP®7: 128/256/512 ms.

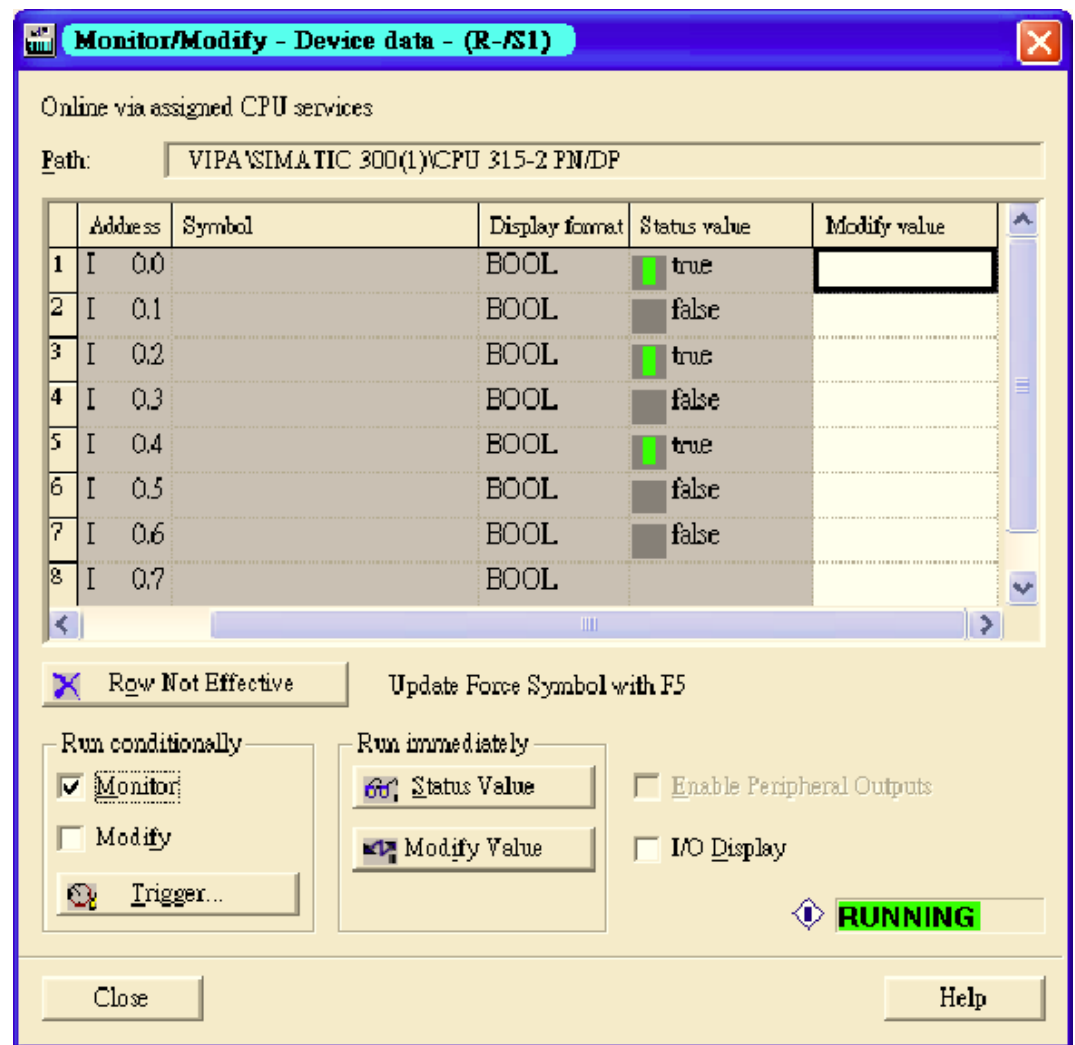
PROFINET Cyclic I/O Data Table

Category	Direction	Byte	Bit	Name	Description
Device	Input	0	0	Device status	0 is failed status, 1 is OK.
			1	Power 1	0 is unavailable, 1 is OK
			2	Power 2	0 is unavailable, 1 is OK
			3	RSTP status	0 is disabled, 1 is enabled
			4	Turbo Ring v1	0 is disabled, 1 is enabled
			5	Turbo Ring v2	0 is disabled, 1 is enabled
			6	Turbo Chain	0 is disabled, 1 is enabled
			7	Turbo Ring v2 status	0 is broken, 1 is healthy
Port	Input	1	0	Port 1 Connection	0 is not connected, 1 is connected
			1	Port 2 Connection	0 is not connected, 1 is connected
			2	Port 3 Connection	0 is not connected, 1 is connected
			3	Port 4 Connection	0 is not connected, 1 is connected

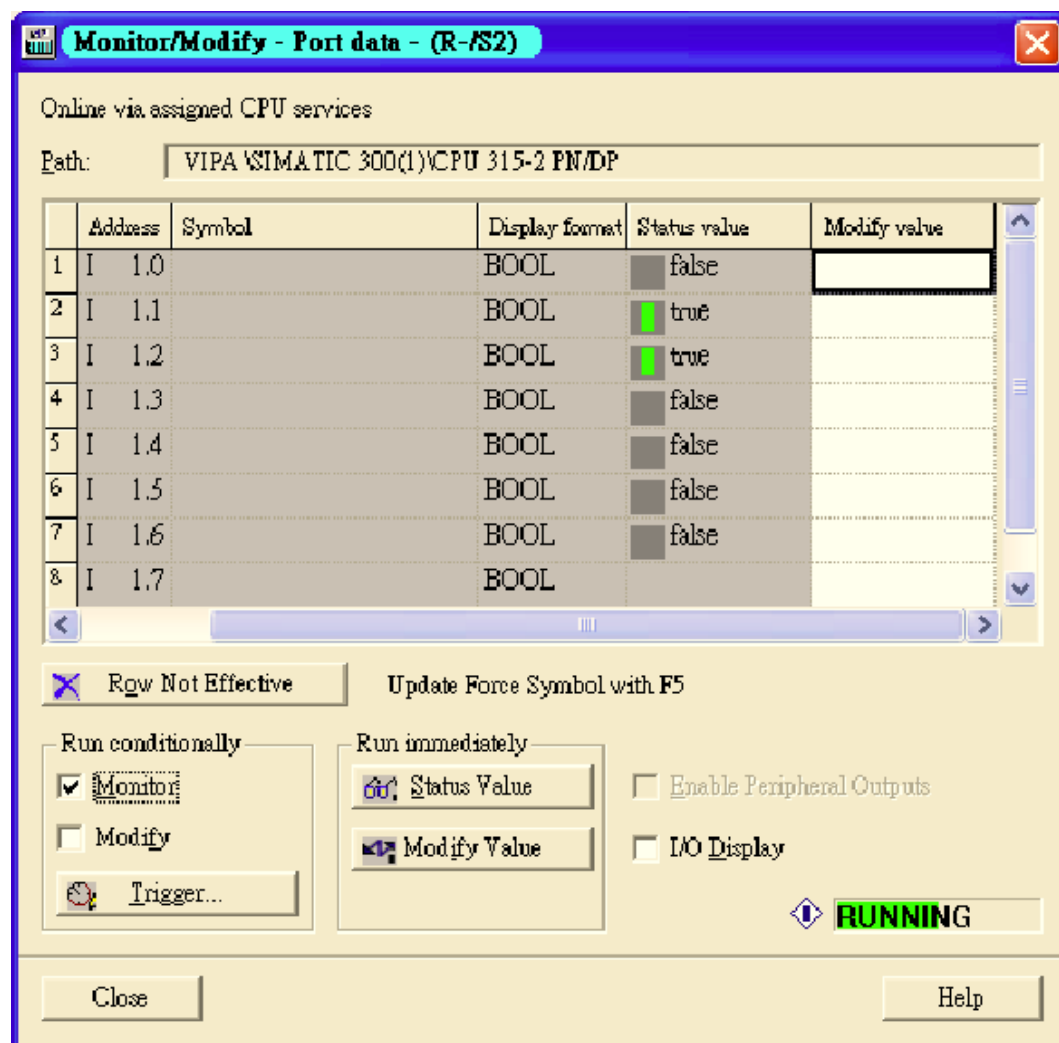
Category	Direction	Byte	Bit	Name	Description
			4	Port 5 Connection	0 is not connected, 1 is connected
			5	Port 6 Connection	0 is not connected, 1 is connected
			6	Port 7 Connection	0 is not connected, 1 is connected
			7	Port 8 Connection	0 is not connected, 1 is connected

You can monitor these attributes in Siemens SIMATIC STEP®7.

Monitor Device I/O Cyclic Data in Siemens SIMATIC STEP®7



Monitor Port I/O Cyclic Data in Siemens SIMATIC STEP®7



PROFINET I/O Parameters

VIPA defines comprehensive PROFINET I/O parameters for more flexible settings and monitoring. These attributes are readable or writable. PROFINET I/O parameters use PROFINET acyclic data to achieve communication in the network. You can use the Siemens SIMATIC STEP®7 tool or engineering deployment software to edit it. There are 3 categories of parameters, including Device Parameters, Device Status and Port Parameters. The following tables provide parameter information:

- **r/w:** Read and Write
- **ro:** Read Only

Device parameters

These parameters control PROFINET Alarm functions. PROFINET Alarm is a message which sends from switch to PLC immediately once the event is triggered.

Byte	Name	Access	Value	Description	Default Value
0	Status Alarm	rw	0	Do not send any alarms	0: No alarms
			1	Send alarm if any status change	
1	Power Alarm 1	rw	0	Do not send power failed alarms	0: No alarms
			1	Send alarm if power supply 1 fails	

PROFINET I/O > PROFINET Attributes

Byte	Name	Access	Value	Description	Default Value
2	Power Alarm 2	rw	0	Do not send power failed alarms	0: No alarms
			1	Send alarm if power supply 2 fails	

Device Status

Byte	Name	Access	Value	Description
0	Device Status	ro	0	Unavailable
			1	OK
			2	Device bootup fails
1	Fault Status	ro	0	Unavailable
			1	OK
			2	Device detect fault
2	Power 1 Status	ro	0	Unavailable
			1	OK
			2	Power 1 fails
3	Power 2 Status	ro	0	Unavailable
			1	OK
			2	Power 2 fails
4	DI 1 Status	ro	0	Unavailable
			1	Closed
			2	Open
5	DI 2 Status	ro	0	Unavailable
			1	Closed
			2	Open
6	Redundant Mode	ro	0	Unavailable
			1	RSTP
			2	Turbo Ring V1
			3	Turbo Ring V2
			4	Turbo Chain
7	Ring Status	ro	0	Unavailable
			1	Healthy
			2	Break
8	Redundant Port 1 Status	ro	0	Unavailable
			1	Link is up
			2	Link is down
9	Redundant Port 2 Status	ro	0	Unavailable
			1	Link is up

Byte	Name	Access	Value	Description
			2	Link is down
10	Ring Coupling Mode	ro	0	Unavailable
			1	Backup
			2	Primary
			3	Dual homing
11	Coupling Port 1 Status	ro	0	Unavailable
			1	Link is up
			2	Link is down
12	Coupling Port 2 Status	ro	0	Unavailable
			1	Link is up
			2	Link is down
13	Connection	ro	0	Unavailable
			1	OK
			2	Connection failure

Port Parameters

Byte	Name	Access	Value	Description
0	Port Alarm	rw	0	Do not send alarm
			1	Send alarm when port link down
1	Port Admin State	rw	0	Unavailable
			1	Off
			2	On
2	Port Link State	ro	0	Unavailable
			1	Link is up
			2	Link is down
3	Port Speed	ro	0	Unavailable
			1	10
			2	100
			3	1000
4	Port duplex	ro	0	Unavailable
			1	Half
			2	Full
5	Port Auto-negotiation	ro	0	Unavailable
			1	Off
			2	On
6	Port flow control	ro	0	Unavailable

Byte	Name	Access	Value	Description
			1	Off
			2	On
7	Port MDI/MDIX		0	Unavailable
		ro	1	MDI
			2	MDIX

6.3.6 Siemens STEP®7 Integration

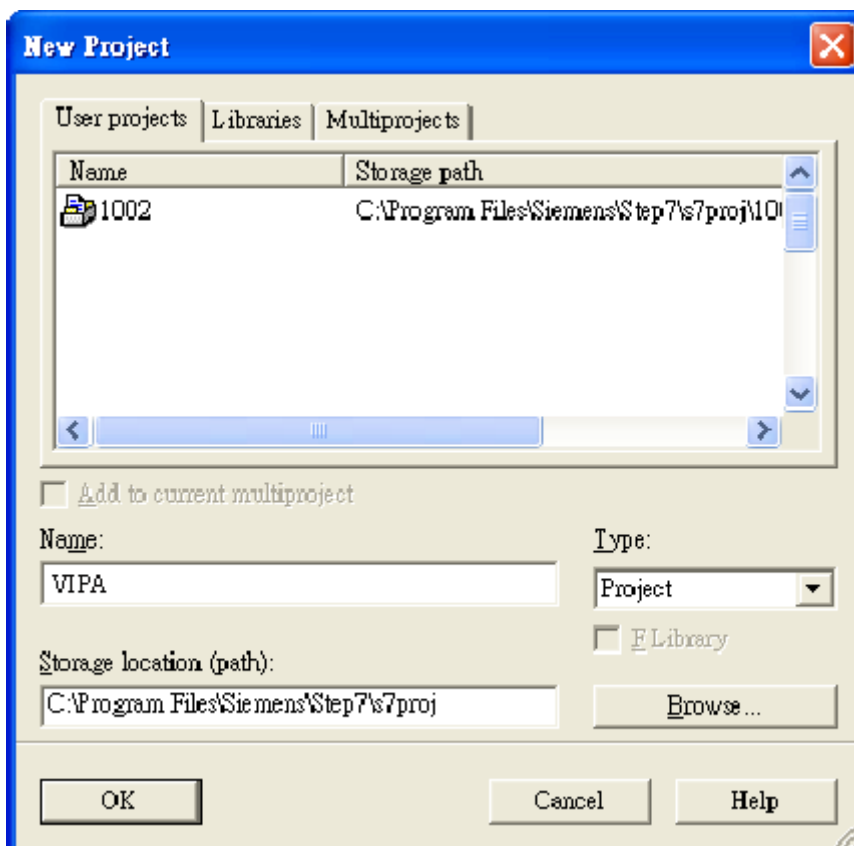
Overview of Operation Procedure

The following steps show how to integrate the switch into a PROFINET network:

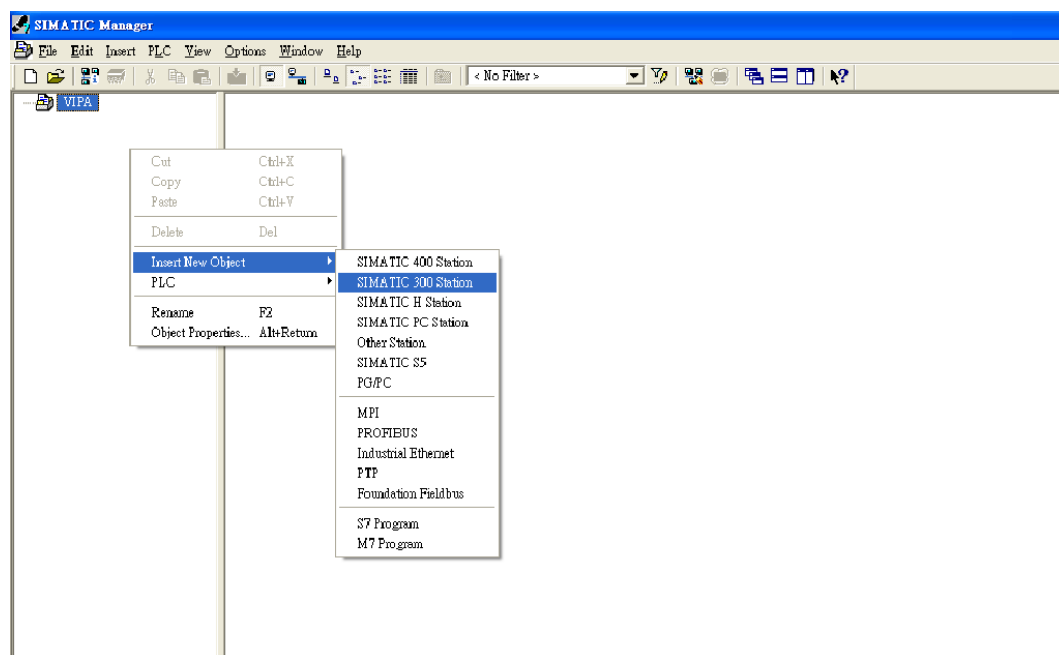
1. ➤ Enable PROFINET IO on the switch
 - Enable PROFINET in switch web UI
2. ➤ Create a PROFINET I/O subnet project in Siemens STEP®7
 - Create a PROFINET I/O Ethernet project for deploying environment
3. ➤ GSD file installation
 - Import VIPA switch GSD into the project
4. ➤ Device configuration
 - Search and discover the switch in Siemens STEP®7. Configure PROFINET attributes such as IP address, device name and I/O parameters.
5. ➤ Save and load the project into the PLC
 - Load this project and into the PLC
6. ➤ Monitoring the Switch
 - Use Siemens STEP®7 to monitor switch attributes

Create a PROFINET I/O Subnet Project

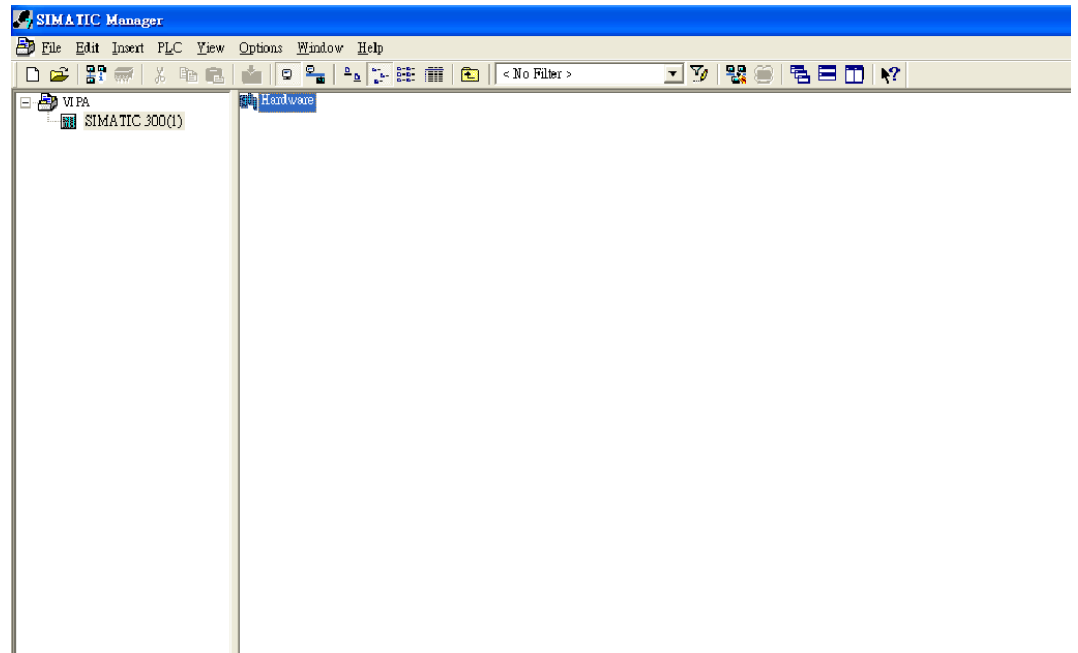
1. In Siemens SIMATIC Manager menu bar, click 'File → New Project'



2. Name your project in the 'Name' field then click [OK].
3. Insert a station in your project. Right click in category column 'Insert New Object → your PLC series' (here we select Siemens SIMATIC 300 station).

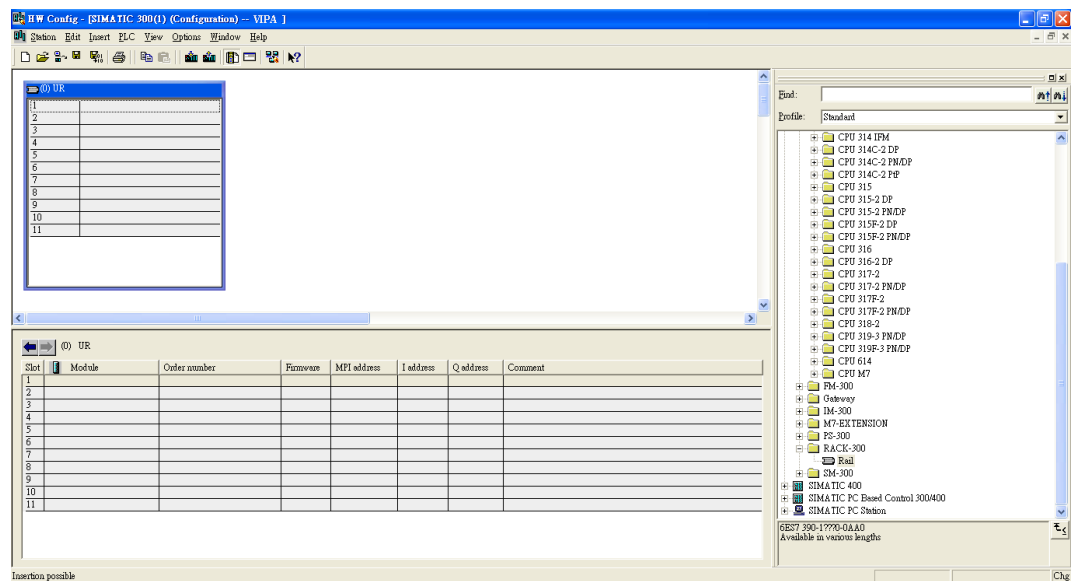


4. Then you can see the new object in the project. Double click on the 'Hardware'.

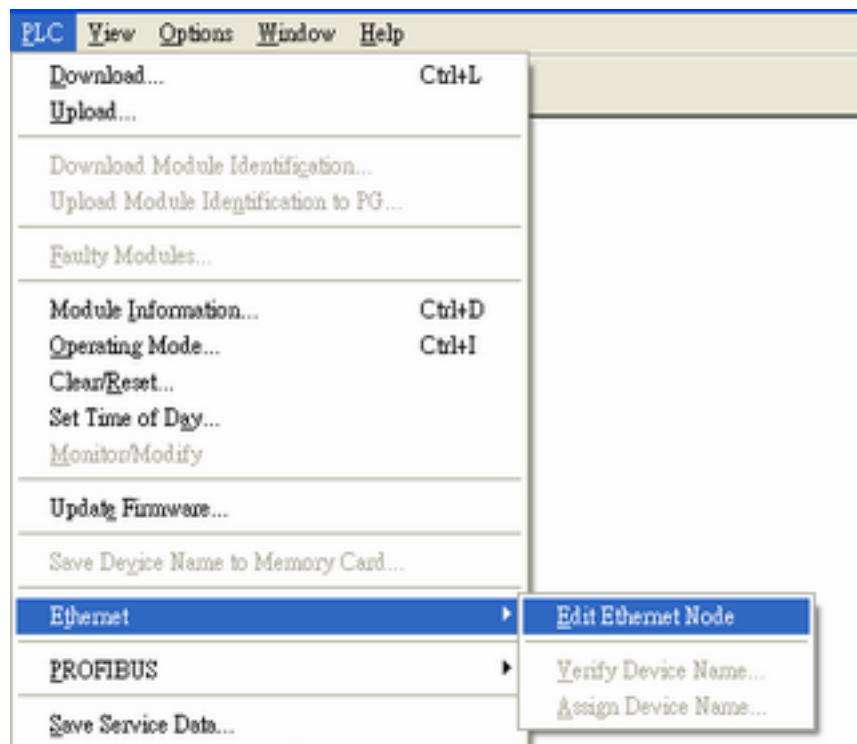


5. Add Rack in HW Config: After double-clicking on HW, you will see the 'HW Config' window.

6. Drag a rack from the side bar to main dashboard. In here, we drag 'Rail', which is under the Rack-300 folder, to the main screen.



7. Search PROFINET Ethernet devices: Use Edit 'Ethernet Node' to browse device information in PROFINET networks. Click 'PLC → Ethernet → Edit Ethernet Node'



8. Then click [Browse]

Edit Ethernet Node

Ethernet node

MAC address: Nodes accessible online

Set IP configuration

Use IP parameters

IP address: Gateway

Subnet mask: Do not use router

Use router

Address:

Obtain IP address from a DHCP server

Identified by

Client ID MAC address Device name

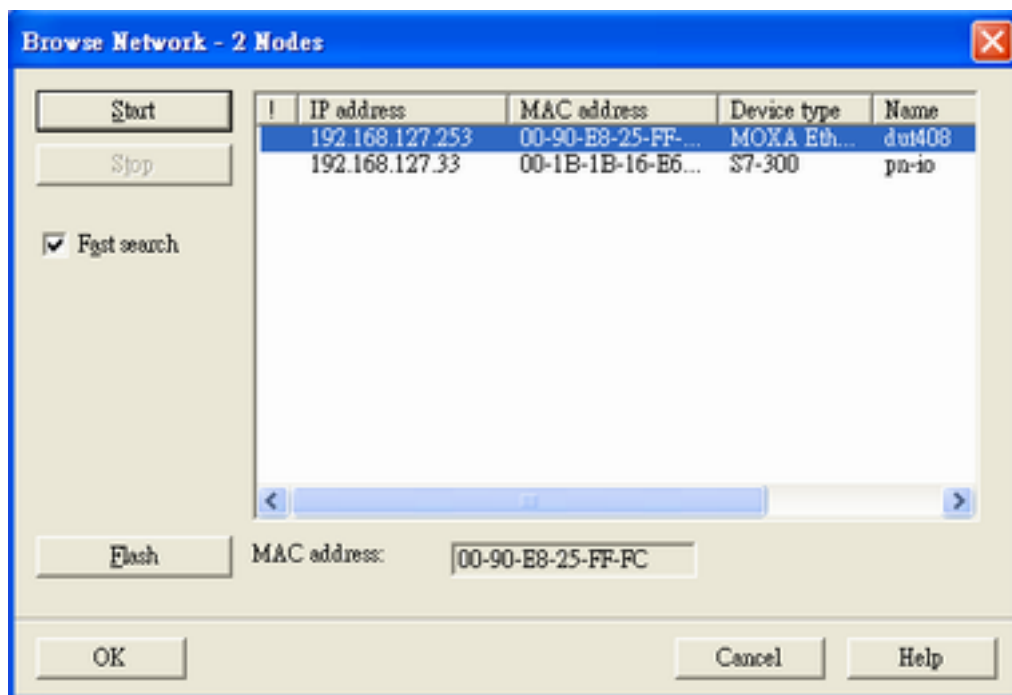
Client ID:

Assign device name

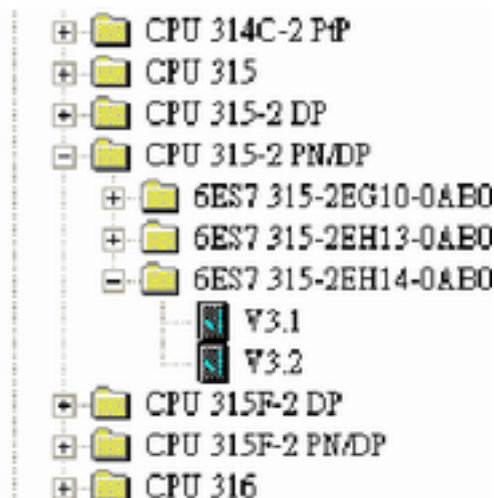
Device name:

Reset to factory settings

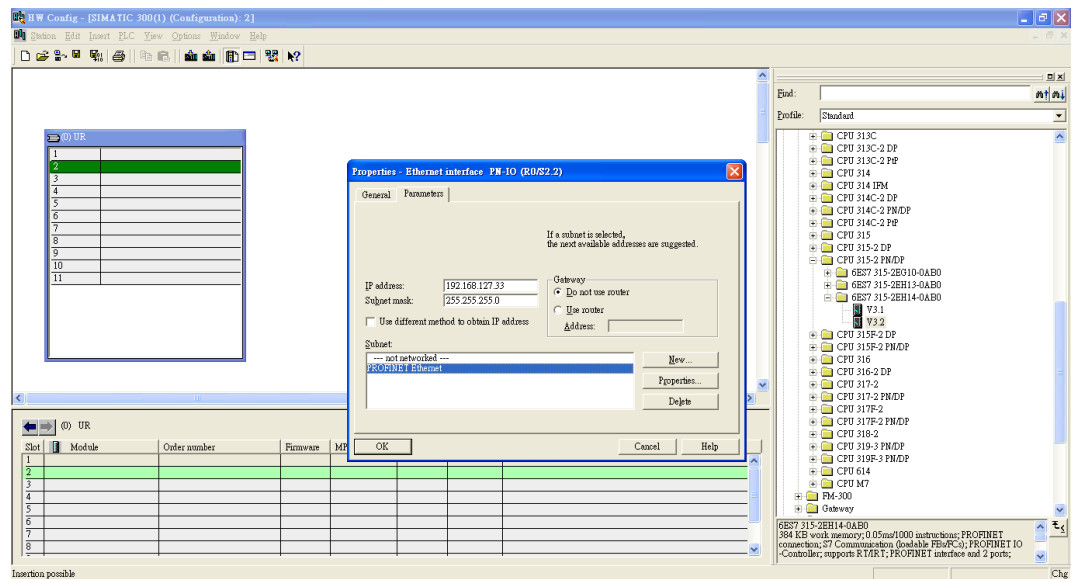
9. Click [Start] to search devices. Use Siemens STEP@7 through PROFINET DCP to discover devices in networks. Find PLC/switch IP addresses, MAC addresses, and device names here.



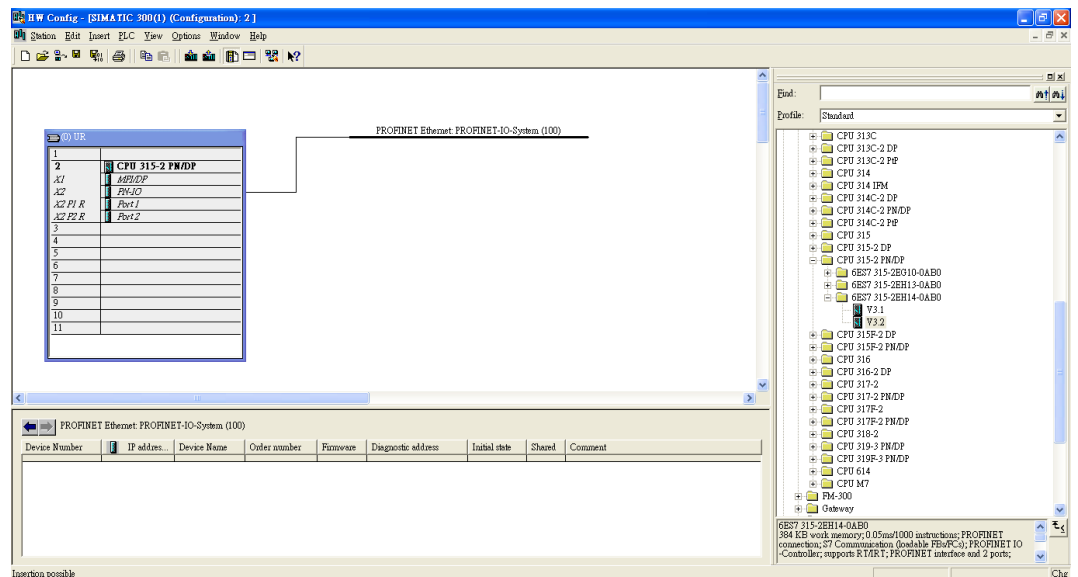
10. Add PLC CPU in HW Config: Select your PLC CPU and drag it to the rack slot 2. Please select by PLC you used. Here we will select 6ES7-315-2EH14-0AB0 V3.1.



- Then click Properties, the Ethernet interface dialog will pop out. Fill in your PLC IP address in 'IP address' column. Then click [New] in subnet to create a new Ethernet subnet. Here we will create a subnet named 'PROFINET Ethernet'.



⇒ PROFINET I/O Ethernet subnet project accomplished



GSDML File Installation

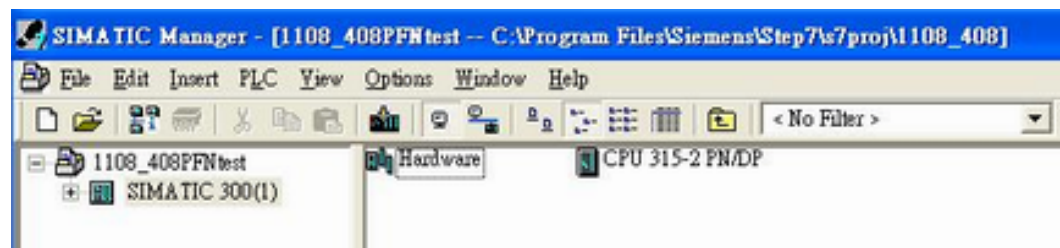
For every Switch from VIPA there is a GSDML file available. This file may either be found on the supplied storage media or at the download area of www.vipa.com.

The assignment of the GSDML file to your slave is shown in the following table:

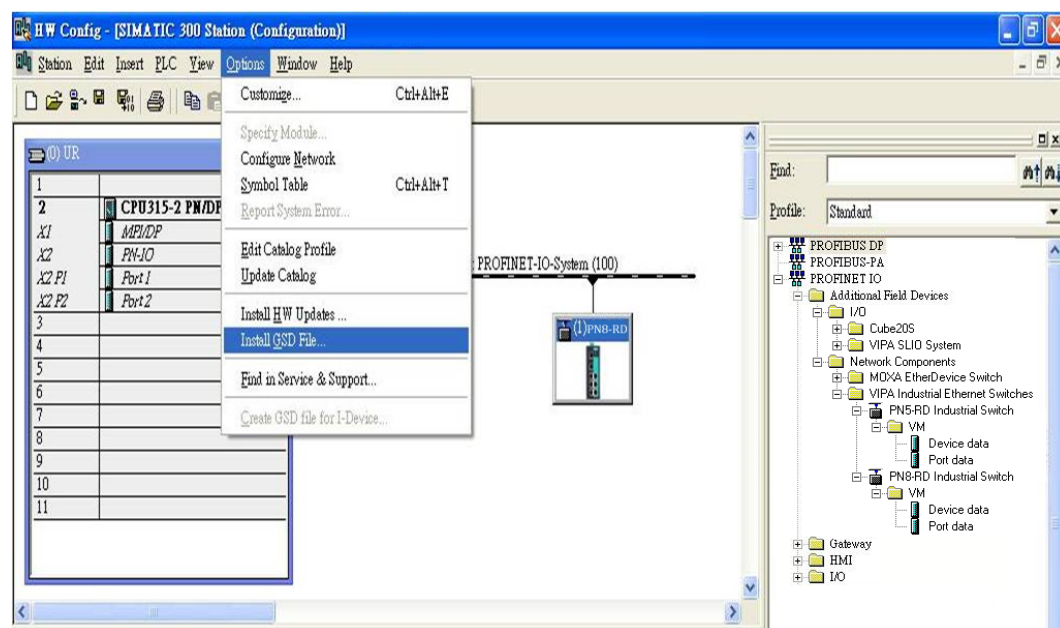
Variant	GSD file
911-2PN50	GSDML-V2.3-VIPA-PN5-RD-20160118.xml
911-2PN80	GSDML-V2.3-VIPA-PN8-RD-20160118.xml

- Open Siemens SIMATIC Manager on your PC.
- Open your project.

3. Open hardware configuration.

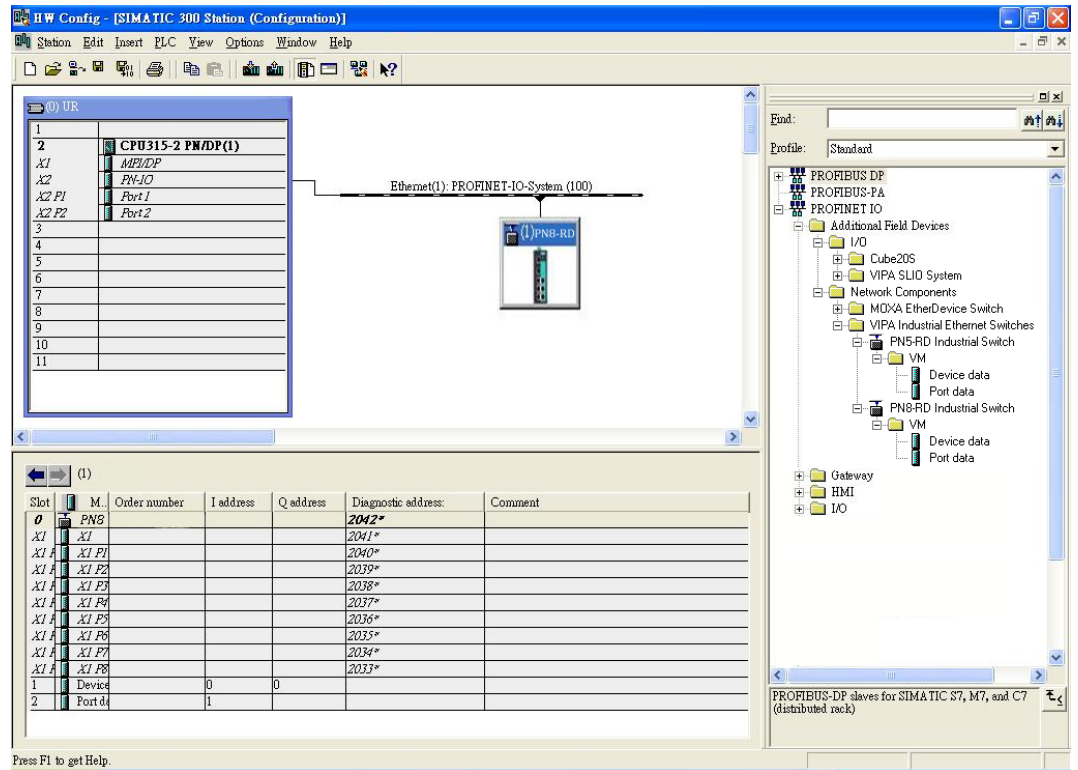


4. Install the GSDML file: Put the GSDML file and the icon file on your PC at the same folder. Click 'Options → Install GSD File'. Click [Browse...] to select the GSDML file just saved and click [Install].



