YASKAWA

Networking Solutions

PNS | 911-2PNx0 | Manual

HB165 | PNS | 911-2PNx0 | en | 25-02

PROFINET Switches PN5-RD/PN8-RD

YASKAWA Europe GmbH
Philipp-Reis-Str. 6
65795 Hattersheim
Germany
Tel.: +49 6196 569-300
Fax: +49 6196 569-398
Email: info@yaskawa.eu
Internet: www.yaskawa.eu.com

911-2PNx0_000_PN5/8-RD,6,GB - © 2025

Table of contents

1 General

1.1 About this manual

Objective and contents

This manual describes the Ethernet Switches PN5-RD/PN8-RD.

- It describes the structure, configuration and application.
- The manual is targeted at users with good basic knowledge in automation technology.
- The manual does not replace sufficient basic knowledge of automation technology or sufficient familiarity with the specific product.
- The manual consists of chapters. Each chapter describes a completed topic.
- For guidance, the manual provides:
  - An overall table of contents at the beginning of the manual
  - References with pages numbers

Validity of the documentation

Product	Order no.	as of state:	
		HW	FW
PN5-RD/PN8-RD	911-2PNx0	01	V3.5.4

Documentation

In the context of the use of the pertinent Yaskawa product, the manual is to be made accessible to the pertinent qualified personnel in:

- Project engineering
- Installation department
- Commissioning
- Operation

Icons and headings

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

⚠ DANGER

- Immediate danger to life and limb of personnel and others.
- Non-compliance will cause death or serious injury.

⚠ CAUTION

- Hazardous situation to life and limb of personnel and others. Non-compliance may cause slight injuries.
- This symbol is also used as warning of damages to property.

! NOTICE

- Designates a possibly harmful situation.
- Non-compliance can damage the product or something in its environment.

ℹ *Supplementary information and useful tips.*

1.2 Copyright © YASKAWA Europe GmbH

All rights reserved

For permission to reproduce or distribute, please contact: YASKAWA Europe GmbH,
European Headquarters, Philipp-Reis-Str. 6, 65795 Hattersheim, Germany

Tel.: +49 6196 569 300
Fax.: +49 6196 569 398
E-mail: info@yaskawa.eu
Internet: www.yaskawa.eu.com

Download Center

By entering the product order number in the *‘Download Center’* at www.yaskawa.eu.com, the pertinent manuals, data sheets, declarations of conformity, certificates and other helpful information for your product can be found.

Trademarks

VIPA is a registered trademark of YASKAWA Europe GmbH.

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

General terms of use

Every effort was made by Yaskawa to ensure that the information contained in this document was complete and correct at the time of publication. Nevertheless, the information contained therein is only owed by Yaskawa as it is available at Yaskawa. Correctness is not assured by Yaskawa, the right to change the information contained herein is always reserved by Yaskawa. There is no obligation to inform the customer of any changes. The customer is requested to actively keep this documentation up to date. The use of the products covered by these instructions, together with the associated documentation, is always at the customer's own risk, in accordance with the applicable guidelines and standards. This documentation describes the hardware and software components and functions of the product. It is possible that units are described which the customer does not have. The exact scope of delivery is described in the respective purchase contract.

Document support

Contact your local representative of YASKAWA Europe GmbH if you have errors or questions regarding the content of this document. You can reach YASKAWA Europe GmbH via the following contact:

Email: Documentation.HER@yaskawa.eu

Technical support

Contact your local representative of YASKAWA Europe GmbH if you encounter problems or have questions regarding the product. If such a location is not available, you can reach the Yaskawa customer service via the following contact:

YASKAWA Europe GmbH,
European Headquarters, Philipp-Reis-Str. 6, 65795 Hattersheim, Germany
Tel.: +49 6196 569 500 (hotline)
Email: support@yaskawa.eu

1.3 Safety instructions

General safety instructions

DANGER

Danger to life due to non-compliance with safety instructions

Non-compliance with the safety instructions in the manual can result in serious injury or death. The manufacturer is not responsible for any injuries or damage to the equipment.

CAUTION

Before commissioning and operating the components described in this manual, it is essential to note the following:

- Modifications to the automation system must only be done in a voltage-free state!
- Connection and modification only by trained electricians
- National regulations and guidelines in the respective country of use must be observed and complied with (installation, protective measures, EMC, etc.)

Intended use

- It is the customer's responsibility to comply with all pertinent standards, codes, or regulations applicable to the use of the product, including those that apply when the Yaskawa product is used in combination with other products.
- The customer must confirm that the Yaskawa product is suitable for the customer's plant, machinery and equipment.
- If the Yaskawa product is used in a manner not specified by this manual, the protection provided by the Yaskawa product may be impaired and the use may result in material or immaterial damage.
- Contact Yaskawa to determine whether use is permitted in the following applications. If the use in the respective application is permissible, the Yaskawa product is to be used by considering additional risk assessments and specifications, and safety measures are to be provided to minimise the dangers in the event of a fault. Special caution is required and protective measures must be taken in the case of:
  - Outdoor use, use with possible chemical contamination or electrical interference, or use under conditions or in environments which are not described in product catalogs or manuals
  - Nuclear control systems, combustion systems, railway systems, aviation systems, automotive systems, medical devices, amusement machines and equipment that is specifically regulated by industry or government
  - Systems, machines and devices that can pose a risk to life or property
  - Systems that require a high degree of reliability, such as gas, water or electricity supply systems or systems that operate 24 hours a day
  - Other systems that require a similarly high level of security
- Never use the Yaskawa product in an application where failure of the product could cause serious danger to life, limb, health or property without first ensuring that the system is designed to provide the required level of safety with risk warnings and redundancy to avoid the realisation of such dangers and that the Yaskawa product is properly designed and installed.
- The connection examples and other application examples described in the product catalogs and manuals of Yaskawa are for reference purposes. Check the functionality and safety of the devices and systems actually to be used before using the Yaskawa product.
- To avoid accidental harm to third parties, read and understand all prohibitions on use and precautions, and operate the Yaskawa product correctly.

Field of application

- The Yaskawa product is not suited for use in life-support machines or systems.
- Please contact your Yaskawa representative or Yaskawa distributor if considering the use of the Yaskawa product for special purposes, such as machines or systems used in passenger cars, in medical, aircraft and aerospace applications, for power supply of networks, for electrical power distribution or for underwater applications.

> ⚠ DANGER
>
> The device is not permitted for use
>
> – in explosive environments (EX zone)

The system is designed and manufactured for proper use and use in accordance with the user manual and is designed for:

- Communication and process control
- general control and automation tasks
- for industrial use
- operation within the environmental conditions specified in the technical data
- installation in a cabinet

> ⚠ DANGER
>
> **If this Yaskawa product is used in applications where failure of the device can result in the loss of human life, a serious accident or physical injury, you must install appropriate safety devices.**
>
> – Death or serious injury can result if you do not install the safety devices properly.

Disclaimer

(1) The contractual and legal liability of Yaskawa and the legal representatives and vicarious agents of Yaskawa for compensation and reimbursement of expenses in relation to the content of this documentation is excluded or limited as follows:

a) For slightly negligent breaches of *Essential Contractual Duties* arising from the contractual obligation, for Yaskawa the amount of liability is limited to the foreseeable damage typical for the contract. *'Essential Contractual Duties'* are those duties that characterise the performance of the contract and on which the Yaskawa customer may reasonably rely.

(b) In each case, Yaskawa is not liable for (i) the slightly negligent breach of duties arising from the duties that are not *Essential Contractual Duties*, as well as (ii) force majeure, i.e. external events that have no operational connection and cannot be averted even by exercising the utmost care that can reasonably be expected.

(2) The aforementioned limitation of liability does not apply (i) in cases of mandatory statutory liability (in particular under the product liability law), (ii) if and to the extent that Yaskawa has assumed a guarantee or same as guaranteed procurement risk according to § 276 BGB, (iii) for culpably caused injuries to life, limb and/or health, also by representatives or vicarious agents, as well as (iv) in case of delay in the event of a fixed completion date.

(3) A reversal of the burden of proof is not associated with the provisions above.

Disposal

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

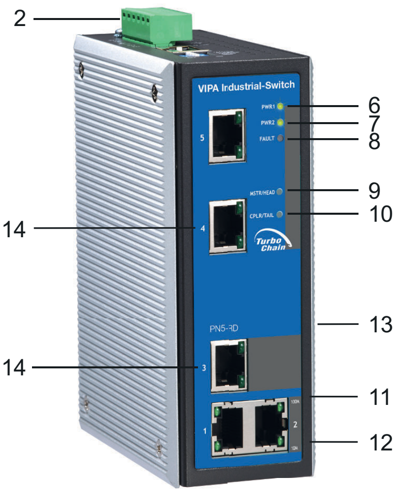
2 Hardware Installation

Overview

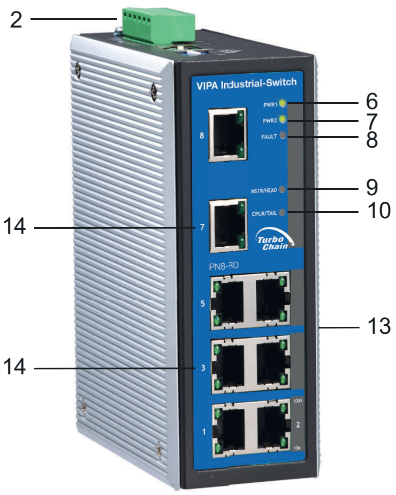
The Switch PN5-RD/PN8-RD series, which includes both 5- and 8-port smart Ethernet switches, is a cost-effective solution for your Ethernet connections. In addition, the built-in smart alarm function helps system maintainers monitor the health of your Ethernet network.

2.1 Panel Layout

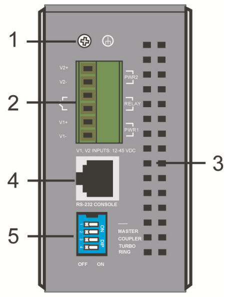
PN5-RD
Front Panel View



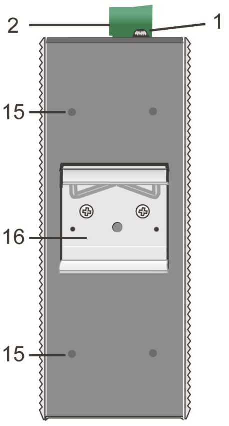
PN8-RD
Front Panel View



Top Panel View

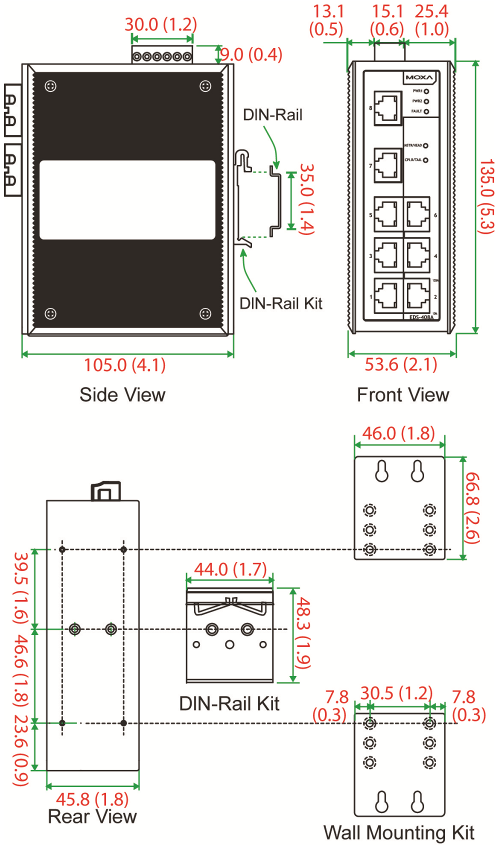


Rear Panel View



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

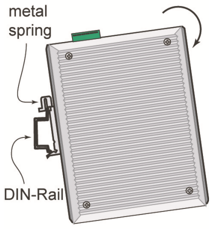


Unit = mm (inch)

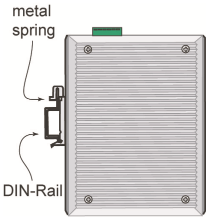
2.3 DIN-Rail Mounting

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.

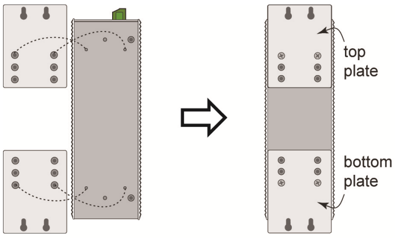


To remove the Switch from the DIN-Rail, simply reverse Steps 1 and 2.

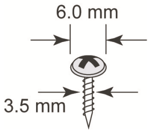
2.4 Wall Mounting (optional)

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°C ≤ Tamb ≤ 75°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 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

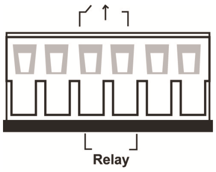
Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices.

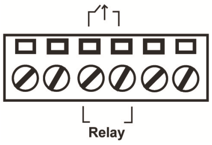
⚠ CAUTION

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-RDs 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.





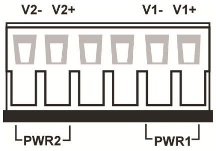
Fault: The two middle contacts of the 6-contact terminal block connector are used to detect both power faults and port faults. The two wires attached to the fault contacts form an open circuit when:

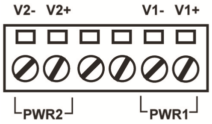
- a relay warning event is triggered.
- the PN5-RD/PN8-RD is the Master of this Turbo Ring and the Turbo Ring is broken.
- there is a start-up failure.

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-RDs 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.

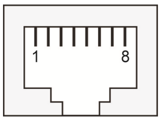
2.10 Communication Connections

PN8-RD models have 8 10/100BaseT(X) Ethernet ports. PN5-RD models have 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 Pinouts



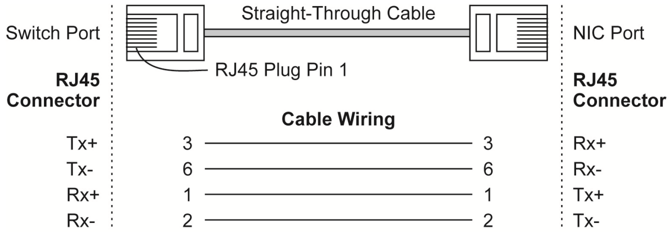
MDI Port Pinouts

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

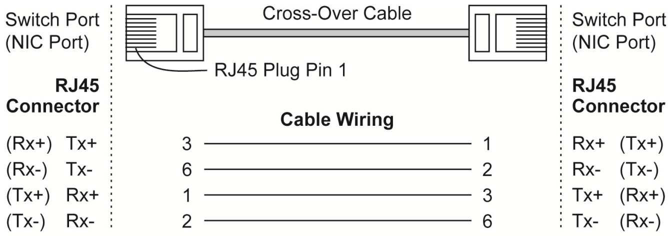
MDI-X Port Pinouts

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.

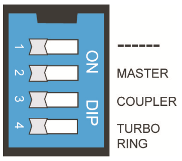
2.12 Relay Contact

The 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 15* 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 to provide better network reliability and faster recovery time. 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. 5.1 'Communication Redundancy' ...page 86*

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/TAIL	🟩 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-RDs 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), 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
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	
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)
Storage Temperature	-40 to 85°C (-40 to 185°F)
Ambient Relative Humidity	5% to 95% (non-condensing)

Technology	
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

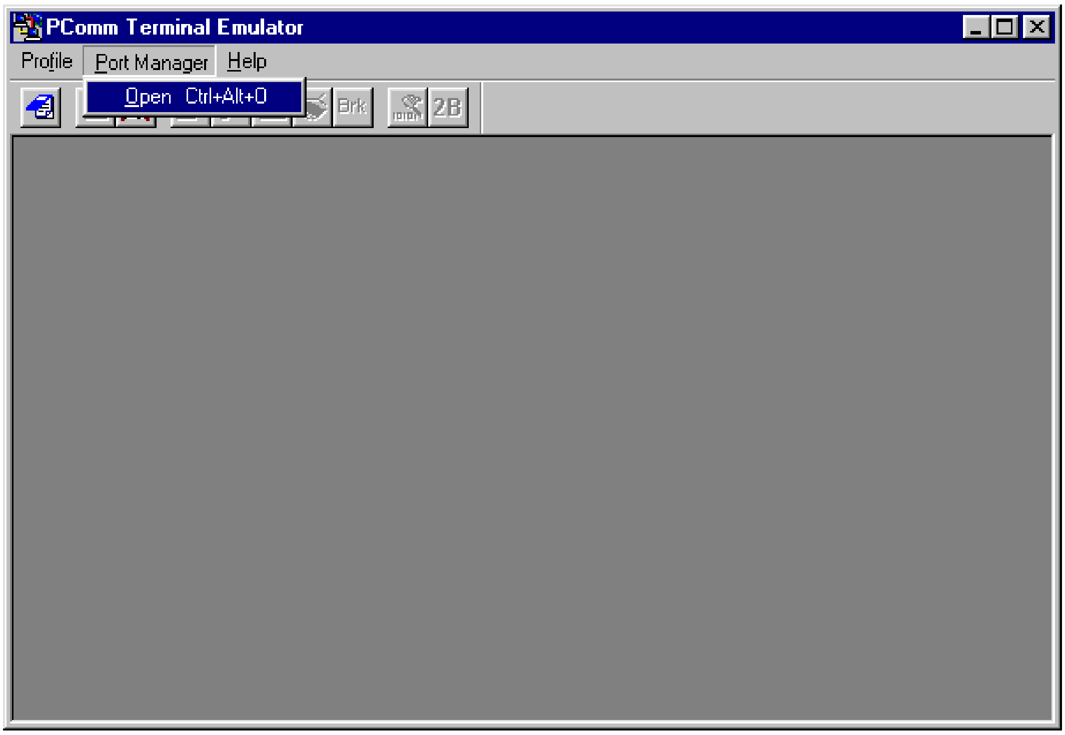
3.1 Serial Console Configuration (115200, None, 8, 1, VT100)

> – *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 Yaskawa website.*

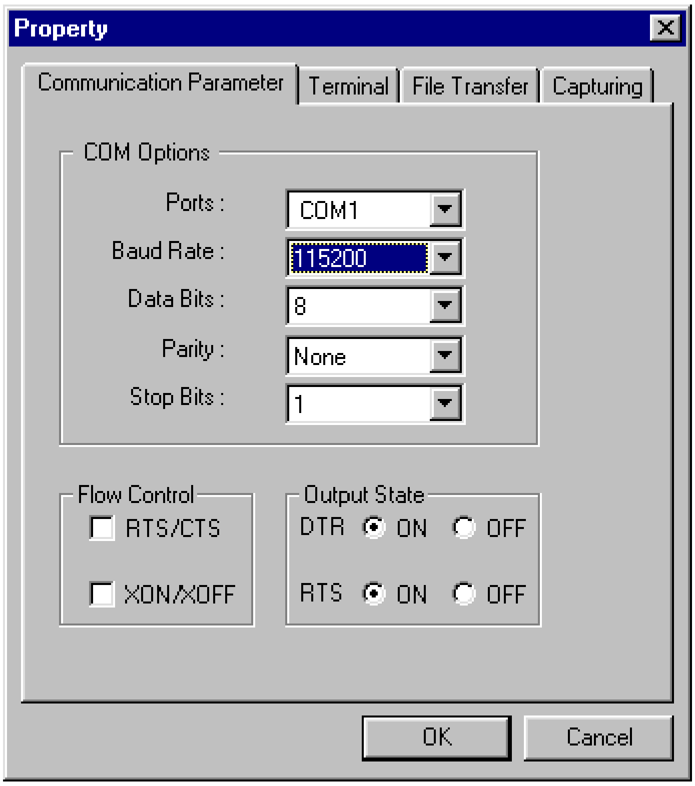
Before running "PComm Terminal Emulator", use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the VIPA switch's console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up). After installing "PComm Terminal Emulator", open the VIPA switch's *serial console*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



Property

Communication Parameter | Terminal | File Transfer | Capturing

COM Options

Ports : COM1

Baud Rate : 115200

Data Bits : 8

Parity : None

Stop Bits : 1

Flow Control

☐ RTS/CTS

☐ XON/XOFF

Output State

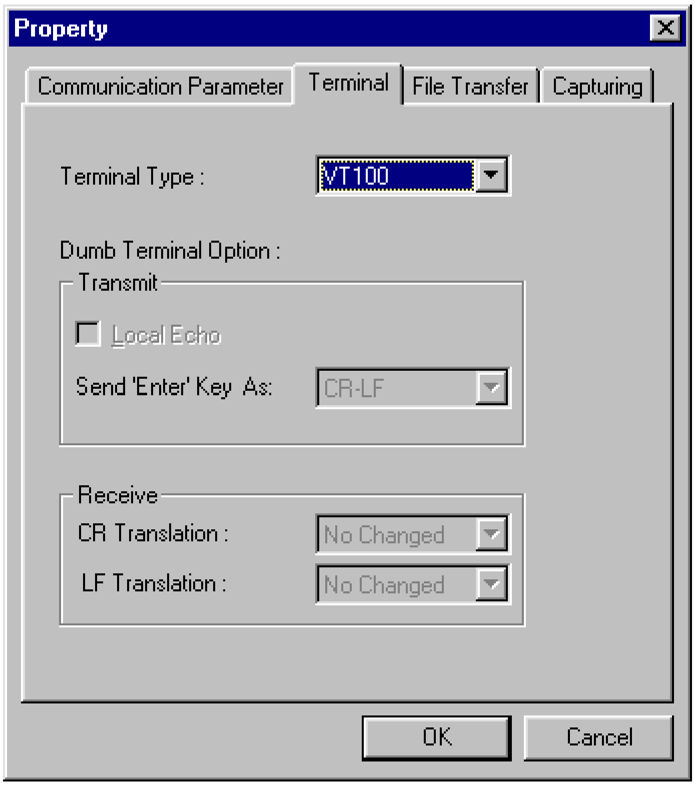
DTR ● ON ○ OFF

RTS ● ON ○ OFF

OK Cancel

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'*.

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



Terminal Type : VT100

Dumb Terminal Option :

Transmit

☐ Local Echo

Send 'Enter' Key As: CR-LF

Receive

CR Translation : No Changed

LF Translation : No Changed

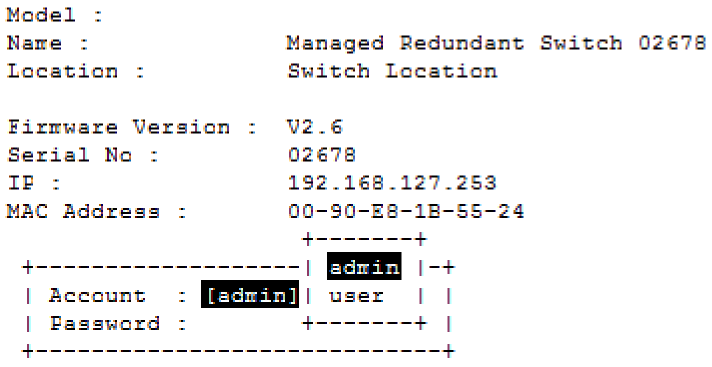
4. On the *'Terminal'* tab, select *'VT100'* for *'Terminal Type'*, and then click [OK] to continue.

   ➡ In the *'Terminal'* window, the VIPA switch will prompt you to select a terminal type.

5. Enter "1" to select *'ansi/vt100'* and then press *[Enter]*.

   ➡ The serial console will prompt you to log in.

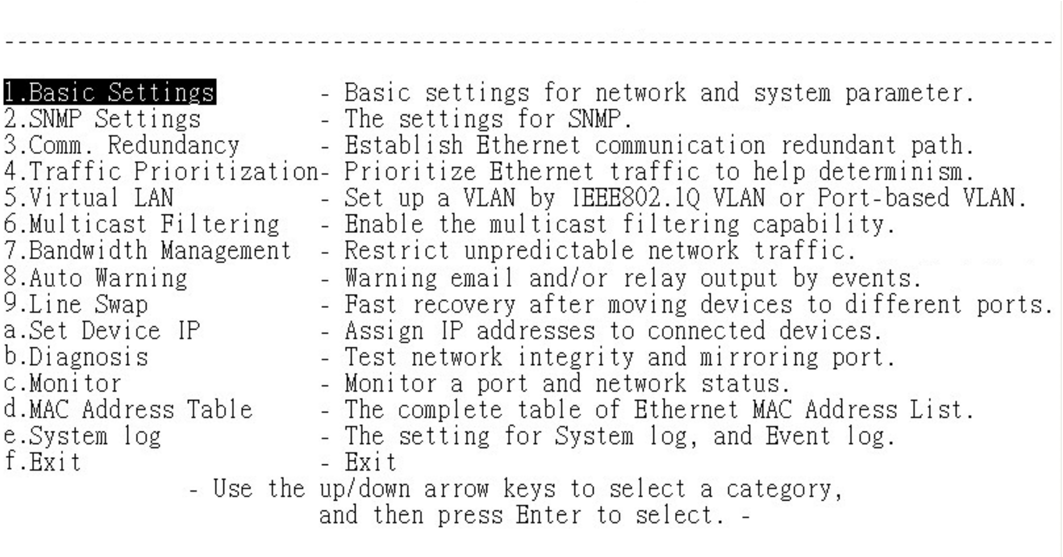
6. Press *[Enter]* and select *'admin'* or *'user'*. Use the down arrow key on your keyboard to select the *'Password'* field and enter a password if desired. This password will be required to access any of the consoles (web, serial, Telnet). If you do not wish to create a password, leave the *'Password'* 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
                           +--------+
 +-------------------| admin |-+
 | 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.

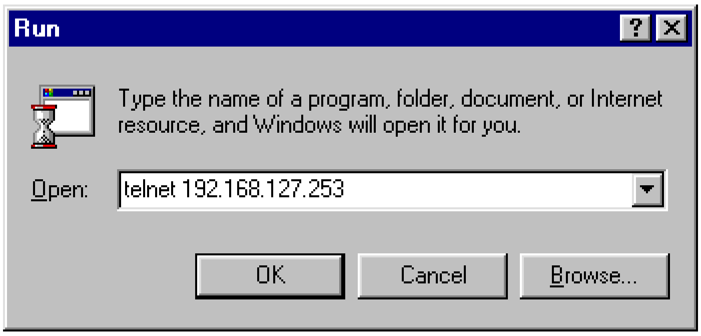
To connect to the VIPA switch’s Telnet or web console, your PC host and the VIPA switch must be on the same logical subnet.

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.

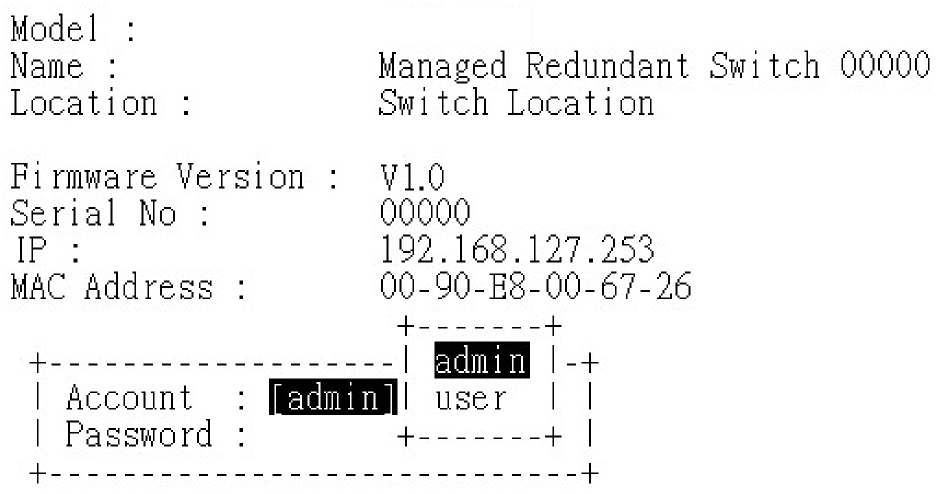


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: telnet 192.168.127.253

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]*.

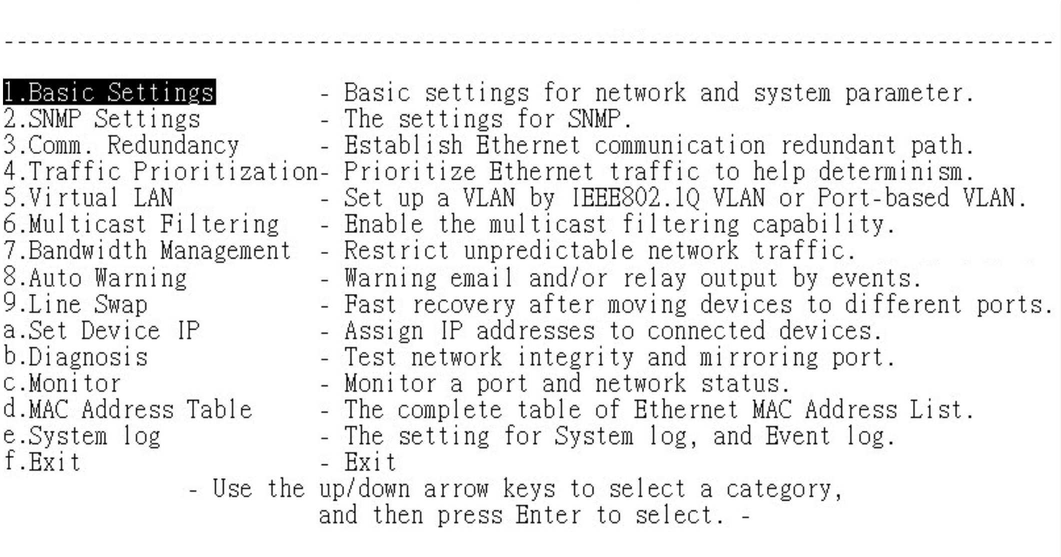
3. The Telnet console will prompt you to log in. Press *[Enter]* and then select *'admin'* or *'user'*. Use the down arrow key on your keyboard to select the *'Password'* field and enter a password if desired. This password will be required to access any of the consoles (web, serial, Telnet). If you 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.

