

PCS-9882XD-H2
Managed Ethernet Switch
Instruction Manual

NR Electric Co., Ltd.

Preface

Introduction

This guide and the relevant operating or service manual documentation for the equipment provide full information on safe handling, commissioning and testing of this equipment.

Documentation for equipment ordered from NR is dispatched separately from manufactured goods and may not be received at the same time. Therefore, this guide is provided to ensure that printed information normally present on equipment is fully understood by the recipient.

Before carrying out any work on the equipment, the user should be familiar with the contents of this manual, and read relevant chapter carefully.

This chapter describes the safety precautions recommended when using the equipment. Before installing and using the equipment, this chapter must be thoroughly read and understood.

Health and Safety

The information in this chapter of the equipment documentation is intended to ensure that equipment is properly installed and handled in order to be maintained in a safe condition.

When electrical equipment is in operation, dangerous voltages will be present in certain parts of the equipment. Failure to observe warning notices, incorrect use, or improper use may endanger personnel and equipment and cause personal injury or physical damage.

Before working in the terminal strip area, the equipment must be isolated.

Proper and safe operation of the equipment depends on appropriate shipping and handling, proper storage, installation and commissioning, and on careful operation, maintenance and servicing. For this reason, only qualified personnel may work on or operate the equipment.

Qualified personnel are individuals who:

- Are familiar with the installation, commissioning, and operation of the equipment and of the system to which it is being connected;
- Are able to safely perform switching operations in accordance with accepted safety engineering practices and are authorized to energize and de-energize equipment and to isolate, ground, and label it;
- Are trained in the care and use of safety apparatus in accordance with safety engineering practices;
- Are trained in emergency procedures (first aid).

Instructions and Warnings

The following indicators and standard definitions are used:



DANGER! means that death, severe personal injury and considerable equipment damage will occur if safety precautions are disregarded.



WARNING! means that death, severe personal and considerable equipment damage could occur if safety precautions are disregarded.



CAUTION! means that light personal injury or equipment damage may occur if safety precautions are disregarded.

NOTICE! is particularly applied to device damage and resulting damage of equipment.



WARNING!

ONLY qualified personnel should work on or near this device. This personnel **MUST** be familiar with all safety regulations and service procedures described in this manual. During operating of electrical device, certain part of the device is under high voltage. Severe personal injury and significant device damage could result from improper behavior.



WARNING!

Do **NOT** touch the exposed terminals of this device while the power supply is on. The generated high voltage causes death, injury, and device damage.



WARNING!

Thirty seconds is **NECESSARY** for discharging the voltage. Hazardous voltage can be present in the DC circuit just after switching off the DC power supply.



CAUTION!

- **Earthing**

Securely earth the device earthing terminal.

- **Operating environment**

ONLY use the device within the range of ambient environment and in an environment free of abnormal vibration.

- **Ratings**

Check the input ratings **BEFORE** applying AC voltage/current and power supply to the device.

- **Printed circuit board**

Do **NOT** attach or remove printed circuit board if the device is powered on.

- **External circuit**

Check the supply voltage used when connecting the device output contacts to external circuits, in order to prevent overheating.

- **Connection cable**

Carefully handle connection cables without applying excessive force.

NOTICE!

The firmware may be upgraded to add new features or enhance/modify existing features, please **MAKE SURE** that the version of this manual is compatible with the product in your hand.

Copyright © 2019 NR. All rights reserved.

We reserve all rights to this document and to the information contained herein. Improper use in particular reproduction and dissemination to third parties is strictly forbidden except where expressly authorized.

The information in this manual is carefully checked periodically, and necessary corrections will be included in future editions. If nevertheless any errors are detected, suggestions for correction or improvement are greatly appreciated.

We reserve the rights to make technical improvements without notice.

NR ELECTRIC CO., LTD.

Headquarters: 69, Suyuan Avenue, Jiangning, Nanjing 211102, China

Manufactory: 18, Xinfeng Road, Jiangning, Nanjing 211111, China

Tel: +86-25-87178888

Fax: +86-25-87178999

Website: www.nrec.com

P/N: ZL_PCS-9882XD-H2_X_Instruction Manual_EN_Overseas General_X

Version: R1.00

Document Structure

The manual provides a functional and technical description of this device and a comprehensive set of instructions for the device's use and application.

All contents provided by this manual are summarized as below.

1 Introduction

Brief introduction of the application, functions and features.

2 Technical Data

Lists of the technical data such as electrical specifications, mechanical specifications, ambient temperature and humidity range, communication port parameters, type tests and accuracy limits.

3 Hardware

Description of communication interfaces, LED indicators and terminal definition.

4 Configurable Functions

Brief introduction of configurable functions and configuration methods.

5 Installation

Recommendation for unpacking, handling, inspection and storage with a guide to the mechanical and electrical installation. A typical wiring connection is also indicated.

6 Commissioning

Commissioning recommendation for comprising checks on the calibration and functionality of device.

7 Maintenance

General maintenance policy.

8 Decommissioning and Disposal

General decommissioning and disposal policy.

9 Revision History

List of document revisions and history records of update.

1 Introduction

Table of Contents

1 Introduction	1-a
1.1 Application	1-1
1.2 Function	1-2
1.2.1 Ethernet Switching	1-2
1.2.2 Flow Control	1-2
1.2.3 VLAN	1-3
1.2.4 Ring Network	1-3
1.2.5 Multicast	1-3
1.2.6 Port Security	1-3
1.2.7 Clock Synchronization	1-3
1.2.8 File Management.....	1-3
1.2.9 Management Method	1-4
1.3 Features.....	1-4



1.1 Application

The PCS-9882XD-H2 series managed Ethernet switches are applicable to conventional and digital substation integrated automation systems, power plant NCS and DCS systems, industrial control systems, etc. They provide gigabit Ethernet interfaces to realize high data transmission rate, to meet the requirements of cascading in power and industrial automation networks and to meet the growing demand of communication equipment.

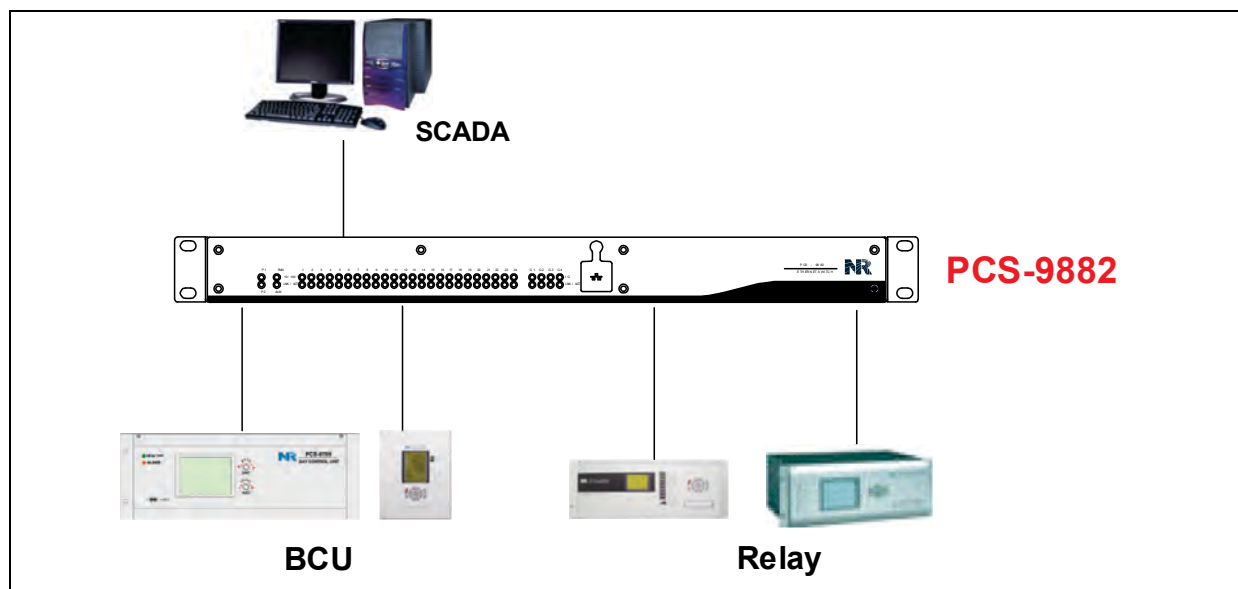


Figure 1.1-1 Typical application

The PCS-9882XD-H2 series managed Ethernet switches could support up to 24 megabit fast Ethernet interfaces and 4 gigabit Ethernet interfaces. The optical interfaces are SFP sockets that support hot-plug technology for LC-type connectors.

The series could be divided into the following models according to interfaces quantity, rated voltage and power supply quantity.

Switch model	Gigabit interface		Megabit interface		Power supply	
	Optic	Copper	Optic	Copper	Quantity	Rated voltage
PCS-9882AD-H2 ^[1]	0~4	0 ^[3]	0~4	24	Double	110Vdc/220Vdc
PCS-9882AD-S-H2 ^[1]	0~4	0 ^[3]	0~4	24	Single	110Vdc/220Vdc
PCS-9882AD-LO-H2 ^[1]	0~4	0 ^[3]	0~4	24	Double	18Vdc~72Vdc
PCS-9882AD-S-LO-H2 ^[1]	0~4	0 ^[3]	0~4	24	Single	18Vdc~72Vdc
PCS-9882BD-H2 ^[2]	0~4	0 ^[3]	0~28	0~24	Double	110Vdc/220Vdc
PCS-9882BD-S-H2 ^[2]	0~4	0 ^[3]	0~28	0~24	Single	110Vdc/220Vdc
PCS-9882BD-LO-H2 ^[2]	0~4	0 ^[3]	0~28	0~24	Double	18Vdc~72Vdc
PCS-9882BD-S-LO-H2 ^[2]	0~4	0 ^[3]	0~28	0~24	Single	18Vdc~72Vdc

[1] For the PCS-9882AD-H2 series, the No.01~24 Ethernet interfaces are fast copper ports (10BASE-T/100BASE-TX).

[2] For the PCS-9882BD-H2 series, the No.01~24 Ethernet interfaces are SFP sockets for LC-

type connector (100BASE-FX) or fast copper port (10BASE-T/100BASE-TX).

- [3] For the PCS-9882XD-H2 series, the No. G1~G4 Ethernet interfaces are SFP sockets for LC-type connector (100BASE-FX/1000BASE-SX) or gigabit copper port (10BASE-T/100BASE-TX/1000BASE-T).

1.2 Function

1.2.1 Ethernet Switching

- Fast 10/100Mbps self-adaptive copper Ethernet ports

These ports are compatible with the 10BASE-T/100BASE-TX standard and are self-adaptive for crossover and straight-through network cable. MDI/MDIX automatic identification is supported.

- 100Mbps SFP sockets

The SFP transceiver complying with IEEE 802.3 100BASE-FX standard supports hot-plug technology.

- 100/1000Mbps SFP sockets

The SFP transceiver complying with IEEE 802.3 100BASE-FX/1000BASE-SX standard (1.25Gb/s) supports hot-plug technology.

- The switching mode is non-blocking store and forward.
- Support of IEEE 802.3x flow control.

1.2.2 Flow Control

- Network storm suppression

The upper rate limit of broadcasting/multicasting/addressing-failure message is configurable.

- Port rate limitation

The message forwarding rate and burst rate of each port is configurable.

- Port mirror

Monitoring the inflow/outflow data of all the ports can be realized through one designed port.

- Link aggregation

Link aggregation can be based on port number, MAC address, etc.

- Quality of Service control (QoS)

The message priority control based on IEEE 802.1p is supported, including the strict priority strategy and the weighted priority strategy.

1.2.3 VLAN

- Support of VLAN based on port
- Support of VLAN based on protocol
- Support of VLAN based on IEEE 802.1Q
- Support of overlapped VLAN configuration
- Support of VLAN tag insertion, modification and deletion
- Support of GARP VLAN registration protocol

1.2.4 Ring Network

- Support of STP (IEEE 802.1D), RSTP (IEEE 802.1w) and MSTP ring network protocol so as to fast switch to a backup link in case of link failure
- Support of MRP protocol

1.2.5 Multicast

- Support of static multicast management based on MAC address
- Support of GMRP dynamic multicast management
- Support of IGMP snooping dynamic multicast management.

1.2.6 Port Security

- Support of port security certification based on static MAC address
- Support of port security certification based on IEEE 802.1X
- Support of RADIUS Server to cooperate with IEEE 802.1X for remote and local certification
- Support of network security protocol based on SSL/SSH
- Free of DoS attack
- Support of security log and operation log

1.2.7 Clock Synchronization

- Support of SNTP Server/Client synchronization mode
- Support of NTP Server synchronization mode

1.2.8 File Management

- Support of offline modification of Ethernet switch configuration file
- Support of uploading and downloading of Ethernet switch configuration file
- Support of PC downloading of Ethernet switch log and event file

- Support of import function of multicast configuration based on CSD

1.2.9 Management Method

- Support of WEB Server, SSH/SSL and CLI
- Support of SNMP V1/V2C/V3.
- Support of RMON
- Providing of alarm output contact and block output contact via relay
- Support of IP conflict detection
- Support of LLDP
- Support of TACACS plus user login management

1.3 Features

The PCS-9882XD-H2 series managed Ethernet switches adopt high-performance switching chip and excellent industrial design to keep the line speed forwarding under full duplex and full rate operation of all the ports. The design and manufacturing of the device has fully considered various adverse conditions and interference factors in industrial applications to ensure a reliable data transmission under harsh environments.

- This device is suitable for IEC 61850 application and digital substation.
- The patented heat dissipation structure design based on the integrated mode of chip and chassis is adopted to ensure that the device has good heat dissipation performance and can work stably and reliably within the range of -40°C to +85°C
- Anti-EMC interference technologies such as fully enclosed chassis, partition grounding, power supply interference suppression, circuit board partition according to voltage grade, signal wire shielding, etc. are adopted to realize zero packet loss under the condition of strong EMC interference
- The data store & forward delay is smaller than 2μs to realize an excellent performance.
- Support of IEC 61850 modeling
- Support of switch monitoring through MMS protocol
- The processing capacity guarantees a handling of any report message (64~1518 bytes) without any loss of package.
- Support of VLAN, traffic prioritization, RSTP, MSTP, port security, GMRP/GVRP and IGMP snooping
- The port security strategy, which is based on static MAC address and IEEE 802.1X, guarantees the access security of connected IEDs.



- To ensure the security access control, SSL/SSH is supported.
- Support of static multicast management, making the flow control more transparent and reliable.
- The device is designed as an industrial managed Ethernet switch with abundant functions (e.g.: port flow control, network storm limitation, port mirroring, SNMP, RMON, WEB, port trunking, STP, etc.).
- Several gigabit interfaces are provided to improve the cascading performance.



2 Technical Data

Table of Contents

2 Technical Data	2-a
2.1 Electrical Specifications	2-1
2.1.1 AC Power Supply	2-1
2.1.2 DC Power Supply	2-1
2.2 Mechanical Specifications	2-1
2.3 Ambient Temperature and Humidity	2-1
2.4 Communication Ports	2-2
2.4.1 Standards	2-2
2.4.2 Fast Ethernet Port (Copper).....	2-2
2.4.3 Megabit SFP Socket (Optic).....	2-2
2.4.4 Gigabit Ethernet Port (Copper)	2-2
2.4.5 Gigabit SFP Socket (Optic).....	2-2
2.5 Type Tests	2-3
2.5.1 Environmental Tests	2-3
2.5.2 Mechanical Tests	2-3
2.5.3 Electrical Tests.....	2-3
2.5.4 Electromagnetic Compatibility.....	2-3
2.6 Certifications.....	2-4



2.1 Electrical Specifications

2.1.1 AC Power Supply

Standard	IEC 61000-4-11:2004
Rated voltage	110Vac/220Vac
Operating range	80%~120% Un
Max. burden (no load)	PCS-9882AD-H2: 10W PCS-9882BD-H2: 9W
Max. burden (full load)	PCS-9882AD-H2: 16W PCS-9882BD-H2: 24W

2.1.2 DC Power Supply

Standard	IEC 61000-4-29:2000	
Rated voltage	110Vdc/220Vdc	18Vdc~7Vdc
Operating range	80%~120% Un	
Permissible AC ripple voltage	Max. 15% Un	
Max. burden (no load)	PCS-9882AD-H2: 9.5W PCS-9882BD-H2: 9W	PCS-9882AD-LO-H2: 9.5W PCS-9882BD-LO-H2: 9W
Max. burden (full load)	PCS-9882AD-H2: < 16W PCS-9882BD-H2: < 24W	PCS-9882AD-LO-H2: < 16W PCS-9882BD-LO-H2: < 24W

2.2 Mechanical Specifications

Mounting Way	Flush mounted
Chassis color	Silver grey
Weight per device	Approx. 3.5kg
Chassis material	Aluminum alloy
Location of terminal	Rear panel of the device
Device structure	Plug-in modular type @ rear side, integrated frontplate
Protection class	
Standard	IEC 60225-1:2009
Front side	IP40
Other sides	IP50
Rear side, connection terminals	IP30

2.3 Ambient Temperature and Humidity

Standard	IEC 60255-1:2009;
Operating temperature	-40°C ~ +85°C
Transport and storage temperature	-40°C ~ +85°C

range	
Permissible humidity	5%-95%, without condensation

2.4 Communication Ports

2.4.1 Standards

Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE802.3z, IEEE802.3x
-----------	---

2.4.2 Fast Ethernet Port (Copper)

Connector type	RJ-45
Transmission rate	10/100Mbps
Transmission standard	10Base-T/100Base-TX
Transmission distance	Max. 100m
Safety level	Isolation to ELV level

2.4.3 Megabit SFP Socket (Optic)

Connector type	LC	
Transmission rate	100Mbps	
Transmission standard	100Base-FX	
Fiber type	Multi mode	Single mode
Transmission distance	Max. 2km	Max. 40km
Wave length	50/125μm or 62.5/125μm	9/125μm

2.4.4 Gigabit Ethernet Port (Copper)

Connector type	RJ-45
Transmission rate	10/100/1000Mbps
Transmission standard	10Base-T/100Base-TX/1000Base-T
Transmission distance	Max. 100m
Safety level	Isolation to ELV level

2.4.5 Gigabit SFP Socket (Optic)

Connector type	LC	
Transmission rate	1000Mbps	
Transmission standard	1000Base-SX	
Fiber type	Multi mode	Single mode
Transmission distance	Max. 500m	Max. 10km
Wave length	50/125μm or 62.5/125μm	9/125μm

2.5 Type Tests

2.5.1 Environmental Tests

Dry cold test	IEC 60068-2-1:2007
Dry heat test	IEC 60068-2-2:2007
Damp heat test, cyclic	IEC 60068-2-30:2005

2.5.2 Mechanical Tests

Vibration	IEC 60255-21-1:1988 Class 1
Shock and bump	IEC 60255-21-2:1988 Class 1

2.5.3 Electrical Tests

Standard	IEC 60255-27:2013
Dielectric tests	Test voltage 2kV, 50Hz, 1min
Impulse voltage tests	Test voltage 5kV
Overvoltage category	Class 3
Insulation resistance measurements	Min. 100MΩ@500VDC

2.5.4 Electromagnetic Compatibility

1MHz burst disturbance test	IEC 60255-26:2013
	Common mode: class III 2.5kV
	Differential mode: class III 1.0kV
Electrostatic discharge test	IEC 60255-26:2013 class IV
	For contact discharge: 8kV
	For air discharge: 15kV
Radio frequency interference tests	IEC 60255-26:2013 class III
	Frequency sweep
	Radiated amplitude-modulated 10V/m (rms), f=80~1000MHz
	Spot frequency Radiated amplitude-modulated 10V/m (rms), f=80MHz/160MHz/450MHz/900MHz Radiated pulse-modulated 10V/m (rms), f=900MHz
Fast transient disturbance tests	IEC 60255-26:2013
	Power supply, I/O, Earth: class IV, 4kV, 2.5kHz, 5/50ns
	Communication terminals: class IV, 2kV, 5kHz, 5/50ns
Surge immunity test	IEC 60255-26:2013
	Power supply, AC input, I/O port: class IV, 1.2/50us
	Common mode: 4kV
	Differential mode: 2kV
Conducted RF Electromagnetic	IEC 60255-26:2013

Disturbance	Power supply, AC, I/O, Comm. Terminal: Class III, 10Vrms, 150 kHz~80MHz
Power Frequency Magnetic Field Immunity	IEC 61000-4-8:2001
	Class 5, 100A/m for 1min, 1000A/m for 3s
Pulse Magnetic Field Immunity	IEC 61000-4-9:2001
	Class 5, 6.4/16μs, 1000A/m for 3s
Damped oscillatory magnetic field immunity	IEC 61000-4-10:2001
	Class 5, 100kHz & 1MHz–100A/m
AC power supply performance - Voltage dips - Voltage short interruptions	IEC 60255-26:2013 Max. 12 cycles for dips to 40%Un without reset Max. 30 cycles for dips to 70%Un without reset Max. 300 cycles for dips to 80%Un without reset Max. 400ms (Un=220Vac) or 40ms (Un=110Vac) for interruption without reboot
DC power supply performance - Voltage dips - Voltage short interruptions	IEC 60255-26:2013 Max. 100ms for dips to 40%Un without reset Max. 100ms for interruption without reboot

2.6 Certifications

- ISO9001:2008
- ISO14001:2004
- OHSAS18001:2007
- ISO10012:2003
- CMMI L5
- EMC: 2014/30/EU, EN60255-26:2013
- LVD: 2014/35/EU, EN60255-27:2014
- KEMA Report of Performance
- KEMA Report of Functional IEC61850 tests

3 Hardware

Table of Contents

3 Hardware.....	3-a
3.1 Overview.....	3-1
3.2 LED Indicators	3-2
3.2.1 Front Panel LED Indicators	3-2
3.2.2 Rear Panel LED Indicators.....	3-3
3.3 Power Supply Module	3-4
3.3.1 Screw Terminal.....	3-4
3.3.2 Phoenix Terminal	3-5
3.4 Communication Interfaces.....	3-6
3.4.1 PCS-9882AD-H2	3-6
3.4.2 PCS-9882BD-H2	3-6
3.5 SFP Sockets.....	3-7
3.6 Debugging Port.....	3-7

List of Figures

Figure 3.1-1 PCS-9882AD-H2	3-1
Figure 3.1-2 PCS-9882AD-LO-H2	3-1
Figure 3.1-3 PCS-9882BD-H2	3-1
Figure 3.1-4 PCS-9882BD-LO-H2	3-1
Figure 3.2-1 LED P1 & P2.....	3-2
Figure 3.2-2 LED RUN	3-2
Figure 3.2-3 LED ALM	3-2
Figure 3.2-4 LED 10/100M & LNK/ACT	3-3
Figure 3.2-5 LED 1G & LNK/ACT.....	3-3

Figure 3.2-6 LED indicator of fast copper port	3-4
Figure 3.2-7 LED indicator of SFP socket.....	3-4
Figure 3.3-1 10-terminal screw connector of power supply module	3-5
Figure 3.3-2 5-terminal phoenix connector for input of power supply module.....	3-5
Figure 3.3-3 3-terminal phoenix connector for output of power supply module	3-6
Figure 3.5-1 SFP sockets	3-7
Figure 3.6-1 Debugging port & cable	3-7

List of Tables

Table 3.2-1 LED indicators layout.....	3-2
Table 3.2-2 Functional description of LED 10/100M & LNK/ACT	3-3
Table 3.2-3 Functional description of LED 1G & LNK/ACT	3-3
Table 3.3-1 Terminal definition of the 10-terminal screw connector.....	3-5
Table 3.3-2 Terminal definition of the 5-terminal phoenix connector for input	3-6
Table 3.3-3 Terminal definition of the 3-terminal phoenix connector for output.....	3-6
Table 3.6-1 Wire definition of 8-core cable for debugging.....	3-8
Table 3.6-2 HyperTerminal parameter setup for debugging	3-8

3.1 Overview

The PCS-9882XD-H2 series Ethernet switches adopt rear connection mode. The power supply and communication ports are all placed in rear panel. Meanwhile, on both front and rear panel, port status indicators are provided.

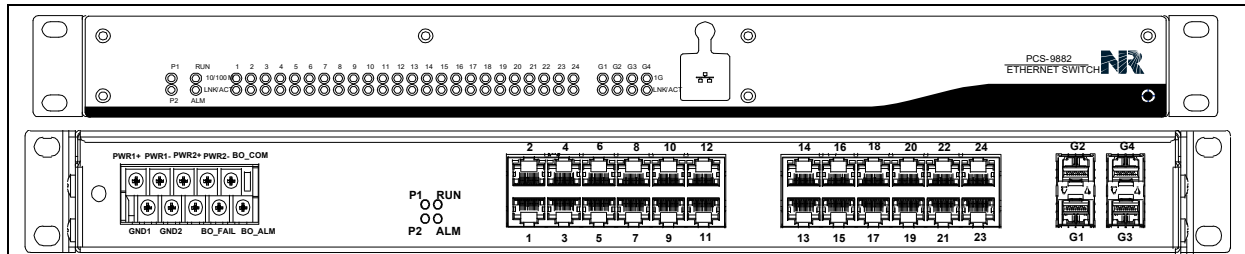


Figure 3.1-1 PCS-9882AD-H2

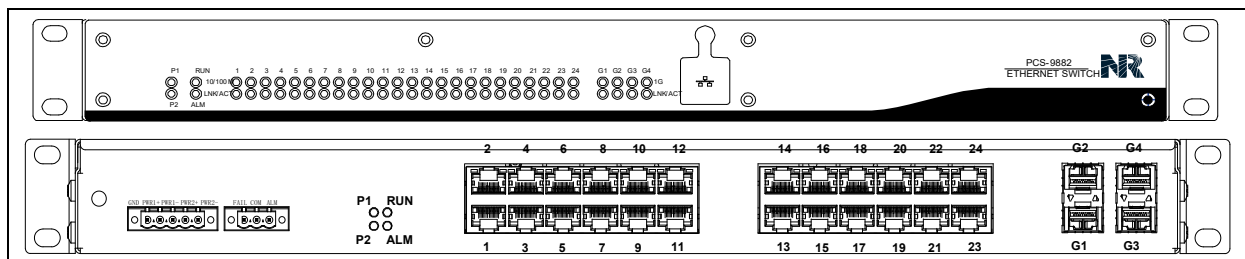


Figure 3.1-2 PCS-9882AD-LO-H2

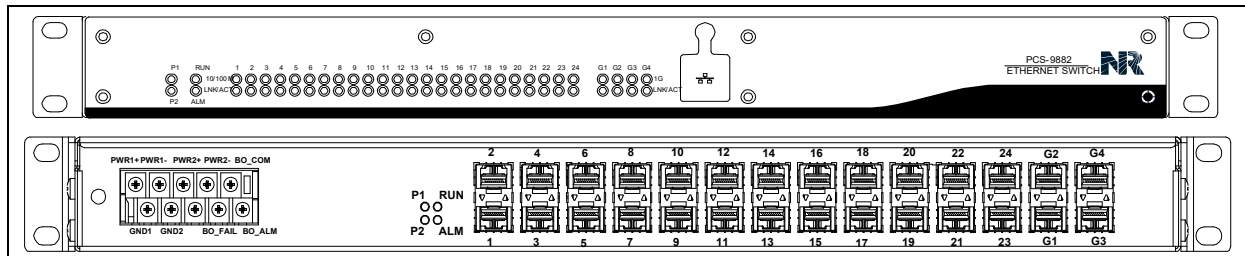


Figure 3.1-3 PCS-9882BD-H2

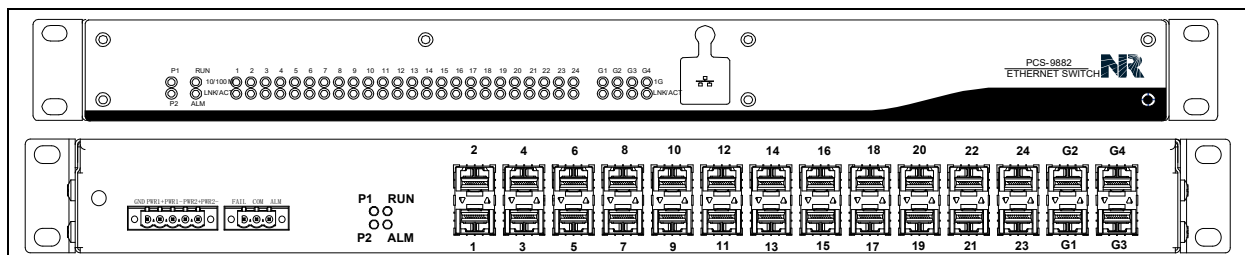


Figure 3.1-4 PCS-9882BD-LO-H2

3.2 LED Indicators

Table 3.2-1 LED indicators layout

Model	Basic LEDs				Front panel LEDs		Rear panel LEDs
	P1	P2	RUN	ALM	Megabit interface	Gigabit interface	
PCS-9882AD-H2	Front 1	Front 1	Front 1	Front 1	24×2	4×2	32
PCS-9882BD-H2	Rear 1	Rear 1	Rear 1	Rear 1	24×2	4×2	32

3.2.1 Front Panel LED Indicators

3.2.1.1 P1 & P2

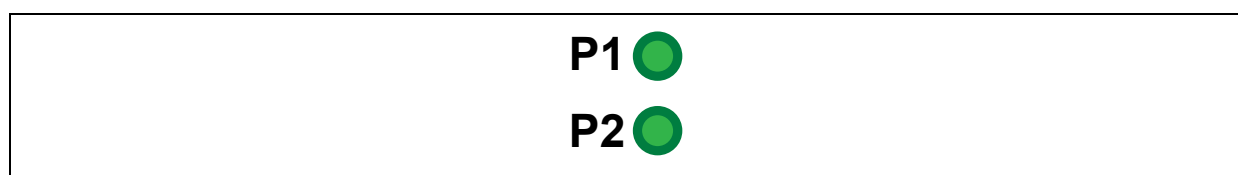


Figure 3.2-1 LED P1 & P2

The LED “P1” and “P2” indicate the power supply module 1 and 2. If the power supply module works normally, the corresponding LED will be lit on as green. In case of power loss or module fault, this LED will be lit off.