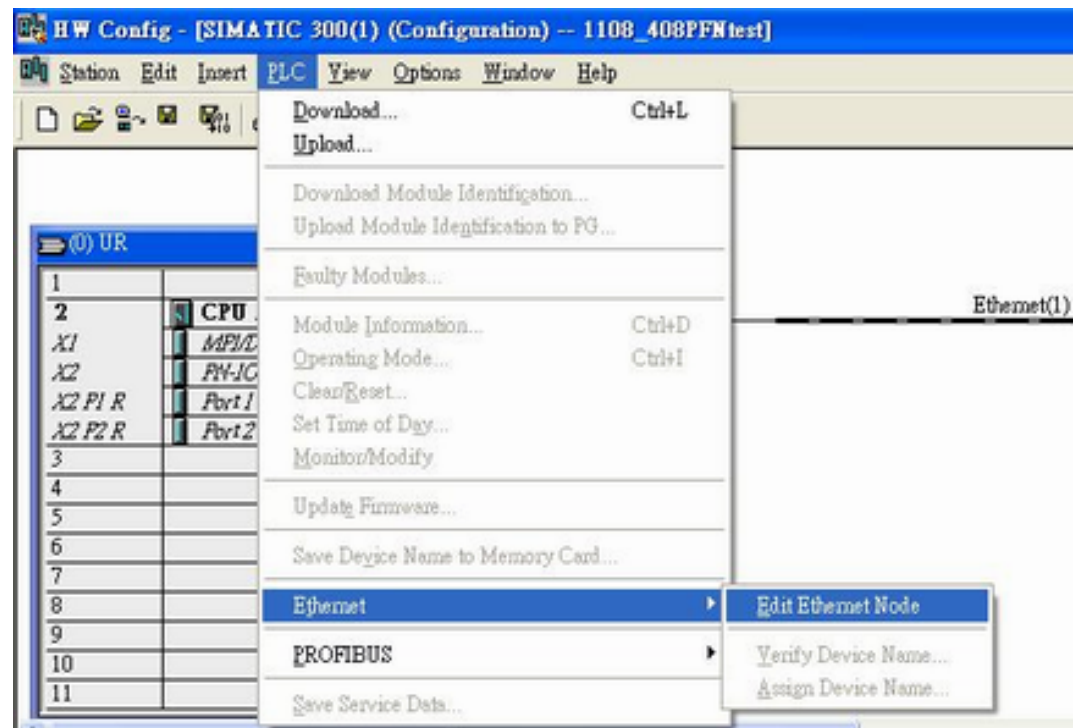
5. You will find the new VIPA switch under 'PROFINET IO → Additional Field Devices → Network Components → EtherDevice Switch'.

- Use Drag & Drop to pull the VIPA switch onto the bus cable. And you can see the VIPA switch icon displayed on the screen



Device Configuration

1. Browse the switch
 - Select 'PLC → Ethernet → Edit Ethernet Node' to open the Browse dialog.



- ⇒ ■ After the Edit 'Ethernet Node' dialog box appears, click [Browse].

Edit Ethernet Node

Ethernet node

MAC address: Nodes accessible online
Browse...

Set IP configuration

Use IP parameters

IP address: Gateway

Subnet mask: Do not use router

Use router

Address:

Obtain IP address from a DHCP server

Identified by

Client ID MAC address Device name

Client ID:

Assign IP Configuration

Assign device name

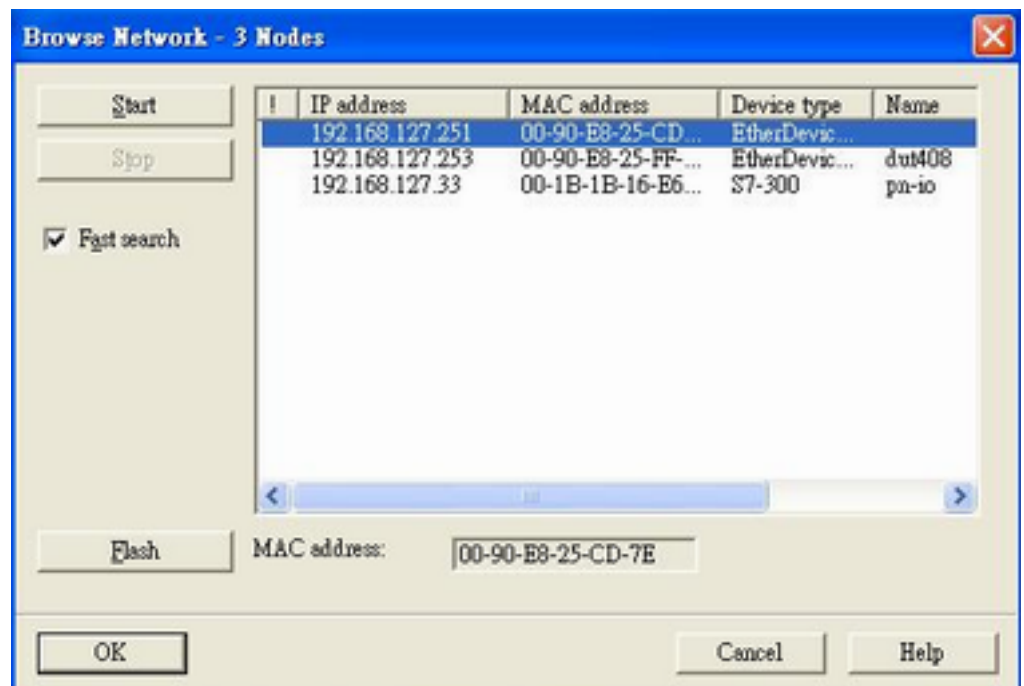
Device name: Assign Name

Reset to factory settings

Reset

Close Help

- Select your target switch and click [OK]



2. ➔ Assign IP address and Device name
 - Click [Assign IP configuration] and give the switch an IP address and subnet mask.
 - Click [Assign Name] and give the switch a name.
 - Click [Close] to finish.



The field 'Device name' does not allow any empty spaces in the name. If the device name is entered with a space, the system will remove words after the space automatically.

3. ➤ Set IP address and device for your project
- Double-click the switch icon to open switch property menu.
 - Set the 'Device name' and 'IP address' corresponding with those you have just assigned in STEP@7.
 - 'Use IP parameters':
 - Manual input of 'IP address' and 'Subnet mask'
 - 'Obtain IP address from a DHCP server':
 - Select 'MAC address' then click [Assign IP configuration].

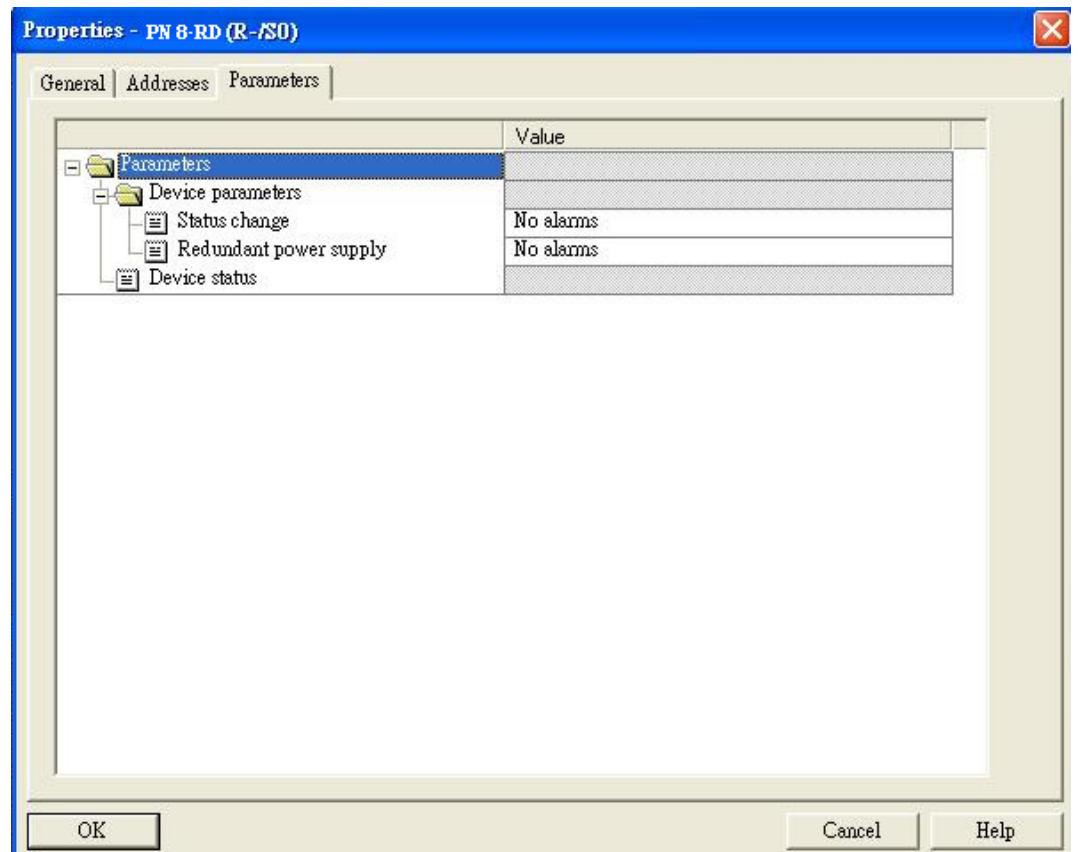
- ⇒ ■ After the IP has been assigned by DHCP, click [Browse] again to check the assigned IP address.
- Click [Save and Compile] then click [download to Module].

4. ➔ Configuring device properties

- Select the switch and double-click the first *sub-module slot 0* to set device properties.

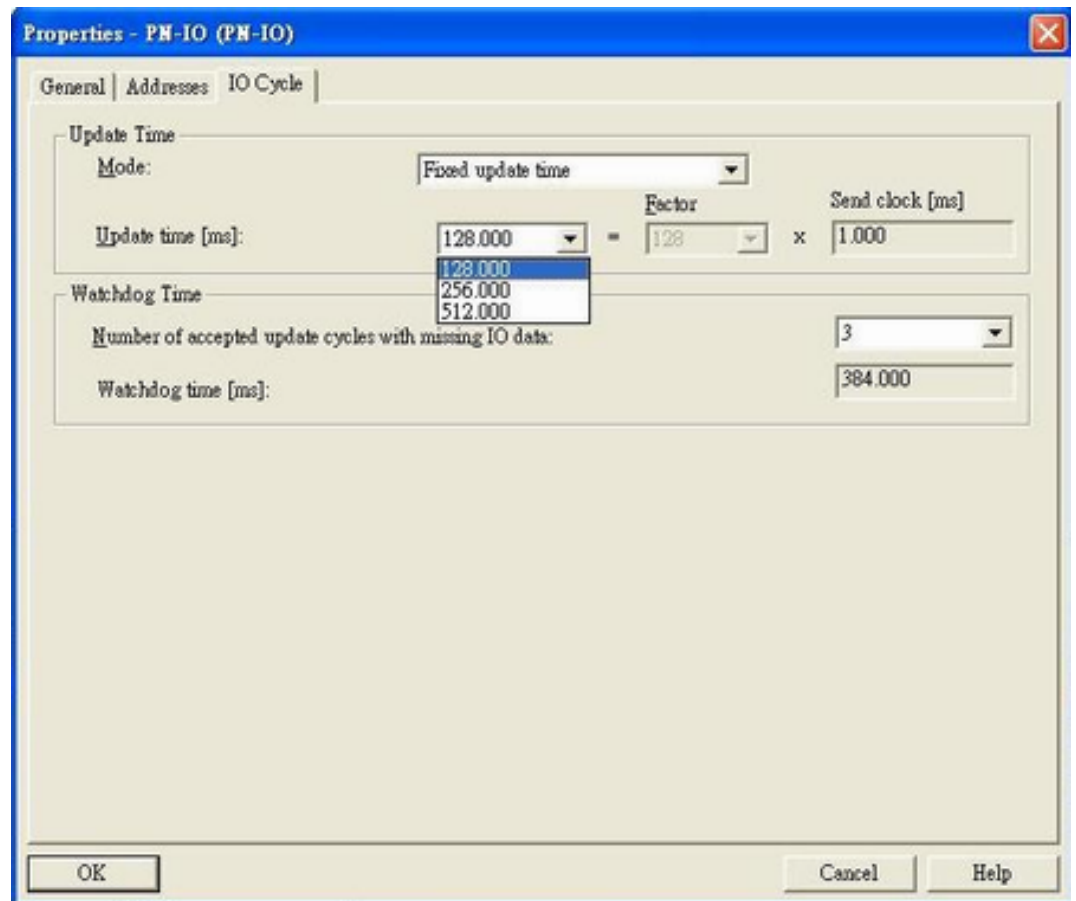
Slot	Module	Order number	I address	Q address
0	PN8-RD			
XI	XI			
XI A	XI F1			
XI A	XI F2			
XI A	XI F3			
XI A	XI F4			
XI A	XI F5			
XI A	XI F6			
XI A	XI F7			
XI A	XI F8			
1	Device data		0	
2	Port data		1	

- ⇒ ■ Select 'Parameters' and change the device parameter settings.
- Click [Save and Compile], then click [download to Module].



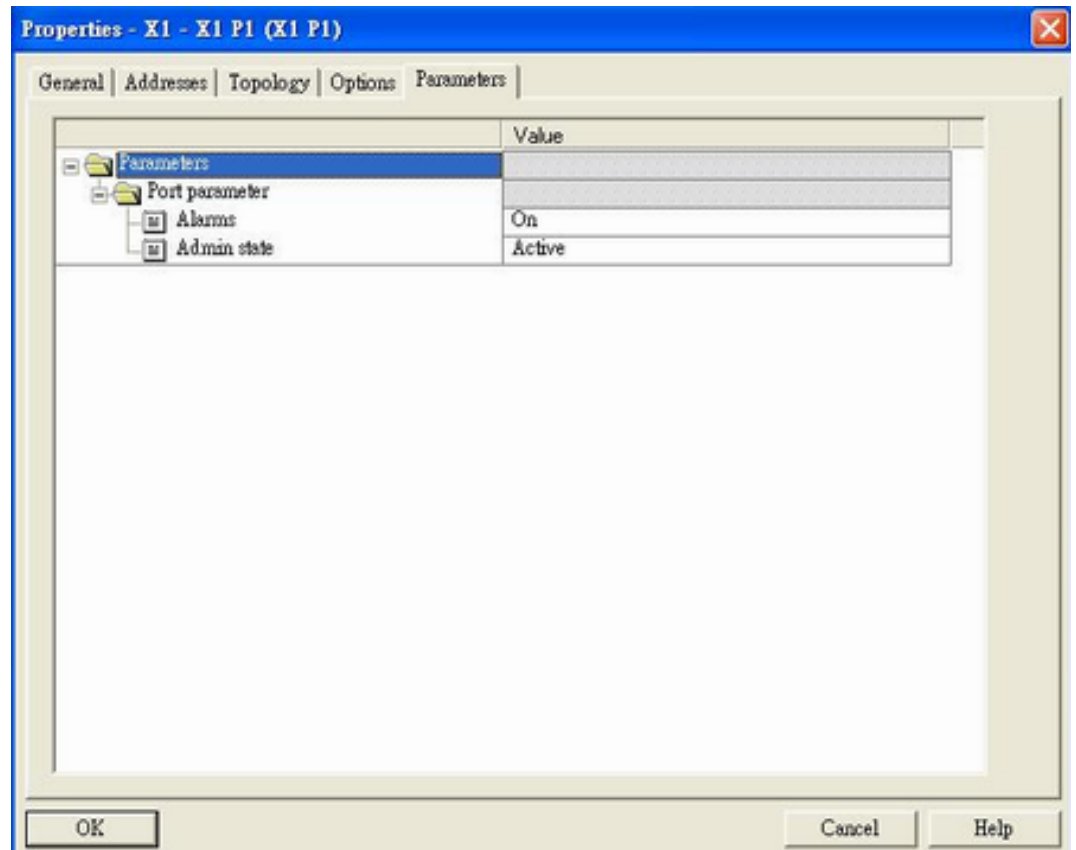
5. ➤ Configuring I/O cycle

- Select the switch and double-click the '*sub-module X1*' to set the I/O cycle.
- Select '*I/O Cycle*' and change the I/O cycle settings. Click [Save and Compile], then click [download to Module].



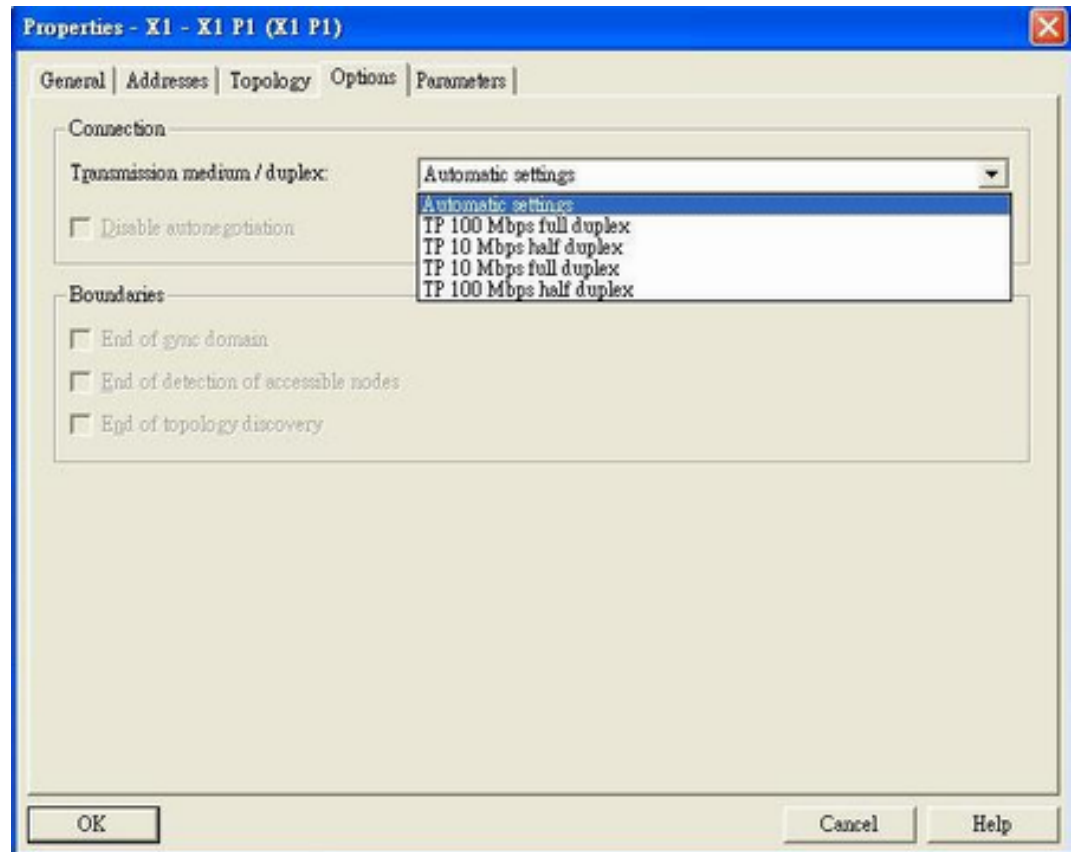
6. → Configuring port property

- Select the switch and double-click the 'sub-module X1 PN' to set port property.
- Select 'Parameters'.
- Change the port parameters settings.
- Click [Save and Compile] then click [download to Module].



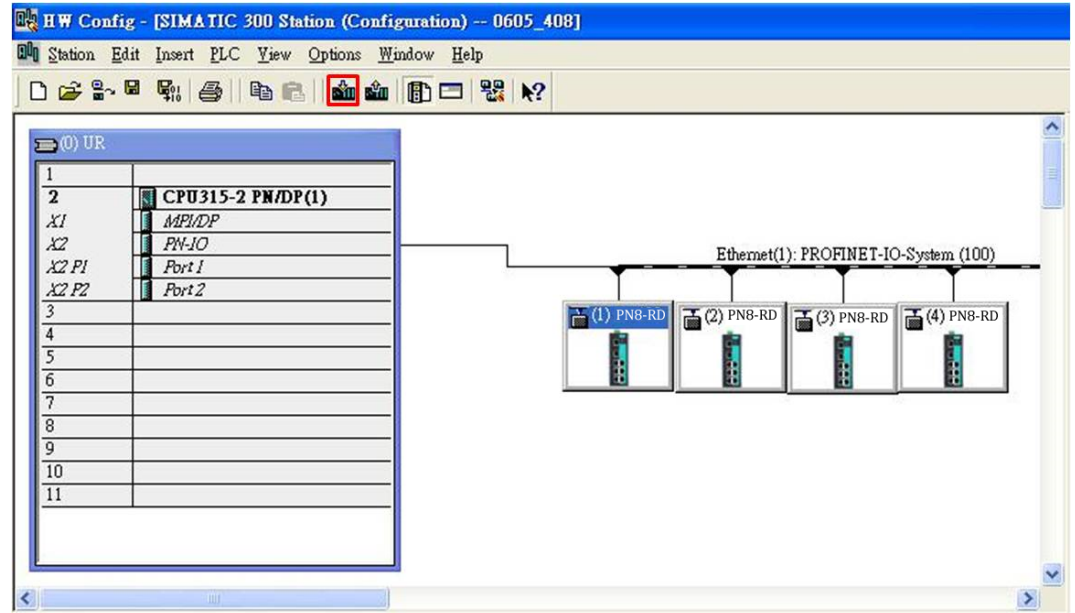
7. ➤ Configuring connection options

- Select the switch and double-click the 'sub-module X1 PN' to set port options.
- Select 'Options'.
- Change the port option settings.
- Click [Save and Compile], then click [download to Module]



Save and Load the Project into the PLC

- ➔ Click the icon (in red box) to download project configuration to the PLC.
- ⇒ After the project is configured, Siemens SIMATIC STEP®7 will load all information required for data exchange to the I/O Controller (PLC), including the IP addresses of the connected I/O devices.

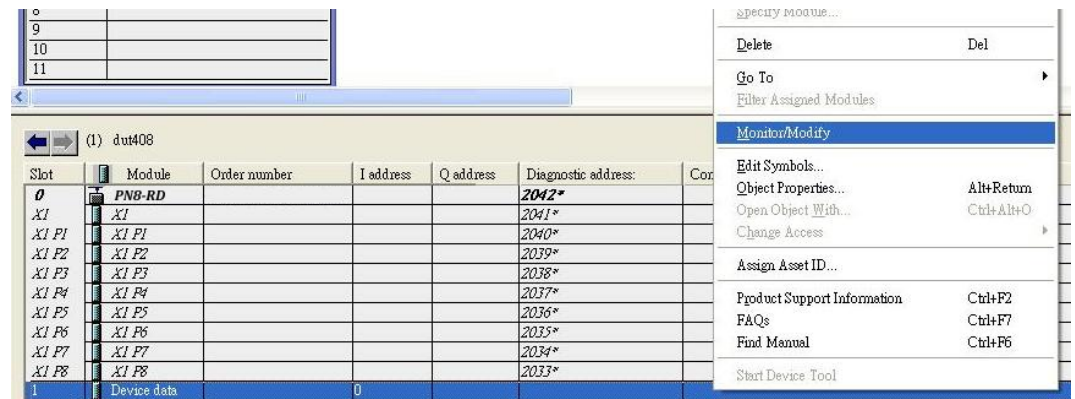


6.3.7 Monitoring the Switch

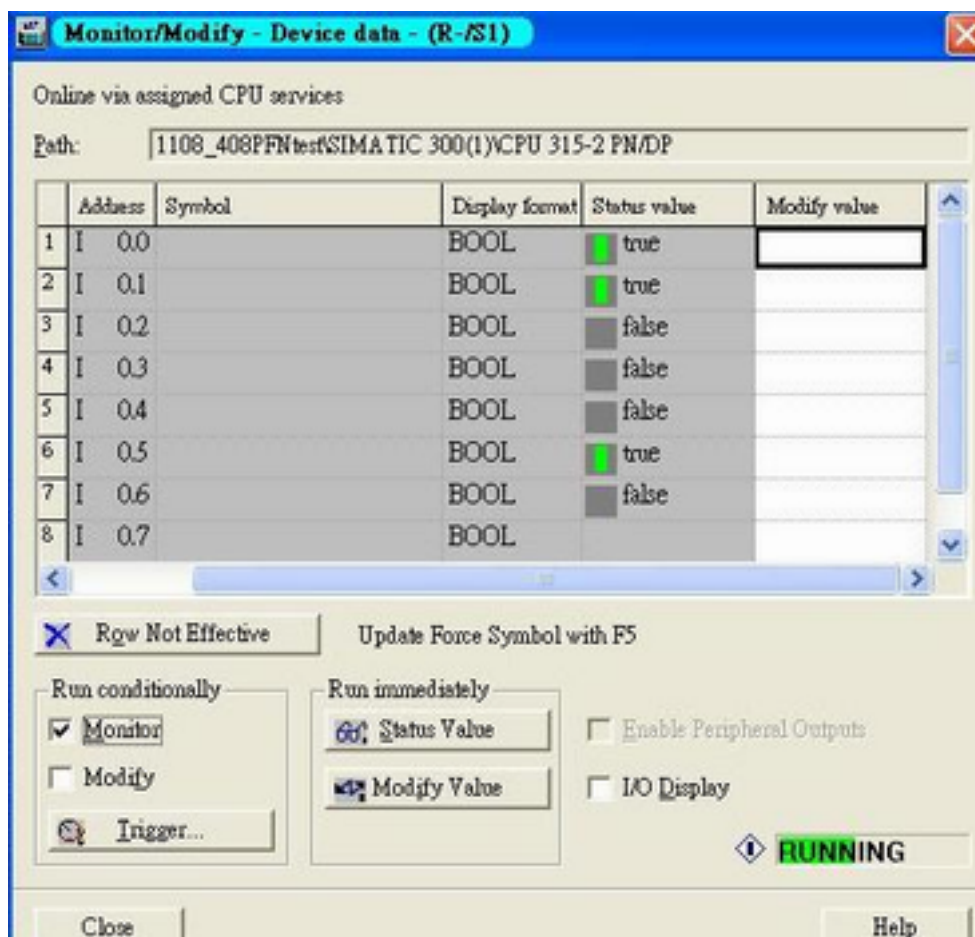
Monitor PROFINET I/O Cyclic Data

VIPA switches provide PROFINET I/O cyclic data for real-time monitoring. In side bar you can see 'Device data' and 'Port data'.

1. ➔ Use Drag & Drop to pull the 'Device data' onto 'slot 1'. Right-click on slot 1, then select 'Monitor/Modify'.



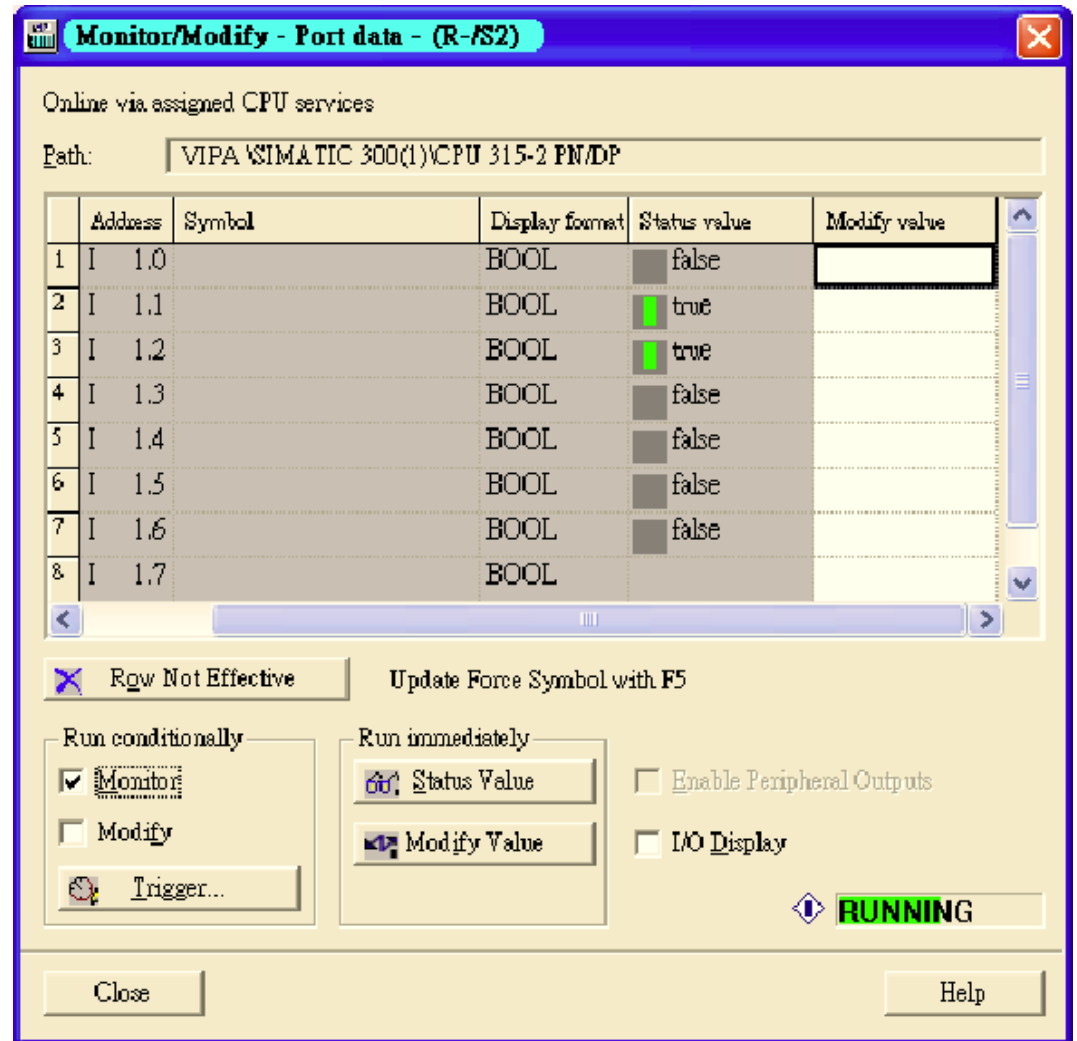
2. Use Monitor to check the input data value. In this dialog, you can see the status value of each address. Please refer to the 'PROFINET Cyclic I/O data table' to see the meaning of each bit. For example, address 0.1 is Bit 1 in the PROFINET Cyclic I/O data table. It represents Power 1 status of the switch. 1 means Power 1 exists and 'Green' will be displayed in the 'Modify/monitor' window



3. To monitor Port data, follow the same steps, drag 'Port data' in the side bar and drop it onto 'slot 2'. VIPA PROFINET I/O cyclic data in the slot 1 and 2

Slot	Module	Order number
0	PN8-RD	
X1	X1	
X1 P1	X1 P1	
X1 P2	X1 P2	
X1 P3	X1 P3	
X1 P4	X1 P4	
X1 P5	X1 P5	
X1 P6	X1 P6	
X1 P7	X1 P7	
X1 P8	X1 P8	
1	Device data	
2	Port data	

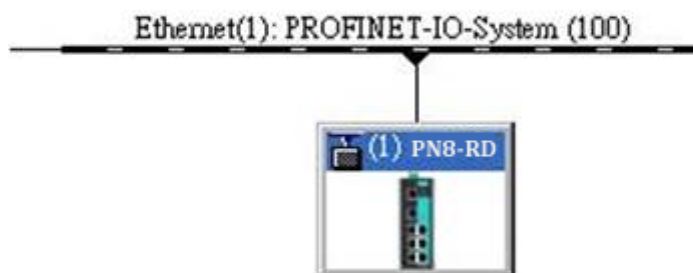
4. Then right click. Select 'Monitor/Modify'. You will see a monitoring window.



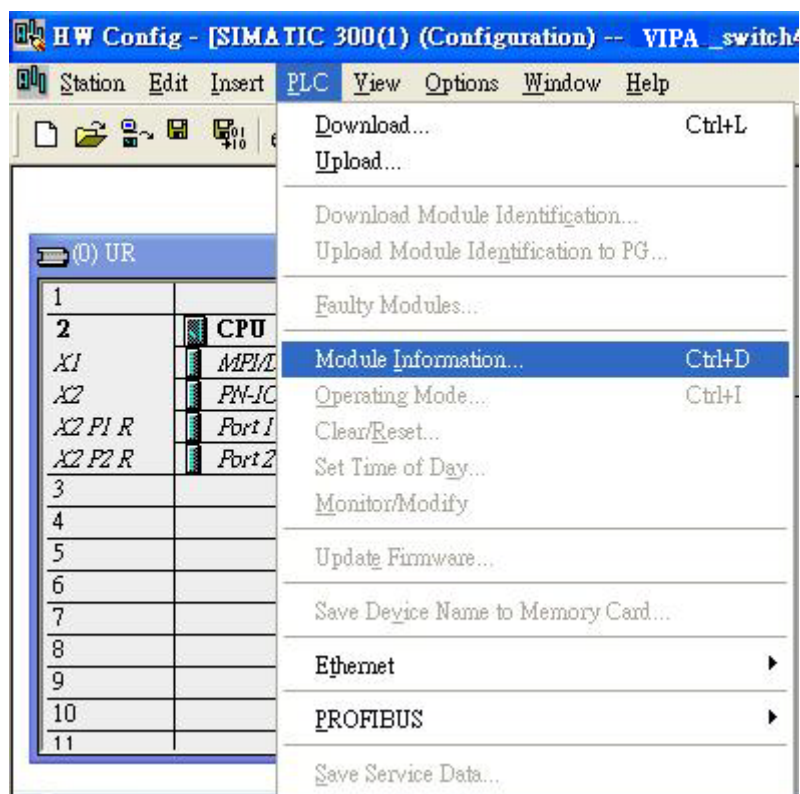
Module Information

VIPA switch supports Siemens SIMATIC STEP®7 Ethernet traffic information monitoring and PROFINET alarms. These attributes can be monitored in module information dialog. Following are the steps of operation.

1. ➤ Select VIPA switch icon on the screen.



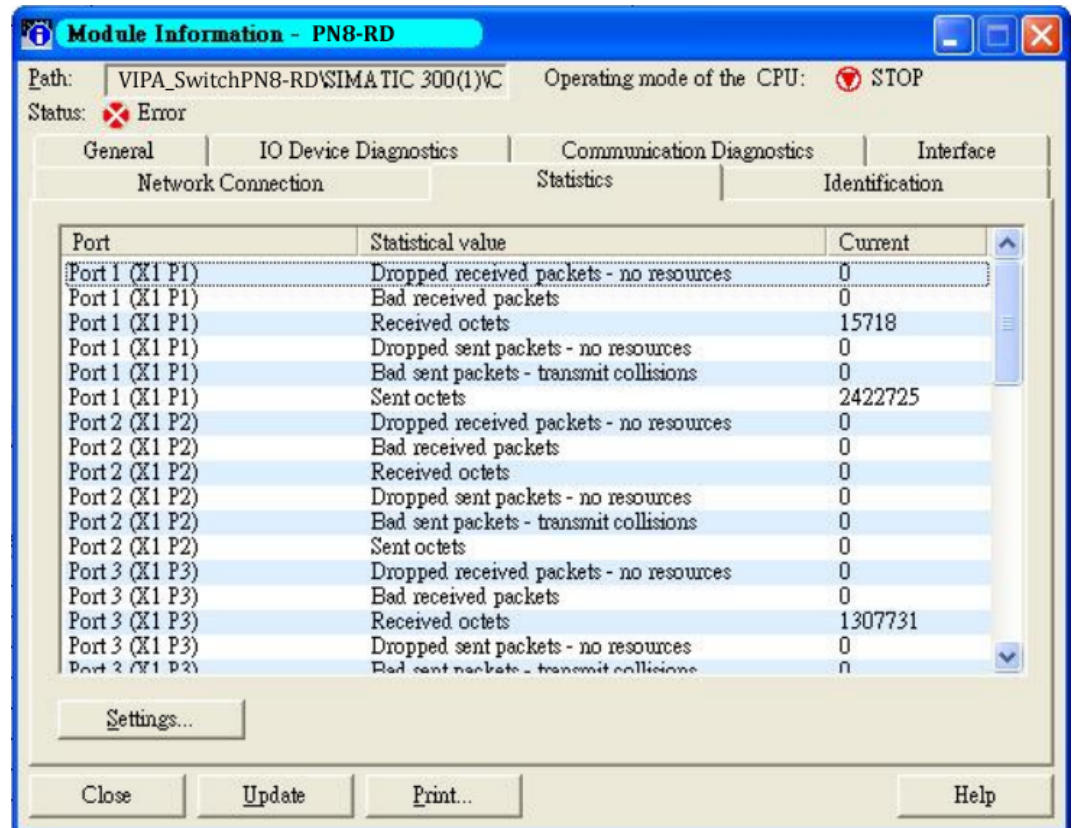
2. ➤ Then, click menu bar 'PLC → Module Information'



- ⇒ The module information dialog will then pop up.