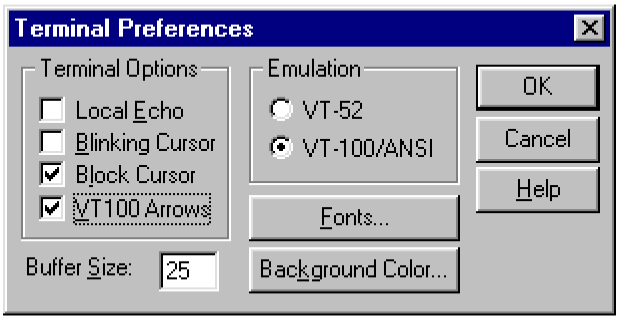


```
---------------------------------------------------------------------------

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.



Terminal Options
☐ Local Echo
☐ Blinking Cursor
☑ Block Cursor
☑ VT100 Arrows

Emulation
○ VT-52
● VT-100/ANSI

Buffer Size: 25

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.

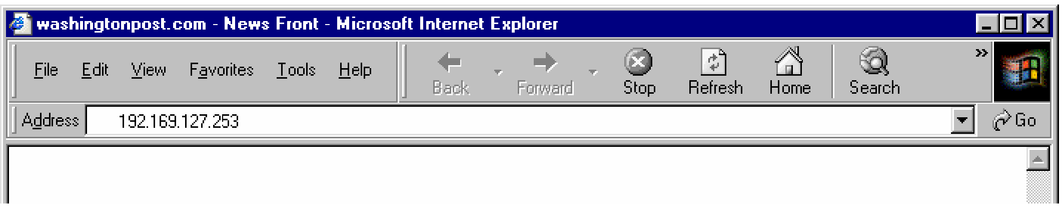
If the VIPA switch is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

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.

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.

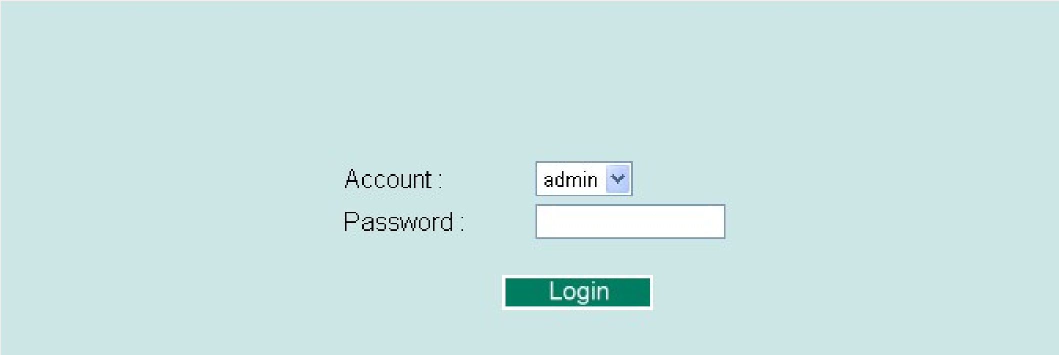


Address 192.169.127.253

➡ 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]*.

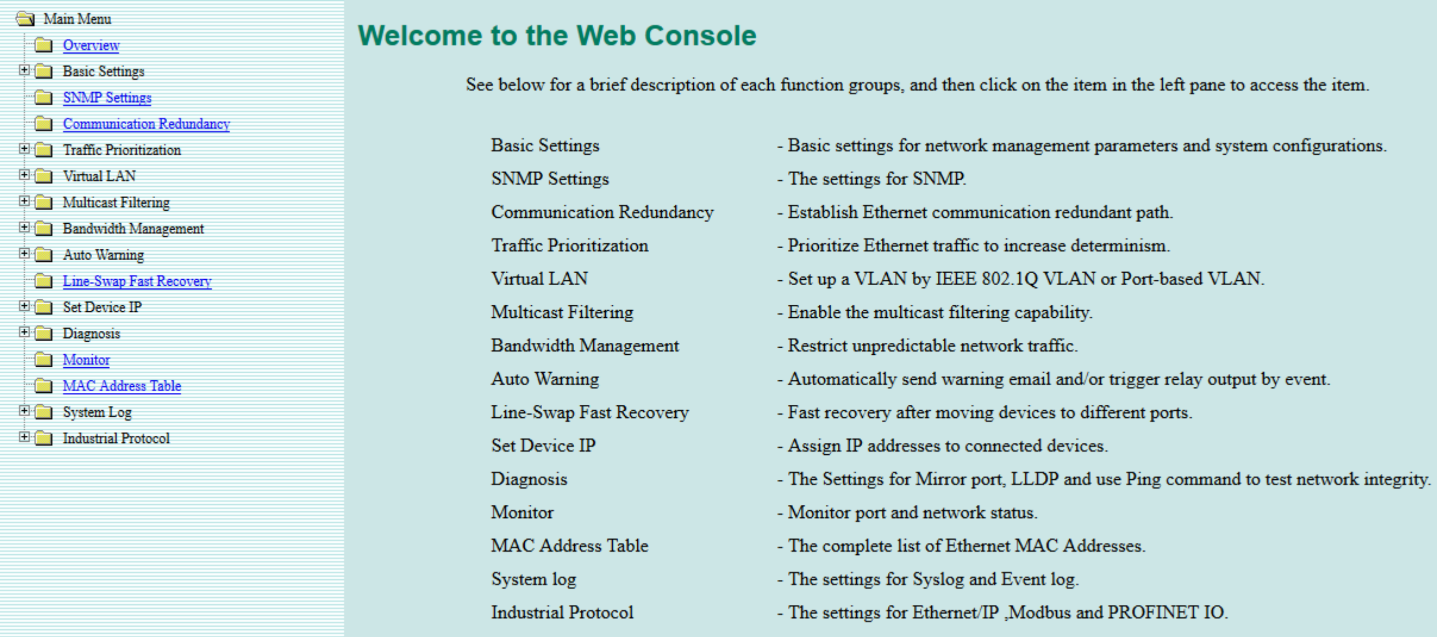
By default, no password is assigned to the VIPA switch's web, serial and Telnet consoles.



Account : admin

Password :

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.



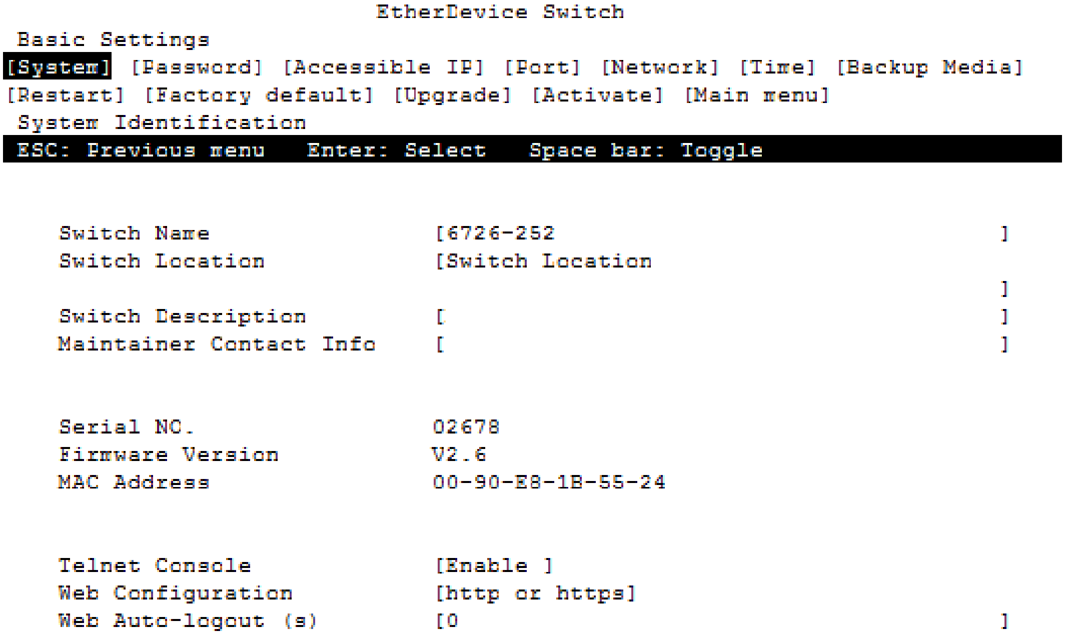
Welcome to the Web Console

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:

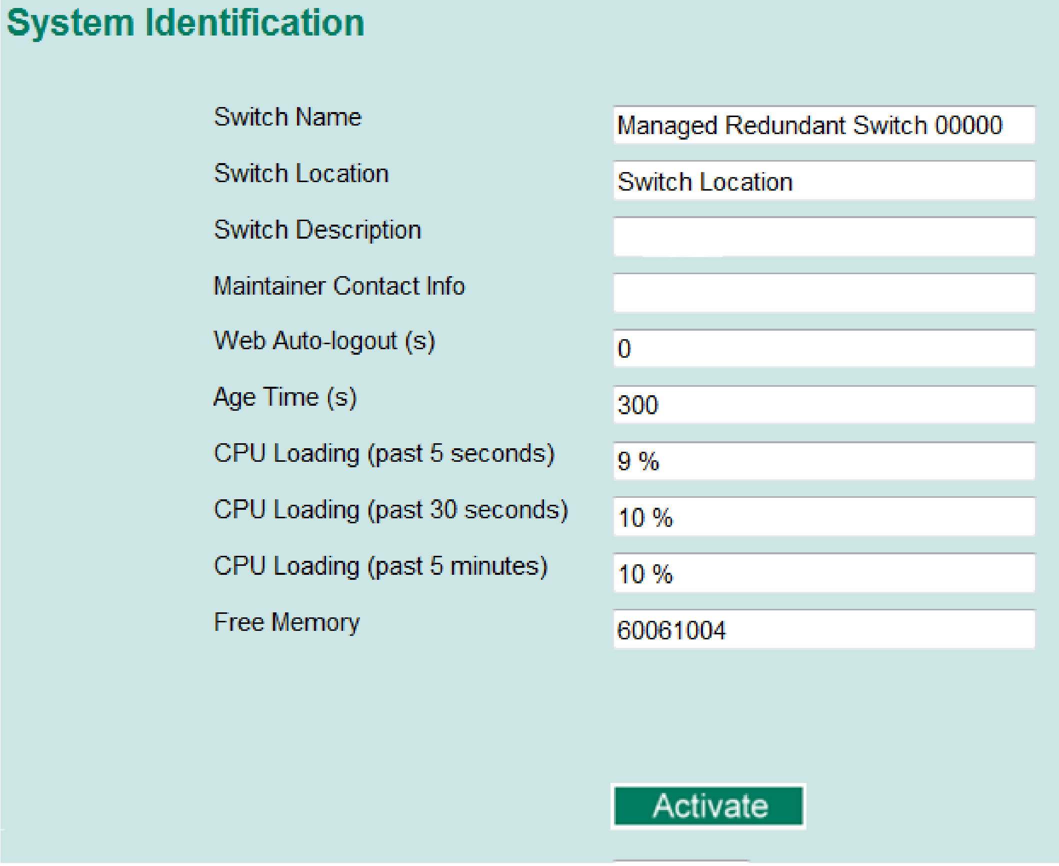
- Configuring Basic Settings
- Loop Protection
- Configuring SNMP
- Using Traffic Prioritization
- Using Virtual LAN
- Using Multicast Filtering
- Using Bandwidth Management
- Using Auto Warning
- Using Line-Swap-Fast-Recovery
- Using Set Device IP
- Using Diagnosis
- Using Monitor
- Using the MAC Address 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	Managed Redundant Switch 00000
Switch Location	Switch Location
Switch Description	
Maintainer Contact Info	
Web Auto-logout (s)	0
Age Time (s)	300
CPU Loading (past 5 seconds)	9 %
CPU Loading (past 30 seconds)	10 %
CPU Loading (past 5 minutes)	10 %
Free Memory	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

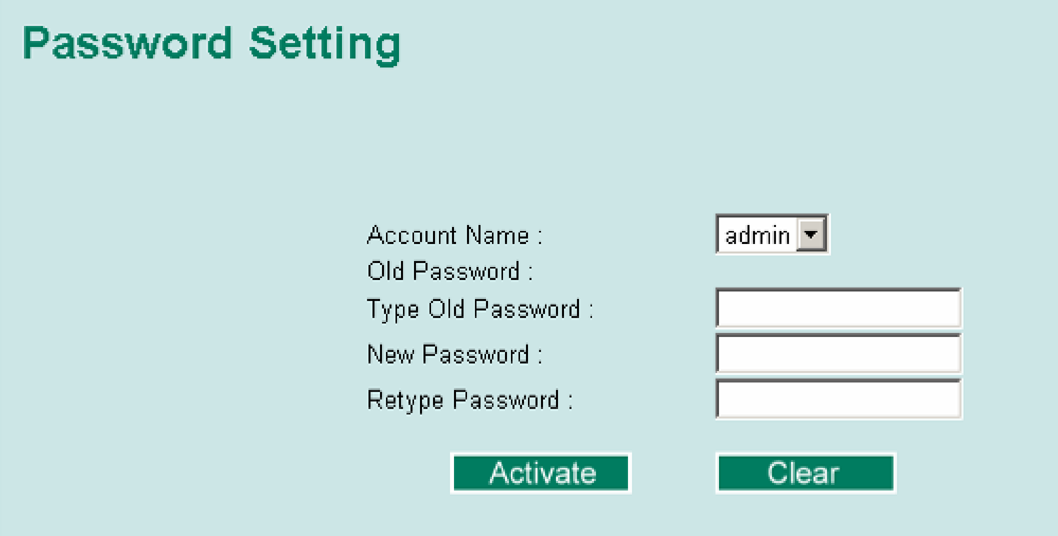
Setting	Description	Factory Default
Read-only	The CPU usage volume in the past 5 seconds, 30 seconds and 5 minutes	None

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 :	admin
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

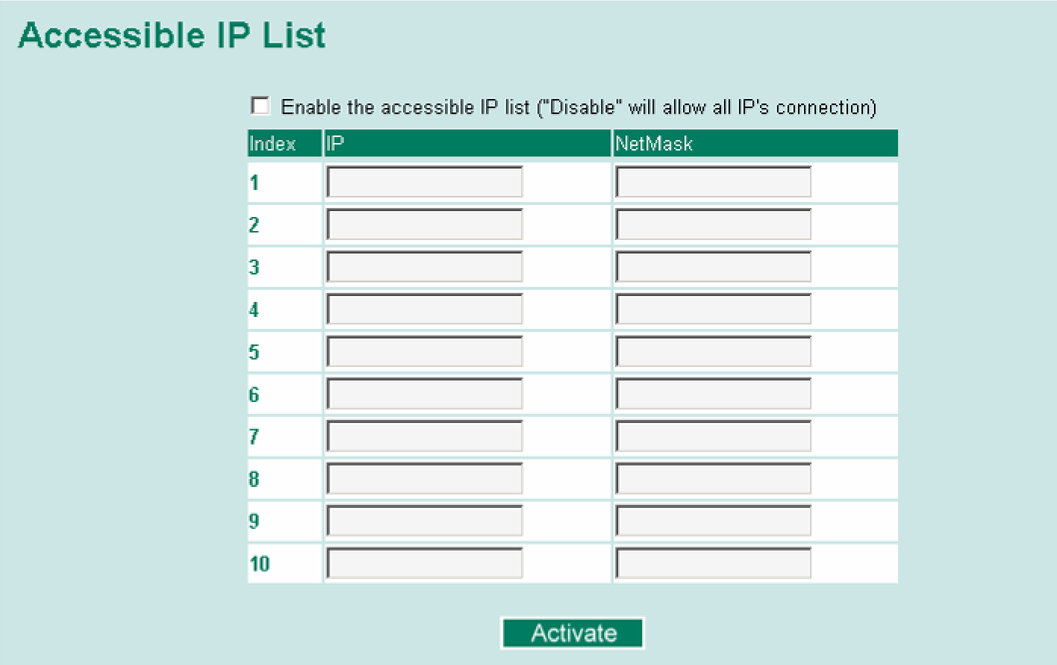
Setting	Description	Factory Default
Admin	This account can modify the VIPA switch's configuration.	admin
User	This account can only view the VIPA switch's configurations.	

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		
2		
3		
4		
5		
6		
7		
8		
9		
10		

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'*.

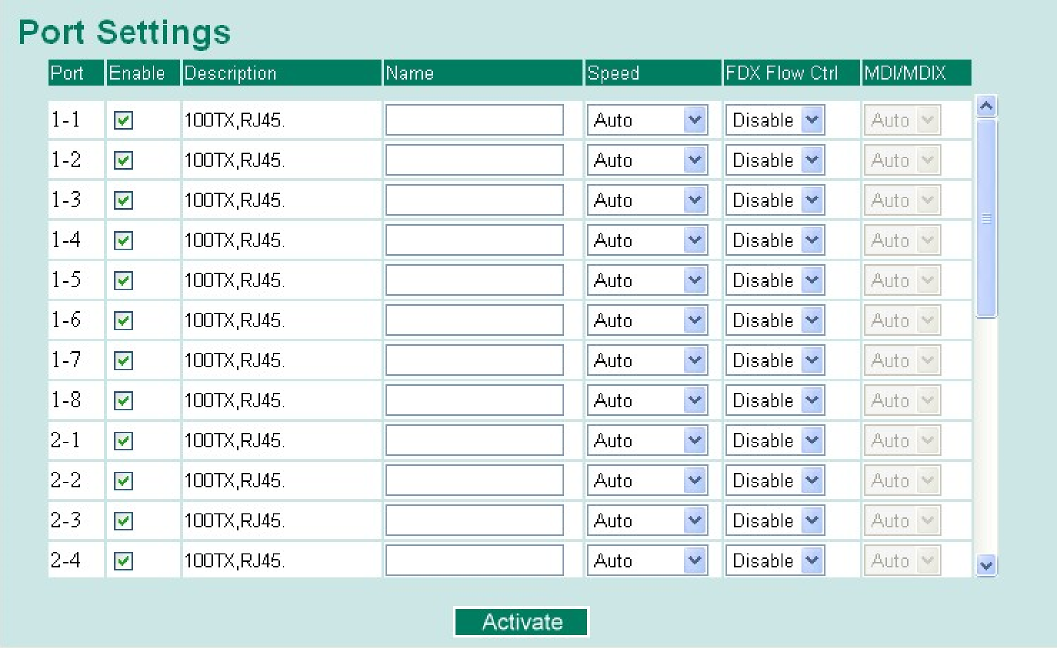
Additional configuration examples:

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	☑	100TX,RJ45.		Auto	Disable	Auto
1-2	☑	100TX,RJ45.		Auto	Disable	Auto
1-3	☑	100TX,RJ45.		Auto	Disable	Auto
1-4	☑	100TX,RJ45.		Auto	Disable	Auto
1-5	☑	100TX,RJ45.		Auto	Disable	Auto
1-6	☑	100TX,RJ45.		Auto	Disable	Auto
1-7	☑	100TX,RJ45.		Auto	Disable	Auto
1-8	☑	100TX,RJ45.		Auto	Disable	Auto
2-1	☑	100TX,RJ45.		Auto	Disable	Auto
2-2	☑	100TX,RJ45.		Auto	Disable	Auto
2-3	☑	100TX,RJ45.		Auto	Disable	Auto
2-4	☑	100TX,RJ45.		Auto	Disable	Auto

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.	

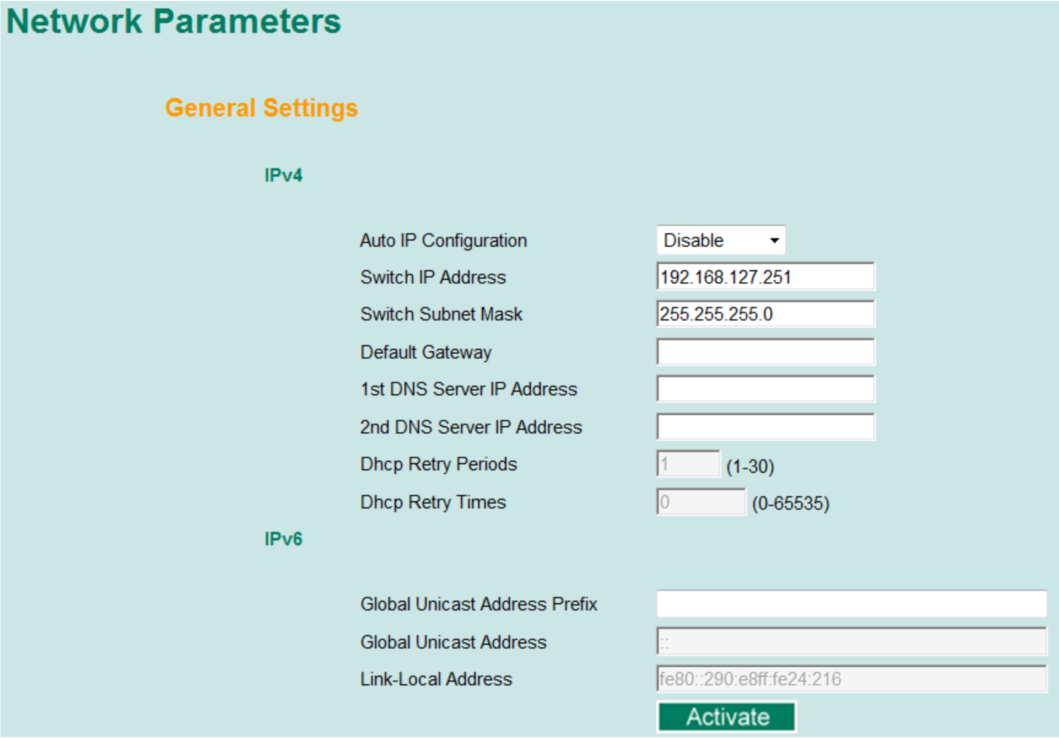
MDI/MDIX

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

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

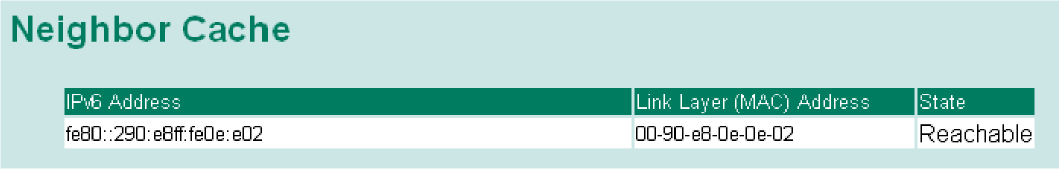
Global Unicast Address

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



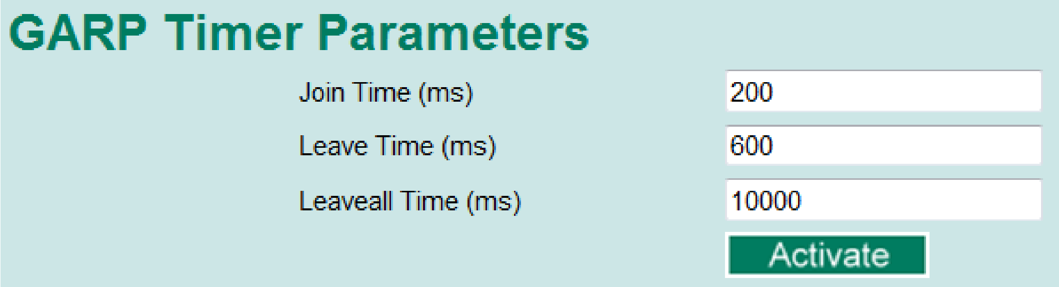
Neighbor Cache

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) 200

Leave Time (ms) 600

Leaveall Time (ms) 10000

Join Time

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

Leave Time

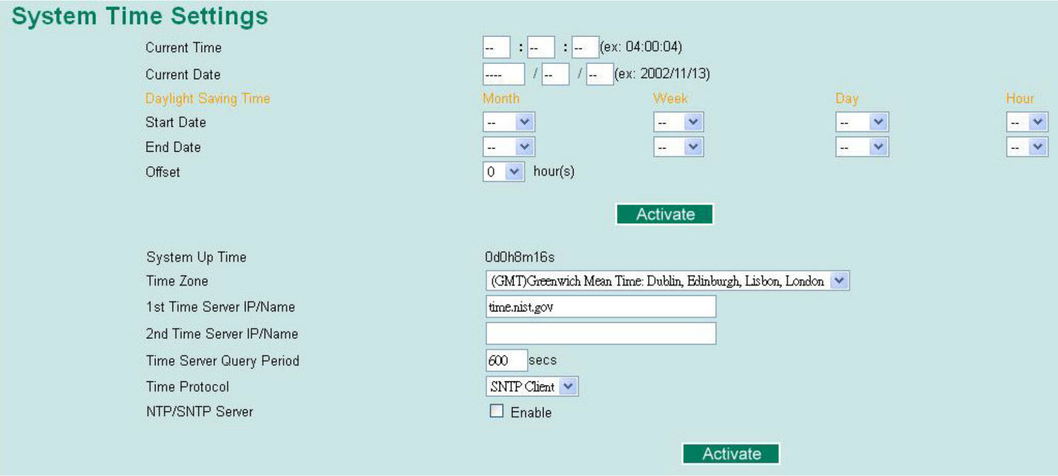
Setting	Description	Factory Default
None	Specifies the period of leave time	600

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



System Time Settings

Current Time	-- : -- : -- (ex: 04:00:04)			
Current Date	---- / -- / -- (ex: 2002/11/13)			
Daylight Saving Time	Month	Week	Day	Hour
Start Date	--	--	--	--
End Date	--	--	--	--
Offset	0 hour(s)			

Activate

System Up Time	0d0h8m16s
Time Zone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
1st Time Server IP/Name	time.nist.gov
2nd Time Server IP/Name	
Time Server Query Period	600 secs
Time Protocol	SNTP Client
NTP/SNTP Server	□ Enable

Activate

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

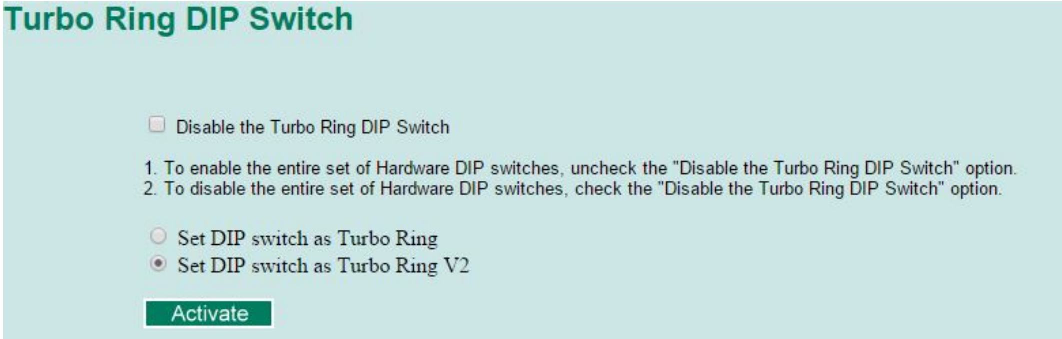
Setting	Description	Factory Default
NTP	NTP (Network Time Protocol) is used to synchronize time with multiple time servers. The time accuracy is up to 50 ms.	-
SNTP	SNTP stands for Simple Network Time Protocol). The synchronization process of SNTP is simpler than NTP. The time accuracy is up to 1 second,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



Turbo Ring DIP Switch

□ Disable the Turbo Ring DIP Switch

1. To enable the entire set of Hardware DIP switches, uncheck the "Disable the Turbo Ring DIP Switch" option.
2. To disable the entire set of Hardware DIP switches, check the "Disable the Turbo Ring DIP Switch" option.

○ Set DIP switch as Turbo Ring
● Set DIP switch as Turbo Ring V2

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.	

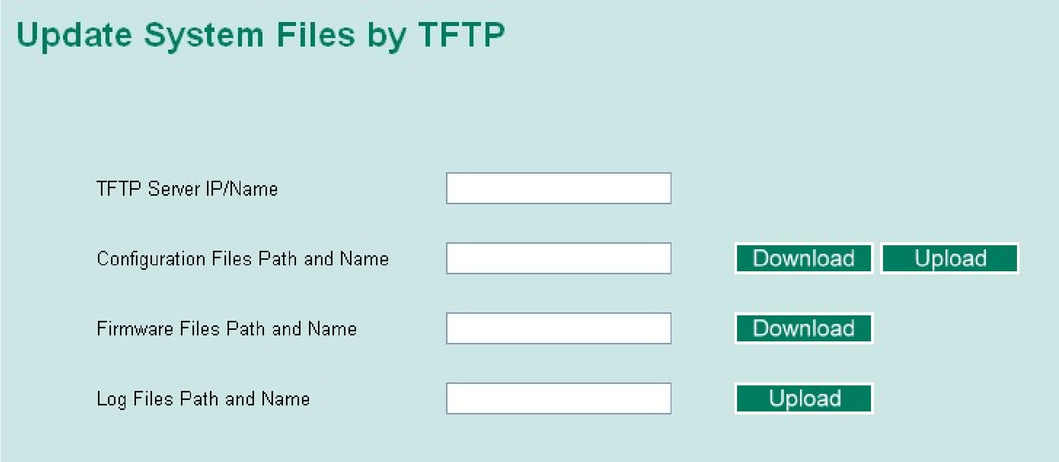
If the 4th DIP switch (Turbo Ring) is configured to ON, you will not be able to disable the Turbo Ring DIP switch from the web interface, console or Telnet.

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
Configuration Files Path and Name
Download
Upload
Firmware Files Path and Name
Download
Log Files Path and Name
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

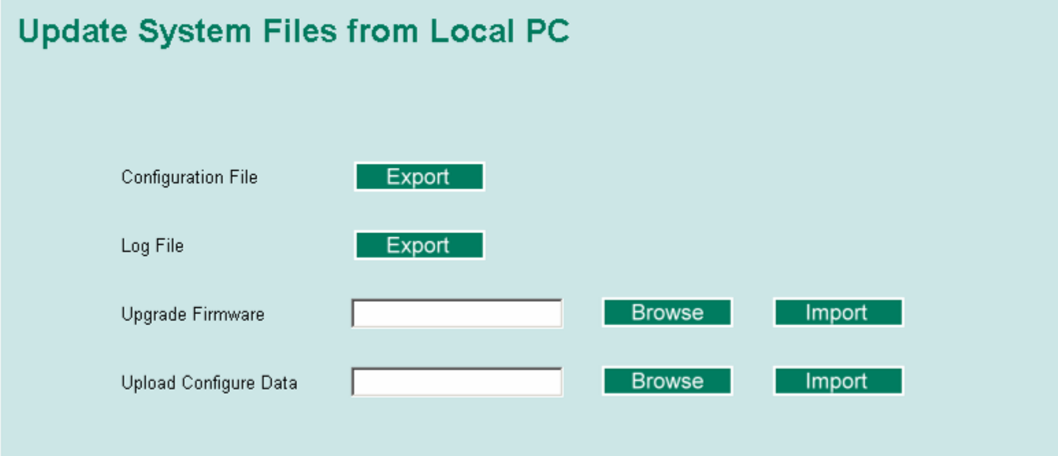
Setting	Description	Factory Default
Max. 40 characters	Specifies the path and file name of the VIPA switch's firmware file.	None

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

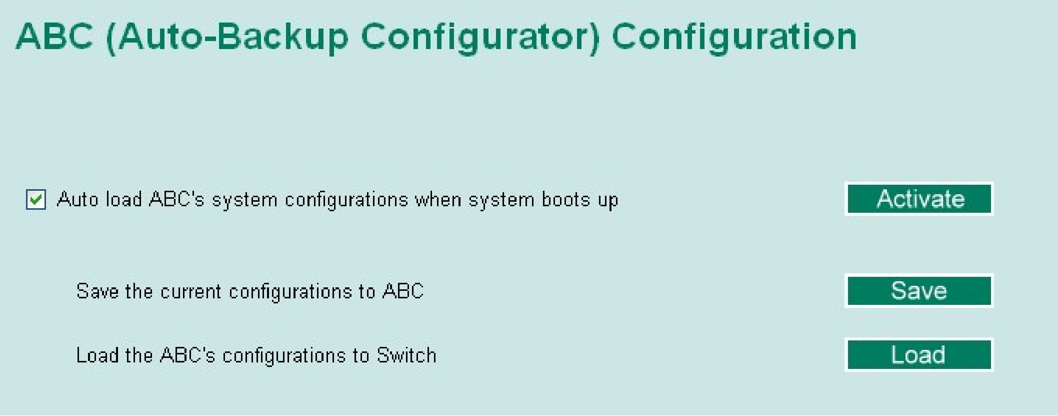
→ To import a new firmware file into the VIPA switch, click [Browse] to select the firmware file that is saved on your computer. The upgrade procedure will proceed automatically after clicking [Import].

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

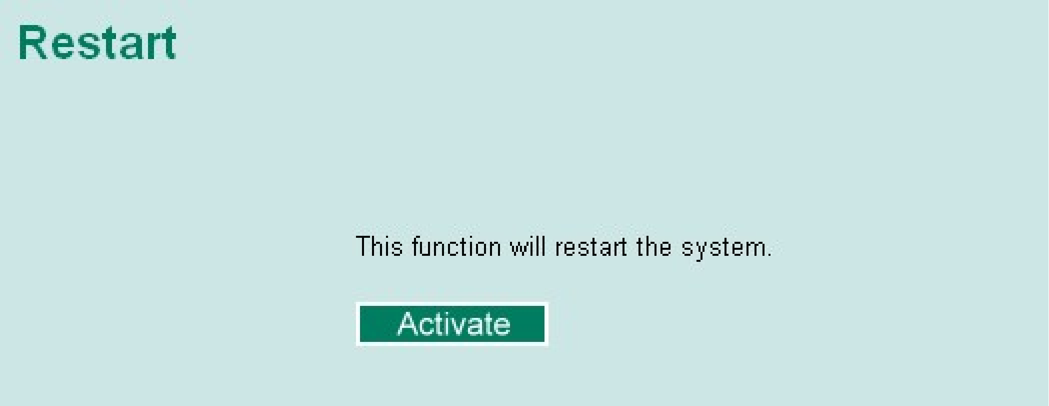
☑ Auto load ABC's system configurations when system boots up — Activate

Save the current configurations to ABC — Save

Load the ABC's configurations to Switch — Load

4.1.11 Restart

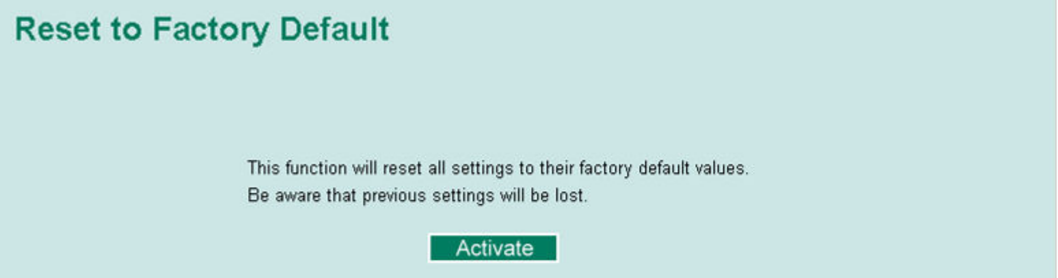
This function provides users with a quick way to restart the system.



Restart

This function will restart the system.

4.1.12 Reset to Factory Default



Reset to Factory Default

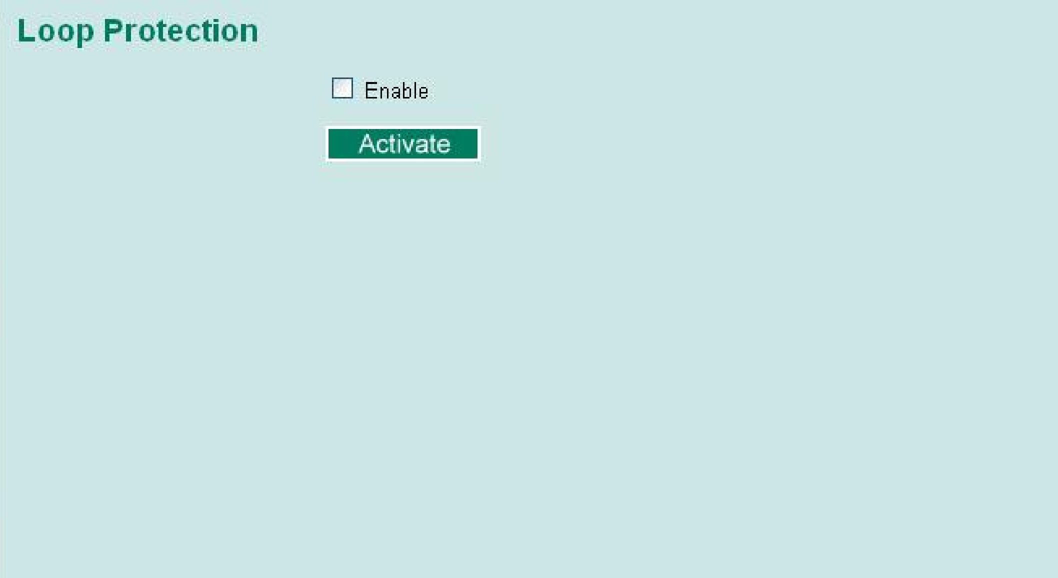
This function will reset all settings to their factory default values.
Be aware that previous settings will be lost.

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.

After restoring the factory default configuration, you will need to use the default network settings to re-establish the web or Telnet console connection with the VIPA switch.

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.



Loop Protection

□ Enable

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

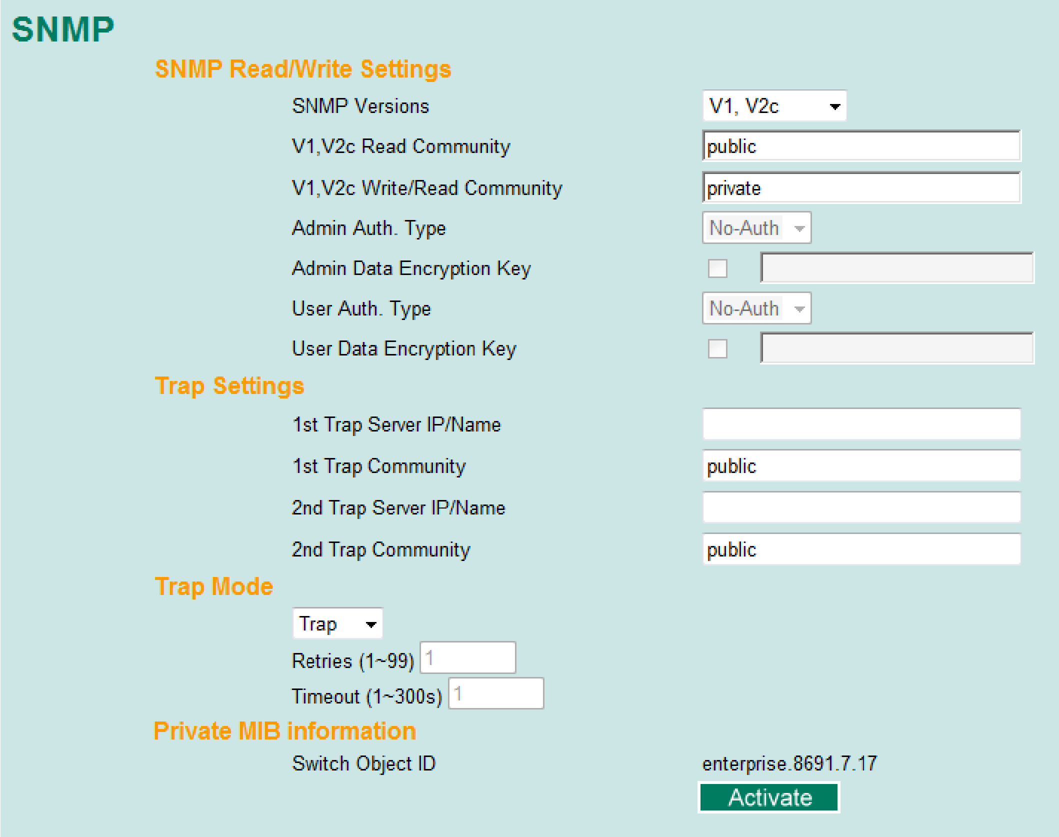
4.3 Configuring SNMP

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.

Protocol Version	UI Setting	Authentication	Encryption	Method
	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	public
V1,V2c Write/Read Community	private
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	public
2nd Trap Server IP/Name	
2nd Trap Community	public

Trap Mode

Trap

Retries (1~99) 1

Timeout (1~300s) 1

Private MIB information

Switch Object ID enterprise.8691.7.17

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)

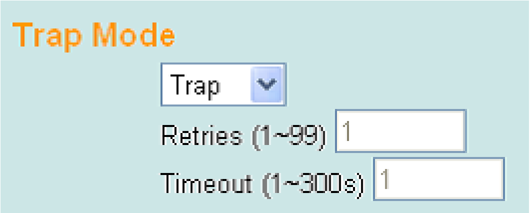
Setting	Description	Factory Default
Enable	Enables data encryption using the specified data encryption key (between 8 and 30 characters).	No
Disable	No data encryption	No

