IEM7110-3G

Embedded Industrial Ethernet Switch Module

User's Manual

Version 2.0.0, Feb. 2017

www.3onedata.com

Announcement and declaration

Before using this manual, please read the following license agreement. The products introducing in this manual can be used only under this case that agree to the following license agreement below

Copyright

This document all copyright belongs to 3onedata co., LTD., and reserve the right to change. Without written authorization, any entities and individuals cannot extract, copy and spread this document in part or in whole.

Trademark

3One data® and 3onedata® are the registered trademark that belong to 3onedata co., LTD.. And other trademark or registered trademark, involved in this document, are belonged to their respective owners.

Announcement

This manual will be updated no scheduled based on the product version upgrade or other reasons. Unless otherwise agreed, this manual is used only as the product using guide, all statement, information and suggestion of this manual are not any express or implied guarantees.

Revision History

Version	Date	Description
1.0.0	2016-04	Create Document
2.0.0	2017-02	Added features

Contents

Chapter 1 Overview 1
1.1 Introduction 1
1.2 Features 1
Chapter 2 Hardware Description 2
2.1 Pin DESCRIPTION 2
2.1.1 Iem7110-3g Pin Map 2
2.1.2 Iem7110-3g Pin Definition 3
2.1.3 Iem7110-3g Pin Description 4
2.2 ETHERNET INTERFACE DESCRIPTION 8
2.2.1 100base-Tx/Fx Port Description 8
2.2.2 1000base-Tx/Fx Description Of Port8 10
2.2.3 Port9 1000base-Tx/Fx Interface Description 12
2.2.4 Port8, Port9 Power Reference Circuit 15
2.3 POWER INTERFACE 15
2.4 UART INTERFACE 15
2.5 RESET 16
2.6 PORT ALARM 17
2.7 Reset TO DEFAULTS 17
Chapter 3 Outline Drawing 18
Chapter 4 Features 19
Chapter 5 Web Management 21
5.1 Network SETTING 21
5.2 Startup AND LOGIN 22
5.3 Configuration DESCRIPTION 22
5.4 Port CONFIGURATION 25
5.4.1 Port Settings 25
5.4.2 Bandwidth Management 27
5.5 L2 FEATURES 28
5.5.1 Vlan 28
5.5.2 Dynamic Multicast 32
5.5.3 Static Multicast Fwd 33
5.6 QOS 34
5.6.1 Qos Classification 34
5.6.2 Cos 34
5.6.3 Dscp 35
5.7 Redundancy 36
5.7.1 Rapid Ring 36
5.7.2 Rstp 40
5.7.3 Port Trunking 42
5.8 Lldp 43
5.8.1 Parameter Configuration 43
5.8.2 Neighbor Information 44

5.9 Access CONTROL 44
5.9.1 User Password 44
5.10 Remote MONITORING 45
5.10.1 Snmp 45
5.10.2 Relay Alarm 46
5.11 Traffic STATISTICS 47
5.11.1 Rx Frame Statistics 47
5.11.2 Tx Frame Statistics 48
5.12 Diagnosis 49
5.12.1 Mirror 49
5.13basic SETTINGS 50
5.13.1 Sntp 50
5.13.2 Network & Reboot 51
5.13.3 System Identification 52
5.13.4 System File Upgrade 53
5.13.5 Logout 54
Chapter 6 Cli Command 55
6.1 Login ETHERNET SWITCH 55
6.2 Agreement 58
6.3 Command LINES PORT 59
6.4 Device INFORMATION 62
6.5 Port CONFIGURATION 63
6.6 Bandwidth MANAGEMENT 66
6.7 Vlan 67
6.8 Qos 70
6.9 Ring CONFIGURATION 72
6.10 Port TRUNKING 75
6.11 Alarm CONFIGURATION 76
6.12 Port MIRRORING 77
6.13 Static MULTICAST CONFIGURATION 78
6.14 System MANAGEMENT 79
6.15 Frame STATISTICS 81
6.16 Lldp 82
6.17 SNMP 82
6.18 Igmp 83
6.19 TIME 84

Chapter 1 Overview

1.1 Introduction

Welcome use the IEM7110-3G series from 3onedata, which is managed Gigabit industrial Ethernet switch embedded modules that designed specifically for industrial applications to connect Ethernet devices. IEM7110-3G supports 10 ports (7-FE + 3-GE). 7-FE ports can be optionally configured as 10 / 100BASE-T / TX electrical or 100BASE-FX fiber ports, 3-GE port can be optionally configured as 1000BASE-X or SGMII mode optical ports (to support 10/100 / 1000BASE- T electrical interface). IEM7110-3G support plug-and-play Ring redundant ring protocol (recovery time <20ms, self-developed patented technology). IEM7110-3G support static IGMP multicast filtering, port-based VLAN, IEEE802.1Q VLAN, RSTP, LLDP, SNMP, IGMP Snooping, port priority, port Trunking, port mirroring, port settings, etc.

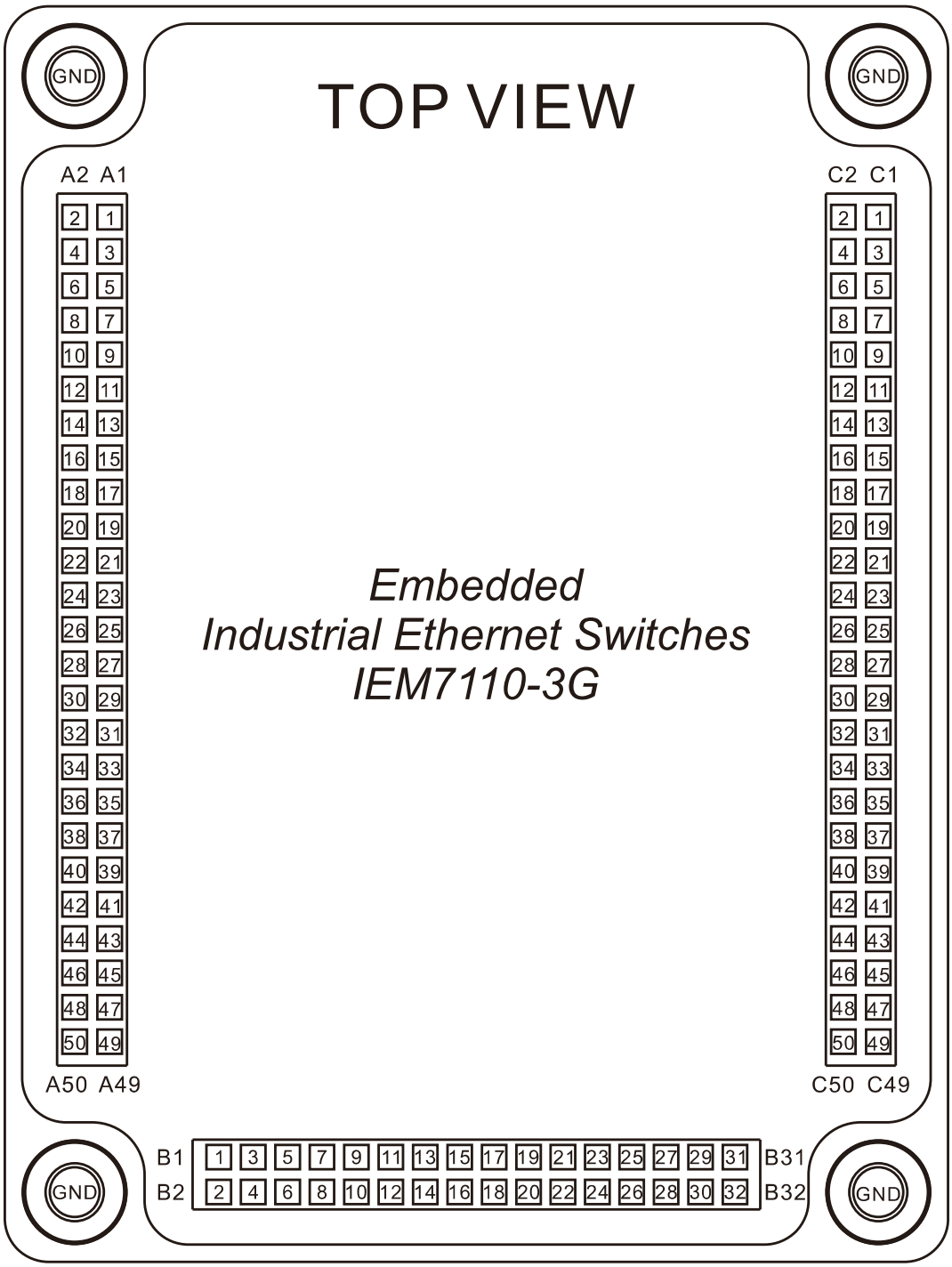
1.2 Features

- Support IEEE802.3, IEEE802.3u, IEEE802.3x, IEEE802.3ab/z, IEEE802.1Q, IEEE802.1p, IEEE802.1D/W, IEEE802.3ad standards
- Support 7 port Fast Ethernet and 3 port Gigabit Ethernet that copper ports and optical fiber port can be optional.
- Support SW-Ring™ ring network patent technology (Fault recovery time<20ms)
- Support RSTP, way exchange time<1s
- Support static multicast, IGMP Snooping and LLDP
- Support Port based VLAN and IEEE802.1Q VLAN
- Support QOS absolutely and opposite priority
- Support WEB, SNMP and Telnet configuration
- Support port Trunking, port mirroring and port frame statistics
- Support 2 channel alarm signal input and output
- Support -40~85℃ working temperature