Port Statistics Output

1. ➔ Select 'Statics' tags. Find out each port traffic information list below.



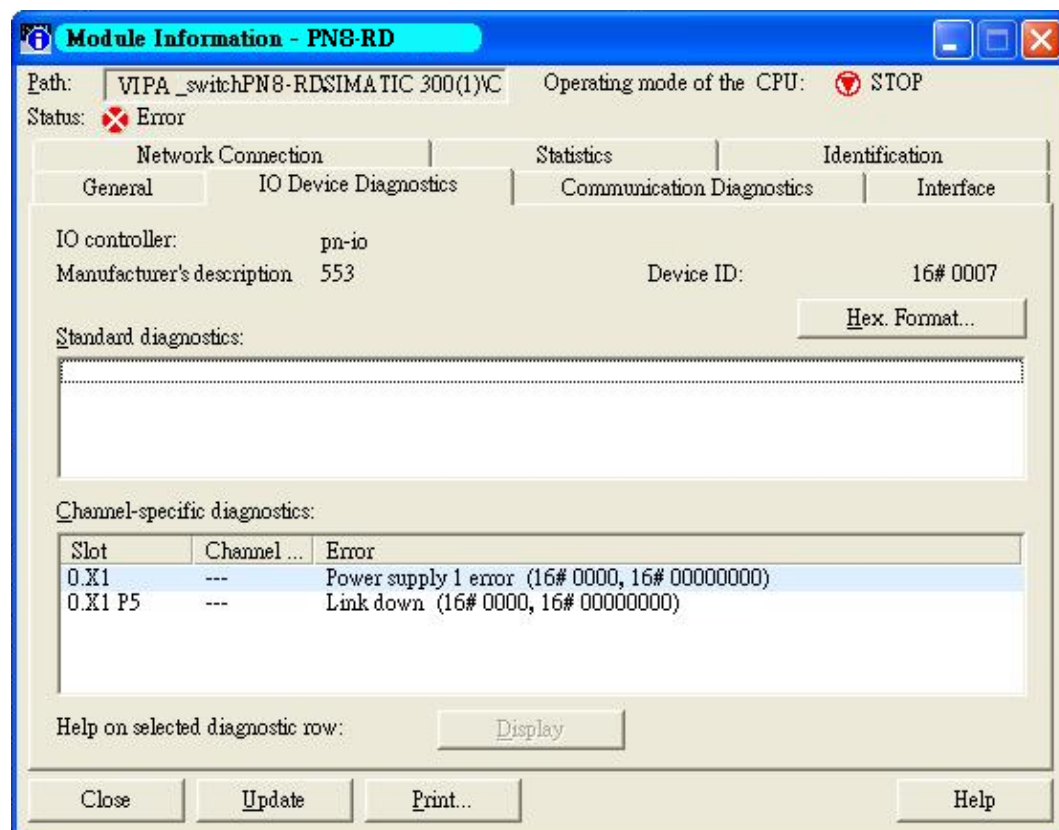
⇒ Statistics tab lists each port traffic status and the number of packets.

2. ➔ Click [Update] to refresh the data.

I/O Device Diagnostics

VIPA PROFINET switches support PROFINET alarms. These alarm messages will be sent by the switch immediately when an event is triggered. These alarms can be enabled/disabled using PROFINET I/O parameters.

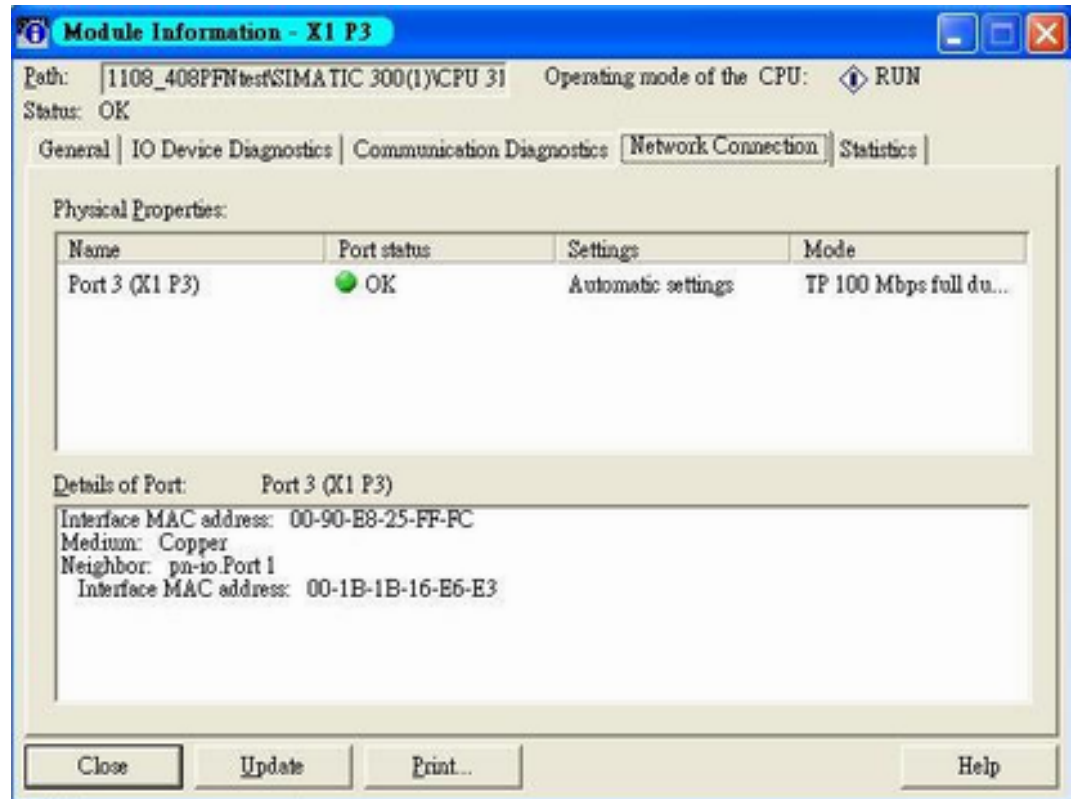
1. ➤ Select 'IO Device Diagnostics' tab to view alarms received by the PLC.



⇒ The 'Channel-specific diagnostics' field is displaying link-down alarm information.

2. ➤ Click [Update] to refresh the data.

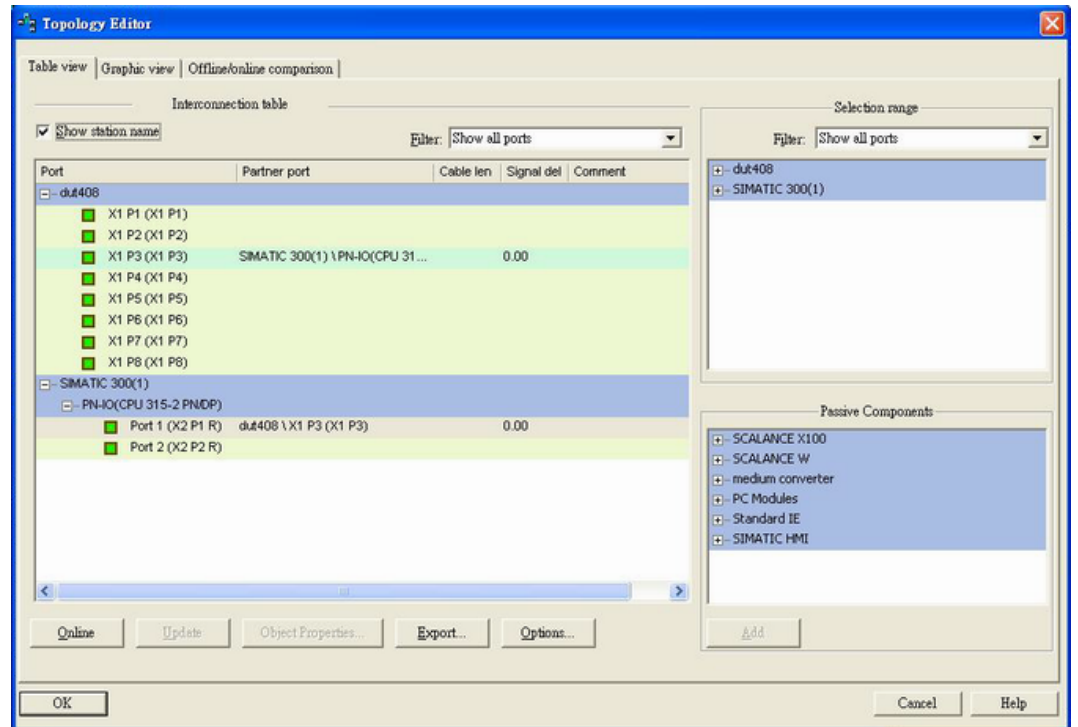
Communication Diagnosis → Select a sub-module and use 'PLC: Module Information' to see the diagnostic data.



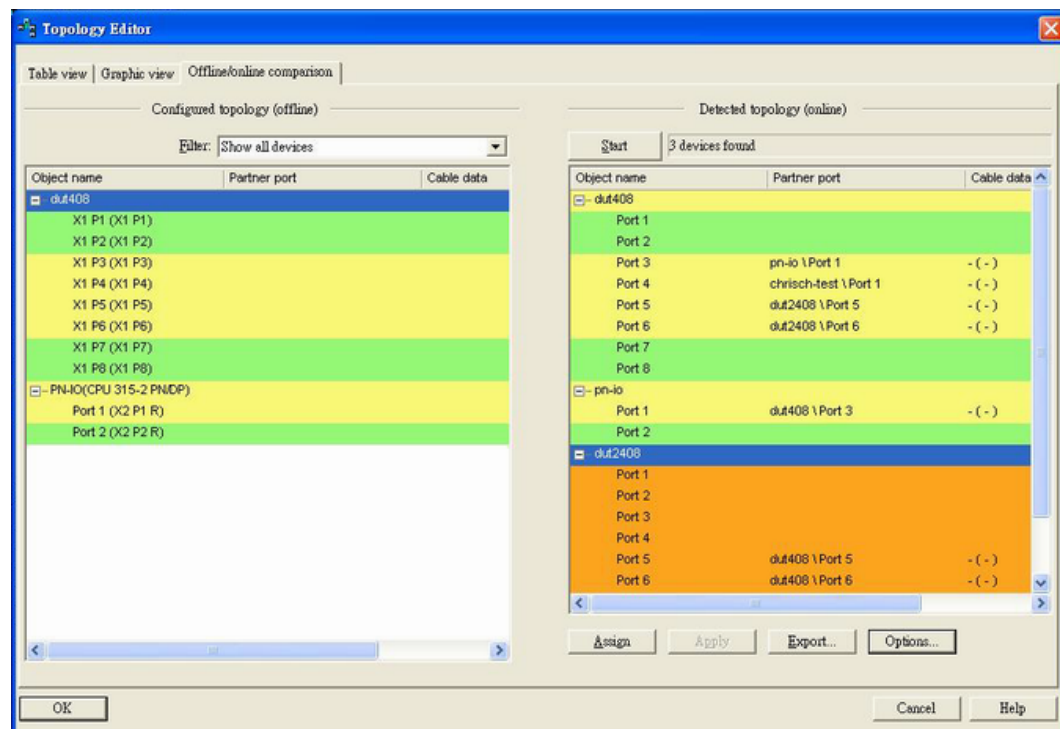
Topology Editor

VIPA devices support Siemens SIMATIC STEP®7 Topology editor.

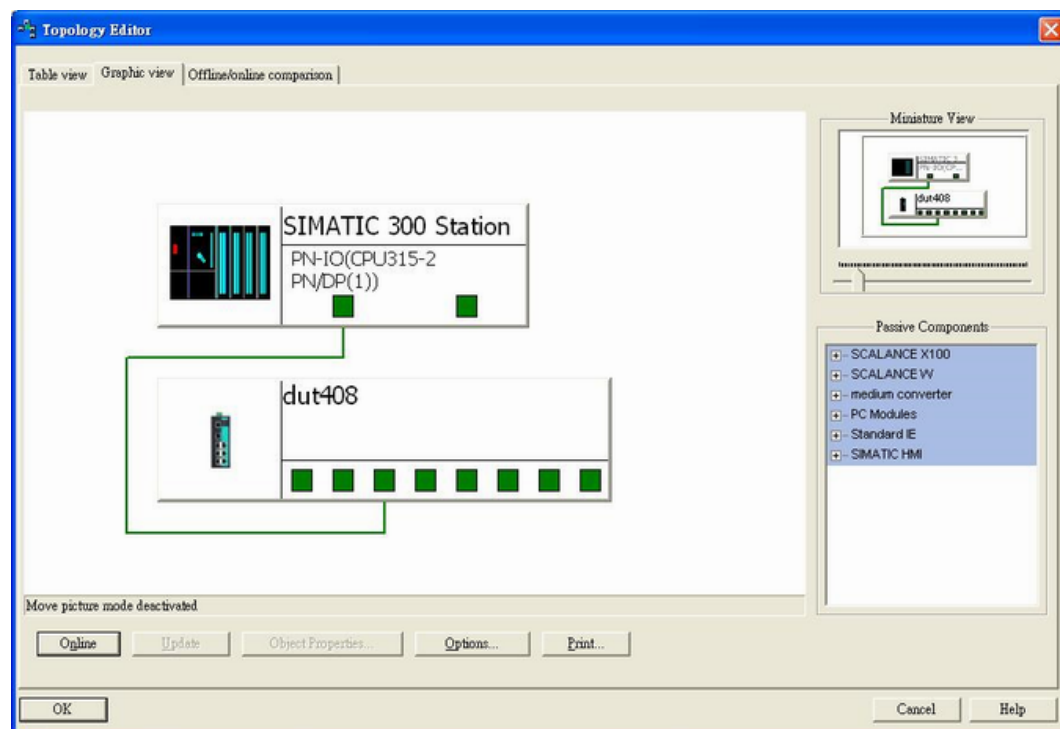
1. → Click Topology Editor. View each port's connection status in table view tag.



2. In the 'Offline/Online Comparison' tab, you can compare device partner ports. Click [Start] to discover connection relationships.



3. You can also draw the connection of each port manually in 'Graphic view' tab.



Appendix

A Command Line Interface

Appendix

A Command Line Interface

Command Modes

CLI (Command Line Interface)

The CLI (command line interface) for VIPA switches can be accessed through either the serial console or Telnet console. For either type of connection, access to the command line interface is generally referred to as an EXEC session.

Configuring a Switch to CLI Mode

The default configuration mode for both the serial console and Telnet console is MENU mode. To change the VIPA switch to CLI configuration mode, **Login Mode** from **Basic Settings** and then press **y** to activate the change. You will then be able to view the CLI display in the console. (Note that the default login user name is **admin**, without a password.)

1. Select **Basic Settings**.

```

1.Basic Settings      - Basic settings for network and system parameter.
2.SNMP Settings      - The settings for SNMP.
3.Comm. Redundancy   - Establish Ethernet communication redundant path.
4.Traffic Prioritization- Prioritize Ethernet traffic to help determinism.
5.Virtual LAN        - Set up a VLAN by IEEE802.1Q VLAN or Port-based VLAN.
6.Multicast Filtering - Enable the multicast filtering capability.
7.Bandwidth Management - Restrict unpredictable network traffic.
8.Auto Warning       - Warning email and/or relay output by events.
9.Line Swap          - Fast recovery after moving devices to different ports.
a.Set Device IP      - Assign IP addresses to connected devices.
b.Diagnosis          - Ping command and the settings for Mirror port, LLDP.
c.Monitor            - Monitor a port and network status.
d.MAC Address Table  - The complete table of Ethernet MAC Address List.
e.System log         - The settings for Syslog and Event log.
f.Exit               - Exit
                    - Use the up/down arrow keys to select a category,
                    and then press Enter to select. -

```

2. Select **Login mode**.

```

Basic Settings
[System] [Password] [Accessible IP] [Port] [Network] [Time] [DIP] [GARP Timer]
[Backup Media] [Restart] [Factory default] [Upgrade] [Login mode] [Activate]
[Main menu]
Toggle login mode
ESC: Previous menu  Enter: Select

Basic Settings

```

3. Press **y** to activate.

```
Basic Settings
[System] [Password] [Accessible IP] [Port] [Network] [Time] [DIP] [GARP Timer]
[Backup Media] [Restart] [Factory default] [Upgrade] [Login mode] [Activate]
[Main menu]
Toggle login mode
ESC: Previous menu   Enter: Select

Current login mode: Menu

Press Y to change to CLI mode? [y/N]
```

4. Now log in to access CLI display mode.

```
login as: █
```

After changing to CLI mode, CLI mode will be the default setting for the next reboot.

Basic Operation

The CLI is organized in different configuration levels. When you first enter CLI mode, type **?** to view a quick help panel that shows the basic commands of the first configuration level. Type any of the commands shown on the screen to access the next configuration level. The quick help panel, accessed from any level by typing **?**, is a useful tool for understanding the commands in any level.

```
quit           - Exit command line interface
exit           - Exit command line interface
reload         - Halt and perform a cold restart
terminal       - Configure terminal page length
login          - Change login mode
copy           - Copy from one file to another
save           - Save running configuration to flash
ping           - Send echo messages
clear          - Clear information
show           - Show running system information
configure      - Enter configuration mode
```

To enter the next level, type the commands shown in the console.

To leave access the next higher level, type **exit**.

To jump directly back to the first level, type **Ctrl + z**.

Useful Interactive “Help” Features

The CLI includes several types of interactive commands. The **Help** commands are listed in the following table:

Command	Purpose
?	Provides a brief description of the Help feature in any command level.
Partial command?	Provides a list of commands that begin with the character string (no space between the command and the question mark).
Partial command<Tab>	Completes a partial command name (no space between the command and <Tab>).
Command ?	Lists the keywords, arguments, or both associated with the command (type a space between the command and the question mark).
Command keyword ?	Lists the arguments that are associated with the keyword (type a space between the keyword and the question mark).

Understanding All Commands

To understand all the details of the commands supported in the CLI of VIPA switches, refer to the following table.

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch and login with user .	Switch>	Enter exit or quit.	Use this mode to display system information.
Privileged EXEC	Begin a session with your switch and login with admin .	Switch#	Enter exit or quit.	Use this mode to verify commands that you have entered.
Global configuration	While in privileged EXEC mode, enter the configure command.	Switch(config)#	To exit to privileged EXEC mode, enter exit or press Ctrl-Z.	Use this mode to configure parameters that apply to the entire switch.
Redundancy configuration	From global configuration mode, enter the redundancy command.	Switch(config-rdnt)#	To exit to privileged EXEC mode, press Ctrl-Z. To exit to global configuration mode, enter the exit command.	Use this mode to configure Turbo Ring V1/V2, Turbo Chain, and Spanning Tree parameters.
Interface configuration	From global configuration mode, specify an interface by entering the interface command followed by an interface identification.	Switch(config-if)#	To exit to privileged EXEC mode, press Ctrl-Z. To exit to global configuration mode, enter the exit command.	
Router configuration	From global configuration mode, specify a protocol by entering the router command.	Switch(config-rip)# Switch(config-ospf)#	To exit to privileged EXEC mode, press Ctrl-Z. To exit to global configuration mode, enter the exit command.	

Commands

access-ip

Use **access-ip** in the VLAN configuration command as to restrict access to the switch to specified IP addresses. Use the **no** form of this command to disable this feature or to remove the IP addresses from access list.

Commands

access-ip [*ip-address netmask*]

no access-ip [*ip-address netmask*]

Syntax	access-ip	Enable the accessible IP list
Description	<i>ip-address</i>	IP address
	<i>netmask</i>	IP netmask
Defaults	The feature is disabled by default.	
Command Modes	VLAN configuration as management VLAN	
Usage Guidelines	This feature will take effect when the access-ip command is executed.	
Examples	<pre>PT-7828(config)# interface mgmt PT-7828(config-vlan)# access-ip 10.10.10.10 255.255.255.0 <IPV4ADDR:ipaddr> - IP address <IPV4ADDR:netmask> - IP netmask PT-7828(config-vlan)# access-ip</pre>	
Error messages	IP or netmask invalid	
	Access IP list full	
Related commands	show interface mgmt access-ip	

acl id

NOTE The command is supported only in Layer 3 switches

Use **acl id** interface configuration commands on the switch to attach ACL to the port. Use the **no** form of this command to return to the default setting.

Commands

acl id { *in* | *out* }

no acl id

Syntax Description	acl	Configure access control list
	<i>id</i>	The access list ID
	in	Inbound traffic
	out	Outbound traffic
Defaults	N/A	
Command Modes	Interface configuration	
Usage Guidelines	N/A	

Examples	PT-7828(config-if)# acl 10 in PT-7828(config-if)# no acl 10
Error messages	Invalid ID!
Related commands	

acl id ip-base

NOTE The command is supported only in Layer 3 switches

Use the **acl id ip-base** global configuration commands on the switch to create an IP-base ACL and add rules. Use the **no** form of this command to remove the rule.

Commands

acl id ip-base { permit | deny } srcip [dstip] [protocol] [port]

acl id ip-base name name_str

no acl id

no acl id rule ruleindex

Syntax Description	acl	Configure access control list
	<i>id</i>	Set ACL ID
	ip-base	IP-base ACL
	permit	Forward packets
	deny	Drop packets
	<i>srcip</i>	Set source IP address and subnet mask. Ex: 192.168.1.1/255.255.255.0 or 192.168.127.1
	<i>dstip</i>	Set destination IP address and subnet mask. Ex: 192.168.1.1/255.255.255.0 or 192.168.127.1
	<i>protocol</i>	Set protocol number, Ex: ICMP, TCP, UDP, etc.
	<i>port</i>	Set TCP/UDP port number
	<i>name_str</i>	ACL name
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	The ACL ID is 1 ~ 16.	
Examples	PT-7828(config)# acl 8 ip-base permit 172.3.1.1/255.255.255.0 201.16.9.7/255.255.0.0 6 23	
Error messages	Invalid ID!	
	This ID is used by MAC-base ACL!	
	Invalid IP address format!	
	Invalid subnet mask format!	
Related commands		

acl id mac-base

NOTE The command is supported only in Layer 3 switches

Use the **acl id mac-base** global configuration commands on the switch to create an MAC-base ACL and add rules. Use the **no** form of this command to remove the rule.

Commands

acl id mac-base { permit | deny } srcmac [dstmac] [ethertype] [vid]

acl id mac-base name name_str

no acl id
no acl id rule ruleindex

Syntax Description	Acl	Configure access control list
	<i>Id</i>	Set ACL ID
	mac-base	MAC-base ACL
	permit	Forward packets
	Deny	Drop packets
	<i>srcmac</i>	Set source MAC address and MAC mask. Ex: 00:90:E8:1D:24:23/FF:FF:FF:FF:00:00 or 00:90:E8:1D:24:23
	<i>dstmac</i>	Set destination IP address and subnet mask. Ex: 192.168.1.1/255.255.255.0 or 192.168.127.1
	<i>ethertype</i>	Set ether type
	<i>Vid</i>	Set VLAN ID
	<i>name_str</i>	ACL name
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	The ACL ID is 1 ~ 100.	
Examples	PT-7828(config)# acl 10 mac-base deny 00:11:22:33:44:55/ff:ff:ff:00:00:00 aa:bb:cc:dd:ee:ff/ff:ff:00:00:00:00 2048 10	
Error messages	Invalid ID!	
	This ID is used by IP-base ACL!	
	Invalid MAC address format!	
	Invalid MAC mask format!	
Related commands		

area

Use the **area** command in Router configuration mode as OSPF to add an OSPF area and configure its type. Use the **no** form of this command to remove the area.

Commands

area area-id [{ stub | nssa } metric value]
no area area-id

Syntax Description	area	Configure OSPF Area
	<i>area-id</i>	OSPF Area id, format is ip address
	stub	Configure OSPF area type to stub
	nssa	Configure OSPF area type to NSSA
	metric	Configure OSPF area metric
	<i>value</i>	Metric value (1 to 65535)
Defaults	N/A	
Command Modes	Router configuration mode as OSPF	
Usage Guidelines	Metric value: 1 to 65535	
Examples	PT-7828(config-ospf)# area 2.2.2.2 PT-7828(config-ospf)# area 2.2.2.2 stub metric 4 PT-7828(config-ospf)# area 2.2.2.2 nssa metric 4	
Error messages	Configuration Error!!	
	Metric value error (1 to 65535)!!	

Related commands	show ip ospf
------------------	--------------

area range

To consolidate and summarize routes at an area boundary, use the **area range** command in router configuration mode. To disable this function, use the **no** form of this command.

Commands

area *area-id* **range** *ip-address netmask*

no area *area-id* **range** *ip-address netmask*

Commands	area	Configure OSPF Area
	<i>area-id</i>	OSPF Area id, format is ip address
	range	Specify an address range for route aggregation
	<i>ip-address</i>	E.g., 11.22.33.44
	<i>netmask</i>	E.g., 255.255.255.0
Defaults	N/A	
Command Modes	Router configuration mode as OSPF	
Usage Guidelines	N/A	
Examples	PT-7828(config-ospf)# area 1.1.1.1 range 192.0.0.0 255.0.0.0	
Error messages	Configuration Error!!	
	IP Prefix format Error!!	
	Netmask format Error!!	
	IP format Error!!	
Related commands	show ip ospf	

area virtual-link

Use the **area virtual-link** command in Router configuration mode as OSPF to add an OSPF virtual link. Use the **no** form of this command to remove the specified OSPF virtual link.

Commands

area *area-id* **virtual-link** *router-id*

no area *area-id* **virtual-link** *router-id*

Syntax Description	area	Configure OSPF Area
	<i>area-id</i>	OSPF Area id
	virtual-link	Establish a virtual link
	<i>router-id</i>	Neighbor Router ID
Defaults	N/A	
Command Modes	Router configuration mode as OSPF	
Usage Guidelines	N/A	
Examples	PT-7828(config-ospf)# area 1.1.1.1 virtual-link 0.0.0.0	
Error messages	Configuration Error!!	
Related commands	show ip ospf	

auth tacacs+

Use the **auth tacacs+** global configuration command on the switch to enable TACACS+ authentication. Use the **no** form of this command to return to the default setting.

Commands

auth tacacs+
no auth tacacs+

Syntax Description	auth	Configure authentication mechanism
	tacacs+	TACACS+ authentication
Defaults	The default setting is disabled.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# auth tacacs+	
Error messages	N/A	
Related commands	show auth tacacs+	

auth tacacs+ auth-type

Use the **auth tacacs+ auth-type** global configuration command on the switch to specify the type of TACACS+ authentication. Use the **no** form of this command to return to the default setting.

Commands

auth tacacs+ auth-type { ascii | pap | chap | arap | mschap }
no auth tacacs+ auth-type

Syntax Description	auth	Configure authentication mechanism
	tacacs+	TACACS+ authentication
	auth-type	Specify the authentication type
	ascii	Normal ASCII code authentication
	pap	Password Authentication Protocol
	chap	Challenge-handshake authentication protocol
	arap	AppleTalk Remote Access Protocol
	mschap	Microsoft Challenge-handshake authentication protocol
Defaults	Default type is ASCII code authentication	
Command Modes	Global configuration	
Usage Guidelines	To enable the TACACS+ authentication, the command “auth tacacs+” must be executed first.	
Examples	<pre>PT-7828(config)# auth tacacs+ auth-type ascii - Normal ASCII code authentication pap - Password Authentication Protocol chap - Challenge-handshake authentication protocol arap - AppleTalk Remote Access Protocol mschap - Microsoft Challenge-handshake authentication protocol</pre>	
Error messages	N/A	

Related commands	auth tacacs+ show auth tacacs+
------------------	-----------------------------------

auth tacacs+ server

Use the **auth tacacs+ server** global configuration command on the switch to set the TACACS+ authentication server address and the shared key information. Use the **no** form of this command to remove the settings.

Commands

auth tacacs+ server server-address **shared-key** key [**timeout** seconds]
no auth tacacs+ server

Syntax Description	auth	Configure authentication mechanism
	tacacs+	TACACS+ authentication
	server	TACACS+ authentication server
	server-address	Authentication server address
	shared-key	Configure the shared key
	key	Key string, max 15 characters
	timeout	Configure server timeout
	seconds	1 to 255 sec.
Defaults	Default timeout is 30 seconds Default tacacs+ server port is 49	
Command Modes	Global configuration	
Usage Guidelines	To enable the TACACS+ authentication, the command “auth tacacs+” must be executed first.	
Examples	<pre>PT-7828(config)# auth tacacs+ server <STRING:auth_server> - Authentication server address PT-7828(config)# auth tacacs+ server tacacs.server.vipa.com shared-key - Configure the shared key PT-7828(config)# auth tacacs+ server tacacs.server. vipa.com shared-key <STRING:key> - Key string, max 15 characters PT-7828(config)# auth tacacs+ server tacacs.server. vipa.com shared-key 1234 <LF> timeout - Configure server timeout PT-7828(config)# auth tacacs+ server tacacs.server.vipa.com shared-key 1234 timeout <UINT:seconds> - 1 to 255 sec. PT-7828(config)# auth tacacs+ server tacacs.server.vipa.com shared-key 1234 timeout 200</pre>	
Error messages	Timeout value must be in the range from 1 to 255 seconds	
	Invalid IP protocol port	
Related commands	auth tacacs+ show auth tacacs+	

auto-backup

Use **auto-backup** to enable Auto load system configurations when the system boots up. To disable it, use the **no** form of this command.

Commands

auto-backup
no auto-backup

Syntax Description	auto-backup	Use auto backup configurator to restore configuration
Defaults	Auto-backup configuration is enabled by default.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# configure terminal PT-7828(config)# auto-backup PT-7828(config)# no au auto-backup - Deactive auto-backup configurator PT-7828(config)# no auto-backup</pre>	
Error messages	N/A	
Related commands	N/A	

bind vlan

Use the **bind vlan** configuration command on the switch to bind the management address with a specified VLAN ID. Use the **no** form of this command to return to the default.

Commands

bind vlan *VLAN-ID*

Syntax Description	bind	Bind VLAN as management VLAN
	vlan	VLAN parameters
	<i>VLAN-ID</i>	1 to 4094
Defaults	Default management VLAN ID is 1	
Command Modes	VLAN configuration mode as management VLAN	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# interface mgmt PT-7828(config-vlan)# bind vlan <UINT:vlanid> - 1 to 4094</pre>	
Error messages	L3 interface cannot be assigned as management interface	
	VLAN id is out of range!	
Related commands	show interfaces mgmt	

clear counters

Use the **clear counters** user EXEC command on the switch to clear the switch's statistics counters.

Commands

clear counters

Syntax Description	clear	Clear information
	counters	Clear statistic counters
Defaults	N/A	
Command Modes	Privileged	

Usage Guidelines	N/A
Examples	PT-7828# clear counters - Clear statistic counters
Error messages	N/A
Related commands	show interfaces counters

clear logging event-log

Use the **clear logging event-log** user EXEC command on the switch to clear the system log of the switch.

Commands

clear logging event-log

Syntax Description	clear	Clear information
	logging	System event logs
	event-log	System event logs
Defaults	N/A	
Command Modes	Privileged	
Usage Guidelines	N/A	
Examples	PT-7828# clear logging - System event logs PT-7828# clear logging event-log - System event logs	
Error messages	N/A	
Related commands	show logging	

clock set

Use the **clock set** global configuration command on the switch to set the current switch time.

Commands

clock set hh:mm:ss month day year

Syntax Description	clock	Configure time-of-day clock
	set	Adjust the clock
	<i>hh:mm:ss</i>	hh:mm:ss
	<i>month</i>	1 to 12
	<i>day</i>	1 to 31
	<i>year</i>	2000 to 2037
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# clock set 11:11:11 1 1 2010	
Error messages	Illegal parameters!	
Related commands	show clock	

clock summer-time

Use the **clock summer-time** global configuration command on the switch to enable the daylight saving time offset and set the apply duration. Use the **no** form of this command to disable it.

Commands

clock summer-time start-date month week day hour

clock summer-time end-date month week day hour

clock summer-time offset offset-hour

Syntax Description	clock	Configure time-of-day clock
	summer-time	Configure Summer time parameter
	start-date	The date when summer time offset start
	end-date	The date when summer time offset end
	<i>month</i>	From 'Jan', 'January' or '1' to 'Dec', 'December', or '12'
	<i>week</i>	From '1st' or '1' to 'Last' or '6'
	<i>day</i>	From 'Sun', 'Sunday' or '1' to 'Sat', 'Saturday' or '7'
	<i>hour</i>	0 to 23
	offset	Summer time offset
	<i>offset-hour</i>	1 to 12
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	When configuring the summer time offset, the start-date and end-date must be configured correctly first.	
Examples	PT-7828(config)# clock timezone gm -4	
Error messages	Invalid parameter	
	Month must be configured as 'Jan', 'January' or a numerical '1'.	
	Week must be configured as '1st', '2nd', '3rd', '4th', '5th' or 'Last'	
	Day must be configured as 'Sun', 'Sunday' or a numerical '1'.	
	Hour must be in the range from 0 to 23.	
	Please input the correct start/end date of the summer time first!	
Related commands	show clock	

clock timezone

Use the **clock timezone** global configuration command on the switch to set the current time zone.

Commands

clock timezone gm offset-hour

Syntax Description	clock	Configure time-of-day clock
	timezone	Time zone hour shifting
	gm	Greenwich Mean Time
	<i>offset-hour</i>	-12 to 12
	<i>Half an hour</i>	Only type 30
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	EDS-G516E(config)# clock timezone gm 5 30	
Error messages	This timezone doesn't support half an hour	

Related commands	show clock
------------------	------------

copy

Use the **copy** privileged command on the switch to copy an image or configuration file from a remote server to the Flash memory or copy the running configuration, startup configuration, or event log to a remote server via TFTP.

Commands

copy tftp device-firmware

copy tftp running-config

copy {running-config|event-log|startup-config} tftp [tftp-address]

Syntax Description	copy	Copy from one file to another
	tftp	Remote server through TFTP
	device-firmware	System firmware
	running-config	Current running configuration of system
	startup-config	System startup configuration
	event-log	Event log file
	<i>tftp-address</i>	TFTP address. E.g., tftp://192.168.127.1/abc.txt
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# copy tftp device-firmware - System firmware running-config - Current running configuration of system PT-7828# copy tftp running-config Address or name of remote host [192.168.127.1]? 192.168.127.95 Source file name ? cli.ini Save import config to flash ? [Y/n] Saving configuration ...Success</pre>	
Error messages	Input error	
	Invalid TFTP Server IP/Name !!!	
	TFTP Configuration File Download Failed	
	Invalid Config Files Path and Name !!!	
	Invalid Firmware Files Path and Name !!!	
	TFTP Firmware Download Failed !!!	
Related commands	N/A	

dot1x auth

Use the **dot1x auth** global configuration command to set dot1x authentication type and relative configurations.

Commands

dot1x auth local

dot1x auth radius server server port port shared-key string

dot1x auth radius-local server server port port shared-key string

Syntax	dot1x	802.1x setting
--------	--------------	----------------

Description	auth	802.1x auth type
	local	802.1x authentication uses local database
	radius	802.1x authentication uses radius server
	radius-local	802.1x authentication uses both local and radius server
	server	802.1x radius server name/ip
	<i>server</i>	802.1x radius server name/ip string
	port	802.1x radius server port
	<i>port</i>	802.1x radius server port (default 1812)
	shared-key	802.1x Shared Key
	<i>string</i>	Shared Key string
Defaults	802.1x local authentication	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# dot1x auth local PT-7828(config)# dot1x auth radius server vipanet port 1812 shared-key vipa PT-7828(config)# dot1x auth radius-local server vipanet port 1812 shared-key vipa</pre>	
Error messages	Local Database is Full !!!	
	Invalid User Name !!!	
	Invalid User Password !!!	
	Invalid User Description !!!	
Related commands	show dot1x	

dot1x auth

Use the **dot1x auth** interface configuration command on the switch to enable port 802.1x authentication. Use the **no** form of this command to return to the default setting.

Commands

dot1x auth
no dot1x auth

Syntax	dot1x	802.1x setting
Description	auth	802.1x port authentication enable/disable
Defaults	802.1x port authentication default disable	
Command Modes	interface configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# interface ethernet 1/1 PT-7828(config-if)# dot1x auth PT-7828(config-if)# no dot1x auth</pre>	
Error messages	N/A	

dot1x local-userdb

To add 802.1x local user database, use the **dot1x local-userdb** global configuration command. To remove the user database, use the **no** form of this command.