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.



Trap Mode

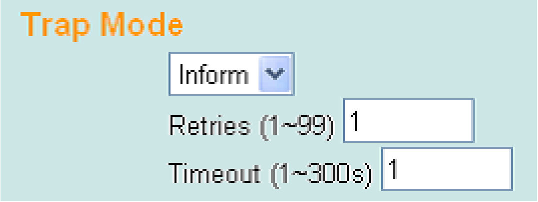
Trap

Retries (1~99) 1

Timeout (1~300s) 1

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.



Trap Mode

Inform

Retries (1~99) 1

Timeout (1~300s) 1

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 controlled 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

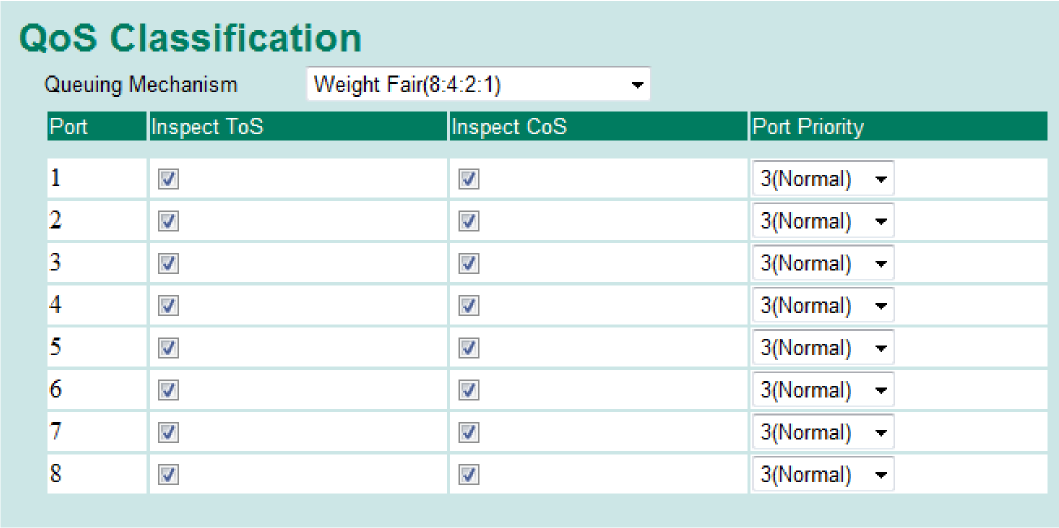
The hardware of VIPA switches has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the VIPA switch without being delayed by lower priority traffic. As each packet arrives in the VIPA switch, it passes through any ingress processing (which includes 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	☑	☑	3(Normal)
2	☑	☑	3(Normal)
3	☑	☑	3(Normal)
4	☑	☑	3(Normal)
5	☑	☑	3(Normal)
6	☑	☑	3(Normal)
7	☑	☑	3(Normal)
8	☑	☑	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:

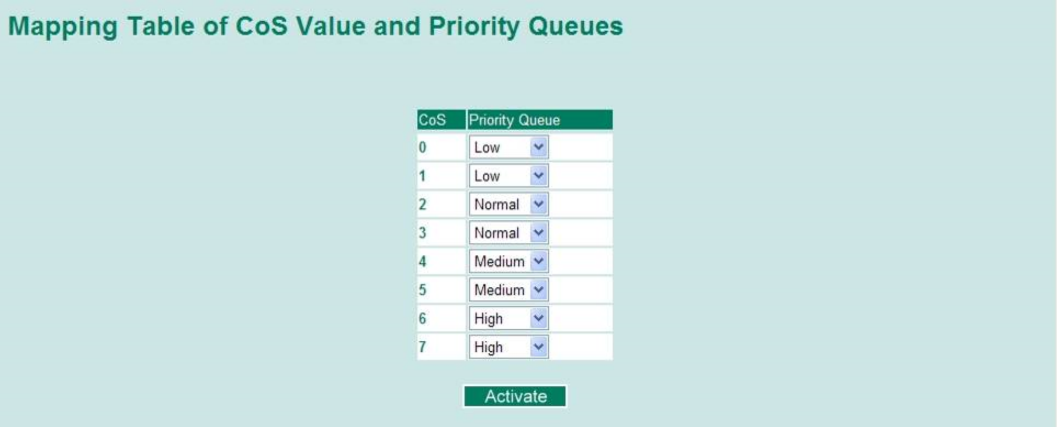
1. Inspect TOS

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



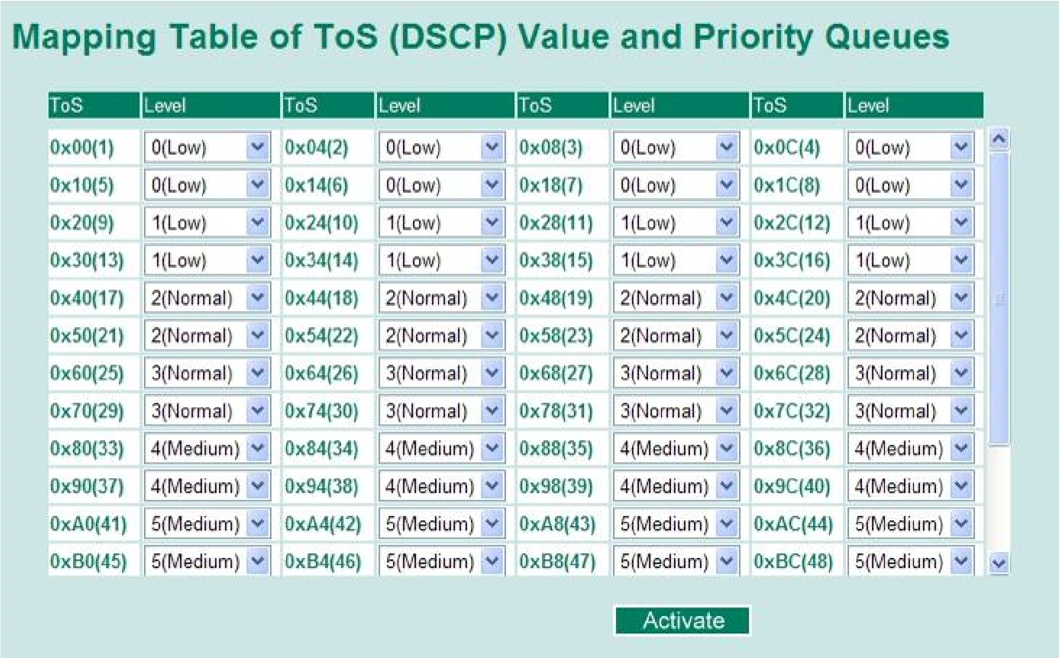
Mapping Table of CoS Value and Priority Queues

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

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)

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?

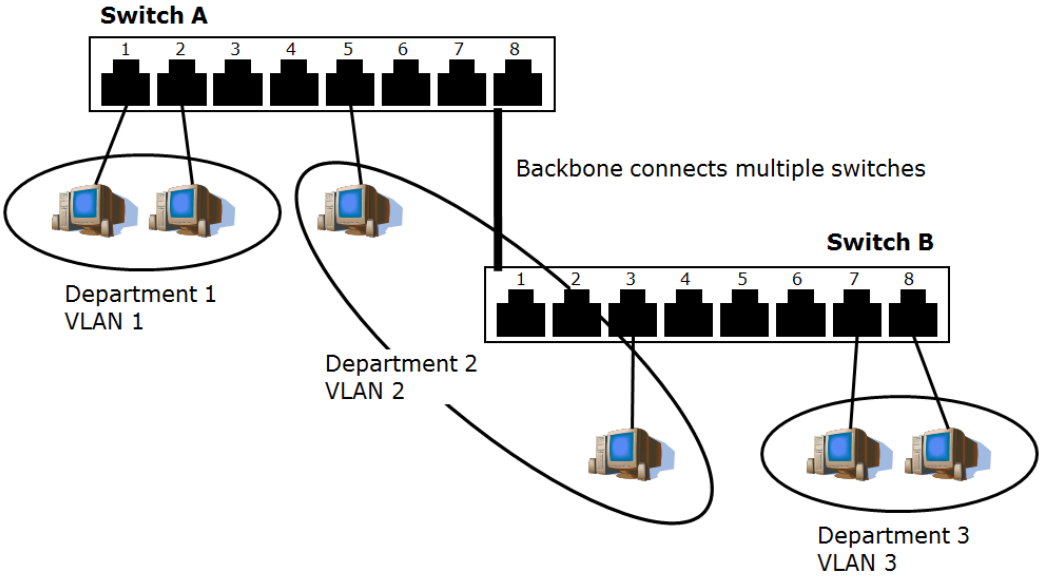
A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections-a limitation of traditional network design. With VLANs you can segment your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

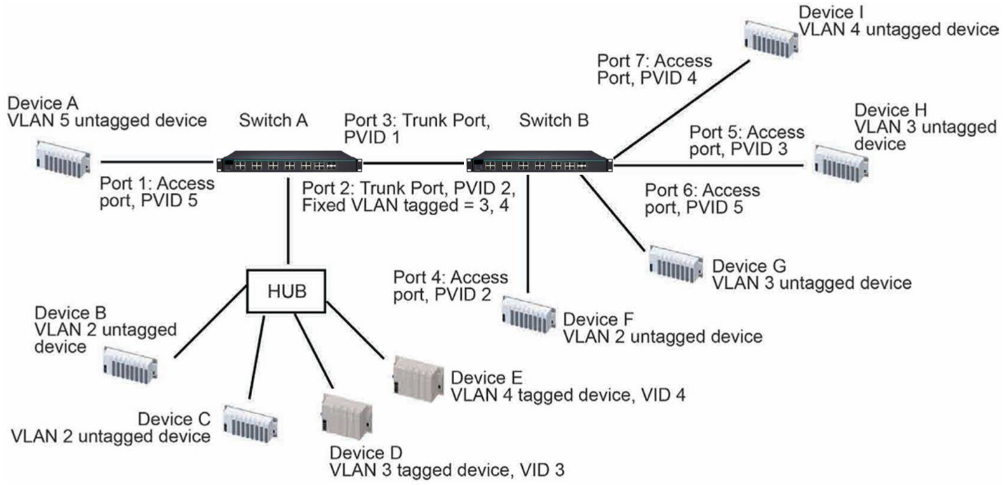
  The port connects to a single device that is not tagged. The user must define the default port PVID that assigns which VLAN the device belongs to. Once the ingress packet of this Access Port egresses to another Trunk Port (the port needs all packets to carry tag information), the VIPA switch will insert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

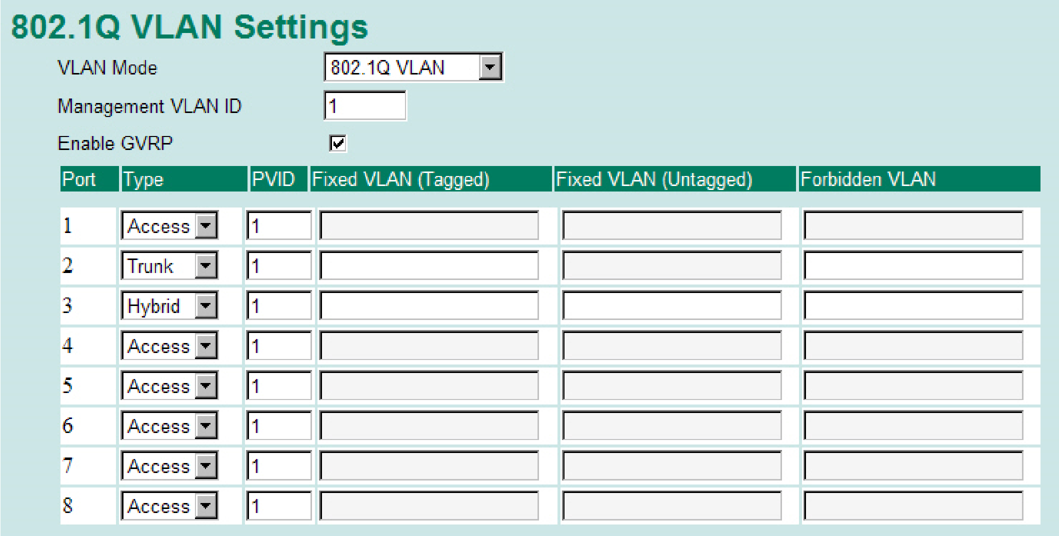
4.5.3 VLAN Settings

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			

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)

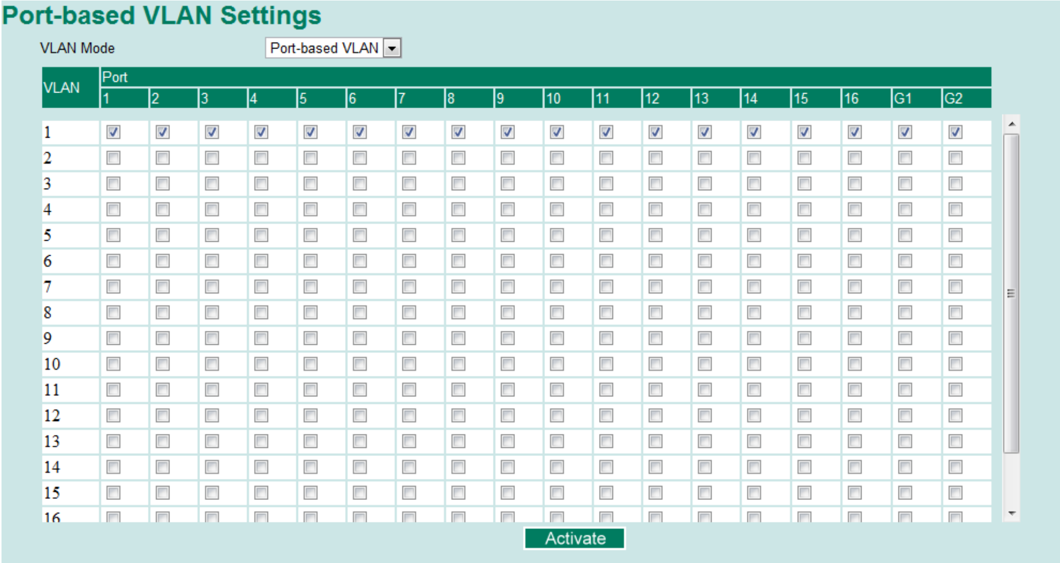
Setting	Description	Factory Default
VID range from 1 to 4094	This field will be active only when selecting the Hybrid port type. Set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs.	None

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.



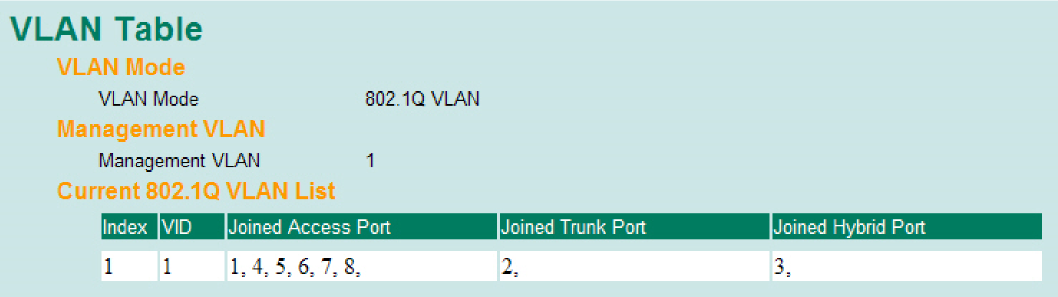
Port-based VLAN Settings

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	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
11	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
12	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
13	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
14	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
15	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
16	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

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

4.5.4 VLAN Table



VLAN Table

VLAN Mode

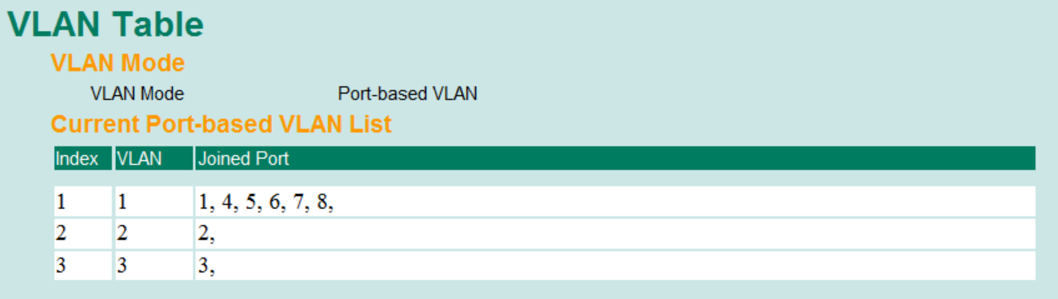
VLAN Mode 802.1Q VLAN

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.

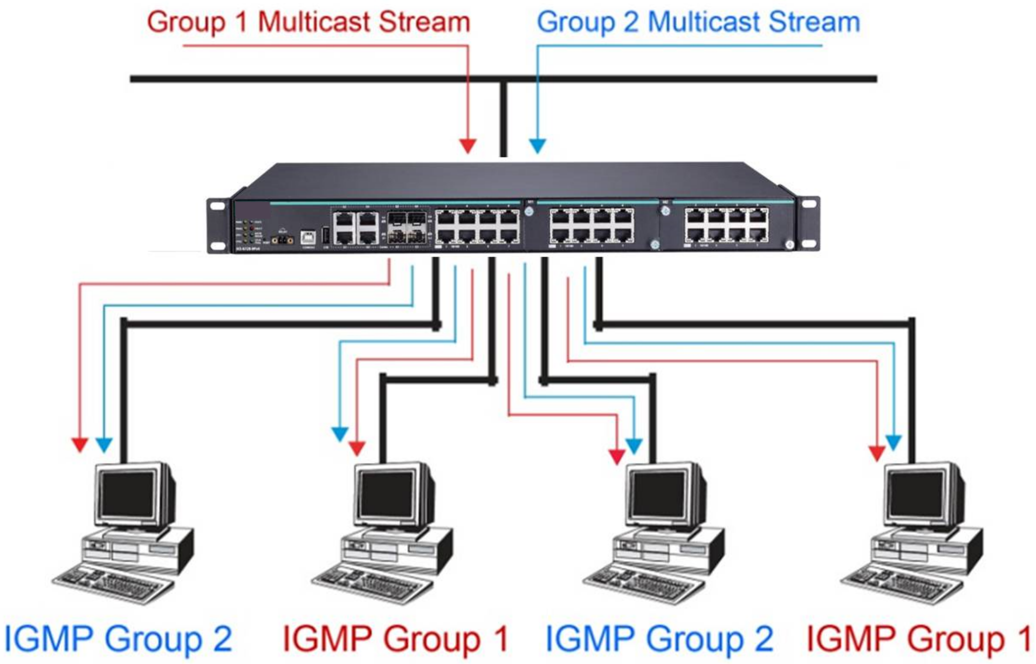
- It makes efficient use of network bandwidth and scales well as the number of multicast group members increases.
- Works with other IP protocols and services, such as Quality of Service (QoS).

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

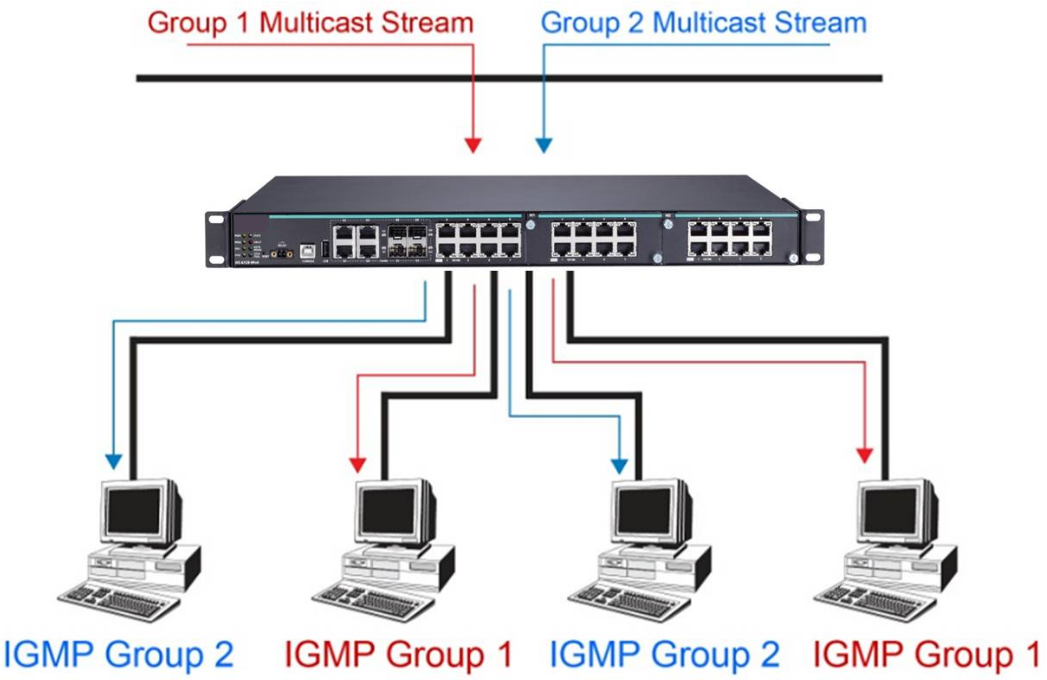
Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves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



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

Multicast Filtering and VIPA's Industrial Rackmount 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

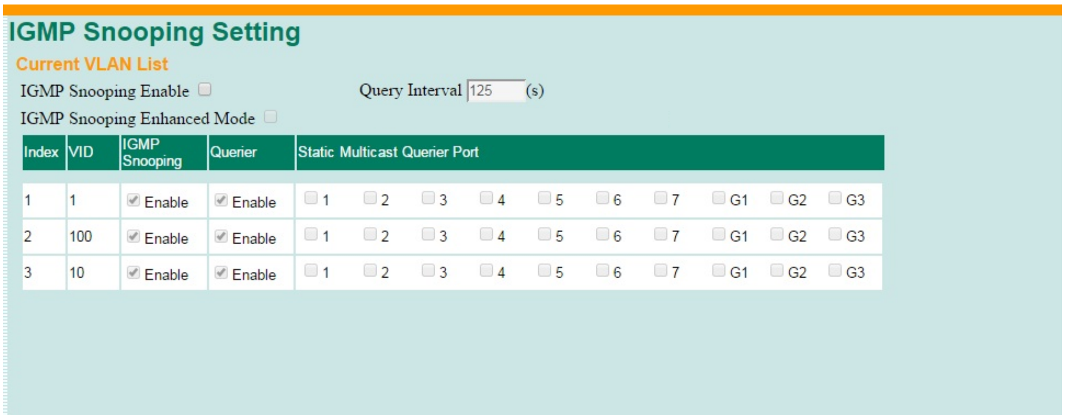
Use the serial console or web interface to enable or disable IGMP Snooping and IGMP querying. If IGMP Snooping is not enabled, then IP multicast traffic is always forwarded, flooding the network.

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 Setting

Current VLAN List

IGMP Snooping Enable □   Query Interval 125 (s)

IGMP Snooping Enhanced Mode □

Index	VID	IGMP Snooping	Querier	Static Multicast Querier Port									
1	1	☑ Enable	☑ Enable	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ G1	□ G2	□ G3
2	100	☑ Enable	☑ Enable	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ G1	□ G2	□ G3
3	10	☑ Enable	☑ Enable	□ 1	□ 2	□ 3	□ 4	□ 5	□ 6	□ 7	□ G1	□ G2	□ G3

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: ■ Auto-Learned Multicast Querier Ports ■ Member Ports	Disable

Setting	Description	Factory Default
Disable	IGMP Multicast packets will be forwarded to: ■ 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

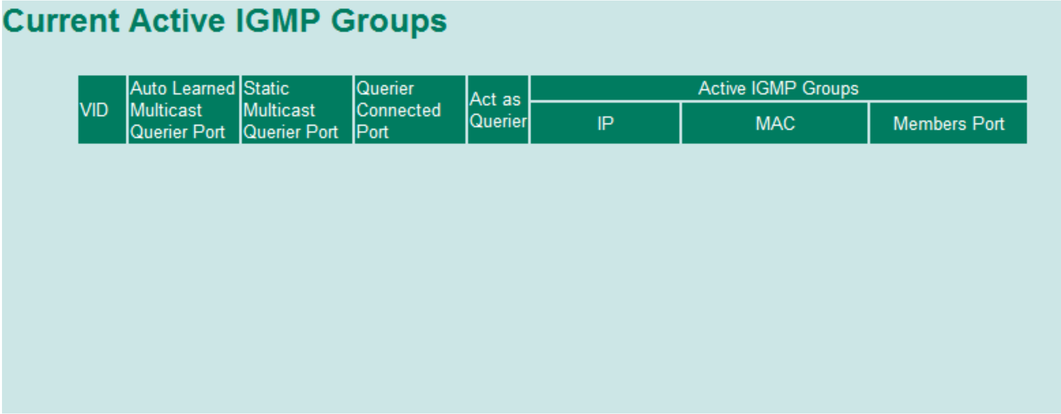
If a router or layer 3 switch is connected to the network, it will act as the Querier, and consequently this Querier option will be disabled on all VIPA layer 2 switches.

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

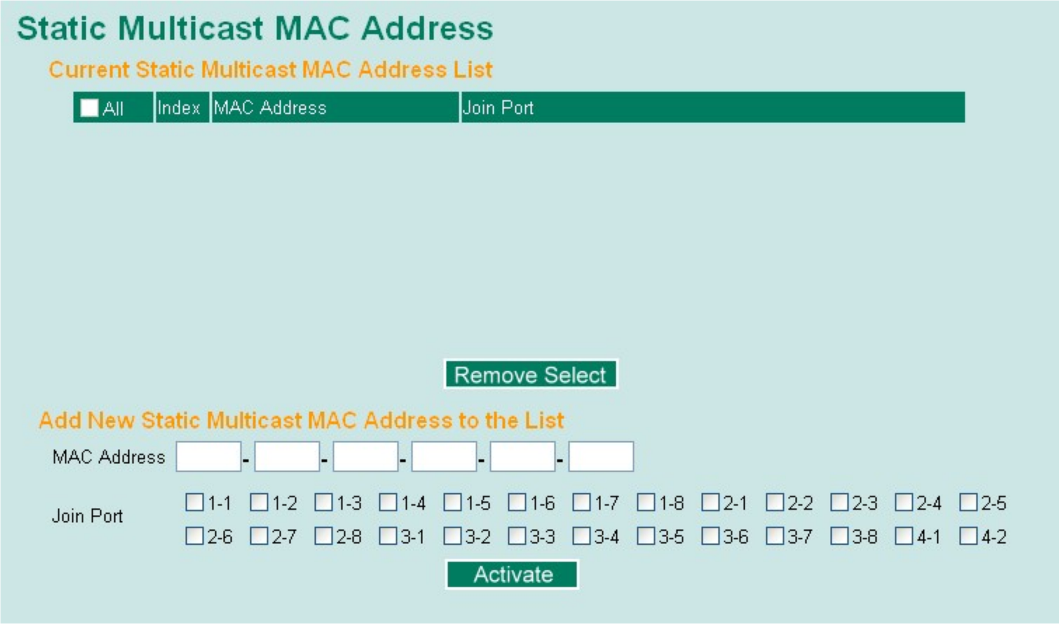


Current Active IGMP Groups

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



Static Multicast MAC Address

Current Static Multicast MAC Address List

□ All	Index	MAC Address	Join Port

Remove Select

Add New Static Multicast MAC Address to the List

MAC Address ▭ - ▭ - ▭ - ▭ - ▭ - ▭

Join Port □1-1 □1-2 □1-3 □1-4 □1-5 □1-6 □1-7 □1-8 □2-1 □2-2 □2-3 □2-4 □2-5
□2-6 □2-7 □2-8 □3-1 □3-2 □3-3 □3-4 □3-5 □3-6 □3-7 □3-8 □4-1 □4-2

Activate

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

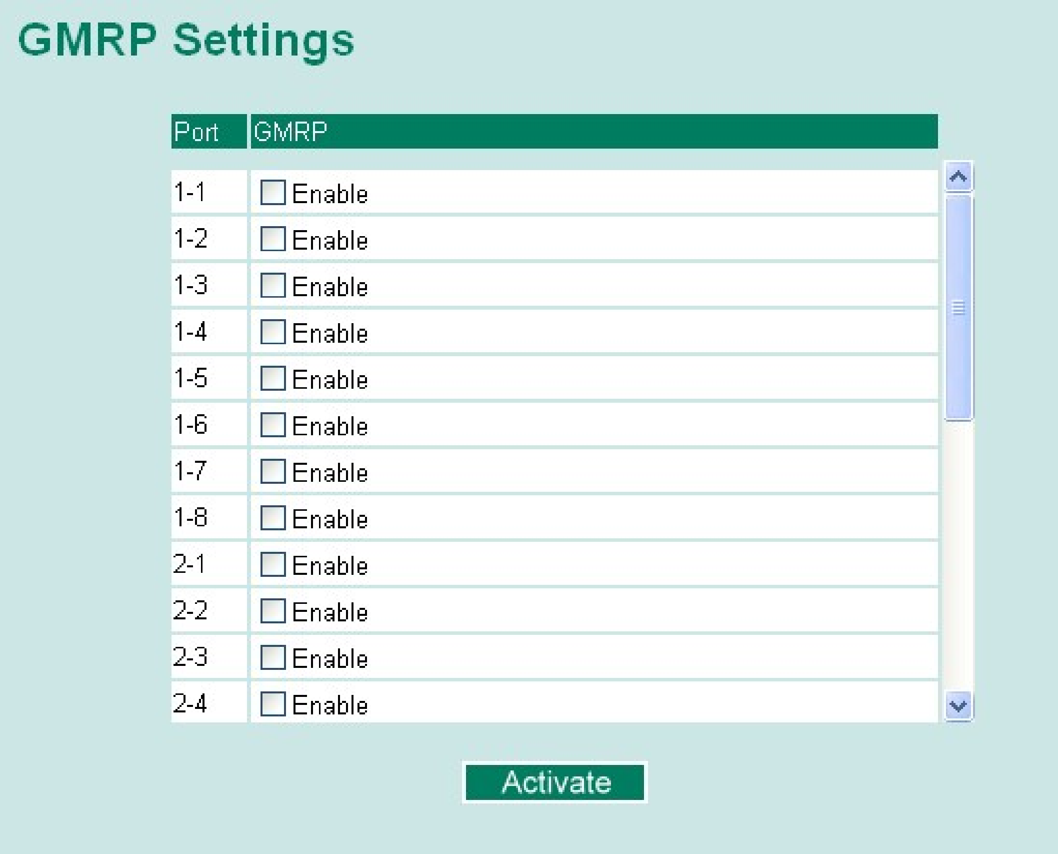
Setting	Description	Factory Default
Integer	Input the number of the VLAN that the host with this MAC address belongs to.	None

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 Settings

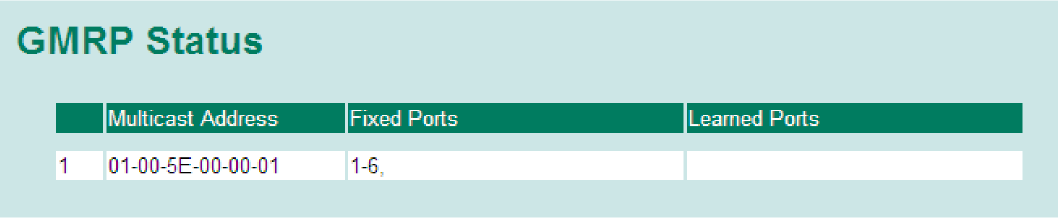
Port	GMRP
1-1	☐ Enable
1-2	☐ Enable
1-3	☐ Enable
1-4	☐ Enable
1-5	☐ Enable
1-6	☐ Enable
1-7	☐ Enable
1-8	☐ Enable
2-1	☐ Enable
2-2	☐ Enable
2-3	☐ Enable
2-4	☐ Enable

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



GMRP Status

	Multicast Address	Fixed Ports	Learned Ports
1	01-00-5E-00-00-01	1-6,	

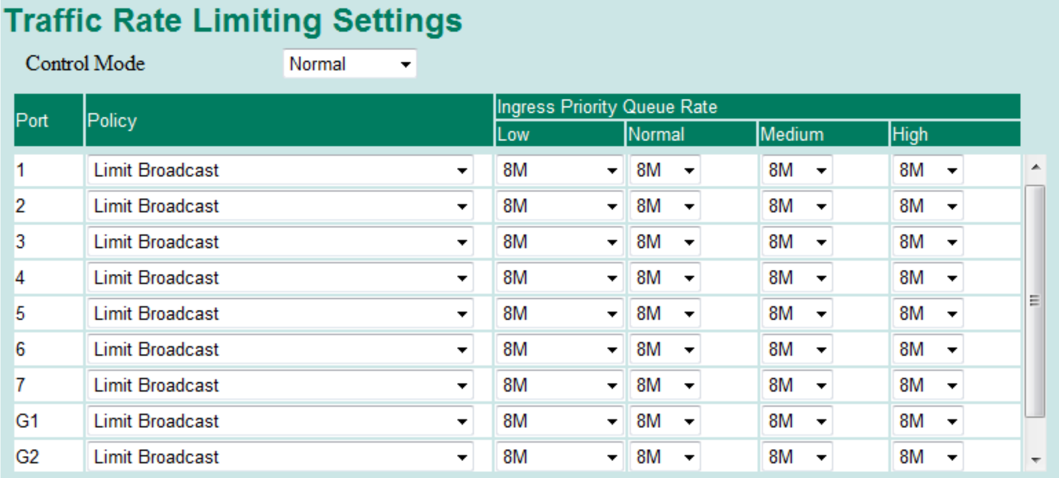
Setting	Description
Fixed Ports	This multicast address is defined by static multicast.
Learned Ports	This multicast address is learned by GMRP.

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

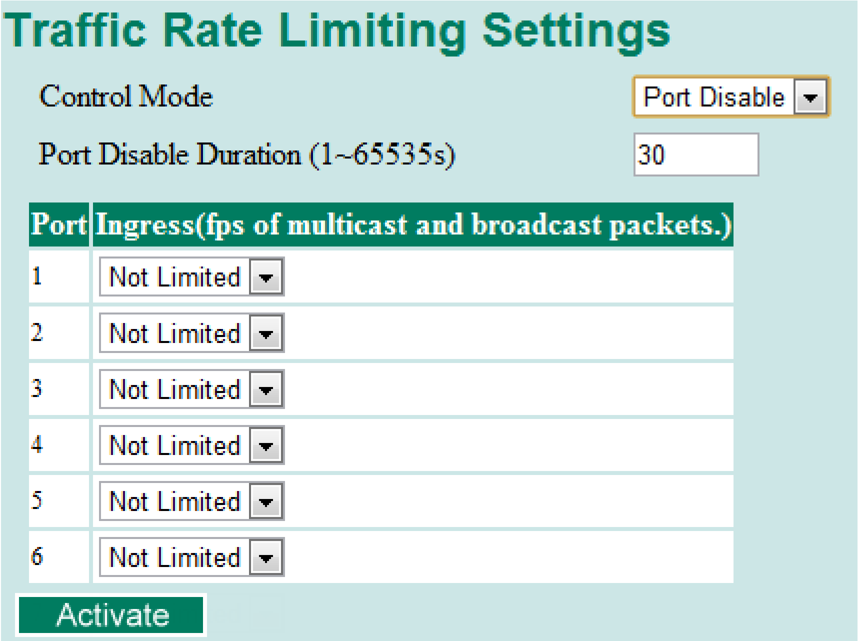
Port	Policy	Ingress Priority Queue Rate			
		Low	Normal	Medium	High
1	Limit Broadcast	8M	8M	8M	8M
2	Limit Broadcast	8M	8M	8M	8M
3	Limit Broadcast	8M	8M	8M	8M
4	Limit Broadcast	8M	8M	8M	8M
5	Limit Broadcast	8M	8M	8M	8M
6	Limit Broadcast	8M	8M	8M	8M
7	Limit Broadcast	8M	8M	8M	8M
G1	Limit Broadcast	8M	8M	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

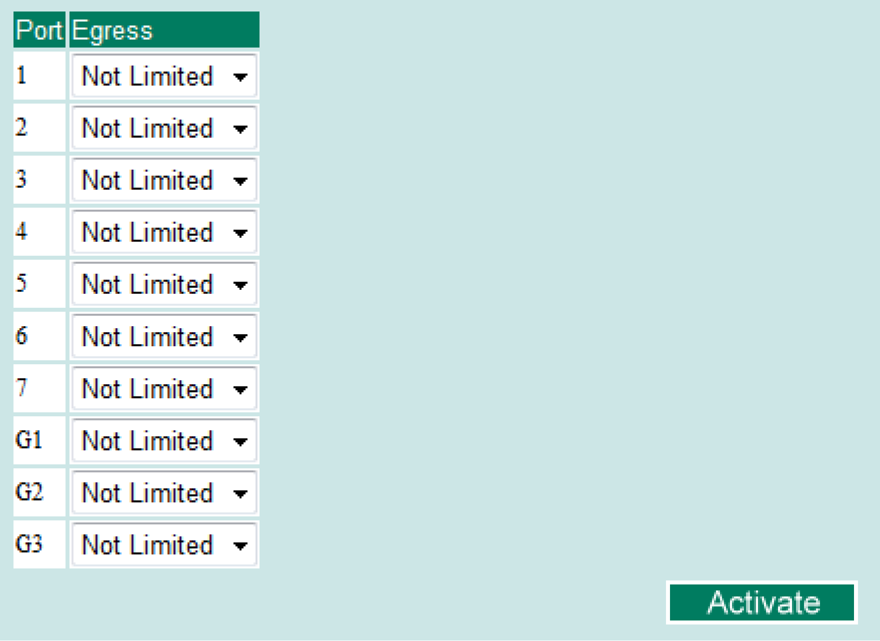
Port Disable Duration (1~65535s): 30

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

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

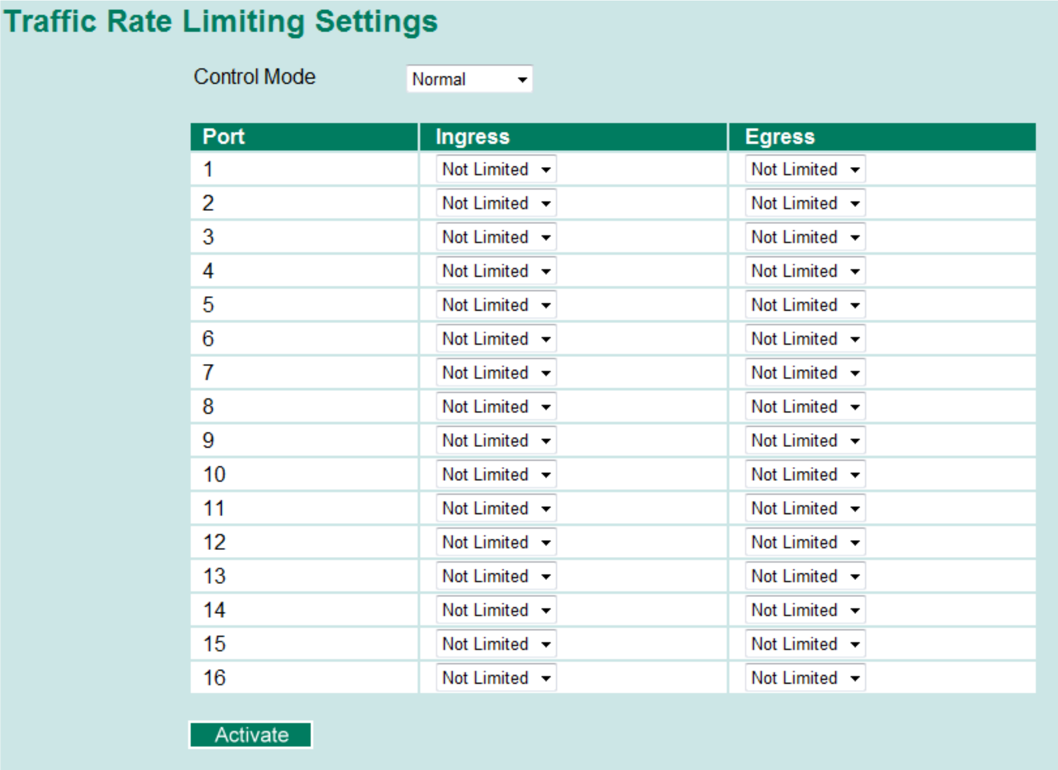
Egress Rate Limit



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

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



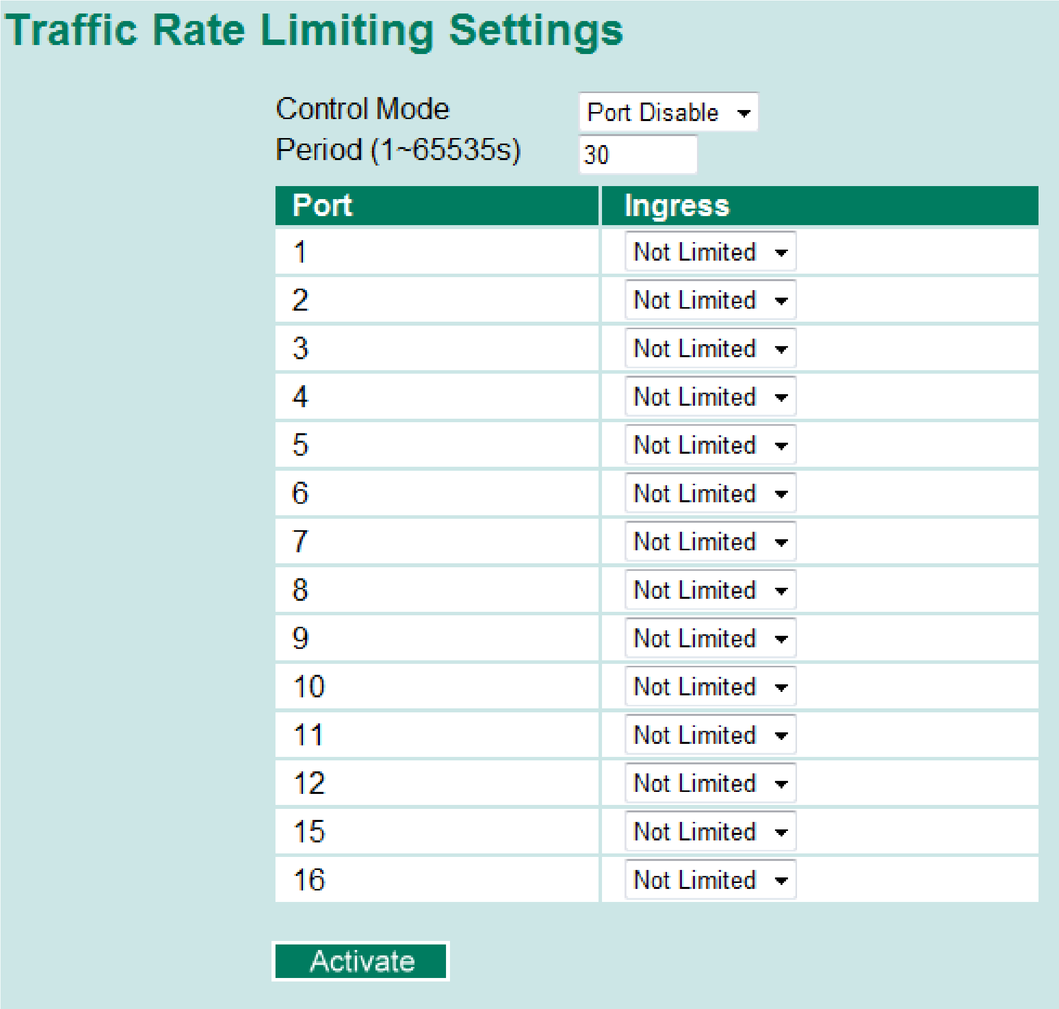
Traffic Rate Limiting Settings

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

Ingress and Egress Rate Limit - Normal

Setting	Description	Factory Default
Ingress rate Egress 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



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

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).

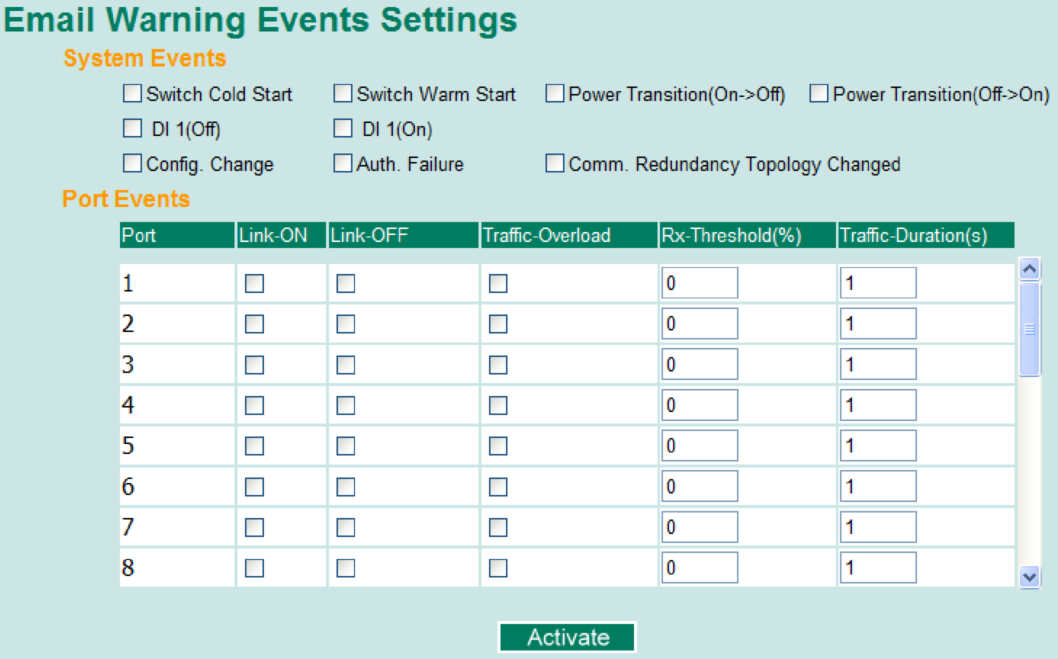
2. **Configure Email Settings**

   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



Email Warning Events Settings

System Events

□ Switch Cold Start □ Switch Warm Start □ Power Transition(On->Off) □ Power Transition(Off->On)

□ DI 1(Off) □ DI 1(On)