Chapter 2 Hardware Description

2.1 Pin Description

2.1.1 IEM7110-3G Pin Map



2.1.2 IEM7110-3G Pin Definition

Pin Num.	Name	Pin Num,	Name
A1	GND	A2	VCT25
A3	nRST_IN	A4	FXSD2
A5	FXSD1	A6	FXSD3
A7	GND	A8	GND
A9	GND	A10	GND
A11	TX1-	A12	TX1+
A13	RX1-	A14	RX1+
A15	RX2+	A16	RX2-
A17	TX2+	A18	TX2-
A19	GND	A20	GND
A21	TX3-	A22	TX3+
A23	RX3-	A24	RX3+
A25	RX4+	A26	RX4-
A27	TX4+	A28	TX4-
A29	GND	A30	GND
A31	TX5-	A32	TX5+
A33	RX5-	A34	RX5+
A35	GND	A36	GND
A37	RX6-	A38	RX6+
A39	TX6-	A40	TX6+
A41	TX7+	A42	TX7-
A43	RX7+	A44	RX7-
A45	GND	A46	GND
A47	FXSD4	A48	FXSD5
A49	FXSD6	A50	FXSD7
C1	GND	C2	GND
C3	GND	C4	VIN_3V3
C5	VIN_3V3	C6	VIN_3V3
C7	P9_MODE0	C8	P9_MODE1
C9	P10_MODE0	C10	P10_MODE1
C11	nRST_PHY9	C12	nRST_PHY8
C13	RUN_LED	C14	ISP_EN
C15	ALARMOUT	C16	nRST_PHY10
C17	RELOAD	C18	PROGRAM
C19	PWR2ALARM	C20	RESERVE
C21	PWR1ALARM	C22	NC
C23	GND	C24	GND
C25	NC	C26	NC
C27	NC	C28	NC
C29	U0Tx	C30	U0Rx
C31	LINK7	C32	SPEED7
C33	LINK6	C34	SPEED6
C35	LINK5	C36	SPEED5
C37	LINK4	C38	SPEED4
C39	LINK3	C40	SPEED3
C41	LINK2	C42	SPEED2
C43	LINK1	C44	SPEED1
C45	NC	C46	LINK9

C47	LINK8	C48	LINK10
C49	GND	C50	WDI
B1	GND	B2	GND
B3	RX8-	B4	RX8+
B5	TX8-	B6	TX8+
B7	GND	B8	GND
B9	RX9+	B10	RX9-
B11	TX9+	B12	TX9-
B13	GND	B14	GND
B15	RX10+	B16	RX10-
B17	TX10+	B18	TX10-
B19	GND	B20	GND
B21	FXSD9	B22	FXSD8
B23	CONFP1	B24	FXSD10
B25	CONFP3	B26	CONFP2
B27	CONFP5	B28	CONFP4
B29	CONFP7	B30	CONFP6
B31	MDC_PHY	B32	MDIO_PHY

2.1.3 IEM7110-3G Pin Description

Name	Pin Num.	Type	Function
RX1+	A14	Typical input	Fast Ethernet interface: signal receiver positive. 1. When the port is configured as 100Base-TX mode, RXP [1:7] is directly connected with the receiving network transformer. 2. When the port is configured as 100Base-FX mode, the pin RXP [1:7] directly with the optical fiber module is connected with the output terminal of the positive. 3. All unused pin should be connected to the ground.
RX2+	A15		
RX3+	A24		
RX4+	A25		
RX5+	A34		
RX6+	A38		
RX7+	A43		
RX1-	A13	Typical input	Fast Ethernet interface: signal receiver negative. 1. When the port is configured as 100Base-TX mode, RXN [1:7] is directly connected with the receiving network transformer. 2. When the port is configured as 100Base-FX mode, the pin RXN [1:7] directly with the optical fiber module is connected with the output terminal of the negative. 3. All unused pin should be connected to the ground.
RX2-	A16		
RX3-	A23		
RX4-	A26		
RX5-	A33		
RX6-	A37		
RX7-	A44		
TX1+	A12	Typical output	Fast Ethernet interface: signal transmitter positive 1. When the port is configured as 100Base-TX mode, TXN [1:7] is directly connected with the transmission network transformer. 2. When the port is configured as 100Base-FX mode, the pin TXP [1:7] directly with the optical fiber module is connected with the input terminal of the positive. 3. All unused pin should be connected to the ground.
TX2+	A17		
TX3+	A22		
TX4+	A27		
TX5+	A32		
TX6+	A40		
TX7+	A41		

TX1-	A11	Typical output	Fast Ethernet interface: signal transmitter negative 1. When the port is configured as 100Base-TX mode, TXN [1:7] is directly connected with the transmission network transformer. 2. When the port is configured as 100Base-FX mode, the pin TXN [1:7] directly with the optical fiber module is connected with the input terminal of the negative. 3. All unused pin should be connected to the ground for saving power.
TX2-	A18		
TX3-	A21		
TX4-	A28		
TX5-	A31		
TX6-	A39		
TX7-	A42		
FXSD1	A5	Input	100M Ethernet interface optical signal detection input. 1. When the 1-7 port is configured as a 100Base-FX mode, the FXSD pin is used to detect whether effective signal optical module. High level indicates a signal detected. 2. When the 1-7 port is configured as a 100Base-TX mode, FXSD pin is not suspended, direct grounding.
FXSD2	A4		
FXSD3	A6		
FXSD4	A47		
FXSD5	A48		
FXSD6	A49		
FXSD7	A50		
FXSD8	B22	Input	1000M Ethernet interface optical signal detection input. 1. When the 8-10 port is configured as a 1000Base-X mode, the FXSD pin is used to detect whether effective signal optical module. High level indicates a signal detected. 2. When the 8-10 port is configured as a SGMII mode, FXSD pin is not suspended, direct grounding.
FXSD9	B21		
FXSD10	B24		
CONFP 1	B23	Input	Work mode configuration of the Ethernet port. 1. Set the port as 10BASE-T /100BASE-TX self-adaption mode when CONFIGn connect to GND. 2. Set the port as 100BASE-FX full-duplex mode when CONFIGn connect to 3.3V power by 4.7kΩ resistance. 3. Direct grounding while unused.
CONFP 2	B26		
CONFP 3	B25		
CONFP 4	B28		
CONFP 5	B27		
CONFP 6	B30		
CONFP 7	B29		
SPEED1	C44	Output	Indicate the Ethernet interface rate 1. Output high level when the port set as 10BASE-T mode. 2. Output low level when the port set as 100BSEA-TX mode.
SPEED2	C42		
SPEED3	C40		
SPEED4	C38		
SPEED5	C36		
SPEED6	C34		
SPEED7	C32		
LINK1	C43	Output	Indicate the link status of Ethernet interface 1. Output high level when port no connection. 2. Output low level when port established connection. 3. Data transmitting that output alternate between high level and low level. When Port8-10 under SGMII mode, LINK8-LINK10 only indicate if the connection successful, and do not stand for external PHY state. Please use the build-in LINK single pin of PHY as its state indicator. LINK8 is a multifunction pin, when module power on and initialization, this pin act as mode setting of port8 (P8_MODE): Low level: SGMII (No connection) High level: 1000BASE-X (Connect to 3.3V power by 4.7kΩ resistance)
LINK2	C41		
LINK3	C39		
LINK4	C37		
LINK5	C35		
LINK6	C33		
LINK7	C31		
LINK8	C47		
LINK9	C46		
LINK10	C48		

RX8+	B4	Input	Gigabit Ethernet interface: signal receiver positive. When the port is configured as Gigabit fiber mode, the pin RXP [8:10] directly with the optical fiber module is connected with the output terminal of the positive.
RX9+	B9		
RX10+	B15		
RX8-	B3	Input	Gigabit Ethernet interface: signal receiver negative. When the port is configured as Gigabit fiber mode, the pin RXN [8:10] directly with the optical fiber module is connected with the output terminal of the negative.
RX9-	B10		
RX10-	B16		
TX8+	B6	Output	Gigabit Ethernet interface: signal transmitter positive When the port is configured as Gigabit fiber mode, the pin TXP [8:10] directly with the optical fiber module is connected with the input terminal of the positive.
TX9+	B11		
TX10+	B17		
TX8-	B5	Output	Gigabit Ethernet interface: signal transmitter negative When the port is configured as Gigabit fiber mode, the pin TXN [8:10] directly with the optical fiber module is connected with the input terminal of the negative.
TX9-	B12		
TX10-	B18		
P9_MODE0	C7		Port9&10 mode setting, Px_MODE[1:0] Direct connecting to GND means 0, connecting to 3.3V via 4.7K resistance means 1. 00:Reserved 01:1000BASE-X 10:SGMII (1000Base-T) 11:Reserved
P9_MODE1	C8		
P10_MODE0	C9		
P10_MODE1	C10		
VIN	C4	Input	Power Input (3.3VDC).
	C5		
	C6		
GND	A1 A7 A8 A9 A10 A19 A20 A29 A30 A35 A36 A45 A46 C1 C2 C3 C23 C24 C49 B1 B2 B7 B8 B13 B14 B19 B20	-	GND
U0TX	C29	Output	UART transmitting pin(program update and factory debugging)
U0RX	C30	Input	UART receiving pin(program update and factory debugging)
nRST_IN	A3	Input	System reset, low level is effective.
VCT25	A2	Output	+2.5V/600mAOutput, power supply for center tap of network transformer.
MDIO_PHY	B32	Input / Output	SMI interface signals, the module use the SMI interface and automatically access external PHY chip. The signal pins have internal pull-up resistor, it is allowed to float.
MDC_PHY	B31	Output	

PWR1ALARM	C21	Input	2 channels power alarm input, the default is low level alarm.
PWR2ALARM	C19		
RELOAD	C17	Input	Reset to defaults. Module reset to defaults when power-on input is low level.
ALARMOUT	C15	Output	Alarm Output, high level indicate alarm. Can configure relay Alarm Output status.
RUN_LED	C13	Output	Module running status indicator.
nRST_PHY8	C12	Output	System reset output. When port8&9 work under SGMII and act as the Giga electrical port combine with external PHY chip, this pin is used to reset corresponding external PHY chip. Low level is effective.
nRST_PHY9	C11		
nRST_PHY10	C16		
PROGRAM	C18	Input	Program update mode. Power on level: Low level: program update; High level: normal running
NC	C22 C25 C26 C27 C28 C45	-	Reserved. Not used, be suspended