Commands

dot1x local-userdb username user password password [desc description]
no dot1x local-userdb username user

Syntax Description	dot1x	802.1x setting
	local-userdb	Local user settings
	username	Local user
	<i>user</i>	Local user name (max. 30 characters)
	password	Local user password
	<i>password</i>	Local user password (max. 16 characters)
	desc	User description
	<i>description</i>	Description string
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# dot1x local-userdb username vipa password vipanet PT-7828(config)# no dot1x local-userdb username vipa	
Error messages	Local Database is Full !!!	
	Invalid User Name !!!	
	Invalid User Password !!!	
	Invalid User Description !!!	
Related commands	show dot1x local-userdb	

dot1x reauth

Use the **dot1x reauth** global configuration command on the switch to globally enable periodic re-authentication of the client. Use the **no** form of this command to return to the default setting.

Commands

dot1x reauth [period period]
no dot1x reauth [period period]

Syntax Description	dot1x	802.1x setting
	reauth	802.1x reauth enable
	period	802.1x reauth period
	<i>period</i>	60 to 65535 seconds
Defaults	802.1x reauth default enable and period 3600 seconds	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# dot1x reauth period 3600 PT-7828(config)# no dot1x reauth	
Error messages	Invalid Re-Auth Period!!! Must not be smaller than 65535 or greater than 60	
Related commands	show dot1x	

dot1x reauth

Use the **dot1x reauth** interface configuration command on the switch to trigger port 802.1x re-authenticate immediately.

Commands

dot1x reauth

Syntax	dot1x	802.1x setting
Description	reauth	802.1x port re-authenticate immediately
Defaults	N/A	
Command Modes	interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# interface ethernet 1/1 PT-7828(config-if)# dot1x reauth	
Error messages	N/A	
Related commands	N/A	

dip-switch

Use the **dip-switch** command to disable/enable HW dip-switch function.

Commands

dip-switch

Syntax Description	disable	Disable HW dip-switch function.
	enable	Enable HW dip-switch function.
	mode turbo-ring-v1	set dip-switch function as turbo-ring-v1.
	mode turbo-ring-v2	set dip-switch function as turbo-ring-v2.
Defaults	1.Enable dip-switch. 2.set to turbo-ring-v2.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# dip-switch disable PT-7828(config-if)# dip-switch mode turbo-ring-v1	
Error messages	N/A	
Related commands	N/A	

eip

Use the **eip** command to disable/enable Ethernet/IP support.

Commands

eip

no eip

Syntax Description	eip	Enable Ethernet/IP
Defaults	Default is disable	
Command Modes	Global configuration	

Usage Guidelines	N/A
Examples	PT-7828 (config)# eip
Error messages	N/A
Related commands	show eip

email-warning account

Use **email-warning account** to configure the account and the password to log in to the remote Mail Server. To clear the setting, use the **no** form of this command.

Commands

email-warning account *name password*

no email-warning account

Syntax	email-warning	Email warning setting
Description	account	Email account on server
	<i>name</i>	User name
	<i>password</i>	User password
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828 (config)# email-warning account test1 1234 PT-7828 (config)# email-warning account test1	
Error messages	Length of SMTP User name is too long !!!	
	Invalid User name	
	Length of password is too long!!!	
Related commands	show email-warning	

email-warning event

Use the **email-warning event** global configuration command to enable the system warning events to send through the email if the event occurs. Use the **no** form of this command to disable the specified warning event notifications.

Commands

email-warning event { **all** | **cold-start** | **warm-start** | **power-trans-off** | **power-trans-on** | **config-change** | **auth-fail** | **topology-change** }

no email-warning event { **cold-start** | **warm-start** | **power-trans-off** | **power-trans-on** | **config-change** | **auth-fail** | **topology-change** }

Syntax	Email-warning	Email warning setting
Description	event	System events
	all	Enable all events
	cold-start	Switch cold start
	warn-start	Switch warm start
	power-trans-off	Power transition (on->off)
	power-trans-on	Power transition (off->on)
	config-change	Configuration changed
	auth-fail	Authentication failed
	topology-change	Topology changed (from redundant protocols)
Defaults	All system events are disabled by default.	

Command Modes	Global configuration
Usage Guidelines	N/A
Examples	<pre> PT-7828(config)# email-warning event all - Enable all events cold-start - Switch cold start warm-start - Switch warm start power-trans-off - Power transition (on->off) power-trans-on - Power transition (off->on) config-change - Configuration changed auth-fail - Authentication failed topology-change - Communication redundancy topology changed PT-7828(config)# email-warning event cold-start PT-7828(config)# email-warning event topology-change PT-7828(config)# email-warning event auth-fail PT-7828(config)# exit PT-7828# show email-warning config Mail Server and Email Setup SMTP Server IP/Name : ms1.hinet.net SMTP Port : 25 Account Name : test1 Account Password : 1234 1st email address: test2@vipa.com 2nd email address : 3rd email address: test3@hinet.net 4th email address : System Events Cold Start : Enable Warm Start : Disable Conf. Changed : Disable Power On->Off : Disable Power Off->On : Disable Auth. Failure : Enable Topology Changed : Enable --More-- </pre>
Error messages	N/A
Related commands	show email-warning

email-warning event

Use the **email-warning event** interface configuration command to allow interface warning events to be sent through the email if the event occurs. Use the **no** form of this command to disable the specified warning event notifications.

Commands

- email-warning event { link-on | link-off }**
- no mail-warning event { link-on | link-off }**
- email-warning event traffic-overload [rxThreshold duration]**
- no email-warning event traffic-overload**

Syntax	email-warning	Configure email warning
Description	event	Port events
	link-on	Link ON

	link-off	Link OFF
	traffic-overload	Traffic overloading
	<i>rxThreshold</i>	0 to 100
	<i>duration</i>	1 to 300
Defaults	All port events are disabled by default.	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# configure terminal PT-7828(config)# interface ethernet 3/1 PT-7828(config-if)# email-warning event - Port events PT-7828(config-if)# email-warning event link-on - Link ON link-off - Link OFF traffic-overload - Traffic overloading PT-7828(config-if)# email-warning event link-on PT-7828(config-if)# email-warning event traffic-overload 80 20 PT-7828(config-if)# PT-7828# show email-warning config Mail Server and Email Setup SMTP Server IP/Name : ms1.hinet.net SMTP Port : 25 Account Name : test1 Account Password : 1234 1st email address: test2@vipa.com 2nd email address : 3rd email address: test3@hinet.net 4th email address : System Events Cold Start : Enable Warm Start : Disable Conf. Changed : Disable Power On->Off : Disable Power Off->On : Disable Auth. Failure : Enable Topology Changed : Enable</pre>	
Error messages	Threshold should be between 0 and 100	
	Duration should be between 1 and 300	
Related commands	show email-warning	

email-warning mail-address

Use **email-warning mail-address** to configure the email address(es) to which warning messages will be sent. To clear the setting, use **no** form of this command.

Commands

email-warning mail-address *mailIndex* *mailAddress*

no email-warning mail-address *mailIndex*

Syntax	email-warning	Email warning setting
Description	mail-address	Target email address
	<i>mailIndex</i>	1 to 4

	<i>mailAddress</i>	Email address
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# email-warning mail-address <UINT:mailIdx> - 1 to 4 PT-7828(config)# email-warning mail-address 1 test2@vipa.com PT-7828(config)# email-warning mail-address 3 test3@hinet.net</pre>	
Error messages	Index should be between 1 and 4	
	Length of email address is too long !!!	
	Invalid Email address format	
Related commands	show email-warning	

email-warning send test email

Use **email-warning send test email** to send a test email.

Commands

switch(config)# email-warning send test email

Syntax Description	email-warning	Email warning setting
	send	Send test email
	test	Test email
	email	Test email address
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	The test email will be sent to the mail address that “ email-warning mail-address ” command configured.	
Examples	<pre>PT-7828(config)# email-warning server 192.168.127.95 <LF> <UINT:smtpPort> - SMTP Port PT-7828(config)# email-warning server 192.168.127.95 25 PT-7828(config)# email-warning account admin 1234 PT-7828(config)# email-warning mail-address 1 <STRING:mailAddress> - Email address PT-7828(config)# email-warning mail-address 1 alanc.wu@vipa.com PT-7828(config)# email-warning send test email Sending test email ... You may check if your dedicated email addresses have received this email! PT-7828(config)#</pre>	
Error messages	Warning !!! You must first do Email Setup before sending the test email.	
	Warning !!! You must first configure DNS Server IP Address before sending the test email.	
	Sending test email failed !!!	

Related commands	email-warning server email-warning account email-warning mail-address
------------------	---

email-warning server

Use **email-warning server** to configure Mail Server IP/Name (IP address or name) for the switch. To clear the setting, use the **no** form of this command.

Commands

email-warning server *smtpServerIp* [*smtpPort*]
no email-warning server

Syntax Description	email-warning	Email warning setting
	server	Email Server
	<i>smtpServerIp</i>	Email Server name/address
	<i>smtpPort</i>	SMTP Port, 1 to 65535
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# email-warning server mail.hinet.net 25 PT-7828(config)# email-warning server msl.hinet.net	
Error messages	Length of server address is too long !!!	
	Invalid SMTP server name/address	
	Invalid Mail Server Port, Range(1 to 65535) !!!	
Related commands	show email-warning	

exit

Use **exit** to exit the current configuration mode.

Commands

exit

Syntax Description	exit	Exit from configure mode
		Exit from port setting mode
		Exit command line interface
		Exit from management interface setting
Defaults	N/A	
Command Modes	N/A	
Usage Guidelines	N/A	
Examples	PT-7828(config)# exit PT-7828 #	
Error messages	N/A	
Related commands	quit	

flowcontrol

To set the method of data flow control between the terminal or other device, use the **flowcontrol** interface configuration command. Use the **no** form of this command to disable flow control

Commands

flowcontrol
no flowcontrol

Syntax Description	flowcontrol	Configure flowcontrol
Defaults	The default is disable	
Command Modes	Interface configuration	
Usage Guidelines		
Examples	<pre>PT-7828(config)# interface ethernet 1/1 PT-7828(config-if)# flowcontrol PT-7828(config-if)# no flowcontrol</pre>	
Error messages	Fiber port can not be set flow control!!	
	Force speed can not be set flow control!!	
	Cannot configure on trunk member port 1/1!	
	This setting cannot be applied on trunk port!	
Related commands	show interfaces ethernet	

gmrp

Use the **gmrp** interface configuration command on the switch to activate the IEEE 802.1D-1998 GMRP (GARP Multicast Registration Protocol). Use the **no** form of this command to stop this function.

Commands

gmrp
no gmrp

Syntax Description	gmrp	Enable GMRP (GARP Multicast Registration Protocol)
Defaults	gmrp is default disable	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# interface ethernet 1/1 PT-7828(config-if)# gmrp PT-7828(config-if)# no gmrp</pre>	
Error messages	GMRP cannot be enabled on static multicast member port!!!	
Related commands		

gvrp

Use the **gvrp** global configuration command on the switch to enable GVRP. Use the **no** form of this command to disable it.

Commands

gvrp
no gvrp

Syntax Description	gvrp	Enable/Disable GVRP
Defaults	The feature is enabled by default.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# gvrp gvrp - Enable GVRP	
Error messages	N/A	
Related commands	show gvrp	

hostname

To specify or modify the host name for the network server, use the **hostname** global configuration command. To return to the default, use the no form of this command.

Commands

hostname *name*

no hostname

Syntax Description	hostname	Set system's network name (maximum 30 characters)
	<i>name</i>	Switch name string
Defaults	Name is the default switch name with the serial number	
Command Modes	Global configuration	
Usage Guidelines	Maximum string tokens are 5. Maximum switch name length is 30 characters.	
Examples	PT-7828(config)# hostname VIPA Ethernet Switch PT 7828 PT-7828(config)# exit PT-7828# show system System Information System Name : VIPA Ethernet Switch PT 7828 System Location : Switch Location System Description : VIPA PT-7828 Maintainer Information : MAC Address : 00:90:E8:1D:24:36 System Uptime : 0d0h36m57s	
Error messages	Length of switch hostname is too long	
Related commands	show system	

interface mgmt

Use the **interface mgmt** global configuration command on the switch to enter the VLAN configuration mode of Mgmt-VLAN.

Commands

interface mgmt

Syntax Description	interface	Select an interface to configure
	mgmt	Configure management VLAN
Defaults	N/A	
Command Modes	Global configuration	

Usage Guidelines	N/A
Examples	PT-7828(config)# interface mgmt - Configure management VLAN PT-7828(config)# interface mgmt PT-7828(config-vlan)#
Error messages	N/A
Related commands	show interfaces mgmt

interface vlan

Use the **interface vlan** global configuration command on the switch to create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode. Use the no form of this command to delete an SVI.

Commands

interface vlan *vlan-id*
no interface vlan *vlan-id*

Syntax Description	interface	Select an interface to configure
	vlan	Configure L3 interface
	<i>vlan-id</i>	Configure L3 interface vlan id
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Management vlan id cannot be same as interface vlan id.	
Examples	PT-7828(config)# interface vlan 2 <UINT:vlanid> - Configure L3 interface vlan id	
Error messages	interface vlan 2 is not exist	
	mgmt vlan id cannot be same as interface vlan id!!	
	vlan interface full	
Related commands	show interfaces vlan	

ip address

Use the **ip address** VLAN configuration command on the switch to configure the address of a Layer 3 interface.

Commands

ip address *ip-address netmask*

Syntax Description	ip	Configure L3 interface ip
	address	Interface ip setting
	<i>ip-address</i>	IP address
	<i>netmask</i>	IP netmask
Defaults	N/A	
Command Modes	VLAN configuration	
Usage Guidelines	N/A	

Examples	PT-7828 (config-vlan)# ip address 10.10.10.10 255.255.255.0 ip - Configure L3 interface ip
Error messages	IP or netmask invalid
	vlan 4097 is invalid!! should be range from 1 to 4094
	vlan interface full Interface VLAN is not allowed to modify!!
Related commands	show interfaces vlan

ip address

Use the **ip address** VLAN configuration command on the switch to configure the IP retrieve mechanism of the switch. Use **no** form of this command to return to the default.

Commands

ip address {static ip-address netmask | dhcp | bootp }
no ip address

Syntax Description	ip	Configure IP paramters
	address	Congiuere IP address
	static	E.g., 11.22.33.44
	<i>ip-address</i>	IP address
	<i>netmask</i>	Subnet mask
	dhcp	Use DHCP to retrieve IP setting automatically
	bootp	Use BOOTP to retrieve IP setting automatically
Defaults	N/A	
Command Modes	VLAN configuration as management VLAN	
Usage Guidelines	N/A	
Examples	PT-7828 (config-vlan)# ip address static - Configure static IP dhcp - Use DHCP to retrieve IP setting automatically bootp - Use BOOTP to retrieve IP setting automatically	
Error messages	N/A	
Related commands	show interfaces mgmt	

ip auto-assign

Use the **ip auto-assign** interface configuration command on the switch to enable and set the auto IP assignment of specified interfaces. Use the **no** form of this command to remove an Ethernet port from a trunk group.

Commands

ip auto-assign ipaddr
no ip auto-assign

Syntax Description	ip	Configure IP paramters
	auto-assign	Automatic port IP assignment through DHCP/BootP/RARP
	<i>ipaddr</i>	E.g., 11.22.33.44
Defaults	N/A	

Command Modes	Interface configuration
Usage Guidelines	This specified IP address must be in the same subnet of the system IP address
Examples (static IP)	PT-7828 (config-if) # ip auto-assign <IPV4ADDR:ipaddr> - E.g., 11.22.33.44
Error messages	Cannot configure on trunk member port This IP address must be in the same subnet of the system IP address
Related commands	show ip auto-assign

ip default-gateway

Use the **ip default-gateway** VLAN configuration command on the switch to configure the IP default gateway address. Use the **no** form of this command to return to the default.

Commands

ip default-gateway *ip-address*
no default-gateway

Syntax Description	ip	Configure IP parameters
	default-gateway	Configure default gateway address
	<i>ip-address</i>	IP address
Defaults	N/A	
Command Modes	VLAN configuration as management VLAN	
Usage Guidelines	N/A	
Examples	PT-7828 (config-vlan) # ip default-gateway 192.168.1.1	
Error messages	Warning! IP and gateway are not in the same subnet	
Related commands	show interfaces mgmt	

ip dhcp retry

Use **ip dhcp retry** to enable the DHCP request retry for a specified period and times. Use the **no** form of this command to return to the default.

Commands

ip dhcp retry *times* **period** *seconds*
no ip dhcp retry

Syntax Description	ip	Global IP configuration subcommands
	dhcp	DHCP related configuration
	retry	Configure DHCP client request retry parameter
	<i>times</i>	0 - 65535 times, 0 means retry forever
	Period	Retry period
	<i>seconds</i>	1 - 30 seconds
Defaults	Default retry times = 0, retry period=1	
Command Modes	VLAN configuration as management VLAN	
Usage Guidelines	N/A	

Examples	<pre>PT-508(config-vlan)# ip dhcp retry 500 period 30 PT-508# show interfaces mgmt IPv4 Management VLAN id : 1 IP configuration : DHCP IP address : 192.168.127.253 Subnet mask : 255.255.255.0 Default gateway : 0.0.0.0 DNS server : Dhcp Retry Periods : 30 seconds Dhcp Retry Times : 500</pre>
Error messages	Illegal parameter!
Related commands	show interface mgmt

ip dhcp-relay server

Use **ip dhcp-relay server** to configure the DHCP server address that the switch will forward DHCP messages to. To remove the DHCP server address, use the **no** form of this command.

Commands

ip dhcp-relay server *serverIndex* *serverAddr*
no ip dhcp-relay server *serverIndex*

Syntax Description	ip	Global IP configuration subcommands
	dhcp-relay	Configure DHCP relay agent parameter
	server	DHCP server IP address
	<i>serverIndex</i>	DHCP server address index, 1 to 4
	<i>serverAddr</i>	DHCP server IP address
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# ip dhcp-relay server 1 192.168.127.100 PT-7828(config)# ip dhcp-relay server 3 192.168.127.200</pre>	
Error messages	Invalid server index	
	Invalid IPv4 address	
Related commands	show ip dhcp-relay	

ip dhcp-relay option82

Use the **ip dhcp-relay option82** global and interface configuration command to enable DHCP Relay with Option 82 messages. To disable it, use the **no** form of this command.

Commands

ip dhcp-relay option82
no ip dhcp-relay option82

Syntax Description	ip	Configure IP parameters
	dhcp-relay	Configure DHCP relay agent parameter
	option82	Option 82
Defaults	Default is disabled.	
Command Modes	Global configuration / Interface configuration	

Usage Guidelines	N/A
Examples	PT-7828(config)# ip dhcp-relay option82 ? <LF> remote-id-type - Remote Id type man-id - Manual remote ID PT-7828(config)# ip dhcp-relay option82
Error messages	N/A
Related commands	N/A

ip dhcp-relay option82 remote-id-type

Use the **ip dhcp-relay option82 remote-id-type** global configuration command to select the remote ID information of DHCP option82 messages. Use **ip dhcp-relay option82 man-id** to manually set the remote id instead of the predefined ones.

Commands

ip dhcp-relay option82 remote-id-type remoteIdType
ip dhcp-relay option82 man-id manualId

Syntax Description	ip	Global IP configuration subcommands
	dhcp-relay	Configure DHCP relay agent parameter
	option82	Option 82
	remote-id-type	Remote Id type
	<i>remoteIdType</i>	ip mac client-id other
	man-id	Manual remote ID
	<i>manualId</i>	Manual remote ID, maximum 15 characters
Defaults	DHCP-relay option82 is disable in factory default. Default remote-id-type is IP.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ip dhcp-relay option82 remote-id-type <STRING:remoteIdType> - ip mac client-id other PT-7828(config)# ip dhcp-relay option82 remote-id-type mac PT-7828(config)# ip dhcp-relay option82 remote-id-type other PT-7828(config)# ip dhcp-relay option82 man-id abcdef	
Error messages	Invalid remote ID type	
	Manual Id is over 15 characters	
Related commands	N/A	

ip http-server

Use **ip http-server** global configuration commands on the switch to enable HTTP/HTTPS service. Use the **no** form of this command to disable HTTP/HTTPS service.

Commands

ip http-server
ip http-server secure
no ip http-sever

Syntax	ip	Global IP configuration subcommands
--------	-----------	-------------------------------------

Description	http-server	Enable HTTP/HTTPS web service
	secure	HTTPS support only
Defaults	HTTP service is enabled.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# ip http-server auto-logout - Web auto-logout timer <LF> secure - HTTPS support only PT-7828(config)# ip http-server secure PT-7828(config)# ip http-server PT-7828(config)# no ip http-server</pre>	
Error messages	N/A	
Related commands	show ip http-server	

ip http-server auto-logout

Use **ip http-server auto-logout** global configuration commands on the switch to enable the auto-logout for the HTTP/HTTPS connections with specified seconds. Use the **no** form of this command to disable it.

Commands

ip http-server auto-logout seconds

Syntax Description	ip	Global IP configuration subcommands
	http-server	Enable HTTP/HTTPS web service
	auto-logout	Web auto-logout timer
	seconds	0 for disable, or 60 to 86400 seconds
Defaults	Auto-logout is disabled by default.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ip http-server auto-logout 120	
Error messages	Switch Web auto-logout interval should be 0(disable) or 60 to 86400s !!!	
Related commands	show ip http-server	

ip igmp static-group

Use the **ip igmp static-group** global configuration command on the switch to add a static multicast MAC address and its member ports. Use the **no** form of this command to remove the static multicast group or just its member ports.

Commands

ip igmp static-group MAC-address interface module/port
no ip igmp static-group [MAC-address] [interface module/port]

Syntax Description	ip	Global IP configuration subcommands
	igmp	IGMP
	static-group	Add New Static Multicast MAC Address
	Mac-address	MAC address XX:XX:XX:XX:XX:XX
	interface	Binding ports
	Module/port	Port(Trunk) ID or list. E.g., 1/1,2,4-5,2/1,Trk1,Trk2-Trk

Defaults	N/A
Command Modes	Global configuration
Usage Guidelines	N/A
Examples	PT-7828(config)# ip igmp static-group 01:00:00:00:00:01 interface 1/2-3 PT-7828(config)# no ip igmp static-group
Error messages	Add new static multicast MAC address Fail !!! Please check the multicast mac address's type !!! Add new static multicast MAC address Fail !!! Not enough space to add a new static multicast MAC address !!! The member port should not be GMRP-enabled port !!!
Related commands	show mac-address-table mcast

ip igmp-snooping

Use the **ip igmp-snooping** global configuration command on the switch to globally enable Internet Group Management Protocol (IGMP) snooping on the switch. Use the command with keywords to enable IGMP snooping. Use the **no** form of this command to disable IGMP snooping.

Commands

ip igmp-snooping
no ip igmp-snooping

Syntax	ip	Global IP configuration subcommands
Description	igmp-snooping	IGMP snooping
Defaults	IGMP snooping is globally disable	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ip igmp-snooping PT-7828(config)# no ip igmp-snooping	
Error messages	IGMP Function is only supported by 802.1Q VLAN mode!	
Related commands	ip igmp-snooping vlan ip igmp-snooping querier ip igmp-snooping query-interval ip igmp-snooping enhanced show ip igmp	

ip igmp-snooping enhanced

Use the **ip igmp-snooping enhanced** global configuration command on the switch to enable the enhanced mode. Use the **no** form of this command to disable the enhanced mode.

Commands

ip igmp-snooping enhanced
no ip igmp-snooping enhanced

Syntax	ip	Global IP configuration subcommands
Description	igmp-snooping	IGMP snooping
	enhanced	IGMP snooping enhanced mode
Defaults	Enhanced mode is globally disabled on the switch	
Command Modes	Global configuration	

Usage Guidelines	The IGMP snooping function must be enabled first.
Examples	PT-7828(config)# ip igmp-snooping enhanced PT-7828(config)# no ip igmp-snooping enhanced
Error messages	IGMP Function is Disabled !!! IGMP Function is only supported by 802.1Q VLAN mode!
Related commands	ip igmp-snooping ip igmp-snooping vlan ip igmp-snooping querier ip igmp-snooping query-interval show ip igmp

ip igmp-snooping querier vlan

Use the **ip igmp-snooping querier** global configuration command to enable and configure the IGMP querier feature on a VLAN interface. Use the **no** form of this command to disable the IGMP querier feature.

Commands

ip igmp-snooping querier vlan *vlan-id*

no ip igmp-snooping querier vlan *vlan-id*

Syntax Description	ip	Global IP configuration subcommands
	igmp-snooping	IGMP snooping
	querier	IGMP snooping query enable
	vlan	VLAN parameters
	<i>vlan-id</i>	1 to 4094
Defaults	The IGMP snooping querier feature is globally disabled on the switch	
Command Modes	Global configuration	
Usage Guidelines	The IGMP snooping function must be enabled first.	
Examples	PT-7828(config)# ip igmp-snooping querier vlan 1 PT-7828(config)# no ip igmp-snooping querier vlan 1	
Error messages	Vlan entry not found!!!	
	Vlan IGMP Function is Disabled !!!	
	IGMP Function is Disabled !!! IGMP Function is only supported by 802.1Q VLAN mode!	
Related commands	ip igmp-snooping ip igmp-snooping vlan ip igmp-snooping query-interval ip igmp-snooping enhanced show ip igmp	

ip igmp-snooping querier vlan vlan-id v3

NOTE The command is supported only in Layer 3 switches

Use the **ip igmp-snooping querier** global configuration command to enable and configure the IGMP querier feature on a VLAN interface. Use **ip igmp-snooping querier vlan** *vlan-id* **v3** can make the switch to send IGMP V3 query, otherwise the default is V2 query.

Syntax	ip	Global IP configuration subcommands
--------	-----------	-------------------------------------

Description	igmp-snooping	IGMP snooping
	querier	IGMP snooping query enable
	vlan	VLAN parameters
	<i>vlan-id</i>	1 ~ 4094
	v3	IGMPv3 mode
Defaults	The IGMP snooping querier feature is globally disabled on the switch	
Command Modes	Global configuration	
Usage Guidelines	The IGMP snooping function must be enabled first.	
Examples	PT-7828(config)# ip igmp-snooping querier vlan 1 v3	
Error messages	Vlan entry not found!!!	
	Vlan IGMP Function is Disabled !!!	
	IGMP Function is Disabled !!!	
	IGMP Function is only supported by 802.1Q VLAN mode!	
Related commands	ip igmp-snooping ip igmp-snooping vlan ip igmp-snooping query-interval	

ip igmp-snooping query-interval

Use the **ip igmp-snooping query-interval** global configuration command on the switch to configure the interval between IGMP queries. Use the **no** form of this command to return to the default.

Commands

ip igmp-snooping query-interval *interval*

Syntax Description	ip	Global IP configuration subcommands
	igmp-snooping	IGMP snooping
	query-interval	IGMP snooping query interval
	<i>interval</i>	20 to 600 seconds
Defaults	Query interval default value is 125 seconds	
Command Modes	Global configuration	
Usage Guidelines	The IGMP snooping function must be enabled first.	
Examples	PT-7828(config)# ip igmp-snooping query-interval 125	
Error messages	The range of Querier interval value should be between 20 and 600 !!!	
	IGMP Function is Disabled !!!	
	IGMP Function is only supported by 802.1Q VLAN mode!	
Related commands	ip igmp-snooping ip igmp-snooping vlan ip igmp-snooping querier ip igmp-snooping enhanced show ip igmp	

ip igmp-snooping vlan

Use the **ip igmp-snooping vlan** global configuration command on the switch to globally enable Internet Group Management Protocol (IGMP) snooping on a VLAN. Use the **no** form of this command to disable IGMP snooping on a vlan.

Commands

ip igmp-snooping vlan *vlan-id* [**mrouter** *module/port*]

no ip igmp-snooping vlan *vlan-id* [**mrouter** *module/port*]

Syntax Description	ip	Global IP configuration subcommands
	igmp-snooping	IGMP snooping

	vlan	VLAN parameters
	<i>vlan-id</i>	1 to 4094
	mrouter	IGMP snooping query port enable
	<i>Module/port</i>	Port(Trunk) ID or list. E.g., 1/1,2,4-5,2/1,Trk1,Trk2-Trk4
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	The IGMP snooping must be enabled first.	
Examples	PT-7828(config)# ip igmp-snooping vlan 1 mrouter 1/1 PT-7828(config)# no ip igmp-snooping vlan 1 mrouter 1/1	
Error messages	Vlan entry not found!!! IGMP Function is Disabled !!! IGMP Function is only supported by 802.1Q VLAN mode!	
Related commands	ip igmp-snooping ip igmp-snooping querier ip igmp-snooping query-interval ip igmp-snooping enhanced show ip igmp	

ip filter-ip

Use the **ip filter-ip** interface configuration command on the switch to add the IP filtering address entries. Use the **no** form of this command to delete the filtering entries.

Commands

ip filter-ip allowed *ip-address*

no ip filter-ip allowed *ip-address*

Syntax	ip	Configure IP paramters
Description	filter-ip	IP filter
	allowed	Configured traffic allowed from specified IP
	<i>ip-address</i>	E.g., 11.22.33.44
Defaults	N/A	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-if)# ip filter-ip allowed 192.168.127.1 <LF>	
Error messages	Not a unicast IP Allowed only 8 filters at most	
Related commands	show interfaces filter-ip	

ip name-server

Use the **ip name-server** VLAN configuration command on the switch to configure the DNS server for the switch. Use the **no** form of this command to return to the default.

Commands

ip name-server *dns-ip-address1* [*dns-ip-address2*]

no name-server

Syntax	ip	Configure IP paramters
Description	name-server	Configure DNS server address
	<i>ip-address</i>	IP address
Defaults	N/A	

Command Modes	VLAN configuration as management VLAN
Usage Guidelines	N/A
Examples	PT-7828 (config-vlan)# ip name-server 192.168.1.1
Error messages	Warning! IP and gateway are not in the same subnet
Related commands	show interfaces mgmt

ip ospf area

Use the **ip ospf area** command in VLAN configuration mode to bind the interfaces with an OSPF area. Use **no ip ospf** to unbind the OSPF area.

Commands

ip ospf area area-id
no ip ospf

Syntax Description	ip	Configure L3 interface ip
	ospf	Configure OSPF
	area	OSPF Area binding
	area-id	OSPF Area id
Defaults	This command is disabled by default.	
Command Modes	VLAN configuration	
Usage Guidelines	Auth Key lengths up to 8 characters MD5 Key ID range 1 to 255	
Examples	PT-7828 (config-vlan)# ip ospf auth md5 5 auth-key abcdabcd	
Error messages	Auth Key lengths up to 8 characters MD5 Key ID range 1 to 255	
Related commands	show ip ospf interface	

ip ospf auth

Use the **ip ospf auth** command in VLAN configuration mode to specify the authentication type for an interface. Use the **no** form of this command to remove the authentication type for an interface.

Commands

ip ospf auth simple auth-key key
ip ospf auth md5 key-id auth-key key
no ip ospf auth

Syntax Description	ip	Configure L3 interface ip
	ospf	Configure OSPF
	auth	Configure OSPF authentication type
	simple	Configure OSPF authentication type to SIMPLE
	md5	Configure OSPF authentication type to MD5
	key-id	MD5 key id
	auth-key	Configure authentication key
	key	Key string
Defaults	This command is disabled by default.	
Command Modes	VLAN configuration	
Usage Guidelines	Auth Key lengths up to 8 characters MD5 Key ID range 1 to 255	

Examples	PT-7828(config-vlan)# ip ospf auth md5 5 auth-key abcdabcd
Error messages	Auth Key lengths up to 8 characters MD5 Key ID range 1 to 255
Related commands	show ip ospf interface

ip ospf cost

Use the **ip ospf cost** command in VLAN configuration mode to explicitly specify the cost of sending a packet on a VLAN interface. Use the **no** form of this command to return to the default.

Commands

ip ospf cost *cost*

no ip ospf cost

Syntax Description	ip	Configure L3 interface ip
	ospf	Configure OSPF
	cost	Configure OSPF Metric
	<i>cost</i>	Metric value (1 to 65535)
Defaults	Default cost is 1	
Command Modes	VLAN configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-vlan)# ip ospf cost 10	
Error messages	Metric Range 1 to 65535	
Related commands	show ip ospf interface	

ip ospf dead-interval

Use the **ip ospf dead-interval** command in interface configuration mode to set the interval at which hello packets must not be seen before neighbors declare the router down. Use the **no** form of this command to return to the default time.

Commands

ip ospf dead-interval *seconds*

no ip ospf dead-interval

Syntax Description	ip	Configure L3 interface ip
	ospf	Configure OSPF
	dead-interval	Configure OSPF dead interval
	<i>seconds</i>	Dead Interval Range 1 to 65535
Defaults	Default dead interval is 40 seconds	
Command Modes	VLAN configuration	
Usage Guidelines	Dead interval Range 1 to 65535	
Examples	PT-7828(config-vlan)# ip ospf dead-interval 100	
Error messages	Dead Interval Range 1 to 65535	
Related commands	show ip ospf interface	

ip ospf hello-interval

Use the **ip ospf hello-interval** command in VLAN configuration mode to specify the interval between hello packets sent on the interface. Use the **no** form of this command to return to the default.

Commands

ip ospf hello-interval *seconds*
no ip ospf hello-interval

Syntax Description	ip	Configure L3 interface ip
	ospf	Configure OSPF
	hello-interval	Configure OSPF hello interval
	<i>seconds</i>	Hello Interval Range 1 to 65535
Defaults	Default interval is 10 seconds	
Command Modes	VLAN configuration	
Usage Guidelines	Hello Interval Range 1 to 65535	
Examples	PT-7828(config-vlan)# ip ospf hello-interval 100	
Error messages	Hello Interval Range 1 to 65535	
Related commands	show ip ospf interface	

ip ospf priority

Use the **ip ospf priority** command in VLAN configuration mode to set the router priority for the determination of the designated router. Use the **no** form of this command to return to the default.

Commands

ip ospf priority *priority*
no ip ospf priority

Syntax Description	ip	Configure L3 interface ip
	ospf	Configure OSPF
	priority	Configure OSPF router priority
	<i>priority</i>	priority range (0 to 255)
Defaults	Default priority is 1	
Command Modes	VLAN configuration	
Usage Guidelines	priority range 0 to 255	
Examples	PT-7828(config-vlan)# ip ospf priority 10	
Error messages	Priority Range 0 to 255	
Related commands	show ip ospf interface	

ip pim-dm

NOTE This command is only supported by Layer 3 switches.

Use the **ip pim-dm** command to enable the PIM-DM function.

Commands

ip pim-dm
no ip pim-dm

Syntax	ip	Configure L3 interface IP
Description	pim-dm	Configure PIM-DM
Defaults	This command is disabled by default	
Command Modes	VLAN interface configuration	
Usage Guidelines	N/A	
Examples	ICS-G7852A-4XG(config-vif)# ip pim-dm ICS-G7852A-4XG(config-vif)# no ip pim-dm	
Error messages	N/A	
Related commands	show ip pim-dm show ip pim-dm neighbor	

ip pim-sm

NOTE This command is only supported by Layer 3 switches.

Use the **ip pim-sm** command to enable the PIM-SM function.

Commands

ip pim-sm
no ip pim-sm

Syntax	ip	Configure L3 interface IP
Description	pim-sm	Configure PIM-SM
Defaults	This command is disabled by default	
Command Modes	VLAN interface configuration	
Usage Guidelines	N/A	
Examples	ICS-G7852A-4XG(config-vif)# ip pim-sm ICS-G7852A-4XG(config-vif)# no ip pim-sm	
Error messages	N/A	
Related commands	show ip pim-sm show ip pim-sm routing show ip pim-sm neighbor show ip pim-sm rp show ip pim-sm bsr	

ip pim-sm dr-priority

NOTE This command is only supported by Layer 3 switches.

Use **ip pim-sm dr-priority** command in VLAN interface configuration mode to setup DR priority.

Commands

ip pim-sm dr-priority *priority*

Syntax	ip	Configure L3 interface IP
Description	pim-sm	Configure PIM-SM
	dr-priority	Configure DR priority
	<i>priority</i>	Priority value
Defaults	Default priority is 0	

Command Modes	VLAN interface configuration
Usage Guidelines	The priority range is 0 to 4294967296
Examples	ICS-G7852A-4XG(config-vif)# ip pim-sm dr-priority 100
Error messages	N/A
Related commands	show ip pim-sm show ip pim-sm routing show ip pim-sm neighbor show ip pim-sm rp show ip pim-sm bsr

ip pim-sm hello-interval

NOTE This command is only supported by Layer 3 switches.

Use **ip pim-sm hello-interval** command in VLAN interface configuration mode to setup PIM-SM hello interval.