□ Config. Change □ Auth. Failure □ Comm. Redundancy Topology Changed

Port Events

Port	Link-ON	Link-OFF	Traffic-Overload	Rx-Threshold(%)	Traffic-Duration(s)
1	□	□	□	0	1
2	□	□	□	0	1
3	□	□	□	0	1
4	□	□	□	0	1
5	□	□	□	0	1
6	□	□	□	0	1
7	□	□	□	0	1
8	□	□	□	0	1

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
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.

System Events	Warning e-mail is sent when…
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.

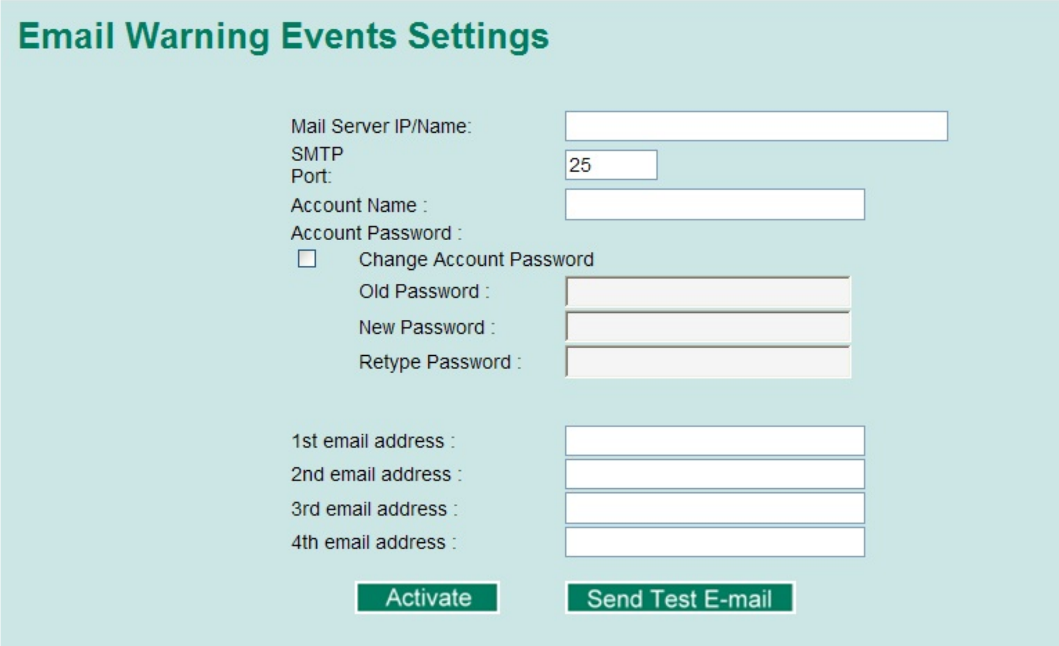
The Traffic-Overload, Traffic-Threshold (%), and Traffic-Duration (sec.) Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a nonzero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

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



Email Warning Events Settings

Mail Server IP/Name:	
SMTP Port:	25
Account Name :	
Account Password :	
□ Change Account Password	
Old Password :	
New Password :	
Retype Password :	
1st email address :	
2nd email address :	
3rd email address :	
4th email address :	

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 charters	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:

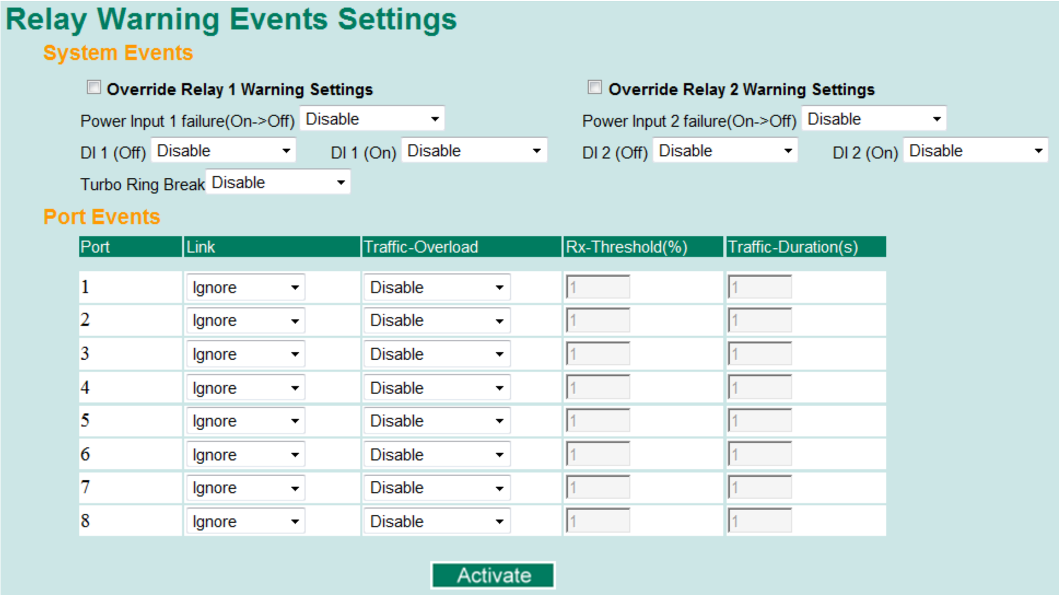
1. **Configure Relay Event Types**

   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

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.

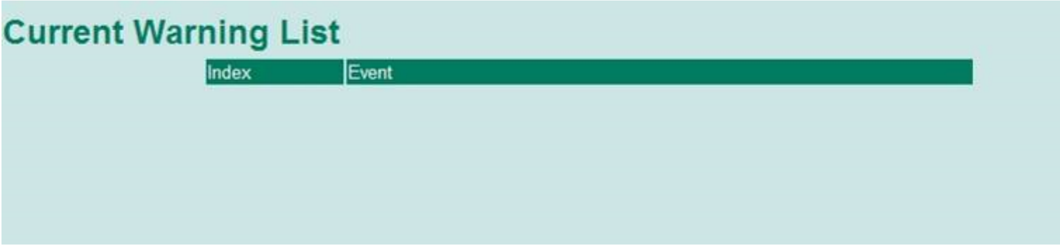
Override relay alarm settings

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.



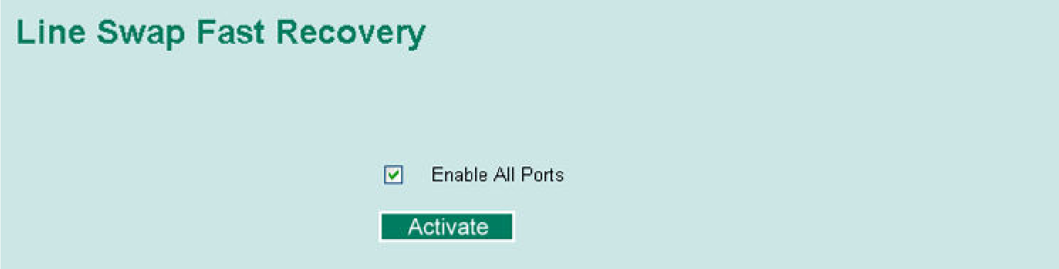
Current Warning List

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



Line Swap Fast Recovery

☑ Enable All Ports

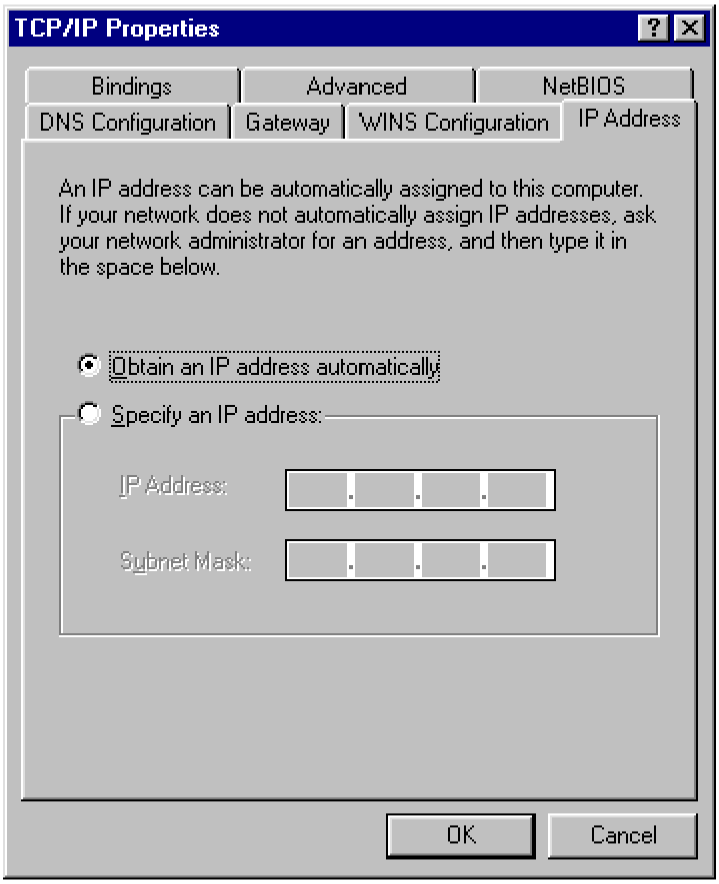
Enable Line-Swap-Fast-Recovery

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:



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

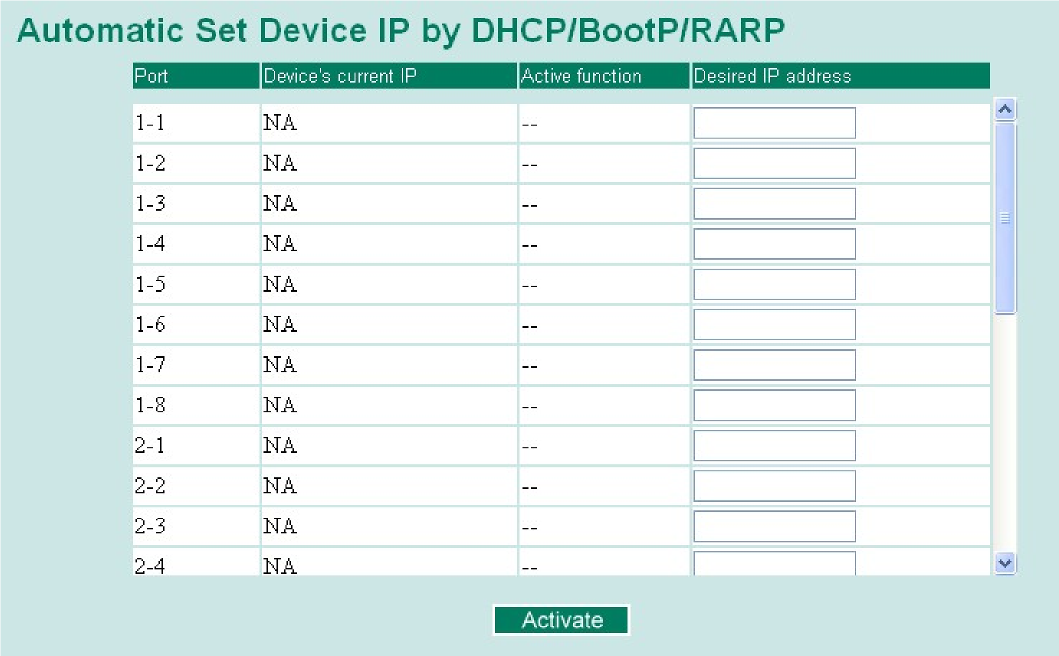
IP Address: . . .

Subnet Mask: . . .

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	--	
1-2	NA	--	
1-3	NA	--	
1-4	NA	--	
1-5	NA	--	
1-6	NA	--	
1-7	NA	--	
1-8	NA	--	
2-1	NA	--	
2-2	NA	--	
2-3	NA	--	
2-4	NA	--	

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

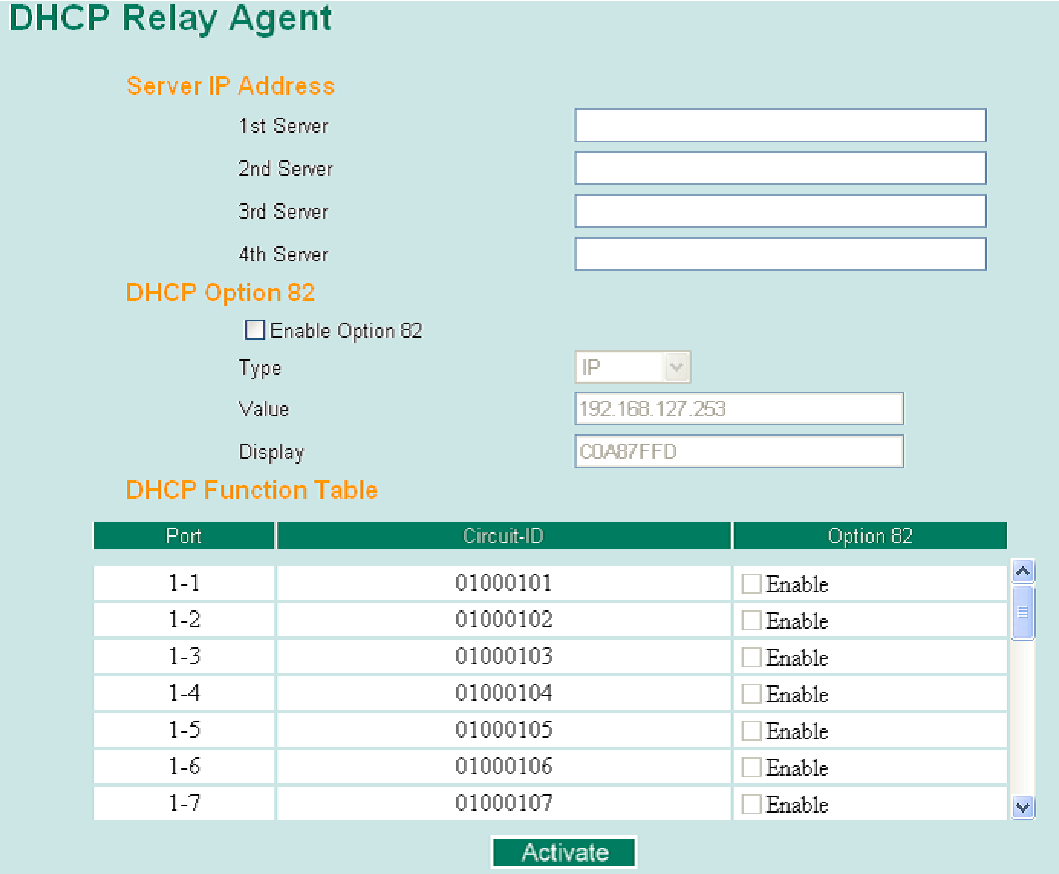
This is where the first byte FF is fixed to "01", the second and the third byte VV-VV is formed by the port VLAN ID in hex, and the last byte PP is formed by the port number in hex. For example:

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.

Using Set Device IP > Configuring DHCP Relay Agent



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	□ Enable
1-2	01000102	□ Enable
1-3	01000103	□ Enable
1-4	01000104	□ Enable
1-5	01000105	□ Enable
1-6	01000106	□ Enable
1-7	01000107	□ Enable

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

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

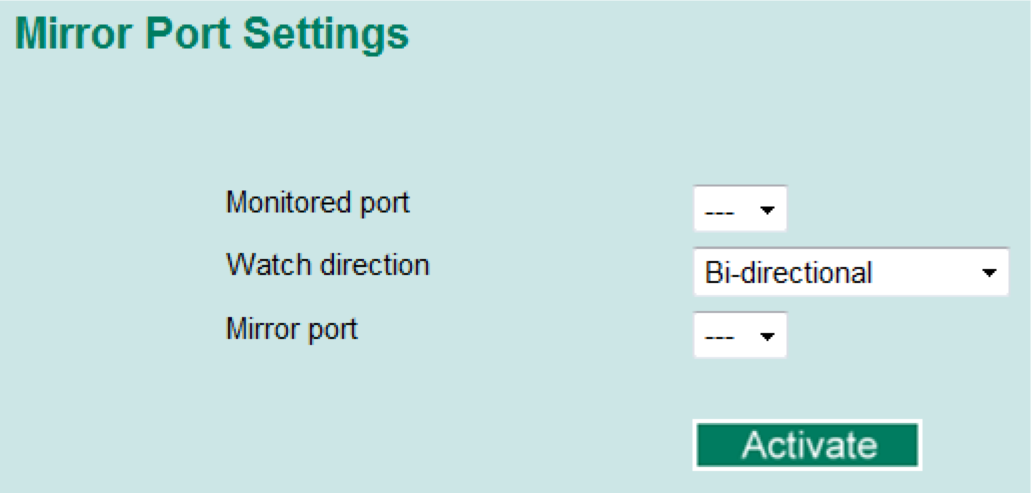
Setting	Description	Factory Default
Enable or Disable	Enable or disable the DHCP Option 82 function for this port.	Disable

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.



Monitored port ---

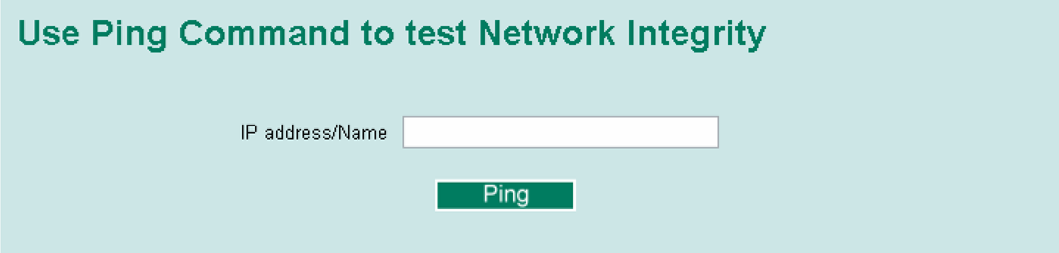
Watch direction Bi-directional

Mirror port ---

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: ■ *Input data stream:* Select this option to monitor only those data packets coming into the VIPA switch's port. ■ *Output data stream:* Select this option to monitor only those data packets being sent out through the VIPA switch's port. ■ *Bi-directional:* 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.

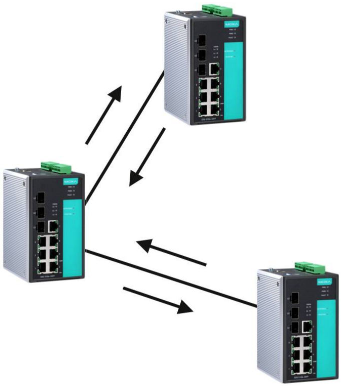
4.11.2 Ping



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.

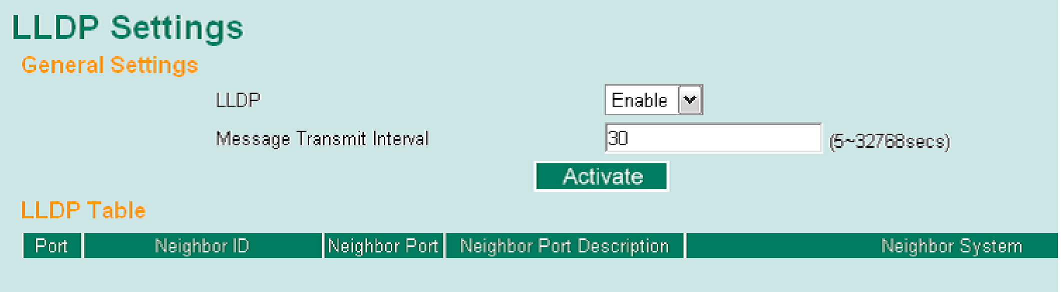
4.11.3 LLDP Function

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



LLDP Settings

General Settings

LLDP: Enable

Message Transmit Interval: 30 (5~32768secs)

LLDP Table

Port	Neighbor ID	Neighbor Port	Neighbor Port Description	Neighbor System

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.

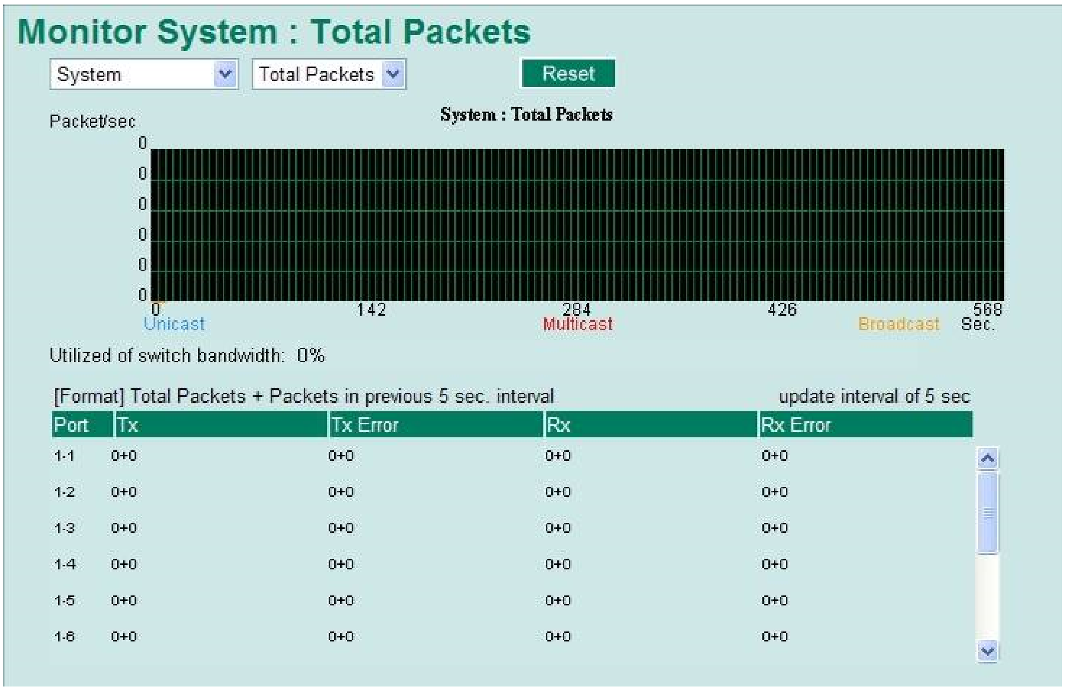
4.12.1 Monitor by Switch

1. 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.

2. 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.



Utilized of switch bandwidth: 0%

[Format] Total Packets + Packets in previous 5 sec. interval

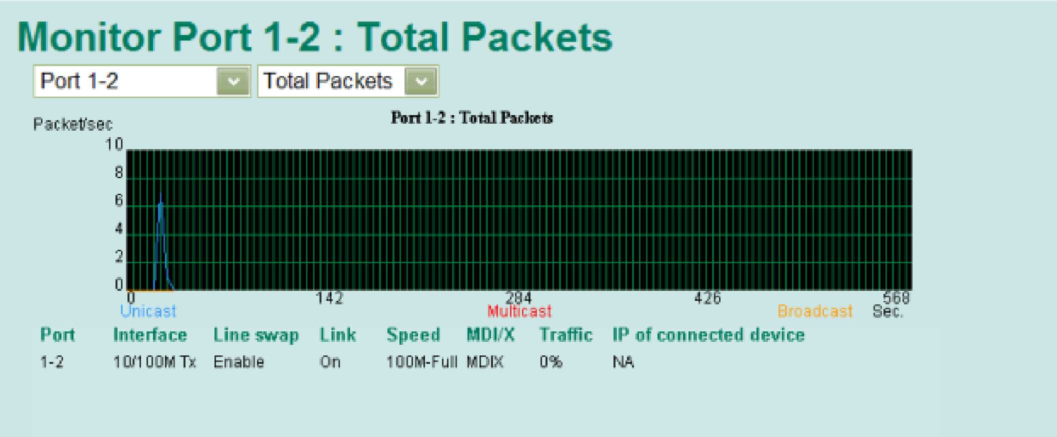
update interval of 5 sec

Port	Tx	Tx Error	Rx	Rx Error
1-1	0+0	0+0	0+0	0+0
1-2	0+0	0+0	0+0	0+0
1-3	0+0	0+0	0+0	0+0
1-4	0+0	0+0	0+0	0+0
1-5	0+0	0+0	0+0	0+0
1-6	0+0	0+0	0+0	0+0

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.



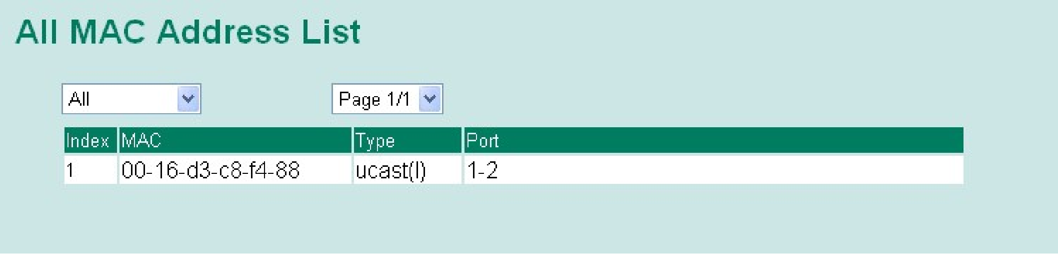
Monitor Port 1-2 : Total Packets

Port 1-2 | Total Packets

Port	Interface	Line swap	Link	Speed	MDI/X	Traffic	IP of connected device
1-2	10/100M Tx	Enable	On	100M-Full	MDIX	0%	NA

4.13 Using the MAC Address Table

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



All MAC Address List

All | Page 1/1

Index	MAC	Type	Port
1	00-16-d3-c8-f4-88	ucast(l)	1-2

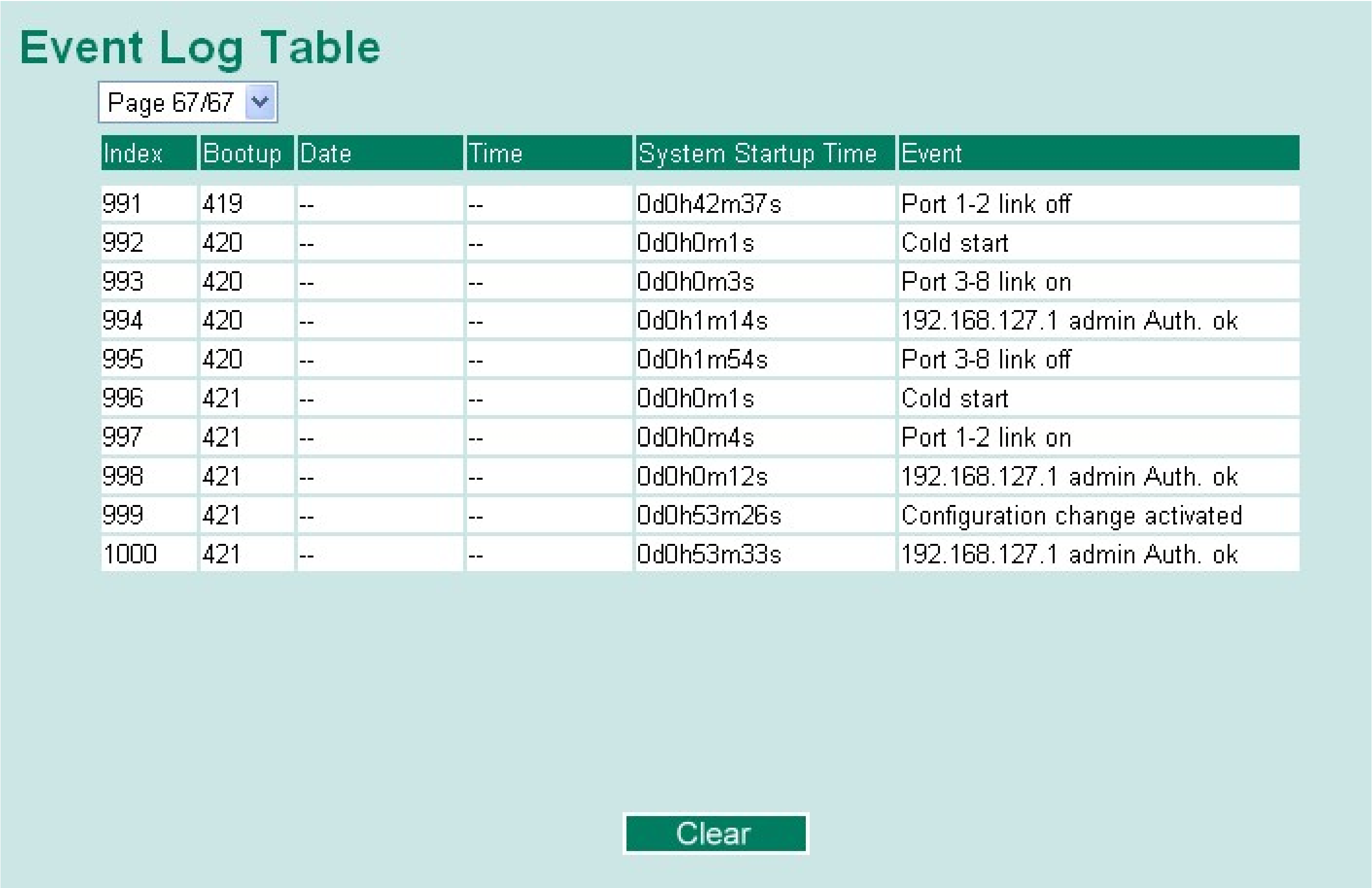
The MAC Address table can be configured to display the following VIPA switch MAC address groups, which are selected from the drop-down list:

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

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

Event Log Table

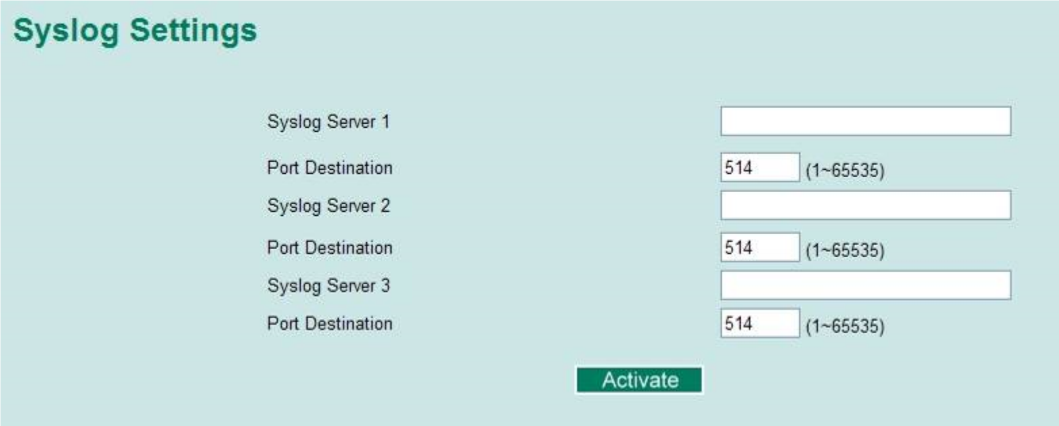
Setting	Description
Bootup	This field shows how many times the VIPA switch has been rebooted or cold started.
Date	The date is updated based on how the current date is set in the Basic Setting page.
Time	The time is updated based on how the current time is set in the Basic Setting page.
System Startup 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	
Port Destination	514 (1~65535)
Syslog Server 2	
Port Destination	514 (1~65535)
Syslog Server 3	
Port Destination	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.

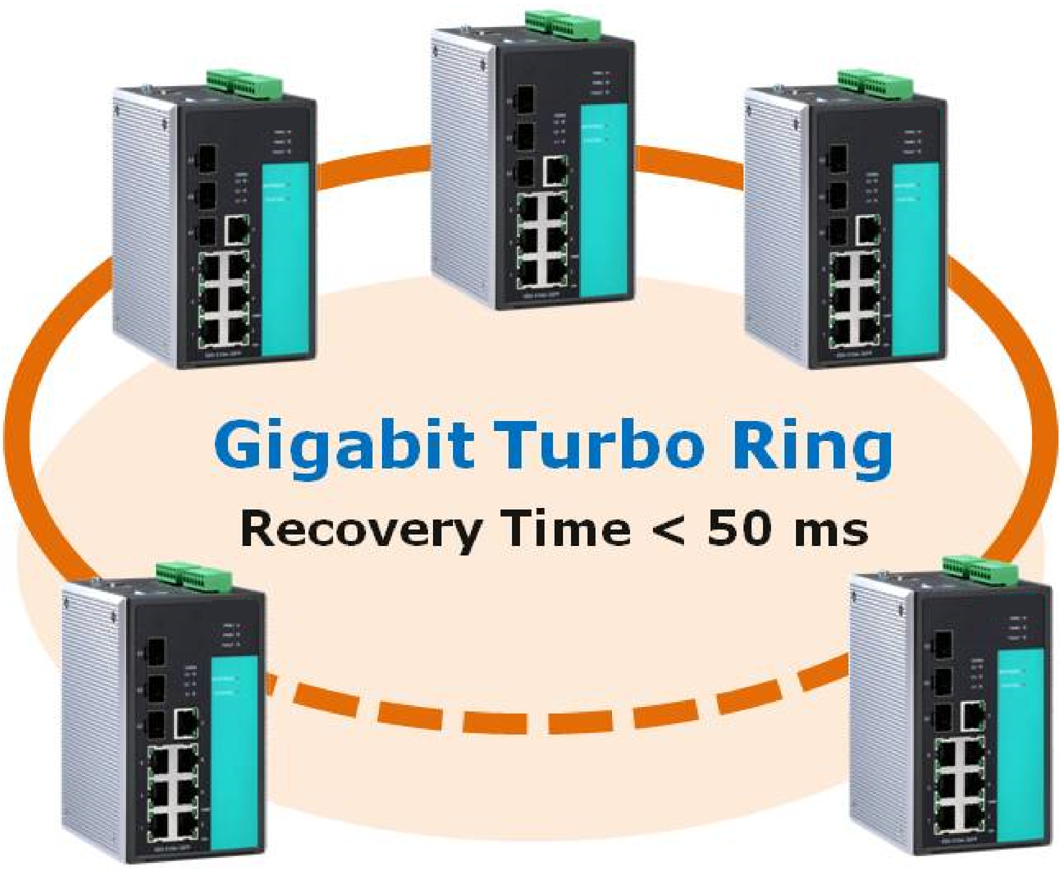
	Turbo Ring	Turbo Ring V2	Turbo Chain	STP	RSTP
Topology	Ring	Ring	Chain	Ring, Mesh	Ring, Mesh
Fast Ethernet Recovery Time	< 300 ms	< 20 ms	< 20 ms	Up to 30 sec.	Up to 5 sec.
Gigabit Ethernet Recovery Time		< 50 ms	< 50 ms		

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

- *Turbo Ring refers to the original version of 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 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.*

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).

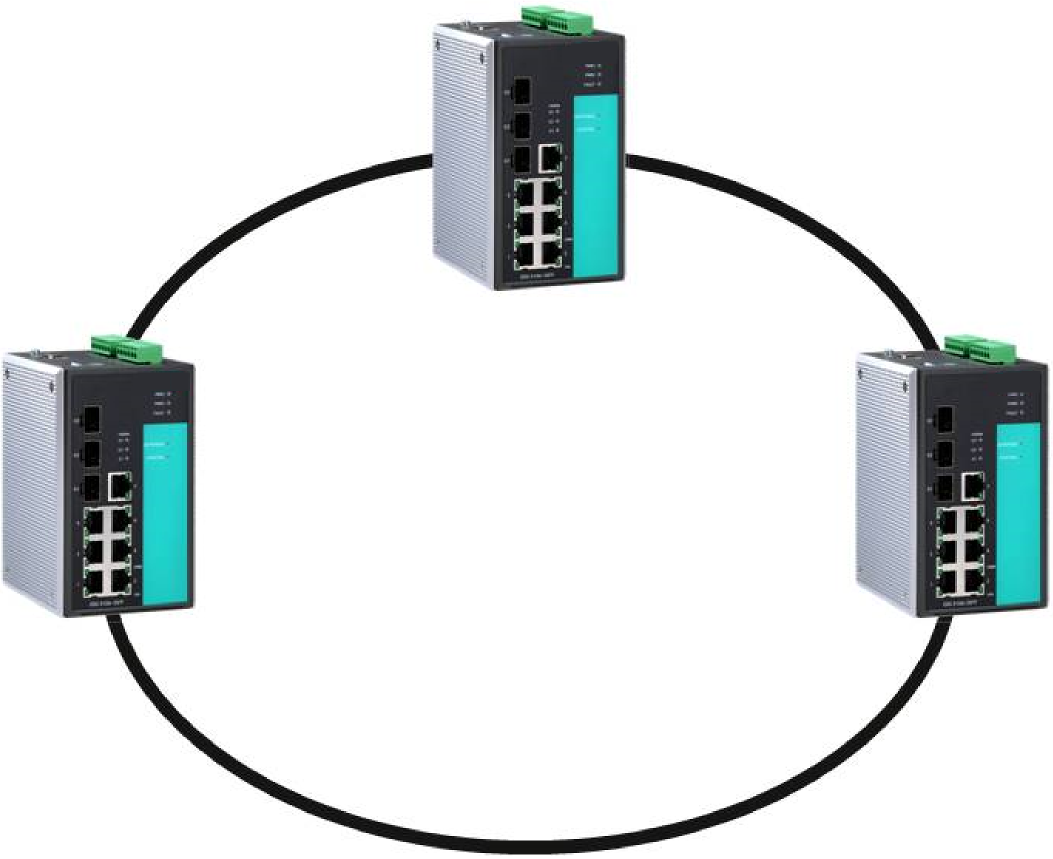
> *Port trunking and Turbo Ring can be enabled simultaneously to form a backbone. Doing so will increase the bandwidth of the backbone, and also provide redundancy. For example, suppose that two physical ports, 1 and 2, are trunked to form trunk group Trk1, and then Trk1 is set as one Turbo Ring path. 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

The proprietary Turbo Ring protocol optimizes communication redundancy and achieves 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.

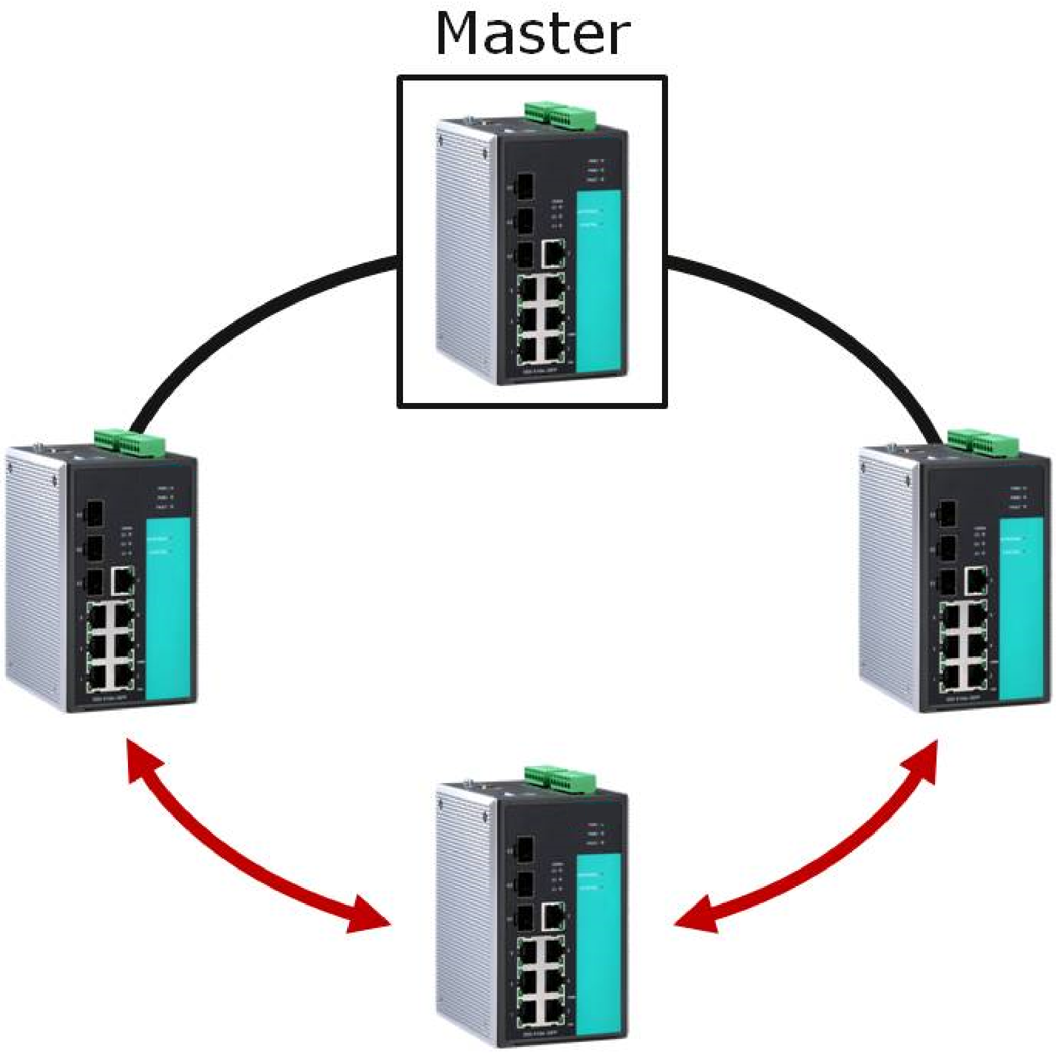
The user does not need to configure any of the switches as the master to use Turbo Ring or Turbo Ring V2. If none of the switches in the ring is configured as the **master**, then the protocol will automatically assign master status to one of the switches. In fact, the master is only used to identify 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.

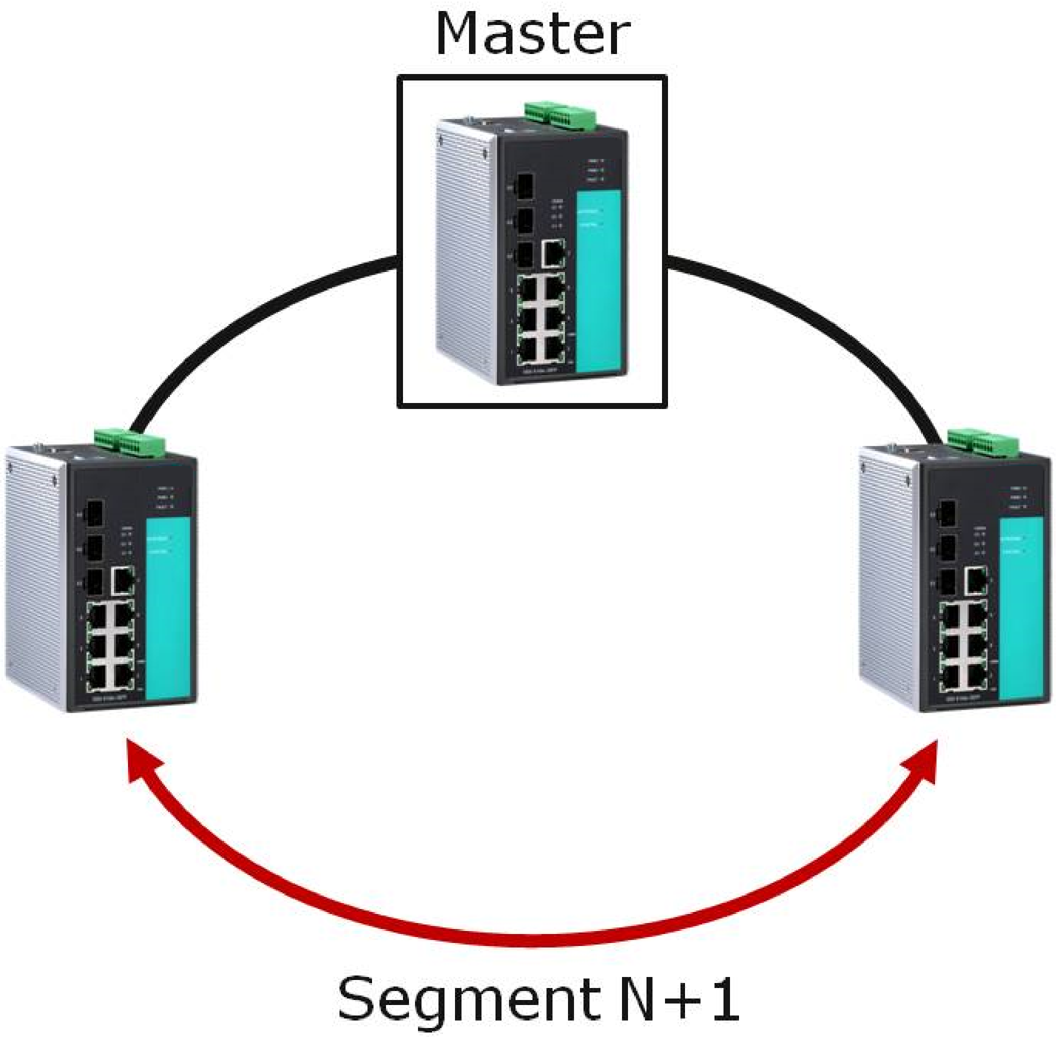
- **When the Number of Switches in the Turbo Ring is Even**

  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).



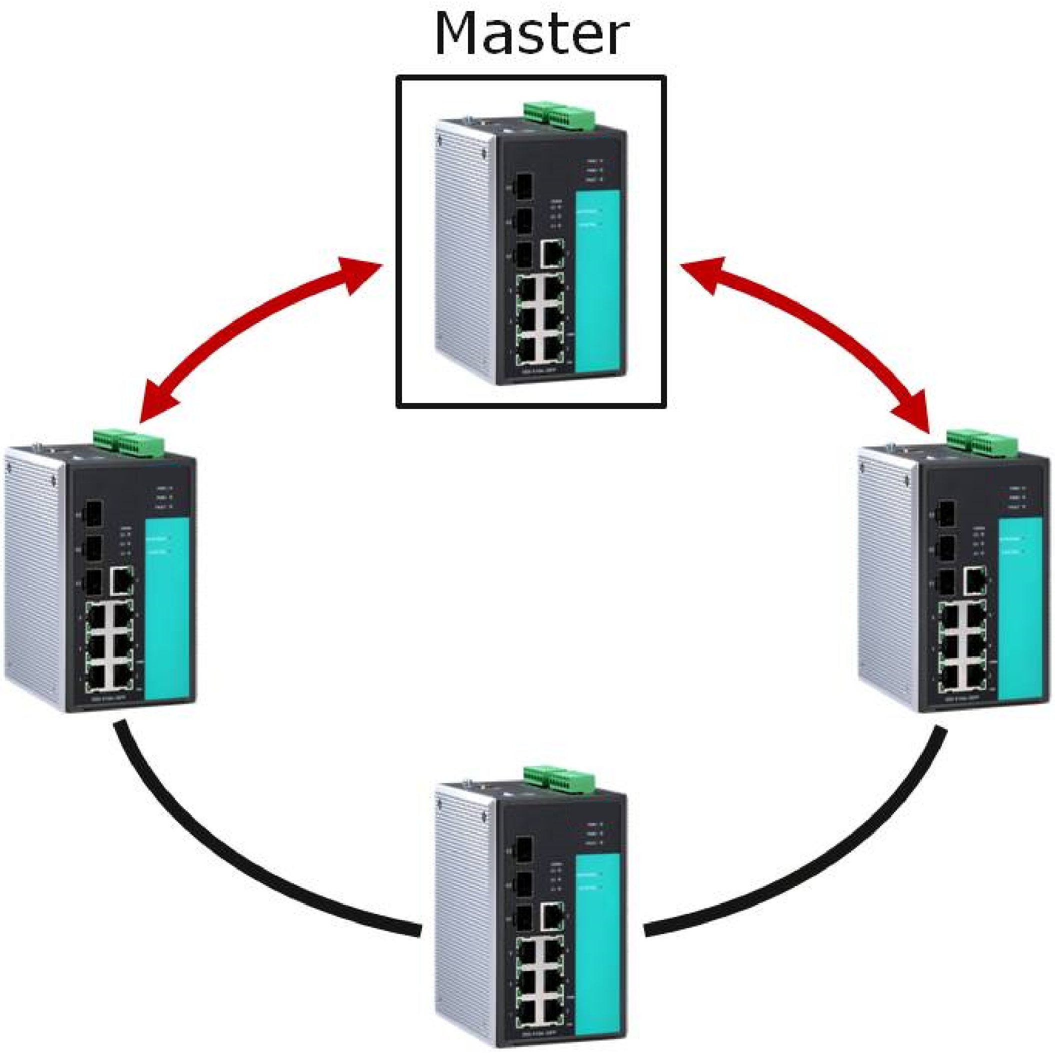
- **When the Number of Switches in the Turbo Ring is Odd**

  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.



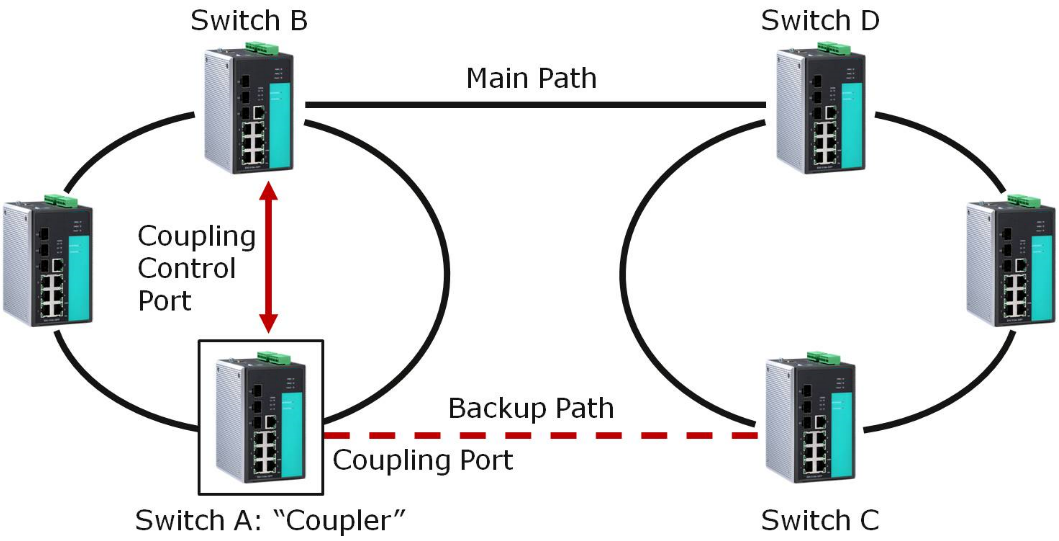
Ring Coupling Configuration

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.

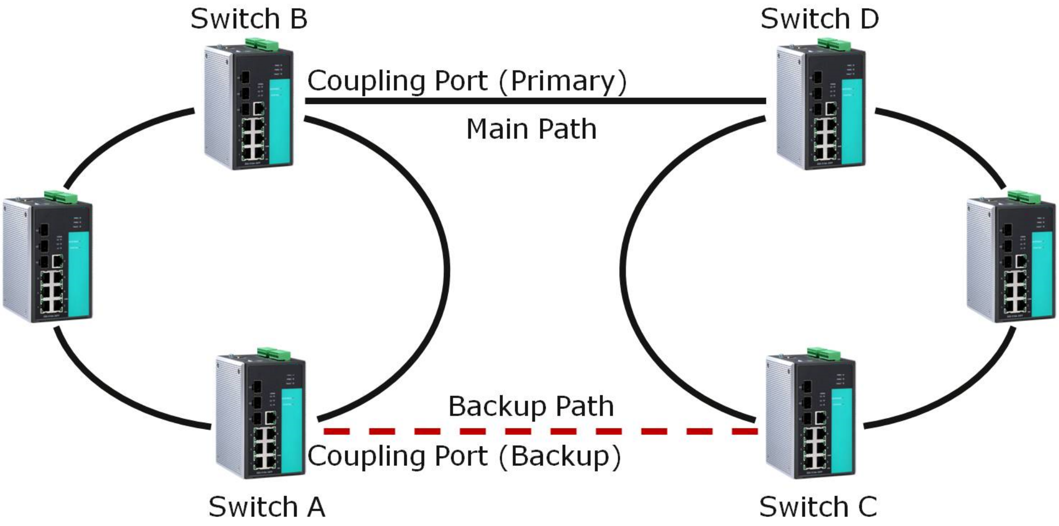
- Ring Coupling for a "Turbo Ring" Ring

  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.