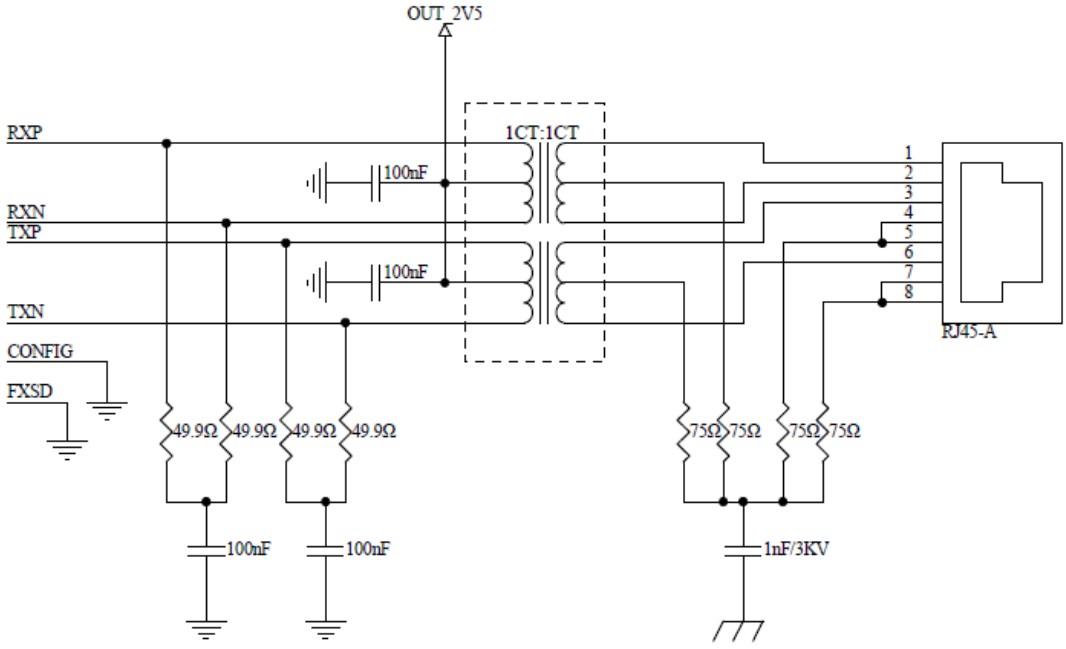
2.2 Ethernet Interface Description

2.2.1 100BASE-TX/FX Port Description

IEM7110-3G support 7 100M ports (port1 to port7), and can be optional set as fiber port or RJ45 port based on user needs.

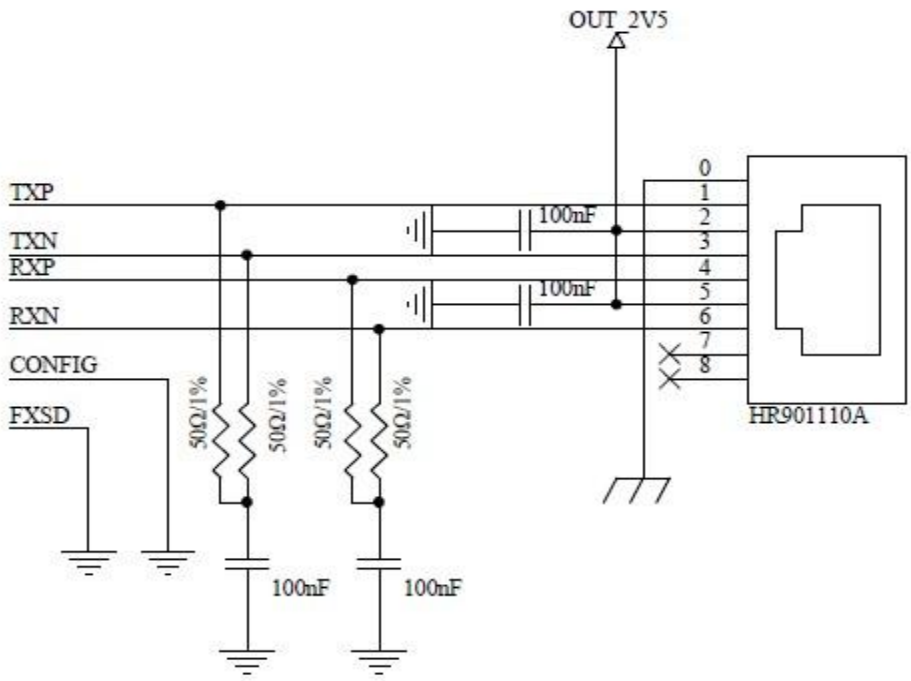
Name	Pin Num.	Type	Description
RX+[1:7]	A14、A15、A24、A25、A34、A38、A43	Positive of receiver.	Ethernet port configuration: 1. Set the 0-7 Ethernet interfaces as 10BASE-T/100BASE-TX when the CONFIGn and FXSDn connect to ground. 2. Set the 0-7 Ethernet interfaces as 100BASE-FX when the CONFIGn connect to 3.3V power by 4.7KΩ and FXSDn connect SD signal of optical module.
RX-[1:7]	A13 、A16、A23、A26、A33、A37、A44	Negative of receiver.	
TX+[1:7]	A12、A17、A22、A27、A32、A40、A41	Positive of transmitter.	
TX-[1:7]	A11、A18、A21、A28、A31、A39、A42	Negative of transmitter.	
FXSD[1:7]	A5、A4、A6、A47、A48、A49、A50	Data acquisition result that if there is optical signal from the optical port.	
CONFIG[1:7]	B23、B26、B25、B28、B27、B30、B29	Work mode configuration of the Ethernet port.	
LINK[1:7]	C43、C41、C39、C37、C35、C33、C31	Output	1. No connection when output high level. 2. Established connection when output low level. 3. Data transmitting when output alternate between high level and low level.
SPEED[1:7]	C44、C42、C40、C38、C36、C34、C32	Output	1. Output high level when the port set as 10BASE-T mode. 2. Output low level when the port set as 100BSEA-TX mode.

Reference circuit of 100BASE-TX (Independent network transformer)

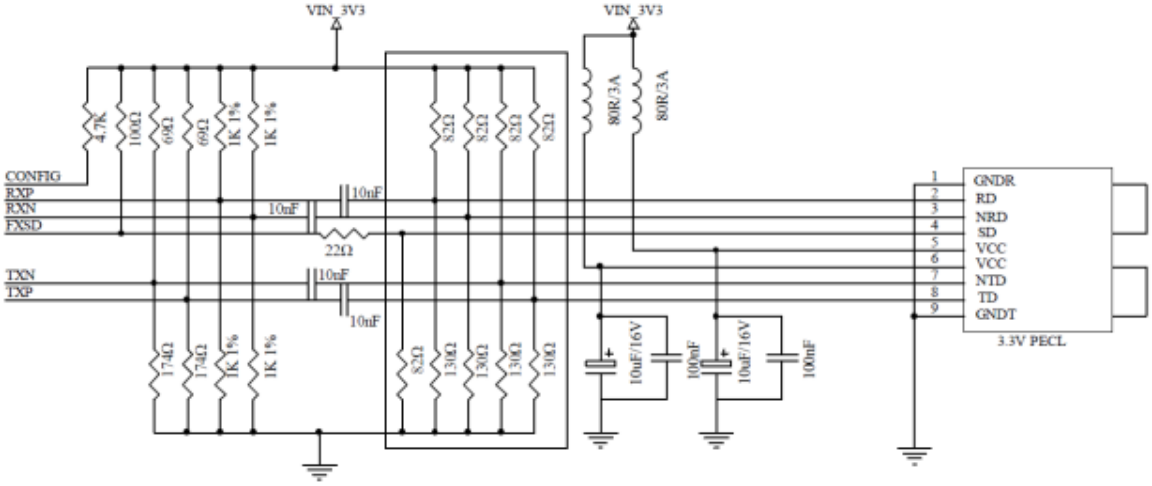


Attention: CONFIGn and FXSDn both connect to ground.

Reference circuit of 100BASE-TX (With a built-in network port transformer)



Reference circuit of 100BASE-FX



Attention:
1) The CONFIGn connect to 3.3V power by 4.7ohm, and FXSDn connect to SD of optical module.
2) Use 3.3V LVPECL optical module.
3) Use AC coupling, not recommend DC coupling.

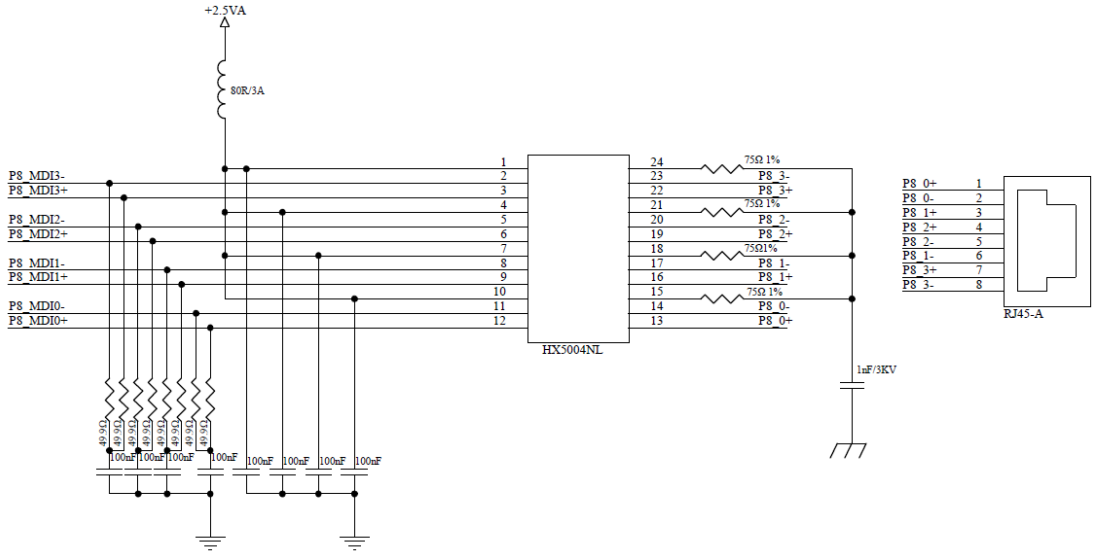
2.2.2 1000BASE-TX/FX description of PORT8