Commands

ip pim-sm hello-interval *interval*

Syntax Description	ip	Configure L3 interface IP
	pim-sm	Configure PIM-SM
	hello-interval	Configure hello interval
	<i>interval</i>	Interval value
Defaults	Default hello-interval is 30	
Command Modes	VLAN interface configuration	
Usage Guidelines	The hello interval range is 1 to 65535	
Examples	ICS-G7852A-4XG(config-vif)# ip pim-sm hello-interval 10	
Error messages	N/A	
Related commands	show ip pim-sm show ip pim-sm routing show ip pim-sm neighbor show ip pim-sm rp show ip pim-sm bsr	

ip pim-sm join-prune-interval

NOTE This command is only supported by Layer 3 switches.

Use **ip pim-sm join-prune-interval** command in VLAN interface configuration mode to setup PIM-SM join-prune interval.

Commands

ip pim-sm join-prune-interval *interval*

Syntax Description	ip	Configure L3 interface IP
	pim-sm	Configure PIM-SM
	join-prune-interval	Configure hello interval
	<i>interval</i>	Interval value
Defaults	Default hello-interval is 30	
Command Modes	VLAN interface configuration	
Usage Guidelines	The join-prune interval range is 1 to 65535	
Examples	ICS-G7852A-4XG(config-vif)# ip pim-sm join-prune-interval 10	
Error messages	N/A	
Related commands	show ip pim-sm show ip pim-sm routing show ip pim-sm neighbor show ip pim-sm rp show ip pim-sm bsr	

ip proxy-arp

Use the **ip proxy-arp** VLAN configuration command on the switch to enable Proxy ARP. Use the **no** form of this command to disable Proxy ARP.

Commands

ip proxy-arp
no ip proxy-arp

Syntax	ip	Configure L3 interface ip
Description	proxy-arp	Enable L3 interface proxy arp
Defaults	N/A	
Command Modes	VLAN configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-vlan)# ip proxy-arp proxy-arp - Enable L3 interface proxy arp	
Error messages	vlan 4097 is invalid!! should be range from 1 to 4094	
	Interface not exist! Please create interface and set ip and netmask first	
Related commands	show interfaces vlan	

ip route

Use the **ip route** command in global configuration mode to establish static routes. Use the **no** form of this command to remove the specified static routes.

Commands

ip route prefix mask next-hop [distance]
no ip route prefix mask next-hop

Syntax	ip	Global IP configuration subcommands
Description	route	Static routing entry
	prefix	Address prefix
	mask	Subnet mask
	next-hop	Next hop address
	distance	Distance metric
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ip route 2.2.0.0 255.0.0.0 2.2.3.1 10	
Error messages	Route Entry Full!!!	
Related commands	show ip route show ip route static	

ipv6 address

Use the **ipv6 address** command in VLAN configuration mode as a management VLAN to set the IPv6 address for the device. Use the **no** form of the command to return to the default.

Commands

ipv6 address ipv6_prefix
no ipv6 address

Syntax	ipv6	Configure IPv6
Description	address	IPv6 address setting

	<i>ipv6_prefix</i>	IPv6 address prefix
Command Modes	VLAN configuration as management VLAN	
Usage Guidelines	N/A	
Examples	<pre>PT-510(config-vlan)# ipv6 address 1::1 PT-510# show interfaces mgmt IPv4 Management VLAN id : 1 IP configuration : Static IP address : 192.168.127.253 Subnet mask : 255.255.255.0 Default gateway : 0.0.0.0 DNS server : IPv6 Global Unicast Address Prefix : 1:0:0:1:201:2ff:fe03 Global Unicast Address : 1::1:201:2ff:fe03:405 Link-Local Address : fe80::201:2ff:fe03:405</pre>	
Error messages	Invalid prefix!	
Related commands	show interface mgmt	

line-swap-fast-recovery

Use the **line-swap-fast-recovery** global configuration command on the switch to enable the fast recovery feature of the MAC address table when line swapping. Use the **no** form of this command to disable it.

Commands

line-swap-fast-recovery
no line-swap-fast-recovery

Syntax Description	line-swap-fast-recovery	Enable Line Swap Fast Recovery feature
Defaults	This feature is enabled by default.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# line-swap-fast-recovery <LF></pre>	
Error messages	N/A	
Related commands	show mac-address-table	

Ildp enable

Use the **lldp enable** global configuration command to enable LLDP. To stop LLDP, use the **no** form of this command.

Commands

lldp run
no lldp run

Syntax	lldp	Configure LLDP parameters
--------	-------------	---------------------------

Description	run	Start up
Defaults	LLDP is enable in factory default.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# lldp enable PT-7828(config)# no lldp enable	
Error messages	N/A	
Related commands	show lldp	

lldp timer

Use the **lldp timer** global configuration command to configure the transmission frequency of LLDP messages. To reset the timer to default, use the **no** form of this command.

Commands

lldp timer *transFreq*
no lldp timer

Syntax	lldp	Configure LLDP parameters
Description	timer	Transmission frequency of LLDP updates
	<i>transFreq</i>	5 to 32768 seconds
Defaults	Transmission frequency of LLDP updates is 30 seconds.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# lldp timer <UINT:transFreq> - 5 to 32768 seconds PT-7828(config)# lldp timer 4 % LLDP transmit frequency should be between 5 to 32768 PT-7828(config)# lldp timer 50	
Error messages	LLDP transmit frequency should be between 5 to 32768	
Related commands	show lldp	

logging

Use the **logging** global configuration command on the switch to configure the remote SYSLOG server. Use the **no** form of this command to remove the server.

Commands

logging *ip-address*
no logging *ip-address*

Syntax	logging	Syslog server setting
Description	<i>ip-address</i>	IP or DNS name w/wo. port, Ex:1.2.3.4 or 1.2.3.4:5678
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	

Examples	PT-7828 (config) # logging 192.168.1.1 <LF>
Error messages	Logging server configurations are full!
Related commands	show logging

login mode

Use the **login mode** global configuration command to change the login UI mode from the console or telnet connection of the switch.

Commands

login mode { cli | menu }

Syntax Description	login	Change login mode
	mode	Login mode
	cli	Command line interface
	menu	Legacy Menu Mode
Defaults	Default UI mode is MENU mode	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828 (config) # login mode menu - Legacy Menu Mode cli - Command line interface PT-7828 (config) # login mode cli PT-7828 (config) # login mode menu	
Error messages	N/A	
Related commands	N/A	

mac-address-table aging-time

Use the **mac-address-table aging-time** global configuration command on the switch to configure the aging time of the MAC address. Use the **no** form of this command to return to the default.

Commands

mac-address-table aging-time seconds

no mac-address-table aging-time

Syntax Description	mac-address-table	Configure MAC address table
	aging-time	Aging time
	<i>seconds</i>	15 to 3825 seconds
Defaults	Default aging time is 300 sec	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828 (config) # mac-address-table aging-time <UINT:seconds> - 15 to 3825 seconds	
Error messages	N/A	
Related commands	show mac-address-table aging-time	

mcast-filter

Use the **mcast-filter** interface configuration command on the switch to activate the multicast filter. Use the **no** form of this command to stop this function.

Commands

mcast-filter [forward-all | forward-unknown | filter-unknown]
no mcast-filter

Syntax Description	mcast-filter	Multicast filter
	forward-all	Forward all
	forward-unknown	Forward unknown
	filter-unknown	Filter unknown
Defaults	Default forward unknown	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# interface ethernet 1/1 PT-7828(config-if)# mcast-filter forward-all PT-7828(config-if)# mcast-filter forward-unknown PT-7828(config-if)# mcast-filter filter-unknown PT-7828(config-if)# no mcast-filter</pre>	
Error messages	N/A	
Related commands	show mcast-filter	

media cable-mode

Use the **media cable-mode** interface configuration command on the switch to enable the medium-dependent interface crossover feature on the interface. Use the **no** form of this command to disable Auto-MDIX.

Commands

media cable-mode [mdi | mdix | auto]
no media cable-mode

Syntax Description	media	Select a media
	cable-mode	Select cable mode
	mdi	MDI
	mdix	MDIX
	auto	Auto select MDI/MDIX
Defaults	The default is auto	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# interface ethernet 1/1 PT-7828(config-if)# media cable-mode auto PT-7828(config-if)# no media cable-mode</pre>	
Error messages	Fiber port can not be set MDI/MDIX!!	
	This setting cannot be applied on trunk port!	
	Cannot configure on trunk member port 1/1!	
Related commands	show interface ethernet	

modbus

Use the **modbus** global configuration command on the switch to enable Modbus/TCP industrial Ethernet protocol supported. Use the **no** form of this command to disable Modbus support.

Commands

modbus
no modbus

Syntax Description	modbus	Enable Modbus
Defaults	Default is enable	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828 (config) # modbus	
Error messages	N/A	
Related commands	show modbus	

monitor

Use **monitor** global configuration commands to enable the monitoring of data transmitted/received by a specific port. Use the **no** form of this command to disable the monitoring.

Commands

monitor source interface *mod_port* [*direction*]
no monitor source interface
monitor destination interface *mod_port*
no monitor destination interface

Syntax Description	monitor	Configure Port mirror
	source	Monitored port
	interface	Port
	destination	Mirror port
	<i>modPort</i>	Port ID. E.g., 1/3, Trk2,...
	<i>direction</i>	tx rx both
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Traffic send/receive by a source port (Monitored port) will be mirrored to the destination port (Mirror port).	
Examples	<pre>PT-7828(config)# monitor source interface 3/1 both Warning !!! Mirror Port don't set ! PT-7828(config)# monitor destination interface <STRING:mirrorPort> - Port ID. E.g., 1/3, 2/1,... PT-7828(config)# monitor destination interface 3/1,2 % Invalid format PT-7828(config)# monitor destination interface 3/1 % Monitored Port is the same with Mirror Port !!! PT-7828(config)# monitor destination interface 3/2 PT-7828(config)# monitor source interface 1/1-2</pre>	
Error messages	Monitored Port is the same with Mirror Port !!!	
	Invalid parameter	
	Warning !!! Mirror Port don't set !	
	Warning !!! Monitored Port don't set !	

Related commands	show port monitor
------------------	-------------------

Management-Interface

Use the **ip** global configuration command on the switch to set management interface

Commands

ip { **http-server** [**secure**] | **telnet** | **ssh** } [**port** *port-number*]
no ip { **http-server** [**secure**] | **telnet** | **ssh** }

Syntax Description	http-server	Enable Http-server service
	secure	Enable SSL service
	telnet	Enable Telnet service
	ssh	Enable SSH service
	Port	Port
	<i>Port-number</i>	Listening port number
Defaults	The feature is enabled by default.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	EDS-G516E(config)# ip http-server port 80 EDS-G516E(config)# ip http-server secure port 443 EDS-G516E(config)# ip telnet 23 EDS-G516E(config)# ip ssh port 22 EDS-G516E(config)# no ip http-server secure	
Error messages	Assigning duplicate port numbers is not allowed	
	HTTP/SSH/Telnet/SSL port number is invalid, the interval is from 1 to 65535.	
Related commands		

name

Use the **name** interface configuration command to configure the interface name. To remove the configuration, use the **no** form of this command.

Commands

name
no name

Syntax Description	name	Port name
Defaults	None	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# interface ethernet 1/1 PT-7828(config-if)# name interfacel_port1 PT-7828(config-if)# no name	
Error messages	The length of port name must between 1 and 63!	
	Cannot configure on trunk member port 1/1	

Related commands	show interfaces ethernet show interfaces trunk
------------------	---

network

Use the **network** command in router configuration mode to enable the routing process on the specified interface. Use the **no** form of this command to disable it.

Commands

network *if-name*

no network *if-name*

Syntax	network	Enable dynamic routing on an IP network
Description	<i>if-name</i>	Interface name
Defaults	N/A	
Command Modes	Router configuration of RIP, OSPF, and Static routes	
Usage Guidelines	N/A	
Examples (for RIP settings)	<pre>PT-7828(config)# vlan create 2 % create vlan id:2 PT-7828(config)# interface vlan 2 PT-7828(config-vlan)# ip address 192.168.102.1 255.255.255.0 PT-7828(config-vlan)# name vlan2if PT-7828(config-vlan)# exit PT-7828(config)# router rip PT-7828(config-rip)# network <STRING:ifname> - Interface name PT-7828(config-rip)# network vlan2if PT-7828(config-rip)# PT-7828# show ip rip RIP Protocol : Enable RIP version : V1 Distribution Connected : Enable Static : Disable OSPF : Disable RIP Enable Table Interface Name IP VID Enable ----- --- vlan2if 192.168.102.1 2 Enable PT-7828#</pre>	
Error messages	No such interface existed	
Related commands	show ip rip	

ntp refresh-time

Use the **ntp refresh-time** global configuration command on the switch to configure the interval of each NTP query. Use the **no** form of this command to return to the default.

Commands

ntp refresh-time *seconds*

no ntp refresh-time

Syntax	ntp	Configure Network Time Protocol
Description	refresh-time	Configure NTP query intervals
	<i>seconds</i>	1-9999 seconds
Defaults	Default query interval is 600 sec	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ntp refresh-time 600 <LF>	
Error messages	Time is out of range	
Related commands	show clock	

ntp remote-server

Use the **ntp remote-server** global configuration command on the switch to configure the remote NTP server. Use the **no** form of this command to return to the default.

Commands

ntp remote-server *server-addr-1* [*server-addr-2*]
no ntp remote-server

Syntax	ntp	Configure Network Time Protocol
Description	remote-server	Configure NTP server for time query
	Simple	Configure Simple Network Time Protocol instead of Network Time Protocol
	<i>server-addr-1</i>	IP address or DNS name
	<i>server-addr-2</i>	IP address or DNS name
Defaults	The default configuration contains one time server "time.nist.gov".	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828 (config)# ntp remote-server 192.168.127.1 time.stdtime.gov.tw	
Error messages	N/A	
Related commands	show clock	

ntp server

Use the **ntp server** global configuration command on the switch to enable the switch as an NTP server. Use the **no** form of this command to return to disable it.

Commands

ntp server
no ntp server

Syntax	ntp	Configure Network Time Protocol
Description	server	Enable NTP server
Defaults	Default is disabled	
Command Modes	Global configuration	
Usage Guidelines	N/A	

Examples	PT-7828 (config) # ntp server
Error messages	N/A
Related commands	show clock

permit

Use the **permit** ACL configuration command on the switch to add a permit rule in the current ACL for traffic with specified IPs. Use the **no** form of this command to delete the rule.

Commands

permit ip-address

no permit ip-address

Syntax	permit	Configure PERMIT filter
Description	ip-address	E.g., 11.22.33.44
Defaults	N/A	
Command Modes	ACL configuration	
Usage Guidelines	N/A	
Examples	PT-7828 (config-acl) # permit <IPV4ADDR:ipaddr> - E.g., 11.22.33.44	
Error messages	Invalid IPv4 address	
Related commands	Show ip access-list ip access-list	

ping

Use the **ping** user EXEC command on the switch to diagnose the remote host if it is alive.

Commands

ping ip-address

Syntax	ping	Send echo messages
Description	ip-address	E.g., 11.22.33.44
Defaults	N/A	
Command Modes	Privileged	
Usage Guidelines	N/A	
Examples	PT-7828# ping 192.168.127.1 PING 192.168.127.1, Send/Recv/Lost = 4/4/0	
Error messages	N/A	
Related commands	N/A	

port-security

Use the **port-security** interface configuration command on the switch to add a static unicast MAC-address on a specified port. Use the **no** form of this command to remove the specified MAC address.

Commands

port-security MAC-address

no port-security MAC-address

Syntax	port-security	Set port security
Description	<i>MAC-address</i>	MAC address XX:XX:XX:XX:XX:XX
Defaults	N/A	
Command Modes	interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-if)# port-security 00:00:00:00:00:01 PT-7828(config-if)# no port-security 00:00:00:00:00:01	
Error messages	Add new static unicast MAC address Fail !!!	
Related commands	N/A	

profinetio

Use the **profinetio** command to disable/enable PROFINET support (EDS-400A-PN series support only).

Commands

profinetio

no profinetio

Syntax	profinetio	Enable PROFINET IO
Description		
Defaults	Default is disabled	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	EDS-G516E(config)# profinetio EDS-G516E(config)# no profinetio	
Error messages	N/A	
Related commands	Show profinetio	

ptp announce-receipt-timeout

Use the **ptp announce-receipt-timeout** configuration command on the switch to set the announce-receipt-timeout parameter.

Commands

ptp announce-receipt-timeout *interval*

Syntax	ptp	Configure PTP
Description	announce-receipt-timeout	Set the integral multiple of announceInterval
	<i>interval</i>	2 to 10
Defaults	default is 3	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp announce-receipt-timeout	

Error messages	announceReceiptTimeout must be in the range from 2 to 10
Related commands	Show ptp settings Show ptp status Show ptp port

ptp arb-time

Use the **ptp arb-time** configuration command on the switch to set the arb-time parameter of the local clock.

Commands

ptp arb-time *time*

Syntax	ptp	Configure PTP
Description	arb-time	Set the ARB time parameter of the local clock
	<i>time</i>	0 to 2147483646
Defaults	default is 0	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp arb-time 0	
Error messages	Arb time must be in the range from 0 to 2147483646	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp clockclass

Use the **ptp clockclass** configuration command on the switch to set the clockclass parameter of the local clock.

Commands

ptp clockclass *class*

Syntax	ptp	Configure PTP
Description	clockclass	Set the clock class parameter of the local clock
	<i>class</i>	0 to 255
Defaults	default is 248	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp clockclass 248	
Error messages	clockclass must be in the range from 0 to 255	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp domain-number

Use the **ptp domain-number** configuration command on the switch to set the domain number of the local clock.

Commands

ptp domain-number *interval*

Syntax	ptp	Configure PTP
Description	domain-number	Set the domain number of the local clock
	<i>interval</i>	0 to 3
Defaults	default is 0	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp domain-number	
Error messages	domainNum must be in the range from 0 to 3	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp enable

Use the **ptp enable** command on the switch to enable the PTP operation. Use the **no** form of this command to disable the PTP operation on the switch.

Commands

ptp enable

no ptp

Syntax	ptp	Configure PTP
Description	enable	Enable the ptp operation
Defaults	ptp is default disable	
Command Modes	Configuration Interface configuration mode	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp enable PT-7828(config)# no ptp PT-7828(config-if)# ptp enable PT-7828(config-if)# no ptp	
Error messages	N/A	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp leap59

Use the **ptp leap59** global configuration command on the switch to enable the PTP leap59. Use the **no** form of this command to disable the PTP leap59 on the switch.

Commands

ptp leap59

no ptp leap59

Syntax Description	ptp leap59	Configure PTP enable the last minute of the current UTC day contains 59 seconds
Defaults	default disable	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp leap59 PT-7828(config)# no ptp leap59	
Error messages	N/A	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp leap61

Use the **ptp leap61** global configuration command on the switch to enable the PTP leap61. Use the **no** form of this command to disable the PTP leap61 on the switch.

Commands

ptp leap61
no ptp leap61

Syntax Description	ptp leap61	Configure PTP enable the last minute of the current UTC day contains 61 seconds
Defaults	default disable	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp leap61 PT-7828(config)# no ptp leap61	
Error messages	N/A	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp log-sync-interval

Use the **ptp log-sync-interval** global configuration command on the switch to set the *log-sync-interval* parameter.

Commands

ptp log-sync-interval *interval*

Syntax Description	ptp	Configure PTP
	log-sync-interval	Set the logarithm to the base 2 of the mean SyncInterval
	<i>interval</i>	-3 to 1
Defaults	default is 0	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp log-sync-interval	
Error messages	logSyncInterval must be in the range from -3 to 1	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp log-announce-interval

Use the **ptp log-announce-interval** global configuration command on the switch to set the *log-announce-interval* parameter.

Commands

ptp log-announce-interval *interval*

Syntax Description	ptp	Configure PTP
	log-announce-interval	Set the logarithm to the base 2 of the mean AnnounceInterval
	<i>interval</i>	0 to 4
Defaults	default is 1	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp log-announce-interval	
Error messages	logAnnounceInterval must be in the range from 0 to 4	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp log-min-delay-req-interval

Use the **ptp log-min-delay-req-interval** global configuration command on the switch to set the *log-min-delay-req-interval* parameter.

Commands

ptp log-min-delay-req-interval *interval*

Syntax	ptp	Configure PTP
Description	log-min-delay-req-interval	Set the logarithm to the base 2 of the mean minDelayReqInterval
	<i>interval</i>	0 to 5
Defaults	default is 0	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp log-min-delay-req-interval	
Error messages	logMinDelayReqInterval must be in the range from 0 to 5	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp log-min-pdelay-req-interval

Use the **ptp log-min-pdelay-req-interval** global configuration command on the switch to set the *log-min-pdelay-req-interval* parameter.

Commands

ptp log-min-pdelay-req-interval *interval*

Syntax	ptp	Configure PTP
Description	log-min-pdelay-req-interval	Set the logarithm to the base 2 of the mean minPDelayReqInterval
	<i>interval</i>	-1 to 5
Defaults	default is 0	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp log-min-pdelay-req-interval	
Error messages	logMinPDelayReqInterval must be in the range from -1 to 5	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp mode

Use the **ptp mode** global configuration command on the switch to set the PTP operation mode.

Commands

ptp mode v1-bc
ptp mode v2-e2e-bc
ptp mode v2-p2p-bc
ptp mode v2-e2e-1step-tc
ptp mode v2-e2e-2step-tc
ptp mode v2-p2p-2step-tc

Syntax Description	ptp	Configure PTP
	mode	Set the ptp operation mode
	v1-bc	ptp v1 boundary clock mode
	v2-e2e-bc	ptp v2 end-to-end boundary clock mode
	v2-p2p-bc	ptp v2 peer-to-peer boundary clock mode
	v2-e2e-1step-tc	ptp v2 end-to-end 1-step transparent clock mode
	v2-e2e-2step-tc	ptp v2 end-to-end 2-step transparent clock mode
Defaults	Default setting of ptp is v1-bc mode	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp mode v1-bc	
Error messages	N/A	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp preferred-master

Use the **ptp enable** configuration command on the switch to enable PTP operation. Use the **no** form of this command to disable PTP operation on the switch.

Commands

ptp enable
no ptp

Syntax Description	ptp	Configure PTP
	preferred-master	Set the local clock as the master clock(only valid in v1-bc mode)
Defaults	default disable	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples (set switch as local master clock)	PT-7828(config)# ptp preferred-master	
Error messages	N/A	

Related commands	Show ptp settings Show ptp status Show ptp port
------------------	---

ptp priority1

Use the **ptp priority1** configuration command on the switch to set the *priority1* parameter of the local clock.

Commands

ptp priority1 *priority*

Syntax	ptp	Configure PTP
Description	priority1	Set the priority1 parameter of the local clock
	<i>priority</i>	0 to 255
Defaults	default is 128	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp priority1 128	
Error messages	priority1 must be in the range from 0 to 255	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp priority2

Use the **ptp priority2** configuration command on the switch to set the *priority2* parameter of the local clock.

Commands

ptp priority2 *priority*

Syntax	ptp	Configure PTP
Description	Priority2	Set the priority2 parameter of the local clock
	<i>priority</i>	0 to 255
Defaults	default is 128	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp priority2 128	
Error messages	priority2 must be in the range from 0 to 255	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp timescale

Use the **ptp timescale** configuration command on the switch to set the transport type of the ptp domain.

Commands**ptp timescale [arb|ptp]**

Syntax Description	ptp	Configure PTP
	timescale	Set the timescale parameter of the local clock
	arb	Set the timescale parameter of the local clock to ARB
	ptp	Set the timescale parameter of the local clock to PTP
Defaults	default is ptp	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp timescale arb PT-7828(config)# ptp timescale ptp	
Error messages	N/A	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp transport

Use the **ptp transport** configuration command on the switch to set the transport type of the ptp domain.

Commands**ptp transport [802_3|ipv4]**

Syntax Description	ptp	Configure PTP
	transport	Set the transport type of the ptp domain
	802_3	Set the transport type of the PTP domain to 802.3/Ethernet
	ipv4	Set the transport type of the PTP domain to IPv4
Defaults	default is ipv4	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# ptp transport 802_3 PT-7828(config)# ptp transport ipv4	
Error messages	N/A	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp utc-offset

Use the **ptp utc-offset** configuration command on the switch to set the PTP utc-offset field.

Commands**ptp utc-offset interval**

Syntax	ptp	Configure PTP
--------	------------	---------------

Description	utc-offset	sets the offset between TAI and UTC
	<i>interval</i>	0 to 65535
Defaults	default is 0	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# <code>ptp utc-offset 0</code>	
Error messages	utc_offset must be in the range from 0 to 65535	
Related commands	Show ptp settings Show ptp status Show ptp port	

ptp utc-offset-valid

Use the **ptp utc-offset-valid** configuration command on the switch to enable the PTP utc-offset field. Use the **no** form of this command to disable the PTP utc-offset field on the switch.

Commands

ptp utc-offset-valid
no ptp utc-offset-valid

Syntax	ptp	Configure PTP
Description	utc-offset-valid	UTC Offset field is valid
Defaults	default disable	
Command Modes	configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# <code>ptp utc-offset-valid</code> PT-7828(config)# <code>no ptp utc-offset-valid</code>	
Error messages	N/A	
Related commands	Show ptp settings Show ptp status Show ptp port	

qos highest-priority

Use the **qos highest-priority** interface configuration command on the switch to set the Port Priority of the ingress frames to "High" queues of the Ethernet ports/Trunks. Use the **no** form of this command to return to the default.

Commands

qos highest-priority
no qos highest-priority

Syntax	qos	Configure QoS
Description	highest-priority	Enable port highest priority queue
Defaults	N/A	

Command Modes	Interface configuration
Usage Guidelines	N/A
Examples	EDS-518A(config-if)# qos highest-priority
Error messages	Cannot configure on trunk member port 1/1!
Related commands	show qos

qos default-cos

Use the **qos default-cos** interface configuration command on the switch to configure the default CoS priority of the Ethernet ports/Trunks. Use the **no** form of this command to return to the default.

Commands

qos default-cos *cos-value*
no qos default-cos

Syntax	qos	Configure QoS
Description	default-cos	Configure Default CoS of each port
	<i>cos-value</i>	CoS value (0 to 7)
Defaults	Default CoS value is 3	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-if)# qos default-cos <UINT:cos> - CoS value (0 to 7)	
Error messages	Cannot configure on trunk member port 1/1!	
Related commands	show qos	

qos inspect

Use the **qos inspect** global/interface configuration command on the switch to enable the inspect criteria. Use the **no** form of this command to disable it.

Commands

qos inspect dscp *module_id*
no qos inspect dscp *module_id*
qos inspect cos
no qos inspect cos

Syntax	qos	Configure QoS
Description	inspect	Configure inspection criteria
	dscp	Enable DSCP inspection
	<i>module_id</i>	Module ID from 1 to 4
	cos	Enable CoS inspection of each port
Defaults	N/A	

Command Modes	Global configuration Interface configuration
Usage Guidelines	In product with 88E6095, the “qos inspect dscp” command is configured in interface configuration mode. In product with BCM5650, the “qos inspect dscp” command is configured in global configuration mode with module index.
Examples	PT-7828(config)# qos inspect dscp - Enable DSCP inspection PT-7828(config-if)# qos inspect cos - Enable CoS inspection of each port
Error messages	Cannot configure on trunk member port 1/1!
Related commands	show qos

qos mapping

Use the **qos mapping** global configuration command on the switch to configure the CoS and DSCP mappings. Use the **no** form of this command to return to the default.

Commands

```
qos mapping cos-to-queue cos-value queue
no qos mapping cos-to-queue
qos mapping dscp-to-cos dscp-value cos-value
no qos mapping dscp-to-cos
qos mapping dscp-to-queue dscp-value queue
no qos mapping dscp-to-queue
```

Syntax Description	qos	Configure QoS
	mapping	Configure QoS mapping
	cos-to-queue	CoS to traffic queue
	<i>cos-value</i>	CoS value (0 to 7)
	<i>queue</i>	Traffic queue
	dscp-to-cos	DSCP to CoS mapping
	<i>dscp-value</i>	DSCP value (0 to 63)
	dscp-to-queue	DSCP to traffic queue
Defaults	Cos (queue): 0 (0), 1(0), 2(1), 3(1), 4(2), 5(2), 6(3), 7(3) DSCP(Cos): 0-7(0), 8-15(1), 16-23(2), 24-31(3), 32-39(4), 40-47(5), 48-55(6), 56-63(7)	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# qos mapping cos-to-queue 7 <UINT:queue> - Traffic queue PT-7828(config)# qos mapping cos-to-queue 7 3 PT-7828(config)# qos mapping dscp-to-cos 23 <UINT:cos> - CoS value (0 to 7) PT-7828(config)# qos mapping dscp-to-cos 23 7	
Error messages	Invalid parameter. CoS value must be 0 to 7 and queue number must be 0 to 3 Invalid parameter. CoS value must be 0 to 7 and DSCP value must be 0 to 63	
Related commands	show qos	

qos mode

Use the **qos mode** global configuration command on the switch to configure the current QoS strategy. Use the **no** form of this command to return to the default.

Commands

qos mode { weighted-fair | strict }
no qos mode

Syntax Description	qos	Configure QoS
	mode	Configure queuing mechanism
	weighted-fair	Weighted fair queuing
	strict	Strict queuing
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# qos mode weighted-fair - Weighted fair queuing strict - Strict queuing</pre>	
Error messages	N/A	
Related commands	show qos	

quit

Use **quit** to quit the current configuration mode.

Commands

exit

Syntax Description	quit	Exit command line interface
Defaults	N/A	
Command Modes	N/A	
Usage Guidelines	N/A	
Examples	PT-7828 # quit	
Error messages	N/A	
Related commands	Exit	

rate-limit

Use the **rate-limit** interface configuration command on the switch to configure the traffic rate allowed for the specified port. Use the **no** form of this command to return to the default. For Marvell 88E6095 chipsets, use **rate-limit ingress rate** to set the ingress rate limiting; for Broadcom chipsets, use **rate-limit ingress percentage** to set the ingress rate limiting.

Commands

rate-limit { ingress | egress } percentage *percentage*
no rate-limit { ingress | egress }
rate-limit ingress rate { none | 128k | 256k | 512k | 1M | 2M | 4M | 8M }
rate-limit ingress mode { bcast | bcast-mcast | bcast-mcast-dlf | all }
rate-limit mode { normal | port-disable }
rate-limit normal { ingress | egress } percentage *percentage*
no rate-limit normal { ingress | egress }
rate-limit normal ingress rate { none | 128k | 256k | 512k | 1M | 2M | 4M | 8M }

rate-limit normal ingress mode { bcast | bcast-mcast | bcast-mcast-dlf | all }
rate-limit port-disable period *period*
rate-limit port-disable ingress rate { none | 44640 | 74410 | 148810 | 223220 | 372030 | 520840 | 744050 }

Syntax Description	rate-limit	Rate limiting
	normal	Rate limiting normal mode
	port-disable	Rate limiting port-disable mode
	ingress	Ingress rate limiting
	egress	Egress rate limiting
	percentage	Percentage correspond to current port speed
	<i>percentage</i>	Limit percentage, and will take effect at the percentage 0/3/5/10/15/25/35/50/65/85
	rate	Specify the rate
	mode	Specify the mode
	bcast	Limit broadcast frames
	bcast-mcast	Limit broadcast and multicast frames
	bcast-mcast-dlf	Limit broadcast, multicast and DLF frames
	all	All traffic
	period	Port disable period
<i>period</i>	Seconds	
Defaults	0 or none means unlimiting.	
Command Modes	Interface configuration	
Usage Guidelines	The <i>percentage</i> will only take effect at the 0/3/5/10/15/25/35/50/65/85 %. For port disable mode, the port will be disabled when the ingress rate reach the specified packet rate.	
Examples	<pre>PT-7828(config-if)# rate-limit percentage <UINT:percent> - Limit percentage, and will take effect at the percentage 0/3/5/10/15/25/35/50/65/85 EDS-408A-1M2S-SC(config-if)# rate-limit ingress rate none none none none PT-7828(config-if)# rate-limit port-disable ingress period 30 EDS-408A-1M2S-SC(config-if)# rate-limit port-disable ingress rate 148810</pre>	
Error messages	Cannot configure on trunk member port 1/1!	
	This setting cannot be applied on trunk port!	
Related commands	show interfaces rate-limit	

redistribute

Use the **redistribute** commands to enable learning routes from another IP routing protocol. Use the **no** form of this command to disable it.

Commands

redistribute connected
no redistribute connected
redistribute static
no redistribute static
redistribute rip
no redistribute rip
resitribute ospf
no redistribute ospf

Commands	redistribute	Enable the switch's import routes learned through another IP routing protocol
----------	---------------------	---

	connected	Import routes learned through directly connected
	Static	Import routes learned through static route
	rip	Import routes learned through RIP
	ospf	Import routes learned through OSPF
Defaults	N/A	
Command Modes	Router configuration mode as OSPF / RIP	
Usage Guidelines	N/A	
Examples	PT-7828(config-ospf)# redistribute rip PT-7828(config-rip)# redistribute ospf	
Error messages	N/A	
Related commands	show ip ospf show ip rip	

redundancy

Use the **redundancy** global configuration command on the switch to enter the redundancy configuration mode.

Commands

redundancy

Syntax Description	redundancy	Enter redundancy configuration mode
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# redundancy PT-7828(config-rdnt)#	
Error messages	N/A	
Related commands	N/A	

redundancy mode

Use the **redundancy mode** global configuration command on the switch to change the redundancy protocol mode.

Commands

redundancy mode { mst | rstp | turbo-ring-v1 | turbo-ring-v2 | turbo-chain }

Syntax Description	redundancy	Enter redundancy configuration mode
	mode	Specify the redundancy protocol
	mst	MSTP
	rstp	Rapid Spanning Tree
	turbo-ring-v1	Turbo ring version 1
	turbo-ring-v2	Turbo ring version 2
	turbo-chain	Turbo chain
Defaults	The default redundancy protocol mode is RSTP.	
Command Modes	Global configuration	

Usage Guidelines	N/A
Examples	PT-7828(config)# redundancy mode rstp - Rapid Spanning Tree turbo-ring-v1 - Turbo ring version 1 turbo-ring-v2 - Turbo ring version 2 turbo-chain - Turbo chain mst - MSTP
Error messages	N/A
Related commands	show redundancy mode

relay-warning config relay

Use **relay-warning config relay** to select relay to trigger when a warning event occurs.

Commands

relay-warning config relay [relayId]

Syntax Description	relay-warning	Configure relay warning
	config	Choose which relay to configure
	relay	Relay
	<i>relayId</i>	Relay's ID = 1 or 2
Defaults	N/A	
Command Modes	Global configuration / Interface configuration	
Usage Guidelines	These commands only existed in device with multiple relays.	
Examples	N/A	
Error messages	Please designate the relay ID Invalid relay ID	
Related commands	show relay-warning	

relay-warning event

Use **relay-warning event** global configuration commands to enable the warning events trigger to the relay. Use the **no** form of this command to disable it.

Commands

relay-warning event { power-input1-fail | power-input2-fail | turbo-ring-break }
no relay-warning event { power-input1-fail | power-input2-fail | turbo-ring-break }

Syntax Description	relay-warning	Configure relay warning
	event	System events
	power-input1-fail	Power input 1 failure (On->Off)
	power-input2-fail	Power input 2 failure (On->Off)
	turbo-ring-break	Turbo Ring break
Defaults	All system events are disabled by default.	
Command Modes	Global configuration	
Usage Guidelines	N/A	

Examples	<pre>PT-7828# configure terminal PT-7828(config)# relay-warning override - Override the relay warning setting - System events event - System events PT-7828(config)# relay-warning event power-input1-fail - Power input 1 failure (ON->Off) power-input2-fail - Power input 2 failure (ON->Off) turbo-ring-break - Turbo Ring break PT-7828(config)# relay-warning event turbo-ring-break</pre>
Error messages	N/A
Related commands	show relay-warning

relay-warning event

Use **relay-warning event** interface configuration commands to enable the warning events trigger to the relay. Use the **no** form of this command to disable it.

Commands

relay-warning event { link-on | link-off }
relay-warning event traffic-overload [rxThreshold duration]
no relay-warning event { link | traffic-overload }

Syntax Description	relay-warning	Configure relay warning
	event	Port events
	link-on	Link ON
	link-off	Link OFF
	traffic-overload	Traffic overloading
	<i>rxThreshold</i>	0 to 100
	<i>duration</i>	1 to 300
Defaults	All interface events are disabled by default.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# interface ethernet 3/1 PT-7828(config-if)# relay-warning event ? link-on - Link ON link-off - Link OFF traffic-overload - Traffic overloading PT-7828(config-if)# relay-warning event link-off PT-7828(config-if)# relay-warning event traffic-overload</pre>	
Error messages	Threshold should be between 0 and 100	
	Duration should be between 1 and 300	
Related commands	show relay-warning	

relay-warning override

Use **relay-warning override relay** to override the relay warning setting temporarily. Releasing the relay output will allow administrators to fix any problems with the warning condition. Use the **no** form of this command to disable the override.

Commands

relay-warning override relay [relayId]
no relay-warning override relay [relayId]

Syntax	relay-warning	Configure relay warning
Description	override	Override the relay warning setting
	relay	Relay
	relayId	Relay's ID = 1 or 2
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	relayId will only be used on the product that have multiple relays.	
Examples	PT-7828(config)# relay-warning override relay	
Error messages	Please designate the relay ID Invalid relay ID	
Related commands	show relay-warning	

reload

Use the **reload** privileged command on the switch to restart the Vipa Switch. Use the **reload factory-default** privileged command to restore the switch configuration to the factory default values.