3.2.1.2 RUN



Figure 3.2-2 LED RUN

The LED “RUN” indicates the device running state. If the switch works normally, this LED will be lit on as green. If any fault occurs, this LED will be lit off.

3.2.1.3 ALM



Figure 3.2-3 LED ALM

The LED “ALM” indicates the device alarm state. If any fault occurs, this LED indicator will be lit on as orange. If all alarm signals have disappeared, it will be lit off.

3.2.1.4 10/100M & LNK/ACT

These 2 LEDs are equipped for each megabit copper Ethernet interface or SFP socket. They

indicate the communication state and the transmission rate.

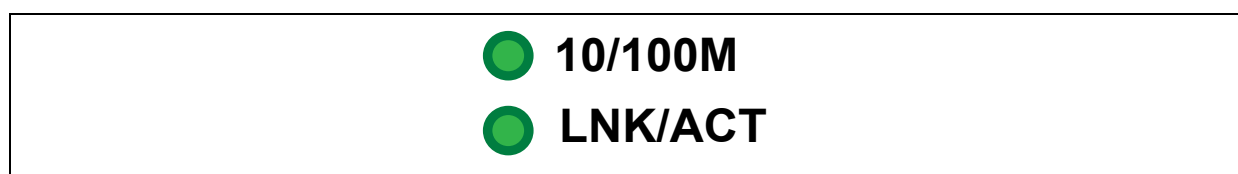


Figure 3.2-4 LED 10/100M & LNK/ACT

Table 3.2-2 Functional description of LED 10/100M & LNK/ACT

LED	Display		Description
	State	Color	
10/100M	ON	Green	The transmission rate via this interface is 100Mbps.
	OFF	/	The transmission rate via this interface is lower than 100Mbps.
LNK/ACT	ON	Green	The physical connection is established, while there is no data transmission.
	FLASH	Green	Data transmission is running.
	OFF	/	The physical connection is disconnected.

3.2.1.5 LED 1G & LNK/ACT

These 2 LEDs are equipped for each gigabit copper Ethernet interface or SFP socket. They indicate the communication state and the transmission rate.



Figure 3.2-5 LED 1G & LNK/ACT

Table 3.2-3 Functional description of LED 1G & LNK/ACT

LED	Display		Description
	State	Color	
1G	ON	Green	The transmission rate via this interface is 1000Mbps.
	OFF	/	The transmission rate via this interface is lower than 1000Mbps.
LNK/ACT	ON	Green	The physical connection is established, while there is no data transmission.
	FLASH	Green	Data transmission is running.
	OFF	/	The physical connection is disconnected.

3.2.2 Rear Panel LED Indicators

There is a group of LED indicators on the rear panel. These LED indicators are applied to indicate link state of each interface. The description of these LED indicators is the same with that of "LNK/ACT" on the front panel.

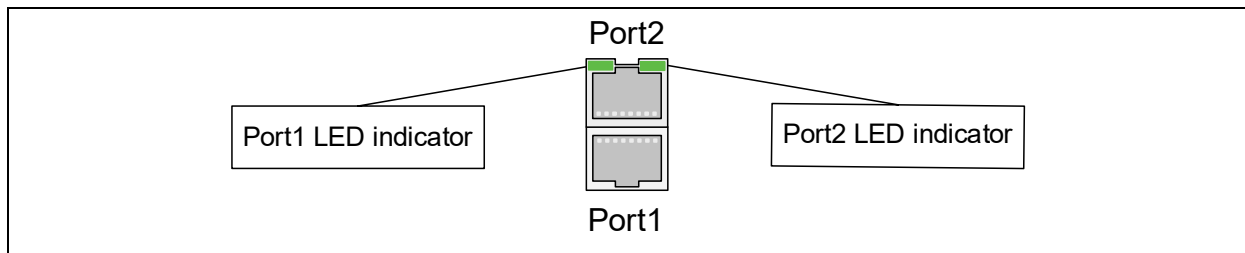


Figure 3.2-6 LED indicator of fast copper port

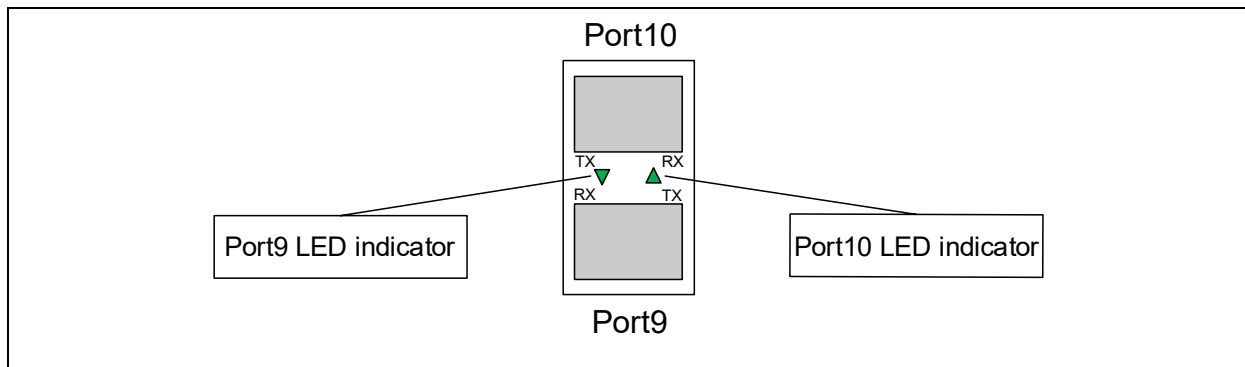


Figure 3.2-7 LED indicator of SFP socket

3.3 Power Supply Module

NOTICE!

Effective grounding is the most important measure for a device to prevent EMI, so effective grounding must be ensured before the device is put into service.

The power supply module provides the terminals 6 & 7 for grounding. The terminals shall be connected to the earthing copper bar of cabinet via dedicated grounding wire.

NOTICE!

This device, like almost all electronic equipments, contains electrolytic capacitors. These capacitors are well known to be subject to deterioration over time if voltage is not applied periodically. Deterioration can be avoided by powering the device up at least once a year.

3.3.1 Screw Terminal

For the PCS-9882XD-H2 series managed Ethernet switches, a 10-terminal screw connector of power supply module is fixed on the rear panel.

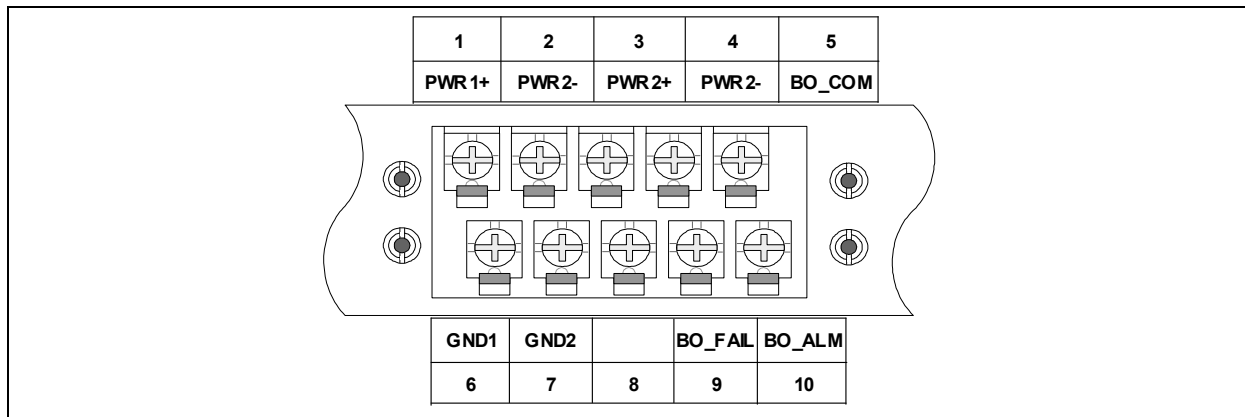


Figure 3.3-1 10-terminal screw connector of power supply module

Table 3.3-1 Terminal definition of the 10-terminal screw connector

No.	Symbol	Description
1	PWR1+	The positive pole (DC) or live pole (AC) of the power supply module 1
2	PWR1-	The negative pole (DC) or neutral pole (AC) of the power supply module 1
3	PWR2+	The positive pole (DC) or live pole (AC) of the power supply module 2 It is valid only if dual power supplies are equipped.
4	PWR2-	The negative pole (DC) or neutral pole (AC) of the power supply module 2 It is valid only if dual power supplies are equipped.
5	BO_COM	The common terminal of "BO_FAIL" and "BO_ALM".
6	GND1	The grounding connection of the power supply module 1.
7	GND2	The grounding connection of the power supply module 2.
8		Empty
9	BO_FAIL	The normally closed output contact, which indicates the device blocking state. If the device is blocked due to failure, this contact will be closed, otherwise, it is open.
10	BO_ALM	The normally opened output contact, which indicates the device abnormal state. If the there is an alarm due to abnormality, this contact will be closed, otherwise, it is open.

3.3.2 Phoenix Terminal

For the PCS-9882XD-LO-H2 series managed Ethernet switches, a 5-terminal phoenix connector for input and a 3-terminal phoenix connector for output of power supply module are fixed on the rear panel.

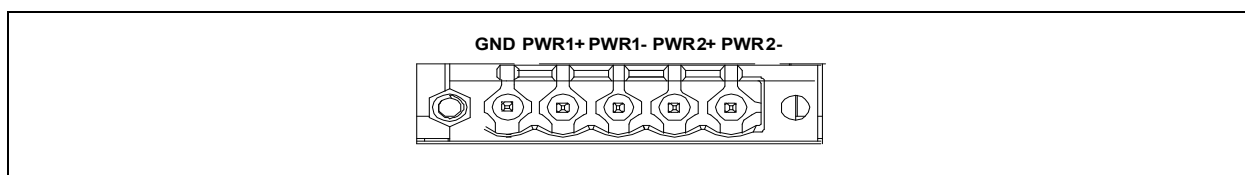


Figure 3.3-2 5-terminal phoenix connector for input of power supply module

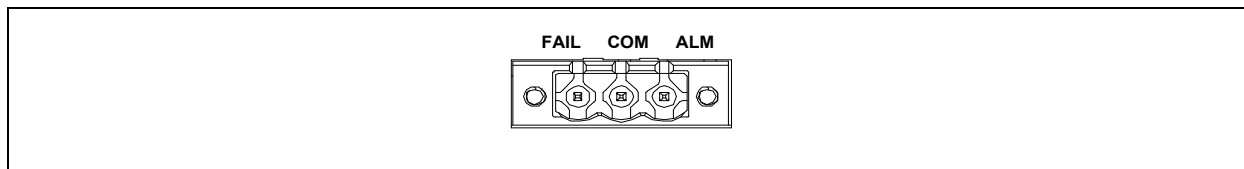


Figure 3.3-3 3-terminal phoenix connector for output of power supply module

Table 3.3-2 Terminal definition of the 5-terminal phoenix connector for input

No.	Symbol	Description
1	GND	The grounding connection of the power supply module
2	PWR1+	The positive pole (DC) of the power supply module 1
3	PWR1-	The negative pole (DC) of the power supply module 1
4	PWR2+	The positive pole (DC) of the power supply module 2 It is valid only if dual power supplies are equipped.
5	PWR2-	The negative pole (DC) of the power supply module 2 It is valid only if dual power supplies are equipped.

Table 3.3-3 Terminal definition of the 3-terminal phoenix connector for output

No.	Symbol	Description
1	FAIL	The normally closed output contact, which indicates the device blocking state. If the device is blocked due to failure, this contact will be closed, otherwise, it is open.
2	COM	The common terminal of "FAIL" and "ALM".
3	ALM	The normally opened output contact, which indicates the device abnormal state. If the there is an alarm due to abnormality, this contact will be closed, otherwise, it is open.

3.4 Communication Interfaces

3.4.1 PCS-9882AD-H2

The No.01~24 interfaces are RJ45 ports for 10/100Mbps data transmission.

The G1~G4 interfaces are 100/1000Mbps SFP sockets for optic transceivers conforming to 100BASE-FX standard in 100Mbps full or half duplex mode. Also, they could be used for optic transceivers conforming to 1000BASE-SX standard in 1000Mbps full or half duplex mode. Furthermore, they could be used for electrical transceivers conforming to 1000BASE-T standard in 1000Mbps full duplex mode.

3.4.2 PCS-9882BD-H2

The No.01~24 interfaces are megabit SFP sockets for optic transceivers conforming to 100BASE-FX standard in 100Mbps full or half duplex mode. Also, they could be used for electrical transceivers (RJ45) conforming to 100BASE-TX standard (requires interface configuration through WEB management).

The G1~G4 interfaces are 1000Mbps SFP sockets for optic transceivers conforming to

1000BASE-SX standard in auto-negotiation, 1000Mbps full or half duplex mode. Furthermore, they could be used for electrical transceivers conforming to 1000BASE-T standard in 1000Mbps full duplex mode.

3.5 SFP Sockets

The PCS-9882XD-H2 series managed Ethernet switches adopt SFP sockets for LC-type connector of optic fibers. Facing from the rear panel, each SFP socket connects two fiber pigtails. The left one is Tx (transmit), the right one is Rx (receive).

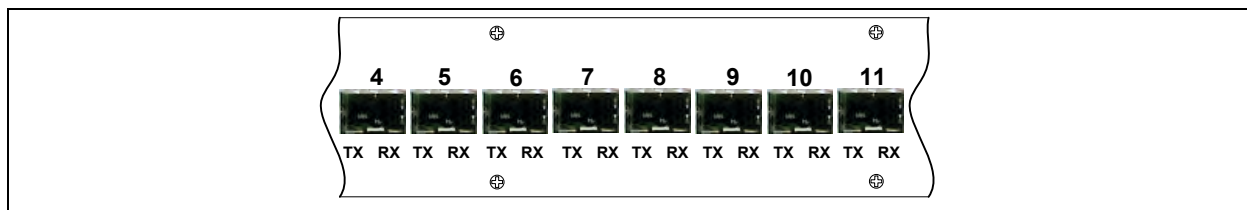


Figure 3.5-1 SFP sockets

Meanwhile, all megabit interfaces could adopt passive SFP electrical transceivers and all gigabit interfaces could adopt 1000Mbps SFP electrical transceivers. Standard Ethernet network cables, which could be cross wires or straight wires, are used for connection.

3.6 Debugging Port

In the front panel, a "**Console**" port is designed for debugging. This RJ45 port can be used as a twisted-pair Ethernet port for configuration via WEB, as well as a RS-232 serial port for the monitoring of switch boot information via HyperTerminal.

As shown in the following figure, a specific cable is applied for debugging via this multiplex RJ45 port.

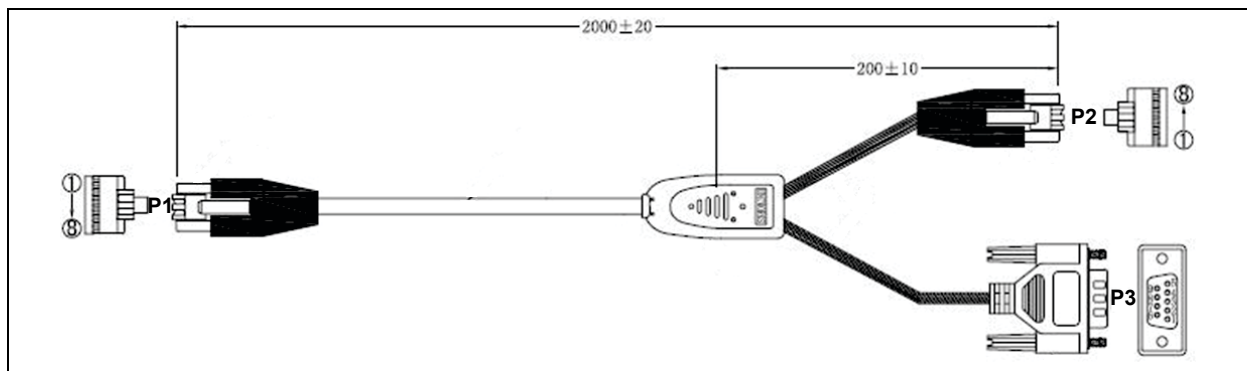


Figure 3.6-1 Debugging port & cable

P1: To connect the multiplex RJ45 port via an 8-core cable

P2: To connect the twisted-pair Ethernet port of the computer

P3: To connect the RS-232 serial port of the computer

Table 3.6-1 Wire definition of 8-core cable for debugging

No.	Core color	Function	Device side (Left)	Computer side (Right)
1	Orange & white	TX+ of the Ethernet port	P1-1	P2-1
2	Orange	TX- of the Ethernet port	P1-2	P2-2
3	Green & white	RX+ of the Ethernet port	P1-3	P2-3
4	Blue	TXD of the RS-232 serial port	P1-4	P3-2
5	Brown & white	RXD of the RS-232 serial port	P1-5	P3-3
6	Green	RX- for the Ethernet port	P1-6	P2-6
7	Blue & white	The ground connection of the RS-232 port.	P1-7	P3-5
8	Brown		P1-8	

Table 3.6-2 HyperTerminal parameter setup for debugging

Parameter	Recommended Value
Baud rate	115200bps
Data bits	8
Parity	None
Stop bit	1
Flow control	None

4 Configurable Functions

Table of Contents

4 Configurable Functions	4-a
4.1 Overview	4-1
4.2 WEB Server Setup	4-2
4.2.1 Normal Login	4-2
4.2.2 Secure Login	4-3
4.3 User Settings	4-4
4.3.1 User Management	4-4
4.4 Auditor Settings	4-4
4.4.1 Local Audit Export	4-4
4.5 Basic Settings	4-5
4.5.1 Switch Information	4-5
4.5.2 Port	4-6
4.5.3 Switch IP Settings	4-7
4.5.4 Bandwidth Management	4-8
4.5.5 MAC Limited Management	4-10
4.5.6 Config File Management	4-10
4.5.7 Factory Default	4-11
4.6 Virtual LAN	4-11
4.6.1 Introduction	4-11
4.6.2 VLAN Settings	4-12
4.6.3 PVID Settings	4-13
4.6.4 Protocol VLAN Settings	4-14
4.6.5 GVRP Management	4-15
4.7 IEC 61850 Settings	4-16
4.8 Multicast Management	4-17

4.8.1 Static Multicast Group	4-17
4.8.2 GMRP Management.....	4-18
4.8.3 IGMP Snooping	4-21
4.9 Port Security	4-22
4.9.1 Introduction of IEEE 802. 1X.....	4-22
4.9.2 Port Security State	4-23
4.9.3 Static MAC Table	4-24
4.9.4 802.1X	4-24
4.9.5 RADIUS Server	4-25
4.10 TACACS+ Settings.....	4-27
4.10.1 TACACS+ Login Method	4-28
4.10.2 TACACS+ Basic Settings	4-29
4.10.3 TACACS+ Server Settings	4-29
4.10.4 Typical Application Configuration Method	4-30
4.11 Traffic Prioritization	4-30
4.11.1 CoS Mapping	4-31
4.12 STP Management.....	4-31
4.12.1 RSTP Settings.....	4-31
4.12.2 MSTP Settings	4-34
4.13 Time Management	4-37
4.13.1 Time Settings.....	4-37
4.13.2 SNTP Settings.....	4-37
4.14 Port Trunking	4-39
4.14.1 Trunking.....	4-39
4.15 SNMP Management	4-40
4.15.1 SNMP Settings	4-42
4.15.2 Trap Settings	4-43
4.16 RMON Management.....	4-44
4.16.1 RMON History Control	4-44
4.16.2 RMON Alarm	4-45

4.16.3 RMON Event	4-48
4.17 Diagnosis	4-48
4.17.1 Mirror Settings	4-49
4.17.2 Alarm Settings	4-49
4.17.3 IP Check Settings	4-50
4.17.4 LLDP Settings	4-50
4.17.5 Security Settings	4-53
4.17.6 Statistic Settings	4-53
4.18 Others	4-54
4.18.1 Restart	4-54

List of Figures

Figure 4.2-1 WEB server normal login	4-2
Figure 4.2-2 WEB server welcome page	4-3
Figure 4.2-3 WEB server security login	4-3
Figure 4.3-1 User Management	4-4
Figure 4.4-1 Local audit export	4-5
Figure 4.5-1 Switch Information	4-5
Figure 4.5-2 Port Settings	4-6
Figure 4.5-3 MAC Settings	4-7
Figure 4.5-4 Switch IP Settings	4-7
Figure 4.5-5 Rate Limiting	4-8
Figure 4.5-6 Port Rate Limiting	4-8
Figure 4.5-7 FP Rate Limiting	4-9
Figure 4.5-8 Port MAC limit	4-10
Figure 4.5-9 Config File Management	4-10
Figure 4.5-10 Factory Default	4-11
Figure 4.6-1 VLAN Settings	4-12

Figure 4.6-2 PVID Settings.....	4-13
Figure 4.6-3 Protocol VLAN Settings	4-14
Figure 4.6-4 GVRP	4-15
Figure 4.6-5 View VLAN Summary.....	4-16
Figure 4.7-1 IEC 61850 Settings.....	4-16
Figure 4.8-1 Static Multicast Group.....	4-17
Figure 4.8-2 GMRP	4-19
Figure 4.8-3 View Multicast Group Summary.....	4-20
Figure 4.8-4 Save Multicast Group	4-21
Figure 4.8-5 IGMP Snooping	4-22
Figure 4.9-1 Port Security State.....	4-23
Figure 4.9-2 Static MAC Table.....	4-24
Figure 4.9-3 IEEE 802.1X Settings	4-25
Figure 4.9-4 RADIUS Server Settings.....	4-26
Figure 4.9-5 RADIUS Client Database	4-26
Figure 4.9-6 Authorize User Database	4-27
Figure 4.10-1 TACACS+ network structure.....	4-28
Figure 4.10-2 TACACS+ Login Method	4-28
Figure 4.10-3 TACACS+ Basic Settings	4-29
Figure 4.10-4 TACACS+ Server Settings.....	4-29
Figure 4.11-1 CoS Mapping	4-31
Figure 4.12-1 RSTP Settings	4-32
Figure 4.12-2 RSTP Advanced Settings	4-33
Figure 4.12-3 MSTP Settings.....	4-35
Figure 4.12-4 MSTP Advanced Settings.....	4-36
Figure 4.13-1 Time Settings.....	4-37
Figure 4.13-2 SNTP Client Settings	4-38
Figure 4.13-3 SNTP Server Settings	4-38
Figure 4.14-1 Trunking	4-39
Figure 4.15-1 SNMP Settings.....	4-42



Figure 4.15-2 SNMP Trap Settings.....	4-43
Figure 4.16-1 RMON History Control.....	4-44
Figure 4.16-2 RMON Alarm	4-45
Figure 4.16-3 RMON Event	4-48
Figure 4.17-1 Mirror Settings	4-49
Figure 4.17-2 Alarm Settings.....	4-49
Figure 4.17-3 IP Check Settings.....	4-50
Figure 4.17-4 LLDP Basic Settings.....	4-51
Figure 4.17-5 LLDP Port Settings	4-51
Figure 4.17-6 LLDP Neighbor Information.....	4-52
Figure 4.17-7 LLDP Statistic Information.....	4-53
Figure 4.17-8 Security Settings.....	4-53
Figure 4.17-9 Statistic Settings.....	4-54
Figure 4.18-1 Restart.....	4-54



4.1 Overview

The configurable functions can be realized by debugging computer via the debugging port on the front panel or an Ethernet interface on the rear panel.

The fixed IP address of the front panel RJ45 debugging port is "192.169.0.82". By default, the IP address of any Ethernet interface on the rear panel is set as "192.168.0.82".

Several different methods are provided for the connection to debugging computer.

- Command-line interface (CLI)

Use the dedicated debugging cable for the CLI connection. Connect the front panel debugging port of the switch to a RS-232 serial port of the computer.

Set the HyperTerminal (or similar software) parameters on the computer according to the following table.

Table 4.1-1 HyperTerminal parameter

Parameter	Value
Baud rate	115200bps
Data bits	8
Stop bit	1
Parity	None
Flow control	None

- WEB server

Use the dedicated debugging cable or a twisted-pair Ethernet cable (4-core megabit cable recommended) for the WEB server connection. Connect the front panel debugging port or any Ethernet interface on the rear panel to the computer. The computer and the switch Ethernet interface IP addresses should be different but share the same network segment. Make sure that the connected interface "PVID" equals to 1 and its IP address does not conflict to any other address in the network.

For these connection methods, the default user definition is the same, including administrator, operator and auditor. For user management, login using "**administrator**" + "**NRadmin123**". For configuration modification, login using "**operator**" + "**NRop123456**". For log audit, login using "**auditor**" + "**NRAud12345**".

NOTICE!

In this chapter, unless stated otherwise, the configuration through WEB server is taken as example.

During normal operating, this method is enough. The configuration through CLI aims to debug the switch under instructions of manufacturer engineer.

NOTICE!

After making changes to the switch parameters, it is recommended to reboot the switch to ensure that the switch configuration file is consistent with the switch operating parameters.

NOTICE!

For security concern, the factory default settings turn off FTP, Telnet and other network services. Please contact the manufacturer for the guide of using CLI to open these services and set related parameters.

4.2 WEB Server Setup

In this chapter, detailed methods and operation steps of WEB server are introduced. After logging in to the WEB configuration interface, the current user will automatically quit if there is no operation for a period of time. For certain critical operations, password verification is necessary. Please pay attention to browser pop-up window.

4.2.1 Normal Login

Launch a browser (IE is recommended) on the computer and input the IP address "192.169.0.82" to access the WEB Server login interface.

Model: L2 Switch		IP: 192.168.0.82		MAC Address: b4-4c-c2-fd-a0-d8		POWER: P1 ALM, P2 Invalid		ALARM: Normal	
Name: PCS-9882B		Location: communication room		Software Version: R6.00		Firmware Version: 6.3.9		Manufacturer: NR Electric Co., Ltd.	

Account :
 Password :

Figure 4.2-1 WEB server normal login

Input the default account and password to login and display the WEB server welcome page.