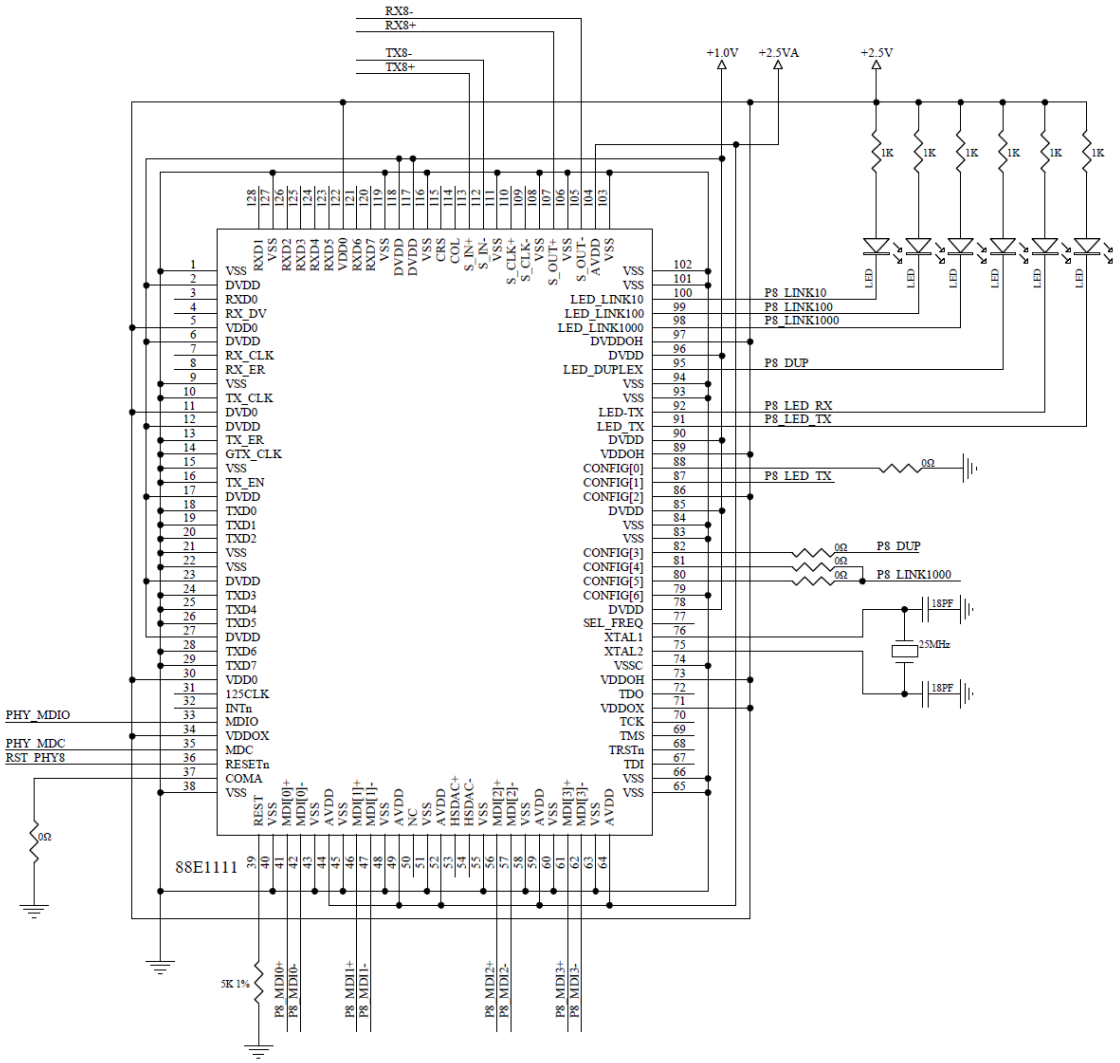
IEM7110-3G support 3 gigabit ports (port8 -port10), and can be optional set as 1000BASE-X or SGMII according to user's needs.

Under SGMII mode, user can extend interface type via external connection of Gigabit physical ship.

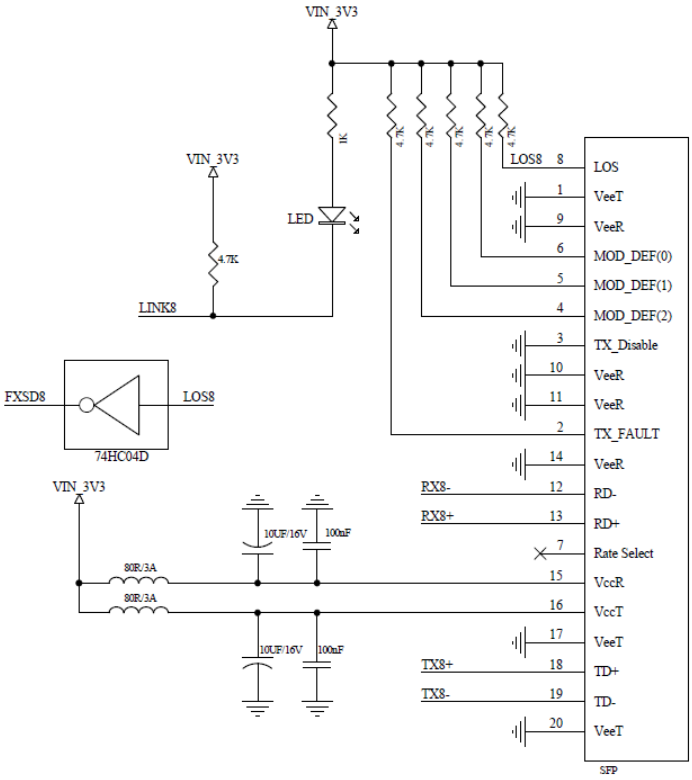
Name	Pin Num.	Type	Description
RX8+	B4	Positive of receiver.	When the link8 pin connect +3.3V by 4.7k that port 8 is optical fiber port. 1. Output high level when port no connection. 2. Output low level when port established connection. 3. Data transmitting that output alternate between high level and low level. When the LINK8 pin is no connect that Port 8 be configured SGMII mode
RX8-	B3	Negative of receiver.	
TX8+	B6	Positive of transmitter.	
TX8-	B5	Negative of transmitter.	
LINK8	C47	output	
FXSD8	B22	Optical Detection input	1000M Ethernet interface optical signal detection input. When the port 8 is configured as a 1000Base-X mode, the FXSD pin is used to detect whether effective signal optical module. High level indicates a signal detected. When the 8 port is configured as a SGMII mode, FXSD pin is not suspended, direct grounding.
nRST_PHY8	C12	output	Software reset PHY chip. Active low.
PHY_MDIO	B32	Input/output	External PHY chip management data input and output pin
PHY_MDC	B31	output	External PHY chip management data clock pin

Reference circuit of port8 setting as SGMII mode, and use external physical PHY to realize 10/100/1000BASE-T.





Reference circuit of port8 setting as 1000BASE-X



Attention:

1） It only apply to the SFP optical mode.

2） LINK8 pull up to 3.3V via 4.7K resistor, so module work under 1000BASE-X after power on.

3） After inversion, the LOS single of SFP connect to FXSDx of module.

2.2.3 PORT9 1000BASE-TX/FX interface description

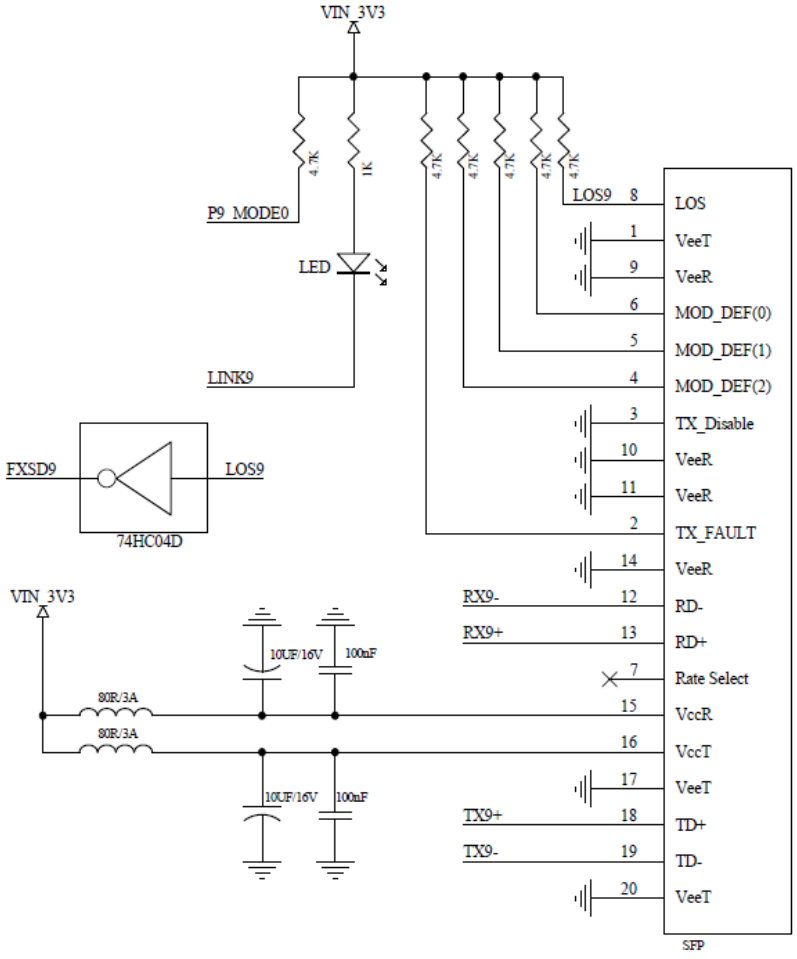
IEM7110-3G support 3 Gigabit ports (port8 -port10), and can be optional set as 1000BASE-X or SGMII according to user's needs.

Under SGMII mode, user can extend interface type via external connection of Gigabit physical ship.

Name	Pin Num.	Type	Description
RX9+	B9	Positive of receiver.	Port9&10 mode setting, Px_MODE[1:0] Direct connecting to GND means 0, connecting to 3.3V via 4.7K resistance means 1. 00:Reserved 01:1000BASE-X 10:SGMII (1000Base-T) 11:Reserved
RX9-	B10	Negative of receiver.	
TX9+	B11	Positive of transmitter.	
TX9-	B12	Negative of transmitter.	
P9_MODE0	C7	Mode configuration	
P9_MODE1	C8		
FXSD9	B21	Optical Detection input	1000M Ethernet interface optical signal detection input. When the port 9 is configured as a 1000Base-X mode, the FXSD pin is used to detect whether effective signal optical module. High level indicates a signal

			detected. When the 9 port is configured as a SGMII mode, FXSD pin is not suspended, direct grounding.
LINK9	C46	output	When port 9 be configured optical fiber port. 1. Output high level when port no connection. 2. Output low level when port established connection. 3. Data transmitting that output alternate between high level and low level.
nRST_PHY9	C11	output	Software reset PHY chip. Active low.
PHY_MDIO	B32	Input/output	External PHY chip management data input and output pin
PHY_MDC	B31	output	External PHY chip management data clock pin

Reference circuit of port9 setting as 1000BASE-X mode.