Commands

reload [factory-default]

Syntax	reload	Halt and perform a cold restart
Description	factory-default	Halt and perform a cold restart with factory default
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# reload <LF> factory-default - Halt and perform a cold restart with factory default PT-7828# rel reload - Halt and perform a cold restart PT-7828# reload factory-default <LF> PT-7828# reload Proceed with reload ? [Y/n] PT-7828# reload factory-default Proceed with reload to factory default? [Y/n]</pre>	
Error messages	N/A	
Related commands	N/A	

router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the **router ospf** command in global configuration mode. To terminate an OSPF routing process, use the **no** form of this command.

Commands

router ospf [router-id]
no router ospf

Syntax Description	router	Enable a routing process
	ospf	Enable OSPF routing, and enter router configuration mode
	<i>router-id</i>	OSPF routing ID has a unique value
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	Use router ospf commands to enable OSPF routing process. Use router ospf router-id to entering the Router configuration mode as OSPF.	
Examples	<pre>PT-7828(config)# router ospf PT-7828(config)# router ospf 0.0.1.1 PT-7828(config-ospf)#</pre>	
Error messages	Invalid parameters!	
Related commands	show ip ospf	

router rip

Use the **router rip** global configuration command to Enable a RIP routing process, and enter router configuration mode. To turn off the RIP routing process, use the **no** form of this command.

Commands

router rip
no router rip

Syntax Description	router	Enable a routing process
	rip	Enable RIP (Routing Information Protocol)
Defaults	RIP is disabled in factory default.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# router rip PT-7828(config-rip)#</pre>	
Error messages	N/A	
Related commands	show ip rip	

router vrrp

To enable Virtual Router Redundancy Protocol (VRRP), use the **router vrrp** command in global configuration mode. To disable the VRRP, use the **no** form of this command

Commands

router vrrp
no router vrrp

Syntax Description	router	Enable a routing process
	vrrp	Enable VRRP (Virtual Router Redundancy Protocol)
Defaults	VRRP is not default disabled.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# router vrrp PT-7828(config)# no router vrrp</pre>	

Error messages	N/A
Related commands	show ip vrrp

router vrrp adver-interval

NOTE This command is only supported by Layer 3 switches.

Use **router vrrp adver-interval** command in global configuration mode to setup VRRP advertisement interval.

Commands

router vrrp adver-interval *interval*

Syntax Description	router	Enable a routing process
	vrrp	Enable VRRP (Virtual Router Redundancy Protocol)
	adver-interval	Configure advertisement interval
	<i>interval</i>	Interval value
Defaults	Default VRRP adver-interval is 1000 ms	
Command Modes	Global configuration	
Usage Guidelines	The join-prune interval range is 25 to 1000 ms	
Examples	ICS-G7852A-4XG(config)# router vrrp adver-interval 25	
Error messages	N/A	
Related commands	show ip vrrp	

save config

Use the **save config** command to save the running configuration to the startup configuration on flash.

Commands

save config

Syntax Description	save	Save running configuration to flash
	config	Save running configuration to flash
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	PT-7828# save config Saving configuration ...Success	
Error messages	N/A	
Related commands	N/A	

show acl

NOTE The command is supported only in Layer 3 switches

Use the **show acl user EXEC** command to display the ACL configuration.

Commands

show acl [*id*]

show acl summary

Syntax	show	Show running system information
Description	acl	Display ACL information
	<i>id</i>	The access list ID
	summary	Display active ACL status
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show acl 10 ACL ID : 10 Name : Type : MAC-base Rule Index : 1 Action : deny Source MAC Address : 00:11:22:33:44:55/FF:FF:FF:00:00:00 Destination MAC Address : AA:BB:CC:DD:EE:FF/FF:FF:FF:00:00:00 Ether Type : 2048 VLAN ID : 10 Ingress Port Map : 0 Egress Port Map : 0 ----- PT-7828# show acl summary Type ID Attached Port Name ----- MAC-base 1 test_acl1 MAC-base 10</pre>	
Error messages	Invalid ID!	
Related commands		

show auth tacacs+

Use the **show auth tacacs+** user EXEC command to display the setting of TACACS+ authentication traffic statistic information of interfaces.

Commands

show auth tacacs+

Syntax	auth	Display authentication settings
Description	tacacs+	Tacacs+ authentication

Defaults	N/A
Command Modes	Privileged EXEC/ User EXEC
Usage Guidelines	N/A
Examples	<pre>PT-7828# show auth tacacs+ Tacacs+ information: Status : Disabled Auth server : tacacs.server.vipa.com, port:49 Shared key : Auth type : ASCII Server Timeout : 23 sec.</pre>
Error messages	N/A
Related commands	<pre>auth tacacs+ auth tacacs+ server auth tacacs+ auth-type</pre>

show clock

Use the **show clock** user EXEC command to display time-related settings.

Commands

show clock

Syntax Description	clock	Display the system clock
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show clock Current Time : Fri Jan 01 08:38:28 2010 Daylight Saving Start Date : End Date : Offset : Time Zone : GMT-4:00 Time Server : Query Period : 600 sec NTP/SNTP Server : Disabled</pre>	
Error messages	N/A	
Related commands	<pre>clock set clock summer-time clock timezone ntp refresh-time ntp remote-server ntp server</pre>	

show dot1x

To check the 802.1x setting, use the **show dot1x** command.

Commands

show dot1x

Syntax Description	dot1x	Display 802.1x settings
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	<pre>PT-7828# show dot1x Database Option: Local Radius Server : localhost Server Port : 1812 Shared Key : Re-Auth : Enable Re-Auth Period : 3600 Port 802.1X Enable ----- 1-1 Disable 1-2 Enable 1-3 Disable 1-4 Disable</pre>	
Examples	N/A	
Error messages	N/A	
Related commands	dot1x auth dot1x reauth	

show dot1x local-userdb

To check the 802.1x local user database, use the **show dot1x local-userdb** command.

Commands

show dot1x local-userdb

Syntax Description	dot1x	Display 802.1x settings
	local-userdb	Display current local database
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	<pre>PT-7828# show dot1x local-userdb Index User Name Description ----- 1 vipanet vipanet</pre>	
Examples	N/A	
Error messages	N/A	
Related commands	dot1 local-userdb	

show eip

Commands

show eip

Syntax Description	eip	Display Ethernet/IP configuration
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	PT-7828# show eip eip disable	
Examples	N/A	
Error messages	N/A	
Related commands	eip	

show PROFINETIO

Use the **show profinetio** user EXEC command to display PROFINET configuration

Commands

show profinetio

Syntax Description	show	Show running system information
	profinetio	Display PROFINET configuration
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	EDS-G516E> show profinetio profinet io disable	
Error messages	N/A	
Related commands	profinetio	

show email-warning config

Commands

show email-warning config

Syntax Description	show	Show running system information
	email-warning	Display Email warning configuration
	config	Email warning configuration
Defaults	N/A	
Command Modes	Privileged EXEC /User EXEC	
Usage Guidelines	N/A	
Examples	PT-7828# show email-warning config Mail Server and Email Setup SMTP Server IP/Name : SMTP Port : 25 Account Name : Account Password :	

	<pre> 1st email address : 2nd email address : 3rd email address : 4th email address : System Events Cold Start : Disable Warm Start : Disable Conf. Changed : Disable Power On->Off : Disable Power Off->On : Disable Auth. Failure : Disable Topology Changed : Disable --More-- Port Events Setting Traffic Link Link Traffic RX Port ON OFF Overload Threshold(%) Duration(s) ----- 1-1 Disable Disable Disable 0 1 1-2 Disable Disable Disable 0 1 1-3 Disable Disable Disable 0 1 1-4 Disable Disable Disable 0 1 1-5 Disable Disable Disable 0 1 1-6 Disable Disable Disable 0 1 1-7 Disable Disable Disable 0 1 1-8 Disable Disable Disable 0 1 3-1 Disable Disable Disable 0 1 3-2 Disable Disable Disable 0 1 3-3 Disable Disable Disable 0 1 3-4 Disable Disable Disable 0 1 3-5 Disable Disable Disable 0 1 3-6 Disable Disable Disable 0 1 3-7 Disable Disable Disable 0 1 3-8 Disable Disable Disable 0 1 PT-7828# </pre>				
Error messages	N/A				
Related	email-warning event				

commands	email-warning account email-warning server email-warning mail-address
----------	---

show gmrp

Use the **show igmp** user EXEC command to display the GMRP table of the switch.

Commands

show gmrp

Syntax Description	gmrp	Show GMRP Settings
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	<pre>PT-7828# show gmrp Index Multicast Address Fixed Ports Learned Ports ----- -----</pre>	
Examples	N/A	
Error messages	N/A	
Related commands	gmrp	

show gvrp

Use the **show gvrp** user EXEC command to display GVRP state information.

Commands

show gvrp

Syntax Description	show	Show running system information
	gvrp	Display GVRP configuration
Defaults	N/A	
Command Modes	Privileged EXEC / User Exec	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show gvrp gvrp enable</pre>	
Error messages	N/A	
Related commands	gvrp	

show interfaces acl

NOTE The command is supported only in Layer 3 switches

Use the **show interfaces acl** user EXEC command to display ACL configurations by port.

Command

show interfaces ethernet [*module/port*] **acl**

Syntax	show	Show running system information
Description	interfaces	Interface status and configuration
	ethernet	IEEE 802.3/IEEE 802.3z
	<i>module/port</i>	Port ID or list. Ex. 1/1,2,3,2/1-3,5,...
	acl	Display ACL configurations by port
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show interfaces ethernet 2/1 acl Type ID Direction Index ----- IP-base 2 Inbound 1 MAC-base 4 Inbound 2 IP-base 7 Inbound 3 MAC-base 11 Outbound 4</pre>	
Error messages	Invalid ID!	
Related commands		

show interfaces counters

Use the **show interfaces counters** user EXEC command to display traffic statistics information of interfaces.

Commands

show interfaces counters

show interfaces ethernet *port-id* **counters**

show interfaces trunk *trunk-id* **counters**

Syntax Description	interfaces	Interface status and configuration	
	counters	Display counters	
	<i>port-id</i>	Port ID or list. E.g., 1/1,2,3,2/1-3,5,...	
	<i>trunk-id</i>	Trunk ID (or list)	
Defaults	N/A		
Command Modes	Privileged EXEC/ User EXEC		
Usage Guidelines	Detail counter information will contain the differences information from last query.		
Examples	<pre>PT-7828# show interfaces counters Port Tx Packets (Load%) Rx Packets (Load%) ----- 1/ 5 662 (0) 364 (0) 1/ 6 0 (0) 0 (0) Trk1 1608 (0) 1608 (0) Trk2 0 (0) 0 (0) PT-7828# show interfaces ethernet 1/5 counters Port 1/5 (last sample time: 16577 sec. ago) - TX - Unicast Packets : 108 +108</pre>		

	<pre> Multicast Packets : 553 +553 Broadcast Packets : 2 +2 Collision Packets : 0 +0 - RX - Unicast Packets : 109 +109 Multicast Packets : 0 +0 Broadcast Packets : 255 +255 Pause Packets : 0 +0 - Error - TX Late : 0 +0 TX Excessive : 0 +0 RX CRC error : 0 +0 RX Discard : 0 +0 RX Undersize : 0 +0 RX Fragments : 0 +0 RX Oversize : 0 +0 RX Jabber : 0 +0 </pre>
Error messages	N/A
Related commands	N/A

show interfaces ethernet

To check the status of interfaces, use the **show interfaces ethernet** command.

Commands

show interfaces ethernet [*module/port* [**config**]]

Syntax Description	interfaces	Interface status and configuration
	ethernet	IEEE 802.3/IEEE 802.3z
	<i>module/port</i>	Port ID or list. E.g., 1/1,2,3,2/1-3,5,...
	config	Show interface module/port settings
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	

Usage Guidelines	<pre>PT-7828# show interfaces ethernet Port Link Description Speed FDX Flow Ctrl MDI/MDIX ----- 1-1 Down 100TX, RJ45. -- -- 1-2 Down 100TX, RJ45. -- -- 1-3 Down 100TX, RJ45. -- -- 1-4 Down 100TX, RJ45. -- -- 1-5 Up 100TX, RJ45. 100M-Full Off MDI 1-6 Down 100TX, RJ45. -- -- 1-7 Down 100TX, RJ45. -- -- 1-8 Down 100TX, RJ45. -- --</pre>
	<pre>PT-7828# show interfaces ethernet 1/1-3 config Port Enable Description Speed FDX Flow Ctrl MDI/MDIX ----- 1-1 Yes 100FX, SC, Single, 40. 100M-Full Disable Auto 1-2 Yes 100FX, SC, Single, 40. 100M-Full Disable Auto 1-3 Yes 100TX, RJ45. Auto Disable Auto</pre>
Examples	N/A
Error messages	N/A
Related commands	N/A

show interfaces filter-ip

Use the **show interfaces filter-ip** user EXEC command to display the setting of IP filtering entries.

Commands

show interfaces ethernet *module/port* filter-ip

Syntax	interfaces	Interface status and configuration
Description	ethernet	IEEE 802.3/IEEE 802.3z
	<i>module/port</i>	Port ID or list. E.g., 1/1,2,3,2/1-3,5,...
	filter-ip	Rate limiting configuration
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show interfaces ethernet 1/1-6 filter-ip Allowed IP in Port 1/1: 192.168.127.1 192.168.127.2 192.168.127.3 192.168.127.4 192.168.127.5 192.168.127.6 192.168.127.7 192.168.127.8 Allowed IP in Port 1/2: Allowed IP in Port 1/3: Allowed IP in Port 1/4: --More-- Allowed IP in Port 1/5: 192.168.127.1 Allowed IP in Port 1/6:</pre>	
Error messages	N/A	
Related commands	ip filter-ip	

show interfaces mgmt

Use the **show interfaces mgmt** user EXEC command to display the Mgmt-VLAN settings.

Commands**show interfaces mgmt**

Syntax Description	interfaces	Interface status and configuration
	mgmt	Display management VLAN information
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show interfaces mgmt IPv4 Management VLAN id : 1 IP configuration : Static IP address : 192.168.127.253 Subnet mask : 255.255.255.0 Default gateway : 0.0.0.0 DNS server :</pre>	
Error messages	N/A	
Related commands	ip address ip default-gateway ip name-server bind vlan	

show interfaces mgmt access-ip

Use the **show interfaces mgmt access-ip** user EXEC command to display the settings of accessible IP list.

Commands**show interfaces mgmt access-ip**

Syntax Description	show	Show running system information
	interfaces	Interface status and configuration
	mgmt	Display management VLAN information
	access-ip	Display accessible IP list
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show interfaces mgmt access-ip Accessible IP List: Enable Index IP / Netmask 1 192.168.127.253 / 255.255.255.0</pre>	
Error messages	N/A	
Related commands	access-ip	

show interfaces rate-limit

Use the **show interfaces rate-limit** user EXEC command to display the setting of Rate-limiting.

Commands

show interfaces ethernet *module/port* **rate-limit**

Syntax Description	interfaces	Interface status and configuration
	ethernet	IEEE 802.3/IEEE 802.3z
	<i>module/port</i>	Port ID or list. E.g., 1/1,2,3,2/1-3,5,...
	rate-limit	Rate limiting configuration
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-508# show interfaces ethernet 1/1-3 rate-limit Port 1/1: Ingress Limit Mode: Broadcast, Multicast, DLF Ingress Limit Rate: 8M Egress Limit Rate : Not Limited Port 1/2: Ingress Limit Mode: Broadcast Ingress Limit Rate: 8M Egress Limit Rate : Not Limited Port 1/3: Ingress Limit Mode: Broadcast Ingress Limit Rate: 8M Egress Limit Rate : Not Limited</pre>	
Error messages	N/A	
Related commands	rate-limit	

show interfaces trunk

Use the **show interfaces trunk** user EXEC command to display spanning-tree state information

Commands

show interfaces trunk [*trunk-id-list*]

Syntax Description	interfaces	Interface status and configuration
	trunk	Show interface trunk information
	<i>trunk-id-list</i>	Trunk ID (or list)
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	

Examples	<pre>PT-7828# show interfaces trunk Trk# Type Enable Description Speed ----- - 1 Static Yes 100M- Full 2 Static Yes 100M- Full PT-7828# show interfaces trunk 1-2 Trunk-1 (Static): Member Status ----- - 1/1 Success 1/2 Success Trunk-2 (Static): Member Status ----- - 1/3 Fail 1/4 Fail</pre>
Error messages	There is no member in Trunk 1
Related commands	trunk-mode trunk-group

show interfaces vlan

Use the **show interfaces vlan** user EXEC command to display vlan ip interface information.

Commands

show interfaces vlan [vlan-id-list]

Syntax	show	Show running system information
Description	Interfaces	Interface status and configuration
	Vlan	Display layer3 IP interface settings
	vlan-id-list	1 to 4094
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show interfaces vlan Interface Name: VLAN2 IP Address: 10.10.10.10 Subnet Mask: 255.255.255.0 VLAN ID: 2 Proxy ARP: Disable</pre>	
Error messages	N/A	
Related commands	Interface vlan	

show interfaces mgmt trusted-access

Same as show interfaces mgmt access-ip.

Commands

show interfaces mgmt trusted-access

Syntax Description	show	Show running system information
	interfaces	Interface status and configuration
	mgmt	Display management VLAN information
	trusted-access	Display trusted access IP list
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show interfaces mgmt trusted-access Trusted Access IP List: Enable Index IP / netmask 1 192.168.127.253 / 255.255.255.0</pre>	
Error messages	N/A	
Related commands	trusted-access	

show ip auto-assign

Use the **show ip auto-assign** user EXEC command to display the setting of the Auto IP Assignment feature.

Commands

show ip auto-assign

Syntax Description	ip	Display IP information
	auto-assign	Display automatic ip assignment settings
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show ip auto-assign Port Device's Current IP Active Function Desired IP ----- 1/ 6 NA -- 192.168.127.8 Trk1 NA -- 192.168.127.7</pre>	
Error messages	N/A	
Related commands	ip auto-assign	

show ip dhcp-relay config

Use the **show ip dhcp-relay config** user EXEC command to display the setting of the DHCP relay feature.

Commands

show ip dhcp-relay config

Syntax Description	show	Show running system information
	ip	Display IP information
	dhcp-relay	Display DHCP relay configuration

	config	DHCP relay configuration
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show ip dhcp-relay config DHCP Relay Agent Setting 1st server IP : 2nd server IP : 3rd server IP : 4th server IP : DHCP Relay Option 82: Enable Remote ID type : Other Remote ID value : 1234567890123 Remote ID display: 31323334353637383930313233 --More-- DHCP Function Table Port Circuit-ID Option 82 ----- 1-1 01000101 Disable 1-2 01000102 Disable 1-3 01000103 Disable 1-4 01000104 Disable 1-5 01000105 Disable 1-6 01000106 Disable 1-7 01000107 Disable 1-8 01000108 Disable 3-1 01000111 Disable 3-2 01000112 Disable 3-3 01000113 Disable 3-4 01000114 Disable 3-5 01000115 Disable 3-6 01000116 Disable 3-7 01000117 Disable 3-8 01000118 Disable PT-7828#</pre>	
Error messages	N/A	
Related commands	N/A	

show ip http-server status

Use `show ip http-server status` to display HTTP server related settings.

Commands

`show ip http-server status`

Syntax Description	show	Show running system information
	ip	Display IP information
	http-server	HTTP server information
	status	Status
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	

Usage Guidelines	N/A
Examples	PT-7828# show ip http-server status HTTP service is enable HTTP server capability: Present HTTPS secure server capability: Present Auto-logout: disable
Error messages	N/A
Related commands	N/A

show ip igmp

Use the **show ip igmp** user EXEC command to display the Internet Group Management Protocol (IGMP) snooping configuration and IGMP table of the switch.

Commands

show ip igmp

Commands	ip	Display IP information
	igmp	Show IGMP snooping settings
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	<pre>PT-7828# show ip igmp IGMP Snooping :Enable IGMP Snooping Enhanced Mode :Enable Query Interval :125(sec) VID Static(S) / Learned(L) Active IGMP Groups Multicast Querier Port & IP MAC Members Port Querier(Q) connected Port ----- 1 1-1 (S) 224.1.1.8 01- 00-5E-01-01-08 1-1 239.255.255.250 01- 00-5E-7F-FF-FA 1-1</pre>	
Examples	N/A	
Error messages	N/A	
Related commands	ip igmp ip igmp snooping	

show ip ospf

Use the **show ip ospf** user EXEC command to display general information about OSPF routing processes.

Commands

show ip ospf

Syntax	show	Show running system information
Description	ip	Display IP information

	ospf	Display OSPF configurations
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show ip ospf OSPF Golbal Configuration ----- OSPF Enabled Router ID 192.168.1.1 Current Router ID 192.168.1.1 Redistribute [Connected] OSPF Area Configuration Idx Area ID Area Type Metric ----- 1 192.168.1.1 Normal 0 OSPF Virtual Link Configuration Idx Transit Area ID Neighbor Router ID ----- 1 192.168.1.1 192.168.0.0 OSPF Aggregation Configuration Idx Area ID Network Address Network Mask -----</pre>	
Error messages	N/A	
Related commands	area area virtual-link network area redistribute	

show ip ospf database

Use the **show ip ospf database** user EXEC command to display information related to the OSPF database for a specific router.

Commands

show ip ospf database

Syntax Description	show	Show running system information
	ip	Display IP information
	ospf	Display OSPF configurations
	database	OSPF database
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	

Examples	PT-7828# show ip ospf database
Error messages	N/A
Related commands	ip ospf area

show ip ospf interface

Use the **show ip ospf interface** user EXEC command to display the OSPF related interfaces information.

Commands

show ip ospf interface

Syntax Description	show	Show running system information
	ip	Display IP information
	ospf	Display OSPF configurations
	interface	OSPF routing interface
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	PT-7828# show ip ospf interface	
Error messages	N/A	
Related commands	ip ospf area ip ospf priority ip ospf hello-interval ip ospf dead-interval ip ospf cost	

show ip ospf neighbor

Use the **show ip ospf neighbor** user EXEC command to display OSPF neighbor information.

Commands

show ip ospf neighbor

Syntax Description	show	Show running system information
	ip	Display IP information
	ospf	Display OSPF configurations
	neighbor	OSPF neighbor information
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	PT-7828# show ip ospf neighbor	
Error messages	N/A	
Related commands	ip ospf area	

show ip pim-dm

NOTE This command is only supported by Layer 3 switches.

Use **show ip pim-dm** command to display the settings of PIM-DM.

Commands

show ip pim-dm

Syntax	show	Show running system information	
Description	ip	Display IP information	
	pim-dm	Display PIM-DM information	
Defaults	N/A		
Command Modes	Privileged EXEC/ User EXEC		
Usage Guidelines	N/A		
Examples	ICS-G7852A-4XG# show ip pim-dm		
	PIM-DM: Enable		
	Interface	Address VID Enable Mode	

	V100	172.100.1.2	100 V
V200	172.200.1.2	200 V	
V10	172.10.1.2	10 V	
V20	172.20.1.2	20 V	
Error messages	N/A		
Related commands	ip pim-dm no ip pim-dm		

show ip pim-dm neighbor

NOTE This command is only supported by Layer 3 switches.

Use **show ip pim-dm neighbor** command to display PIM-DM neighbor information.

Commands

show ip pim-dm neighbor

Syntax	show	Show running system information	
Description	ip	Display IP information	
	pim-dm	Display PIM-DM information	
	neighbor	PIM-DM neighbor information	
Defaults	N/A		
Command Modes	Privileged EXEC/ User EXEC		
Usage Guidelines	N/A		
Examples	ICS-G7852A-4XG# show ip pim-dm neighbor		
	PIM Neighbor Table		
	Index Neighbor	Address Interface Uptime Expire	

	1	172.100.1.4	V100 89 ---
2	172.100.1.1	V100 89 ---	
3	172.200.1.3	V200 75 ---	
Error messages	N/A		
Related commands	ip pim-dm no ip pim-dm		

show ip pim-sm

NOTE This command is only supported by Layer 3 switches.

Use **show ip pim-sm** command to display the settings of PIM-SM.

Commands

show ip pim-sm

Syntax Description	show	Show running system information			
	ip	Display IP information			
	pim-sm	Display PIM-SM information			
Defaults	N/A				
Command Modes	Privileged EXEC/ User EXEC				
Usage Guidelines	N/A				
Examples	ICS-G7852A-4XG# show ip pim-sm				
	PIM-SM: Enable				
		Interface	Address	VID	Enable Mode

		V100	172.100.1.2	100	V
		V200	172.200.1.2	200	V
	V10	172.10.1.2	10	V	
	V20	172.20.1.2	20	V	
Error messages	N/A				
Related commands	ip pim-sm no ip pim-sm ip pim-sm dr-priority ip pim-sm hello-interval ip pim-sm join-prune-interval				

show ip pim-sm bsr

NOTE This command is only supported by Layer 3 switches.

Use **show ip pim-sm bsr** command to display PIM-SM BSR information.

Commands

show ip pim-sm bsr

Syntax Description	show	Show running system information			
	ip	Display IP information			
	pim-sm	Display PIM-SM information			
	bsr	PIM-SM BSR information			
Defaults	N/A				
Command Modes	Privileged EXEC/ User EXEC				
Usage Guidelines	N/A				
Examples	ICS-G7852A-4XG# show ip pim-sm bsr				
	PIM BSR				
		BSR Address	Priority	Hash Mask	Length

	172.230.1.1	0	4		
Error messages	N/A				
Related commands	ip pim-sm no ip pim-sm ip pim-sm dr-priority ip pim-sm hello-interval ip pim-sm join-prune-interval				

show ip pim-sm neighbor

NOTE This command is only supported by Layer 3 switches.

Use **show ip pim-sm neighbor** command to display PIM-SM neighbor information.

Commands

show ip pim-sm neighbor

Syntax Description	show	Show running system information
	ip	Display IP information
	pim-sm	Display PIM-SM information
	neighbor	PIM-SM neighbor information
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>ICS-G7852A-4XG# show ip pim-sm neighbor PIM Neighbor Table Index Neighbor Address Interface Uptime Expire ----- 1 172.100.1.4 V100 89 --- 2 172.100.1.1 V100 89 --- 3 172.200.1.3 V200 75 ---</pre>	
Error messages	N/A	
Related commands	<pre>ip pim-sm no ip pim-sm ip pim-sm dr-priority ip pim-sm hello-interval ip pim-sm join-prune-interval</pre>	

show ip pim-sm routing

NOTE This command is only supported by Layer 3 switches.

Use **show ip pim-sm routing** command to display current PIM-SM routing table entries.

Commands

show ip pim-sm

Syntax Description	show	Show running system information
	ip	Display IP information
	pim-sm	Display PIM-SM information
	routing	Display routing entries
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>ICS-G7852A-4XG# show ip pim-sm routing PIM-SM Routing Multicast Source RP Address VID Left time Downstream Group Address Address (Second) Interface VID ===== 0.0.0.0 * 0.0.0.0 local - NULL 232.0.0.1 172.20.2.1 0.0.0.0 20 38s 100 200 10 0 232.0.0.1 * 0.0.0.0 local - NULL 232.0.0.2 172.20.2.1 0.0.0.0 20 48s 100 200 10 0</pre>	
Error messages	N/A	
Related	ip pim-sm	

commands	no ip pim-sm ip pim-sm dr-priority ip pim-sm hello-interval ip pim-sm join-prune-interval
----------	--

show ip pim-sm rp

NOTE This command is only supported by Layer 3 switches.

Use **show ip pim-sm rp** command to display PIM-SM RP information.

Commands

show ip pim-sm rp

Syntax Description	show	Show running system information
	ip	Display IP information
	pim-sm	Display PIM-SM information
	rp	PIM-SM RP information
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>ICS-G7852A-4XG# show ip pim-sm rp PIM-SM RP Set Group Address R RP Address Holdtime Priority Hash ===== 224.0.0.0/4 172.230.1.4 112 0 7331bd32 224.0.0.0/4 172.230.1.1 78 0 2a523511 224.0.0.0/4 *172.200.1.3 86 0 7d18d1eb 224.0.0.0/4 172.200.1.2 112 0 3edf2058</pre>	
Error messages	N/A	
Related commands	ip pim-sm no ip pim-sm ip pim-sm dr-priority ip pim-sm hello-interval ip pim-sm join-prune-interval	

show ip rip

Use the **show ip rip** command to display the settings of RIP.

Commands

show ip rip

Syntax Description	show	Show running system information
	ip	Display IP information
	rip	Display RIP configurations
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	

Examples	<pre>PT-7828# show ip rip RIP Protocol : Enable RIP version : V2 Distribution Connected : Enable Static : Disable OSPF : Disable RIP Enable Table Interface Name IP VID Enable ----- --- vlan2if 192.168.102.1 2 Enable</pre>
Error messages	N/A
Related commands	N/A

show ip route

Use the **show ip route** user EXEC command to display current routing table entries.

Commands

show ip route [static]

Syntax Description	show	Show running system information
	ip	Display IP information
	route	Display routing entries
	static	Static routing entries
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	PT-7828# show ip ospf neighbor	
Error messages	N/A	
Related commands	N/A	

show ip vrrp

To display a detailed status of all Virtual Router Redundancy Protocol (VRRP) virtual routers, use the **show ip vrrp** command in EXEC mode.

Commands

show ip vrrp

Commands	ip	Display IP information
	vrrp	Display VRRP information
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	

Usage Guidelines	<pre> PT-7828# show ip vrrp VRRP Enable Enable VRRP Interface Table Interface Name IP Address VID Status 1 1.1.1.1 2 Init VRRP Basic Setting VRRP Entry Enable :Enable Virtual IP :0.0.0.0 Virtual Router ID :0 Priority :100 Preemption Mode :Enable ----- Interface Name IP Address VID Status 2 2.2.2.2 3 Init VRRP Basic Setting VRRP Entry Enable :Disable Virtual IP :0.0.0.0 Virtual Router ID :0 Priority :100 Preemption Mode :Enable ----- </pre>
Examples	N/A
Error messages	N/A
Related commands	<pre> router vrrp vrrp vrrp preempt vrrp priority </pre>

show lldp

Use the **show lldp** command to display the LLDP settings and the LLDP neighbor information.

Commands

show lldp
show lldp entry

Syntax Description	show	Show running system information
	lldp	Display LLDP information
	entry	LLDP entries
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	

Examples	<pre>PT-7828# show lldp LLDP Enable : Enable Message Transmit Interval: 30 seconds PT-7828# show lldp entry Port : 23 Neighbor ID : 00:90:e8:0a:0a:0a Neighbor Port : 3 Neighbor Port Descript : 100TX,RJ45. Neighbor System : Managed Redundant Switch 00000 Port : 19 Neighbor ID : 00:90:e8:0a:0a:0a Neighbor Port : 2 Neighbor Port Descript : 100TX,RJ45. Neighbor System : Managed Redundant Switch 00000 Port : 24 Neighbor ID : 00:90:e8:0a:0a:0a Neighbor Port : 1 Neighbor Port Descript : 100TX,RJ45. Neighbor System : Managed Redundant Switch 00000</pre>
Error messages	N/A
Related commands	lldp timer lldp run

show logging

Use the **show logging** user EXEC command to display the setting of the IP filter feature.

Commands

show logging [event-log]

Syntax	logging	Display syslog information
Description	event-log	Display system event logs
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show logging Syslog server #1: Syslog server #2: 192.168.1.2, port: 514 Syslog server #3: 192.168.1.3, port: 514 PT-7828# show logging event-log Idx Boot Time or Uptime Log ----- ----- 1 337 2037/06/23, 20:46:08 192.168.127.1 admin Auth. ok 2 337 2037/06/23, 20:52:47 Authentication fail 3 338 2037/06/23, 21:51:59 Port 1-1(Trk1) link on 4 338 2037/06/23, 21:51:59 Port 1-2 link on</pre>	

	5 338 2037/06/23, 21:51:59 Port 1-5 link on
	6 338 2037/06/23, 21:52:03 Port 1-5 link off
	7 338 2037/06/23, 21:52:03 Warm start by Firmware Upgrade
	8 338 2037/06/23, 21:52:04 Port 1-5 link on
	9 338 2037/06/23, 22:03:43 192.168.127.1 admin Auth. ok
	10 338 2037/06/23, 22:04:04 192.168.127.1 admin Auth. ok
	11 338 2037/06/24, 00:02:47 Port 1-5 link off
	12 338 2037/06/24, 00:02:48 Port 1-5 link on
Error messages	N/A
Related commands	logging

show mac-address-table

Use the **show mac-address-table** user EXEC command to display MAC addresses in the MAC address table.

Commands

show mac-address-table [**static** | **learned** | **mcast**]

show mac-address-table [**interface**{ **ethernet** *module/port* | **trunk** *trunk-id* }]

Syntax Description	mac-address-table	Display MAC address forwarding table
	static	Retrieve static MAC addresses
	learned	Retrieve learned MAC addresses
	mcast	Retrieve Multicast address
	interface	Retrieve MAC address by interface
	ethernet	Ethernet Port interface
	<i>module/port</i>	Port ID. E.g., 1/3, 2/1,...
	trunk	Trunk interface
	<i>trunk-id</i>	Trunk ID. From 1 to 4
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show mac-address-table Line Swap Fast Recovery : Enabled MAC Type VLAN Port ----- 00-40-F4-8D-0D-F7 ucast(1) 1 1/5 PT-7828# show mac-address-table learned MAC Type VLAN Port ----- 00-40-F4-8D-0D-F7 ucast(1) 1 1/5</pre>	
Error messages	N/A	
Related commands	N/A	

show mac-address-table aging-time

Use the **show mac-address-table aging-time** user EXEC command to display the aging time setting of the MAC address table.

Commands

show mac-address-table aging-time

Syntax Description	mac-address-table	Display MAC address forwarding table
	aging-time	MAC entry aging time
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show mac-address-table aging-time - MAC entry aging time PT-7828# show mac-address-table aging-time MAC address aging time: 300 sec</pre>	
Error messages	N/A	
Related commands	mac-address-table aging-time	

show mcast-filter

Use the **show mcast-filter** user EXEC command to display the multicast filter configuration.

Commands

show mcast-filter [module/port]

Commands	mcast-filter	Multicast Filtering Behavior
	Module/port	Port(Trunk) ID or list. E.g., 1/1,2,4-5,2/1,Trk1,Trk2-Trk4
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	<pre>PT-7828# show mcast-filter Port Multicast Filtering Behavior ----- 1-1 Forward All 1-2 Forward Unknown 1-3 Filter Unknown</pre>	
Examples	N/A	
Error messages	N/A	
Related commands	mcast-filter	

show modbus

Use the **show modbus** user EXEC command to display Modbus configuration.

Commands

show modbus

Syntax Description	modbus	Display Modbus configuration
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	PT-7828# show modbus Modbus enable	
Examples	N/A	
Error messages	N/A	
Related commands	modbus	

show port monitor

Use the **show port monitor** EXEC command to display the port mirror settings.

Commands

show port monitor

Syntax Description	show	Show running system information
	port	Display Port configuration
	monitor	Display Port mirror configuration
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show port monitor Port Being Monitored Direction Mirror Port ----- 1-1 1-2 both 3-2 PT-7828#</pre>	
Error messages	N/A	
Related commands	monitor	

show port-security

To check the port access control table, use the **show port-security** command.

Commands

show port-security [module/port]

Commands	port-security	Display port access control table
	<i>module/port</i>	Port ID or list. E.g., 1/1,2,3,2/1-3,5,...
Defaults	N/A	

Command Modes	Privileged EXEC/ User EXEC
Usage Guidelines	<pre>PT-7828# show port-security Port Index Mac Address Status ----- - 1-2 1 00-00-00-00-00-01 static lock</pre>
Examples	N/A
Error messages	N/A
Related commands	port-security

show qos

Use the **show qos** user EXEC command to display QoS related settings.

Commands

show qos [cos-to-queue | dscp-to-cos | dscp-to-queue]

Syntax Description	qos	Display QoS configuration
	cos-to-queue	CoS to traffic queue mappings
	dscp-to-cos	DSCP to CoS mappings
	dscp-to-queue	DSCP to traffic queue mappings
Defaults	N/A	
Command Modes	Privileged	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show qos Queuing Mechanism : Weighted Fair (1:2:4:8) Tos Inspection Module 1 : Disabled Module 3 : Disabled Int# CoS Inspection CoS ---- - 1/3 Enabled 3 1/4 Enabled 3 1/5 Enabled 3 1/6 Enabled 3 3/1 Enabled 3 3/2 Enabled 3 3/3 Enabled 3 3/4 Enabled 3 3/5 Enabled 3 3/6 Enabled 3 3/7 Enabled 3 3/8 Enabled 3 Trk1 Enabled 3 PT-7828# show qos cos-to-queue CoS Queue # ----- 0 Q0</pre>	

	<pre> 1 Q0 2 Q1 3 Q1 4 Q2 5 Q2 6 Q3 7 Q3 PT-7828# show qos dscp-to-cos DSCP Cos DSCP Cos DSCP Cos DSCP Cos ----- 0 0 1 0 2 0 3 0 4 0 5 0 6 0 7 0 8 1 9 1 10 1 11 1 12 1 13 1 14 1 15 1 16 2 17 2 18 2 19 2 20 2 21 2 22 2 23 2 24 3 25 3 26 3 27 3 28 3 29 3 30 3 31 3 32 4 33 4 34 4 35 4 36 4 37 4 38 4 39 4 40 5 41 5 42 5 43 5 44 5 45 5 46 5 47 5 48 6 49 6 50 6 51 6 52 6 53 6 54 6 55 6 56 7 57 7 58 7 59 7 60 7 61 7 62 7 63 7 </pre>
Error messages	N/A
Related commands	<pre> qos mode qos inspect qos mapping qos default-cos </pre>

show redundancy mst configure

Use the **show redundancy mst configure** user EXEC command to display settings of Multiple Spanning Tree (MSTP).