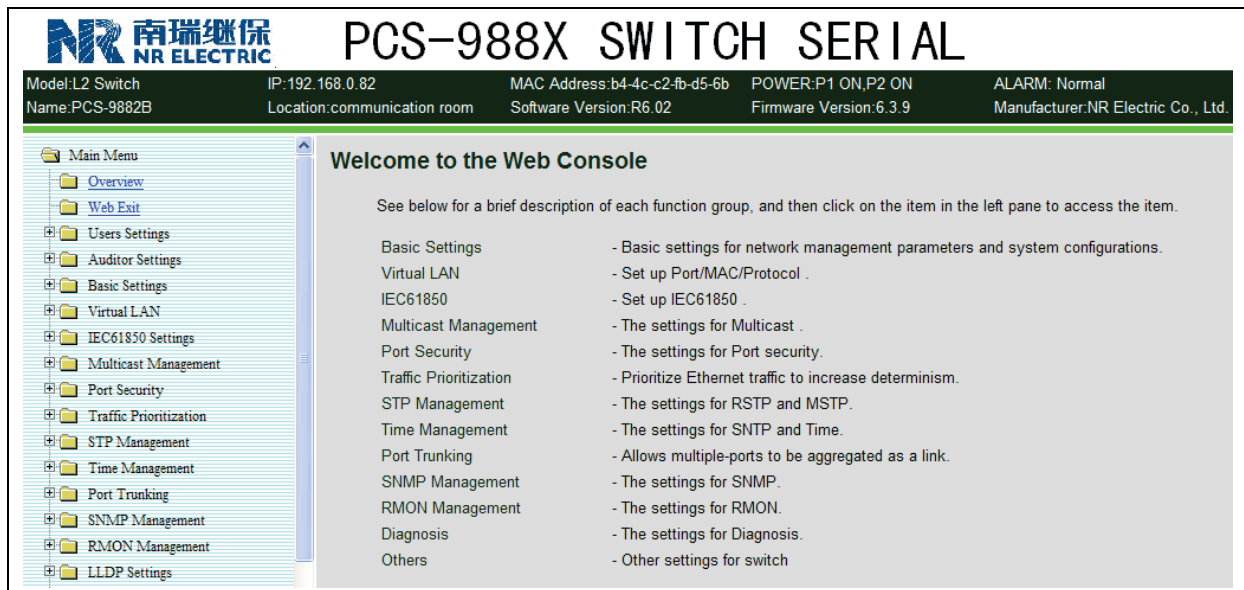


Figure 4.2-2 WEB server welcome page

4.2.2 Secure Login

The PCS-9882XD-H2 series managed Ethernet switches support Security Socket Layer (SSL) for encrypted secure login of WEB server.

Launch a browser (IE is recommended) on the computer and input the IP address "https://192.169.0.82" to access the WEB Server login interface. Normally, a security alert will be pop-up. Please select "Yes". All network messages will be encrypted to enhance the security.

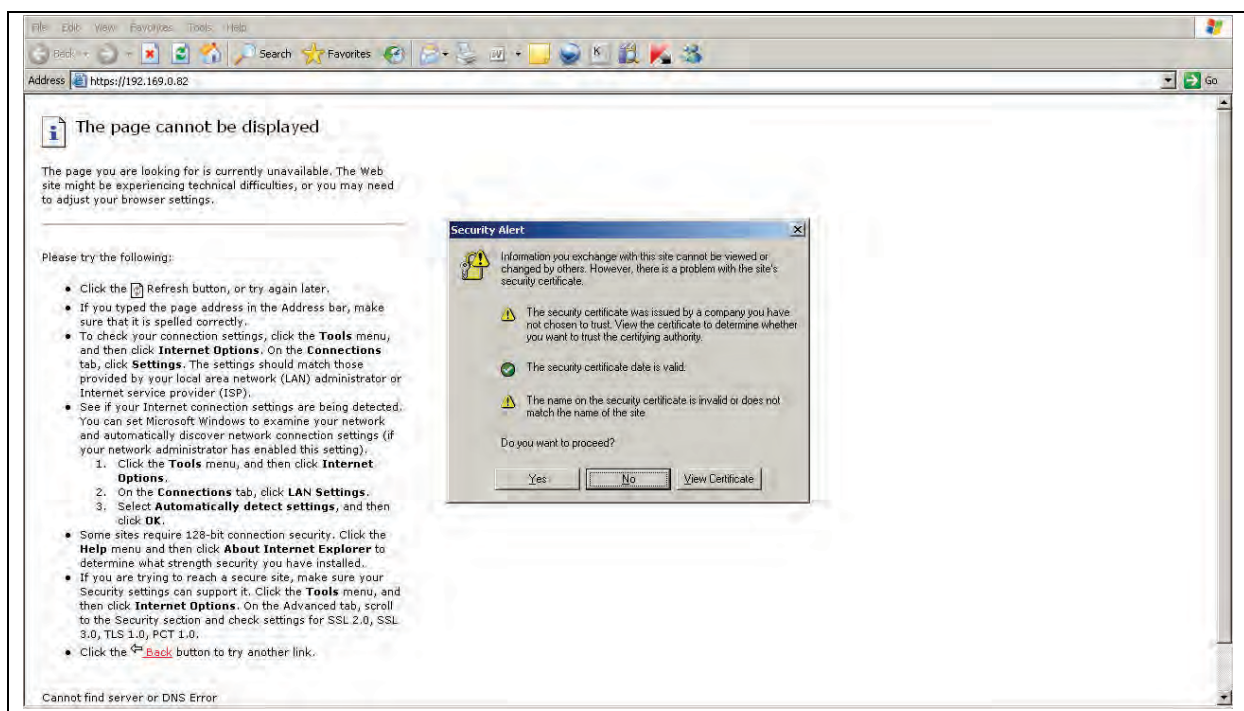


Figure 4.2-3 WEB server security login

4.3 User Settings

4.3.1 User Management

Use this menu to set user, authority and password parameters for WEB server login. As shown in the following figure, by default, there is an administrator user who has the highest administrative authority and could manage users and browse switch parameters. The administrator is undeletable. By default, there is an operator user who has the authority to set parameters and an auditor user who has read-only authority to browse parameters and read logs. The auditor user is undeletable.

An user name should consist of letters and numbers for the length of at least 4 characters. A password should consist of upper- and lower-case letters and numbers for the length of at least 4 but less than or equal to 16 characters.

User Administration Settings

Add User

User Name:

User Role:

User Authority:

Old Password:

New Password: (8-16 characters, must including numbers and letters)

Confirm New Password:

User Table

Select	Index	User Name	Authority	Role
☐	1	administrator	ADMIN USER	SYS USER
☐	2	operator	READ WRITE	OP USER
☐	3	auditor	READ ONLY	AUD USER

Figure 4.3-1 User Management

4.4 Auditor Settings

4.4.1 Local Audit Export

Use this menu to export switch logs for further use.

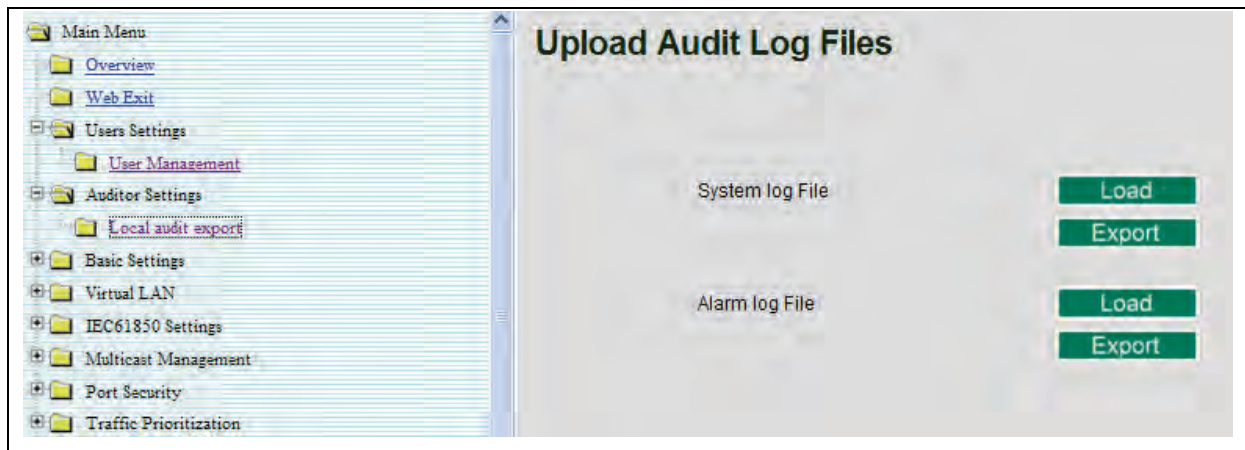


Figure 4.4-1 Local audit export

4.5 Basic Settings

4.5.1 Switch Information

Use this menu to set the system information of switch.

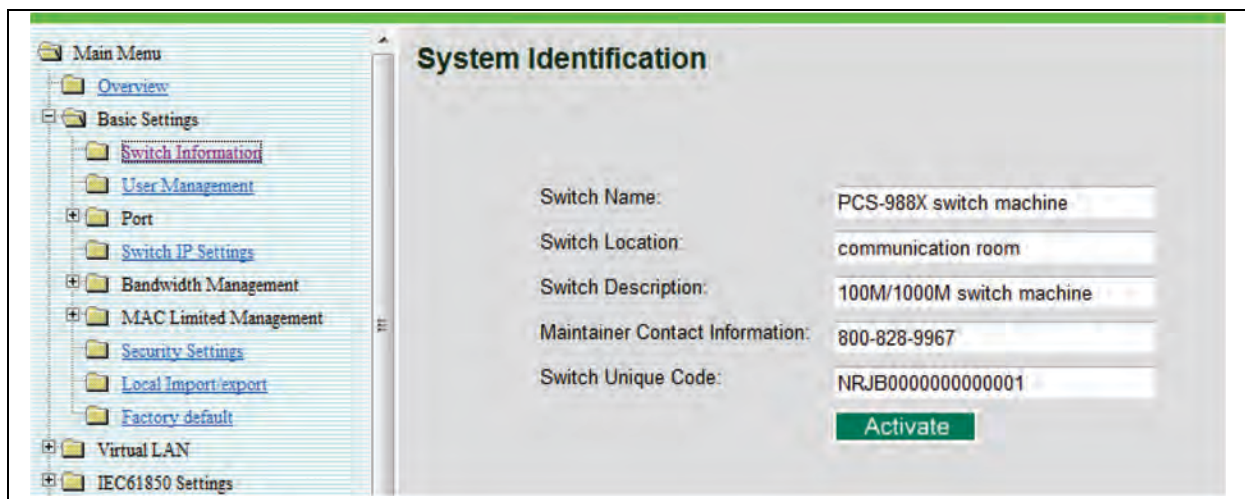


Figure 4.5-1 Switch Information

By default, the “**Maintainer Contact Information**” is the manufacture service hot line and the “**Switch Unique Code**” is the factory code of device.

4.5.2 Port

4.5.2.1 Port Settings

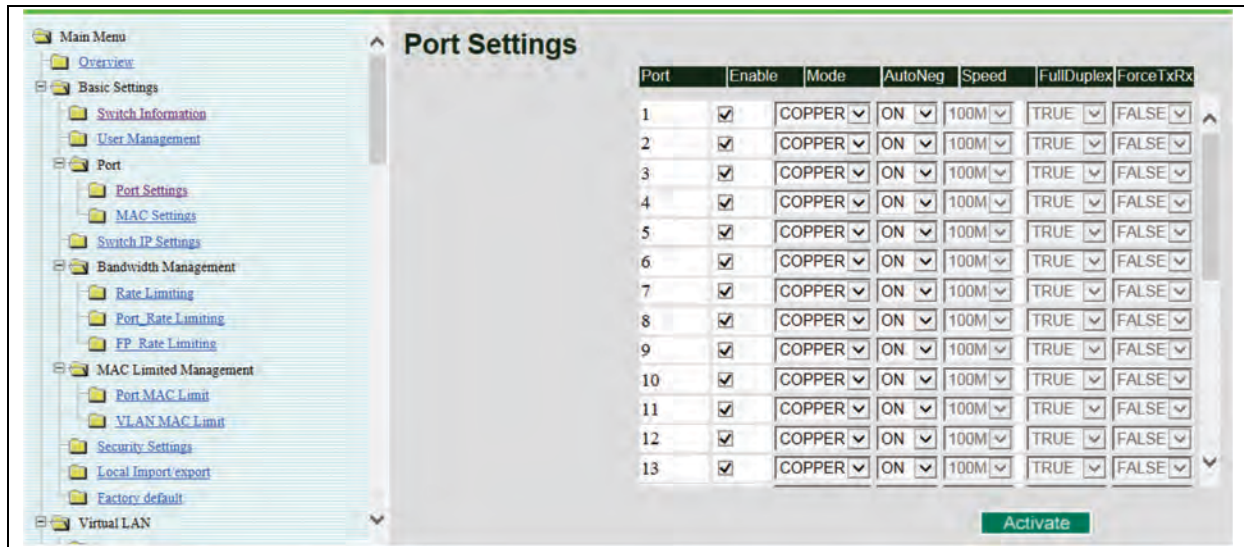


Figure 4.5-2 Port Settings

- **Enable**

Tick to enable the port

- **AutoNeg**

To enable or disable the auto-negotiation mode. An enabling auto-negotiation results in speed and duplex being negotiated upon link detection; both end devices must be auto-negotiated compliant for the best possible results. Fiber optic media does not support auto-negotiation so it must be configured to either half or full duplex.

- **Speed**

If auto-negotiation is enabled, this setting is invalid.

If auto-negotiation is disabled, the port transmission speed is forced to this setting value.

- **FullDuplex**

If auto-negotiation is enabled, this setting is invalid.

If auto-negotiation is disabled the port working mode is forced to this working mode (“**TRUE**” for full duplex and “**FALSE**” for half duplex).

NOTICE!

For the No.01~24 interfaces of PCS-9882BD-H2 series switches adopting SFP electrical transceivers, the interface corresponding “**Mode**” should be “**COPPER**” and “**AutoNeg**” should be “**ON**”.

NOTICE!

For the use of G1~G4 interfaces adopting megabit SFP optic transceivers, the

interface corresponding “**Speed**” should be “**100M**”.

4.5.2.2 MAC Settings

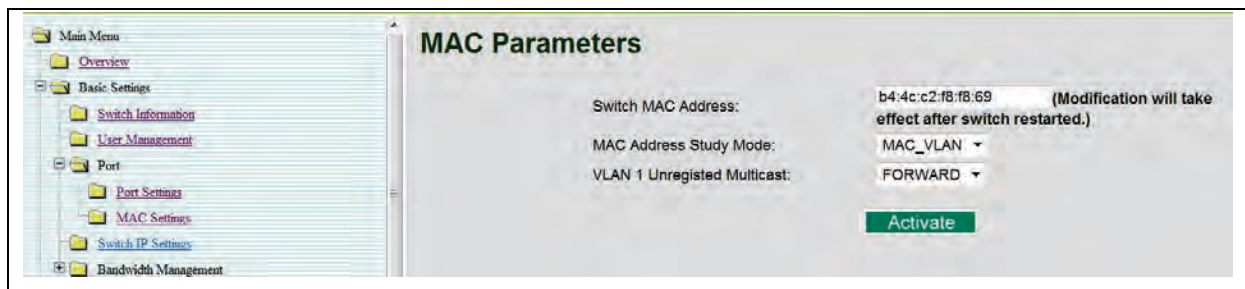


Figure 4.5-3 MAC Settings

- **Unregistered Multicast MAC Strategy**

To select the treatment strategy of the unregistered multicast address message (i.e.: the multicast address neither configured in static table nor studied by GMRP or IGMP Snooping)

FORWARD (default) Forward to all ports except the CPU port

DROP Discard

NOTICE!

The “**Activate**” pressing after a modification of one of the two parameters “**Switch MAC Address**” and “**MAC Address Study Mode**” will cause automatic reboot of switch.

4.5.3 Switch IP Settings

These parameters could be set according to site requirements.

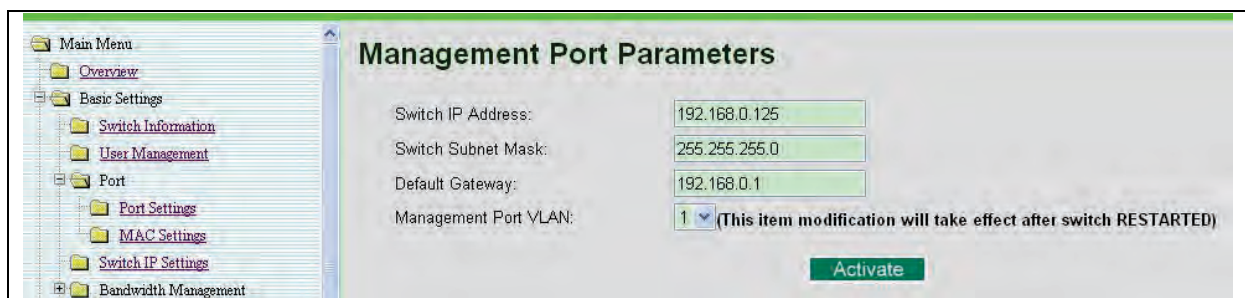


Figure 4.5-4 Switch IP Settings

NOTICE!

A modification of “**Management Port VLAN**” will be valid after a reboot of switch.

4.5.4 Bandwidth Management

4.5.4.1 Rate Limiting

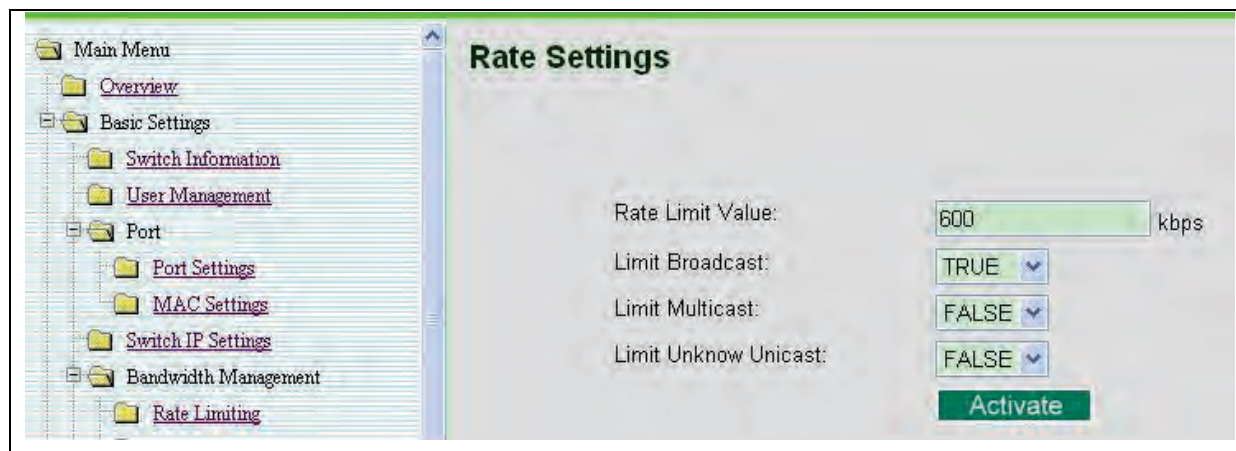


Figure 4.5-5 Rate Limiting

NOTICE!

The minimal value of “**Rate Limit Value**” should be greater than or equal to 64.

4.5.4.2 Port Rate Limiting

Use this menu to set limiting of port transmission rate and network burst rate. For the PCS-9882XD-H2 series switches, the ingress rate and egress rate of each port could be set separately.

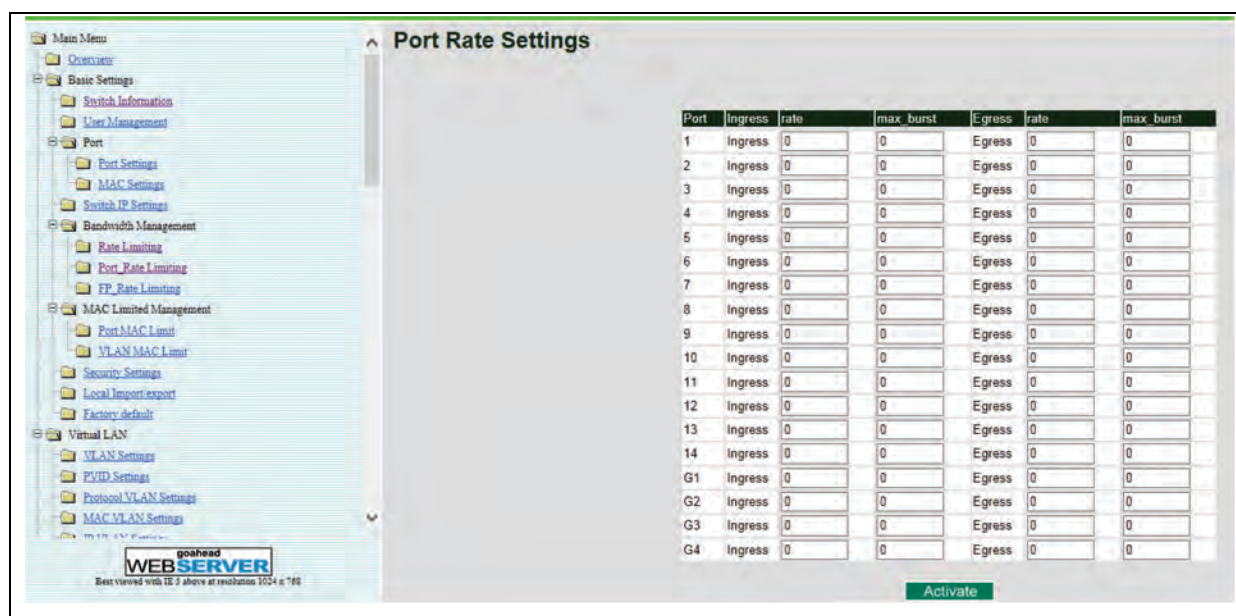


Figure 4.5-6 Port Rate Limiting

- **Ingress rate**

The default value "0" signifies no limit.

Minimal value: 64, Resolution: 32, Unit: kbps.

- **Ingress max_burst**

The default value "0" signifies no limit.

Generally, this setting value is the same to that of "**Ingress rate**". This setting should coordinate with "**Ingress rate**". Only if both these parameters values are nonzero, the rate limit will be valid. Otherwise, the port still operates at a linear rate.

- **Egress rate**

The default value "0" signifies no limit.

Minimal value: 64, Resolution: 32, Unit: kbps.

- **Egress max_burst**

The default value "0" signifies no limit.

Generally, this setting value is the same to that of "**Egress rate**". This setting should coordinate with "**Egress rate**". Only if both these parameters values are nonzero, the rate limit will be valid. Otherwise, the port still operates at a linear rate.

4.5.4.3 FP Rate Limiting

Use this menu to set rate limiting of a specific type of messages.

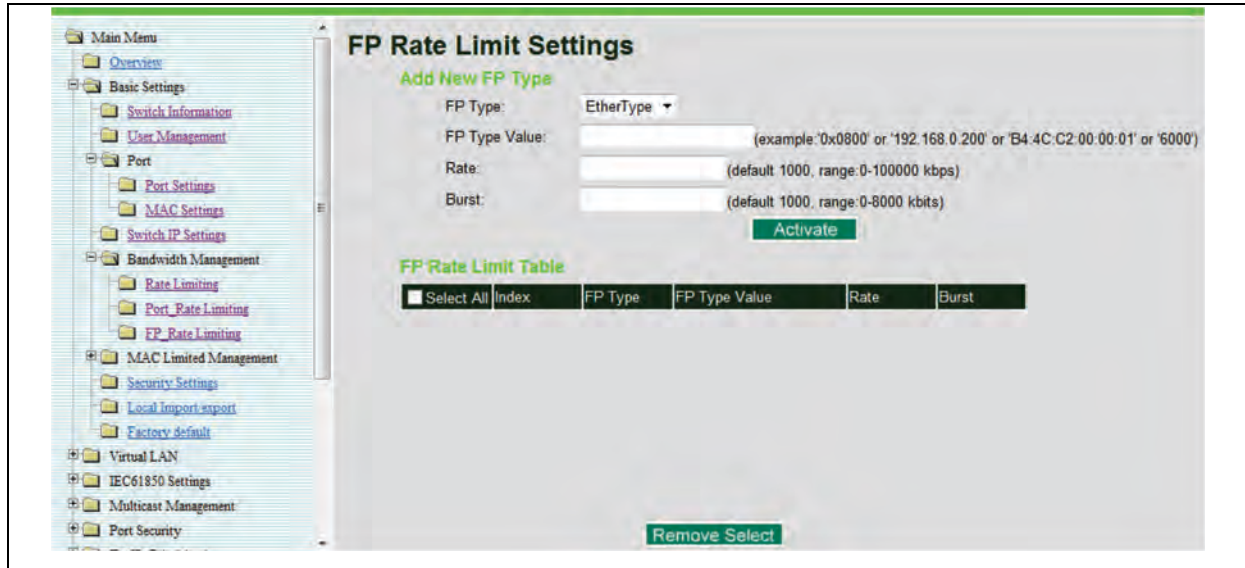


Figure 4.5-7 FP Rate Limiting

- **FPTYPE**

Specific type for rate limiting filter

EtherType Ethernet

SrcMAC Source MAC address

DstMAC

Object MAC address

4.5.5 MAC Limited Management

4.5.5.1 Port MAC Limit

Use this menu to set the maximum number of MAC addresses that each port is allowed

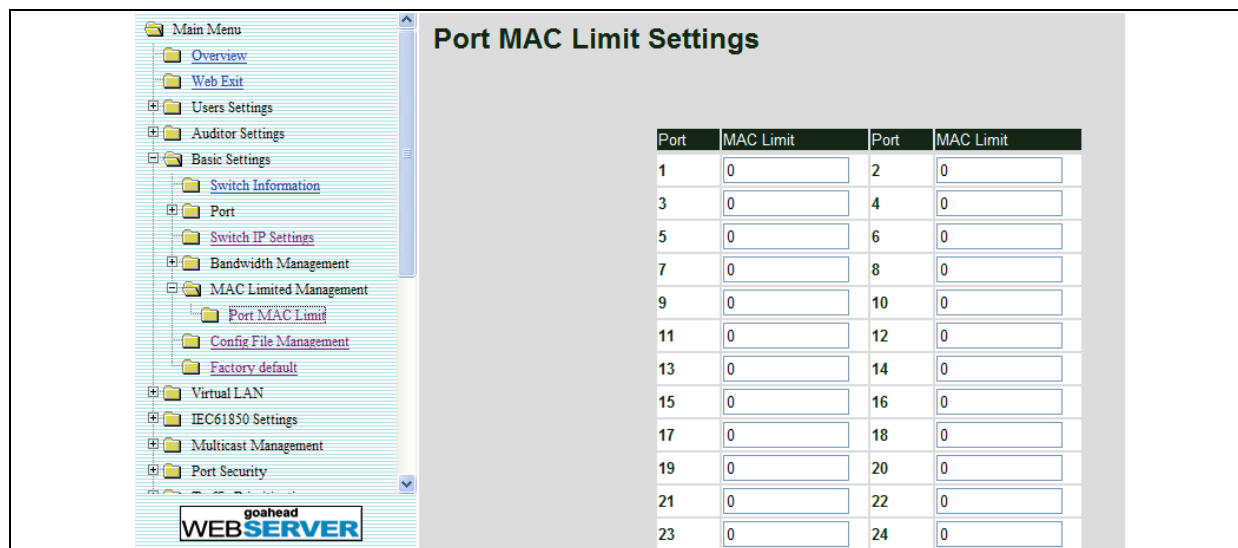


Figure 4.5-8 Port MAC limit

- **MAC Limit**

The maximum number of MAC addresses.

The default value “0” signifies no limiting.

Maximal value: 8191.

4.5.6 Config File Management

Use this menu to upload and download configuration files from and to debugging computer.

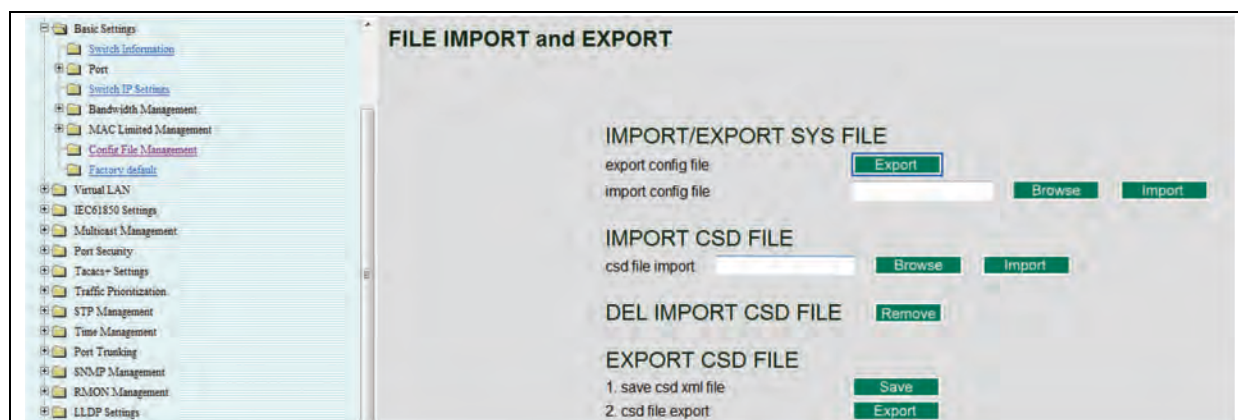


Figure 4.5-9 Config File Management

NOTICE!

The “**SYS**” file is the switch system configuration file which contains the switch parameters.

The “**CSD**” file is the multicast configuration file in xml format. Normally, the file name is “multicast_csd.xml”.

NOTICE!