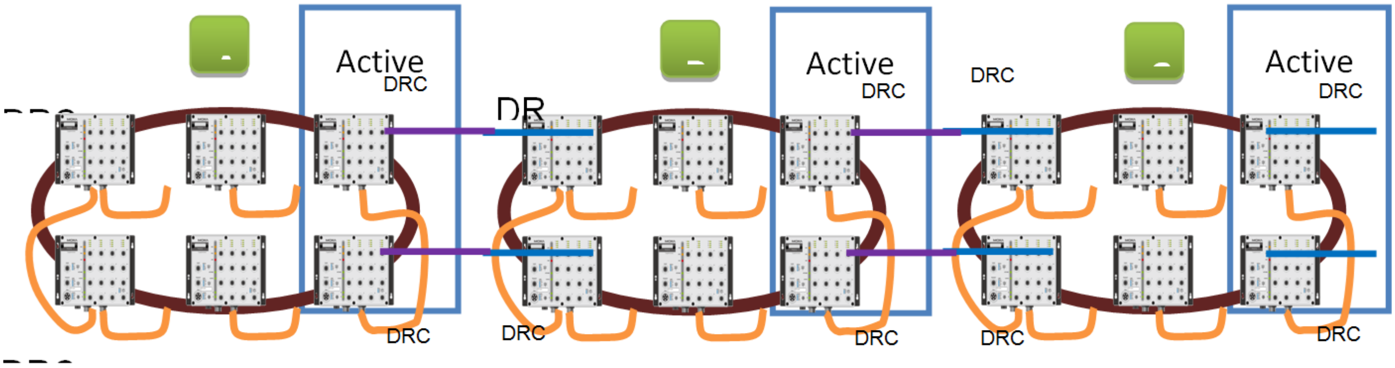
CAUTION

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.

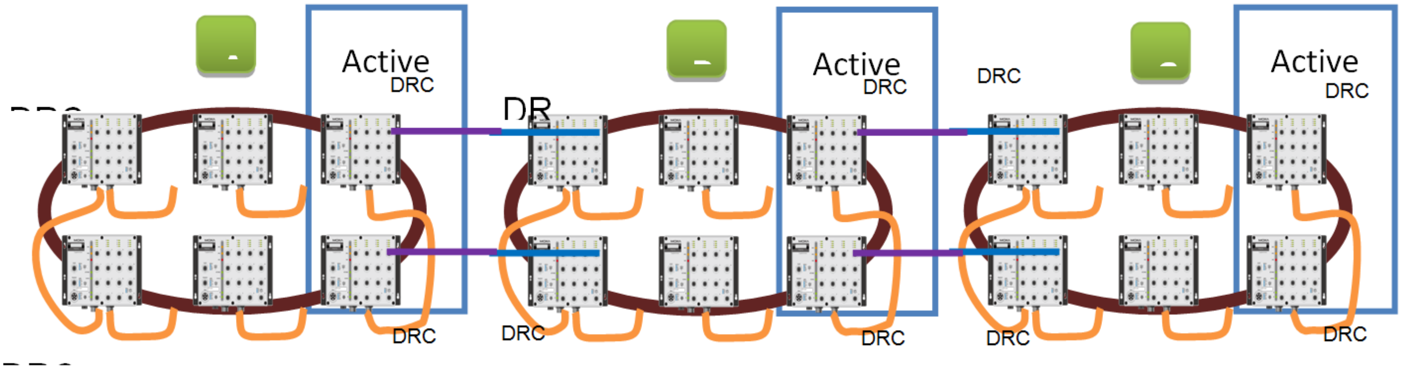
You do not need to use the same switch for both Ring Coupling and Ring Master.

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

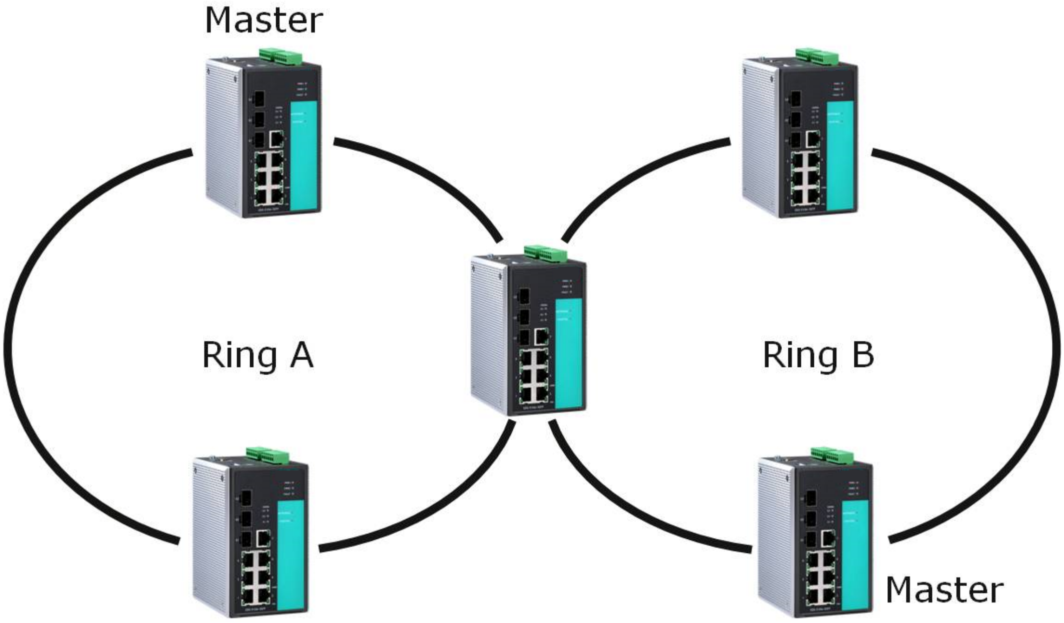
The ports which support bypass function cannot be used in redundant protocol like STP, RSTP, MSTP, Turbo Ring, Turbo Ring v2, Turbo Ring V2 with DRC (Dynamic Ring Coupling) and Turbo Chain.

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.

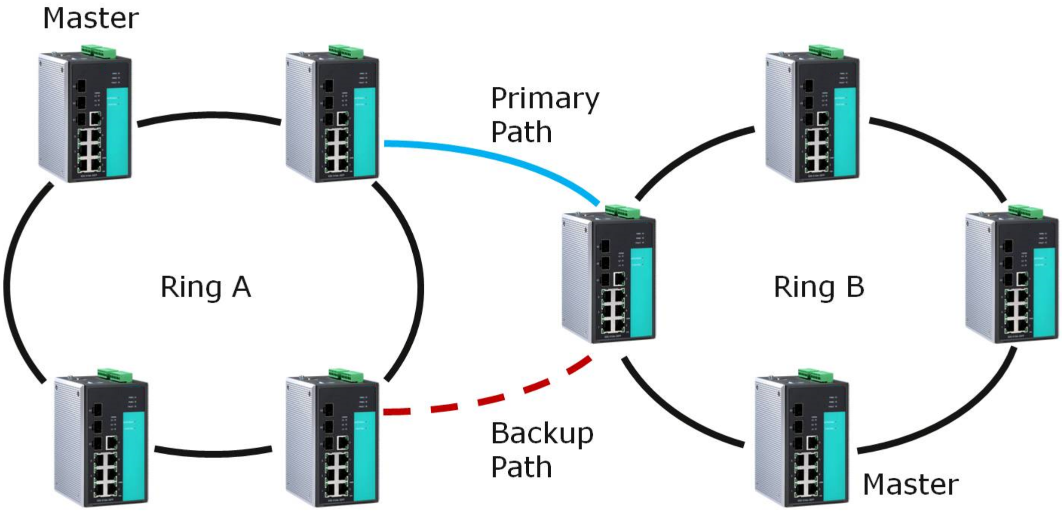
- Dual-Ring for a Turbo Ring V2 Ring



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.

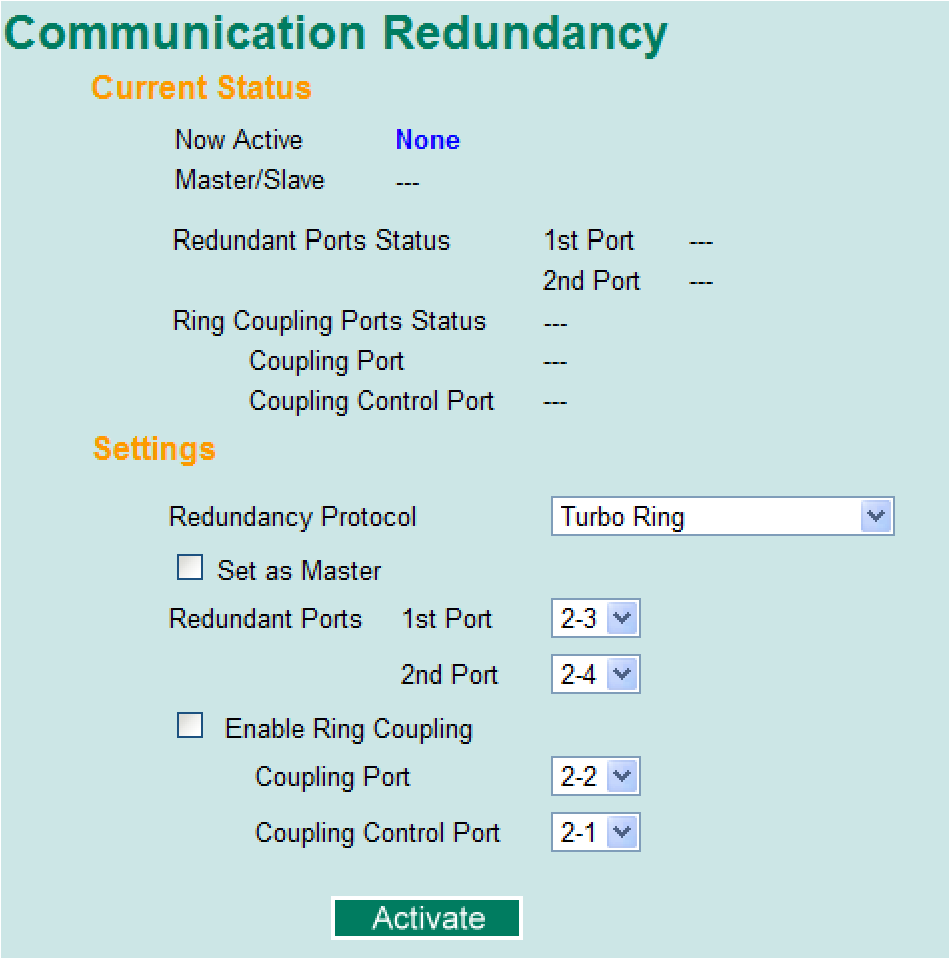
- Dual-Homing for a Turbo Ring V2 Ring



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

□ Set as Master

Redundant Ports 1st Port: 2-3

2nd Port: 2-4

□ Enable Ring Coupling

Coupling Port: 2-2

Coupling Control Port: 2-1

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.)

> ℹ *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	

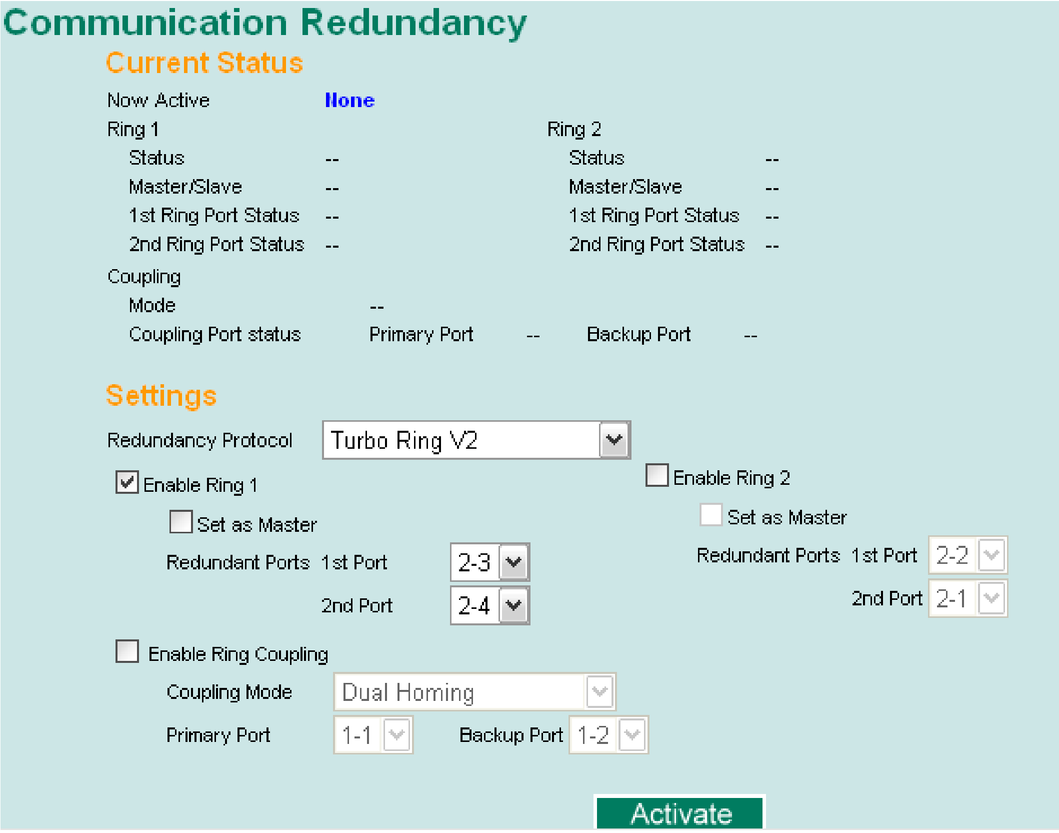
Coupling Port

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 2
□ Set as Master
Redundant Ports 1st Port 2-2
2nd Port 2-1

□ Enable Ring Coupling
Coupling Mode: Dual Homing
Primary Port 1-1 Backup Port 1-2

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	

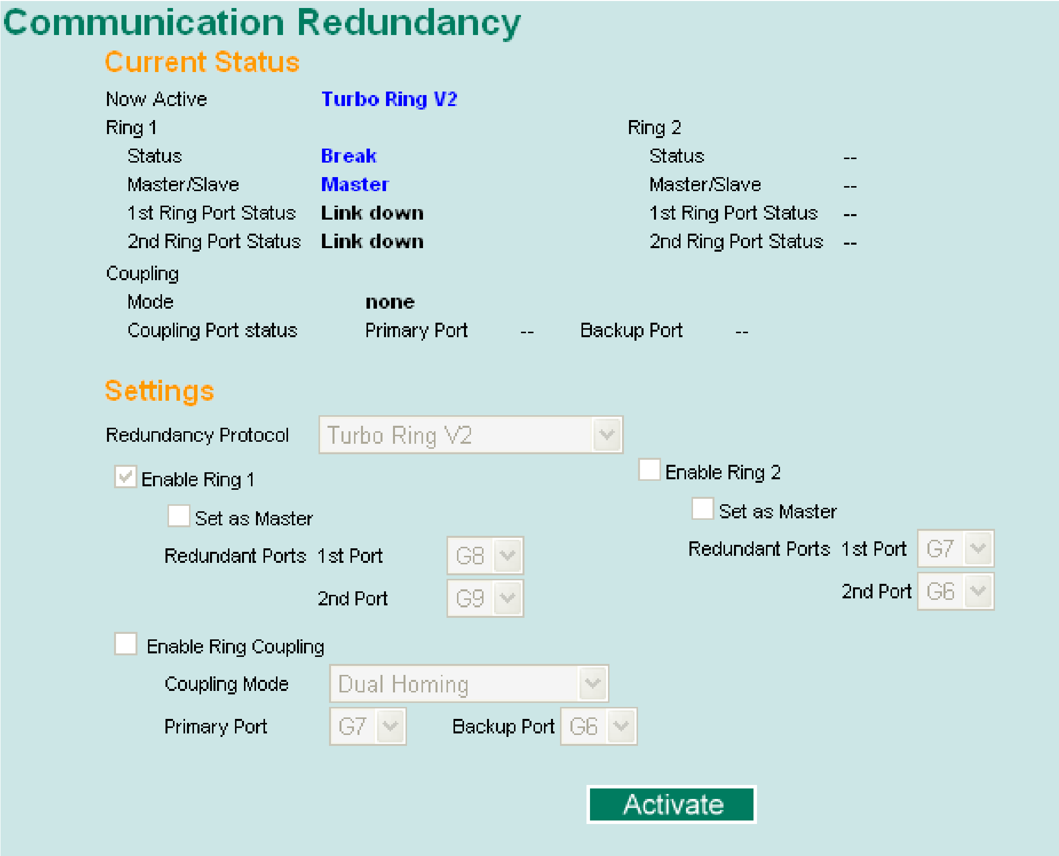
Coupling Mode

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
- □ Set as Master
- Redundant Ports 1st Port G8
- 2nd Port G9

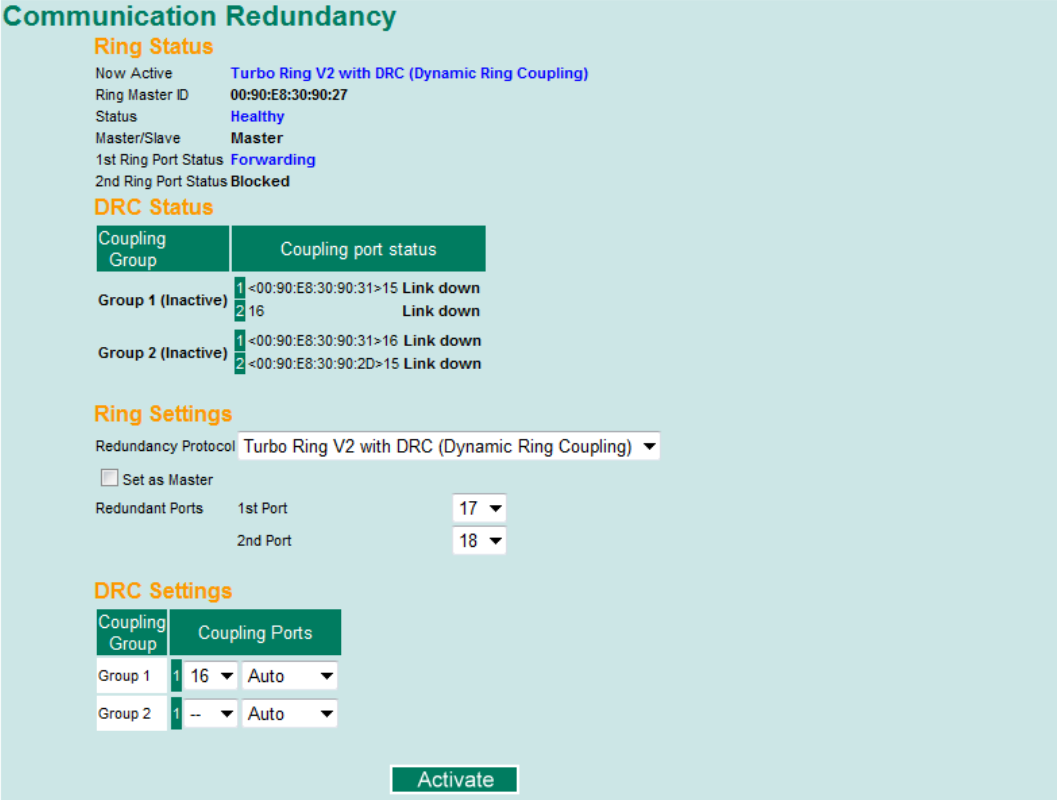
□ Enable Ring 2
- □ Set as Master
- Redundant Ports 1st Port G7
- 2nd Port G6

□ Enable Ring Coupling
- Coupling Mode: Dual Homing
- Primary Port: G7 Backup Port: G6

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
Group 2	1	--	Auto

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

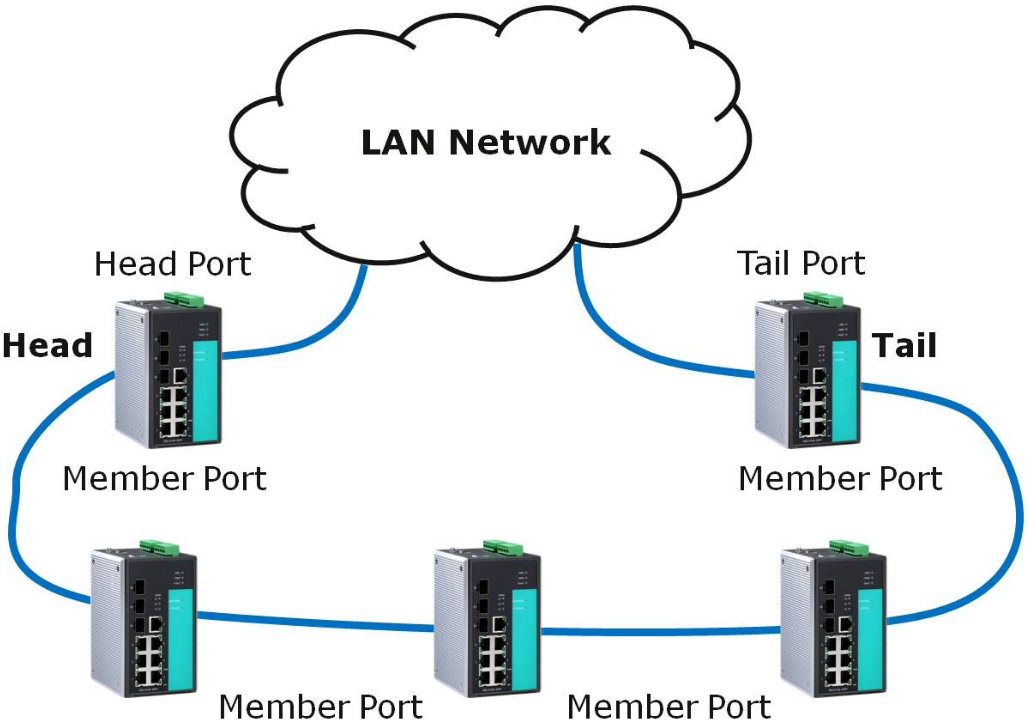
Setting	Description	Factory Default
Group1/Coupling Ports	Select any port of the switch to be one of the coupling group 1 port and choose auto, primary, backup as the port role	Port number: None Role: Auto
Group2/Coupling Ports	Select any port of the switch to be one of the coupling group 2 port and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

5.3 Turbo Chain

5.3.1 The Turbo Chain Concept

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

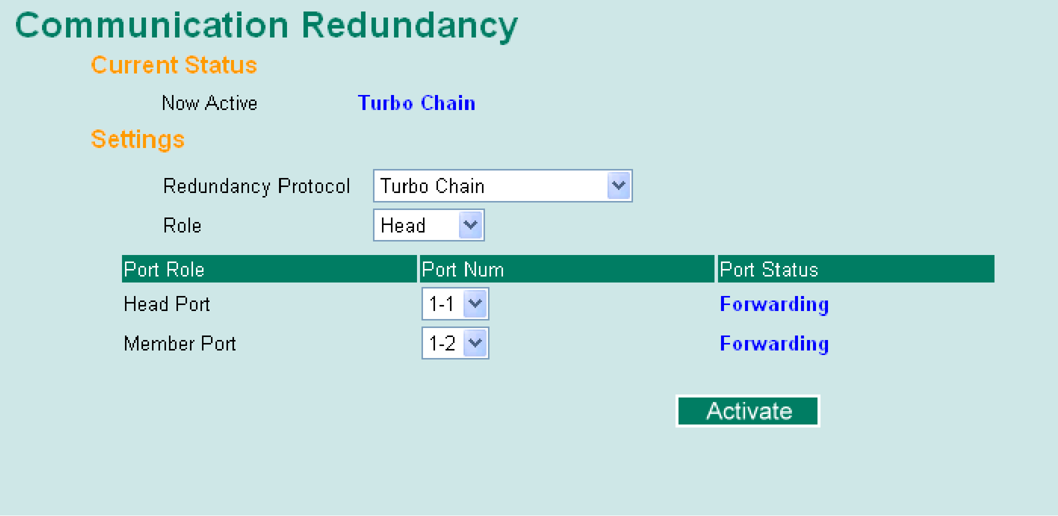


1. Select the Head switch, Tail switch, and Member switches.
2. Configure one port as the Head port and one port as the Member port in the Head switch, configure one port as the Tail port and one port as the Member port in the Tail switch, and configure two ports as Member ports in each of the Member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

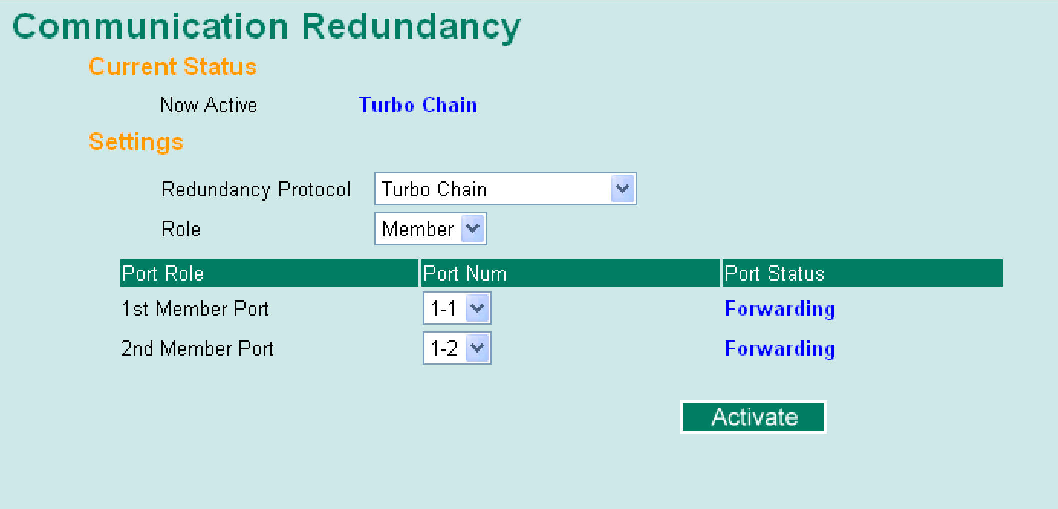
Settings

Redundancy Protocol: Turbo Chain

Role: Head

Port Role	Port Num	Port Status
Head Port	1-1	Forwarding
Member Port	1-2	Forwarding

Member Switch Configuration



Communication Redundancy

Current Status

Now Active: Turbo Chain

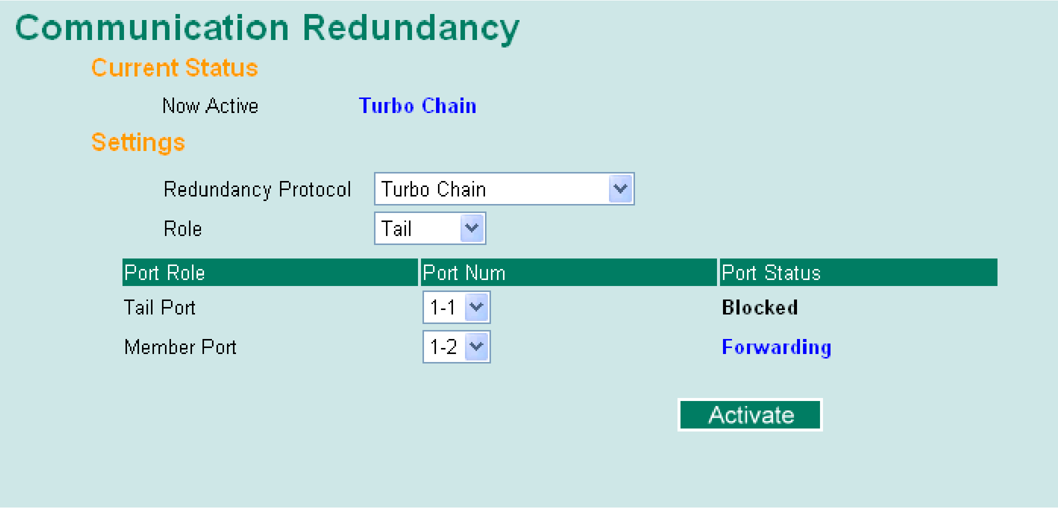
Settings

Redundancy Protocol: Turbo Chain

Role: Member

Port Role	Port Num	Port Status
1st Member Port	1-1	Forwarding
2nd Member Port	1-2	Forwarding

Tail Switch Configuration



Communication Redundancy

Current Status

Now Active: Turbo Chain

Settings

Redundancy Protocol: Turbo Chain

Role: Tail

Port Role	Port Num	Port Status
Tail Port	1-1	Blocked
Member Port	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.

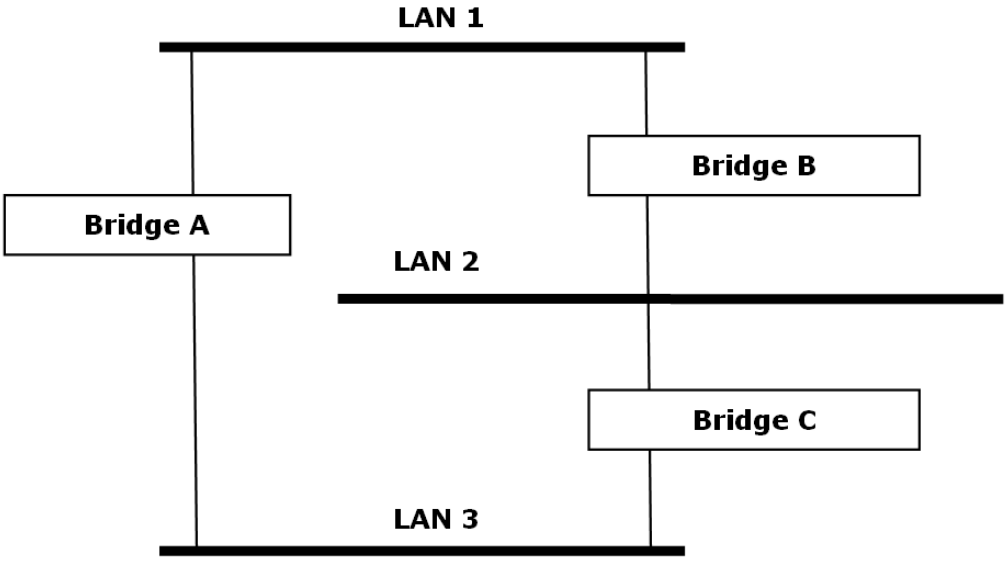
The STP protocol is part of the IEEE Std 802.1D, 2004 Edition bridge specification. The following explanation uses bridge instead of switch.

What is STP?

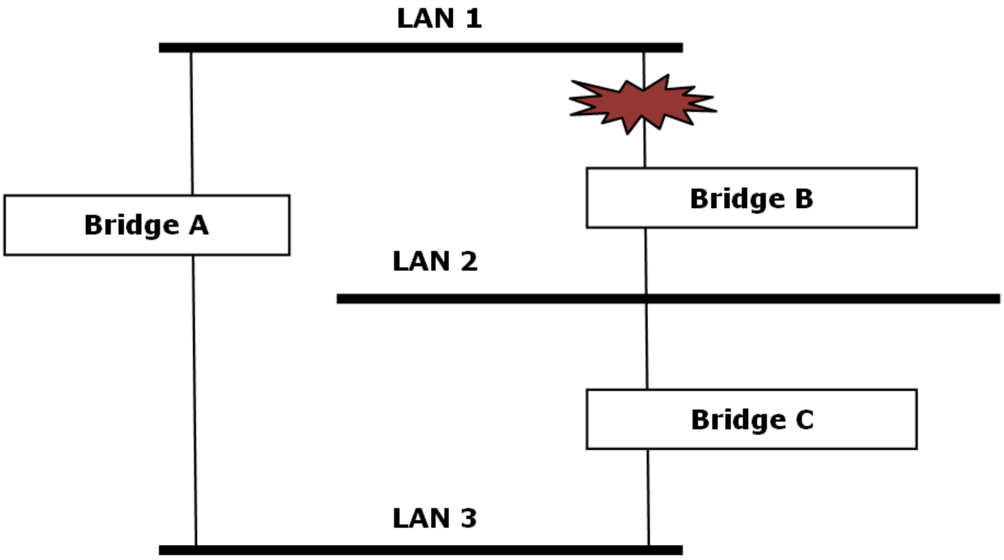
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

- 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.

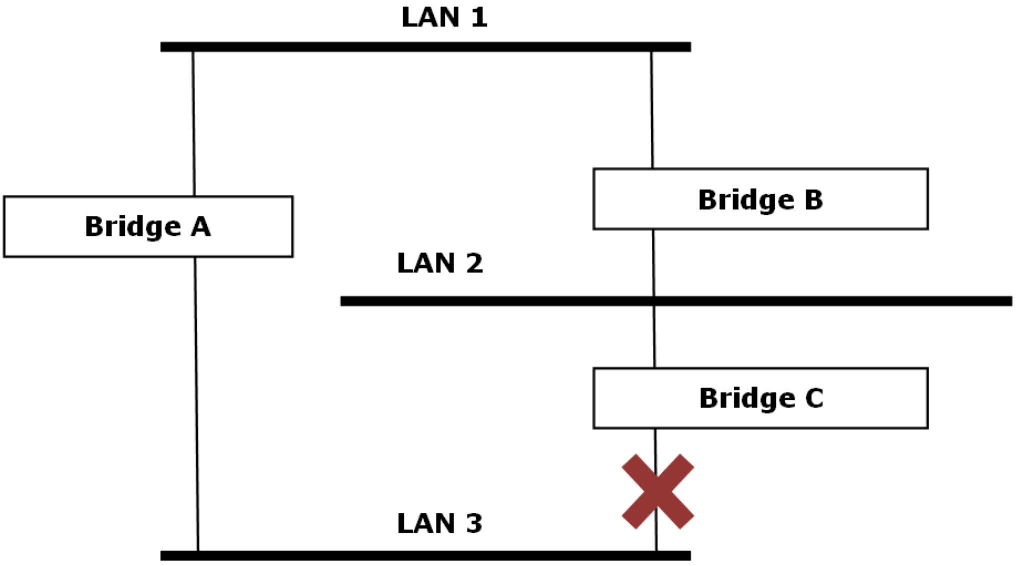
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



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

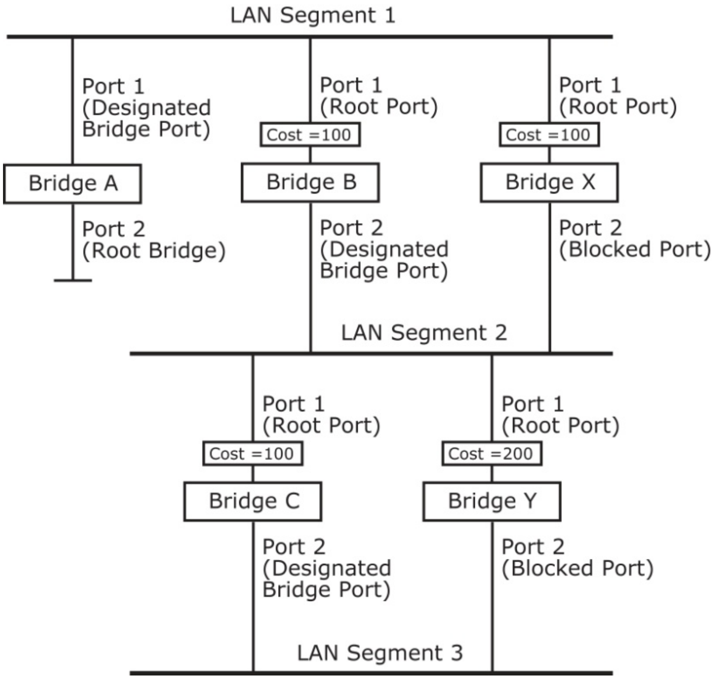
  Once the network topology has stabilized, each bridge listens for Hello BPDUs transmitted from the Root Bridge at regular intervals. If a bridge does not receive a Hello BPDU after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, 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

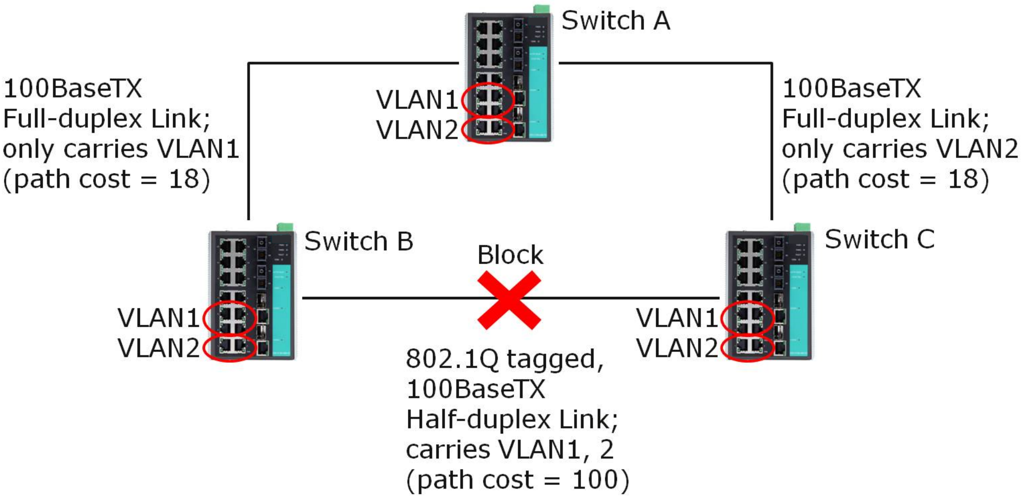
The LAN shown in the following figure has three segments, with adjacent segments connected using two possible links. The various STP factors, such as Cost, Root Port, Designated Bridge Port, and Blocked Port are shown in the figure.



- 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

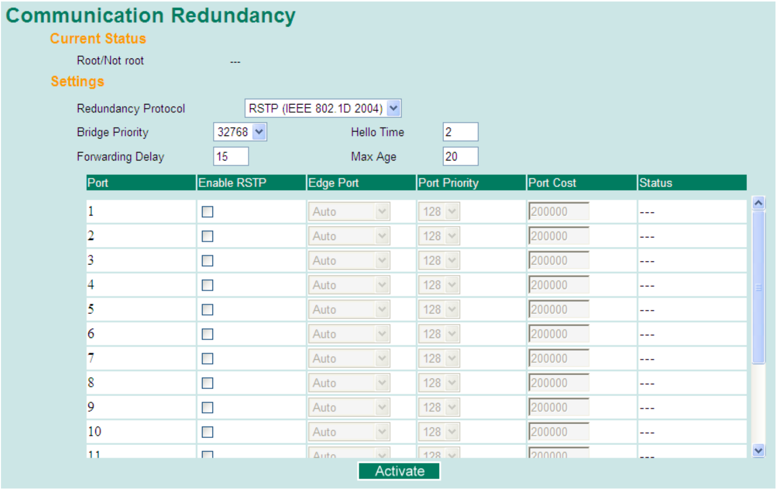
IEEE Std 802.1D, 1998 Edition, does not take into account VLANs when calculating STP information-the calculations only depend on the physical connections. Consequently, some network configurations will result in VLANs being subdivided into a number of isolated sections by the STP system. You must ensure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



Communication Redundancy

Current Status

Root/Not root ---

Settings

Redundancy Protocol: RSTP (IEEE 802.1D 2004)

Bridge Priority: 32768 Hello Time: 2

Forwarding Delay: 15 Max Age: 20

Port	Enable RSTP	Edge Port	Port Priority	Port Cost	Status
1	□	Auto	128	200000	---
2	□	Auto	128	200000	---
3	□	Auto	128	200000	---
4	□	Auto	128	200000	---
5	□	Auto	128	200000	---
6	□	Auto	128	200000	---
7	□	Auto	128	200000	---
8	□	Auto	128	200000	---
9	□	Auto	128	200000	---
10	□	Auto	128	200000	---
11	□	Auto	128	200000	---

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

Setting	Description	Factory Default
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 *Max. Age*, 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 sec ≦ Hello Time ≦ 10 sec

[Eq. 2]: 6 sec ≦ Max. Age ≦ 40 sec

[Eq. 3]: 4 sec ≦ Forwarding Delay ≦ 30 sec

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

[Eq. 4]: 2 x (Hello Time + 1 sec) ≦ Max. Age ≦ 2 x (Forwarding Delay – 1 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 x (Hello Time + 1 sec) = 12 sec, and 2 x (Forwarding Delay – 1 sec) = 6 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.

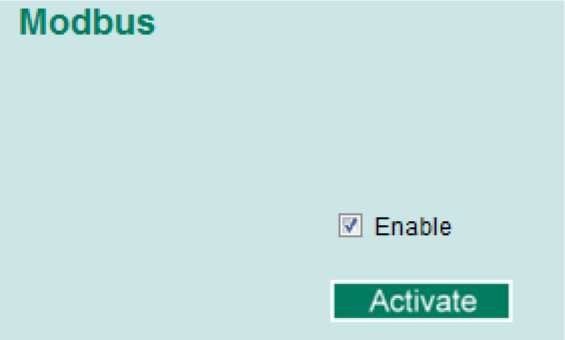
6.1.2 Data Format and Function Code

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	Support
	Physical Output Registers	3	Read Holding Registers	

6.1.3 Configuring MODBUS/TCP on VIPA Switches

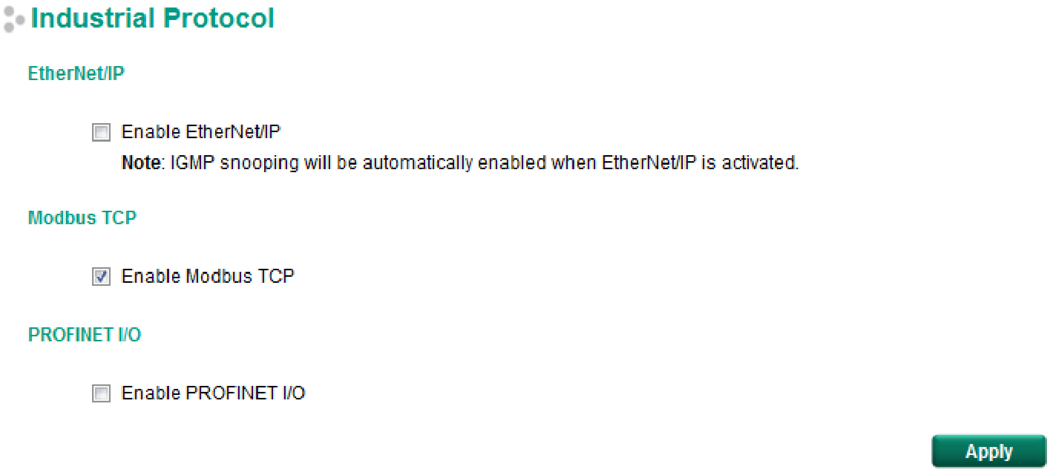
Type 1



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].



Industrial Protocol

EtherNet/IP

□ Enable EtherNet/IP

Note: IGMP snooping will be automatically enabled when EtherNet/IP is activated.

Modbus TCP

☑ Enable Modbus TCP

PROFINET I/O

□ Enable PROFINET I/O

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	Interpreta-tion	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’
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’

Address Offset	Data Type	Interpretation	Description
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
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

Address Offset	Data Type	Interpreta-tion	Description
0x0083	1 word	HEX	DO2 0x0000: Off 0x0001: On
Port Information			
0x1000 to0x1011	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
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			

Address Offset	Data Type	Interpretation	Description
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			
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

Address Offset	Data Type	Interpreta-tion	Description
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
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

Address Offset	Data Type	Interpretation	Description