Commands

show redundancy mst configuration

Syntax	show	Show running system information
Description	redundancy	Display redundancy protocol status
	mst	Display multiple spanning tree settings
	configure	Display multiple spanning tree global settings
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	

Examples	PT-7828# show redundancy mst configuration MSTP global setting: Forwarding Delay: 15 Hello Time: 2 Max Hops: 20 Max Age: 20 Revision Level: 0 Region Name: MSTP
Error messages	N/A
Related commands	spanning-tree mst

show redundancy mst instance

Use the **show redundancy mst instance** user EXEC command to display Multiple Spanning Tree (MSTP) instance state information.

Commands

show redundancy mst instance *instance-id*

Syntax Description	show	Show running system information
	redundancy	Display redundancy protocol status
	mst	Display multiple spanning tree settings
	instance	Display MSTP msti status
	<i>instance-id</i>	MSTP instance ID
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show redundancy mst instance 1 MSTP msti root status: MSTI Root: --- MSTP msti 1 bridge status: Vlan Mapping: Birdge Priority: 32768 Int# Enable Prio Cost Oper Cost Edge State Role ----- -----</pre>	
Error messages	N/A	
Related commands	spanning-tree mst instance	

show redundancy spanning-tree

Use the **show redundancy spanning-tree** user EXEC command to display spanning-tree state information

Commands

show redundancy spanning-tree

Syntax	redundancy	Display redundancy protocol status
Description	spanning-tree	Display spanning tree settings
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show redundant spanning-tree Spanning tree status: Enabled Role : Root Bridge priority : 32768 Hello time : 2 sec Forwarding delay : 30 sec Max age time : 20 sec Int# Enable Edge Port Prio Cost Status ----- ----- 1/1 Disabled Auto 128 200000 -- - 1/2 Disabled Auto 128 200000 -- - 1/3 Disabled Auto 128 200000 -- - 1/4 Disabled Auto 128 200000 -- - 1/5 Disabled Auto 128 200000 -- - 1/6 Disabled Auto 128 200000 ---</pre>	
Error messages	N/A	
Related commands	spanning-tree forward-delay spanning-tree hello-time spanning-tree max-age spanning-tree priority spanning-tree spanning-tree cost spanning-tree edge-port spanning-tree priority show redundancy spanning-tree	

show redundancy turbo-chain

Use the **show redundancy turbo-chain** user EXEC command to display turbo-chain state information

Commands

show redundancy turbo-chain

Commands	redundancy	Display redundant settings
	turbo-chain	Display turbo chain status

Defaults	N/A
Command Modes	Privileged EXEC/ User EXEC
Usage Guidelines	N/A
Examples	<pre>PT-7828# show redundancy turbo-chain Role :HEAD ----- Port Role Port Number Port Status ----- Head Port 1-1 Forwarding Member Port 1-2 Forwarding</pre>
Error messages	N/A
Related commands	turbo-chain

show redundancy turbo-ring-v1

Use the **show redundancy turbo-ring-v1** user EXEC command to display Turbo Ring v1 configure and state information.

Commands

show redundancy turbo-ring-v1

Syntax Description	show	Show running system information
	redundancy	Display redundancy protocol status
	turbo-ring-v1	Display turbo ring v1 status
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show redundancy turbo-ring-v1 Turbo Ring V1 settings: Set as master: Disabled 1st port: 4-3 2nd port: 4-4 Ring Coupling: Disabled Coupling Port: 4-1 Coupling Control Port: 4-2 Turbo Ring V1 status: Master/Slave: --- Redundant Ports Status: 1st port: --- 2nd port: --- Ring Coupling Ports Status: --- Coupling Port: --- Coupling Control Port: ---</pre>	
Error messages	N/A	

Related commands	turbo-ring-v1
------------------	---------------

show redundancy turbo-ring-v2

Use the **show spanning-tree turbo-ring-v2** user EXEC command to display Turbo Ring v2 configuration and state information.

Commands

show redundancy turbo-ring-v2

Syntax	show	Show running system information
Description	redundancy	Display redundancy protocol status
	turbo-ring-v2	Display turbo ring v2 status
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show redundancy turbo-ring-v2 Turbo Ring V2 settings: Ring 1: Enabled Set as master: Disabled 1st port: 4-3 2nd port: 4-4 Ring 2: Disabled Set as master: Disabled 1st port: 4-1 2nd port: 4-2 Ring Coupling: Disabled Primary Port:4-1 Backup Port:4-2 Turbo Ring V2 status: Ring 1: Status:--- Master/Slave:--- 1st Ring Port Status:--- 2nd Ring Port Status:--- Ring 2: Status:--- Master/Slave:--- 1st Ring Port Status:--- 2nd Ring Port Status:--- Coupling: Mode:--- Coupling Port Status: ---</pre>	
Error messages	N/A	
Related commands	turbo-ring-v2	

show relay-warning

Use the **show relay-warning** command to display the Relay Warning settings.

Commands

show relay-warning config
show relay-warning status

Syntax Description	show	Show running system information		
	relay-warning	Display relay warning configuration		
	config	Relay warning configuration		
	status	Current relay warning list		
Defaults	N/A			
Command Modes	Privileged EXEC / User EXEC			
Usage Guidelines	N/A			
Examples	<pre>PT-7828# show relay-warning config System Events Setting Override Relay Warning Settings : Disable Power Input 1 failure(On->Off) : Disable Power Input 2 failure(On->Off) : Disable Turbo Ring Break : Disable --More-- Port Events Setting Traffic Traffic RX Traffic Port Link Overload Threshold(%) Duration(s) ----- 1-1 Ignore Disable 1 1 1-2 Ignore Disable 1 1 1-3 Ignore Disable 1 1 1-4 Ignore Disable 1 1 1-5 Ignore Disable 1 1 1-6 Ignore Disable 1 1 1-7 Ignore Disable 1 1 1-8 Ignore Disable 1 1 3-1 Ignore Disable 1 1 3-2 Ignore Disable 1 1 3-3 Ignore Disable 1 1 3-4 Ignore Disable 1 1 3-5 Ignore Disable 1 1 3-6 Ignore Disable 1 1 3-7 Ignore Disable 1 1</pre>			

	3-8 1 PT-7828#	Ignore	Disable	1
Error messages	N/A			
Related commands	N/A			

show running-config

Use **show running-config** to display the current running configuration of the switch.

Commands

show running-config

Syntax	show	Show running system information
Description	running-config	Current operating configuration
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show running-config Building configuration ... ! ip telnet ip http-server ip http-server auto-logout 120 ! ntp remote-server time.nist.gov ! ! vlan mode lqvlan gvrp ! snmp-server version v1-v2c snmp-server community public ro snmp-server community private rw snmp-server trap-mode trap ! lldp run lldp timer 30 ! ! dhcp-relay option82 dhcp-relay option82 remote-id-type other dhcp-relay option82 man-id 1234567890123 ! ! interface ethernet 1/1 no shutdown speed-duplex Auto no flowcontrol</pre>	

	media cable-mode auto --More--
Error messages	N/A
Related commands	show startup-config

show startup-config

Use **show startup-config** to display the system startup configuration of the switch.

Commands

show running-config

Syntax	show	Show running system information
Description	startup-config	Contents of startup configuration
Defaults	N/A	
Command Modes	Privileged EXEC / User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show startup-config Building configuration ... ! ip telnet ip http-server ip http-server auto-logout 120 ! ntp remote-server time.nist.gov ! ! vlan mode lqvlan gvrp ! snmp-server version v1-v2c snmp-server community public ro snmp-server community private rw snmp-server trap-mode trap ! lldp run lldp timer 30 ! ! dhcp-relay option82 dhcp-relay option82 remote-id-type other dhcp-relay option82 man-id 1234567890123 ! ! interface ethernet 1/1 no shutdown speed-duplex Auto no flowcontrol media cable-mode auto --More--</pre>	
Error	N/A	

messages	
Related commands	show running-config

show snmp

To check the status of Simple Network Management Protocol (SNMP) communications, use the **show snmp** command.

Commands

show snmp

Syntax Description	snmp	Display SNMP configuration
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	<pre>PT-7828# show snmp SNMP Read/Write Settings SNMP Versions : v1-v2c V1,V2c Read Community : public V1,V2c Write/Read Community : private Trap Settings 1st Trap Server IP/Name : 1st Trap Community : public 2nd Trap Server IP/Name : 2nd Trap Community : public Trap Mode Mode : Trap Private MIB information Switch Object ID : enterprise.8691.7.15</pre>	
Examples	N/A	
Error messages	N/A	
Related commands	snmp-server community snmp-server host snmp-server trap-mode snmp-server user snmp-server version	

show storm-control

Use the **show storm-control** user EXEC command to display the setting of storm protection.

Commands

show storm-control

Syntax Description	stom-control	Display storm protection settings
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show storm-control Storm Supress: Broadcast,DLF</pre>	

Error messages	N/A
Related commands	storm-control

show system

Use the **show system** command to display system identification settings.

Commands

show system

Syntax	show	Show running system information
Description	system	System hardware and software status
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show system System Information System Name : Managed Redundant Switch 09458 System Location : Xidian No. 135 6F Taiwan System Description : VIPA PT Series Maintainer Information : 8860289191230 MAC Address : 00:90:E8:1D:24:36 System Uptime : 0d0h6m46s</pre>	
Error messages	N/A	
Related commands	snmp-server description snmp-server contact snmp-server location	

show users

Use the **show users** user EXEC command to display the username/password configuration.

Commands

show users

Syntax	show	Show running system information
Description	Users	Display login user settings
Defaults	N/A	
Command Modes	Privileged EXEC/ User EXEC	
Usage Guidelines	N/A	
Examples	<pre>EDS-G516E# show users Login account information: Name Authority ----- - admin admin user user</pre>	
Error messages	N/A	

Related commands	username
------------------	----------

show vlan

Use the **show vlan** user EXEC command to display VLAN status information.

Commands

show vlan

Syntax	show	Show running system information
Description	vlan	Display VLAN status
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# show vlan vlan mode: 802.1Q vlan mgmt vlan: 1 VLAN 1: Access Ports: 1-1, 1-2, 1-3, 1-4, 1-5, 1-6, 1-7, 1-8, Trunk Ports: Hybrid PT</pre>	
Error messages	N/A	
Related commands	N/A	

show vlan config

Use the **show vlan** user EXEC command to display VLAN configuration information.

Commands

show vlan config

Syntax	show	Show running system information
Description	vlan	Display VLAN status
	config	Display VLAN configuration
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	

Examples	<pre> vlan mode: 802.1Q vlan VLAN Ports (Type) ----- ----- 1 1-1 (A), 1-2 (A), 1-3 (A), 1-4 (A), 1-5 (A), 1-6 (A), 1-7 (A), 1-8 (A), Port Trunk Native vlan Port Fixed VLAN (Tagged) Port Forbidden VLAN Port Fixed VLAN (Untagged) Current VLAN interface vid: 1, 2, </pre>
Error messages	N/A
Related commands	interface vlan

shutdown

To disable an interface, use the **shutdown** interface configuration command. To restart a disabled interface, use the **no** form of this command.

Commands

shutdown
no shutdown

Syntax Description	shutdown	Shutdown the selected interface
Defaults	None	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	<pre> PT-7828(config-if)# shutdown PT-7828(config-if)# no shutdown </pre>	
Error messages	Cannot configure on trunk member port 1/1!	
Related commands	<pre> show interfaces ethernet show interfaces trunk </pre>	

snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** global configuration command.

Commands

snmp-server community *text mode*

Syntax Description	snmp-server	Configure SNMP server
	community	SNMP community setting
	<i>text</i>	SNMP community string
	<i>mode</i>	ro rw
Defaults	Public community is ro Private community is rw	
Command Modes	Global configuration	
Usage Guidelines	Specifies read-only access. Authorized management stations are only able to retrieve MIB objects. Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects	
Examples	PT-7828(config)# snmp-server community public ro	
Error messages	SNMP community mode must be (ro rw)!!	
	The longest snmp community string length is 30!!	
Related commands	show snmp	

snmp-server contact

To set the system contact string, use the **snmp-server contact** global configuration command. To remove the contact string, use the **no** form of this command.

Commands

snmp-server contact *text*

no snmp-server contact

Syntax Description	snmp-server	Configure SNMP server
	contact	Switch maintainer contact information
	<i>text</i>	Maintainer contact information
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	“ <i>text</i> ” parameter can be set as string separated by space. Maximum string tokens are 5. Maximum length of switch maintainer contact info is 40.	
Examples	PT-7828(config)# snmp-server contact <STRING:token1> - Maintainer contact information PT-7828(config)# no snmp-server contact	
Error messages	Length of maintainer info is too long	
Related commands	show snmp	

snmp-server description

To set the system description string, use the **snmp-server description** global configuration command. To remove the description string, use the **no** form of this command.

Commands**snmp-server description** *text***no snmp-server description**

Syntax	snmp-server	Configure SNMP server
Description	description	Switch description
	<i>text</i>	Description string
Defaults	The default description is the model name.	
Command Modes	Global configuration	
Usage Guidelines	<p>“<i>text</i>” parameter can be set as string separated by space.</p> <p>Maximum string tokens are 5.</p> <p>Maximum length of switch maintainer contact info is 40.</p>	
Examples	<pre>PT-7828(config)# snmp-server description VIPA PT Series PT-7828(config)# exit PT-7828# show system System Information System Name : Managed Redundant Switch 09458 System Location : Xidian No. 135 6F Taiwan System Description : VIPA PT Series Maintainer Information : 8860289191230 MAC Address : 00:90:E8:1D:24:36 System Uptime : 0d0h6m46s</pre>	
Error messages	Length of system description is too long	
Related commands	show snmp	

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** global configuration command. To remove the specified host, use the **no** form of this command

Commands**snmp-server host** *host-addr* *community-string***no snmp-server host** [*host-addr*]

Syntax	snmp-server	Configure SNMP server
Description	host	SNMP host setting
	<i>host-addr</i>	SNMP host address
	<i>community-string</i>	SNMP Community string
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# snmp-server host 192.168.127.253 vipacli PT-7828(config)# no snmp-server host</pre>	
Error messages	Trap server are full, please remove at least one first!!!	
Related commands	show snmp	

snmp-server location

To set the system location string, use the **snmp-server location** global configuration command. To remove the location string, use the **no** form of this command.

Commands

snmp-server location *text*
no snmp-server location

Syntax Description	snmp-server	Configure SNMP server
	location	Switch location
	<i>text</i>	Location string
Defaults	The default text is Switch Location	
Command Modes	Global configuration	
Usage Guidelines	<p><i>“text”</i> parameter can be set as string separated by space. Maximum string tokens are 5. Maximum length of switch location is 80.</p>	
Examples	<pre>PT-7828(config)# snmp-server location <STRING:token1> - Location string token 1 PT-7828(config)# no snmp-server location</pre>	
Error messages	Length of location is too long	
Related commands	show snmp	

snmp-server trap-mode

To enable all Simple Network Management Protocol (SNMP) notifications (traps or informs) available on your system, use the **snmp-server trap-mode** global configuration command. To disable all available SNMP notifications, use the **no** form of this command

Commands

snmp-server trap-mode trap
snmp-server trap-mode trap-v2c
snmp-server trap-mode inform [*retry times timeout seconds*]
no snmp-server trap-mode

Syntax Description	snmp-server	Configure SNMP server
	trap-mode	SNMP Trap/Inform mode setting
	trap	SNMP Trap
	trap-v2c	SNMP Trap v2c instead of v1
	inform	SNMP Inform
	retry	Inform retries times
	<i>times</i>	1 to 99
	timeout	Timeout timer
	<i>seconds</i>	1 to 300 seconds
Defaults	The default mode is “trap”	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# snmp-server trap-mode trap PT-7828(config)# snmp-server trap-mode inform retry 3 timeout 10 PT-7828(config)# no snmp-server trap-mode</pre>	

Error messages	Invalid inform retries value !!!
	Invalid inform timeout value !!!
Related commands	show snmp

snmp-server user

To configure a user and its authentication type and password to a Simple Network Management Protocol (SNMP), use the **snmp-server user** global configuration command.

Commands

snmp-server user *username* **auth** *auth-type* *password*

Syntax Description	snmp-server	Configure SNMP server
	user	SNMP user setting
	<i>user-privilege</i>	SNMP user privilege
	auth	Specifies which authentication level should be used
	<i>auth-type</i>	no-auth md5 sha
	<i>password</i>	Password (maximum 30 characters)
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	<i>username</i> is only allowed to be set as “admin” or “user” <i>auth-type</i> is only allowed to be set as “no-auth”, “md5” or “sha”	
Examples	PT-7828(config)# snmp-server user admin auth md5 vipacli	
Error messages	SNMP user must be (admin user)!!	
	SNMP authtype must be (no-auth md5 sha)!!	
	Admin/User Password must be at least 8 bytes !!!	
	Admin/User Data Encryption must be at least 8 bytes !!!	
Related commands	show snmp	

snmp-server version

To set up the snmp version, use the **snmp-server version** global configuration command.

Commands

snmp-server version [**v1-v2c-v3** | **v1-v2c** | **v3**]

Syntax Description	snmp-server	Configure SNMP server
	version	SNMP version setting
	v1-v2c-v3	Version 1, 2C and 3 support
	v1-v2c	Version 1 and 2C support
	v3	Only version 3 support
Defaults	Default version is v1-v2c	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# snmp-server version v1-v2c-v3 - Version 1, 2C and 3 support v1-v2c - Version 1 and 2C support v3 - Only version 3 support	
Error messages	N/A	
Related commands	show snmp	

spanning-tree forward-delay

Use the **spanning-tree forward-delay** redundancy configuration command on the switch to set the forward-delay time for the spanning-tree. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. Use the **no** form of this command to return to the default setting.

Commands

spanning-tree forward-delay *seconds*

no spanning-tree forward-delay

Syntax	spanning-tree	Configure spanning tree
Description	forward-delay	Configure spanning tree BPDU forward delay
	<i>seconds</i>	Range from 4 to 30 seconds
Defaults	Forward delay = 15 sec.	
Command Modes	Redundancy configuration	
Usage Guidelines	$2 * (\text{hello-time} + 1.0 \text{ sec}) \leq \text{max-age} \leq 2 * (\text{forward-delay} - 1.0 \text{ sec})$	
Examples	PT-7828(config-rdnt)# spanning-tree forward-delay <UINT:seconds> - Range from 4 to 30 seconds	
Error messages	The BPDU forward delay time must be in the range from 4 to 30 sec.	
	The formula must be obeyed: $2 * (\text{Hello Time} + 1 \text{ sec}) \leq \text{Max age} \leq 2 * (\text{Forward Delay} - 1 \text{ sec})$	
Related commands	spanning-tree hello-time spanning-tree max-age show redundancy spanning-tree	

spanning-tree hello-time

Use the **spanning-tree hello-time** redundancy configuration command on the switch to set the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages. Use the **no** form of this command to return to the default setting.

Commands

spanning-tree hello-time *seconds*

no spanning-tree hello-time

Syntax	spanning-tree	Configure spanning tree
Description	hello-time	Configure spanning tree BPDU hello time
	<i>seconds</i>	Range from 1 to 2 seconds
Defaults	Hello time = 2 sec.	
Command Modes	Redundancy configuration	
Usage Guidelines	$2 * (\text{hello-time} + 1.0 \text{ sec}) \leq \text{max-age} \leq 2 * (\text{forward-delay} - 1.0 \text{ sec})$	
Examples	PT-7828(config-rdnt)# spanning-tree hello-time <UINT:seconds> - Range from 1 to 2 seconds	
Error messages	BPDU hello time must be in the range from 1 to 2 sec.	
	The formula must be obeyed: $2 * (\text{Hello Time} + 1 \text{ sec}) \leq \text{Max age} \leq 2 * (\text{Forward Delay} - 1 \text{ sec})$	
Related commands	spanning-tree forward-delay spanning-tree max-age show redundancy spanning-tree	

spanning-tree max-age

Use the **spanning-tree max-age** redundancy configuration command on the switch to set the interval between messages that the spanning tree receives from the root switch. If a switch does not receive a

bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputes the spanning-tree topology. Use the **no** form of this command to return to the default setting.

Commands

spanning-tree max-age *seconds*
no spanning-tree max-age

Syntax Description	spanning-tree	Configure spanning tree
	max-age	Configure spanning tree max age
	<i>seconds</i>	Range from 6 to 40 seconds
Defaults	Forward delay = 20 sec.	
Command Modes	Redundancy configuration	
Usage Guidelines	$2 * (\text{hello-time} + 1.0 \text{ sec}) \leq \text{max-age} \leq 2 * (\text{forward-delay} - 1.0 \text{ sec})$	
Examples	PT-7828(config-rdnt)# spanning-tree max-age <UINT:seconds> - Range from 6 to 40 seconds	
Error messages	The BPDU forward delay time must be in the range from 4 to 30 sec.	
	The formula must be obeyed: $2 \times (\text{Hello Time} + 1 \text{ sec}) \leq \text{Max age} \leq 2 \times (\text{Forward Delay} - 1 \text{ sec})$	
Related commands	spanning-tree forward-delay spanning-tree max-age show redundancy spanning-tree	

spanning-tree mst cist cost

Use the **spanning-tree mst cist cost** interface configuration command on the switch to set the port cost of the Multiple Spanning Tree (MSTP). Use the **no** form of this command to return to the default setting.

Commands

spanning-tree mst cist cost *cost*
no spanning-tree mst cist cost

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	cist	Configure mstp cist port
	cost	Configure mstp cist port path cost
	<i>cost</i>	Configure mstp cist port path cost
Defaults	<i>cost=0</i>	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-if)# spanning-tree mst cist cost 2000000 <UINT:time> - Set mstp forwarding delay	
Error messages	MSTP port path cost must be in the range from 0 to 200000000	
	MSTP port 2/1 path cost set error	
Related commands	show redundancy mst configuration	

spanning-tree mst cist port-priority

Use the **spanning-tree mst cist port-priority** interface configuration command on the switch to set the port priority for the Multiple Spanning Tree (MSTP). Use the **no** form of this command to return to the default setting.

Commands

spanning-tree mst cist port-priority *priority*
no spanning-tree mst cist port-priority

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	cist	Configure mstp cist port
	port-priority	Configure mstp cist port priority
	<i>priority</i>	Configure mstp cist port priority
Defaults	<i>priority = 128</i>	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config-if)# spanning-tree mst cist port-priority 128 <UINT:priority> - Configure mstp cist port priority</pre>	
Error messages	MSTP port priority must be in the range from 0 to 240	
	MSTP port %s priority set error	
	MSTP port priority should be 16 times the value	
Related commands	show redundancy mst configuration	

spanning-tree mst cist priority

Use the **spanning-tree mst cist priority** redundancy configuration command on the switch to set the switch priority for the Multiple Spanning Tree (MSTP). Use the **no** form of this command to return to the default setting.

Commands

spanning-tree mst cist priority *priority*
no spanning-tree mst cist priority

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	cist	Configure mstp cist
	priority	Set mstp cist bridge priority
	<i>priority</i>	Set mstp cist bridge priority
Defaults	<i>priority = 32768</i>	
Command Modes	Redundancy configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config-rdnt)# spanning-tree mst cist priority 32768 <UINT:priority> - Set mstp cist bridge priority</pre>	
Error messages	MSTP bridge priority must be in the range from 0 to 61140	
	MSTP cist bridge priority set error	
	CIST bridge priority should be 4096 times the value	
Related commands	show redundancy mst cist	

spanning-tree mst edge-port

Use the **spanning-tree mst edge-port** interface configuration command on the switch to enable the Edge port feature for the Multiple Spanning Tree (MSTP). Use the **no** form of this command to disable the setting.

Commands

spanning-tree mst edge-port
no spanning-tree mst edge-port

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	edge-port	Enable mstp edge port
Defaults	N/A	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-if)# spanning-tree mst edge <edge> - Enable mstp edge port	
Error messages	MSTP edge port enable set error	
Related commands	show redundancy mst configuration	

spanning-tree mst enable

Use the **spanning-tree mst enable** interface configuration command on the switch to enable the Multiple Spanning Tree (MSTP) feature on the port. Use the **no** form of this command to disable the setting.

Commands

spanning-tree mst enable
no spanning-tree mst

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	enable	Enable mstp port
Defaults	N/A	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-if)# spanning-tree mst enable <enable> - Enable mstp port	
Error messages	MSTP port 2-1 enable set error	
Related commands	show redundancy mst configuration	

spanning-tree mst forward-time

Use the **spanning-tree mst forward-time** redundancy configuration command on the switch to set the forward delay of Multiple Spanning Tree (MSTP). Use the **no** form of this command to return to the default setting.

Commands

spanning-tree mst forward-time time
no spanning-tree mst forward-time

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	forward-time	Set mstp forwarding delay
	<i>time</i>	Set mstp forwarding delay
Defaults	<i>time=15</i>	
Command Modes	Redundancy configuration	

Usage Guidelines	$2 * (\text{hello-time} + 1.0 \text{ sec}) \leq \text{max-age} \leq 2 * (\text{forward-delay} - 1.0 \text{ sec})$
Examples	PT-7828(config-rdnt)# spanning-tree mst forward-time 15 <UINT:time> - Set mstp forwarding delay
Error messages	MSTP forward delay must be in the range from 4 to 30 MSTP forward delay set error
Related commands	show redundancy mst configuration

spanning-tree mst hello-time

Use the **spanning-tree priority** redundancy configuration command on the switch to set the hello time of Multiple Spanning Tree (MSTP). Use the **no** form of this command to return to the default setting.

Commands

spanning-tree mst hello-time time
no spanning-tree mst hello-time

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	hello-time	set mstp hello time
	<i>time</i>	set mstp hello time
Defaults	<i>time=2</i>	
Command Modes	Redundancy configuration	
Usage Guidelines	$2 * (\text{hello-time} + 1.0 \text{ sec}) \leq \text{max-age} \leq 2 * (\text{forward-delay} - 1.0 \text{ sec})$	
Examples	PT-7828(config-rdnt)# spanning-tree mst hello-time 1 <UINT:time> - set mstp hello time	
Error messages	MSTP hello time must be in the range from 1 to 10 MSTP hello time set error	
Related commands	show redundancy mst configuration	

spanning-tree mst instance

Use the **spanning-tree mst instance** redundancy configuration command on the switch to setting the MSTP instances. Use the **no** form of this command to remove the setting.

Commands

spanning-tree mst instance instance-id **vlan** vlan-id-list
no spanning-tree mst instance instance-id **vlan** vlan-id-list

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	Instance	Configure mstp msti
	<i>instance-id</i>	MSTP instance ID
	vlan	Configure mstp msti vlan mapping
	<i>vlan-id-list</i>	Configure mstp msti vlan mapping
Defaults	N/A	
Command Modes	Redundancy configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# spanning-tree mst instance 1 vlan 2 <STRING:instids> - Configure mstp msti <STRING:vidlist> - Configure mstp msti vlan mapping	

Error messages	The instance id must be in the range from 1 to 16.
	vlan 4097 is invalid!! should be range from 1 to 4094
	The maximum VLAN mapping is 64.
	The vlan id 2 setting is exist in another instance.
	MSTI 1 vlan id 2 set error
Related commands	show redundancy mst instance

spanning-tree mst instance cost

Use the **spanning-tree mst instance cost** interface configuration command on the switch to set the port cost of the MSTP instances. Use the **no** form of this command to return to the default setting.

Commands

spanning-tree mst instance *instance-id-list* **cost** *cost*

no spanning-tree mst instance *instance-id-list* **cost**

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	instance	Configure mstp msti port
	<i>instance-id-list</i>	MSTP instance IDs
	cost	Configure mstp msti port path cost
	<i>cost</i>	Configure mstp msti port path cost
Defaults	<i>cost</i> =0	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-if)# spanning-tree mst cist cost 0 <UINT:cost> - Configure mstp msti port path cost	
Error messages	MSTP port path cost must be in the range from 0 to 200000000	
	MSTP forward delay set error	
Related commands	show redundancy mst configuration	

spanning-tree mst instance port-priority

Use the **spanning-tree mst instance port-priority** interface configuration command on the switch to set the port priority for the MSTP instances. Use the **no** form of this command to return to the default setting.

Commands

spanning-tree mst instance *instance-id-list* **port-priority** *priority*

no spanning-tree mst instance *instance-id-list* **port-priority**

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	instance	Configure mstp msti port
	<i>instance-id-list</i>	MSTP instance ID
	port-priority	Configure mstp msti port priority
	<i>priority</i>	Configure mstp msti port priority
Defaults	<i>priority</i> =128	
Command Modes	Interface configuration	
Usage Guidelines	N/A	

Examples	PT-7828 (config-if)# spanning-tree mst instance 1 port-priority 128 <STRING:instids> - Configure mstp msti port priority <UINT:priority> - Configure mstp msti port priority
Error messages	MSTP port priority must be in the range from 0 to 240
	MSTI 2 port 2-1 priority set error MSTI 2 port priority should be 16 times the value
Related commands	show redundancy mst configuration

spanning-tree mst instance priority

Use the **spanning-tree mst instance priority** redundancy configuration command on the switch to set the switch priority for the MSTP instances. Use the **no** form of this command to return to the default setting.

Commands

spanning-tree mst instance *instance-id-list* **priority** *priority*
no spanning-tree mst instance *instance-id-list* **priority**

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	instance	Configure mstp msti
	<i>instance-id</i>	MSTP instance ID
	priority	Set mstp msti bridge priority
	<i>priority</i>	Set mstp msti bridge priority
Defaults	priority = 32768	
Command Modes	Redundancy configuration	
Usage Guidelines	N/A	
Examples	PT-7828 (config-rdnt)# spanning-tree mst instance 1 priority 32768 <UINT:priority> - Set mstp msti bridge priority	
Error messages	MSTP bridge priority must be in the range from 0 to 61140	
	MSTP cist bridge priority set error MSTI bridge priority should be 4096 times the value	
Related commands	show redundancy mst instance	

spanning-tree mst max-age

Use the **spanning-tree mst max-age** redundancy configuration command on the switch to set the switch maximum age time for Multiple Spanning Tree (MSTP). Use the **no** form of this command to return to the default setting.

Commands

spanning-tree mst max-age *age*
no spanning-tree mst max-age

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	max-age	Set mstp max age
	<i>age</i>	Set mstp max age
Defaults	<i>age=20</i>	

Command Modes	Redundancy configuration
Usage Guidelines	$2 * (\text{hello-time} + 1.0 \text{ sec}) \leq \text{max-age} \leq 2 * (\text{forward-delay} - 1.0 \text{ sec})$
Examples	PT-7828(config-rdnt)# spanning-tree mst max-age 10 <UINT:age> - Set mstp max age
Error messages	MSTP max age must be in the range from 6 to 40 MSTP max age set error
Related commands	show redundancy mst configuration

spanning-tree mst max-hops

Use the **spanning-tree mst max-hops** redundancy configuration command on the switch to set the switch maximum hop number for Multiple Spanning Tree (MSTP). Use the **no** form of this command to return to the default setting.

Commands

spanning-tree mst max-hops hops
no spanning-tree mst max-hops

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	max-hops	Set mstp max hops
	hops	Set mstp max hops
Defaults	hops=20	
Command Modes	Redundancy configuration	
Usage Guidelines	$2 * (\text{hello-time} + 1.0 \text{ sec}) \leq \text{max-age} \leq 2 * (\text{forward-delay} - 1.0 \text{ sec})$	
Examples	PT-7828(config-rdnt)# spanning-tree mst max-hops 10 <UINT:hops> - Set mstp max hops	
Error messages	MSTP max hops must be in the range from 6 to 40 MSTP max hops set error	
Related commands	show redundancy mst configuration	

spanning-tree mst name

Use the **spanning-tree mst name** redundancy configuration command on the switch stack to set the name of MSTP region for the spanning-tree.

Commands

spanning-tree mst name region-name

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	name	Set mstp regional name
	region-name	Set mstp regional name
Defaults	N/A	
Command Modes	Redundancy configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-rdnt)# spanning-tree mst name mstp <STRING:region> - Set mstp regional name	
Error messages	The length of mstp regional name should be smaller than 32 MSTP regional name set error	

Related commands	show redundancy mst instance
------------------	------------------------------

spanning-tree mst revision

Use the **spanning-tree mst revision** redundancy configuration command on the switch to set revision level for Multiple Spanning Tree (MSTP).

Commands

spanning-tree mst revision *revision-level*

Syntax Description	spanning-tree	Configure spanning tree
	mst	Configure mstp
	revision	Set mstp revision level
	<i>revision-level</i>	Set mstp revision level
Defaults	<i>revision-level=0</i>	
Command Modes	Redundancy configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-rdnt)# spanning-tree mst revision 1 <UINT:level> - Set mstp revision level	
Error messages	MSTP revision level must be in the range from 0 to 65535	
	MSTP revision level set error	
Related commands	show redundancy mst configuration	

spanning-tree priority

Use the **spanning-tree priority** redundancy configuration command on the switch to set the switch priority for the spanning-tree. Use the **no** form of this command to return to the default setting.

Commands

spanning-tree priority *priority*

no spanning-tree priority

Syntax Description	spanning-tree	Configure spanning tree
	priority	Configure spanning tree bridge priority
	<i>priority</i>	Range from 0 to 61440, and must be the multiples of 4096
Defaults	priority = 32768	
Command Modes	Redundancy configuration	
Usage Guidelines	0 <= priority <= 61440, and must be multiples of 4096.	
Examples	PT-7828(config-rdnt)# spanning-tree priority <UINT:prio> - Range from 0 to 61440, in steps of 4096	
Error messages	The bridge priority must be in the range from 0 to 61440	
	The bridge priority must be the multiples of 4096	
Related commands	show redundancy spanning-tree	

spanning-tree

Use the **spanning-tree** interface configuration command on the switch to enable the spanning-tree feature of the specified interfaces. Use the **no** form of this command to disable it.

Commands

spanning-tree
no spanning-tree

Syntax Description	spanning-tree	Enable spanning tree
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-if)# spanning-tree	
Error messages	Cannot configure on trunk member port 1/1!	
Related commands	redundancy mode show redundancy spanning-tree	

spanning-tree cost

Use the **spanning-tree cost** interface configuration command on the switch to set the path cost for spanning-tree algorithms calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

Commands

spanning-tree cost cost
no spanning-tree cost

Syntax Description	spanning-tree	Enable spanning tree
	cost	Configure port path cost
	<i>cost</i>	Range from 1 to 200000000
Defaults	cost = 200000	
Command Modes	Interface configuration	
Usage Guidelines	1 <= Cost <= 200000000	
Examples	PT-7828(config-if)# spanning-tree cost <UINT:cost> - Range from 1 to 200000000	
Error messages	Cost value must be in the range 1 to 200000000	
	Cannot configure on trunk member port 1/1!	
Related commands	show redundancy spanning-tree	

spanning-tree edge-port

Use the **spanning-tree edge-port** interface configuration command on the switch to enable the Edge Port feature on an interface in all its associated VLANs. When the Edge Port feature is enabled, the interface changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes. Use the **no** form of this command to disable the feature.

Commands

spanning-tree edge-port { auto | force }
no spanning-tree edge-port

Syntax Description	spanning-tree	Enable spanning tree
	edge-port	Configure as edge port
	auto	Auto determine as edge port
	force	Force the port as edge port
Defaults	port-fast = auto	
Command Modes	Interface configuration	

Usage Guidelines	N/A
Examples	PT-7828(config-if)# spanning-tree edge-port auto - Auto determine as edge port force - Force the port as edge port
Error messages	Cannot configure on trunk member port 1/1!
Related commands	show redundancy spanning-tree

spanning-tree priority

Use the **spanning-tree priority** interface configuration command on the switch to set the interfaces priority for the spanning-tree. Use the **no** form of this command to return to the default setting.

Commands

spanning-tree priority priority
no spanning-tree priority

Syntax Description	spanning-tree	Enable spanning tree
	priority	Configure port priority
	priority	Range from 0 to 240, in steps of 16
Defaults	priority = 128	
Command Modes	interface configuration	
Usage Guidelines	0 <= priority <= 240, and must be multiples of 16.	
Examples	PT-7828(config-rdnt)# spanning-tree priority <UINT:prio> - Range from 0 to 61440, in steps of 4096	
Error messages	The bridge priority must be in the range from 0 to 240	
	The bridge priority must be multiples of 16	
Related commands	show redundancy spanning-tree	

speed-duplex

Use the **speed-duplex** interface configuration command to specify the speed of the interface and its duplex mode. Use the **no** form of this command to return the interface to its default value.