In case of abnormality, it is recommended to backup/download the running parameters of switch before any modification of configuration.

NOTICE!

The “multicast_csd.xml” file may be deleted after file uploading and before switch rebooting. During such period, the imported parameters has not been parsed.

NOTICE!

Please be patient, the operations (such as xml file generation, uploading and downloading) of CSD file may take a while.

4.5.7 Factory Default

Use this menu to reset all the switch configuration and parameters to factory default values.

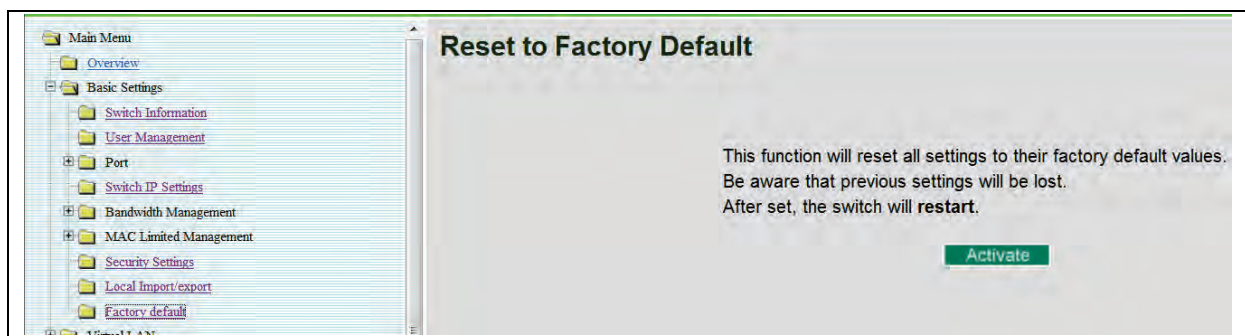


Figure 4.5-10 Factory Default

4.6 Virtual LAN

4.6.1 Introduction

Virtual Local Area Network (VLAN) is mainly used to solve the problem that switches cannot restrict broadcasting when interconnecting Local Area Networks (LAN). This technology can divide a LAN into multiple logical LANs. Each VLAN is a broadcast domain. The communication between hosts in a VLAN is the same as that in a LAN, while the inter-VLANs cannot communicate directly. Thus, broadcast messages are limited to one VLAN.

“**VLAN Settings**” are the basis of “**PVID Settings**”, “**Protocol VLAN Settings**”, and “**MAC VLAN Settings**”. The discrimination relation of different VLANs is: 802.1Q VLAN > MAC Base VLAN > Protocol Base VLAN > Port Base VLAN. The 802.1Q VLAN configuration menu is “**VLAN**”

Settings", the MAC Base VLAN configuration menu is "**MAC VLAN Settings**", the Protocol Base VLAN configuration menu is "**Protocol VLAN Settings**", and the Port Base VLAN configuration menu is "**PVID Settings**".

GARP VLAN Registration Protocol (GVRP) is an application of General Attribute Registration Protocol (GARP). It mainly provides dynamic VLAN management functions. The operation of GVRP is based on the services provided by GARP, which allows terminal stations to dynamically register VLAN with connected switches, and this information can be propagated to all switches that support GVRP.

When a host joins a VLAN, it needs to send a GVRP join message. Once the GVRP join message is received, the switch will add the port that received the message to the appropriate VLAN. The switch sends GVRP join message to all other hosts. In addition, the switch periodically sends a GVRP query. If the host wants to stay in the VLAN, it will respond to the GVRP query. In this case, the switch has no operation. If the host does not want to stay in the VLAN, it can either send a leave message or not respond to periodic GVRP queries. Once the switch receives a host leave message or does not receive a response message during the setting of "leaveAll" timer, it deletes the host from the VLAN.

4.6.2 VLAN Settings

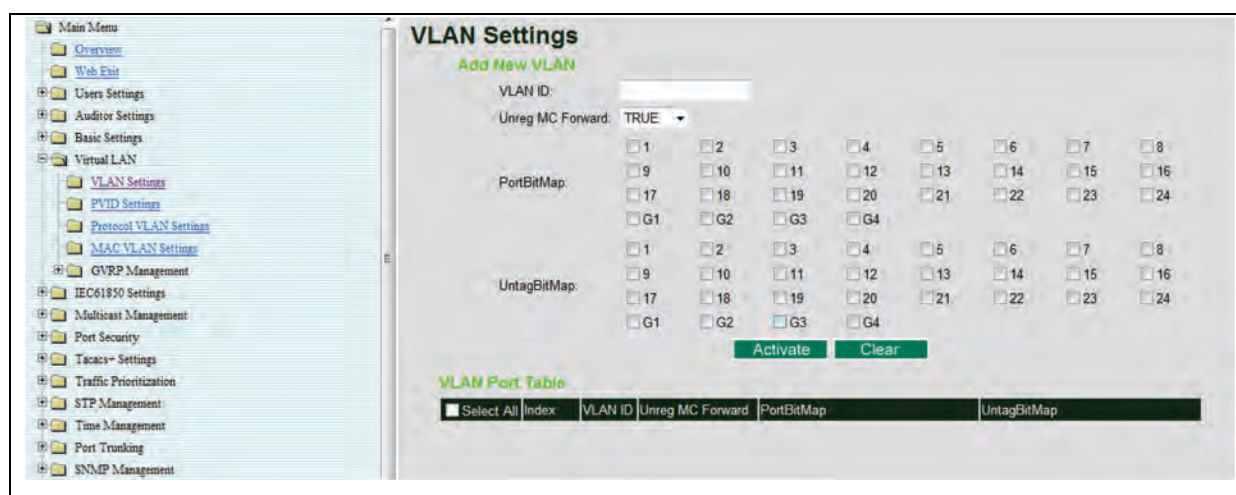


Figure 4.6-1 VLAN Settings

- **Table Select**

VLAN_Port_Table Display the configured VLAN list by VLAN ID

- **VLAN ID**

Current VLAN ID (Range: 2~4094)

A VLAN with VLAN ID = 1 is the default setting and does not need to be changed.

- **Unreg MC Forward**

The forward mode of unregistered multicast for the current VLAN

TRUE Forward

FALSE Drop

- **PortBitMap**

The port(s) included in the current VLAN ID.

Multiple checks are allowed. All ports can be checked, and at least 1 port must be checked.

- **UntagBitMap**

The untagged port(s) included in the current VLAN ID.

Empty space could be accepted. The checked ports in "**PortBitMap**" do not need to be set.

Click the "**Activate**" button to save the currently set VLAN, which will be displayed in the VLAN table after successful setting. Select the VLAN to be deleted from the VLAN table, and click the "**Remove Select**" button to delete the selected VLAN.

To edit an existing VLAN information, select the VLAN ID that already exists in the VLAN table, add or delete ports in "**PortBitMap**" and add or delete untagged ports in "**UntagBitMap**" in the existing VLAN through the "**Activate**" or "**Clear**" buttons.

4.6.3 PVID Settings

PVID is used to determine the default VLAN for untagged messages entering the port to be transmitted in the switch. For example, if the PVID of a port is set to 2, untagged messages entering the port will be transmitted in VLAN 2 of the switch, and this setting will not affect tagged messages entering the port.

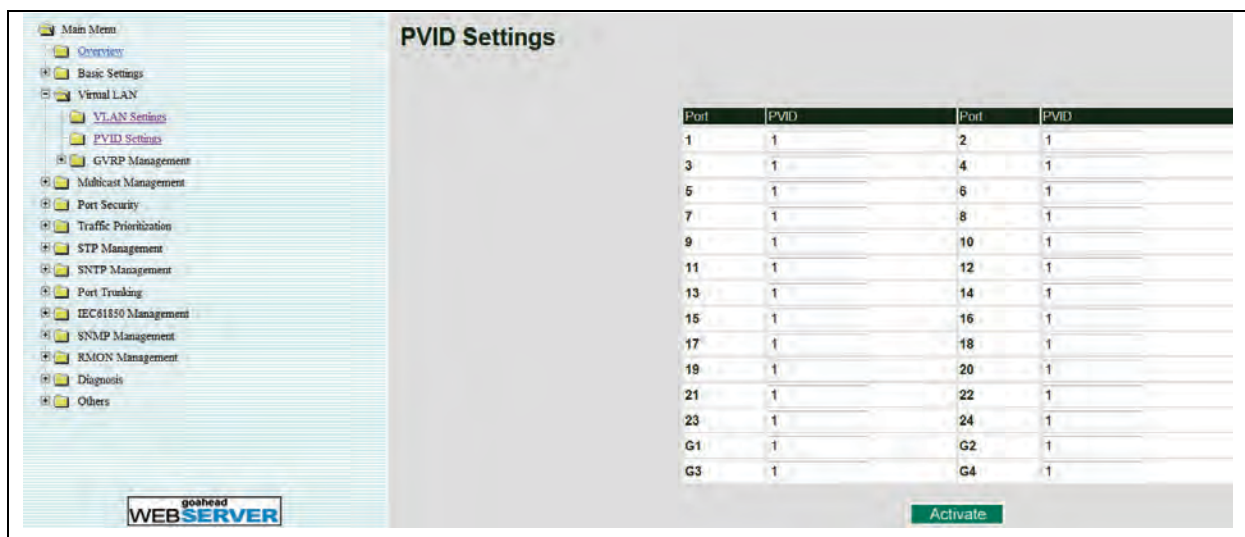


Figure 4.6-2 PVID Settings

NOTICE!

PVID must be the VLAN already set in VLAN settings, otherwise the message will be discarded directly.

4.6.4 Protocol VLAN Settings

Protocol VLAN is used to determine the VLAN that the untagged designated protocol type message entering the port is transmitted in the switch. For example, if the protocol type of the message is 0x0800 and the Protocol VLAN of the protocol message is set to 2, the untagged message with protocol type 0x0800 entering the port will be transmitted in VLAN 2 of the switch.

Figure 4.6-3 Protocol VLAN Settings

- **PortBitMap**

The port(s) included in the current VLAN ID.

Multiple checks are allowed. All ports can be checked, and at least 1 port must be checked.

- **Priority**

Frame priority (invalid for PCS-9882XD-H2 series)

NOTICE!

PVID must be the VLAN already set in VLAN settings, otherwise the message will be discarded directly.

4.6.5 GVRP Management

4.6.5.1 GVRP

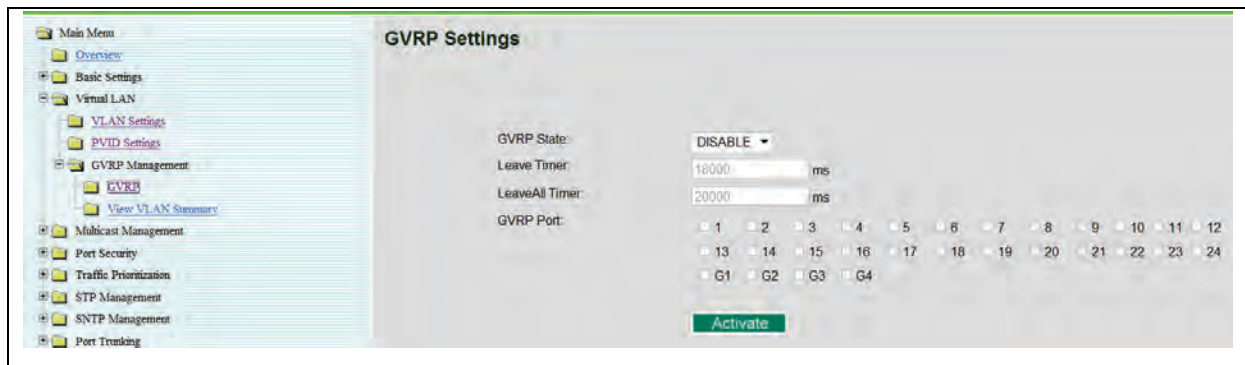


Figure 4.6-4 GVRP

- **Leave Timer**

The "Leave" interval in GVRP

Recommended value: 18000ms; Minimum value: 600ms.

- **LeaveAll Timer**

The "LeaveAll" interval in GVRP

Recommended value: 20000ms; Minimum value: 10000ms.

NOTICE!

"LeaveAll Timer" must be greater than "Leave Timer".

- **GVRP Port**

GVRP-enabled port(s) (Allow multiple selections)

NOTICE!

All ports learned dynamically by GVRP are applied to tag mode.

NOTICE!

If both GVRP and static VLAN are enabled, the switch will register static VLAN to all GVRP-enabled ports.

NOTICE!

If both GVRP and static VLAN are enabled, when the static VLAN table has changed, please disable the GVRP function and then enable it again, or reboot the switch.

4.6.5.2 View VLAN Summary

Use this menu to view all registered VLAN and dynamic and static VLAN table learned by GVRP.

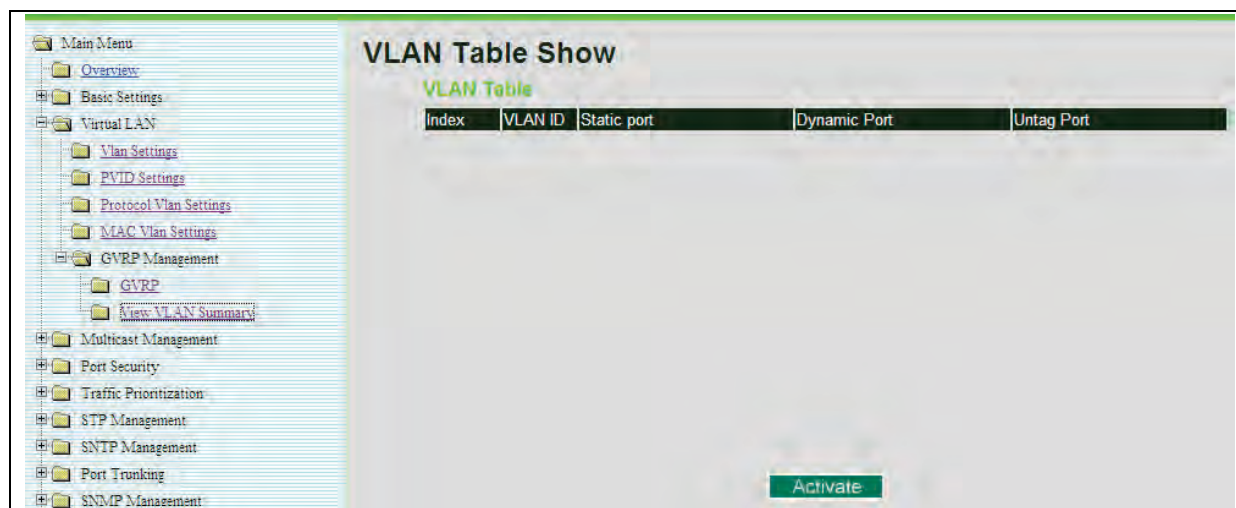


Figure 4.6-5 View VLAN Summary

NOTICE!

If the GVRP function is disabled, this table is hidden.

4.7 IEC 61850 Settings

The PCS-9882XD-H2 series switches support IEC 61850 modeling. After the IEC 61850 function is enabled, the switch starts the IEC 61850 server process. Client could connect to the switch and read the IEC 61850 model of the switch and related data.

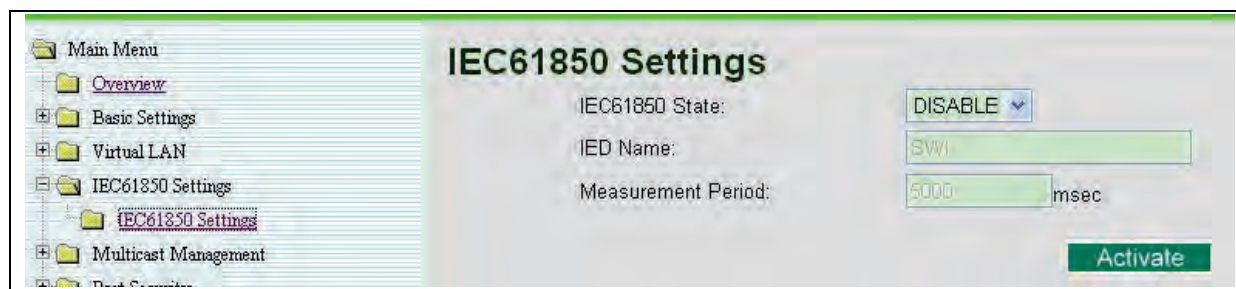


Figure 4.7-1 IEC 61850 Settings

- **IED Name**

IED name of switch

Type: string; Length: max. 32 bytes.

- **Measurement Period**

Upload period of measurement

Unit: ms; Default value: 5000ms.

4.8 Multicast Management

Multicast data frame refers to the message whose destination MAC address is multicast address. The PCS-9882XD-H2 series managed Ethernet switches support multicast data frame management functions. The supported management methods include static multicast management, GMRP, IGMP Snooping.

4.8.1 Static Multicast Group

Static configuration is used to control the forwarding range of multicast addresses in the switch. The configured entries will be displayed in the static multicast table and forwarded according to the configured port range. Unconfigured entries can be controlled to be forwarded or not forwarded to all ports except the CPU port.

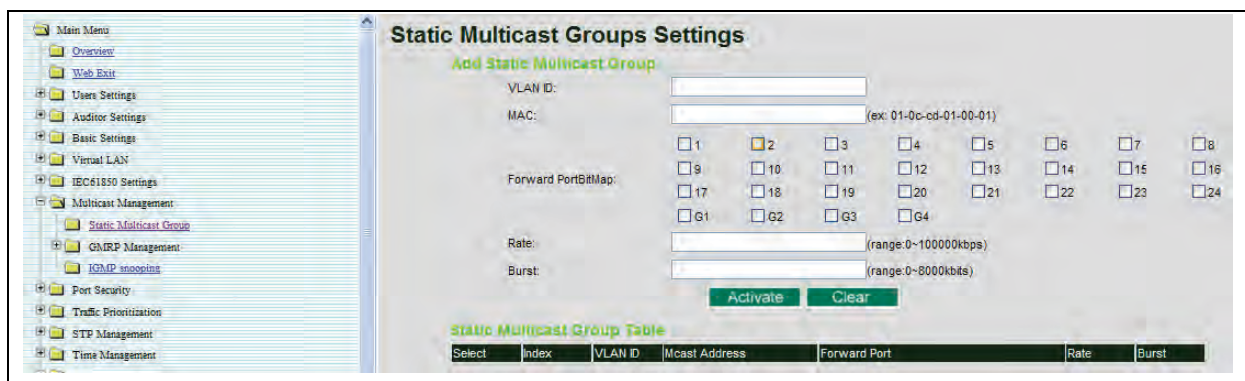


Figure 4.8-1 Static Multicast Group

- **VLAN ID**

The VLAN to add the multicast MAC address

In "Basic Settings" -> "Port" -> "MAC Parameters", if "MAC Address Study Mode" = "VLAN_MAC", the current VLAN ID must be inputted. Each multicast MAC address can adopt different forward strategies in different VLAN. Else if "MAC Address Study Mode" = "MAC", VLAN ID will be configured as the default value "1". All multicast MAC addresses adopt the same forward strategy in all VLAN.

- **Forward PortBitMap**

The ports to forward multicast message

Multiple checks are allowed. All ports can be checked, and at least 1 port must be checked.

- **Rate**

Rate limit of the configured MAC address in this VLAN

Default value: 0 (no limit); Min. value: 64; Resolution: 8; Unit: kbps.

- **Burst**

Burst limit of the configured MAC address in this VLAN

Default value: 0 (no limit); Unit: kbits.

Click the **"Activate"** button to add static multicast entries, which will be displayed in the static multicast table after successful setting. If the MAC address to be added already exists in the same VLAN in the static multicast table, clicking the **"Activate"** button indicates adding a port to the original static multicast table entry.

User can delete some forwarding ports from the original static multicast table entry by filling in VLAN ID, MAC and the port to be deleted and clicking the **"Clear"** button. If all forwarding ports of an entry are deleted, the entry will also be deleted.

User can select one or more static multicast entries to delete in the static multicast table, and click the **"Remove Select"** button to delete the selected static multicast entries.

NOTICE!

When using static multicast management, pay attention to the **"VLAN 1 Unregistered Multicast"** option in the **"Basic Settings"** -> **"Port"** -> **"MAC Parameters"** menu. Multicast addresses added to the static multicast table are forwarded according to the forwarding strategy of the static multicast table, unregistered multicast addresses in VLAN 1 can be controlled to be forwarded or not forwarded to all ports except the CPU port through this option. Unregistered multicast addresses in other VLANs can be controlled to be forwarded or not forwarded to all ports except the CPU port when configuring VLANs.

NOTICE!

If the **"MAC Address Study Mode"** option in the **"Basic Settings"** -> **"Port"** -> **"MAC Parameters"** menu is changed, the switch will reboot automatically. After reboot, the entries of the static multicast table will be reset according to the new MAC address study mode. At this time, the configuration of the static multicast table needs to be checked.

NOTICE!

If both GMRP and static multicast management are enabled, the switch will register static multicast address to all GMRP-enabled ports.

NOTICE!

If both GMRP and static multicast management are enabled, when the static multicast table has changed, please disable the GMRP function and then enable it again, or reboot the switch.

4.8.2 GMRP Management

GARP Multicast Registration Protocol (GMRP) is an application of General Attribute Registration Protocol (GARP). It mainly provides two-layer multicast management functions. The GMRP operation is based on the services provided by GARP, allowing the terminal station to dynamically register with the connected switches, and this information can be propagated to all switches supporting GMRP.

When a host wants to join a multicast group, it needs to send a GMRP join message. Once the GMRP join message is received, the switch will join the port that received the message to the appropriate multicast group. The switch sends GMRP join message to all other hosts in the VLAN, one of which serves as the multicast source. When the multicast source sends the multicast messages, the switch sends them only through the port previously added to the multicast group. In addition, the switch periodically sends GMRP queries. If the host wants to stay in the multicast group, it will respond to GMRP queries. In this case, the switch does not operate at all. If the host does not want to stay in the multicast group, it can either send a leave message or not respond to periodic GMRP queries. Once the switch receives the host leave message or does not receive the response message during the setting of "**leaveAll timer**", it deletes the host from the multicast group.

4.8.2.1 GMRP

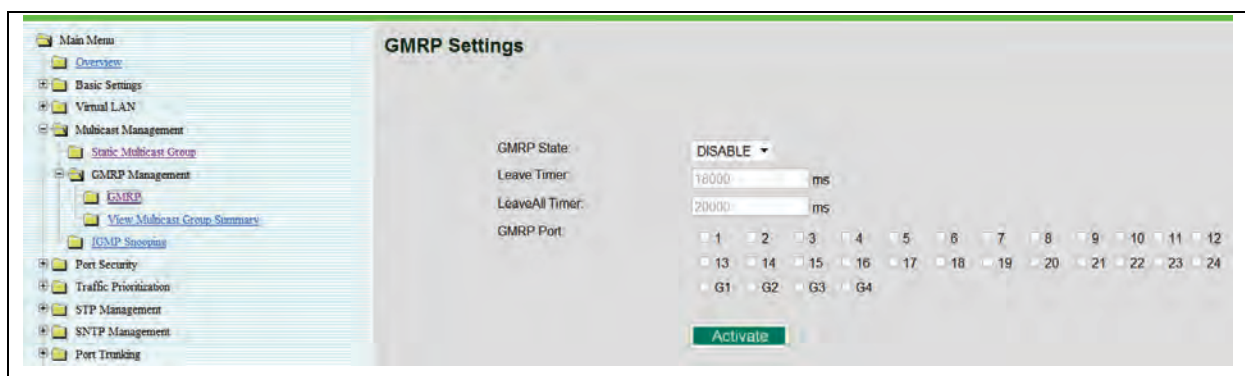


Figure 4.8-2 GMRP

- **Leave Timer**

The "Leave" interval in GMRP

Recommended value: 18000ms; Minimum value: 600ms.

- **LeaveAll Timer**

The "LeaveAll" interval in GMRP

Recommended value: 20000ms; Minimum value: 10000ms.

NOTICE!

"**LeaveAll Timer**" must be greater than "**Leave Timer**".

- **GMRP Port**

GMRP-enabled port(s) (Allow multiple selections)

NOTICE!

When using GMRP, pay attention to the "**VLAN 1 Unregistered Multicast**" option in the "**Basic Settings**" -> "**Port**" -> "**MAC Parameters**" menu. The multicast address learned by GMRP is forwarded according to the learned forwarding strategy and unregistered multicast addresses in VLAN 1 can be controlled to be forwarded or not

forwarded to all ports except the CPU port through this option. Unregistered multicast addresses in other VLANs can be controlled to be forwarded or not forwarded to all ports except the CPU port when configuring VLANs.

NOTICE!

If both GMRP and static multicast management are enabled, the switch will register its static multicast table to all GMRP-enabled ports.

NOTICE!

If both GMRP and static multicast management are enabled, when the static multicast table has changed, please disable the GMRP function and then enable it again, or reboot the Ethernet switch.

4.8.2.2 View Multicast Group Summary

Use this menu to view all registered multicast group and dynamic and static multicast group learned by GMRP.



Figure 4.8-3 View Multicast Group Summary

NOTICE!

If the GMRP function is disabled, this table is hidden.

4.8.2.3 Save Multicast Group

Use this menu to solidify the dynamic multicast learned by GMRP, i.e. to save the dynamic multicast as static multicast.



Figure 4.8-4 Save Multicast Group

- **Rate**

Rate limit of the data stream whose destination MAC address is SV or GOOSE address in GMRP dynamic multicast table

Default value: 0 (no limit); Min. value: 64; Resolution: 32; Unit: kbps.

- **Burst**

Burst limit of the data stream whose destination MAC address is SV or GOOSE address in GMRP dynamic multicast table

Default value: 0 (no limit); Unit: kbits.

Click the “**Activate**” button to save the multicast group, which will be displayed in the static multicast table after successful setting. If the MAC address to be saved already exists in the same VLAN in the static multicast table, clicking the “**Activate**” button indicates adding a port to the original static multicast table entry. At the same time, all dynamic ports on the “**View Multicast Group Summary**” menu will be displayed in static ports.

4.8.3 IGMP Snooping

Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast constraint mechanism running on 2-layer devices, which is used to manage and control the forwarding of multicast data frames. The 2-layer device running IGMP Snooping analyzes the received IGMP message, establishes a mapping relationship between the port and the MAC multicast address, and forwards multicast data according to the mapping relationship.

IGMP Snooping is the same as IGMP protocol. Both of them are used for multicast group management and control. Both of them use IGMP messages. IGMP protocol runs on the network layer, while IGMP Snooping runs on the link layer. When the 2-layer Ethernet switch receives the IGMP message passed between the host and the router, IGMP Snooping analyzes the information carried by the IGMP message, establishes and maintains the MAC table on the layer 2, and then forwards the multicast messages sent from the router according to the MAC table. IGMP Snooping will only actively send IGMP specific group query messages to a port when it receives an IGMP leave message from a port or the aging time timer of a port expires. In addition, it will not send any IGMP messages to the port.



Figure 4.8-5 IGMP Snooping

- **Mode**

PASSIVE Monitoring IGMP frames without any query

ACTIVE Monitor IGMP frames with periodic query

4.9 Port Security

The PCS-9882XD-H2 series managed Ethernet switches support two port security access control policies to control the security of data packets flowing into the switches, namely, port security based on static MAC address and port security based on IEEE 802.1X protocol.

The port security policy based on static MAC refers to assigning one or more MAC addresses to each port in the static MAC address table of the device in advance. When the port security policy based on static MAC is adopted, the port discriminates the source MAC address of the incoming data packet. If the source MAC address exists in the static MAC table and is associated with the port, the data packet is forwarded, otherwise, the data packet will be discarded.

IEEE 802.1X protocol defines an authentication mode based on the client and server model. The switch must receive the authentication request from the client and only open the controlled port to forward data packets when it confirms to the authentication server that the requested user information is correct. Otherwise, the controlled port of the switch closes, waits for the authentication application message, and does not forward data packets other than the authentication application message.

4.9.1 Introduction of IEEE 802. 1X

802.1X is a port-based authentication protocol, the ultimate purpose of which is to determine whether a port is available. For a port, if the authentication is successful, the port will be "opened" to allow all messages to pass through. If the authentication is not successful, the port will remain "closed", i.e. only 802.1X authentication protocol messages will be allowed to pass.

The 802.1X architecture consists of three parts, namely the requester system, the authentication system and the authentication server system.

- Requester system

A requestor is usually a user terminal device supporting 802.1X authentication, and the user initiates 802.1X authentication by starting the client.

- Authentication system

Authentication system is usually a network device supporting 802.1X protocol (such as PCS-9882XD-H2 series managed Ethernet switch), which provides service port for requestor to realize 802.1X authentication.