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
0x3502	1 word	HEX	TurboRing V2 Coupling Port Backup Status (Only using in Dual Homing) 0x0000: Port Disabled 0x0001: Not Coupling Port 0 0x002: 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

Address Offset	Data Type	Interpretation	Description
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
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

Address Offset	Data Type	Interpretation	Description
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			
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

Address Offset	Data Type	Interpretation	Description
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 / 0x01Discarding 0x02: RootPort / 0x02Learning 0x03: AlternatePort / 0x03Forwarding 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 / x01 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
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

Address Offset	Data Type	Interpretation	Description
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

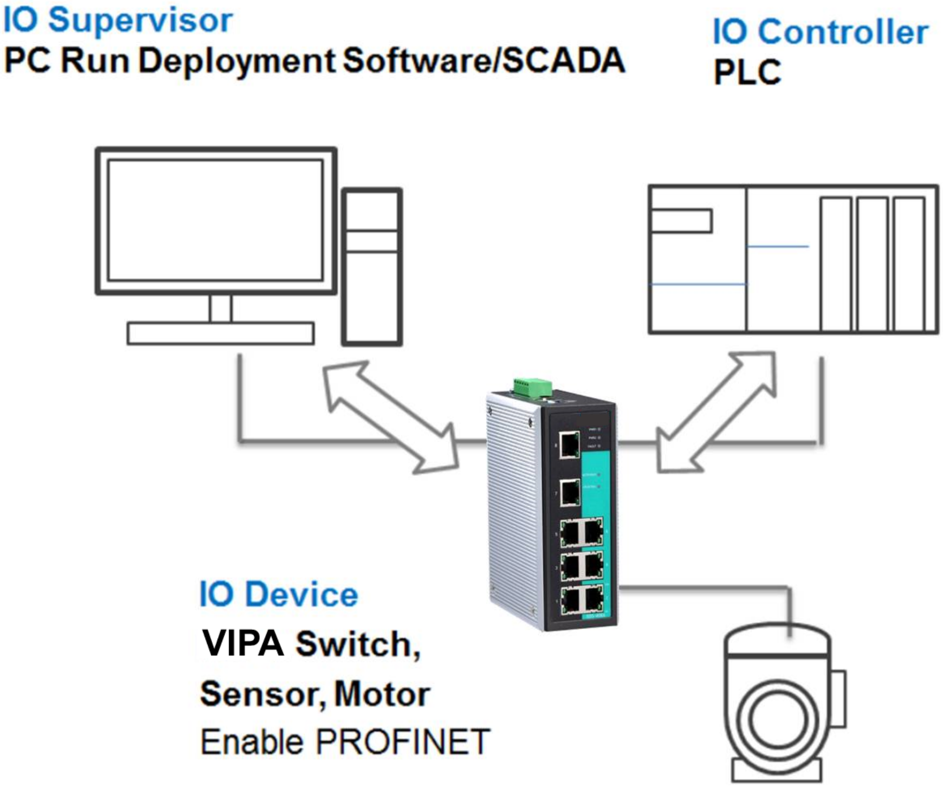
6.3.1 Introduction

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

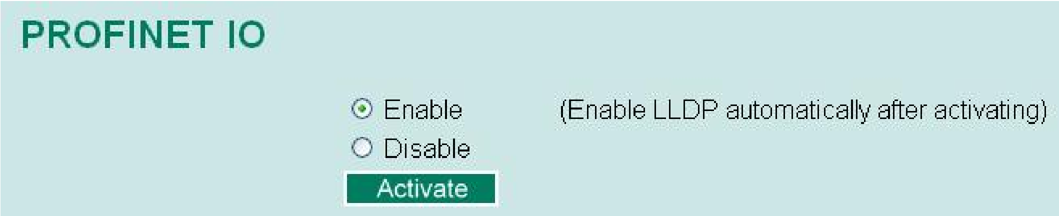
- DCP
  - In PROFINET I/O, each field device has a symbolic name that uniquely identifies the field device within a PROFINET I/O system. This name is used for assigning the IP address and the MAC address. The DCP protocol (Dynamic Configuration Protocol) integrated in every I/O device is used for this 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



PROFINET IO

● Enable (Enable LLDP automatically after activating)

○ Disable

Activate

→ 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

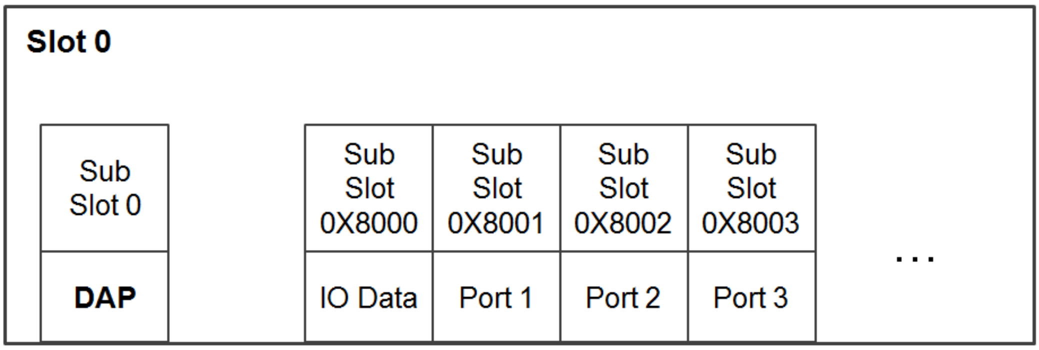
The CLI (command line interface) can be used to enable or disable PROFINET for the switch.

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.



Slot 0

Sub Slot 0	Sub Slot 0X8000	Sub Slot 0X8001	Sub Slot 0X8002	Sub Slot 0X8003	...
DAP	IO Data	Port 1	Port 2	Port 3	

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:

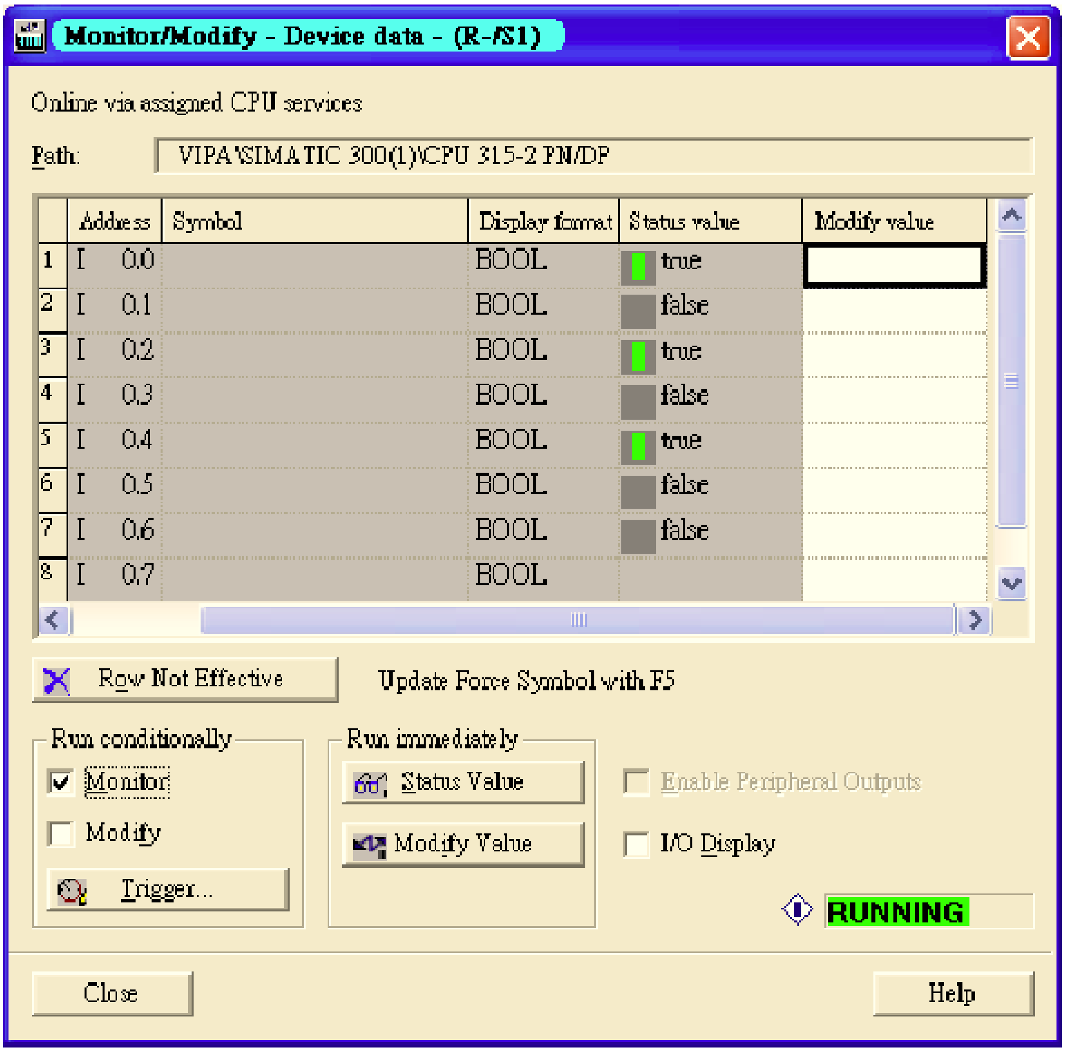
The default transfer frequency of PROFINET Cyclic I/O data is 128 ms. There are 3 options available in Siemens SIMATIC STEP®7: 128/256/512 ms.

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
			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/Modify - Device data - (R-/S1)

Online via assigned CPU services

Path: VIPA\SIMATIC 300(1)\CPU 315-2 PN/DP

	Address	Symbol	Display format	Status value	Modify value
1	I 0.0		BOOL	🟩 true	
2	I 0.1		BOOL	■ false	
3	I 0.2		BOOL	🟩 true	
4	I 0.3		BOOL	■ false	
5	I 0.4		BOOL	🟩 true	
6	I 0.5		BOOL	■ false	
7	I 0.6		BOOL	■ false	
8	I 0.7		BOOL		

Update Force Symbol with F5

Run conditionally: ☑ Monitor; □ Modify

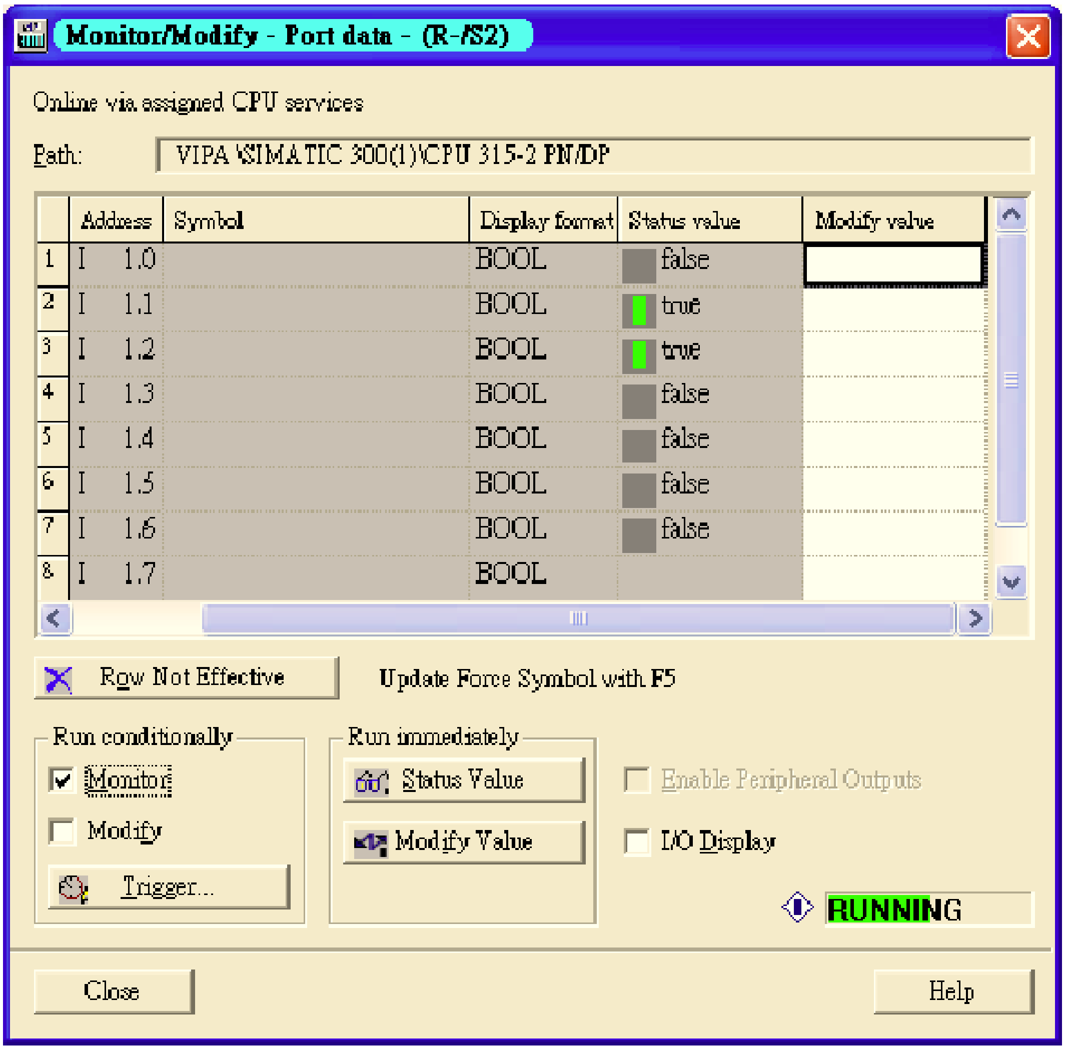
Run immediately

□ Enable Peripheral Outputs

□ I/O Display

RUNNING

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



Monitor/Modify - Port data - (R-/S2)

Online via assigned CPU services

Path: VIPA \SIMATIC 300(1)\CPU 315-2 PN/DP

	Address	Symbol	Display format	Status value	Modify value
1	I 1.0		BOOL	false	
2	I 1.1		BOOL	🟩 true	
3	I 1.2		BOOL	🟩 true	
4	I 1.3		BOOL	false	
5	I 1.4		BOOL	false	
6	I 1.5		BOOL	false	
7	I 1.6		BOOL	false	
8	I 1.7		BOOL		

Run conditionally: ☑ Monitor □ Modify

□ Enable Peripheral Outputs

□ I/O Display

RUNNING

PROFINET I/O Parameters

PROFINET I/O parameters are for more flexible settings and monitoring. There 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	
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

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

6.3.6 Siemens STEP®7 Integration

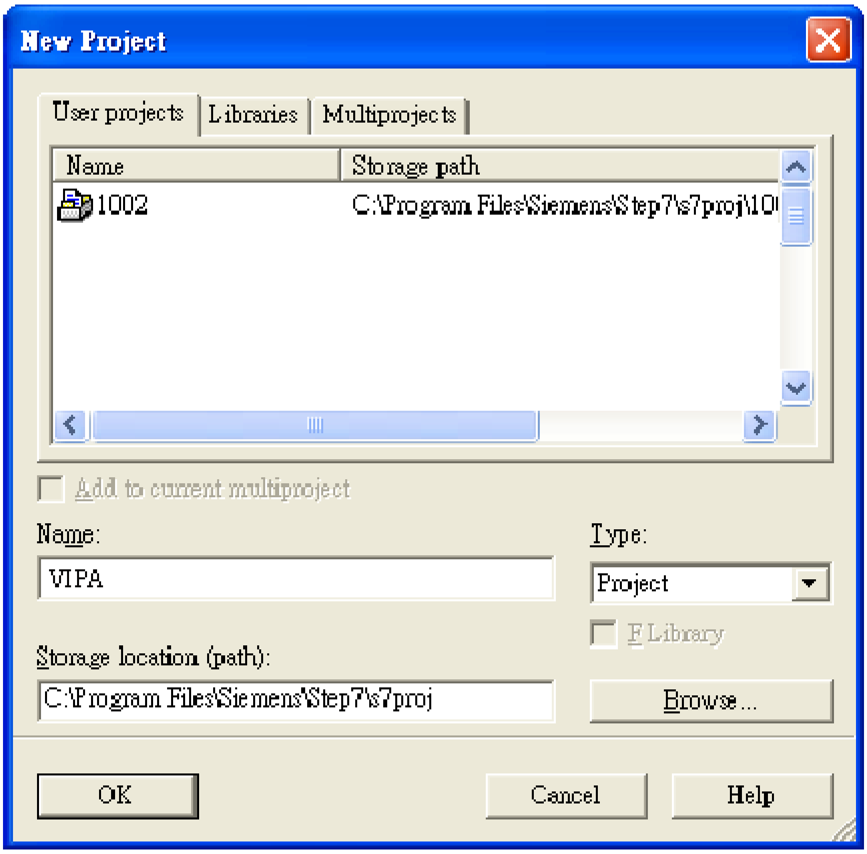
Overview of Operation Procedure

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'*



Name	Storage path
1002	C:\Program Files\Siemens\Step7\s7proj\10

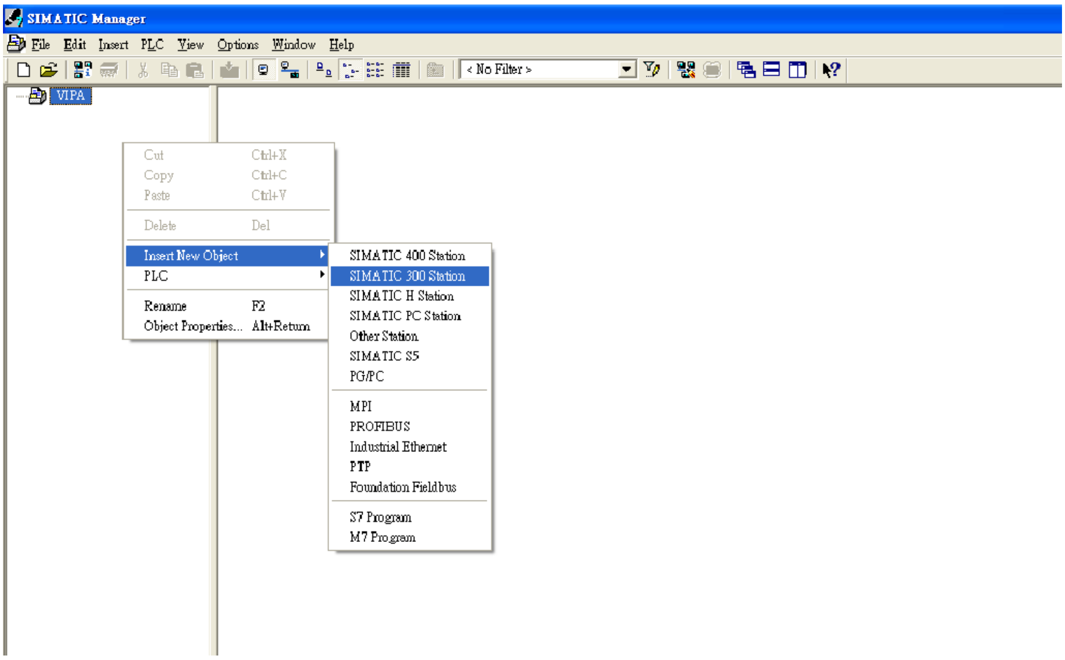
Name: VIPA

Type: Project

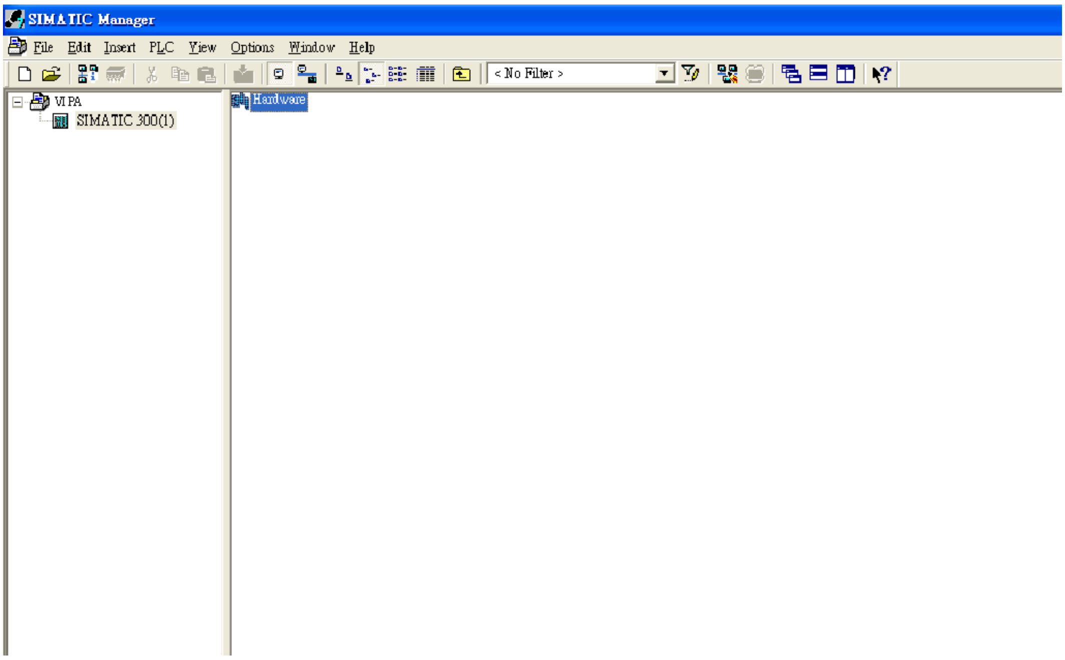
F Library

Storage location (path): C:\Program Files\Siemens\Step7\s7proj

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).

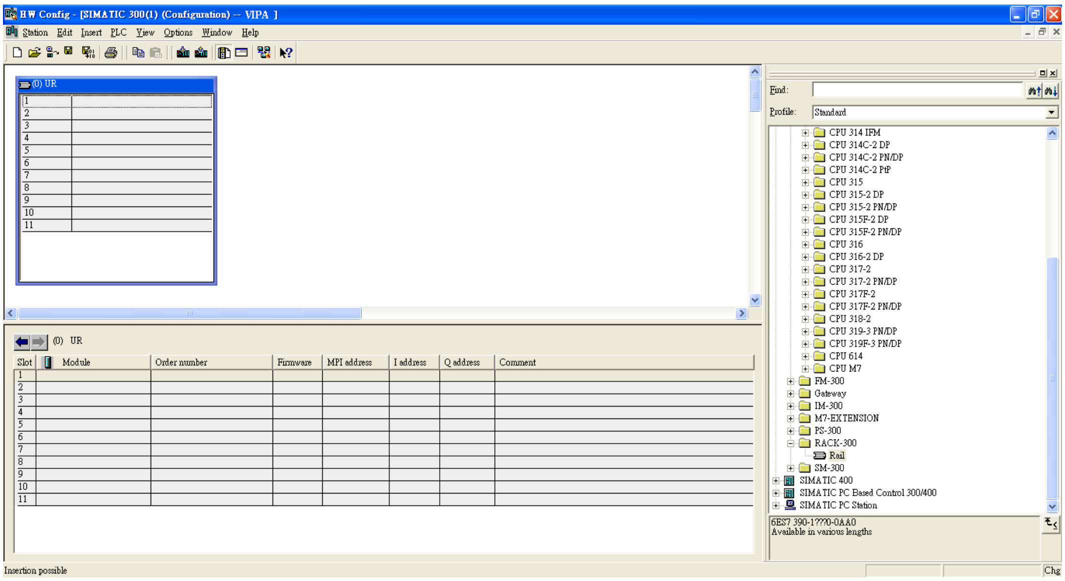


4. Then you can see the new object in the project. Double click on the *'Hardware'*.

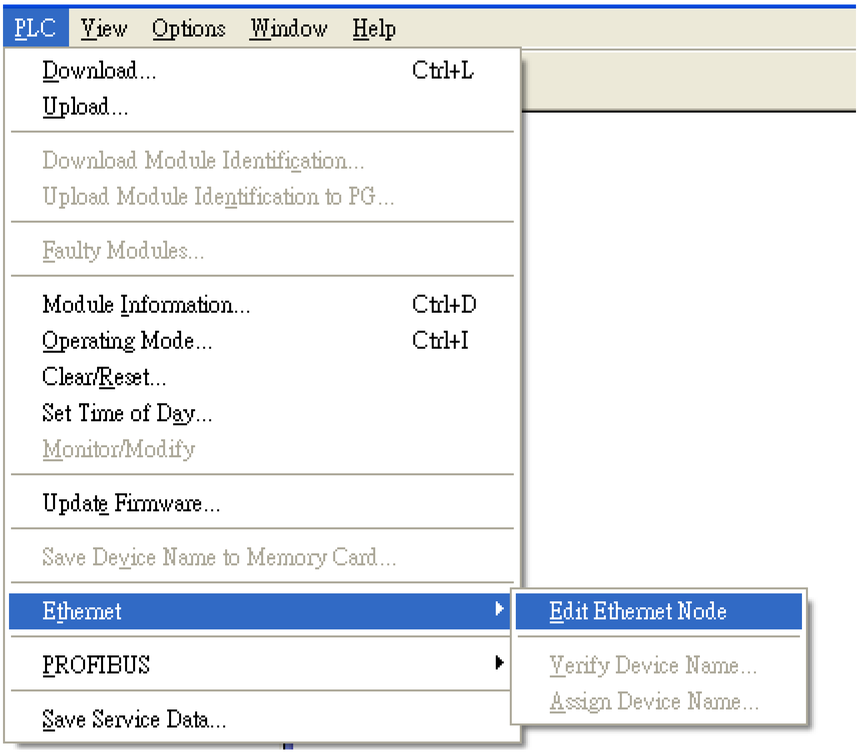


5. Add Rack in HW Config: After double-clicking on HW, you will see the *'HW Config'* window.

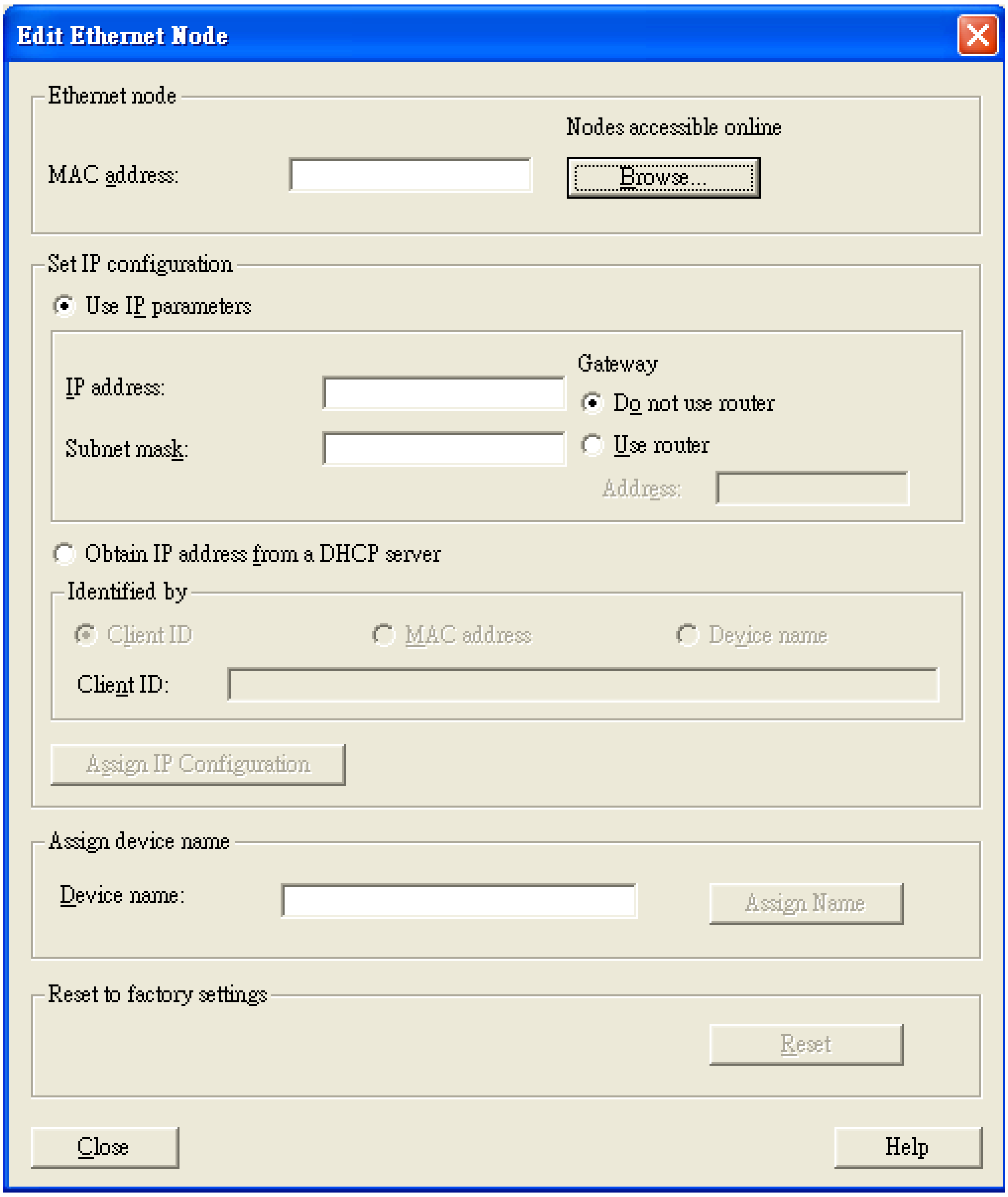
6. Drag a rack from the side bar to main dashboard. In here, we drag *'Rail'*, which is under the Rack-300 folder, to the main screen.



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 [Browse...]

Set IP configuration

● Use IP parameters

IP address:

Subnet mask:

Gateway

● 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

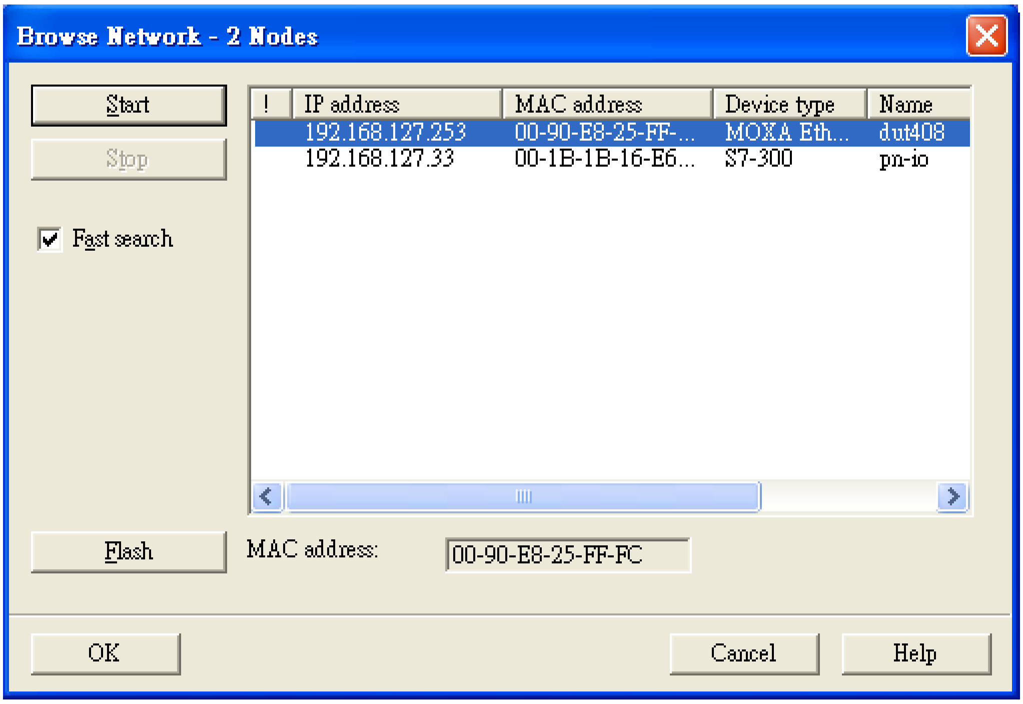
Device name: [Assign Name]

Reset to factory settings

[Reset]

[Close] [Help]

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.

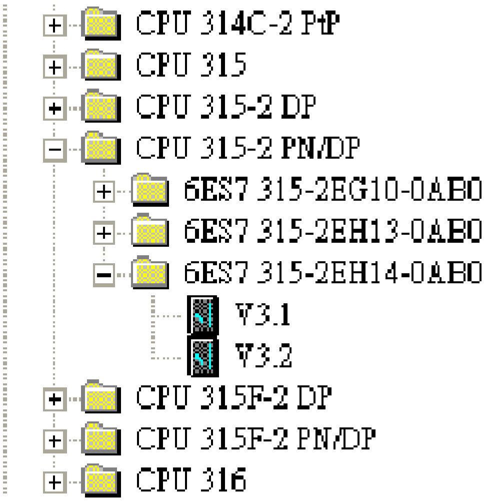


☑ Fast search

!	IP address	MAC address	Device type	Name
	192.168.127.253	00-90-E8-25-FF-...	MOXA Eth...	dut408
	192.168.127.33	00-1B-1B-16-E6...	S7-300	pn-io

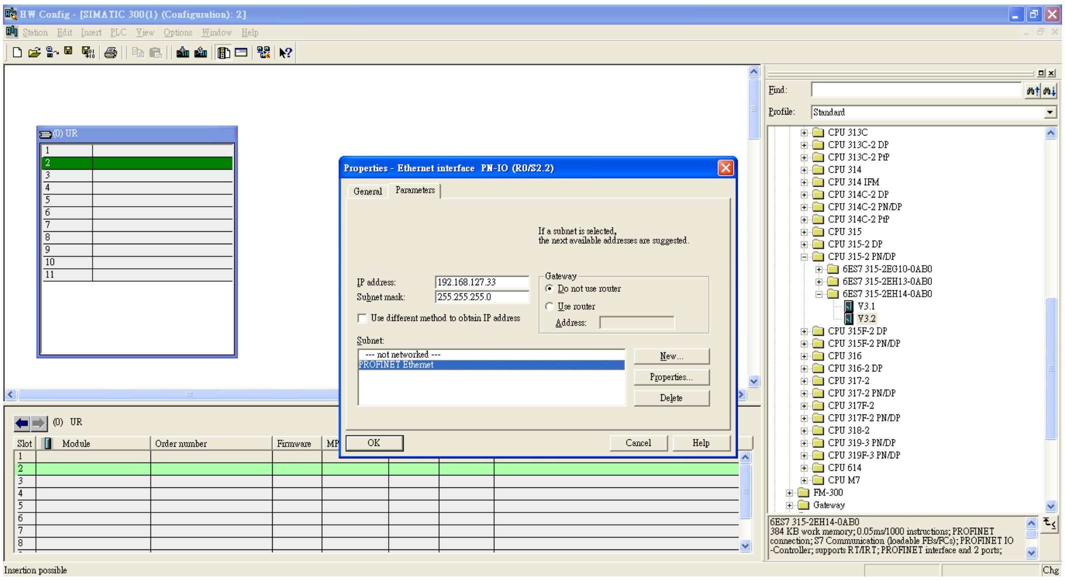
MAC address: 00-90-E8-25-FF-FC

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.



CPU 314C-2 PtP
CPU 315
CPU 315-2 DP
CPU 315-2 PN/DP
6ES7 315-2EG10-0AB0
6ES7 315-2EH13-0AB0
6ES7 315-2EH14-0AB0
V3.1
V3.2
CPU 315F-2 DP
CPU 315F-2 PN/DP
CPU 316

11. 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'*.



HW Config - [SIMATIC 300(1) (Configuration): 2]

Properties - Ethernet interface PN-IO (R0/S2.2)

General | Parameters

If a subnet is selected,
the next available addresses are suggested.

IP address: 192.168.127.33
Subnet mask: 255.255.255.0
□ Use different method to obtain IP address

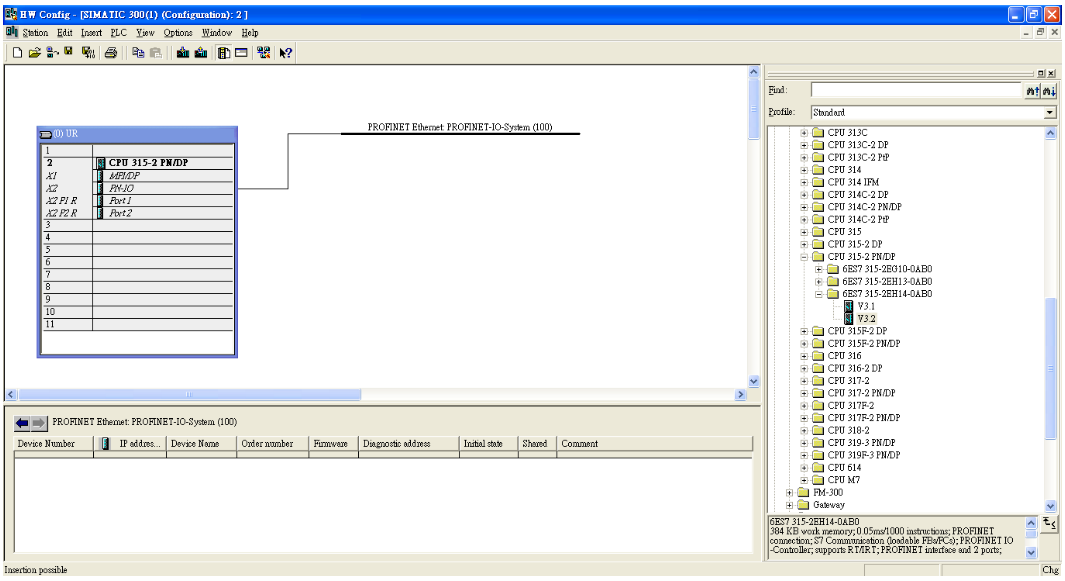
Gateway
● Do not use router
○ Use router
Address:

Subnet:
--- not networked ---
PROFINET Ethernet

6ES7 315-2EH14-0AB0
384 KB work memory; 0.05ms/1000 instructions; PROFINET connection; S7 Communication (loadable FBs/FCs); PROFINET IO -Controller; supports RT/IRT; PROFINET interface and 2 ports;

Insertion possible

➡ PROFINET I/O Ethernet subnet project accomplished



HW Config - [SIMATIC 300(1) (Configuration): 2]

(0) UR
1
2 CPU 315-2 PN/DP
X1 MPI/DP
X2 PN-IO
X2 P1 R Port 1
X2 P2 R Port 2

PROFINET Ethernet: PROFINET-IO-System (100)

Insertion possible

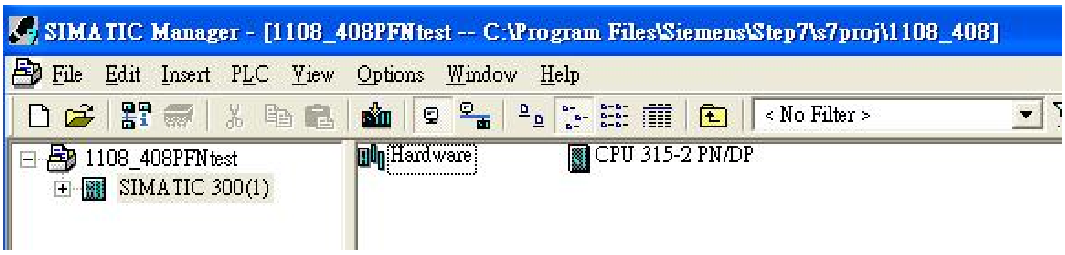
GSDML File Installation

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

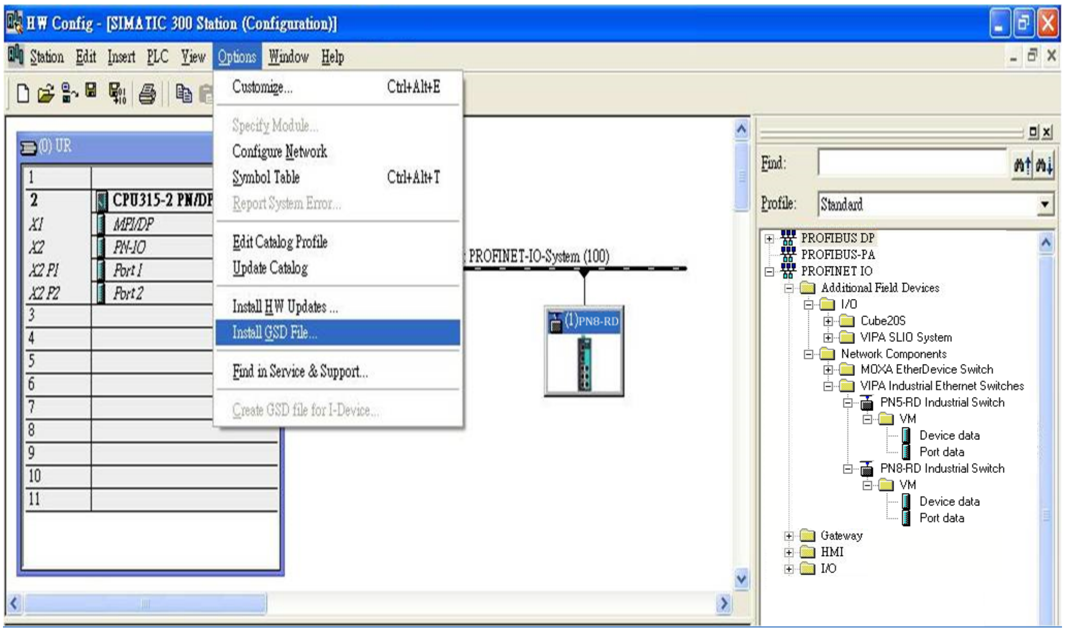
The assignment of the GSDML file to your slave is shown in the following table:

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

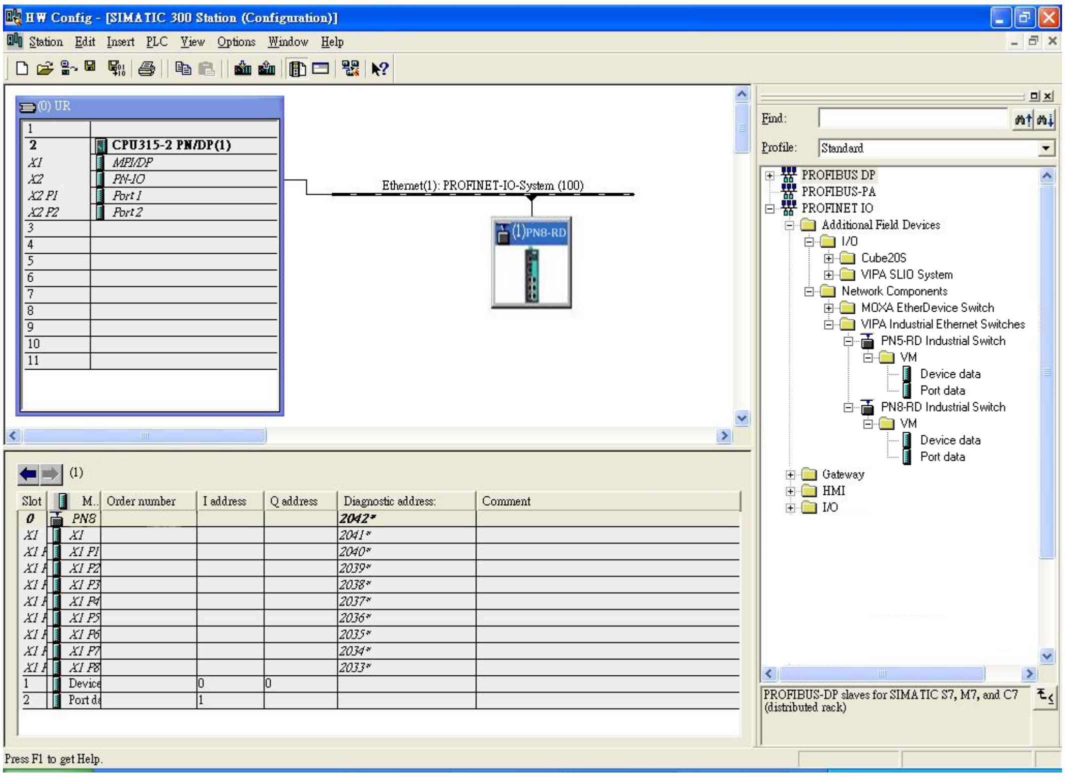
1. Open Siemens SIMATIC Manager on your PC.
2. Open your project.
3. Open hardware configuration.


SIMATIC Manager - [1108_408PFNtest -- C:\Program Files\Siemens\Step7\s7proj\1108_408]
File Edit Insert PLC View Options Window Help
< No Filter >
1108_408PFNtest
SIMATIC 300(1)
Hardware
CPU 315-2 PN/DP

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



(0) UR

1	
2	CPU315-2 PN/DP(1)
X1	MPI/DP
X2	PN-IO
X2 P1	Port 1
X2 P2	Port 2
3	
4	
5	
6	
7	
8	
9	
10	
11	

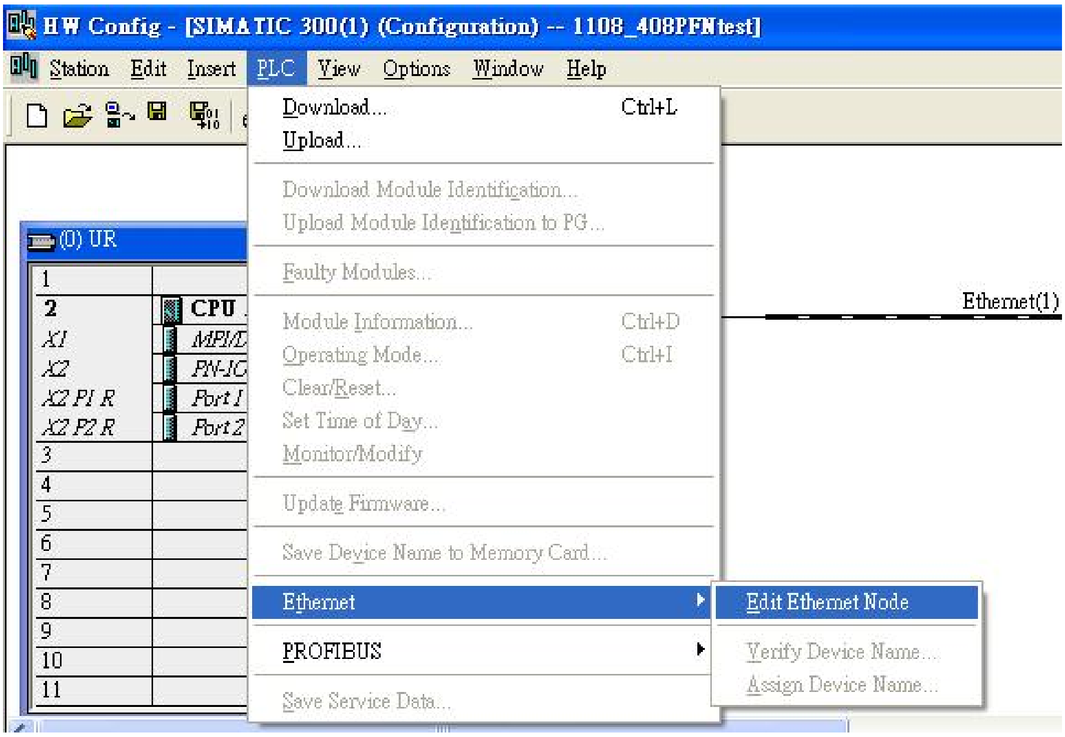
(1)

Slot	M..	Order number	I address	Q address	Diagnostic address:	Comment
0	PN8				2042*	
X1	X1				2041*	
X1 F	X1 P1				2040*	
X1 F	X1 P2				2039*	
X1 F	X1 P3				2038*	
X1 F	X1 P4				2037*	
X1 F	X1 P5				2036*	
X1 F	X1 P6				2035*	
X1 F	X1 P7				2034*	
X1 F	X1 P8				2033*	
1	Device		0	0		
2	Port da		1			

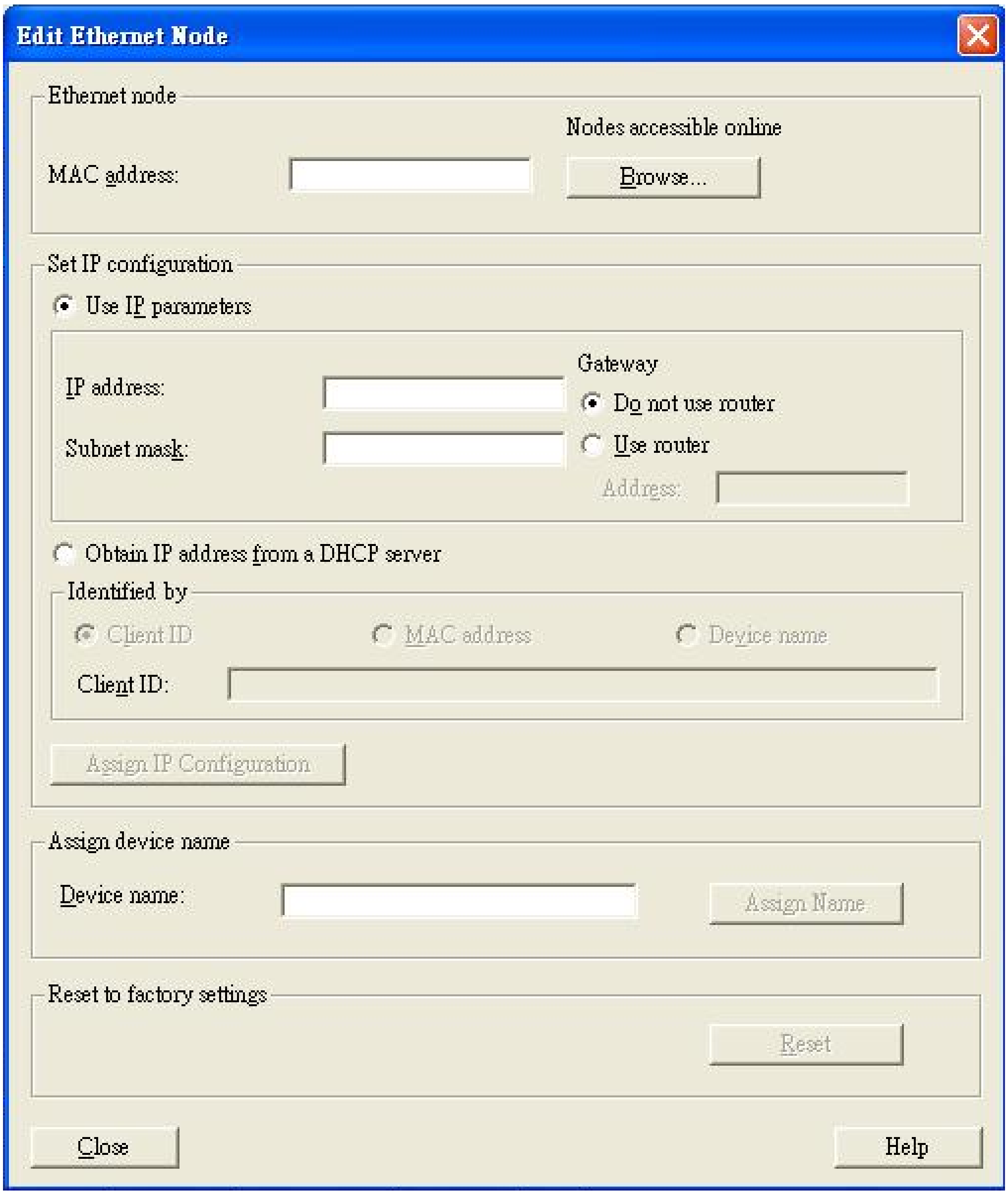
Device Configuration

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].



● Use IP parameters

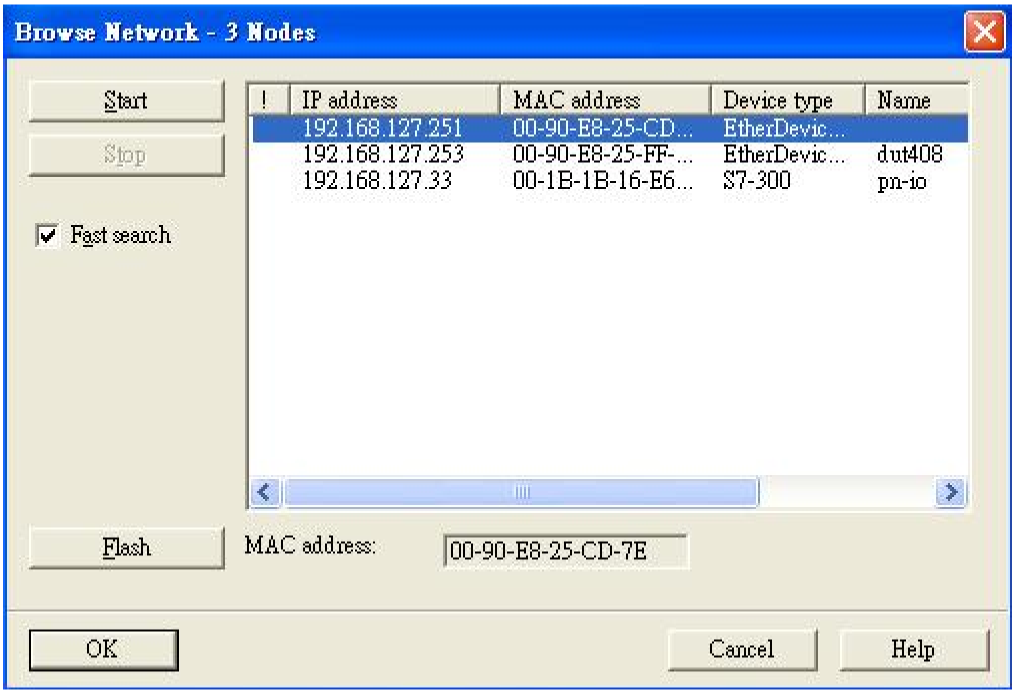
● Do not use router

○ Use router

○ Obtain IP address from a DHCP server