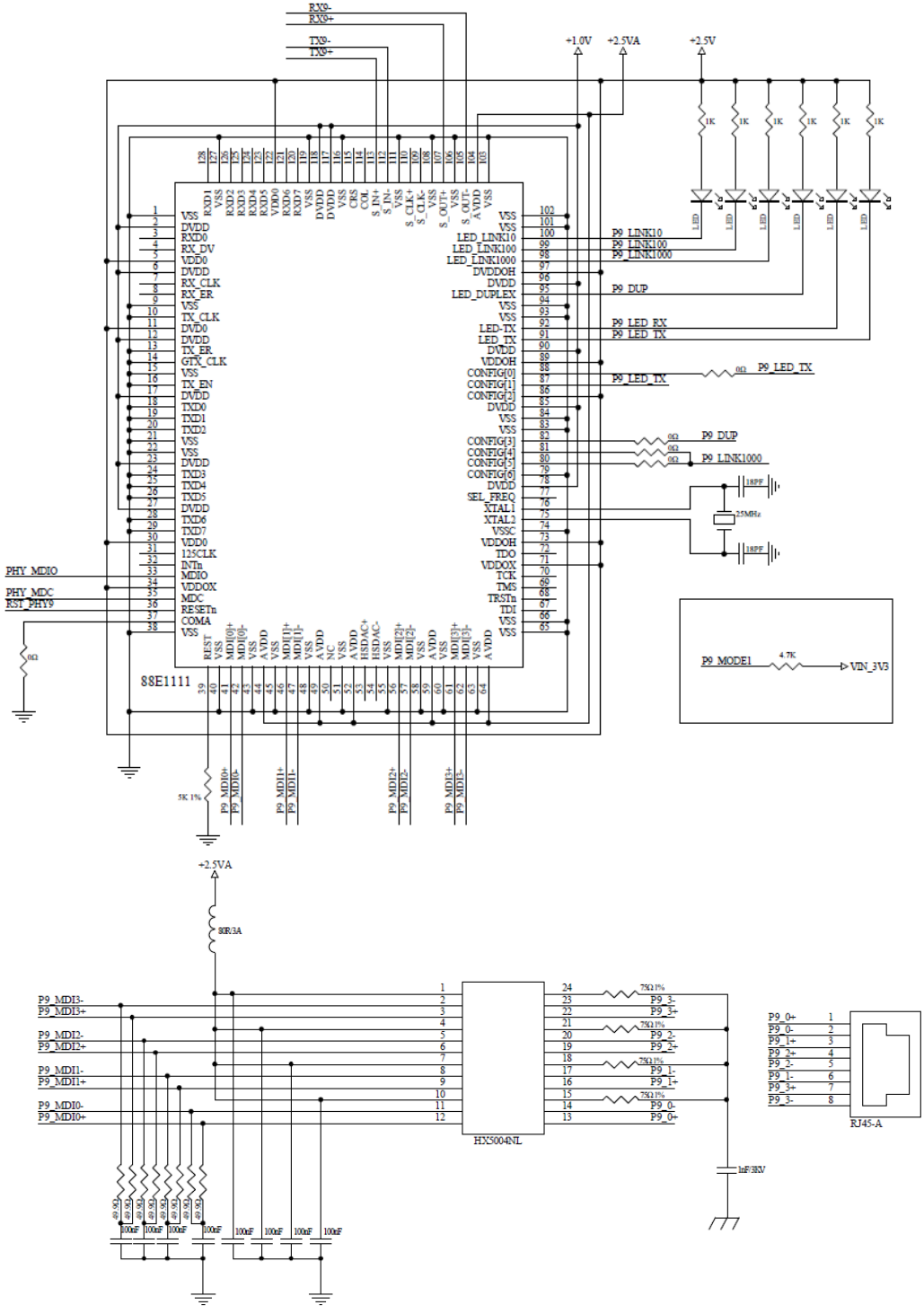


Attention:

1） It only apply to the SFP optical mode.

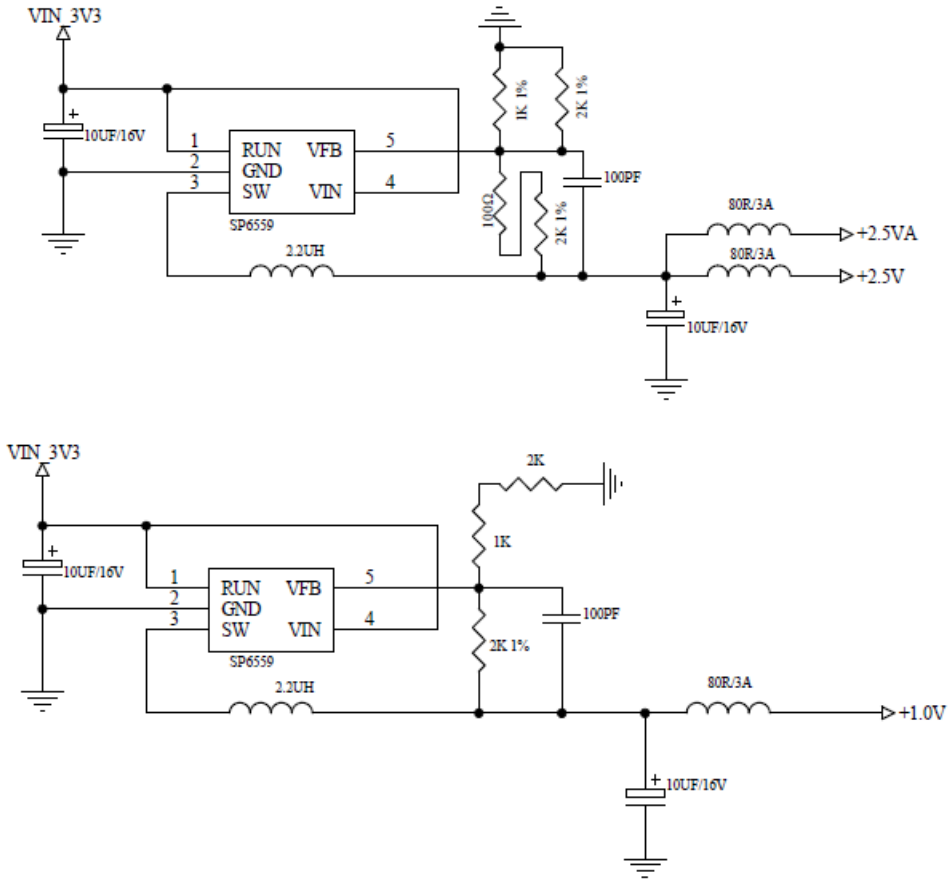
2） Cause set Px_MODE[1:0] as 01, the module work under 1000BASE-X after power on.
3） After inversion, the LOS single of SFP connect to FXSDx of module.
4） LINKx PINs only serve as LINK, and do not connect to 3.3V power via 4.7K resistor.

Reference circuit of port9 setting as SGMII mode, and use external physical PHY to realize 10/100/1000BASE-T.



Port 10 circuit can reference Port 9.

2.2.4 PORT8, PORT9 power reference circuit



The 1.1V, 2.5V, 2.5VA stable DC voltage power supply to PHY chip of Port8 and Port9 Gigabit Ethernet port, in order to make the PHY chip can work stably, recommended in the PHY chip of each power supply pin with 100nF filter capacitor

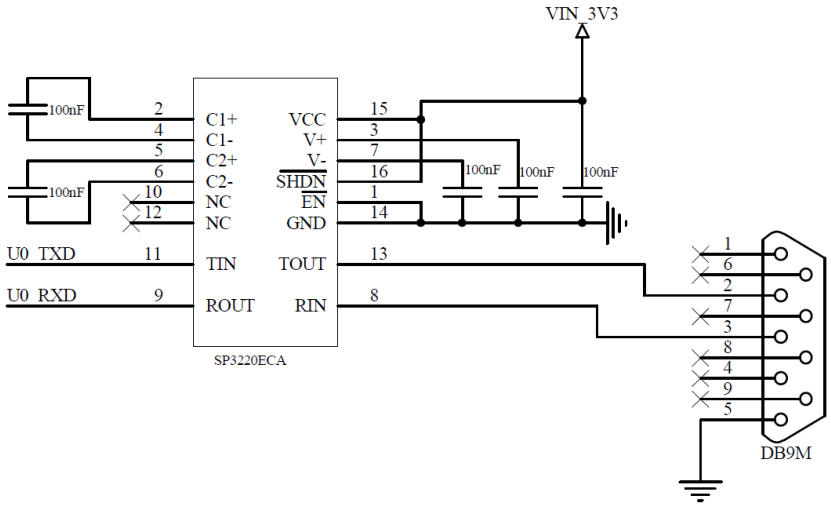
2.3 Power Interface

Name	Pin Num.	Type	Description
VIN	C4、C5、C6	Input	Power Input(3.3VDC)
VCT25	A2	-	+2.5V/600mAOutput, only supply to the center tap of the network transformer
GND	A1 A7 A8 A9 A10 A19 A20 A29 A30 A35 A36 A45 A46 C1 C2 C3 C23 C24 C49 B2 B1 B8 B7 B14 B13 B20 B19	-	GND

2.4 UART Interface

Module support an UART serial interface, only use as program update and factory debugging. Users should reserve the interface when product design for convenient upgrade and debugging

Name	Pin Num.	Type	Description
U0TX	C29	Output	UART transmitting pin(program update and factory debugging)
U0RX	C30	Input	UART receiving pin(program update and factory debugging)

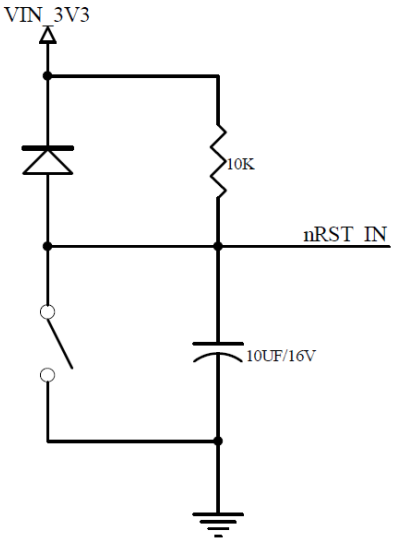


3.3V TTL level input and output, compatible with 5V TTL level inputs

2.5 Reset

IEM7110-3G support a reset input. The input reset use to reset module, and output reset use to reset external PHY chip when start or find fault.