- Authentication server system

Authentication server is an entity that provides authentication service for authentication system. RADIUS server is commonly used to realize authentication and authorization functions of authentication server.

Extensible Authentication Protocol Over Lan (EAPOL) protocol defined by 802.1X runs between the requestor and the authentication system. The authentication system converts EAPOL into other authentication protocols (such as RADIUS) and transmits user authentication information to the authentication server system.

Each physical port of the authentication system contains a controlled port and an uncontrolled port. Uncontrolled ports are always in a two-way connected state and are mainly used for transmitting EAPOL protocol frames and can ensure receiving EAPOL authentication messages sent by authentication requesters at any time. Controlled ports are opened only when authentication is passed, and are used to transfer network resources and services.

4.9.2 Port Security State

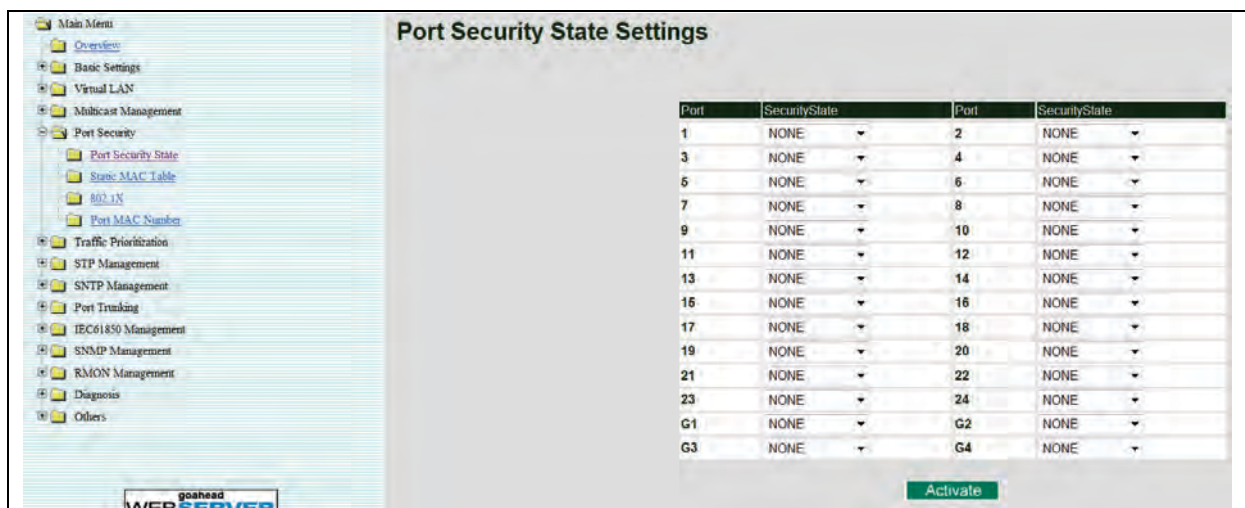


Figure 4.9-1 Port Security State

NOTICE!

If the port adopts 802.1X security policy, the 802.1X authentication module needs

to be enabled (see the following section), otherwise the port will be in a failed authentication state and will not process authentication requests.

4.9.3 Static MAC Table

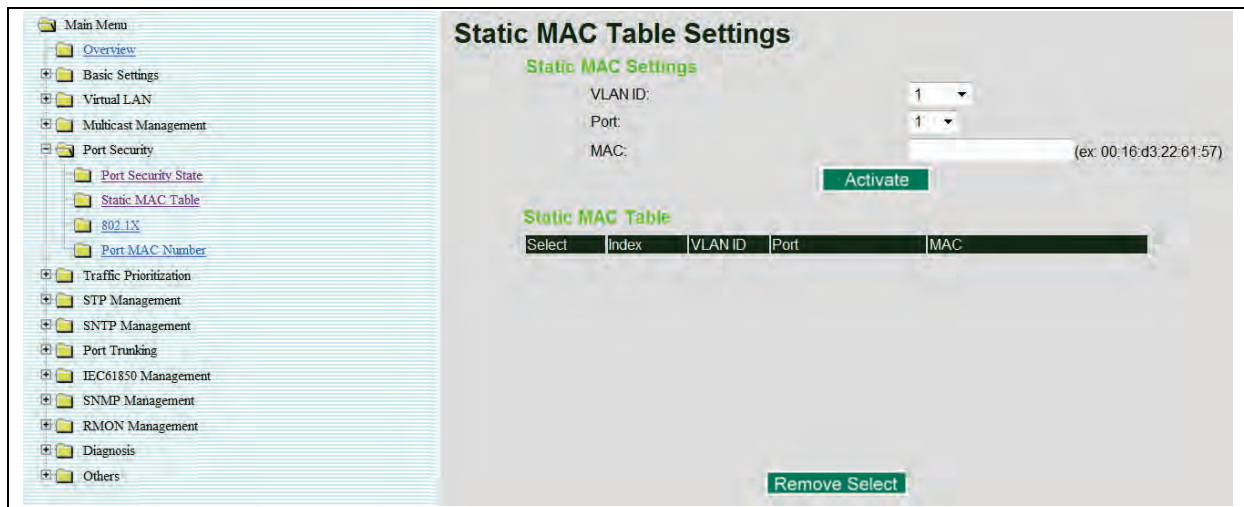


Figure 4.9-2 Static MAC Table

● VLAN ID

VLAN of the static MAC address to be added

If "VLAN_MAC" is selected in "MAC Address Study Mode" in "Basic Settings" -> "Port" -> "MAC parameters" menu, the actual VLAN ID can be selected here, and at this time, each MAC address can adopt different forwarding policies in different VLANs. Else if "MAC" is selected, then this value can only be selected as 1. At this time, each MAC address adopts the same forwarding policy in all VLANs.

Click the "Activate" button to add static MAC address table entries. Select the entries that have been added, and click the "Remove Select" button to delete the selected entries.

NOTICE!

In the static MAC address table, entries with the same VLAN ID and MAC address are not allowed to be added.

NOTICE!

If the MAC address study mode of the switch is changed, i.e. the "MAC Address Study Mode" option in the "Basic Settings" -> "Port" -> "MAC Parameters" menu is changed, the switch will reboot automatically. After rebooting, the entries in the static MAC address table will be reset according to the new MAC address study mode. At this time, the configuration of the static MAC address table needs to be checked.

4.9.4 802.1X

Use this menu to set IEEE 802.1X related parameters. The 802.1X parameters can only be displayed and edited when the 802.1x module is enabled.

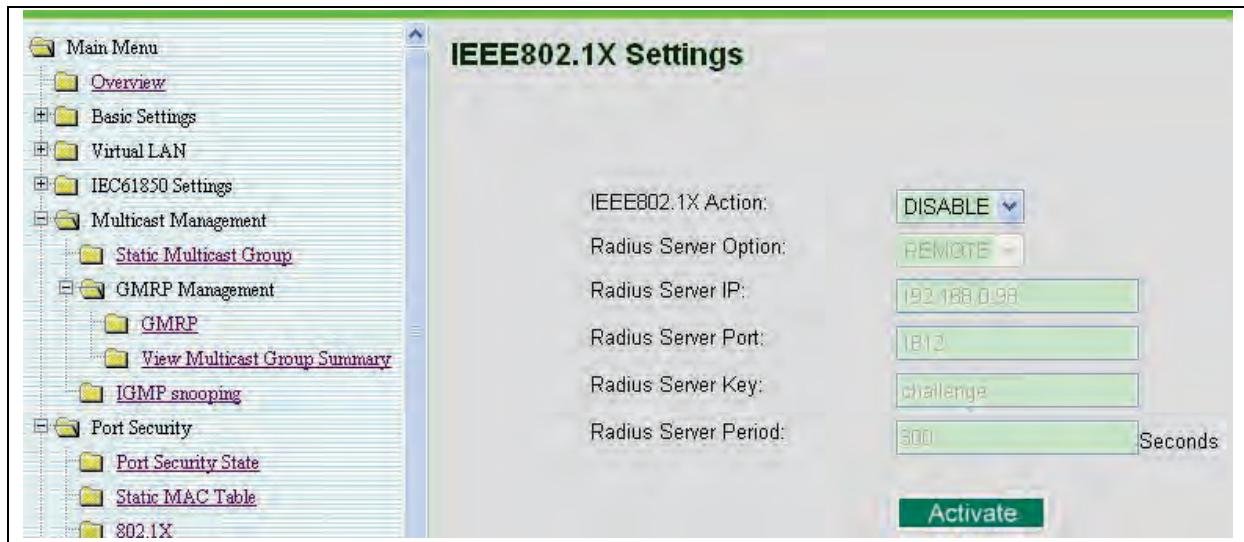


Figure 4.9-3 IEEE 802.1X Settings

- **RADIUS Server Key**

Authentication key string in 1~31 character(s), which should be the same with setting in authentication server.

- **RADIUS Server Period**

Re-authentication period from the switch to client

Range: 30-2100000000; Recommended value: 300.

NOTICE!

If only parameters other than “**IEEE 802.1X Action**” are modified, the parameters will not take effect until the IEEE802.1X function is disabled and enabled again or the device reboots.

4.9.5 RADIUS Server

Remote Authentication Dial-In User Service (RADIUS) is an authentication protocol with C/S structure. The RADIUS server in this switch can be used as authentication server system in IEEE 802.1X authentication system by cooperating with local internal or remote IEEE 802.1X authentication system.

4.9.5.1 RADIUS Server Settings

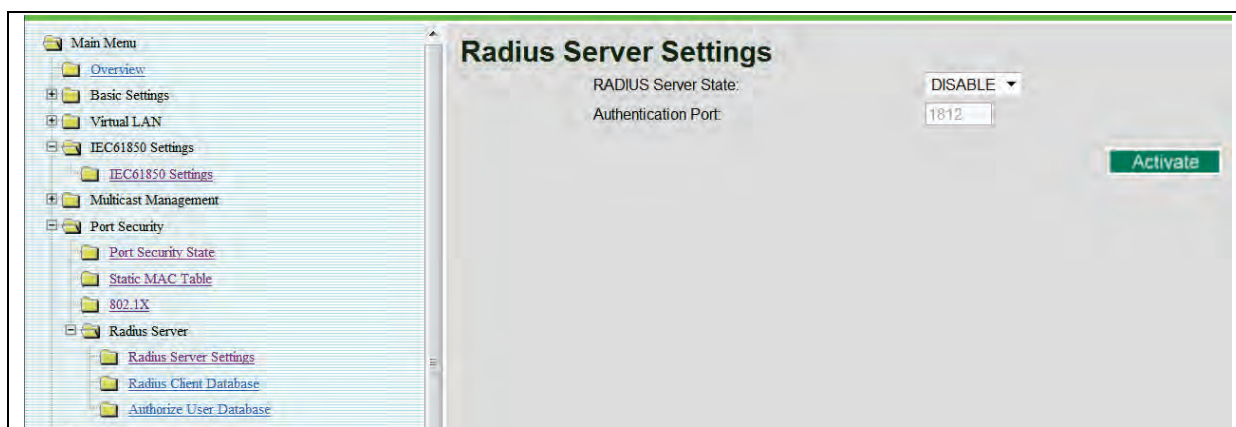


Figure 4.9-4 RADIUS Server Settings

- **Authentication Port**

The port number of authentication, which should be the same with that in the authentication system (such as IEEE 802.1X).

NOTICE!

If only parameters other than “**RADIUS Server State**” are modified, the parameters will not take effect until the RADIUS function is disabled and enabled again or the device reboots.

4.9.5.2 Radius Client Database

Use this menu to set legitimate authentication client information.

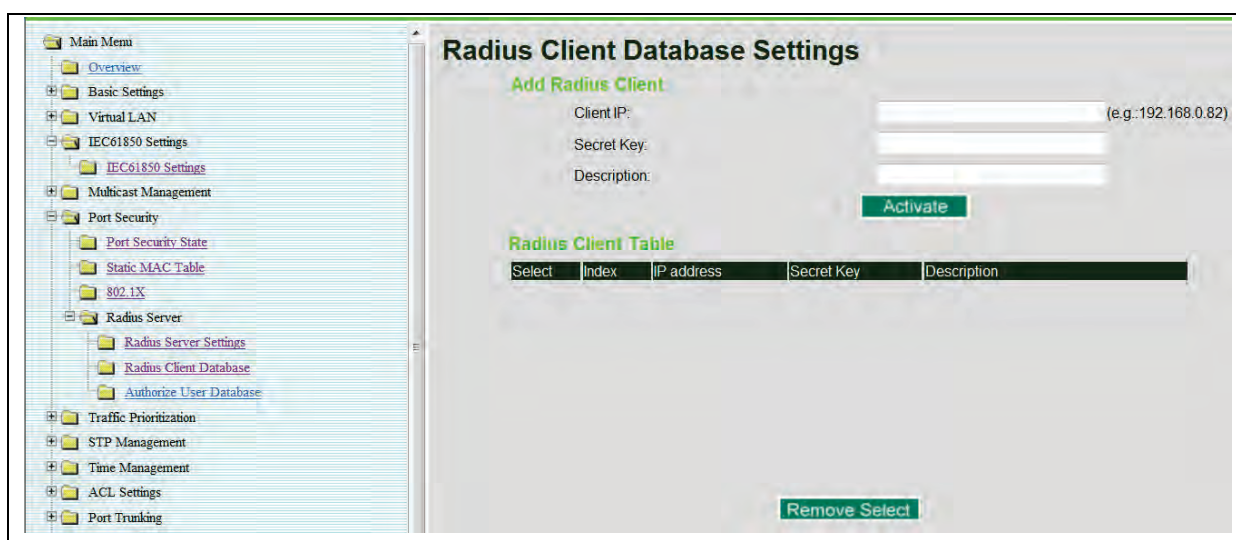


Figure 4.9-5 RADIUS Client Database

- **Client IP**

The IP address of authentication client

A client may be local (the IP address of switch CPU) or remote.

- **Secret Key**

Range: 1~31 character(s)

- **Description**

Range: 1~127 character(s)

NOTICE!

Only configured authentication client can pass authentication.

4.9.5.3 Authorize User Database

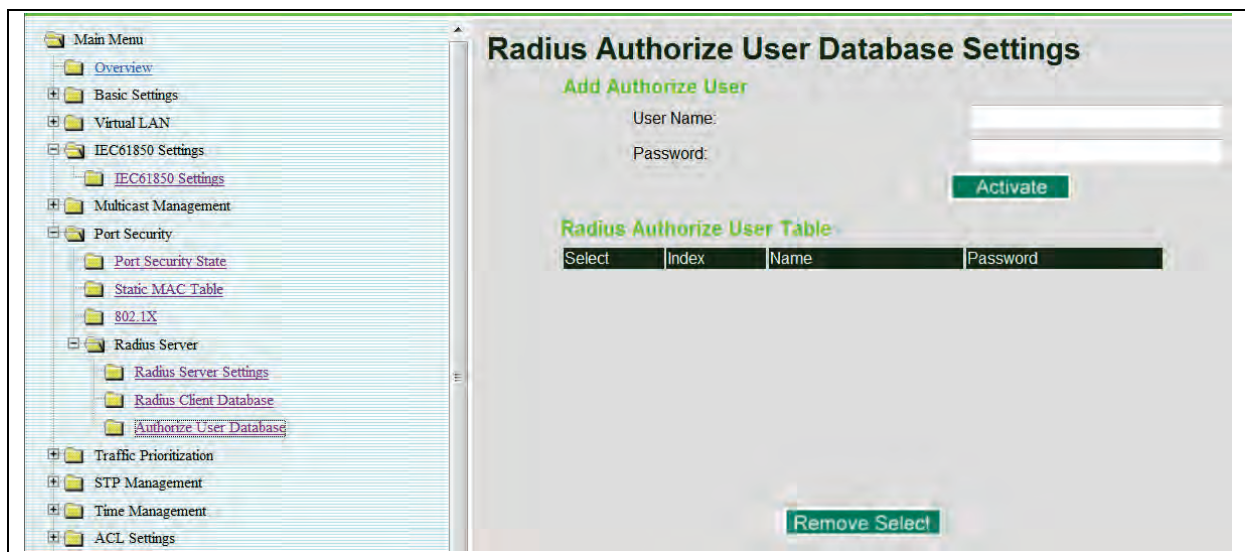


Figure 4.9-6 Authorize User Database

- **User Name**

Range: 1~31 character(s)

- **Password**

Range: 1~31 character(s)

4.10 TACACS+ Settings

Terminal Access Controller Access-Control System (TACACS) refers to a family of related protocols handling remote authentication and related services for networked access control through a centralized server. TACACS+ is a separate protocol that handles Authentication, Authorization, and Accounting (AAA) services. It takes switch login user (i.e. terminal device) through authentication and encrypts all the information such as the username, password, and authorization. The TACACS+ server certificates and responds the result to the TACACS+ client (i.e. terminal device). With the success, user may log in and proceed to operate.

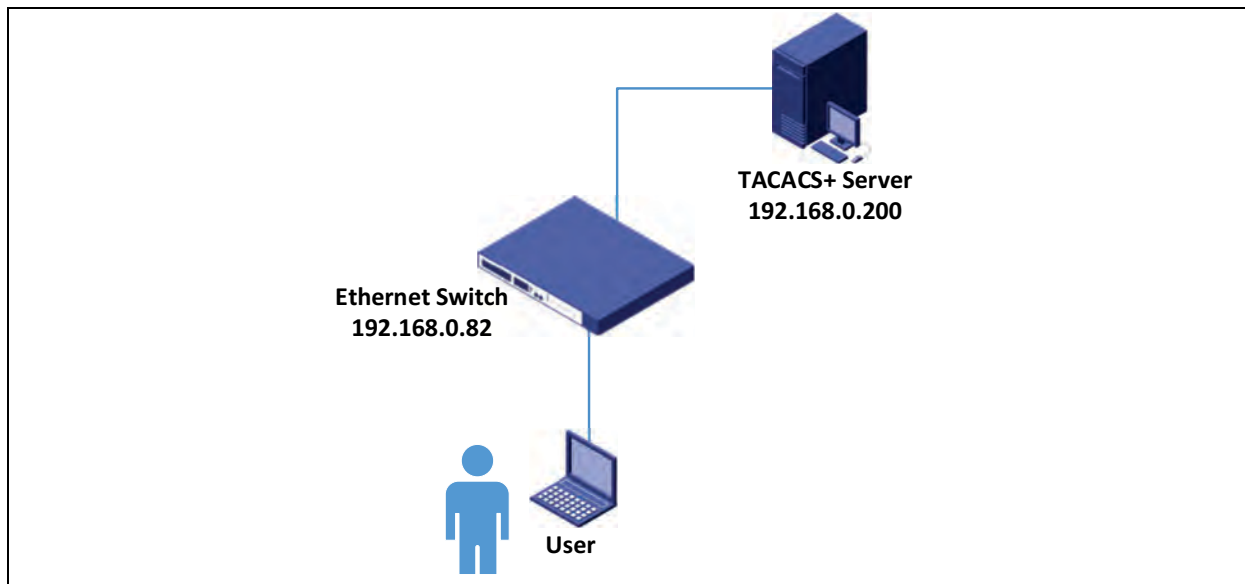


Figure 4.10-1 TACACS+ network structure

4.10.1 TACACS+ Login Method

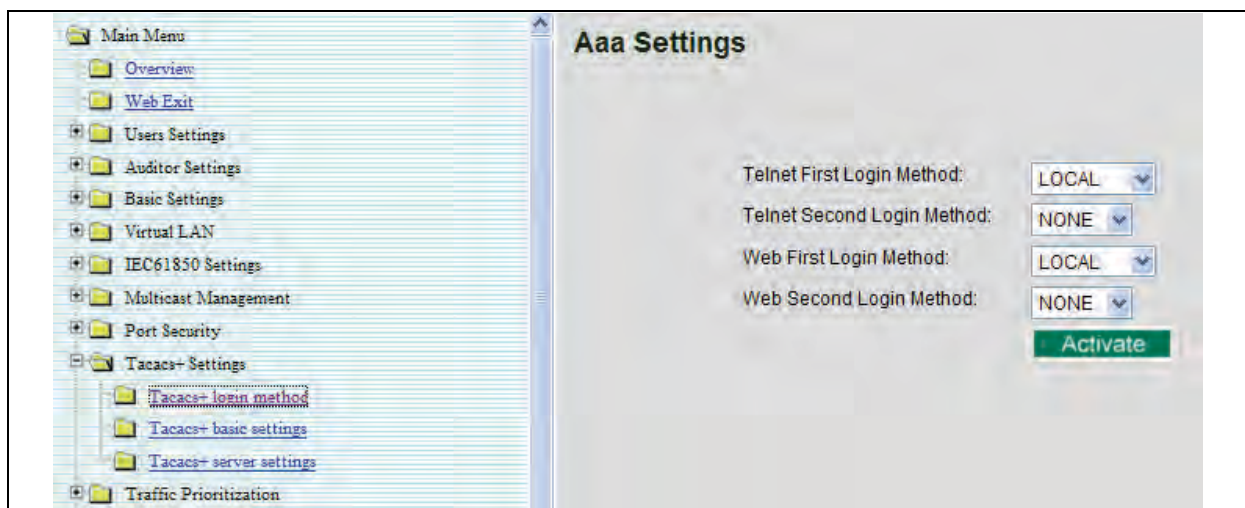


Figure 4.10-2 TACACS+ Login Method

- **Telnet/Web First Login Method**

TACACS+	If selected, the second method could be LOCAL or NONE.
LOCAL	If selected, the second method can only be NONE.

4.10.2 TACACS+ Basic Settings

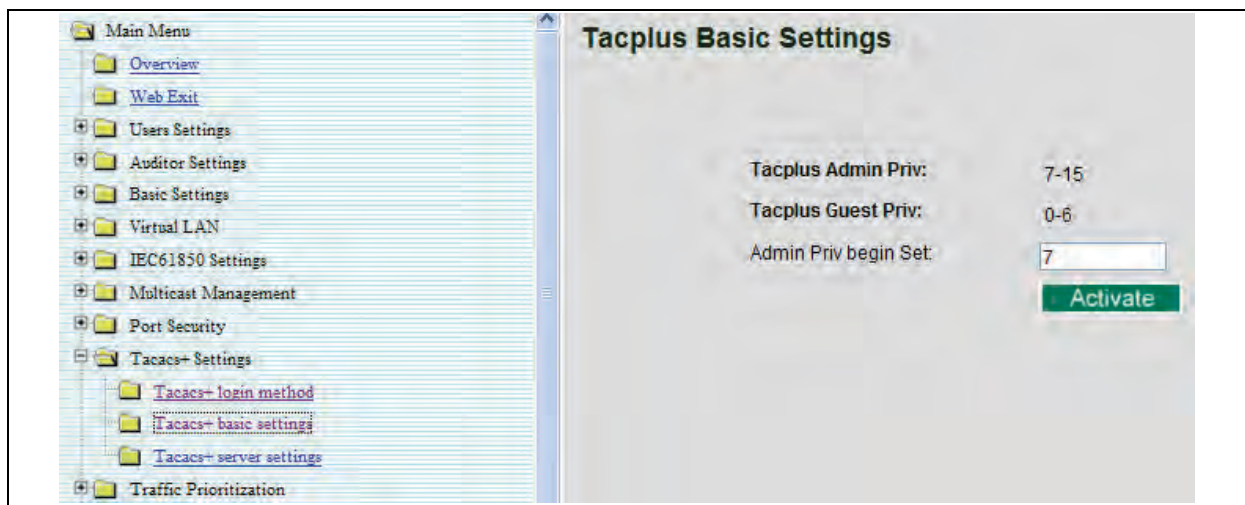


Figure 4.10-3 TACACS+ Basic Settings

- **Admin Priv Begin Set**

The initial value of “admin” authority, which will take effect after clicking “**Activate**”.

In the TACACS+ authorization process, if the value of the “priv-lvl” field returned by the TACACS+ server is within this interval defined by the initial value, the user is granted the “admin” authority (read and write). Otherwise, the value of the “priv-lvl” field returned is beyond the interval, the user is granted the “guest” authority (read only).

4.10.3 TACACS+ Server Settings

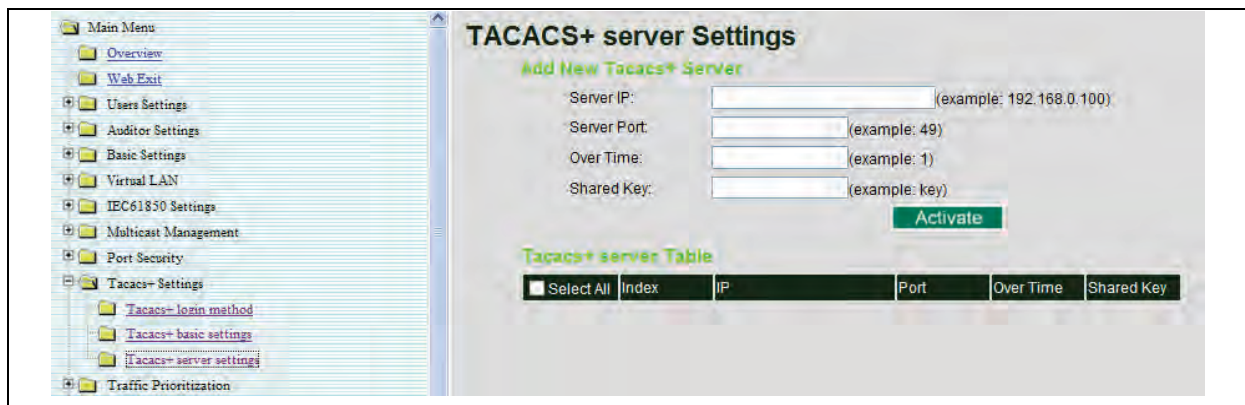


Figure 4.10-4 TACACS+ Server Settings

- **Over Time**

The response timeout parameter of TACACS+ server

If the device does not receive a response from TACACS+ server within this period of time after sending out the request, the authentication fails this time. Generally, the default value is 1 second.

- **Shared Key**

The shared key between the device and TACACS+ server

Both ends verify the legitimacy of messages by setting the shared key. Both ends must have the same key before authentication can be carried out.

Range: 1~63 character(s).

NOTICE!

Click **“Activate”** after completing the filling, and up to 5 TACACS+ servers could be added.

4.10.4 Typical Application Configuration Method

1. Organize the network according to the function brief introduction;
2. For TACACS+ server configuration:
 - a) Set the server IP address to “192.168.0.200”;
 - b) Add the username, password and shared key used by the switch to log on to the web.
3. For switch configuration:
 - a) Set the IP address to “192.168.0.82”;
 - b) In the **“TACACS+ Login Method”** menu, set the web to use TACACS+ authentication;
 - c) In the **“TACACS+ Server Settings”** menu, add the previously configured TACACS+ server.
4. When using web to login to the switch, the remote TACACS+ server authentication access can be realized by entering the user name and password.

4.11 Traffic Prioritization

Class of Service (CoS) is a method to manage network messages by using similar clustering methods, and to prioritize each type of data. The switch maps messages with different priorities to different output queues, and realizes different output sequences of messages with different priorities through output management of different output queues. This switch supports the traffic prioritization technology based on IEEE 802.1p, realizes the mapping relationship between the message priority and the output queue through CoS Mapping setting, and realizes the message output management through setting the weight priority output mode and the strict priority output mode.

4.11.1 CoS Mapping

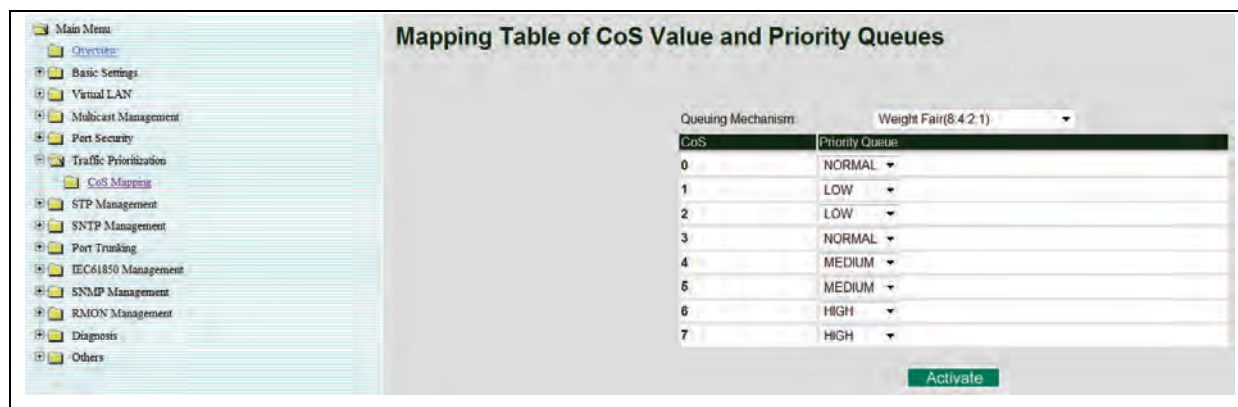


Figure 4.11-1 CoS Mapping

- **Queuing Mechanism**

- Strict**

High Priority First Always

Higher priority frame will always be transmitted firstly, while lower priority frame will only be transmitted after all the higher ones' transmission are completed.