Commands

speed-duplex {10M-Full | 10M-Half | 100M-Full | 100M-Half | 1G-Full | Auto}
no speed-duplex

Syntax Description	speed-duplex	Configure speed and duplex operation
	10M-Full	Speed 10M-full
	10M-Half	Speed 10M-Half
	100M-Full	Speed 100M-Full
	100M-Half	Speed 100M-Half
	1G-Full	Speed 1G-Full
	Auto	Speed Auto
Defaults	The default is Auto	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# interface ethernet 1/1 PT-7828(config-if)# speed-duplex 100M-Full	

Error messages	Fiber port can not be set speed-duplex!!!
	This port can not be set to 1G!!!
	Parameter does not be defined!!!
	Cannot configure on trunk member port 1/1
	This setting cannot be applied on trunk port!
Related commands	show interfaces ethernet

storm-control

Use the **storm-control** global configuration command on the switch to enable the storm protection. Use the **no** form of this command to disable it or return to the default.

Commands

```
storm-control { bcast | mcast }
no storm-control bcast
no storm-control mcast
no storm-control
```

Syntax	storm-control	Storm protection
Description	bcast	Storm protection for broadcast traffic
	mcast	Storm protection for Multicast traffic
Defaults	The broadcast storm protection is default enabled.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>storm-control bcast - Storm protection for broadcast traffic mcast - Storm protection for Multicast traffic</pre>	
Error messages	N/A	
Related commands	show storm-control	

switchport access vlan

Use the **switchport access vlan** interface configuration command on the switch to configure a port as a static-access or dynamic-access port. If the switchport mode is set to access, the port operates as a member of the specified VLAN. If set to dynamic, the port starts discovery of VLAN assignment based on the incoming packets it receives. Use the **no** form of this command to reset the access mode to the default VLAN for the switch.

Commands

```
switchport access vlan vlan-id
no switchport access vlan
```

Syntax Description	switchport	Set switching mode characteristics
	access	Set access mode characteristics of the interface
	vlan	Set (default) pvid in access mode
	<i>vlan-id</i>	1 to 4094
Defaults	<i>vlan-id</i> = 1	
Command Modes	Interface configuration	
Usage Guidelines	You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 4094.	

Examples	PT-7828 (config-if)# switchport access vlan 2 <UINT:vlanid> - 1 to 4094
Error messages	vlan 4097 is invalid!! should be range from 1 to 4094
Related commands	show vlan show vlan config

switchport hybrid fixed vlan add

Use the **switchport hybrid fixed vlan add** interface configuration command on the switch to add the trunk hybrid characteristics when the interface is in hybrid mode. Use the **no** form of this command to reset to the default.

Commands

switchport hybrid fixed vlan add *vlan-id-list* **tag**
switchport hybrid fixed vlan add *vlan-id-list* **untag**
no switchport hybrid fixed vlan tag
no switchport hybrid fixed vlan untag

Syntax Description	switchport	Set switching mode characteristics
	hybrid	Set hybrid mode characteristics of the interface
	fixed	Set fixed VLAN characteristics
	vlan	1 to 4094
	add	Add VLANs to the current list
	<i>vlan-id-list</i>	VLAN IDs of the VLANs
	untag	Configure egress traffic as VLAN untagged traffic
	tag	Configure egress traffic as VLAN tagged traffic
Defaults	N/A	
Command Modes	Interface configuration	
Usage Guidelines	You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 4094.	
Examples	PT-7828 (config-if)# switchport hybrid fixed vlan add 1,3-5,7 tag <STRING:vlanids> - VLAN IDs of the VLANs	
Error messages	vlan 4097 is invalid!! should be range from 1 to 4094 vlan interfaces are full, total vlan interface is 64 !!	
Related commands	show vlan show vlan config switchport trunk hybrid vlan remove	

switchport hybrid forbidden vlan add

Use the **switchport hybrid forbidden vlan add** interface configuration command on the switch to add the trunk forbidden characteristics when the interface is in hybrid mode. Use the **no** form of this command to reset to the default.

Commands

switchport hybrid forbidden vlan add *vlan-id-list*
no switchport hybrid forbidden vlan

Syntax Description	switchport	Set switching mode characteristics
	hybrid	Set hybrid mode characteristics of the interface
	forbidden	Set forbidden VLAN characteristics
	vlan	1 to 4094
	add	Add VLANs to the current list
	<i>vlan-id-list</i>	VLAN IDs of the VLANs
Defaults	N/A	

Command Modes	Interface configuration
Usage Guidelines	You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 4094.
Examples	PT-7828(config-if)# switchport hybrid forbidden vlan add 1,3-5,7 <STRING:vlanids> - VLAN IDs of the VLANs
Error messages	vlan 4097 is invalid!! should be range from 1 to 4094 vlan interfaces are full, total vlan interface is 64 !!
Related commands	show vlan show vlan config switchport hybrid forbidden vlan remove

switchport hybrid forbidden vlan remove

Use the **switchport hybrid forbidden vlan add** interface configuration command on the switch to remove the trunk forbidden characteristics when the interface is in hybrid mode. Use the **no** form of this command to reset to the default.

Commands

switchport hybrid forbidden vlan remove *vlan-id-list*
no switchport hybrid forbidden vlan

Syntax Description	switchport	Set switching mode characteristics
	hybrid	Set hybrid mode characteristics of the interface
	forbidden	Set forbidden VLAN characteristics
	vlan	1 to 4094
	remove	Remove VLANs from the current list
	<i>vlan-id-list</i>	VLAN IDs of the VLANs
Defaults	N/A	
Command Modes	Interface configuration	
Usage Guidelines	You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 4094.	
Examples	PT-7828(config-if)# switchport hybrid forbidden vlan remove 1,3-5,7 <STRING:vlanids> - VLAN IDs of the VLANs	
Error messages	vlan 4097 is invalid!! should be range from 1 to 4094 vlan interfaces are full, total vlan interface is 64 !!	
Related commands	show vlan show vlan config switchport hybrid forbidden vlan add	

switchport hybrid native vlan

Use the **switchport hybrid native vlan** interface configuration command on the switch to configure PVID of a port. Use the **no** form of this command to return to the default PVID.

Commands

switchport hybrid native vlan *vlan-id*
no switchport hybrid native vlan

Syntax Description	switchport	Set switching mode characteristics
	hybrid	Set hybrid mode characteristics of the interface
	native	Set trunking native characteristics
	vlan	Set pvid vlanid in hybrid mode
	<i>vlan-id</i>	1 to 4094
Defaults	vlan-id = 1	

Command Modes	Interface configuration
Usage Guidelines	You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 4094.
Examples	PT-7828(config-if)# switchport hybrid native vlan 2 <UINT:vlanid> - 1 to 4094
Error messages	vlan 4097 is invalid!! should be range from 1 to 4094
Related commands	show vlan show vlan config

switchport pvlan

Use the **switchport pvlan** interface configuration command on the switch stack to define a port-based VLAN association for an isolated or community port or a mapping for a promiscuous port. Use the **no** form of this command to remove the port-based VLAN association or mapping from the port.

Commands

switchport pvlan *vlan-groups*

no switchport pvlan *vlan-groups*

Syntax Description	switchport	Set switching mode characteristics
	pvlan	Configure port-based vlan
	<i>vlan-groups</i>	Set/unset port-based vlan group
Defaults	N/A	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-if)# switchport pvlan 2,3,4 <STRING:groups> - set port-based vlan group	
Error messages	vlan 4097 is invalid!! should be range from 1 to 4094	
Related commands	show vlan show vlan config	

switchport trunk fixed vlan add

Use the **switchport trunk fixed vlan add** interface configuration command on the switch to add the trunk characteristics when the interface is in trunking mode. Use the **no** form of this command to reset a trunking characteristic to the default.

Commands

switchport trunk fixed vlan add *vlan-id-list*

no switchport trunk fixed vlan

Syntax Description	switchport	Set switching mode characteristics
	trunk	Set trunking mode characteristics of the interface
	fixed	Set fixed VLAN characteristics
	vlan	1 to 4094
	add	Add VLANs to the current list
	<i>vlan-id-list</i>	VLAN IDs of the VLANs
Defaults	N/A	
Command Modes	Interface configuration	
Usage Guidelines	You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 4094.	

Examples	PT-7828(config-if)# switchport trunk fixed vlan add 1,3-5,7 <STRING:vlanids> - VLAN IDs of the VLANs
Error messages	vlan 4097 is invalid!! should be range from 1 to 4094 vlan interfaces are full, total vlan interface is 64 !!
Related commands	show vlan show vlan config switchport trunk fixed vlan remove

switchport trunk fixed vlan remove

Use the **switchport trunk fixed vlan add** configuration command on the switch stack to remove the trunk characteristics when the interface is in trunking mode. Use the **no** form of this command to reset a trunking characteristic to the default.

Commands

switchport trunk fixed vlan remove *vlan-id-list*
no switchport trunk fixed vlan

Syntax Description	switchport	Set switching mode characteristics
	trunk	Set trunking mode characteristics of the interface
	fixed	Set fixed VLAN characteristics
	vlan	1 to 4094
	remove	Remove VLANs from the current list
	<i>vlan-id-list</i>	VLAN IDs of the VLANs
Defaults	N/A	
Command Modes	Interface configuration	
Usage Guidelines	You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 4094.	
Examples	PT-7828(config-if)# switchport trunk fixed vlan remove 1,3-5,7 <STRING:vlanids> - VLAN IDs of the VLANs	
Error messages	vlan 4097 is invalid!! should be range from 1 to 4094 vlan interfaces are full, total vlan interface is 64 !!	
Related commands	show vlan show vlan config switchport trunk fixed vlan add	

switchport trunk forbidden vlan add

Use the **switchport trunk forbidden vlan add** configuration command on the switch to add the trunk forbidden characteristics when the interface is in trunking mode. Use the **no** form of this command to reset a trunking characteristic to the default.

Commands

switchport trunk forbidden vlan add *vlan-id-list*
no switchport trunk forbidden vlan

Syntax Description	switchport	Set switching mode characteristics
	trunk	Set trunking mode characteristics of the interface
	forbidden	Set forbidden VLAN characteristics
	vlan	1 to 4094
	add	Add VLANs to the current list
	<i>vlan-id-list</i>	VLAN IDs of the VLANs
Defaults	N/A	
Command Modes	Interface configuration	

Usage Guidelines	You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 4094.
Examples	PT-7828(config-if)# switchport trunk forbidden vlan add 1,3-5,7 <STRING:vlanids> - VLAN IDs of the VLANs
Error messages	vlan 4097 is invalid!! should be range from 1 to 4094 vlan interfaces are full, total vlan interface is 64 !!
Related commands	show vlan show vlan config switchport trunk forbidden vlan remove

switchport trunk forbidden vlan remove

Use the **switchport trunk forbidden vlan remove** configuration command on the switch stack or on a standalone switch to remove the trunk forbidden characteristics when the interface is in trunking mode. Use the **no** form of this command to reset a trunking characteristic to the default.

Commands

switchport trunk forbidden vlan remove *vlan-id-list*
no switchport trunk forbidden vlan

Syntax Description	switchport	Set switching mode characteristics
	trunk	Set trunking mode characteristics of the interface
	forbidden	Set forbidden VLAN characteristics
	vlan	1 to 4094
	remove	Remove VLANs from the current list
	<i>vlan-id-list</i>	VLAN IDs of the VLANs
Defaults	N/A	
Command Modes	Interface configuration	
Usage Guidelines	You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 4094.	
Examples	PT-7828(config-if)# switchport trunk forbidden vlan remove 1,3-5,7 <STRING:vlanids> - VLAN IDs of the VLANs	
Error messages	vlan 4097 is invalid!! should be range from 1 to 4094 vlan interfaces are full, total vlan interface is 64 !!	
Related commands	show vlan show vlan config switchport trunk forbidden vlan add	

switchport trunk native vlan

Use the **switchport trunk native vlan** interface configuration command on the switch to configure PVID of a port as a trunking port. Use the **no** form of this command to return to the default.

Commands

switchport trunk native vlan *vlan-id*
no switchport trunk native vlan

Syntax Description	switchport	Set switching mode characteristics
	trunk	Set trunking mode characteristics of the interface
	native	Set trunking native characteristics
	vlan	Set pvid vlanid in trunk mode
	<i>vlan-id</i>	1 to 4094
Defaults	vlan-id = 1	
Command Modes	Interface configuration	

Usage Guidelines	You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 4094.
Examples	PT-7828(config-if)# switchport trunk native vlan 2 <UINT:vlanid> - 1 to 4094
Error messages	vlan 4097 is invalid!! should be range from 1 to 4094
Related commands	show vlan show vlan config

trunk-group

Use the **trunk-group** interface configuration command on the switch to assign an Ethernet port to a trunk group. Use the **no** form of this command to remove an Ethernet port from a trunk group.

Commands

trunk-group *trunk_id*
no trunk-group

Syntax	trunk-group	Join trunk group as members
Description	<i>trunk_id</i>	Trunk ID. From 1 to 4
Defaults	N/A	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-if)# trunk-group <UINT:trunk id> - Trunk ID. From 1 to 4	
Error messages	This setting cannot be applied on trunk port! Trunk ID is only allowed from 1 to 4	
Related commands	show interfaces trunk	

trunk-mode

Use the **trunk-mode** interface configuration command on the switch to set the trunk mode of the specified trunk group. Use the **no** form of this command to return to the default setting.

Commands

trunk-mode { **static** | **lACP** }
no trunk-mode

Syntax	trunk-mode	Trunk mode configuration
Description	static	Configure as static trunk
	lACP	Configure as LACP trunk
Defaults	The default trunk mode of creating trunk manually is static.	
Command Modes	Interface configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-if)# trunk-mode static - Configure as static trunk lACP - Configure as LACP trunk	
Error messages	This setting cannot be applied on normal port!	
Related commands	show interfaces trunk	

turbo-chain

Use the **turbo-chain** redundancy configuration command on the switch stack or on a standalone switch to configure Turbo Chain.

Commands

turbo-chain role {head | member | tail} primary interface module/port secondary interface module/port

Syntax Description	turbo-chain	Configure turbo chain
	role	Turbo chain role setting
	head	Turbo chain role head setting
	member	Turbo chain role member setting
	tail	Turbo chain role tail setting
	primary interface	Turbo chain primary port setting
	secondary interface	Turbo chain secondary port setting
	<i>module/port</i>	Port ID. E.g., 1/3, 2/1,...
Defaults	N/A	
Command Modes	redundancy configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-rdnt)# turbo-chain role head primary interface 1/1 secondary interface 1/2	
Error messages	N/A	
Related commands	show redundancy turbo-chain	

turbo-ring-v1

Use the **turbo-ring-v1** redundancy configuration command on the switch to enable the Turbo Ring v1 with specified Ring ports.

Commands

turbo-ring-v1 primary interface primary-port secondary interface secondary-port

Syntax Description	turbo-ring-v1	Configure turbo ring v1
	primary interface	Turbo ring v1 ring ports setting
	<i>primary-port</i>	Port ID. E.g., 1/3, Trk2,...
	secondary interface	Turbo ring v1 ring ports setting
	<i>secondary-port</i>	Port ID. E.g., 1/3, Trk2,...
	Defaults	N/A
Command Modes	Redundancy configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config-rdnt)# turbo-ring-v1 primary interface 2/1 secondary interface 2/2 <STRING:pri_port> - Port ID. E.g., 1/3, Trk2, ... <STRING:sec_port> - Port ID. E.g., 1/3, Trk2, ...	
Error messages	Interface 2-1 not exist	
	One port is the same in ring ports or coupling ports	
Related commands	show turbo-ring-v1	

turbo-ring-v1 coupling

Use the **turbo-ring-v1 coupling** redundancy configuration command on the switch to set the coupling for Turbo Ring v1. Use the **no** form of this command to disable it.

Commands

turbo-ring-v1 coupling interface *primary-port* **coupling-control-port interface** *secondary-port*
no turbo-ring-v1 coupling

Syntax Description	turbo-ring-v1	Configure turbo ring v1
	coupling	Configure ring coupling
	interface	Turbo ring v1 ring ports setting
	<i>primary-port</i>	Primary port ID. E.g., 1/3, Trk2,...
	coupling-control-port	Turbo ring v1 coupling ports setting
	interface	Turbo ring v1 ring ports setting
	<i>secondary-port</i>	Secondary port ID. E.g., 1/3, Trk2,...
Defaults	N/A	
Command Modes	Redundancy configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config-rdnt)# turbo-ring-v1 coupling interface 2/1 coupling-control-port interface 2/2 <STRING:pri_port> - Port ID. E.g., 1/3, Trk2,... <STRING:sec_port> - Port ID. E.g., 1/3, Trk2,...</pre>	
Error messages	Interface 2-1 not exist	
	One port is the same in ring ports or coupling ports	
Related commands	show turbo-ring-v1	

turbo-ring-v1 master

Use the **turbo-ring-v1 master** redundancy configuration command on the switch to set the switch as the Turbo Ring v1 Master. Use the **no** form of this command to return to the normal Turbo Ring v1 member.

Commands

turbo-ring-v1 master
no turbo-ring-v1 master

Syntax Description	turbo-ring-v1	Configure turbo ring v1
	master	Set ring as master
Defaults	N/A	
Command Modes	Redundancy configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config-rdnt)# turbo-ring-v1 master master - Set ring as master</pre>	
Error messages	N/A	
Related commands	show turbo-ring-v1	

turbo-ring-v2

Use the **turbo-ring-v2** redundancy configuration command on the switch to configure the Turbo Ring v2 with specified Ring ports. Use the **no** form of this command to disable the specified ring.

Commands

turbo-ring-v2 *ring-id* **primary interface** *primary-port* **secondary interface** *secondary-port*
no turbo-ring-v2 *ring-id*

Syntax Description	turbo-ring-v2	Configure turbo ring v2
	<i>ring-id</i>	Turbo ring v2 ring id
	primary	Turbo ring v2 ring ports setting
	interface	Turbo ring v2 ring ports setting
	<i>primary-port</i>	Port ID. E.g., 1/3, 2/1,...
	secondary interface	Turbo ring v2 ring ports setting
	<i>secondary-port</i>	Port ID. E.g., 1/3, 2/1,...
Defaults	N/A	
Command Modes	Redundancy configuration	
Usage Guidelines	At least enable one turbo-ring domain or coupling. But cannot enable two turbo-ring domains and coupling in the same time.	
Examples	<pre>PT-7828(config-rdnt)# turbo-ring-v2 1 primary interface 2/1 secondary interface 2/2 <STRING:pri_port> - Port ID. E.g., 1/3, Trk2,... <STRING:sec_port> - Port ID. E.g., 1/3, Trk2,...</pre>	
Error messages	Turbo ring v2 only supports maximum 2 ring domains	
	Interface 2-1 not exist	
	Ring1: One port couldn't be set as 1st and 2nd redundant port simultaneously !!!	
	Ring2: One port couldn't be set as Ring1 redundant port simultaneously !!!	
	Coupling: One port couldn't be set as 1st and 2nd redundant port simultaneously !!!	
	Primary port couldn't be set as Ring2 redundant port simultaneously !!!	
	Backup port couldn't be set as Ring2 redundant port simultaneously !!!	
	Coupling port couldn't be set as Ring2 redundant port simultaneously !!!	
	Please select at least one Ring!!!	
Ring1, ring2, coupling couldn't be enabled simultaneously!!!		
Please enable one Ring in "Ring Coupling" mode!!!		
Related commands	show turbo-ring-v2	

turbo-ring-v2 coupling backup

Use the **turbo-ring-v2 coupling** redundancy configuration command on the switch to configure the backup port of Ring coupling for Turbo Ring v2. Use the **no** form of this command to disable the coupling.

Commands

turbo-ring-v2 coupling backup interface *backup-port*
no turbo-ring-v2 coupling

Syntax Description	turbo-ring-v2	Configure turbo ring v2
	coupling	Configure ring coupling
	backup	Configure ring coupling mode
	interface	Turbo ring v2 coupling ports setting
	<i>backup-port</i>	Port ID. E.g., 1/3, 2/1,...
Defaults	N/A	
Command Modes	Redundancy configuration	
Usage Guidelines	At least enable one turbo-ring domain or coupling. But cannot enable two turbo-ring domains and coupling in the same time.	

Examples	PT-7828 (config-rdnt)# turbo-ring-v2 coupling backup interface 2/1 <STRING:pri_port> - Port ID. E.g., 1/3, Trk2,...
Error messages	Turbo ring v2 only supports maximum 2 ring domains
	Ring1: One port couldn't be set as 1st and 2nd redundant port simultaneously !!!
	Ring2: One port couldn't be set as Ring1 redundant port simultaneously !!!
	Coupling: One port couldn't be set as 1st and 2nd redundant port simultaneously !!!
	Primary port couldn't be set as Ring2 redundant port simultaneously !!!
	Backup port couldn't be set as Ring2 redundant port simultaneously !!!
	Coupling port couldn't be set as Ring2 redundant port simultaneously !!!
	Please select at least one Ring!!!
Related commands	show turbo-ring-v2

turbo-ring-v2 coupling dual-homing

Use the **turbo-ring-v2 coupling dual-homing** redundancy configuration command on the switch to enable dual homing feature of Ring coupling for the Turbo Ring v2. Use the no form of this command to disable it.

Commands

turbo-ring-v2 coupling dual-homing primary interface primary-port backup interface secondary-port
no turbo-ring-v2 coupling

Syntax Description	turbo-ring-v2	Configure turbo ring v2
	coupling	Configure ring coupling
	dual-homing	Configure dual homing mode
	primary interface	Turbo ring v2 ring ports setting
	<i>primary-port</i>	Port ID. E.g., 1/3, 2/1,...
	backup interface	Turbo ring v2 ring ports setting
	<i>secondary-port</i>	Port ID. E.g., 1/3, 2/1,...
	Defaults	N/A
Command Modes	Redundancy configuration	
Usage Guidelines	At least enable one turbo-ring domain or coupling. But cannot enable two turbo-ring domains and coupling in the same time.	
Examples	PT-7828 (config-rdnt)# turbo-ring-v2 coupling dual-homing primary interface 2/1 secondary interface 2/2 <STRING:pri_port> - Port ID. E.g., 1/3, Trk2, ... <STRING:sec_port> - Port ID. E.g., 1/3, Trk2, ...	
Error messages	Turbo ring v2 only supports maximum 2 ring domains	
	Ring1: One port couldn't be set as 1st and 2nd redundant port simultaneously !!!	
	Ring2: One port couldn't be set as Ring1 redundant port simultaneously !!!	
	Coupling: One port couldn't be set as 1st and 2nd redundant port simultaneously !!!	
	Primary port couldn't be set as Ring2 redundant port simultaneously !!!	
	Backup port couldn't be set as Ring2 redundant port simultaneously !!!	
	Coupling port couldn't be set as Ring2 redundant port simultaneously !!!	
Please select at least one Ring!!!		

	Ring1, ring2, coupling couldn't be enabled simultaneously!!! Please enable one Ring in "Ring Coupling" mode!!!
Related commands	show turbo-ring-v2

turbo-ring-v2 coupling primary

Use the **turbo-ring-v2 coupling primary** redundancy configuration command on the switch to configure the primary port of Ring coupling for Turbo Ring v2. Use the **no** form of this command to return to the default setting.

Commands

turbo-ring-v2 coupling primary interface *primary-port*
no turbo-ring-v2 coupling

Syntax Description	turbo-ring-v2	Configure turbo ring v2
	coupling	Configure ring coupling
	primary	Configure ring coupling mode
	interface	Turbo ring v2 coupling ports setting
	<i>primary-port</i>	Port ID. E.g., 1/3, 2/1,...
Defaults	N/A	
Command Modes	Redundancy configuration	
Usage Guidelines	At least enable one turbo-ring domain or coupling. But cannot enable two turbo-ring domains and coupling in the same time.	
Examples	<pre>PT-7828(config-rdnt)# turbo-ring-v2 coupling primary interface 2/1 <STRING:pri_port> - Port ID. E.g., 1/3, Trk2,...</pre>	
Error messages	Turbo ring v2 only supports maximum 2 ring domains	
	Ring1: One port couldn't be set as 1st and 2nd redundant port simultaneously !!!	
	Ring2: One port couldn't be set as Ring1 redundant port simultaneously !!!	
	Coupling: One port couldn't be set as 1st and 2nd redundant port simultaneously !!!	
	Primary port couldn't be set as Ring2 redundant port simultaneously !!!	
	Backup port couldn't be set as Ring2 redundant port simultaneously !!!	
	Coupling port couldn't be set as Ring2 redundant port simultaneously !!!	
	Please select at least one Ring!!!	
Related commands	Ring1, ring2, coupling couldn't be enabled simultaneously!!! Please enable one Ring in "Ring Coupling" mode!!!	
	show turbo-ring-v2	

turbo-ring-v2 master

Use the **turbo-ring-v2 master** redundancy configuration command on the switch to configure the switch as the Ring Master of specified ring for Turbo Ring v2. Use the **no** form of this command to configure the switch as the normal member of specified ring for Turbo Ring v2.

Commands

turbo-ring-v2 ring-id master
no turbo-ring-v2 ring-id master

Syntax Description	turbo-ring-v2	Configure turbo ring v2
	<i>ring-id</i>	Turbo ring v2 ring id
	master	Set turbo ring v2 ring id as master
Defaults	N/A	

Command Modes	Redundancy configuration
Usage Guidelines	N/A
Examples	PT-7828 (config-rdnt) # turbo-ring-v2 1 master master - Set turbo ring v2 ring id as master
Error messages	Turbo ring v2 only supports maximum 2 ring domains
Related commands	show turbo-ring-v2

trusted-access

Same as **access-ip**.

Commands

trusted-access [*ip-address netmask*]

no trusted-access [*ip-address netmask*]

Syntax Description	trusted-access	Enable the trusted IP list for access
	<i>ip-address</i>	IP address
	<i>netmask</i>	IP netmask
Defaults	The feature is disabled by default.	
Command Modes	VLAN configuration as management VLAN	
Usage Guidelines	This feature will take effect when the “ trusted-access ” command is executed.	
Examples	PT-7828 (config) # interface mgmt PT-7828 (config-vlan) # trusted-access 10.10.10.10 255.255.255.0 <IPV4ADDR:ipaddr> - IP address <IPV4ADDR:netmask> - IP netmask PT-7828 (config-vlan) # trusted-access	
Error messages	Trusted access ip list full	
	IP: IP-format mask: mask-format does not exist in trusted access IP list	
Related commands	show interface mgmt trusted-access	

username

Use the **username** global configuration command on the switch to set the username and password of the local login user. Use the **no** form of this command will clear the password setting of the specified user.

Commands

username { **admin** | **user** } **password** *password*

no username { **admin** | **user** } **password**

Syntax Description	username	Configuration for login account authentication
	<i>username</i>	User name
	privilege	Privilege for account
	<i>privilege-level</i>	3 values, “admin” and “user” for account leve, “no login” indicates account as non-login user
	password	Specify the password

	<i>password</i>	Password string (Length of password should be from 4 to 16, and empty password is no longer allowed)
Defaults	There is no password for each user	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	<pre>PT-7828(config)# username admin password 1234 <LF> PT-7828(config)# username user password 5678 <LF></pre>	
Error messages	N/A	
Related commands	show users	

version

Use the **version** command in router configuration mode as RIP on the switch to change the version of the current running RIP.

Commands

version *version*

Syntax	version	Set RIP version
Description	<i>version</i>	1 2 1c
Defaults	Default is 1 (i.e. RIP version 1)	
Command Modes	Router configuration as RIP	
Usage Guidelines	N/A	
Examples	<pre>PT-7828# configure terminal PT-7828(config)# router rip PT-7828(config-rip)# version 2 PT-7828(config-rip)# PT-7828# show ip rip RIP Protocol : Enable RIP version : V2 Distribution Connected : Enable Static : Disable OSPF : Disable RIP Enable Table Interface Name IP VID Enable ----- vlan2if 192.168.102.1 2 Enable</pre>	
Error messages	Invalid version	
Related commands	N/A	

vlan create

Use the **vlan create** global configuration command on the switch to create a VLAN in the VLAN database. Use the **no** form of this command to delete a VLAN.

Commands

vlan create *vlan-id-list*
no vlan create *vlan-id-list*

Syntax	vlan	Configure VLAN parameters
Description	create	Configure VLAN parameters
	<i>vlan-id-list</i>	VLAN IDs of the VLANs
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	You can only use this command mode for configuring normal-range VLANs, that is, VLAN IDs 1 to 4094.	
Examples	PT-7828(config)# vlan create 1,3-5,7 <STRING:vlanids> - VLAN IDs of the VLANs	
Error messages	vlan 4097 is invalid!! should be range from 1 to 4094	
	vlan interfaces are full, total vlan interface is 64 !!	
Related commands	show vlan config	

vlan mode

Use the **vlan mode** configuration command on the switch to change current VLAN mode operated on the switch. Use the **no** form of this command to return to the default.

Commands

vlan mode { **1qvlan** | **pvlan** | **unaware** }
no vlan mode

Syntax Description	vlan	Configure VLAN parameters
	mode	Set (default) vlan mode
	1qvlan	IEEE 802.1Q
	pvlan	Port-based vlan
	unaware	Unaware vlan
Defaults	The default mode is 802.1Q mode in the product with 802.1Q supported; otherwise is port-based VLAN mode.	
Command Modes	Global configuration	
Usage Guidelines	N/A	
Examples	PT-7828(config)# vlan mode 1qvlan 1qvlan - IEEE 802.1Q pvlan - Port-based vlan unaware - Unaware vlan	
Error messages	N/A	
Related commands	show vlan	

vrrp

To configure the Virtual Router Redundancy Protocol (VRRP) on an interface, use the **vrrp** command in VRRP interface configuration mode. To disable the VRRP configuration, use the **no** form of this command

Commands

vrrp

vrrp vrid **vrip** ip-address

no vrrp

Syntax Description	vrrp	VRRP interface setting
	vrid	VRRP interface virtual router ID
	vrip	set virtual router ID and virtual IP
	ip-address	virtual IP(IPv4 address)
Defaults	VRRP is not configured	
Command Modes	VRRP interface configuration	
Usage Guidelines	Use vrrp command in VLAN configuration mode to enable vrrp in the VLAN interface.	
Examples	PT-7828(config-vlan)# vrrp 1 vrip 1.1.1.1 PT-7828(config-vlan)# no vrrp	
Error messages	Entry not Found!	
Related commands	vrrp preempt vrrp priority show ip vrrp	

vrrp preempt

VRRP preempt is enabled by default. This means that a VRRP router with higher priority than the master VRRP router will take over as master router. To disable this feature, use the **no** form of this command.

Commands

vrrp preempt

no vrrp preempt

Syntax Description	vrrp	VRRP interface setting
	preempt	VRRP preemption mode enable VRRP preemption mode disable
Defaults	VRRP preempt is enable	
Command Modes	VRRP interface configuration	
Usage Guidelines	Use vrrp command in VLAN configuration mode to enable vrrp in the VLAN interface.	
Examples	PT-7828(config-vlan)# vrrp preempt PT-7828(config-vlan)# no vrrp preempt	
Error messages	Entry not Found!	
Related commands	vrrp vrrp priority	

vrrp priority

To set the priority of the virtual router, use the **vrrp priority** command in VRRP interface configuration mode. To remove the priority of the virtual router, use the **no** form of this command.

Commands

vrrp priority

no vrrp priority

Syntax Description	vrrp	VRRP interface setting
	priority	VRRP priority (1 to 254) Set VRRP priority to default(100)
Defaults	priority 100	
Command Modes	VRRP interface configuration	
Usage Guidelines	Use vrrp command in VLAN configuration mode to enable vrrp in the VLAN interface.	
Examples	PT-7828(config-vlan)# vrrp priority 100 PT-7828(config-vlan)# no vrrp priority	
Error messages	Entry not Found!	
	Invalid parameters!	
Related commands	vrrp vrrp preempt	

warning-notification system-event

Use **warning-notification system-event** global configuration commands to enable the system warning events trigger to email, relay, syslog or trap. Use **no** form of this command to disable it.

Commands

warning-notification system-event { cold-start | warm-start | config-changed | pwr1-trans-on | pwr2-trans-on | pwr1-trans-off | pwr2-trans-off | auth-fail | password-changed | tacacs-auth-fail | radius-auth-fail | topology-changed | coupling-changed | master-changed | rstp-admin-changed | rstp-topology-changed | turbo-ring-break | di1-trans-on|di1-trans-off } {action *action-index* | severity *severity-level* | active}
no warning-notification system-event { cold-start | warm-start | config-changed | pwr1-trans-on | pwr2-trans-on | pwr1-trans-off | pwr2-trans-off | auth-fail | password-changed | tacacs-auth-fail | radius-auth-fail | topology-changed | coupling-changed | master-changed | rstp-admin-changed | rstp-topology-changed | turbo-ring-break | di1-trans-on|di1-trans-off } active}

Syntax Description	warning-notification	
	system-event	
	cold-start	
	warm-start	
	config-changed	
	pwr1-trans-on	
	pwr2-trans-on	
	pwr1-trans-off	
	pwr2-trans-off	
	auth-fail	
	password-changed	
	tacacs-auth-fail	
	radius-auth-fail	

	topology-changed	
	coupling-changed	
	master-changed	
	rstp-admin-changed	
	rstp-topology-changed	
	turbo-ring-break	
	di1-trans-on	
	di1-trans-off	
	action	
	<i>action-index</i>	
	severity	
	<i>severity-level</i>	
	active	
Defaults	N/A	
Command Modes	Global configuration	
Usage Guidelines	<p><i>action-index</i> as follow, Trap only(1), Email only(2), Trap+Email(3), Syslog only(4), Trap+Syslog(5), Email+Syslog(6), Trap+Email+Syslog(7), Relay1 only(8), Trap+Relay1(9), Email+Relay1(10), Trap+Email+Relay1(11), Syslog+Relay1(12), Trap+Syslog+Relay1(13), Email+Syslog+Relay1(14), Trap+Email+Syslog+Relay1(15), Relay2 only(16), Trap+Relay2(17), Email+Relay2(18), Trap+Email+Relay2(19), Syslog+Relay2(20), Trap+Syslog+Relay2(21), Email+Syslog+Relay2(22), Trap+Email+Syslog+Relay2(23), Relay1+Relay2(24), Trap+Relay1+Relay2(25), Syslog+Relay1+Relay2(28), Email+Syslog+Relay1+Relay2(30), Trap+Email+Syslog+Relay1+Relay2(31), None(0) <i>severity-level</i> as follow, Emergency(0), Alert(1), Critical(2), Error(3), Warning(4), Notice(5), Information(6), Debug(7)</p>	
Examples	<pre>EDS-G516E(config)# warning-notification system-event cold-start action 5 EDS-G516E(config)# warning-notification system-event cold-start severity 3 EDS-G516E(config)# no warning-notification system- event cold-start active</pre>	
Error messages	Invalid action value or non-support this combination action Invalid severity type	
Related commands	show relay-warning config	

warning-notification port-event

Use **warning-notification port-event** interface configuration commands to enable the port warning events trigger to email, relay, syslog or trap. Use **no** form of this command to disable it.

Commands

warning-notification port-event {event { link-on | link-off | traffic-overload *rx-threshold* duration} | action *action-index* | severity *severity-level* | active}

no warning-notification port-event {event { link-on | link-off | traffic-overload} | active}

Syntax Description	warning-notification	
	port-event	
	event	
	link-on	
	link-off	
	traffic-overload	
	<i>rx-threshold</i>	
	<i>duration</i>	
	action	
	<i>action-index</i>	
	severity	
	<i>severity-level</i>	
	active	
Defaults	N/A	
Command Modes	Interface configuration	
Usage Guidelines	<p><i>action-index</i> as follow, Trap only(1), Email only(2), Trap+Email(3), Syslog only(4), Trap+Syslog(5), Email+Syslog(6), Trap+Email+Syslog(7), Relay1 only(8), Trap+Relay1(9), Email+Relay1(10), Trap+Email+Relay1(11), Syslog+Relay1(12), Trap+Syslog+Relay1(13), Email+Syslog+Relay1(14), Trap+Email+Syslog+Relay1(15), Relay2 only(16), Trap+Relay2(17), Email+Relay2(18), Trap+Email+Relay2(19), Syslog+Relay2(20), Trap+Syslog+Relay2(21), Email+Syslog+Relay2(22), Trap+Email+Syslog+Relay2(23), Relay1+Relay2(24), Trap+Relay1+Relay2(25), Syslog+Relay1+Relay2(28), Email+Syslog+Relay1+Relay2(30), Trap+Email+Syslog+Relay1+Relay2(31), None(0)</p> <p><i>severity-level</i> as follow, Emergency(0), Alert(1), Critical(2), Error(3), Warning(4), Notice(5), Information(6), Debug(7)</p>	
Examples	<pre>EDS-G516E(config-if)#warning-notification port-event event traffic-overload 30 150 EDS-G516E(config-if)# no warning-notification port- event event link-on</pre>	
Error messages	Invalid action value or non-support this combination action Invalid severity type	

Related commands	show relay-warning config
------------------	---------------------------