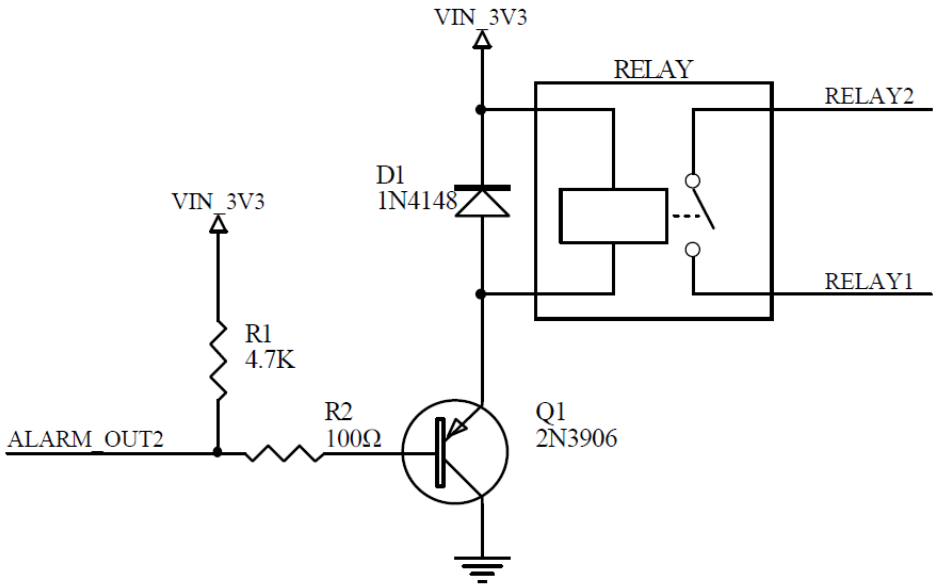
Name	Pin Num.	Type	Description
nRST_IN	A3	Input	System reset pin, low level effectively. When the input of this pin is low level and last more than 200ms, the system turn into reset state.



2.6 Port Alarm

Module support 2 channels power alarm input, whether use can set through the software. Module support 1 channel alarm output, user can set the detailed content of the alarm through the software, such as power alarm, ring broken, port lost connecting.

Name	Pin Num.	Type	Description
PWR2ALARM	C19	Input	2 channels Alarm Input, low level indicate alarm.
PWR1ALARM	C21		
ALARMOUT	C15	Output	Alarm Output, low level indicate alarm.



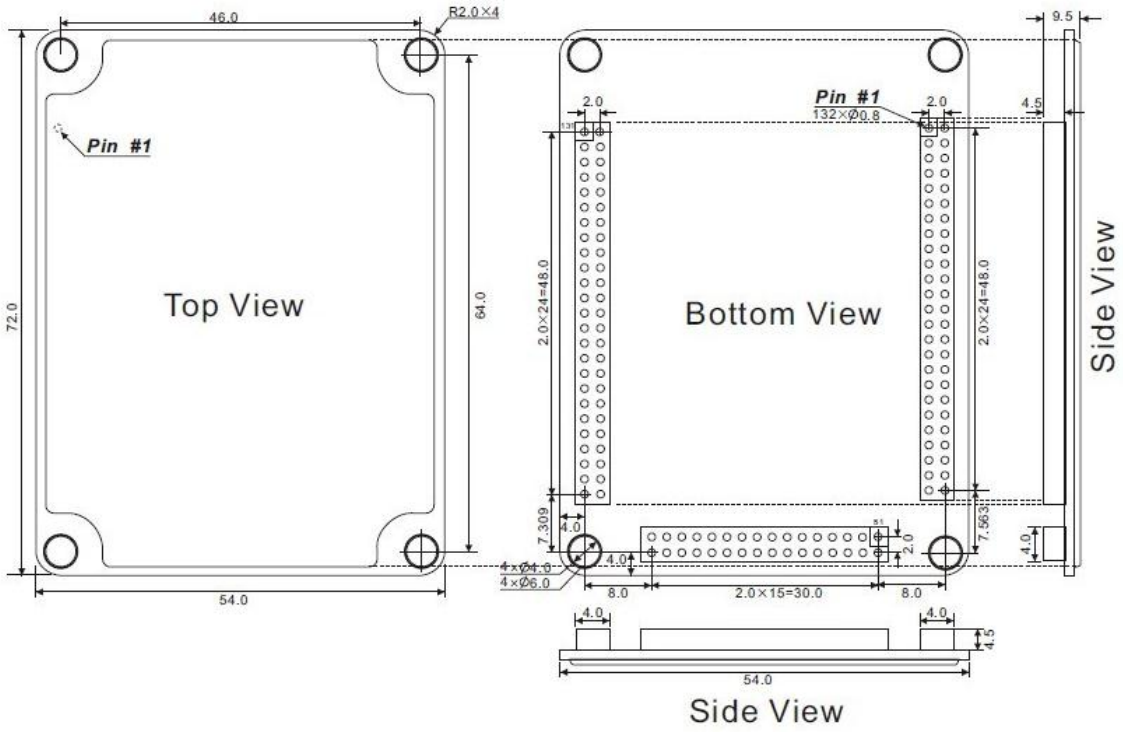
2.7 Reset to defaults

This module supports two factory default function: hardware and software. Hardware factory default priority is higher than the software.

Name	Pin Num.	Type	Description
RELOAD	C17	3.3v TTLInput	Reset to defaults. Module reset to defaults when power-on input is low level.

Chapter 3 Outline Drawing

Unit: mm



Chapter 4 Features

Interface:

- Ethernet interface: Support 7 channels Fast Ethernet and 3 channels Gigabit Ethernet interface, can deploy as electric port or fiber port at will.
- Redundancy ring network interface: 10*Ethernet interface can deploy as redundancy ring network interface at will.
- Management interface: anyone Ethernet interface can be the management interface.
- Alarm interface: 2 channels LVTTL monitoring signal input and 1 channel LVTTL alarm output, support the local or remote alarm of the power status, link status, or the ring network status.

Protocol:

- IEEE 802.3 10Base-T Ethernet
- IEEE 802.3u 100Base-TX Fast Ethernet
- IEEE 802.3u 100Base-FX Fast Ethernet
- IEEE 802.3z 1000BaseSX/LX/LHX/ZX
- IEEE 802.3ab 1000Base-T
- IEEE 802.3x Flow Control and Back-pressure
- IEEE 802.1p Quality of Service
- IEEE 802.1Q VLAN
- IEEE 802.1D RSTP
- IEEE 802.3ad Port Trunking

Switch Properties:

- Support maximum 250 devices in a ring.
- Recovery time < 20ms
- 100M Forward speed: 148810pps
- 1000M Forward speed: 1488100pps
- Switch Architecture: store-and-forward
- Switch bandwidth: 7.6G
- MAC Address table: 8K
- Memory: 1M

Features:

- Support VLAN.
- Support QoS.
- Support static multicast, IGMP Snooping
- Support RSTP
- Support LLDP
- Support unknown unicast storm inhibition.
- Support port mirroring.
- Support port trunking.
- Support SNMP
- Support safe WEB interface management.
- Support Single, Couple, Chain, Dual homing ring.
- Support port rate limiting.
- Support port package statistics
- Support fault alarm.

Power supply:

- DC3.3V±5%
- Power consumption < 3W

Mechanical Structure

- Signal Pin: 2 * Dual in-line package (50 pins and 2mm pin spacing), 1 * DIP (16 pins and 2mm pin spacing), pin wide 0.5 mm.

- Dimensions (H×W×D): 72mm×54mm×9.5mm(including the pin)

Environmental Limits

- Operating Temperature: -40℃~85℃
- Storage Temperature: -40℃~85℃
- Ambient Relative Humidity: 5%~95%(non-condensing)

Chapter 5 Web management

Module support Web management, it can be managed and maintained via the Web interface intuitively. The under below stating module is a switch consisting of Module and DEMO board.

Before configuration, please make sure your PC install the necessary software and network setting reasonable. Minimum request to user PC:

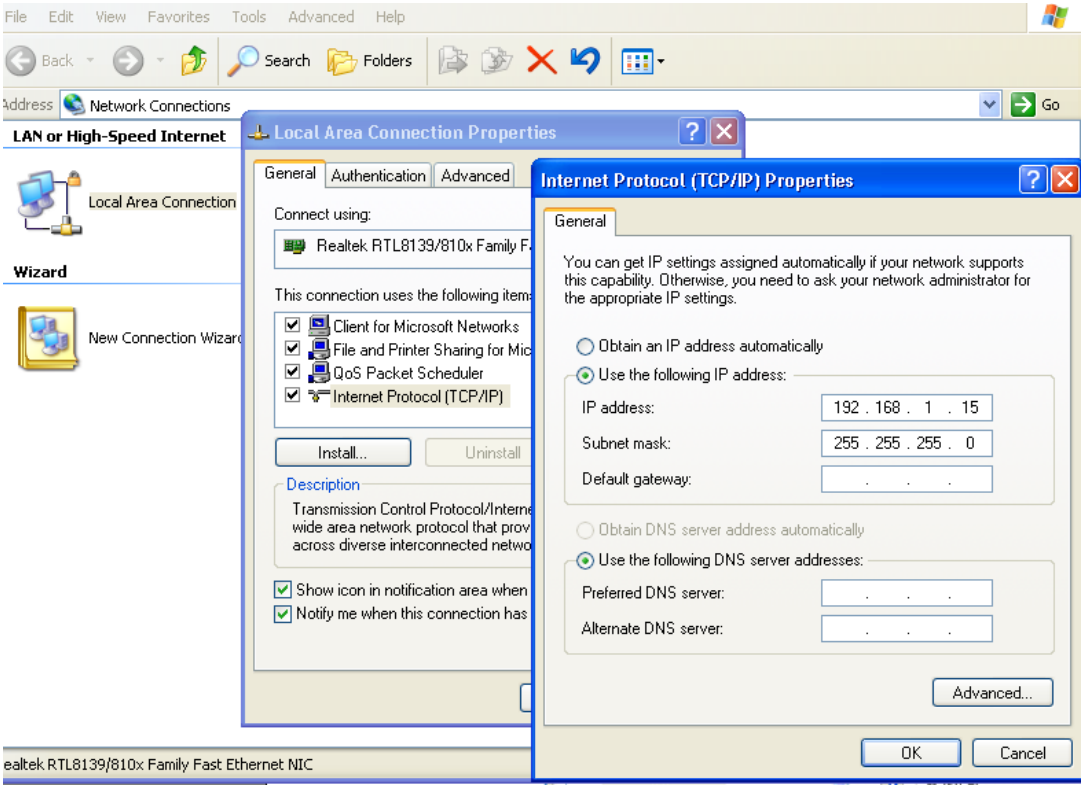
- Been installed operating system, such as Windows XP/2000
- Been installed Ethernet card
- Been installed Web Brower
- Been installed and started TCP/IP protocol

5.1 Network setting

The default IP of module is 192.168.1.254, and subnet mask is 255.255.255.0. When access to the module via Web, the IP of switch and PC must be in one LAN. Can modify the PC IP or switch IP to make sure them in one LAN, the setting could refer to the method 1 or 2 as following.