- Weight Fair**

1:2:4:8:16:32:64:127

Each Ethernet switch port will transmit frame in 8 priority queues according to the proportions shown above.

- **CoS**

The 8 priorities defined in IEEE 802.1p (the highest = 7, the lowest = 0)

- **Priority Queue**

The CoS priority queue assigned to received tagged frames with specified IEEE 802.1p priority

4.12 STP Management

4.12.1 RSTP Settings

Rapid Spanning Tree Protocol (RSTP) can converge the network faster when the network structure changes. The protocol has several port types: designed port, root port, alternate port and backup port. RSTP could be applied to the loop network, realizing path redundancy through a certain algorithm, and pruning the loop network into a loop-free tree network, thus avoiding the proliferation and infinite circulation of messages in the loop network.

The main application of RSTP protocol is to avoid network loopback in LAN and solve the "network storm" problem of looped Ethernet network. In a sense, RSTP protocol is a network protection technology, which can eliminate loop connection caused by mistake or accident.

RSTP is developed on the basis of Spanning Tree Protocol (STP) and adds a fast convergence mechanism of P/A negotiation, which greatly improves the self-healing time of the loop network. At present, the switch has realized RSTP recovery time less than 2ms/hop.

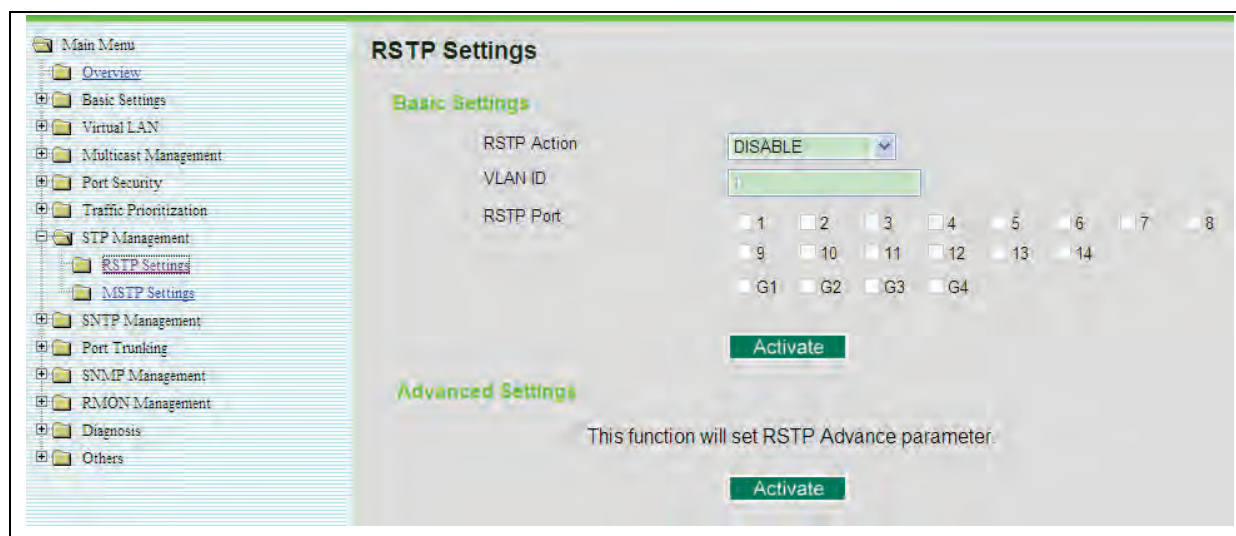


Figure 4.12-1 RSTP Settings

- **RSTP Action**

DISABLE Disable the RSTP function

STANDARD RSTP Enable the RSTP function according to IEEE Std 802.1w

NR RSTP Enable the RSTP function according to NR Electric Co., Ltd. single ring network. Up to two ports can be selected as "RSTP Port".

- **VLAN ID**

Default value: 1, which is unnecessary to be modified.

- **RSTP Port**

Multiple selection is allowed, all ports could be checked, and at least one must be checked.

4.12.1.1 Advanced Settings

RSTP Advanced Settings

Advanced Settings

Bridge Priority:

Hello Time: Seconds

Forwarding Delay: Seconds

Max Age: Seconds

Edge Port:

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8
☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14
☐ G1 ☐ G2 ☐ G3 ☐ G4

BPDUGuard Port:

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8
☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14
☐ G1 ☐ G2 ☐ G3 ☐ G4

Root Guard Port:

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8
☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14
☐ G1 ☐ G2 ☐ G3 ☐ G4

goahead
WEB SERVER
Best viewed with IE 5 above at resolution 1024 x 768

Figure 4.12-2 RSTP Advanced Settings

- **Bridge Priority**

Default value: 32768; Range: 0~61440.

The smaller the value, the higher the priority.

- **Hello Time**

Default value: 2; Range: 1~10.

- **Forwarding Delay**

Default value: 15; Range: 4~30.

- **Max Age**

Default value: 20; Range: 6~40.

- **Edge Port**

Select the port number for a direct connection to a device or terminal so as to transform the forwarding state rapidly.

By default, this function is disabled. It should be enabled for a RSTP-enabled port

- **BPDUGuard Port**

Select the port number for a prevention of ring network because of a connection of edge port to another bridge or switch.

By default, this function is disabled. It should be enabled for a RSTP-enabled and Edge Port-enabled port.

- **Root Guard Port**

Select the port number to be a designed port.

By default, this function is disabled. It should be enabled for a RSTP-enabled port

NOICE!

The relation between "**Hello Time**", "**Forwarding Delay**", and "**Max Age**":

$$2 * (\text{Forwarding Delay} - 1.0 \text{ second}) \geq \text{Max Age}$$

$$\text{Max Age} \geq 2 * (\text{Hello Time} + 1.0 \text{ second})$$

NOTICE!

Normally, "**Advanced Settings**" is unnecessary to be configured. If more than 20 Ethernet switches are included in a network, the "**Max Age**" must be configured to be greater than the Ethernet switch quantity. Moreover, the above relation should be obeyed.

4.12.2 MSTP Settings

Multiple Spanning Tree Protocol (MSTP) is developed from traditional STP and RSTP protocols and is compatible with STP and RSTP.

MSTP introduces the concept of "Region" and divides a network into multiple domains. Each domain forms an Internal Spanning Tree (IST) and a Common Spanning Tree (CST) between domains. Using the Common and Internal Spanning Tree (CIST), connectivity of the entire network is ensured.

Traditional spanning tree algorithm has no connection with VLAN. Messages with different VLAN ID share the same transmission path, while blocked paths do not bear any traffic, resulting in uneven load and waste of resources. MSTP initiates multiple Multi-Spanning Tree Instances (MSTI) on the network. Different VLANs are mapped to different MSTI, and each MSTI independently calculates the network topology. In this way, messages with different VLAN ID can be transmitted through different network topologies to achieve traffic balance.

The calculation of each CIST or MSTI is basically the same as that of RSTP, so the port state fast migration mechanism of RSTP is also maintained, which can realize fast convergence when topology changes.

MSTP bridge role and port role are different from RSTP:

- **Bridge role**

CIST Root	Total root bridge of the whole network
CIST Regional Root	Root bridge of IST(MSTI 0) in the domain
MSTI Regional Root	A MSTI root bridge in the domain
CIST Port Role	Root Port, Designed Port, Alternate Port and Backup Port.

MSTI Port Role

Master Port, which provides the shortest path from the domain to CIST Root, root port, designed port, alternate port and backup port.

For the PCS-9882XD-H2 series managed Ethernet switches, up to 16 MSTI are supported. Public and CIST correspond to MST ID "0", and 16 MSTI correspond to MST ID 01-16 respectively.

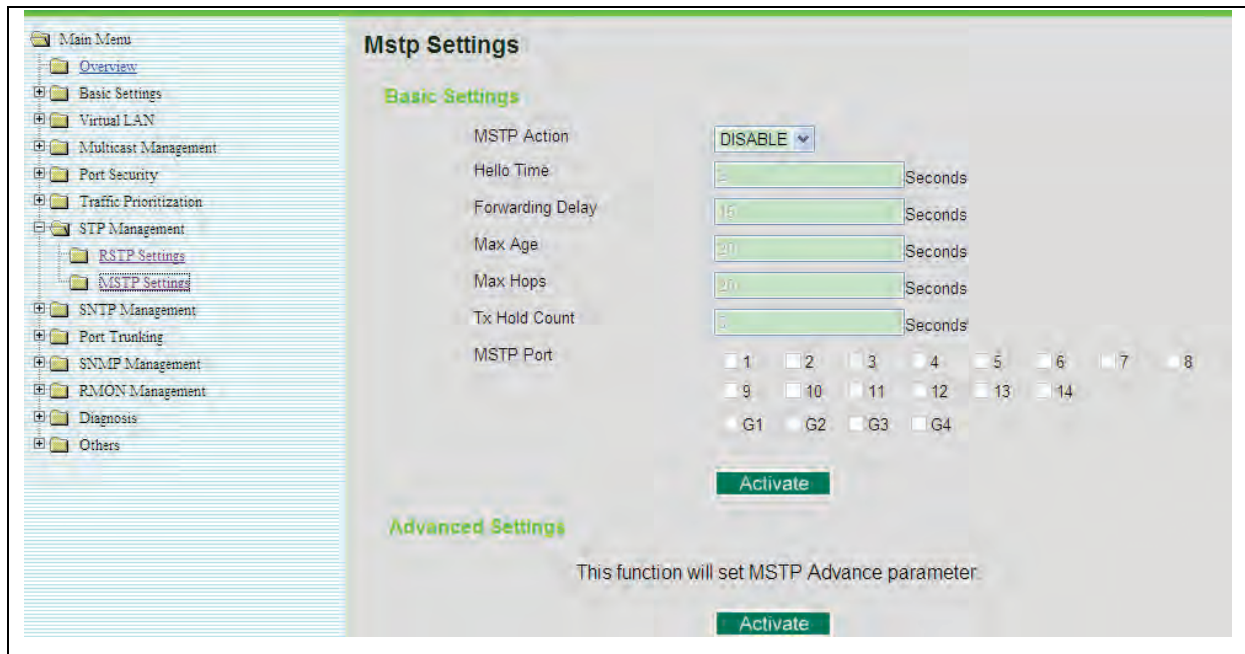


Figure 4.12-3 MSTP Settings

- **Hello Time**

Default value: 2; Range: 1~10.

- **Forwarding Delay**

Default value: 15; Range: 4~30.

- **Max Age**

Default value: 20; Range: 6~40.

- **Max Hops**

Default value: 20; Range: 6~40.

- **Tx Hold Count**

Default value: 5; Range: 3~10.

- **MSTP Port**

Multiple selection is allowed. All ports can be checked, and at least one must be checked.

NOTICE!

The RSTP function and the MSTP function are exclusive. Only one of them can be

enabled at a time.

NOTICE!

An enabled MSTP function without any advanced configuration equals a RSTP function.

NOTICE!

The relation between "Hello Time", "Forwarding Delay", and "Max Age":

$2 * (\text{Forwarding Delay} - 1.0 \text{ second}) \geq \text{Max Age}$

$\text{Max Age} \geq 2 * (\text{Hello Time} + 1.0 \text{ second})$

4.12.2.1 Advanced Settings

MST ID	Bridge Priority	Port Priority	VID
0	32768	128	Not Configured Vlan IDs
1	32768	128	Not Configured Vlan IDs

Figure 4.12-4 MSTP Advanced Settings

- **Region Name**

Hexadecimal ASCII character string (max. 32 bytes)

Default value: the MAC address of this switch

- **Revision Level**

Default value: 0; Range: 0~65535.

- **Bridge Priority**

For MST ID 0~16

Default value: 32768; Range: 0~61440; Multiple of 4096.

- **Port Priority**

For MST ID 0~16

Default value: 128; Range: 0~240; Multiple of 16.

- **MST ID Table**

Range of "MST ID": 0~16; Range of "VID": 2~4094.

By default, all VIDs are configured in the MST ID 0, i.e., all VLANs are mapped to CIST.

NOTICE!

For Ethernet switches in the same region, the "**Region Name**", "**Revision Level**" and mapping table of "VID-MST ID" must be consistent. Otherwise, these Ethernet switches will be regarded to be in different regions.

4.13 Time Management

4.13.1 Time Settings

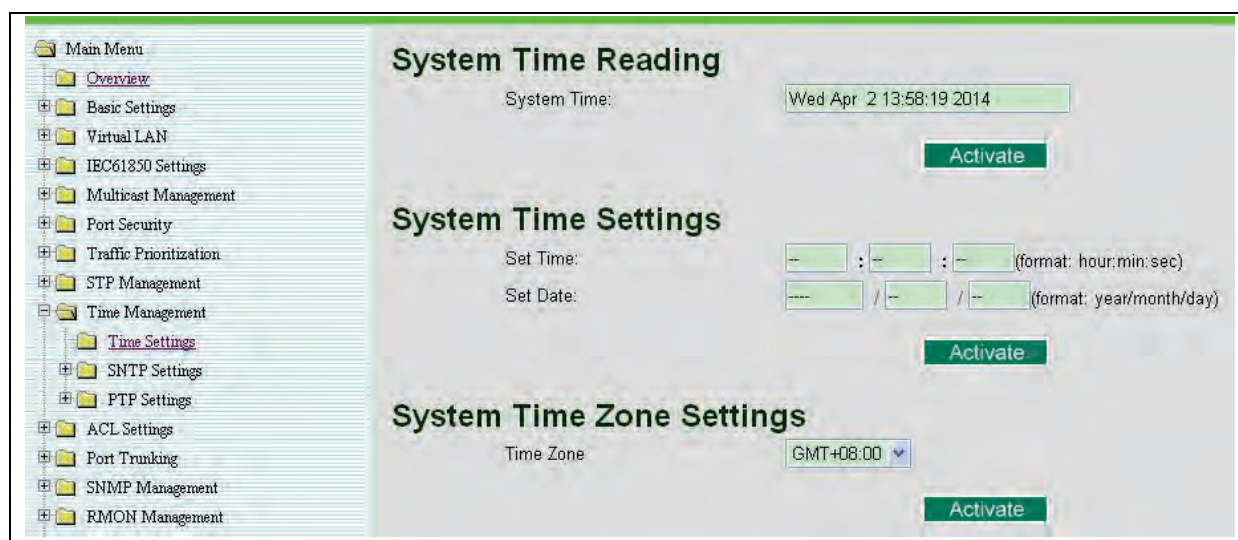


Figure 4.13-1 Time Settings

4.13.2 SNTP Settings

4.13.2.1 SNTP Client Settings

"SNTP Client" means that the switch acts as a client to synchronize with the SNTP clock source in the system.

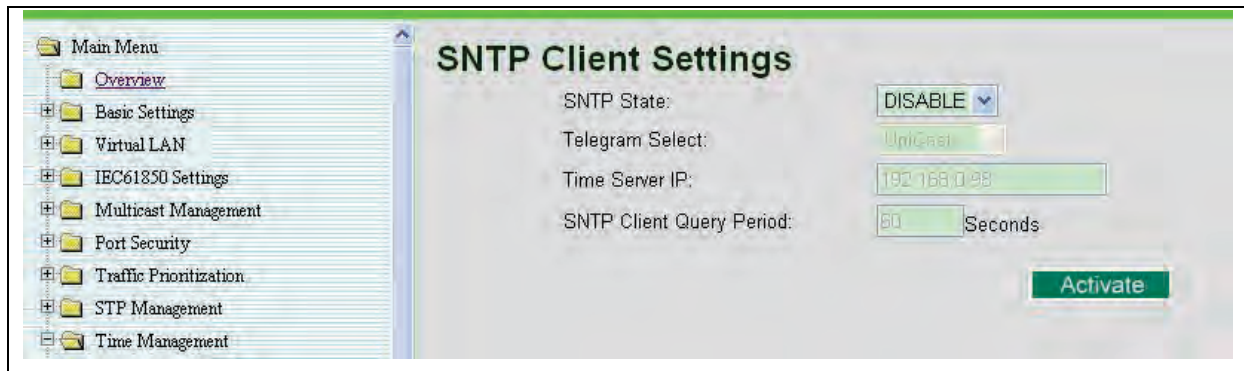


Figure 4.13-2 SNTP Client Settings

- **Telegram Select**

Selection of client synchronization mode

UniCast Client sends query to source, which responds to the current time.

BroadCast Client receives broadcast synchronization message sent by source.

- **Time Server IP**

SNTP source IP address

Valid only when the synchronization mode is UniCast.

- **Time Server Query Period**

Default value: 60; Minimum value: 30.

Valid only when the synchronization mode is UniCast.

4.13.2.2 SNTP Server Settings

"SNTP Server" means that the switch synchronizes the connected devices with its own internal system time.

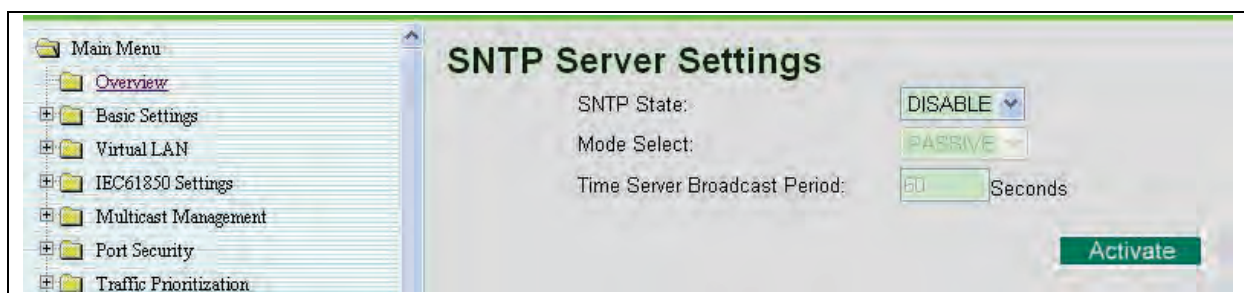


Figure 4.13-3 SNTP Server Settings

- **Mode Select**

PASSIVE Server receives client query and responds to the current time.

ACTIVE Server broadcasts periodically synchronization messages.

- **Time Server Broadcast Period**

Default value: 60; Minimum value: 30.

Invalid when the synchronization mode is UniCast.

4.14 Port Trunking

Trunk means port aggregation by configuring settings. Two or more physical ports are combined into a logical path to increase the bandwidth between switches and network nodes. The bandwidths belonging to these ports are combined to provide ports with an exclusive high bandwidth several times that of independent ports. Trunk is an encapsulation technology for point-to-point link. Both ends of the link can be switches, switch and router, host and switch or router. Based on the port trunk function, it allows switches, switch and router, host and switch or router to transmit simultaneously through parallel connection of two or more ports to provide higher bandwidth, greater throughput and greatly improve the overall network capability..

Under normal circumstances, when trunk function is not used, the transmission medium characteristics of twisted pair cable of megabyte Ethernet determine that the bandwidth of two interconnected common 10M/100M switches is only 100M. If full duplex mode is adopted, the maximum bandwidth of transmission can reach 200M, thus forming the bottleneck of network backbone and server. In order to achieve higher data transmission rate, it is necessary to replace the transmission medium, use gigabit optical fiber or upgrade to gigabit Ethernet, which is very expensive. If the trunk technology is used, the four ports are bundled together to reach 800M bandwidth, which can better solve the contradiction between cost and performance.

4.14.1 Trunking

Use this menu to set port aggregation related functions. By default, trunk mode is off. This switch supports port aggregation of up to 8 IDs.

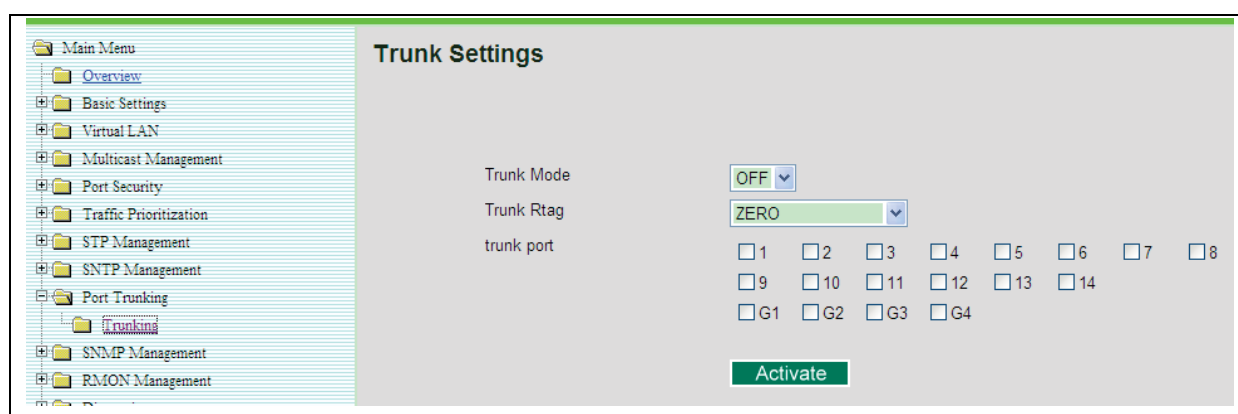


Figure 4.14-1 Trunking

- **Trunk Rtag**

The frame classification mode of the currently set port aggregation function, which is selected by adopting the Hashi table index.

SA	Source MAC address index
DA	Object MAC address index
SA_DA	Source-Object MAC addresses index
SIP	Source IP address index
DIP	Object IP address index
SIP_DIP	Source-Object IP addresses index

- **Trunk port**

Up to 8 ports could be selected.

4.15 SNMP Management

Simple Network Management Protocol (SNMP) is an industry standard widely accepted and in service. It is used to ensure that management information is transmitted between any two points, which is convenient for network administrators to retrieve information, modify information, find faults, complete fault diagnosis, carry out capacity planning and generate reports at any node on the network.

SNMP is divided into two parts: Network Management Station (NMS) and Agent. NMS is a workstation that runs server-side programs. Agent is client software running on network devices. NMS can send GetRequest, GetNextRequest, GetBulk, and SetRequest messages to the Agent. After the Agent receives the NMS request message, it performs Read or Write operations according to the message type to generate a Response message and return the message to NMS. Agent will actively report the event by sending Trap message to NMS when the equipment finds abnormal conditions such as reboot.

Management Information Base (MIB) is the standard for network management data. In this standard, the data items, data types and operations allowed in each data item that the network proxy device must keep are specified. By accessing these data items, all statistical contents of the device can be obtained. The basic network management can be realized through comprehensive analysis of the statistical contents of multiple devices.

SNMP V1 and SNMP V2C use group name authentication. The SNMP Community is named after a string, called the Community Name. SNMP community names are used to define the relationship between SNMP manager and SNMP Agent. The community name acts like a password and can restrict SNMP manager from accessing SNMP Agent on switches.

SNMP V3 defines a framework for integrating security features into the overall functions of SNMP V1 or SNMP V2C. SNMP V3 is only a security specification and does not define new SNMP functions. It only provides security functions for SNMP V1 or SNMP V2C. Therefore, there can form a formula: SNMP V3 = SNMP V2C + Security + Management. SNMP V3 uses authentication method to ensure its data integrity, and MD5 algorithm can be used for authentication. The method of encryption is adopted to ensure the data security, and CBC-DES algorithm can be

used for encryption.

The PCS-9882XD-H2 series managed Ethernet switches support the SNMP V1, SNMP V2C, and SNMP V3 protocols. The standard MIBs supported are mainly contained in the following standard RFC files.

- RFC1213MIB(MIB-2-MIB)
- RFC1907MIB(SNMPv2-MIB)
- RFC2578MIB(SNMPv2-SMI)
- RFC2579MIB(SNMPv2-TC)
- RFC2580MIB(SNMPv2-CONF)
- RFC2819MIB(RMON-MIB)
- RFC2863MIB(IF-MIB)
- RFC3411MIB(SNMP-FRAMEWORK-MIB)
- RFC3412MIB(SNMP-MPD-MIB)
- RFC3414MIB(SNMP-USER-BASED-SM-MIB)
- RFC3415MIB(SNMP-VIEW-BASED-ACM-MIB)

Since these switches are layer-2 network equipment, in principle, the above MIBs beyond layer-2 need not to be realized. Particular MIB groups to be realized include:

- In MIB-II, System Group, Interfaces Group, IP Group (only including CPU management port data statistics), TCP Group (only including CPU management port data statistics), UDP Group (only including CPU management port data statistics), and SNMP Group;
- Some groups of IF-MIB (mainly ifxTable table);
- In RMON-MIB, Statistics Group, History Group, Alarm Group, and Event Group;
- Some groups of SNMP-FRAMEWORK-MIB;
- Some groups of SNMP-MPD-MIB;
- Some groups of SNMP-USER-BASED-SM-MIB;
- Some groups of SNMP-USER-BASED-SM-MIB

Moreover, these switches support NR Electric proprietary MIBs within the file NR_PCS_Switch_MIB. The node of the MIBs is 1.3.6.1.4.1.34572.

These switches support all standard Traps and NR Electric Traps. The Trap transmission adopts SNMP V1, V2C, or V3 format.

In the switch, the SNMP function is disabled by default. When it is enabled, all MIBs supported are enabled. If the SNMP function is disabled, the relevant information of SNMP can be displayed and configured, but any SNMP read/write operation of NMS will not be responded to, and no Trap

will be transmitted.

For the read/write function, the versions V1, V2C, and V3 are supported at the same time. However, user needs to select a version or simultaneous support of all versions. The NMS IP does not need to be set.

For the version V1 or V2C, the default Read Community is "public" and the default Read/Write Community is "private". The name of community is configurable in a maximum length of 32 characters. What's more, the Read/Write community names at the NMS and the switch must be consistent to allow normal read/write operation. For the version V3, by default, there is no user. To use it, a V3 user should be added firstly. For the Trap function, by default, there is no user (i.e. no Trap transmission). User can add or delete Trap user. The switch transmits Trap to all Trap users in the format of V1, V2C, or V3. The maximum Trap user number is 32.

4.15.1 SNMP Settings

Figure 4.15-1 SNMP Settings

4.15.1.1 SNMP State Settings

● NMS IP Address

IP address of NMS

If the IP address is filled in, only the management station with this IP address can access the switch, and the switch will no longer respond to the access requests of management stations with other IP addresses; If "0.0.0.0" is filled here, the NMS IP address is not limited, and multiple management stations with different IP addresses can access the switch at the same time. The default configuration is "0.0.0.0".

4.15.1.2 V1/V2C Settings

- **V1/V2C Read Community**

Default value: public; Range: 1~31 characters.

- **V1/V2C Read/Write Community**

Default value: private; Range: 1~31 characters.

4.15.1.3 V3 Settings

- **User Name**

Range: 1~31 characters

- **Auth Password**

Range: 6~31 characters

- **Privacy Password**

Range: 6~31 characters

4.15.2 Trap Settings

Figure 4.15-2 SNMP Trap Settings

- **IP Address**

IP address of NMS to receive Trap, in the format of "192.168.0.98".

The NMS receiving Trap and the NMS reading and writing data can be a same host or different hosts. The switch supports sending Trap to up to 32 NMS simultaneously.

- **Trap Community**

Range: 1-31 characters

- **Trap User Name**

Range: 1-31 characters

- **Auth Password**

Range: 6-31 characters

- **Privacy Password**

Range: 6-31 characters

NOTICE!

All switches have the same factory default IP. If SNMP is used, the IP addresses of each switch on the network cannot conflict, otherwise the access object will be uncertain.

4.16 RMON Management

Remote MONitor (RMON) is generated to meet the demand of subnet traffic monitoring. It is actually a branch of SNMP. RMON uses SNMP operations and monitors dedicated to subnet monitoring to collect information on subnet traffic and respond to management stations.

The RMON function of the PCS-9882XD-H2 series managed Ethernet switches is disabled by default and is enabled and disabled together with SNMP function. After SNMP is enabled, RMON-MIB is automatically enabled. When SNMP function is disabled, RMON related information can be displayed and configured, but RMON statistics function cannot be realized.

The switch implements statistics group, history group, alarm group and event group in RMON-MIB (RFC2819). The NMS can monitor subnet traffic, historical data, alarm information, events and other data by reading RMON.

RMON's statistics group does not need to be set, and all ports have been added by default. The settings for the other 3 groups of RMON will be described in the following sections.