● Client ID ○ MAC address ○ Device name

- Select your target switch and click [OK]

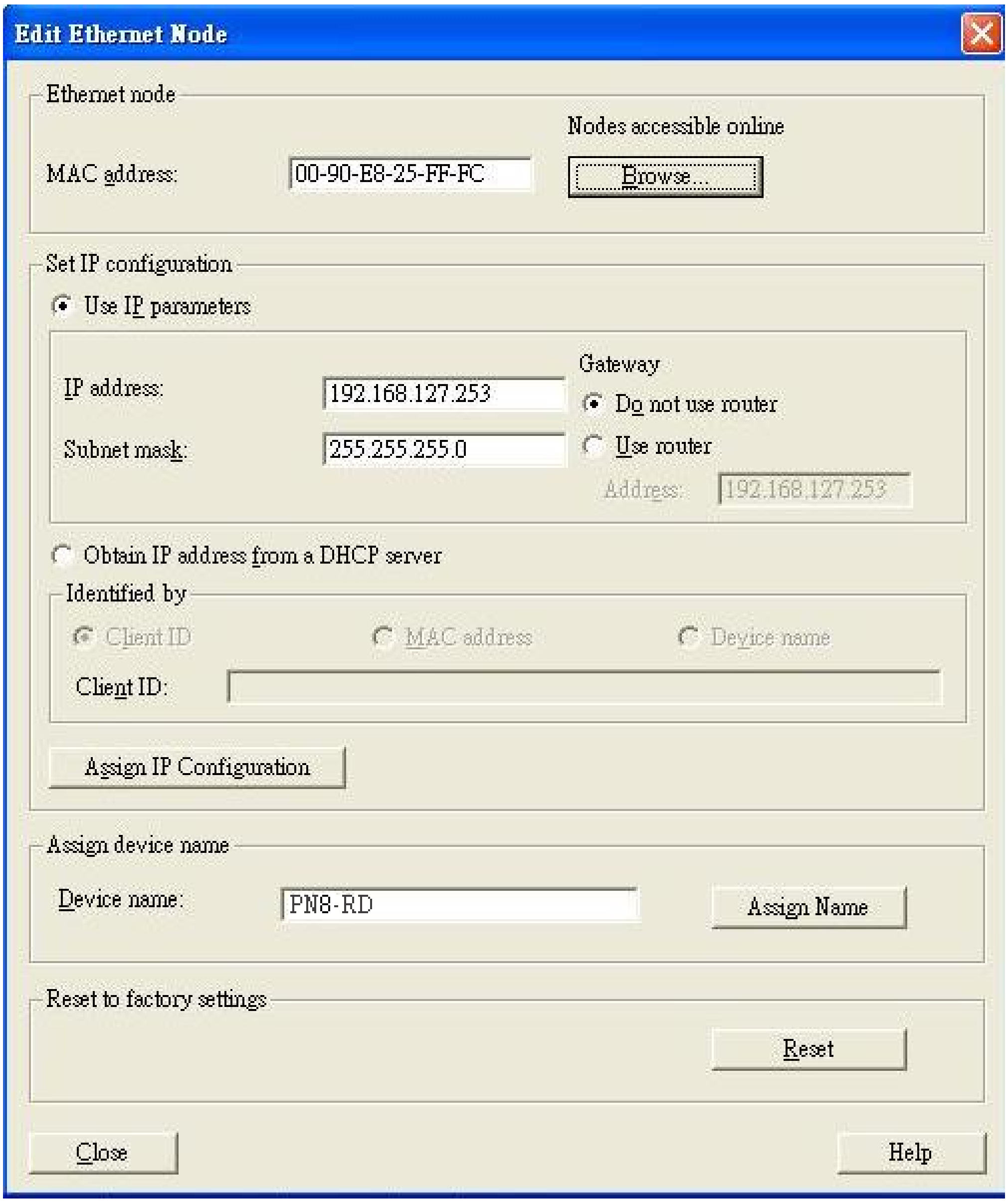


!	IP address	MAC address	Device type	Name
	192.168.127.251	00-90-E8-25-CD...	EtherDevic...	
	192.168.127.253	00-90-E8-25-FF-...	EtherDevic...	dut408
	192.168.127.33	00-1B-1B-16-E6...	S7-300	pn-io

MAC address: 00-90-E8-25-CD-7E

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.



Edit Ethernet Node

Ethernet node

MAC address: 00-90-E8-25-FF-FC

Set IP configuration

● Use IP parameters

IP address: 192.168.127.253

Subnet mask: 255.255.255.0

Gateway

● Do not use router

○ Use router

Address: 192.168.127.253

○ Obtain IP address from a DHCP server

Identified by

● Client ID ○ MAC address ○ Device name

Client ID:

Assign device name

Device name: PN8-RD

Reset to factory settings

➡

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

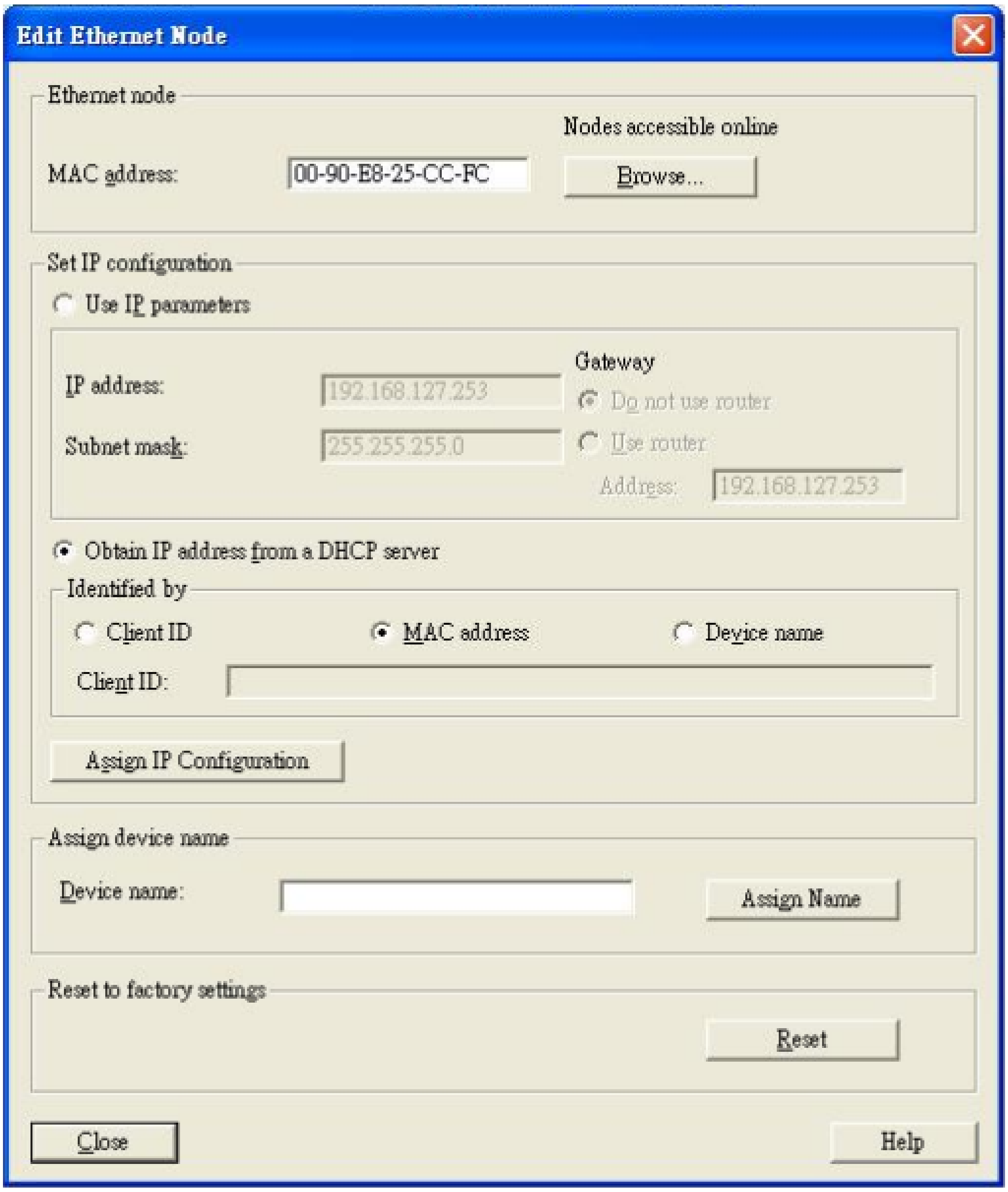
- Double-click the switch icon to open switch property menu.
- Set the*' Device name'* and *'IP address'* corresponding with those you have just assigned in STEP®7.

  '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].



Edit Ethernet Node

Ethernet node

MAC address: 00-90-E8-25-CC-FC

Set IP configuration

○ Use IP parameters

IP address: 192.168.127.253

Subnet mask: 255.255.255.0

Gateway

● Do not use router

○ Use router

Address: 192.168.127.253

● Obtain IP address from a DHCP server

Identified by

○ Client ID ● MAC address ○ Device name

Client ID:

Assign device name

Device name:

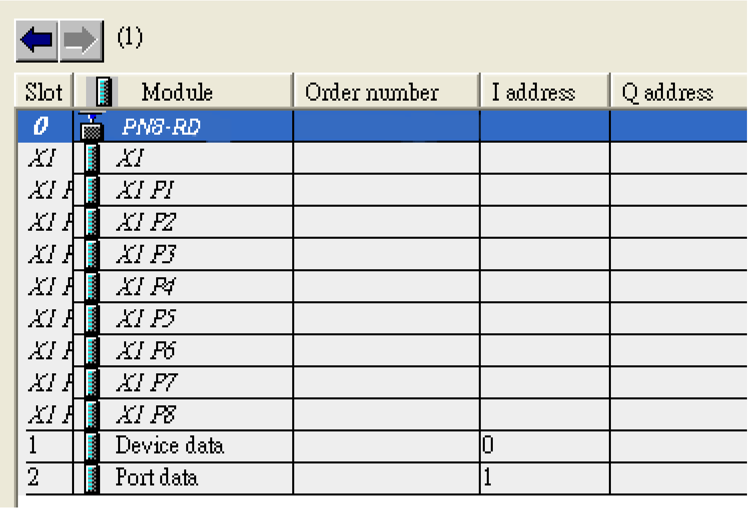
Reset to factory settings

➡ 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].

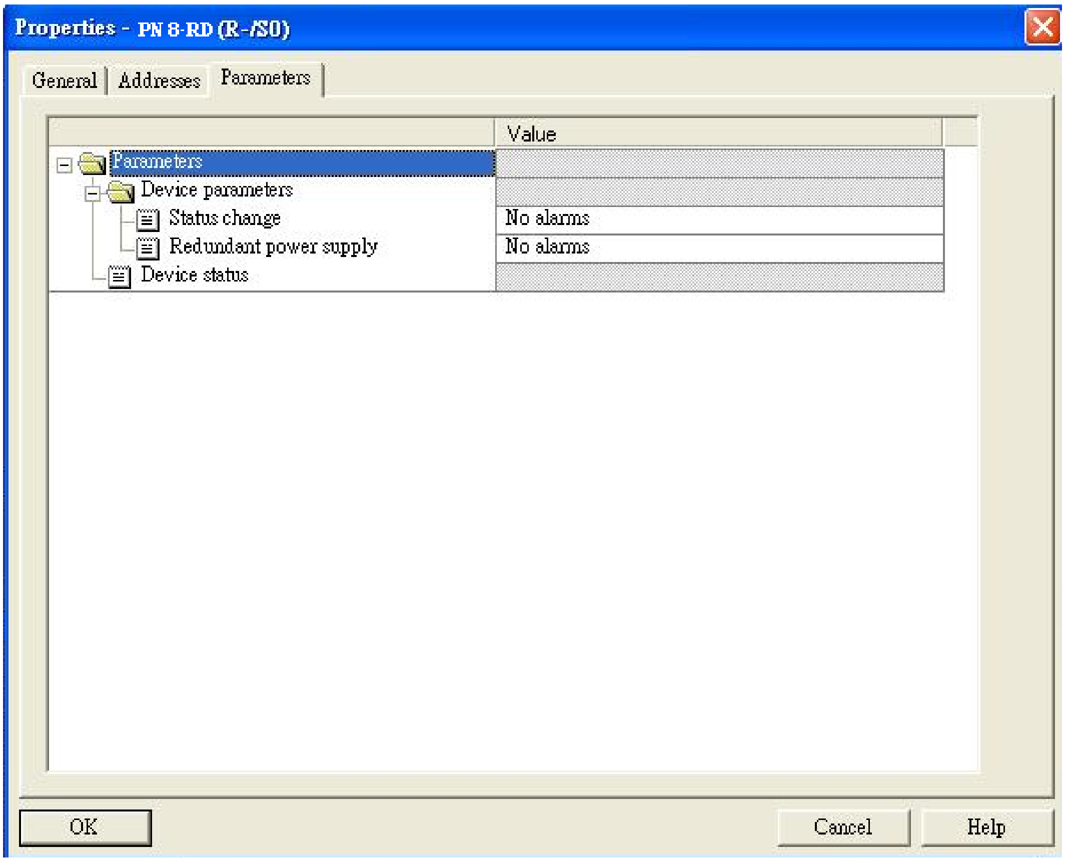
4. Configuring device properties

- 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*			
X1	*X1*			
X1 P	*X1 P1*			
X1 P	*X1 P2*			
X1 P	*X1 P3*			
X1 P	*X1 P4*			
X1 P	*X1 P5*			
X1 P	*X1 P6*			
X1 P	*X1 P7*			
X1 P	*X1 P8*			
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].

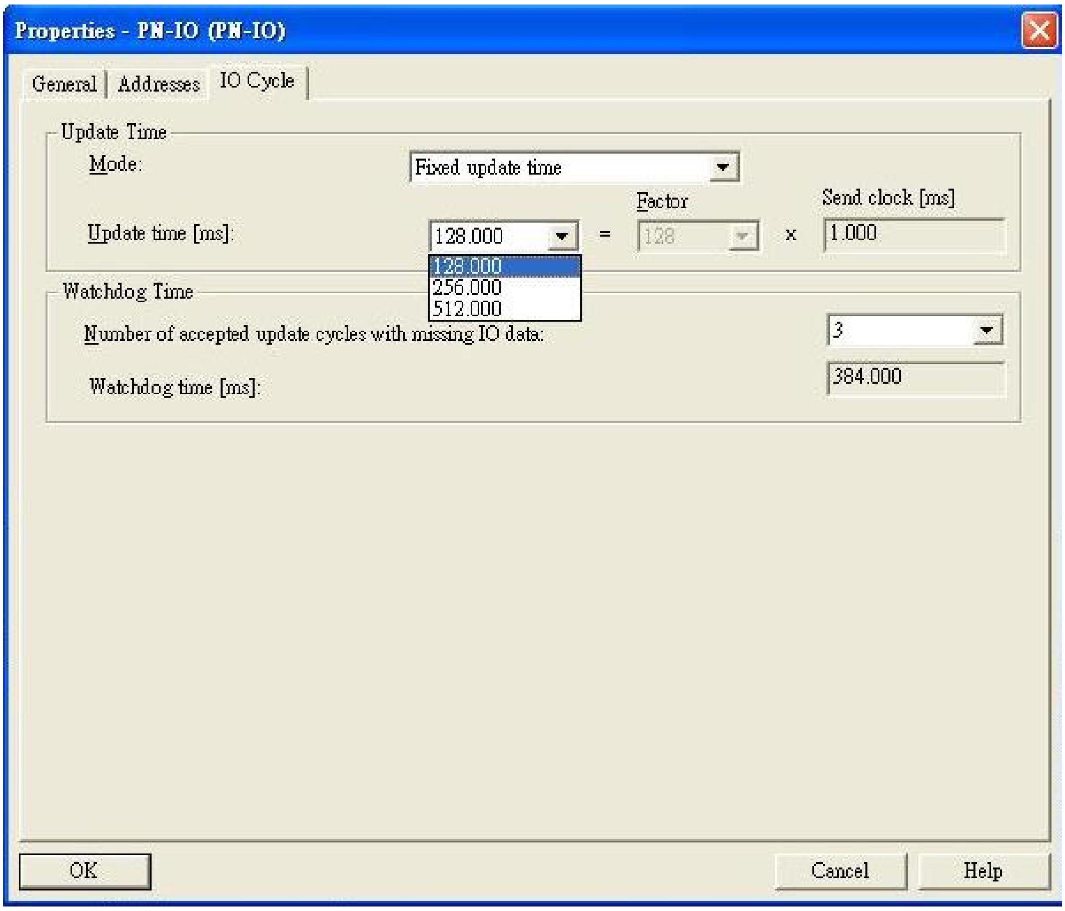


Properties - PN 8-RD (R-/S0)

	Value
Parameters	
Device parameters	
Status change	No alarms
Redundant power supply	No alarms
Device status	

5. Configuring I/O cycle

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



Mode: Fixed update time

Update time [ms]: 128.000 = Factor 128 x Send clock [ms] 1.000

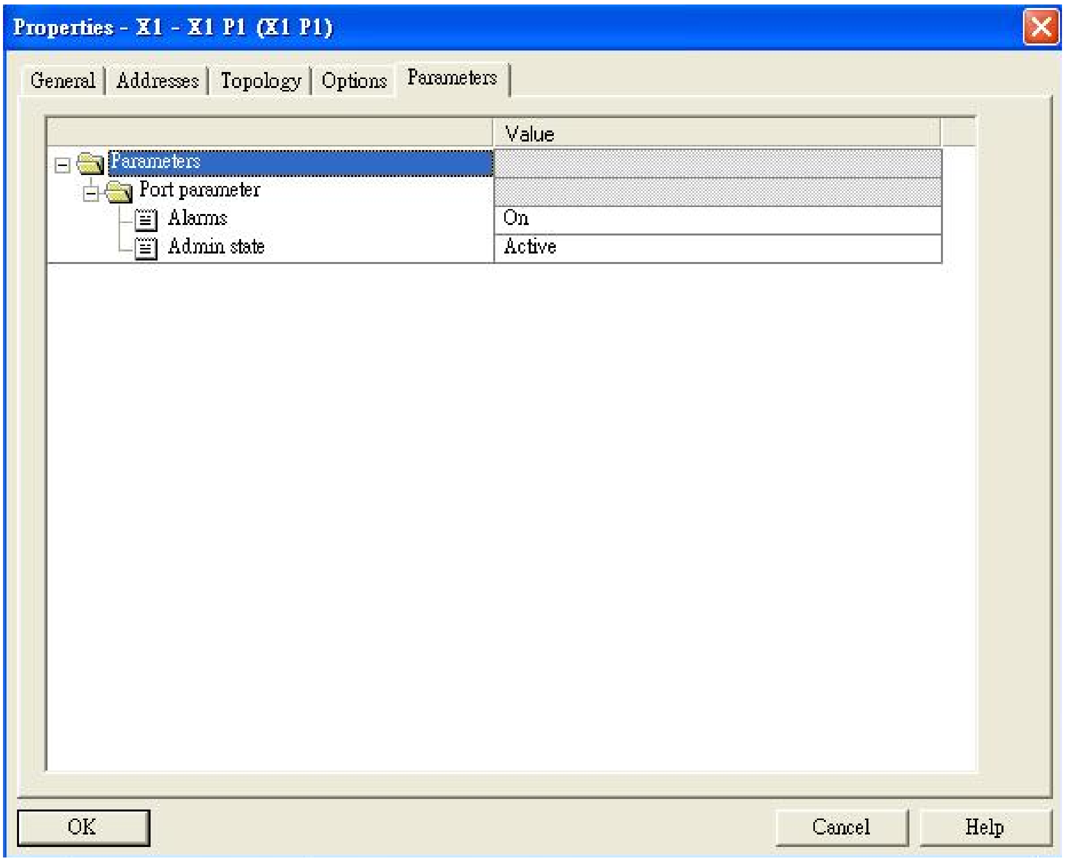
128.000
256.000
512.000

Number of accepted update cycles with missing IO data: 3

Watchdog time [ms]: 384.000

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].

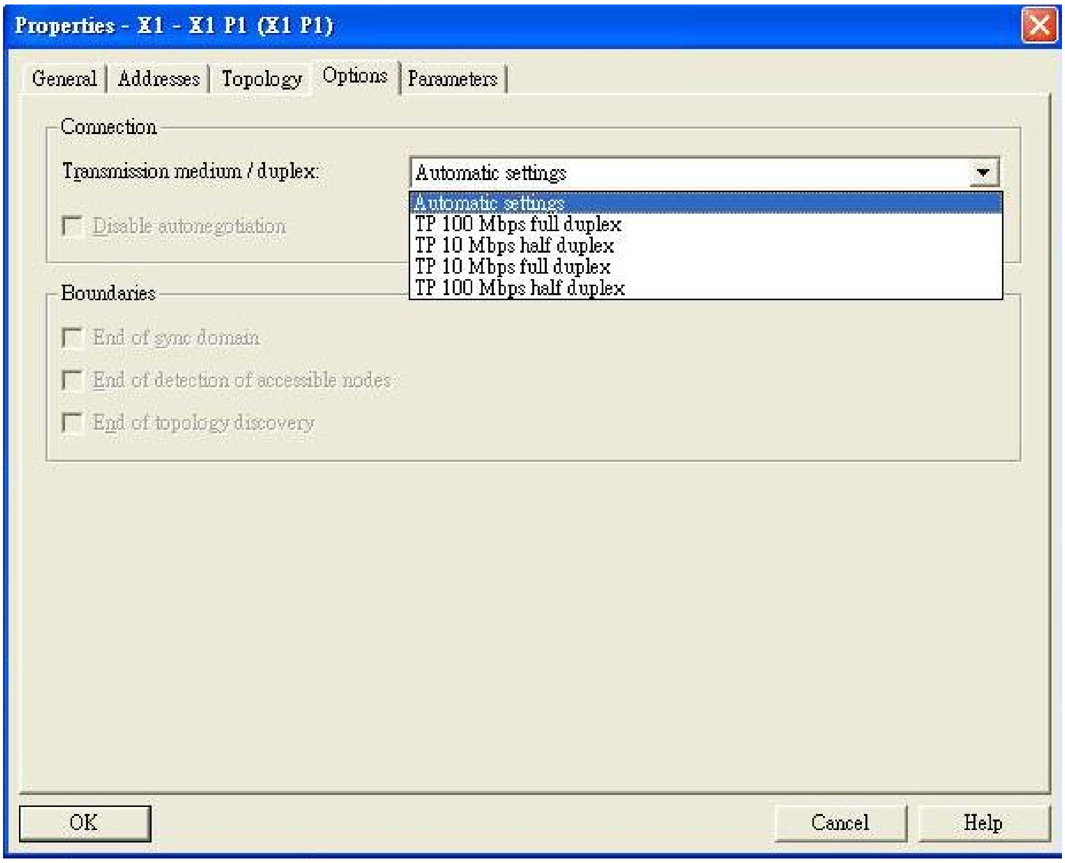


Properties - X1 - X1 P1 (X1 P1)

	Value
Parameters	
Port parameter	
Alarms	On
Admin state	Active

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]



Properties - X1 - X1 P1 (X1 P1)

Connection

Transmission medium / duplex: Automatic settings

□ Disable autonegotiation

Boundaries

□ End of sync domain

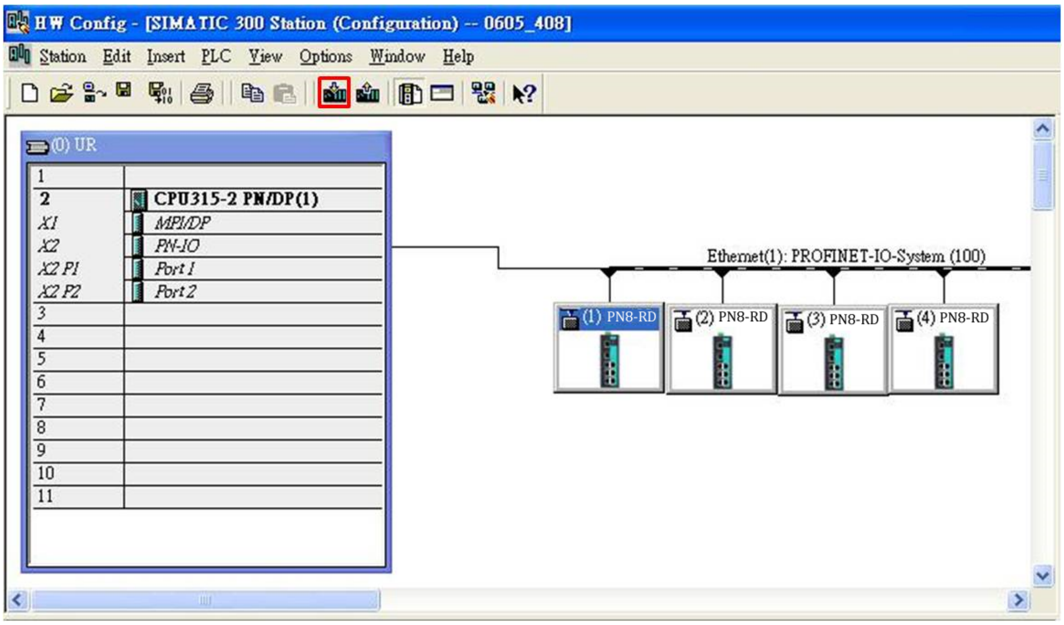
□ End of detection of accessible nodes

□ End of topology discovery

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.



HW Config - [SIMATIC 300 Station (Configuration) -- 0605_408]

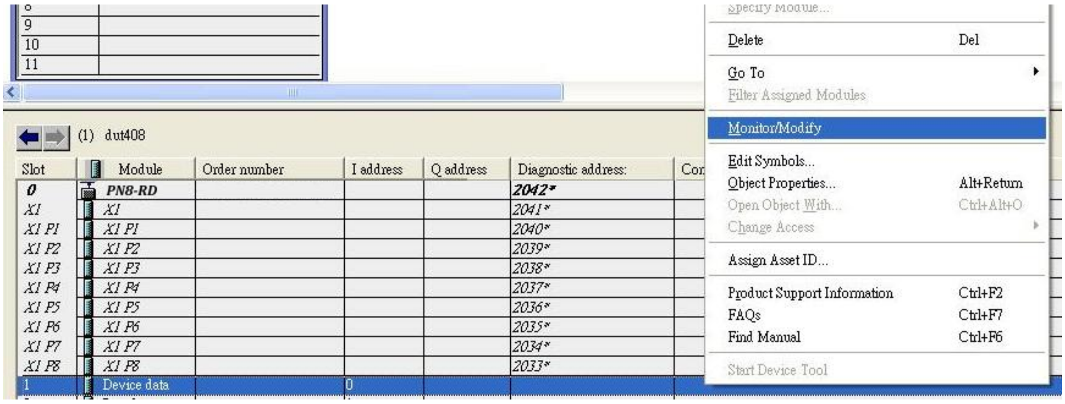
1	
2	CPU315-2 PN/DP(1)
X1	MPI/DP
X2	PN-IO
X2 P1	Port 1
X2 P2	Port 2
3	
4	
5	
6	
7	
8	
9	
10	
11	

6.3.7 Monitoring the Switch

Monitor PROFINET I/O Cyclic Data

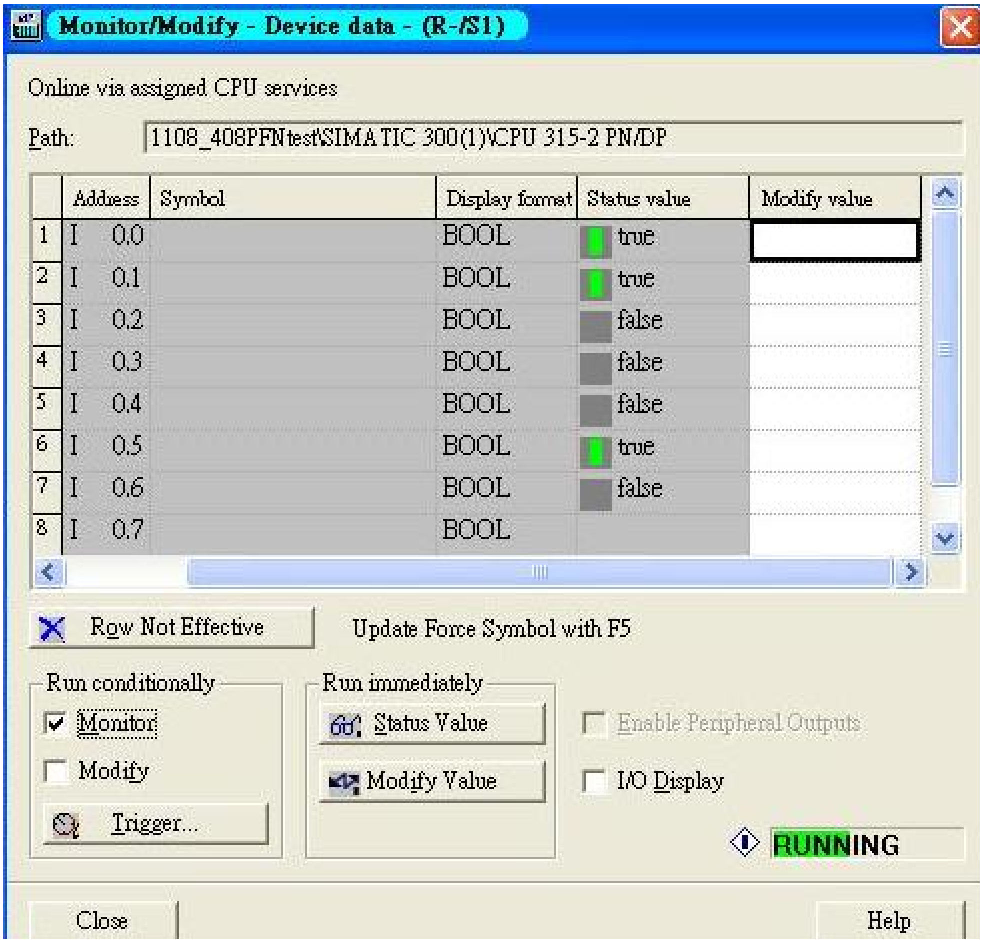
VIPA switches provide PROFINET I/O cyclic data for real-time monitoring. In side bar you can see *'Device data'* and *'Port data'*.

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



Slot	Module	Order number	I address	Q address	Diagnostic address:	Cor
0	***PN8-RD***				***2042****	
X1	*X1*				*2041**	
X1 P1	*X1 P1*				*2040**	
X1 P2	*X1 P2*				*2039**	
X1 P3	*X1 P3*				*2038**	
X1 P4	*X1 P4*				*2037**	
X1 P5	*X1 P5*				*2036**	
X1 P6	*X1 P6*				*2035**	
X1 P7	*X1 P7*				*2034**	
X1 P8	*X1 P8*				*2033**	
1	Device data		0			

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



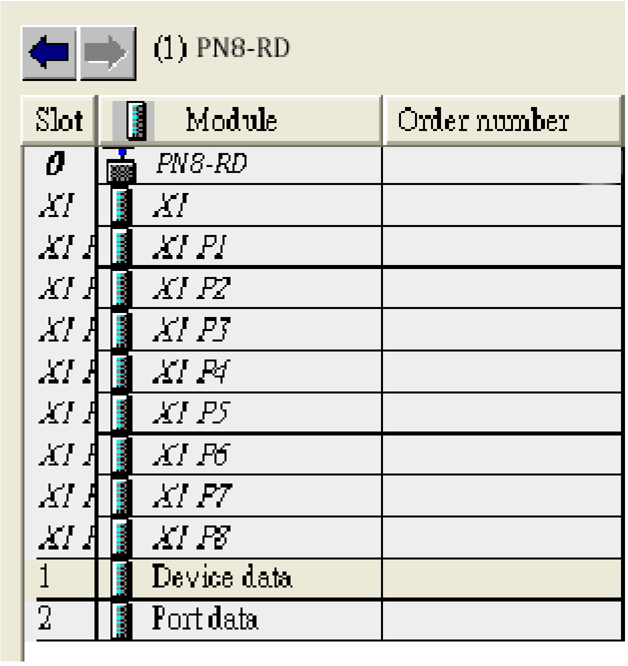
Online via assigned CPU services

Path: 1108_408PFNtest\SIMATIC 300(1)\CPU 315-2 PN/DP

	Address	Symbol	Display format	Status value	Modify value
1	I 0.0		BOOL	🟩 true	
2	I 0.1		BOOL	🟩 true	
3	I 0.2		BOOL	■ false	
4	I 0.3		BOOL	■ false	
5	I 0.4		BOOL	■ false	
6	I 0.5		BOOL	🟩 true	
7	I 0.6		BOOL	■ false	
8	I 0.7		BOOL		

☑ Monitor
☐ Modify
☐ Enable Peripheral Outputs
☐ I/O Display

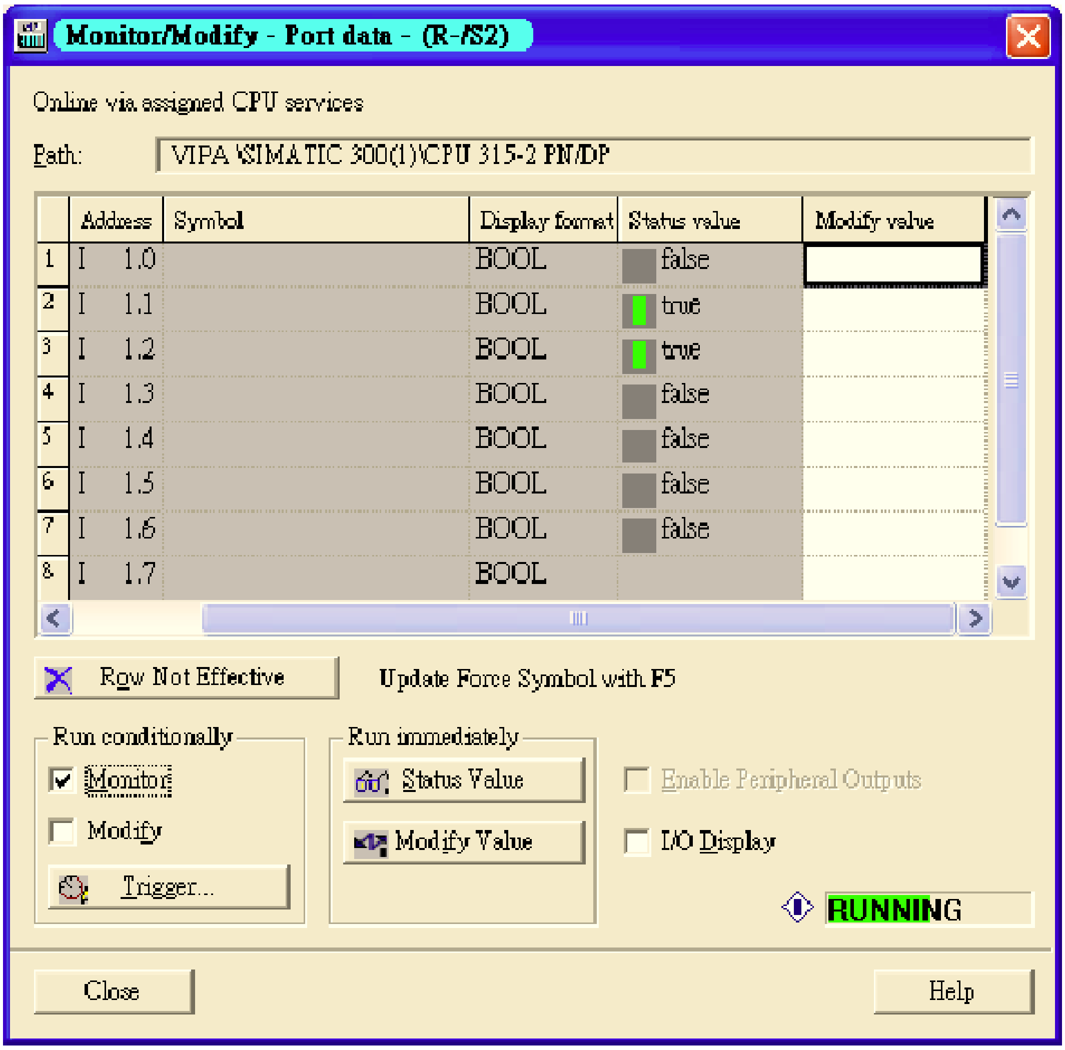
3. To monitor Port data, follow the same steps, drag *'Port data'* in the side bar and drop it onto *'slot 2'*. VIPA PROFINET I/O cyclic data in the slot 1 and 2



(1) PN8-RD

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

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



Monitor/Modify - Port data - (R-/S2)

Online via assigned CPU services

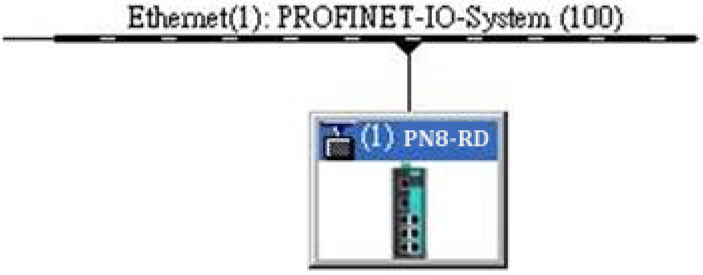
Path: VIPA \SIMATIC 300(1)\CPU 315-2 PN/DP

	Address	Symbol	Display format	Status value	Modify value
1	I 1.0		BOOL	■ false	
2	I 1.1		BOOL	🟩 true	
3	I 1.2		BOOL	🟩 true	
4	I 1.3		BOOL	■ false	
5	I 1.4		BOOL	■ false	
6	I 1.5		BOOL	■ false	
7	I 1.6		BOOL	■ false	
8	I 1.7		BOOL		

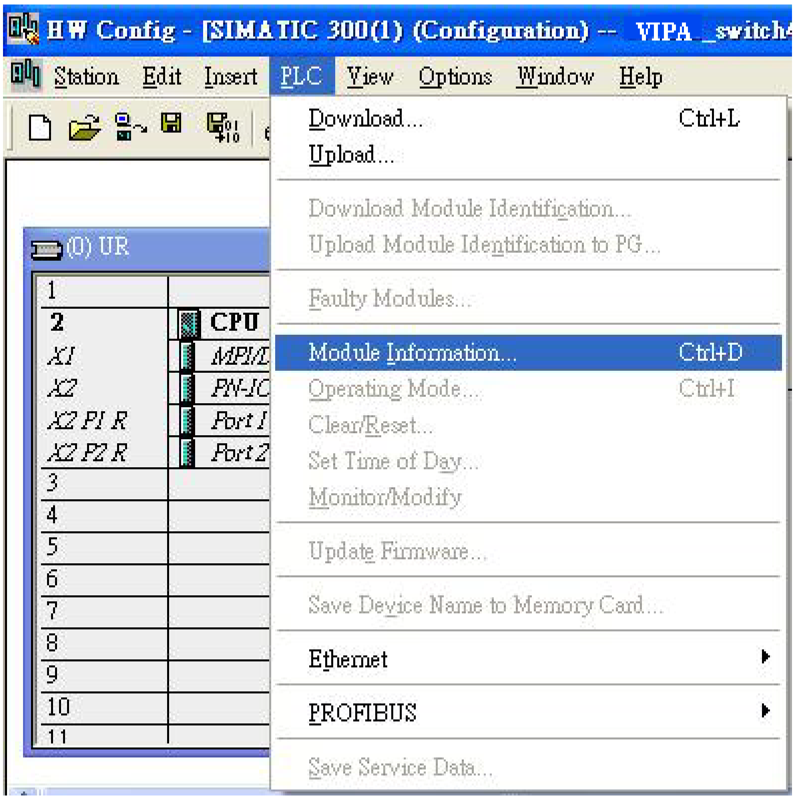
Module Information

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.



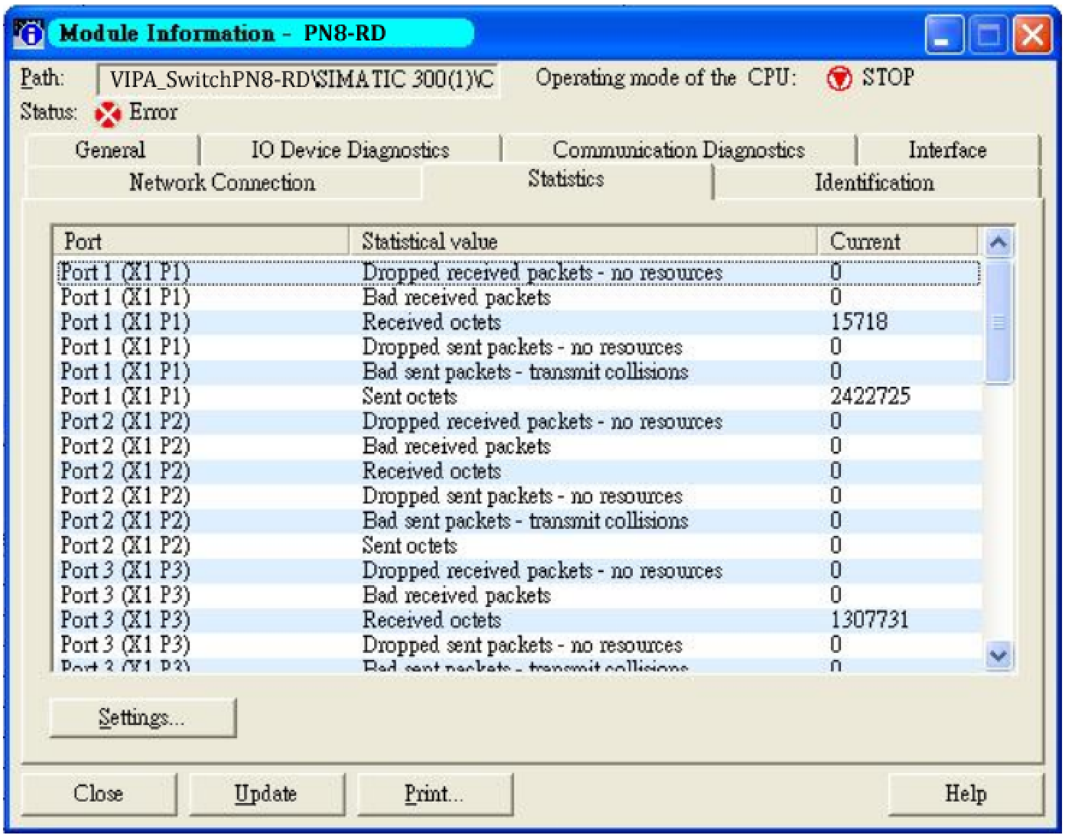
2. Then, click menu bar *'PLC → Module Information'*


HW Config - [SIMATIC 300(1) (Configuration) -- VIPA _switch
Station Edit Insert PLC View Options Window Help
Download... Ctrl+L
Upload...
Download Module Identification...
Upload Module Identification to PG...
Faulty Modules...
Module Information... Ctrl+D
Operating Mode... Ctrl+I
Clear/Reset...
Set Time of Day...
Monitor/Modify
Update Firmware...
Save Device Name to Memory Card...
Ethernet
PROFIBUS
Save Service Data...
(0) UR
1
2 CPU
X1 MPI/D
X2 PN-IO
X2 P1 R Port 1
X2 P2 R Port 2
3
4
5
6
7
8
9
10
11

➡ The module information dialog will then pop up.

Port Statistics Output

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



Path: VIPA_SwitchPN8-RD\SIMATIC 300(1)\C

Operating mode of the CPU: STOP

Status: Error

Port	Statistical value	Current
Port 1 (X1 P1)	Dropped received packets - no resources	0
Port 1 (X1 P1)	Bad received packets	0
Port 1 (X1 P1)	Received octets	15718
Port 1 (X1 P1)	Dropped sent packets - no resources	0
Port 1 (X1 P1)	Bad sent packets - transmit collisions	0
Port 1 (X1 P1)	Sent octets	2422725
Port 2 (X1 P2)	Dropped received packets - no resources	0
Port 2 (X1 P2)	Bad received packets	0
Port 2 (X1 P2)	Received octets	0
Port 2 (X1 P2)	Dropped sent packets - no resources	0
Port 2 (X1 P2)	Bad sent packets - transmit collisions	0
Port 2 (X1 P2)	Sent octets	0
Port 3 (X1 P3)	Dropped received packets - no resources	0
Port 3 (X1 P3)	Bad received packets	0
Port 3 (X1 P3)	Received octets	1307731
Port 3 (X1 P3)	Dropped sent packets - no resources	0
Port 3 (X1 P3)	Bad sent packets - transmit collisions	0

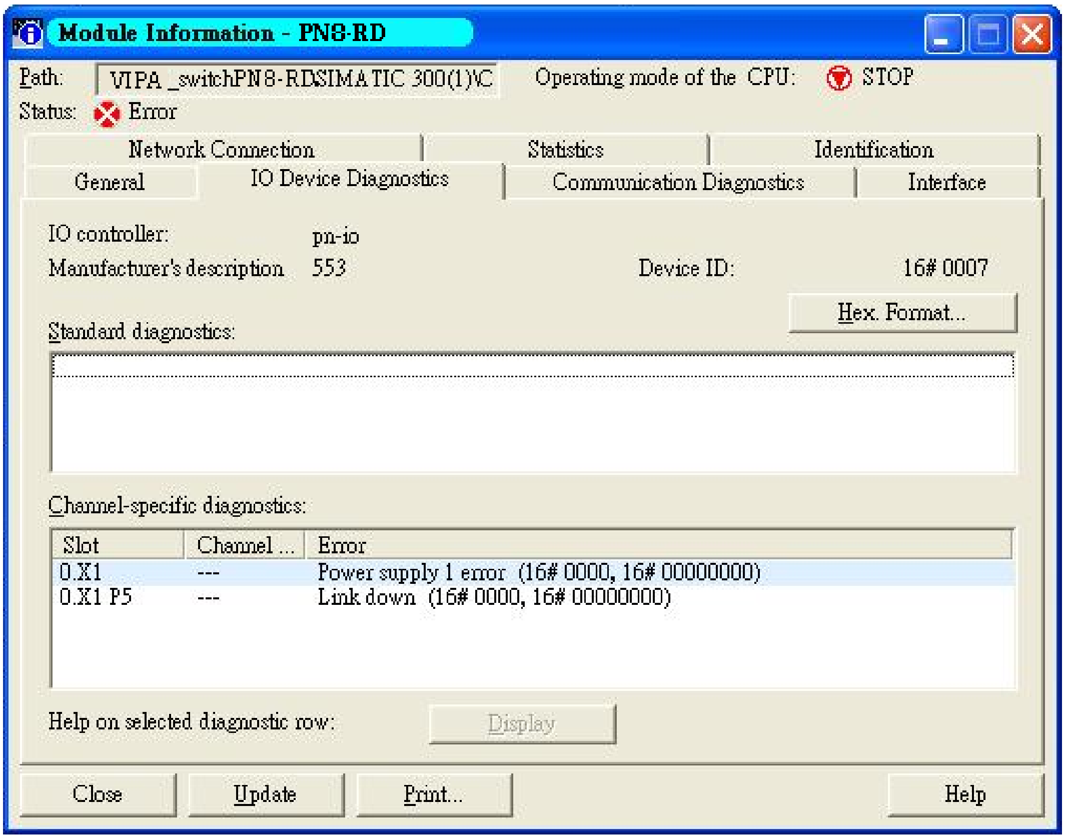
➡ Statistics tab lists each port traffic status and the number of packets.

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.



Path: VIPA _switchPN8-RD\SIMATIC 300(1)\C

Operating mode of the CPU: STOP

Status: Error

IO controller: pn-io

Manufacturer's description 553

Device ID: 16# 0007

Standard diagnostics:

Channel-specific diagnostics:

Slot	Channel ...	Error
0.X1	---	Power supply 1 error (16# 0000, 16# 00000000)
0.X1 P5	---	Link down (16# 0000, 16# 00000000)

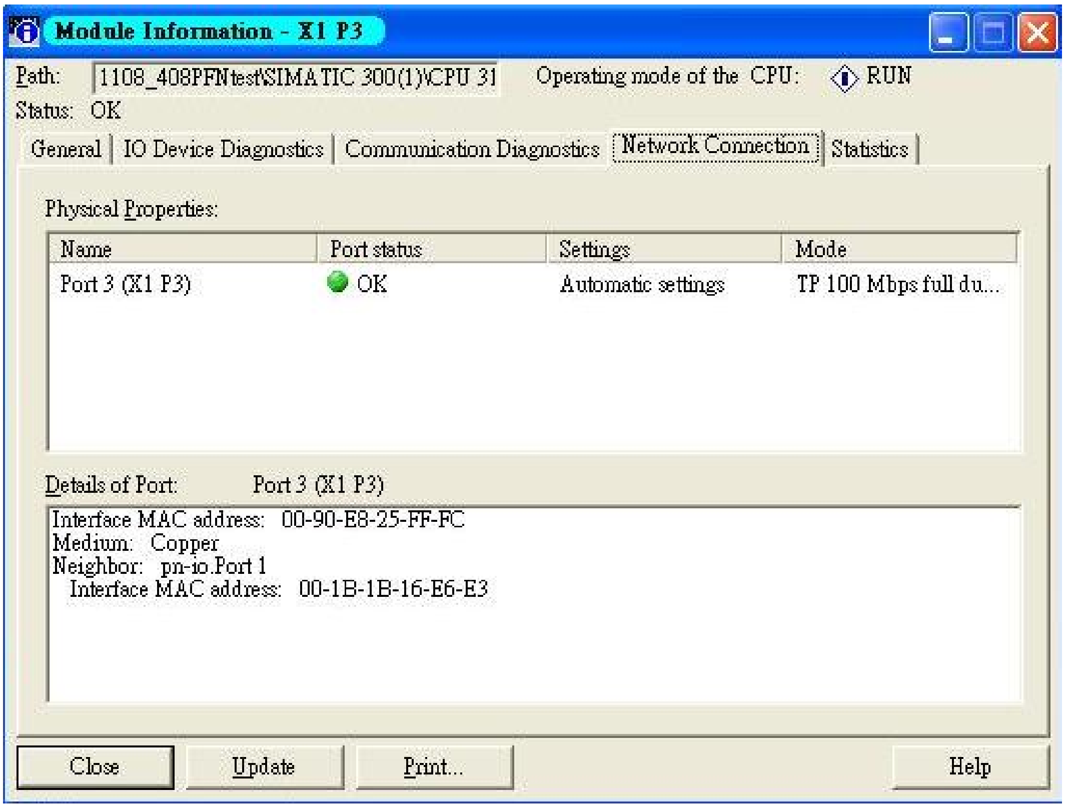
Help on selected diagnostic row:

➡ 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.



Path: 1108_408PFNtest\SIMATIC 300(1)\CPU 31

Operating mode of the CPU: RUN

Status: OK

Physical Properties:

Name	Port status	Settings	Mode
Port 3 (X1 P3)	● OK	Automatic settings	TP 100 Mbps full du...

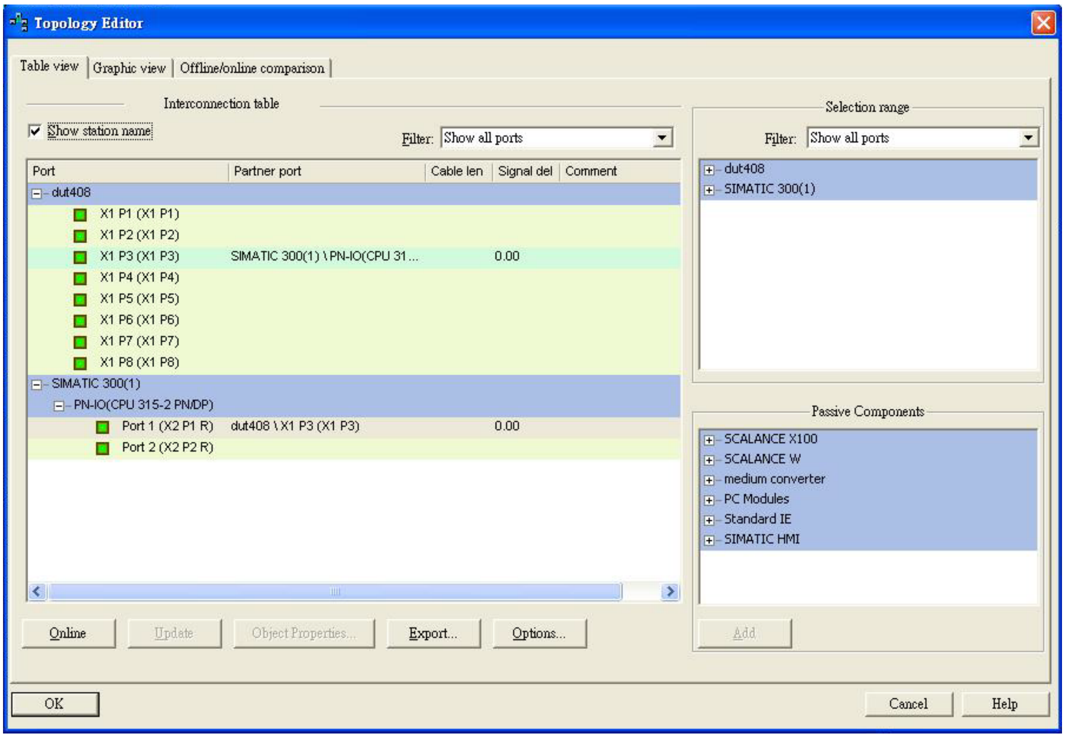
Details of Port: Port 3 (X1 P3)