Method 1: modify the PC IP

- Reset to default: switch the pin1 of the toggle switch to ON, reboot and then switch to OFF.
- Click Start->Control panel->network connections->Local area Connection->Properties->Internet protocol(TCP/IP)Setting PC's IP address: 192.168.1.X(X is from 2 to 253 expect 254)
- Click "OK", IP address modified successful.
- The Windows system operation interface is as figure 5-1.



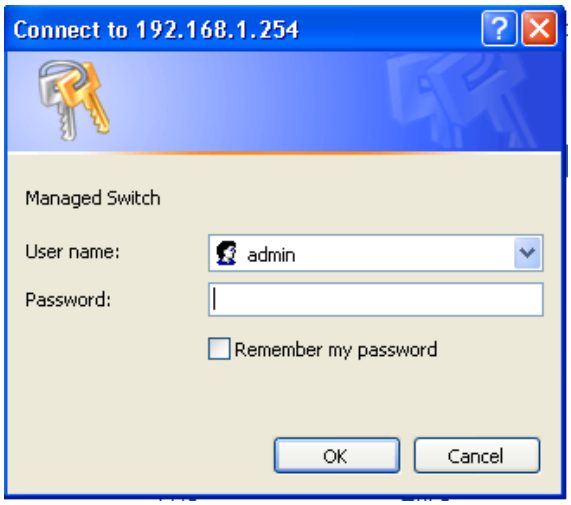
(Figure5-1)

Method 2: Modify module IP through our Blue_eyes management software

- Install the Blue_eyes management software on the PC.
- Enter into Blue_eyes management interface, click “Search” to search the module.
- After searched the module, move the mouse cursor on the module, click right key, modify the module’s IP address, make sure module and PC must be in one LAN.

5.2 Startup and Login

Open IE, input http://192.168.1.254 in the address bar, and click “Enter”, as figure 5-2:



(Figure5-2)

Input correct user name and password, then enter successfully (default user name is “admin”, password is “admin”). If user name or password input incorrectly 3 times continuously, you must login again.

Attention:

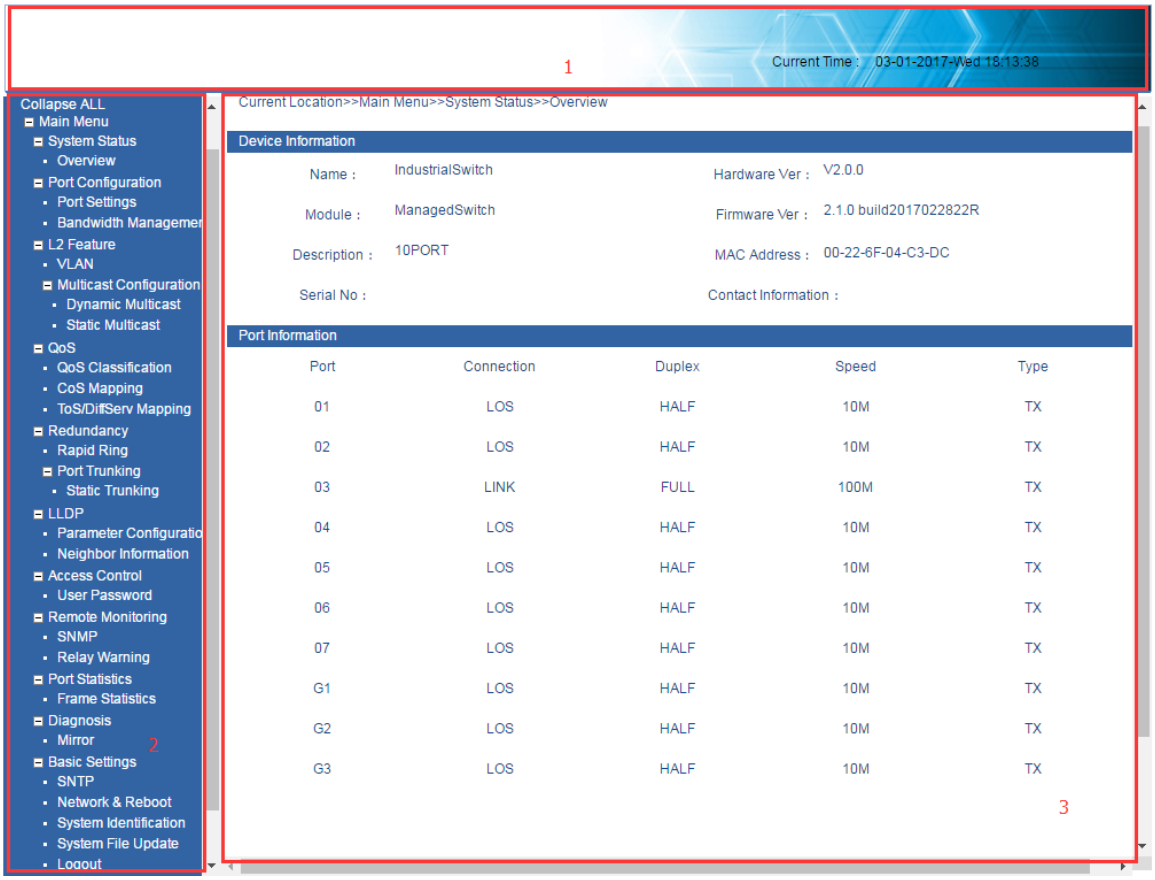
User name and password are case-sensitive. If you are not clear about IP address, you can find it by searching function of Blue_eyes management software.

5.3 Configuration Description

Enter the Web interface as shown in Figure 5-3. This interface can be divided into 3 parts:

1. Title area
2. Main Menu
3. Setting area.

By clicking items in the main menu, you can enter relevant interface. Setting area presents the status and setting items.



(Figure 5-3)

➢ **Main Menu**

Main menu consists of 11 parts

Main Menu	Tag	Function
System Status	System information	Display device information and port information such as software version, IP address, etc.
Port Configuration	Port settings	Display and configure information of each port: such as connection status, configuration modes, flow status etc.
	Bandwidth management	Set the maximum rate of the input/output packets for port.
L2 feature	VLAN	Displays the current list of 802.1Q VLAN, configure and manage 802.1Q VLAN.
	IGMP snooping	Display port-based VLAN list, and to configure and manage port-based VLAN.
	Static Multicast	Configure the static multicast MAC address and its corresponding port.
QOS	QoS classification	Configure the the QOS queue mode, QOS implementation and port default priority.
	Cos Mapping	Configure the meaning of COS value.
	Dscp	Configure the DSCP priority.
Redundancy	Port Trunking	Configure port trunking group.
	Rapid Ring	Configure the rapid ring network port and type.
	RSTP	Configure the parameters of RSTP.

Main Menu	Tag	Function
LLDP	Parameter Configuration	LLDP Parameter Configuration and LLDP configuration of port
	Neighbor Information	Display LLDP neighbor information
Access control	User password	Configure different permissions for the user name and password.
Remote Monitoring	SNMP	SNMPv1/v2, SNMP configuration
	Relay Warning	External input Alarm Settings, Port connection state alarm
Port Statistics	Frame statistics	RX and TX frame statistics
Diagnosis	Mirror	Configure the mirror port and mirrored port.
Basic Settings	SNTP	Time setting
	Network & Reboot	Network IP and DNS setting, device reboot
	System Identification	Model, name and other information.
	System File update	Software upgrade, acquire, preserve or restore the switch configuration.
	Logout	System log off

Web Time-out Handling

If user doesn't operate the Web interface for a long time, the system will logout (but the modification made by this login will be saved in Web configuration interface.). If the user wants to do any operating on Web configuration interface again, the system will reminds user and returns to the login dialog box. Users need to log in again if operating is needed.

System time-out is 300s.

➢ Setting Area

Setting area consists of device information and port information.

Device information mainly display the basic information of module, such as model, name, description, Serial No., hardware version, Firmware version, MAC address, contact information, as shown in Figure 5-5:



(Figure 5-5)

Among them, Model, Hardware Version, Firmware Version and MAC address can't be changed. Name, Description, Serial No. and Contact Information can be changed or custom-made. Please refer to chapter 6 Device Information if change is necessary.
Port Information area presents the every port status.

For example, in the following figure we can get the information of Port 5: connection status is LINK, Port status is FULL, Speed is 100M, Port Type is TX, as shown in Figure 5-6:

Port Information

Port	Connection	Duplex	Speed	Type
01	LOS	HALF	10M	TX
02	LOS	HALF	10M	TX
03	LINK	FULL	100M	TX
04	LOS	HALF	10M	TX
05	LOS	HALF	10M	TX
06	LOS	HALF	10M	TX
07	LOS	HALF	10M	TX
G1	LOS	HALF	10M	TX
G2	LOS	HALF	10M	TX
G3	LOS	HALF	1000M	FX

(Figure 5-6)

5.4 Port Configuration

5.4.1 Port Settings

The port configuration interface mainly include port type (Electric port or optical port), setup speed mode and duplex mode, flow control. Only when the port is enabled for the port speed, duplex, flow control will work. Select auto-negotiation, speed, and duplex auto-negotiation.

Current Location>>Main Menu>>Port Configuration>>Port Settings

Port Settings

Port	Type	Speed	Duplex	Enable	Flow Control
01	TX	10 M	Half Duplex	☑	☐
02	TX	100 M	Full Duplex	☑	☐
03	TX	AUTO	Half Duplex	☑	☐
04	TX	AUTO	Half Duplex	☑	☐
05	TX	AUTO	Half Duplex	☑	☐
06	TX	AUTO	Half Duplex	☑	☐
07	TX	AUTO	Half Duplex	☑	☐
G1	TX	AUTO	Half Duplex	☑	☐
G2	TX	1000 M	Half Duplex	☑	☐
G3	FX	AUTO	Half Duplex	☑	☐

Apply Cancel

(Figure 5.4.1)

Configuration Items	Description
Port	Port name, corresponding to mark in panel.
Type	Display port type (TX or FX).
Speed	Display configurable speed of port or auto-negotiation mode.
Duplex	Auto-negotiation (AUTO), full duplex (FULL), half duplex (HALF) optional, default mode is auto-negotiation mode.
Enable	Configurable port enable or disable. Selecting square frame is for enable the corresponding port. It cannot transmit data if any port disable. The default is “Enable”.
Flow Control	Whether selecting flow control to the port. Only can selecting flow control when the port enable. The default is off.