4.16.1 RMON History Control

RMON History Settings

RMON History Control Settings

Port: 3-1

Requested Buckets:

Interval: Seconds

Owner:

Activate

RMON History Controls Table

Select	Index	Port	Requested Buckets	Interval	Buckets Granted	Owner	Status

Figure 4.16-1 RMON History Control

- **Requested Buckets**

The maximum number of history data buckets saved by this port

Range: 1~2000

- **Interval**

Interval for recording historical data

Range: 1~3600

- **Owner**

Range: 1~63 characters

4.16.2 RMON Alarm

Figure 4.16-2 RMON Alarm

- **Variable**

The specified variable identifier of the sample, which can only be filled in by ASN.1 variables of original type INTEGER

Variable in RMON AlarmTable must be filled in in the form of "Leaf node + Index", with "." in the middle. The meaning is the same as that of the leaf node in the corresponding MIB.

Adding entries with variable identifiers in illegal format will fail. The correct variable format such as "ifInOctets.6" indicates the number of bytes input at port 6, or the scalar "snmpInPkts.0" indicates the number of SNMP data packets received by the device.

No.	Leaf Node	Min. Index	Max. Index
1	ifInOctets	1	28
2	ifInUcastPkts	1	28
3	ifInNUcastPkts	1	28
4	ifInDiscards	1	28
5	ifInErrors	1	28

No.	Leaf Node	Min. Index	Max. Index
6	ifInUnknownProtos	1	28
7	ifOutOctets	1	28
8	ifOutUcastPkts	1	28
9	ifOutNUcastPkts	1	28
10	ifOutDiscards	1	28
11	ifOutErrors	1	28
12	snmpInPkts	0	0
13	snmpOutPkts	0	0
14	snmpInBadVersions	0	0
15	snmpInBadCommunityNames	0	0
16	snmpInBadCommunityUses	0	0
17	snmpInASNParseErrs	0	0
18	snmpInTooBigs	0	0
19	snmpInNoSuchNames	0	0
20	snmpInBadValues	0	0
21	snmpInReadOnlys	0	0
22	snmpInGenErrs	0	0
23	snmpInTotalReqVars	0	0
24	snmpInTotalSetVars	0	0
25	snmpInGetRequests	0	0
26	snmpInGetNexts	0	0
27	snmpInSetRequests	0	0
28	snmpInGetResponses	0	0
29	snmpInTraps	0	0
30	snmpOutTooBigs	0	0
31	snmpOutNoSuchNames	0	0
32	snmpOutBadValues	0	0
33	snmpOutGenErrs	0	0
34	snmpOutGetRequests	0	0
35	snmpOutGetNexts	0	0
36	snmpOutSetRequests	0	0
37	snmpOutGetResponses	0	0
38	snmpOutTraps	0	0
39	snmpEnableAuthenTraps	0	0
40	snmpSilentDrops	0	0
41	snmpProxyDrops	0	0
42	etherStatsDropEvents	1	28
43	etherStatsOctets	1	28
44	etherStatsPkts	1	28
45	etherStatsBroadcastPkts	1	28
46	etherStatsMulticastPkts	1	28
47	etherStatsCRCAlignErrors	1	28

No.	Leaf Node	Min. Index	Max. Index
48	etherStatsUndersizePkts	1	28
49	etherStatsOversizePkts	1	28
50	etherStatsFragments	1	28
51	etherStatsJabbers	1	28
52	etherStatsCollisions	1	28
53	etherStatsPkts64Octets	1	28
54	etherStatsPkts65to127Octets	1	28
55	etherStatsPkts128to255Octets	1	28
56	etherStatsPkts256to511Octets	1	28
57	etherStatsPkts512to1023Octets	1	28
58	etherStatsPkts1024to1518Octets	1	28
59	etherStatsPkts256to511Octets	1	28
60	etherStatsPkts256to511Octets	1	28
61	etherStatsPkts256to511Octets	1	28
62	ifInMulticastPkts	1	28
63	ifInBroadcastPkts	1	28
64	ifOutMulticastPkts	1	28
65	ifOutBroadcastPkts	1	28
66	ifHCInOctets	1	28
67	ifHCInUcastPkts	1	28
68	ifHCInMulticastPkts	1	28
69	ifHCInBroadcastPkts	1	28
70	ifHCOctets	1	28
71	ifHCOUcastPkts	1	28
72	ifHCOMulticastPkts	1	28
73	ifHCOBroadcastPkts	1	28

- **Rising Threshold**

Range: 1~2100000000

- **Falling Threshold**

Range: 1~2100000000

- **Type**

DELTA Difference value

ABSOLUTE Absolute value

- **Interval**

Interval for recording historical data

Range: 1~2100000000

- **Owner**

Range: 1~63 characters

4.16.3 RMON Event

Figure 4.16-3 RMON Event

- **Community**

Trap community generated by RMON

Range: 1~127 characters

- **Description**

Range: 1~127 characters

- **Owner**

Range: 1~63 characters

4.17 Diagnosis

Port mirroring is a method of mirroring data from one or more ports of a switch to one port.

4.17.1 Mirror Settings

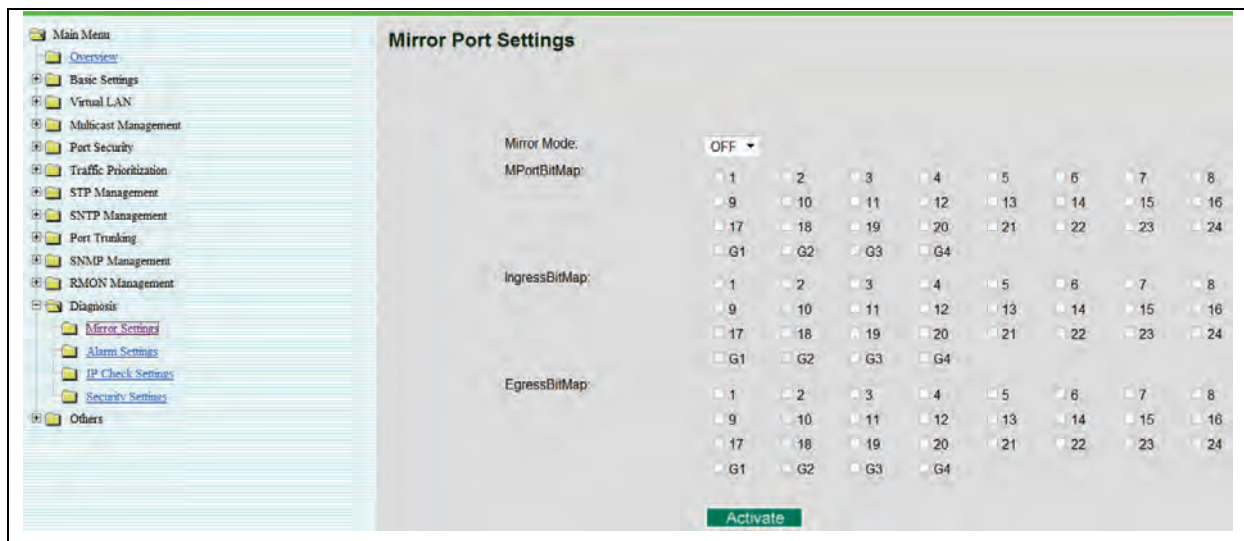


Figure 4.17-1 Mirror Settings

- **MPortBitMap**

Selection of mirror port(s)

A mirror port cannot be selected in **IngressBitMap** and **EgressBitMap**.

- **IngressBitMap**

Selection of port(s) to mirror the input traffic

- **EgressBitMap**

Selection of port(s) to mirror the output traffic

4.17.2 Alarm Settings

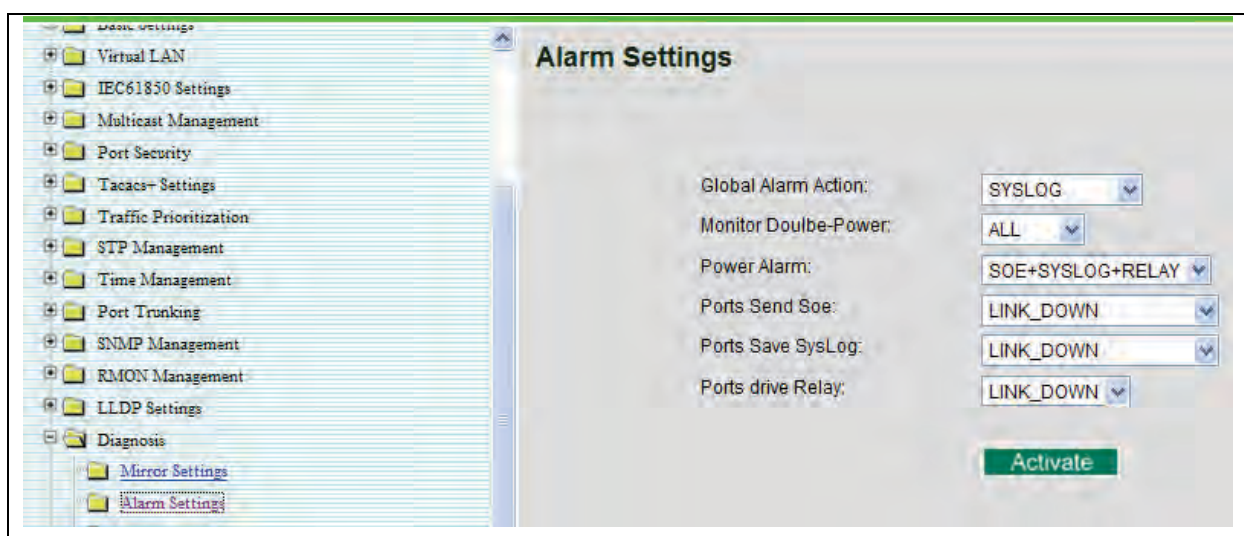


Figure 4.17-2 Alarm Settings

- **Global Alarm Action**

SYSLOG	System log
SOE	Sequence Of Events
NONE	Disabled

4.17.3 IP Check Settings

Use this menu to set the detection function of IP addresses confliction.

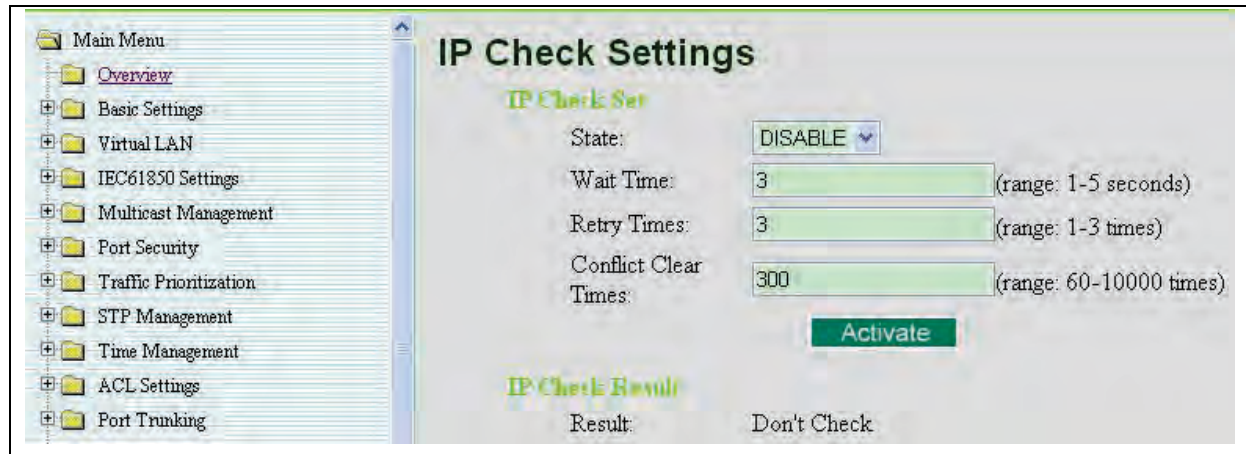


Figure 4.17-3 IP Check Settings

4.17.4 LLDP Settings

At present, there are more and more kinds of network devices and their configurations are complicated. In order to enable devices from different manufacturers to discover and interact with each other's systems and configuration information in the network, a standard information exchange platform is needed.

Link Layer Discovery Protocol (LLDP) is produced under such a background. LLDP is a 2-layer protocol defined in 802.1ab. It provides a standard link layer discovery method, which can organize the main capabilities, management address, device identification, interface identification and other information of the local device into different Type/Length/Value (TLV). It is encapsulated in Link Layer Discovery Protocol Data Unit (LLDPDU) and released to its directly connected neighbors. After receiving this information, neighbors save it in the form of standard Management Information Base (MIB) for the network management system to query and judge the communication status of the link. LLDP does not configure or control network elements or traffic; it only reports on layer 2 configurations.

The PCS-9882XD-H2 series managed Ethernet switches support the standard LLDP protocol. They run this function and provide basic information display. They can also monitor data through SNMP or IEC 61850.

4.17.4.1 LLDP Basic Settings

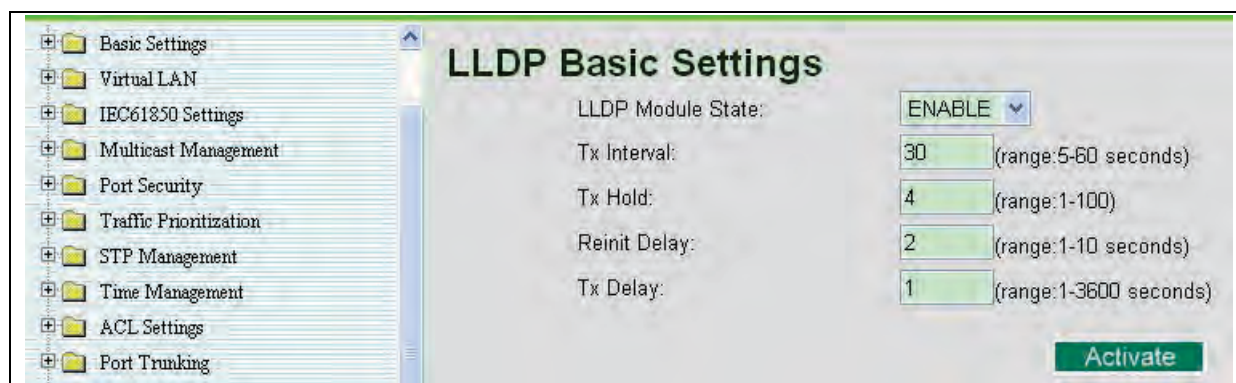


Figure 4.17-4 LLDP Basic Settings

- **Tx Interval, Tx Hold**

The result of “**Tx Interval**” multiplied by “**Tx Hold**” is the actual Time To Live (TTL) of the LLDP packet.

- **Reinit Delay**

Reinitialization delay, which is the time interval from the port to the closed state to the beginning of reinitialization.

- **Tx Delay**

Sending delay after a change of parameters or states

4.17.4.2 LLDP Port Settings

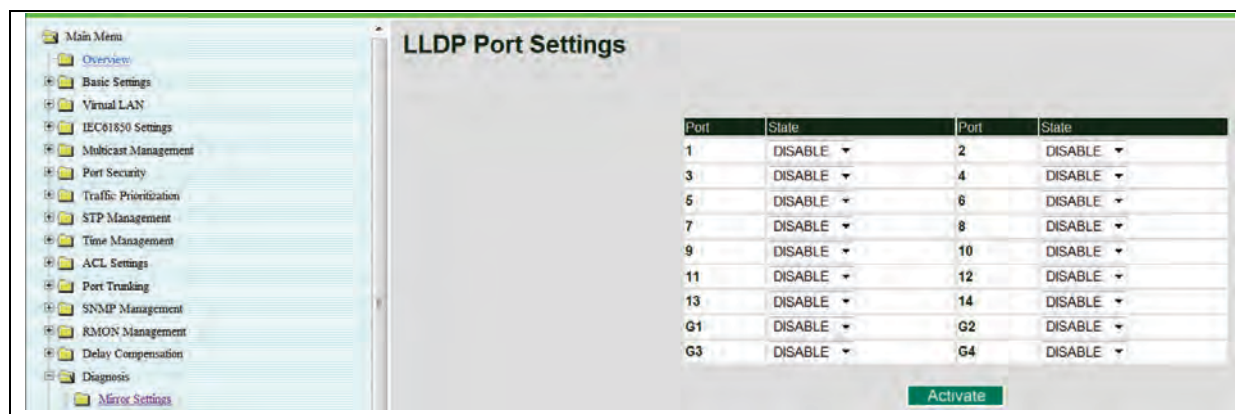


Figure 4.17-5 LLDP Port Settings

- **State**

DISABLE	The LLDP function is disabled
TX_ONLY	Transmission only of LLDP packets
RX_ONLY	Reception only of LLDP packets
TX_RX	Transmission and reception of LLDP packets

4.17.4.3 LLDP Neighbor Information



Figure 4.17-6 LLDP Neighbor Information

- **Port**
Port number of local switch
- **ChassisID**
MAC address of remote device
- **PortID**
Port number of remote device
- **SysName**
Description of remote device
- **ManagementAddress**
Management IP address of remote device

4.17.4.4 LLDP Statistic Information

Use this interface to display the LLDP statistic information.

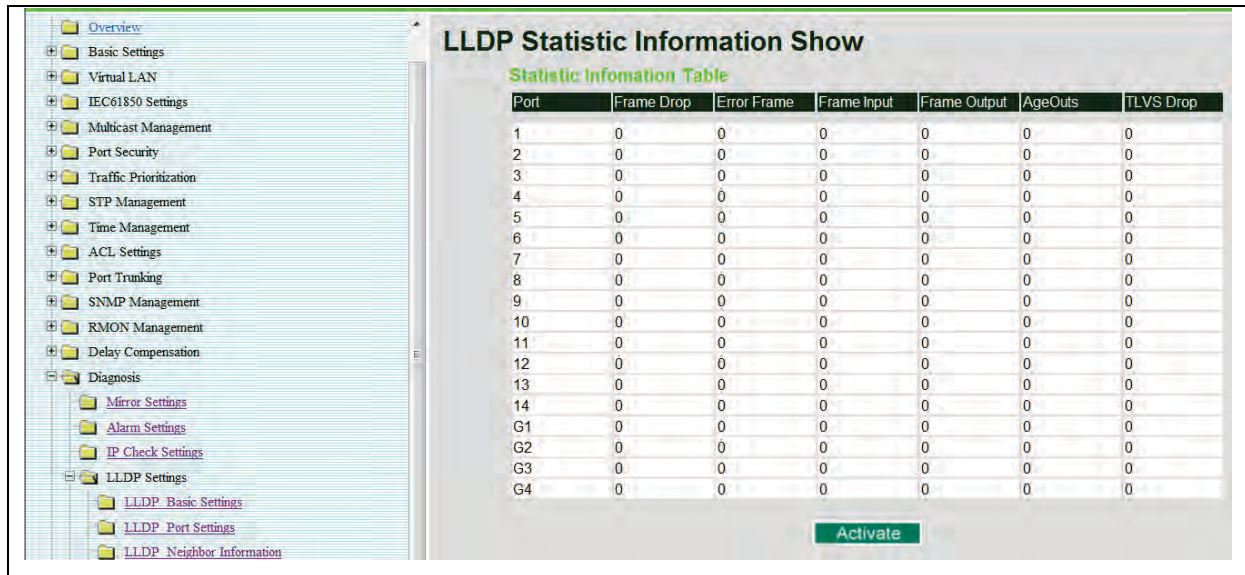


Figure 4.17-7 LLDP Statistic Information

- **Port**

Port number of local switch

- **AgeOuts**

The total number of neighbor messages that timed out

4.17.5 Security Settings

Use this menu to manage the maximum number of connections accessed by various switches

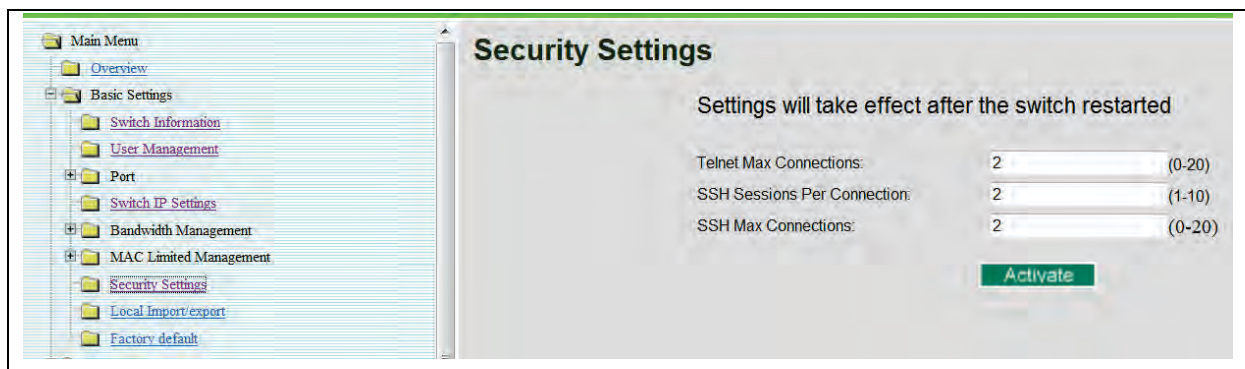


Figure 4.17-8 Security Settings

4.17.6 Statistic Settings

Use this menu to enable/disable the switch statistic function.

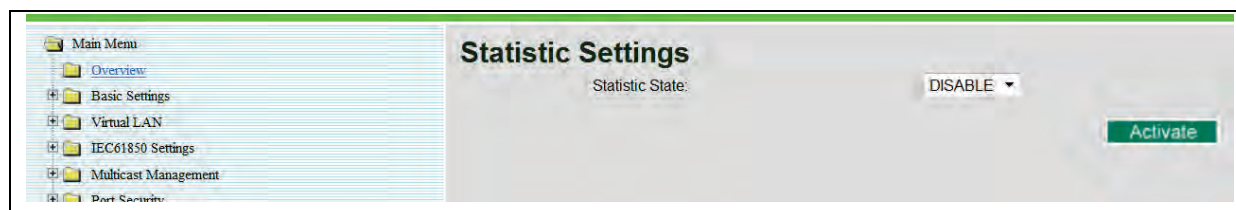


Figure 4.17-9 Statistic Settings

4.18 Others

4.18.1 Restart

Use this menu to reboot the switch. After a reboot, user needs to log in WEB server again.

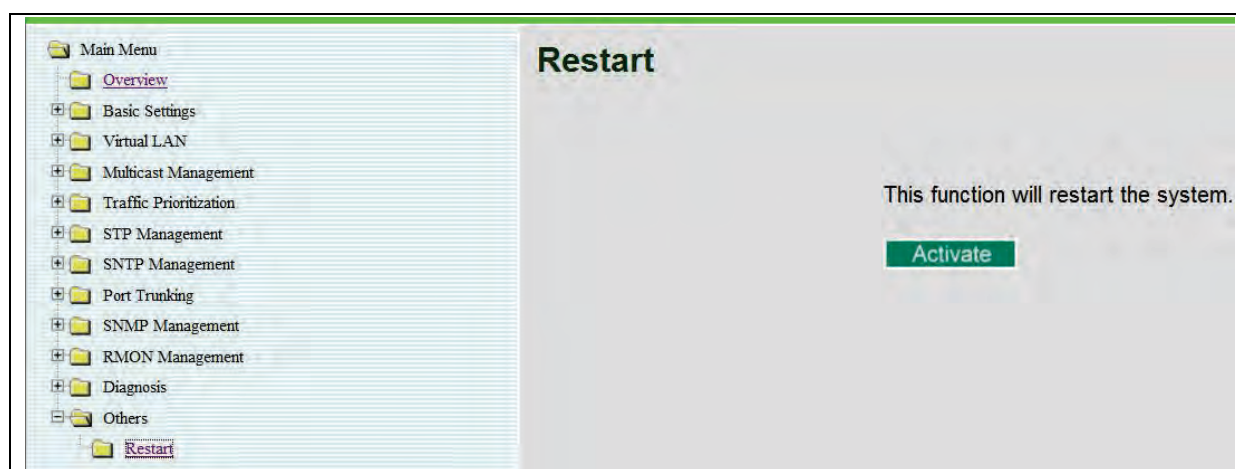


Figure 4.18-1 Restart

5 Installation

Table of Contents

5 Installation	5-a
5.1 Overview.....	5-1
5.2 Safety Instructions	5-1
5.3 Check Shipment	5-2
5.4 Material and Tools Required.....	5-2
5.5 Device Location and Ambient Conditions	5-2
5.6 Mechanical Installation	5-3
5.7 Electrical Installation and Wiring	5-3
5.7.1 Grounding Guidelines	5-3
5.7.2 Cubicle Grounding.....	5-4
5.7.3 Grounding Connection on the Device.....	5-5
5.7.4 Grounding Strips and their Installation.....	5-5
5.7.5 Guidelines of Wiring	5-6
5.7.6 Wiring for Electrical Cables.....	5-6
5.7.7 Wiring for Optical Fiber Cables	5-7

List of Figures

Figure 5.6-1 Dimensions of PCS-9882XD-H2 (unit: mm).....	5-3
Figure 5.7-1 Cubicle grounding system.....	5-5
Figure 5.7-2 Device grounding terminal	5-5
Figure 5.7-3 Grounding strip and termination.....	5-6
Figure 5.7-4 Glancing demo about the wiring for power supply.....	5-7



5.1 Overview

The equipment must be shipped, stored and installed with the greatest care.

Choose the place of installation such that the communication interface and the controls on the front of the device are easily accessible.

Air must circulate freely around the equipment. Observe all the requirements regarding place of installation and ambient conditions given in *Chapter 2* of this instruction manual.

Take care that the external wiring is properly brought into the equipment and terminated correctly and pay special attention to grounding. Strictly observe the corresponding guidelines contained in this section.

5.2 Safety Instructions

Modules and units may only be replaced by correspondingly trained personnel. Always observe the basic precautions to avoid damage due to electrostatic discharge when handling the equipment.

In certain cases, the settings have to be configured according to the demands of the engineering configuration after replacement. It is therefore assumed that the personnel who replace modules and units are familiar with the use of the operator program on the service PC.



WARNING!

ONLY insert or withdraw a module while the device power supply is switched off. To this end, disconnect the power supply cable that connects with the PWR module.

NOTICE!

Industry packs and ribbon cables may **ONLY** be replaced on a workbench for electronic equipment. Electronic components are sensitive to electrostatic discharge when not in the unit's housing.

NOTICE!

Jumper links may **ONLY** be changed on a workbench for electronic equipment. Electronic components are sensitive to electrostatic discharge when not in the unit's housing.

The basic precautions to guard against electrostatic discharge are as follows:

- Should boards have to be removed from this device installed in a grounded cubicle in an HV switchgear installation, please discharge yourself by touching station ground (the cubicle) beforehand.
- Only hold electronic boards at the edges, taking care not to touch the components.

- Only works on the board that has been removed from the cubicle on a workbench designed for electronic equipment and wear a grounded wristband. Do not wear a grounded wristband, however, while inserting or withdrawing units.
- Always store and ship the electronic boards in their original packing. Place electronic parts in electrostatic screened packing materials.

5.3 Check Shipment

Check that the consignment is complete immediately upon receipt. Notify the nearest NR Company or agent, should departures from the delivery note, the shipping papers or the order be found.

Visually inspect all the material when unpacking it. When there is evidence of transport damage, lodge a claim immediately in writing with the last carrier and notify the nearest NR Company or agent.

If the equipment is not going to be installed immediately, store all the parts in their original packing in a clean dry place at a moderate temperature. The humidity at a maximum temperature and the permissible storage temperature range in dry air are listed in *Chapter "Technical Data"*.

5.4 Material and Tools Required

The necessary mounting kits will be provided, including screws, pincers and assembly instructions.

A suitable drill and spanners are required to secure the cubicles to the floor using the plugs provided (if this device is mounted in cubicles).

5.5 Device Location and Ambient Conditions

NOTICE!

Excessively high temperature can appreciably reduce the operating life of this device.

The place of installation should permit easy access especially to front of the device, i.e. to the human machine interface of the equipment.

There should also be free access at the rear of the equipment for additions and replacement of electronic boards.

Since every piece of technical equipment can be damaged or destroyed by inadmissible ambient conditions, such as:

- The location should not be exposed to excessive air pollution (dust, aggressive substances).
- Surge voltages of high amplitude and short rise time, extreme changes of temperature, high

levels of humidity, severe vibration and strong induced magnetic fields should be avoided as far as possible.

- Air must not be allowed to circulate freely around the equipment.

The equipment can in principle be mounted in any attitude, but it is normally mounted vertically (visibility of markings).

5.6 Mechanical Installation

NOTICE!

It is necessary to leave enough space top and bottom of the cutout in the cubicle for heat emission of this device.