```
Interface MAC address:  00-90-E8-25-FF-FC
Medium:  Copper
Neighbor:  pn-io.Port 1
  Interface MAC address:  00-1B-1B-16-E6-E3
```

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.



☑ Show station name

Filter: Show all ports

Port	Partner port	Cable len	Signal del	Comment
⊟ dut408				
🟩 X1 P1 (X1 P1)				
🟩 X1 P2 (X1 P2)				
🟩 X1 P3 (X1 P3)	SIMATIC 300(1) \ PN-IO(CPU 31 ...		0.00	
🟩 X1 P4 (X1 P4)				
🟩 X1 P5 (X1 P5)				
🟩 X1 P6 (X1 P6)				
🟩 X1 P7 (X1 P7)				
🟩 X1 P8 (X1 P8)				
⊟ SIMATIC 300(1)				
⊟ PN-IO(CPU 315-2 PN/DP)				
🟩 Port 1 (X2 P1 R)	dut408 \ X1 P3 (X1 P3)		0.00	
🟩 Port 2 (X2 P2 R)				

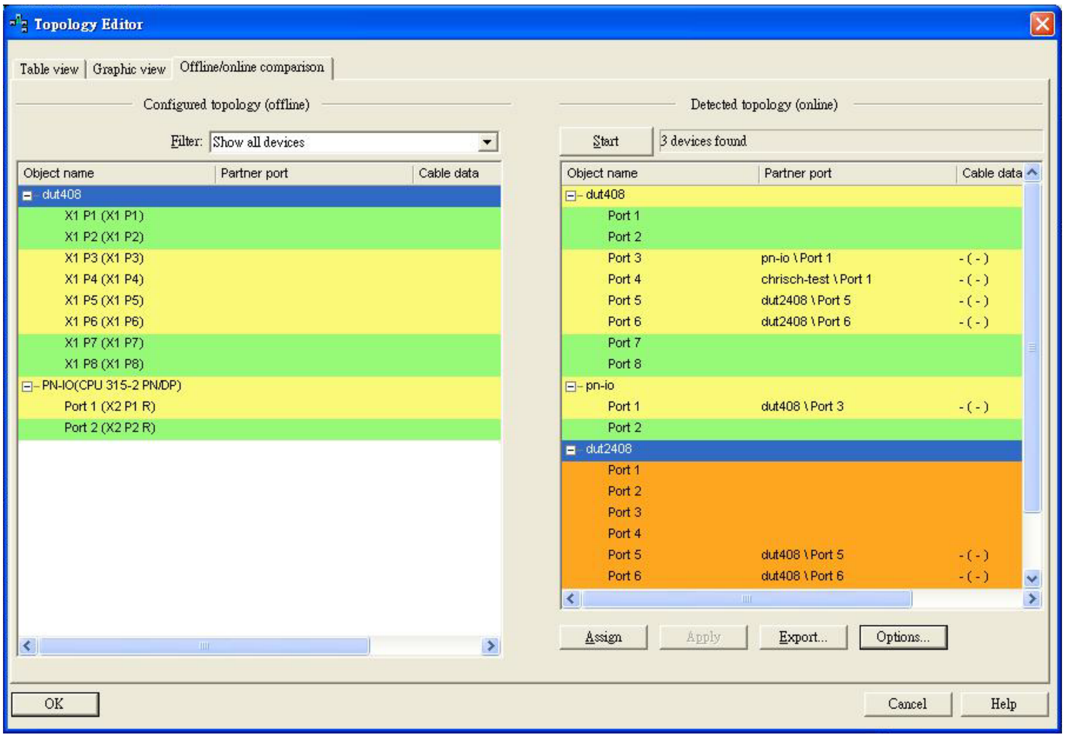
Selection range — Filter: Show all ports

- ⊞ dut408
- ⊞ SIMATIC 300(1)

Passive Components

- ⊞ SCALANCE X100
- ⊞ SCALANCE W
- ⊞ medium converter
- ⊞ PC Modules
- ⊞ Standard IE
- ⊞ SIMATIC HMI

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



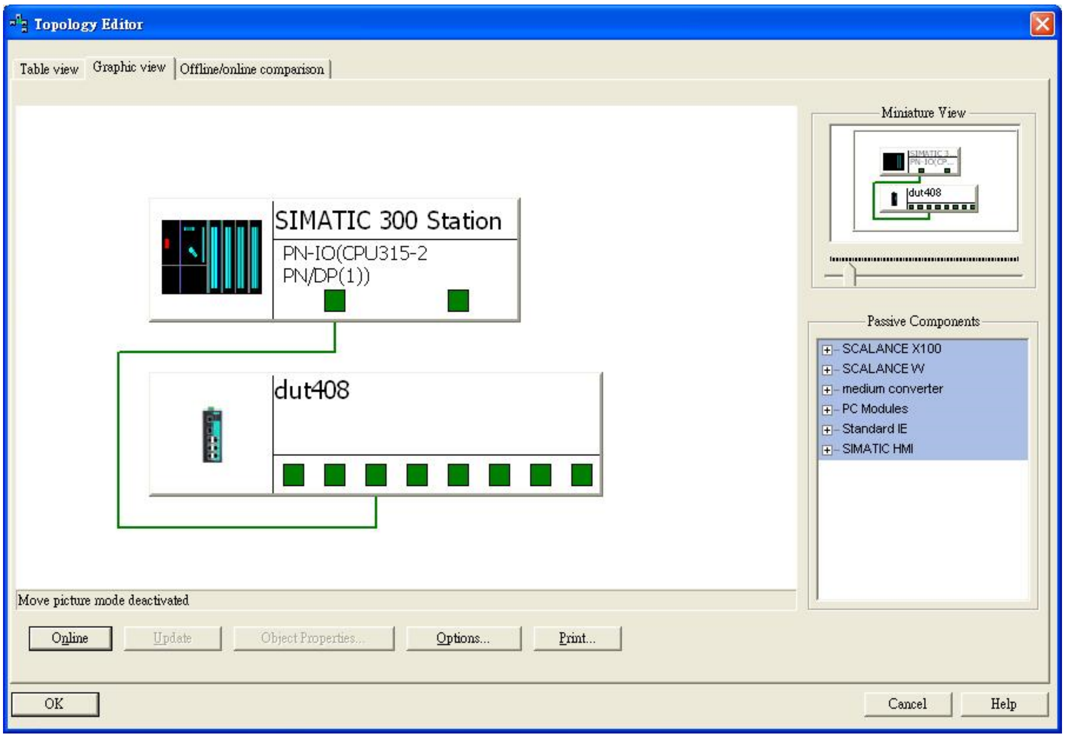
Configured topology (offline) — Filter: Show all devices

Object name	Partner port	Cable data
⊟ dut408		
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)		
⊟ PN-IO(CPU 315-2 PN/DP)		
Port 1 (X2 P1 R)		
Port 2 (X2 P2 R)		

Detected topology (online) — 3 devices found

Object name	Partner port	Cable data
⊟ dut408		
Port 1		
Port 2		
Port 3	pn-io \ Port 1	- (-)
Port 4	chrisch-test \ Port 1	- (-)
Port 5	dut2408 \ Port 5	- (-)
Port 6	dut2408 \ Port 6	- (-)
Port 7		
Port 8		
⊟ pn-io		
Port 1	dut408 \ Port 3	- (-)
Port 2		
⊟ dut2408		
Port 1		
Port 2		
Port 3		
Port 4		
Port 5	dut408 \ Port 5	- (-)
Port 6	dut408 \ Port 6	- (-)

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



Topology Editor
Table view
Graphic view
Offline/online comparison
SIMATIC 300 Station
PN-IO(CPU315-2 PN/DP(1))
dut408
Miniature View
Passive Components
SCALANCE X100
SCALANCE W
medium converter
PC Modules
Standard IE
SIMATIC HMI
Move picture mode deactivated
Online
Update
Object Properties...
Options...
Print...
OK
Cancel
Help

7 Appendix

Appendix - Table of contents

A Command Line Interface

Appendix

A Command Line Interface

Command Modes

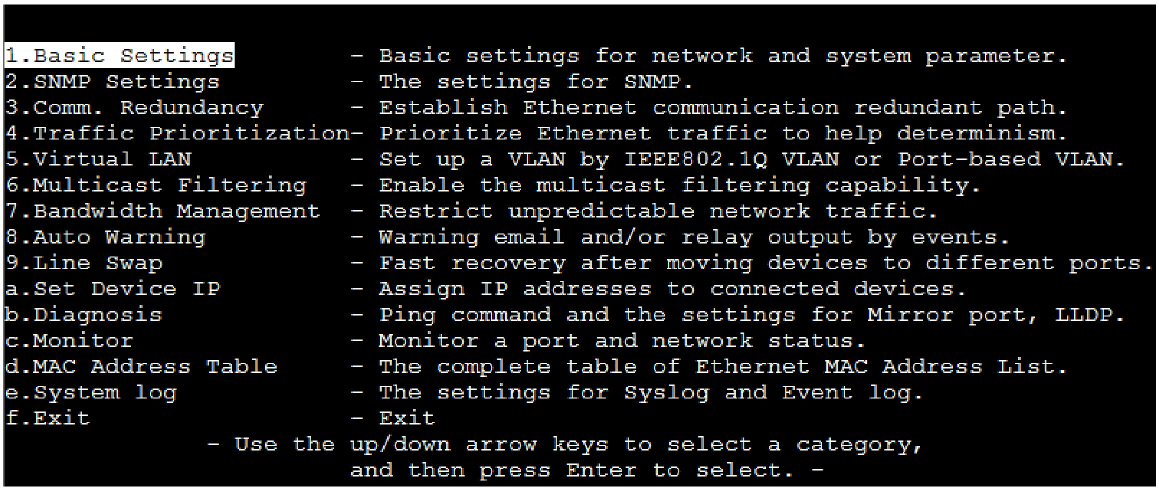
CLI (Command Line Interface)

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

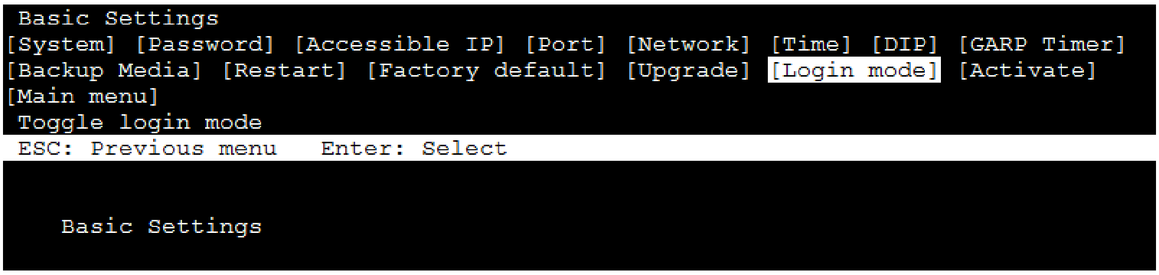
The default configuration mode for both the serial console and Telnet console is MENU mode. To change the VIPA switch to CLI configuration mode, **Login Mode** from **Basic Settings** and then press **y** to activate the change. You will then be able to view the CLI display in the console. (Note that 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
```