This device is made of a single layer 1U height chassis. The following figures show the dimensions and cut-out size in the cubicle of this device for reference in mounting.

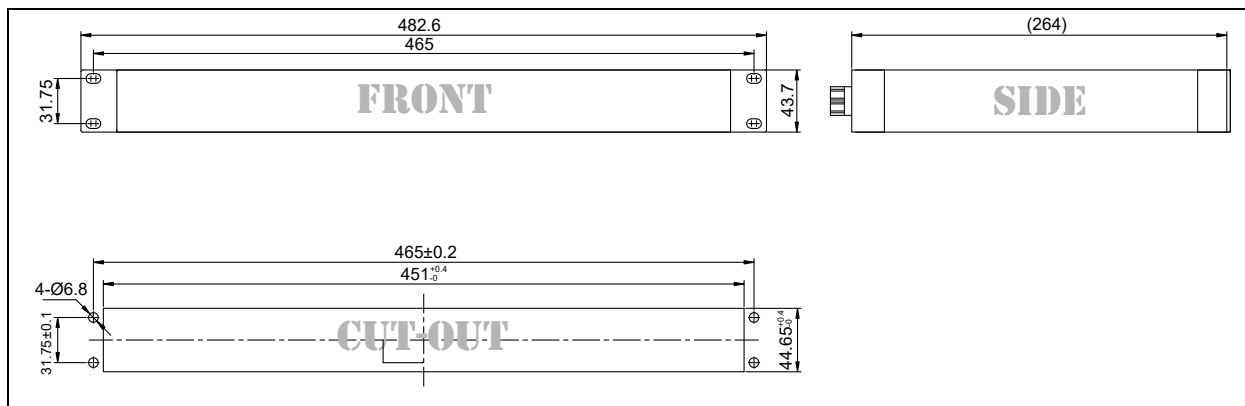


Figure 5.6-1 Dimensions of PCS-9882XD-H2 (unit: mm)

In the case of equipment supplied in cubicles, place the cubicles on the foundations that have been prepared. Take care while doing so not to jam or otherwise damage any of the cables that have already been installed. Secure the cubicles to the foundations.

5.7 Electrical Installation and Wiring

5.7.1 Grounding Guidelines

NOTICE!

All these precautions can only be effective if the station ground is of good quality.

Switching operations in HV installations generate transient over voltages on control signal cables. There is also a background of electromagnetic RF fields in electrical installations that can induce spurious currents in the devices themselves or the leads connected to them.

All these influences can influence the operation of electronic apparatus.

On the other hand, electronic apparatus can transmit interference that can disrupt the operation of other apparatus.

In order to minimize these influences as far as possible, certain standards have to be observed with respect to grounding, wiring and screening.

5.7.2 Cubicle Grounding

The cubicle must be designed and fitted out such that the impedance for RF interference of the ground path from the electronic device to the cubicle ground terminal is as low as possible.

Metal accessories such as side plates, blanking plates etc., must be effectively connected surface-to-surface to the grounded frame to ensure a low-impedance path to ground for RF interference. The contact surfaces must not only conduct well, they must also be non-corroding.

NOTICE!

If the above conditions are not fulfilled, there is a possibility of the cubicle or parts of it forming a resonant circuit at certain frequencies that would amplify the transmission of interference by the devices installed and reduce their immunity to induced interference.

Movable parts of the cubicle such as doors (front and back) or hinged equipment frames must be effectively grounded to the frame by three braided copper strips.

The metal parts of the cubicle housing and the ground rail are interconnected electrically conducting and corrosion proof. The contact surfaces shall be as large as possible.

NOTICE!

For metallic connection, please observe the voltage difference of both materials according to the electrochemical code.

The cubicle ground rail must be effectively connected to the station ground rail by a grounding strip (braided copper).

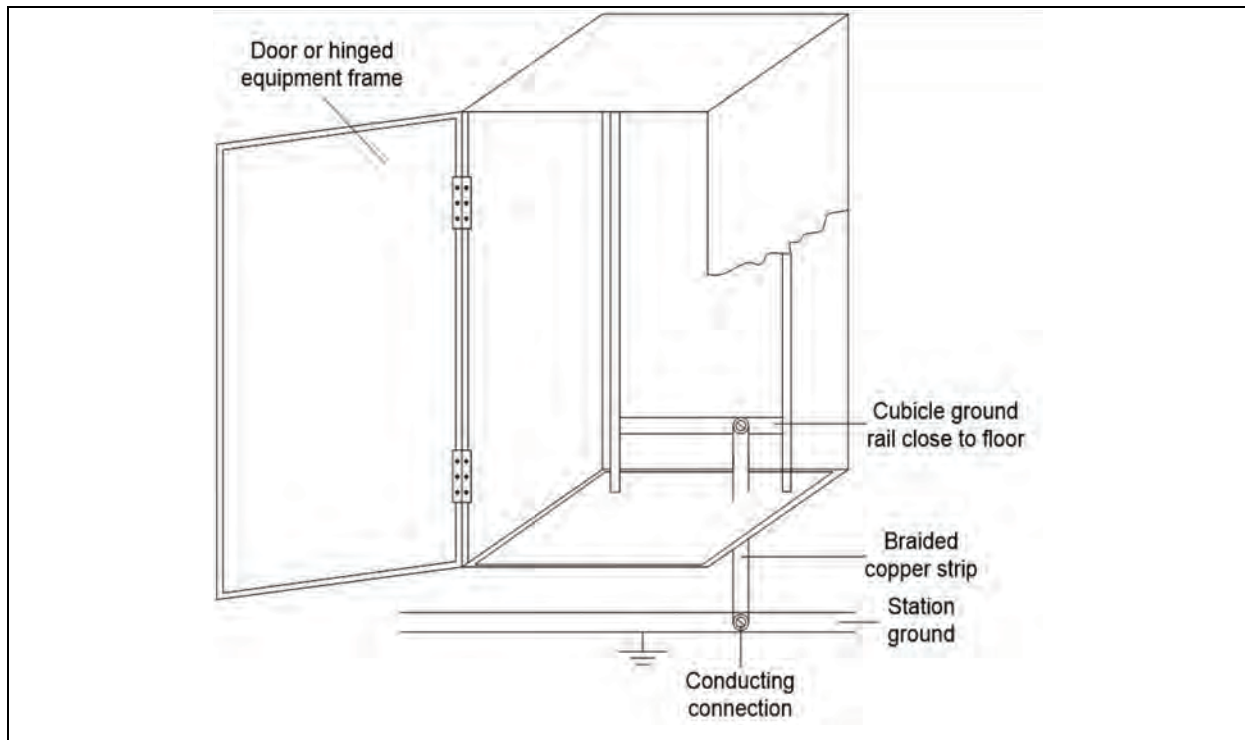


Figure 5.7-1 Cubicle grounding system

5.7.3 Grounding Connection on the Device

There is a grounding terminal on the rear panel, and the grounding braided copper strip can be connected with it. Take care that the grounding strip is always as short as possible. The main thing is that the device is only grounded at one point. Grounding loops from unit to unit are not allowed.

There are some grounding terminals on some connectors of this device, and the sign is “GND”. All the grounding terminals are connected in the cabinet of this device. Therefore, the grounding terminal on the rear panel is the only grounding terminal of this device.

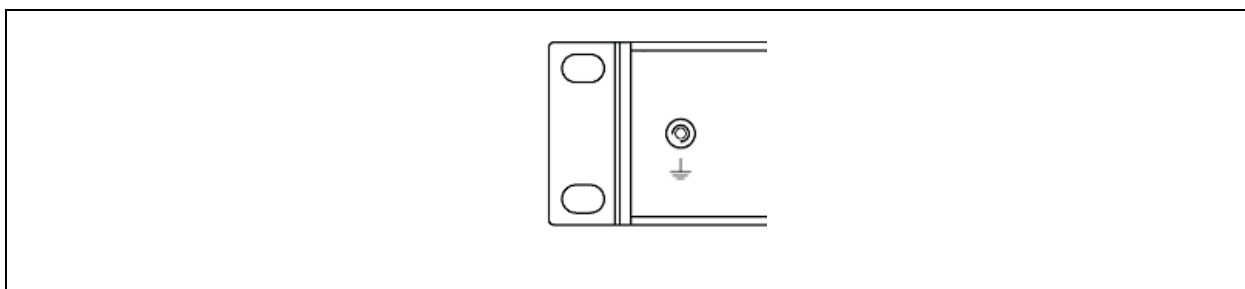


Figure 5.7-2 Device grounding terminal

5.7.4 Grounding Strips and their Installation

High frequency currents are produced by interference in the ground connections and because of skin effect at these frequencies, only the surface region of the grounding strips is of consequence.

The grounding strips must therefore be of (preferably tinned) braided copper and not round copper conductors, as the cross-section of round copper would have to be too large.

Proper terminations must be fitted to both ends (press/pinch fit and tinned) with a hole for bolting them firmly to the items to be connected.

The surfaces to which the grounding strips are bolted must be electrically conducting and non-corroding.

The following figure shows the ground strip and termination.

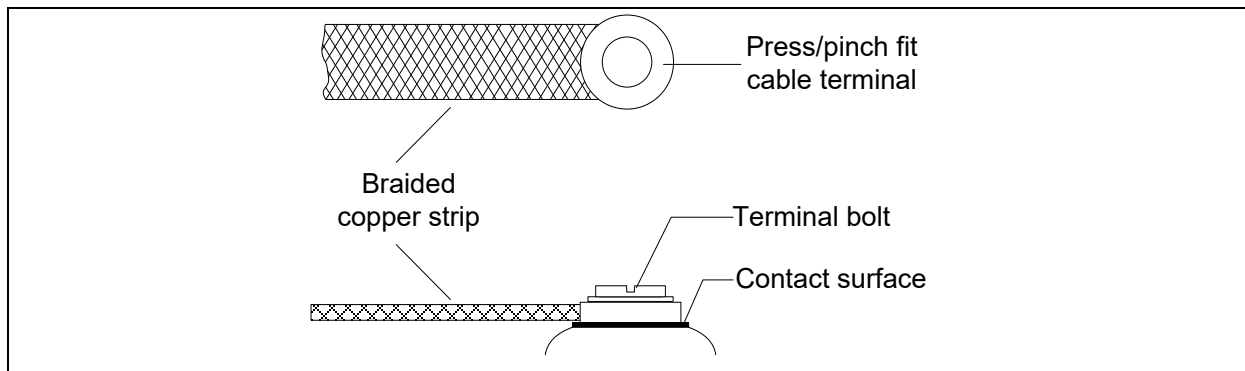


Figure 5.7-3 Grounding strip and termination

5.7.5 Guidelines of Wiring

There are several types of cables that are used for connection of this device. Recommendation of cable is:

- Power supply, binary input & output: stranded conductor, $1.0\text{mm}^2 \sim 2.5\text{mm}^2$ lead
- Earthing connection: braided copper cable, $2.5\text{mm}^2 \sim 6.0\text{mm}^2$ lead
- Serial communication: 4-core shielded cable
- Electrical Ethernet communication: 4-pair twisted shielded cable (category 5E)

5.7.6 Wiring for Electrical Cables

A female connector is used for connecting the wires with it, and then a female connector plugs into a corresponding male connector that is in the front of one board. See *Chapter "Hardware"* for further details about the pin defines of these connectors.

The following figure shows the glancing demo about the wiring for the electrical cables.

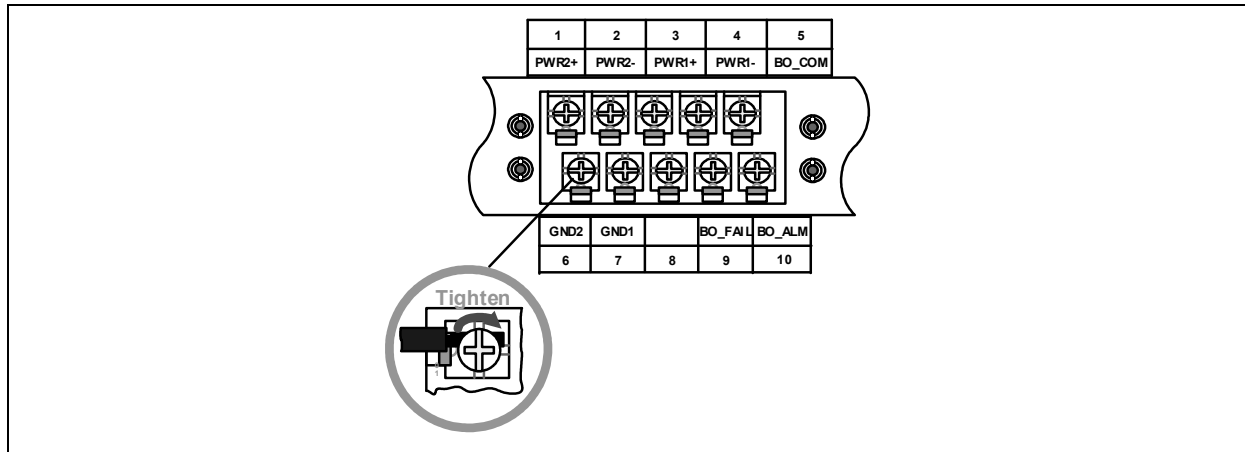


Figure 5.7-4 Glancing demo about the wiring for power supply

5.7.7 Wiring for Optical Fiber Cables

Pay attention when laying an optical fiber cable.

NOTICE!

Do not damage the protective caps on the end.

NOTICE!

Strictly observe the minimum permissible radius when bending or twisting the cable. The bending radius influences the attenuation of an optical fiber cable.

NOTICE!

The characteristics of an optical fiber cable are influenced by the ambient temperature. The temperature for laying or rewinding an optical fiber cable should be considered. Make sure the cable is not exposed to a temperature outside the permissible range during the continuing 12 hours.

NOTICE!

It is recommended that optical fiber cables be laid in plastic cable ducts.





6 Commissioning

Table of Contents

6 Commissioning	6-a
6.1 Overview.....	6-1
6.2 Safety Instructions	6-1
6.3 Commission Tools.....	6-1
6.4 Configuration Familiarization	6-2
6.5 Product Checks	6-2
6.5.1 With De-energized Device	6-2
6.5.2 With Energized Device	6-3
6.5.3 Data Exchange.....	6-4
6.5.4 Final Check.....	6-4



6.1 Overview

This device is numerical in the design, implementing all functions in software. It employs a high degree self-checking so in the unlikely event of a failure, there will be an alarm.

Before carrying out any work on the equipment, the user should be familiar with the contents of the safety and technical data sections and the ratings on the equipment's rating label.

6.2 Safety Instructions



WARNING!

ONLY qualified personnel should work on or near this device. This personnel **MUST** be familiar with all safety regulations and service procedures described in this manual. During operating of electrical device, certain part of the device is under high voltage. Severe personal injury and significant device damage could result from improper behavior.

Particular attention must be drawn to the following:

- The earthing screw of the device must be connected solidly to the protective earth conductor before any other electrical connection is made.
- Hazardous voltages can be present on all circuits and components connected to the supply voltage or to the measuring and test quantities.
- Hazardous voltages can be present in the device even after disconnection of the supply voltage (storage capacitors!)
- The limit values stated in the *Chapter "Technical Data"* must not be exceeded at all, not even during testing and commissioning.

6.3 Commission Tools

NOTICE!

Modern test set may contain many of the above features in one unit.

- PC or IED with electrical Ethernet port
- PC or IED with optical Ethernet port
- Professional network performance analyzer

6.4 Configuration Familiarization

When commissioning this device for the first time, sufficient time should be allowed to become familiar with the method by which the configuration is applied via WEB browser. A detailed description of the WEB configuration of this device is contained in the chapter "*Configurable Functions*".

6.5 Product Checks

These product checks cover all aspects of the device that should be checked to ensure that it has not been physically damaged prior to commissioning, is functioning correctly and all input quantity measurements are within the stated tolerances.

6.5.1 With De-energized Device

6.5.1.1 Visual Inspection

After unpacking the product, check for any damage to the device case. If there is any damage, the internal module might also have been affected, contact the vendor. The following items listed are necessary.

- Device panel

Carefully examine the device panel, device inside and other parts inside to see that no physical damage has occurred since installation.

- Panel wiring

Check the conducting wire that is used in the panel to assure that their cross section meeting the requirement.

Carefully examine the wiring to see that they are no connection failure exists.

- Device plug-in modules

Check each plug-in module of the equipment on the panel to make sure that they are well installed into the equipment without any screw loosened.

- Earthing cable

Check whether the earthing cable from the panel terminal block is safely screwed to the panel steel sheet.

6.5.1.2 Insulation Test (If required)

Insulation resistance tests are only necessary during commissioning if it is required for them to be done and they have not been performed during installation.

Isolate all wiring from the earth and test the isolation with an electronic or brushless insulation tester at a DC voltage not exceeding 500V, The circuits need to be tested should include:

- Power supply
- Output contacts
- Communication ports

The insulation resistance should be greater than 100MΩ at 500V.

6.5.1.3 External Wiring

Check that the external wiring is correct to the relevant device diagram and scheme diagram.

Check the wiring against the schematic diagram for the installation to ensure compliance with the customer's normal practice.

6.5.1.4 Power Supply

The device only can be operated under the auxiliary power supply depending on the device's nominal power supply rating.

The incoming voltage must be within the operating range specified in *Chapter "Technical Data"*, before energizing the device, measure the auxiliary supply to ensure it within the operating range.

Other requirements to the auxiliary power supply are specified in *Chapter "Technical Data"*. See this section for further details about the parameters of the power supply.

6.5.2 With Energized Device

The following groups of checks verify that the device hardware and software is functioning correctly and should be carried out with the auxiliary supply applied to the device.

6.5.2.1 LED Indicator P1

Energize the first power supply module 1, after the starting up process, the LED indicator "**P1**" will be lit on. If the power supply module 1 works normally, this LED is lit on as green. In case of power loss or module fault, this LED will be lit off.

6.5.2.2 LED Indicator P2

Energize the first power supply module 2, after the starting up process, the LED indicator "**P2**" will be lit on. If the power supply module 2 works normally, this LED is lit on as green. In case of power loss or module fault, this LED will be lit off.

6.5.2.3 LED Indicator for Megabit Interface on the Front Panel

If a 100Mbps Ethernet port is used to connect an external 100Mbps port, the corresponding "**10/100M**" and "**LNK/ACT**" LEDs will be lit on as green. If the port is transmitting or receiving data, the corresponding "**LNK/ACT**" LED flashes.

If a 100Mbps Ethernet port is used to connect an external 10Mbps port, the corresponding "**10/100M**" LED will be lit off, while the "**LNK/ACT**" LED is lit on as green. If the port is transmitting or receiving data, the corresponding "**LNK/ACT**" LED flashes.

If no equipment is connected with the port, the corresponding "**10/100M**" and "**LNK/ACT**"

LEDs are lit off.

Check each megabit Ethernet port LED Indicator on the front panel in this way.

6.5.2.4 LED Indicator for Gigabit Interfaces on the Front Panel

If a 1000Mbps Ethernet port is used to connect an external 1000Mbps port, the corresponding **"1G"** and **"LNK/ACT"** LEDs will be lit on as green. If the port is transmitting or receiving data, the corresponding **"LNK/ACT"** LED flashes.

If a 1000Mbps Ethernet port is used to connect an external 10/100Mbps port, the corresponding **"1G"** LED will be lit off, while the **"LNK/ACT"** LED is lit on as green. If the port is transmitting or receiving data, the corresponding **"LNK/ACT"** LED flashes.

If no equipment is connected with the port, the corresponding **"1G"** and **"LNK/ACT"** LEDs are lit off.

Check each gigabit Ethernet port LED Indicator on the front panel in this way.

6.5.2.5 LED Indicators on the Rear Panel

As the definition of the LED indicators on the rear panel is the same with that of the **"LNK/ACT"** LED indicators on the front panel, the test method is also the same.

6.5.3 Data Exchange

A network performance analyzer should be used with its own rules to test the data exchange performance of this device.

6.5.4 Final Check

After the above tests are completed, remove all test or temporary shorting leads, etc. If it has been necessary to disconnect any of the external wiring from the device in order to perform the wiring verification tests, it should be ensured that all connections are replaced in accordance with the relevant external connection or scheme diagram.

Ensure that the device has been restored to service.



7 Maintenance

Table of Contents

7 Maintenance	7-a
7.1 Introduction.....	7-1
7.2 Appearance Check	7-1
7.3 Failure Tracing and Repair.....	7-1
7.4 Cleaning	7-1
7.5 Storage	7-1



7.1 Introduction

This device is designed to require no special maintenance. Since the it is almost completely self-monitored, any hardware or software defect will be automatically detected. The self-monitoring ensures the high availability of the device and generally allows for a corrective rather than preventive maintenance strategy. Therefore, maintenance checks in short intervals are not required.

Operation of the device is automatically blocked when a hardware failure is detected.

7.2 Appearance Check

It is recommended that products supplied by NR receive periodic monitoring after installation. In view of the critical nature of the device, it is desirable to confirm that they are operating correctly at regular intervals.

7.3 Failure Tracing and Repair

- If the "P1" or "P2" LED indicator is lit off, please check the corresponding power supply input.
- If the Ethernet port status LED indicator is incorrect, please check the following items:
 - Whether the equipment connected operates normally.
 - Whether the cable is intact and is fixed tightly.
 - Whether the specific Ethernet port is failed

7.4 Cleaning

Before cleaning the device, ensure that all AC/DC supplies, current transformer connections are isolated to prevent any chance of an electric shock whilst cleaning. Use a smooth cloth to clean the front panel. Do not use abrasive material or detergent chemicals.

7.5 Storage

The spare device or module should be stored in a dry and clean room. Based on IEC standard 60255-1 the storage temperature should be from -40°C to +85°C, but the temperature of from 0°C to +40°C is recommended for long-term storage.





8 Decommissioning and Disposal

Table of Contents

8 Decommissioning and Disposal	8-a
8.1 Decommissioning.....	8-1
8.2 Disposal.....	8-1



8.1 Decommissioning



DANGER!

Switch **OFF** the circuit breaker for primary CTs and VTs **BEFORE** disconnecting the cables of AI module.



WARNING!

Switch **OFF** the external miniature circuit breaker of device power supply **BEFORE** disconnecting the power supply cable connected to the PWR module.



WARNING!

KEEP an adequate safety distance to live parts of the power substation.

1. Switching off

To switch off this device, switch off the external miniature circuit breaker of the power supply.

2. Disconnecting Cables

Disconnect the cables in accordance with the rules and recommendations made by relational department.

3. Dismantling

The device rack may now be removed from the system cubicle, after which the cubicles may also be removed.

8.2 Disposal

NOTICE!

Strictly observe all local and national laws and regulations when disposing the device.



9 Glossary

Abbreviation	Description
A	
ACL	An Access Control List is a list of permissions attached to an object.
C	
CLI	Command-Line Interface is a means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines)
CMMI	Capability Maturity Model Integration is a process improvement training and appraisal program and service administered and marketed by Carnegie Mellon University (CMU) and required by many DoD and U.S. Government contracts, especially in software development.
CoS	Class of Service is a 3-bit field called the Priority Code Point (PCP) within an Ethernet frame header when using VLAN tagged frames as defined by IEEE 802.1Q. It specifies a priority value of between 0 and 7 inclusive that can be used by QoS disciplines to differentiate traffic.
D	
DCS	Distributed Control Systems
DoS	Denial-of-Service attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.
E	
ELV	Extra-Low Voltage
F	
FOT	Fiber Optic Transceiver
G	
GARP	Generic Attribute Registration Protocol is a generic registration framework defined by the IEEE 802.1ak amendment to the IEEE 802.1Q standard. It allows bridges, switches or other similar devices to be able to register and de-register attribute values, such as VLAN identifiers and multicast group membership across a large LAN.
GMRP	GARP MAC Registration Protocol is a data link layer (layer 2) protocol to register group MAC addresses (i.e. multicast) on multiple switches. It is an GARP application, originally defined in IEEE 802.1ak-2007 and subsequently included in 802.1Q.
GVRP	GARP VLAN Registration Protocol is a standards-based Layer 2 network protocol, for automatic configuration of VLAN information on switches. It was defined in the 802.1ak amendment to 802.1Q-2005.
GOOSE	Generic Object Oriented Substation Events is a controlled model mechanism in which any

Abbreviation	Description
	format of data (status, value) is grouped into a data set and transmitted within a time period of 4 millisecond.
H	
HMI	Human Machine Interface
I	
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IGMP	The Internet Group Management Protocol is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.
IGMP snooping	This is the process of listening to Internet Group Management Protocol network traffic.
IRIG	Inter-Range Instrumentation Group time code
ISO	International Organization for Standardization
K	
KEMA	Established in 1927, Keuring Van Elektrotechnische Materialen (KEMA) is an independent knowledge leader and a global provider of high-quality services to the energy value chain, including business & technical consultancy, operational support, measurements & inspection, and testing & certification. KEMA provides impartial advice and support to producers, suppliers and end users of energy, as well as to governmental bodies and manufacturers of energy related equipment.
L	
LC	Lucent Connector connectors are sometimes called "Little Connectors". LC connectors have replaced SC connectors in corporate networking environments due to their smaller size; they are often found on small form-factor pluggable transceivers.
LED	Light-Emitting Diode
LLDP	Link Layer Discovery Protocol is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet.
M	
MAC	Media Access Control address is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the Media Access Control protocol sub-layer of the OSI reference model.
MDI/MDI-X	Medium-Dependent Interface & Medium-Dependent Interface Crossover
MMS	Manufacturing Message Specification
MRP	Multiple Registration Protocol is a generic registration framework defined by the IEEE 802.1ak

Abbreviation	Description
	amendment to the IEEE 802.1Q standard. MRP allows bridges, switches or other similar devices to be able to register and de-register attribute values, such as VLAN identifiers and multicast group membership across a large LAN.
MSTP	Multiple Spanning Tree Protocol is originally defined in IEEE 802.1s and later merged into IEEE 802.1Q-2005. It defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs).
N	
NCS	Networked Control System
NTP	Network Time Protocol is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
O	
OHSAS	Occupational Health and Safety Assessment Series
P	
PCB	Printed Circuit Board mechanically supports and electrically connects electronic components using conductive tracks, pads and other features etched from copper sheets laminated onto a non-conductive substrate.
PTP	Precision Time Protocol is a protocol used to synchronize clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems.
Q	
QinQ	IEEE 802.1ad is an Ethernet networking standard informally known as QinQ and is an amendment to IEEE standard IEEE 802.1Q-1998.
QoS	The Quality Of Service (QoS) refers to several related aspects of telephony and computer networks that allow the transport of traffic with special requirements.
R	
RADIUS	Remote Authentication Dial-In User Service is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.
RAM	Random-Access Memory
RMON	Remote network MONitoring management information base was developed by the IETF to support monitoring and protocol analysis of LANs. It is an industry standard specification that provides much of the functionality offered by proprietary network analyzers.
RSTP	Rapid Spanning Tree Protocol RSTP adds new bridge port roles in order to speed convergence following a link failure.
S	
SAS	Substation Automation System
SCADA	Supervisory Control And Data Acquisition

Abbreviation	Description
SFP socket	Small Form-factor Pluggable sockets are found in Ethernet switches and network interface cards. Because of their ability to provide a connection to different types of optical fiber, SFP provides such equipment with enhanced flexibility.
SFP transceiver	The Small Form-factor Pluggable (SFP) or Mini-GBIC is a compact, hot-pluggable transceiver used for both telecommunication and data communications applications. It interfaces a network device mother board (for a switch, router, media converter or similar device) to a fiber optic or copper networking cable. It is a popular industry format supported by many network component vendors.[citation needed] SFP transceivers are designed to support SONET, Gigabit Ethernet, Fiber Channel, and other communications standards.
SNMP	Simple Network Management Protocol is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.
SNTP	Simple Network Time Protocol is a less complex implementation of NTP, using the same protocol but without requiring the storage of state over extended periods of time.
SSL	Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. TLS and SSL encrypt the segments of network connections above the Transport Layer, using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.
SSH	Secure Shell is a network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network: a server and a client (running SSH server and SSH client programs, respectively). The protocol specification distinguishes two major versions that are referred to as SSH-1 and SSH-2.
STP	Spanning Tree Protocol is a network protocol that builds a logical loop-free topology for Ethernet networks
SV	Sampled Values
SYN flood	A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.
T	
Telnet	Telnet is an application layer protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.
TCP/IP	Transport Control Protocol/Internet Protocol
U	
UTC	Coordinated Universal Time is the primary time standard by which the world regulates clocks and time.
V	
VLAN	Virtual Local Area Network is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their



Abbreviation	Description
	physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if they are not located on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections.





10 Revision History

Manual Version	Firmware Version	Release Date	Description of change
R1.00	R6.03	3 July 2019	Initial draft