The described Electric port is the common network device RJ-45 port, commonly known as "crystal head", it's is a twisted-pair Ethernet interface type. This interface can be used in 10Base-T, 100Base-Tx and 1000Base-Tx Ethernet, transmission media is twisted pair, but according to different bandwidth media have different requirements, in particular, 1000Base-Tx Gigabit Ethernet connection, at least to use cat5e.

Port Speed
Port speed shows the connecting speed of the port. It includes 3 kinds of speed: 10M, 100M and auto-negotiation.
10M uses 10base-T standard and UTP cable for connection. When the port is in 10M speed, Link/Act indicator will blink continuously while data transmitting and status indicator of 10M/100Mbps will stay OFF.

100M uses 100Base-TX standard and UTP/STP cable for connection. When the port is in 100M speed, Link/Act indicator will blink continuously while data transmitting. 100M fiber port uses 100Base-FX standard and single/multi-mode fiber for connection. Main fiber of 100Base-FX standard includes: 62.5nm multi-mode fiber and 50nm multi-mode fiber. Auto-negotiation includes 2 kinds of speed according the capability of the other end: 10M and 100M.

Port Enable
This item provides a device to enable/disable the port. When choosing disable, the device would cut off power supply of this port. Even if other device is connected to this port, all status indicators of this port are OFF. Only enable this port, all settings about this port will be valid. This item provides a kind of safety mechanism to protect the port from illegal use. It is not allowed to disable all the ports.

Duplex Mode
Full duplex of the switch means switch can transmit and receive data at the same time. Half duplex of the switch means switch can transmit or receive data in a certain time. Generally the speed will choose auto-negotiation so that the port can automatically judge the connection type of the device connected to it and automatically adjust the connection type to ensure the maximum compatibility.

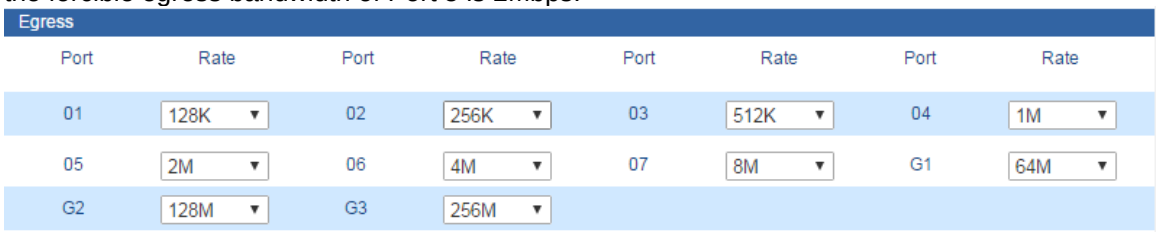
Flow Control
Flow control is used to prevent the frames from discard while port is blocked. This method is to send back the blocking signal to its original address while sending or receiving buffer area start to overflow. It limits the abnormal flows into a certain range. Flow control can be effective in preventing large amounts of data in the network instant impact on the network to ensure the efficient and stable user network running.

Two types of flow control:

1. In the half duplex mode, flow control is through back pressure. It is to send a jamming signal to the transmission source to reduce transmission speed.
2. In the full duplex mode, flow control generally follow IEEE 802.3x standard. Switch sends "pause" to information source to pause its sending information.
Use flow control to control the data flow between the sending and receiving nodes, can prevent packet loss.

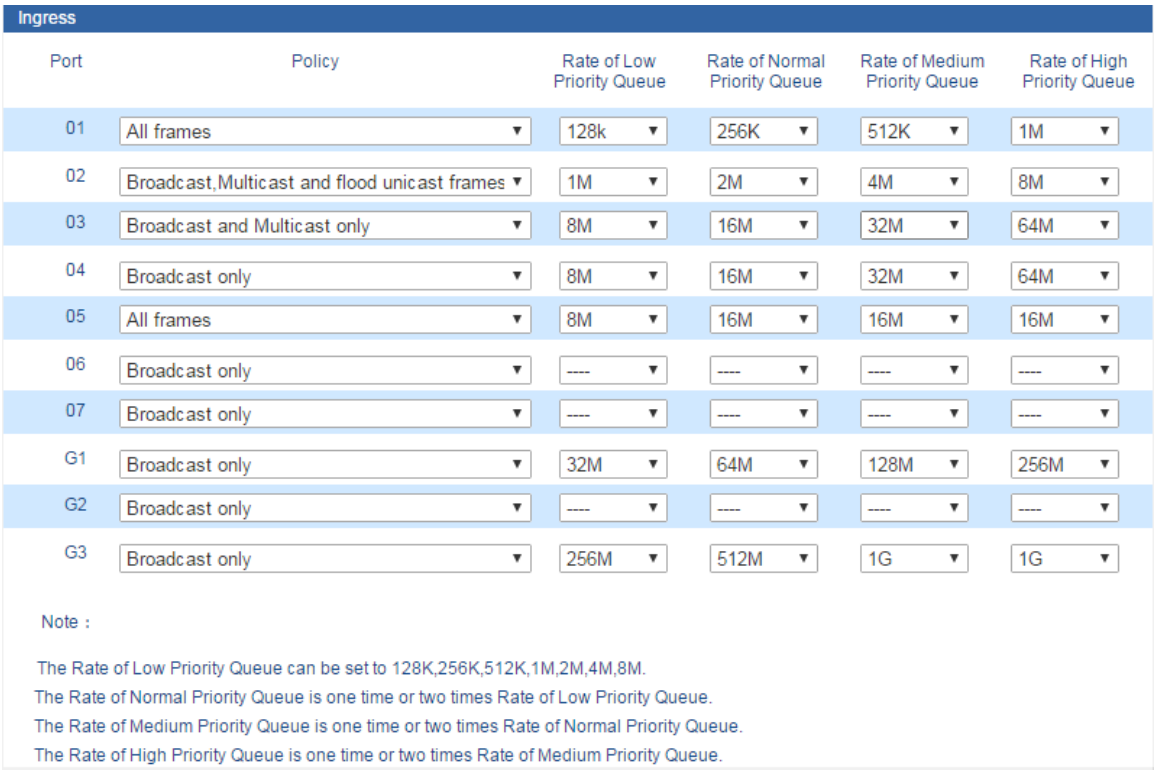
5.4.2 Bandwidth Management

Bandwidth management mainly refers to limit the data's egress and ingress bandwidth to save the network sources.
Click [port setting/bandwidth management] and enter into the following interface.
Egress Bandwidth Configuration:
"----" stands for no limitation for the speed, the others are corresponding speed.
As shown in following figure 5.4.2, the forcible egress rate of Port 5 is 2Mbps. Only need to select 2Mbps in egress rate setting of Port 5. The bandwidth of Port 5 as receiver is still 100Mbps, but the forcible egress bandwidth of Port 5 is 2Mbps.



(Figure 5.4.2)

Ingress Bandwidth Configuration:
Ingress bandwidth limit includes 4 kinds:
1 All frames;
2 Broadcast & Multicast & unicast frames;
3 Broadcast & Multicast only;
4 Broadcast only
"----" stands for no limitation, the rate of low priority queues (L) can be setted:128k, 256k, 512k, 1M, 2M, 4M, 8M.The rate of normal priority queues (N) is 1 or 2 times as wide as that of low priority queues. The rate of medium priority queues (M) is 1 or 2 times as wide as that of normal one. The rate of high priority queues is 1 or 2 times as wide as that of medium one.
For example, the rate of low priority queues is 256k, then the rate of normal priority queues can be set for 256k or 512k. Detailed operating as shown in Figure 5.4.3



Ingress

Port	Policy	Rate of Low Priority Queue	Rate of Normal Priority Queue	Rate of Medium Priority Queue	Rate of High Priority Queue
01	All frames	128k	256K	512K	1M
02	Broadcast,Multicast and flood unicast frames	1M	2M	4M	8M
03	Broadcast and Multicast only	8M	16M	32M	64M
04	Broadcast only	8M	16M	32M	64M
05	All frames	8M	16M	16M	16M
06	Broadcast only	----	----	----	----
07	Broadcast only	----	----	----	----
G1	Broadcast only	32M	64M	128M	256M
G2	Broadcast only	----	----	----	----
G3	Broadcast only	256M	512M	1G	1G

Note：

The Rate of Low Priority Queue can be set to 128K,256K,512K,1M,2M,4M,8M.
The Rate of Normal Priority Queue is one time or two times Rate of Low Priority Queue.
The Rate of Medium Priority Queue is one time or two times Rate of Normal Priority Queue.
The Rate of High Priority Queue is one time or two times Rate of Medium Priority Queue.

(Figure 5.4.3)

The ingress rate is related to CoS priority. Priority Queue is based on QoS setting (the same as QoS assorted setting includes checking CoS priority), or ingress rate will be based on default. CoS priority includes 4 queues: Low, Normal, Medium, High.
Operation method:
1. Choice 2 port at first, for example open the COS priority of port 4 and port 5, please according to 6.5 part
2. Then set port 4's CoS is High, port 5's CoS is LOW in COS mapping setting interface
3. Last, set the type of limit package and bandwidth of priority queue in Ingress bandwidth configuration
For example, keep up step 1 and 2, choice "All frame" in port 4 and 5 at step 3. Set 2M in all low priority queue

:

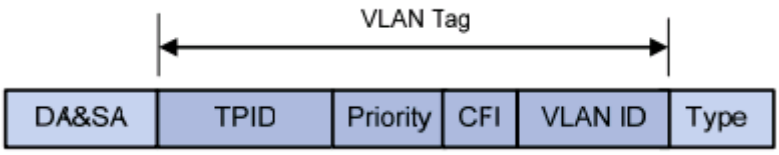
If priority queue bandwidth configuration is available, must mark the enter into port's data pack as CoS.

5.5 L2 Features

5.5.1 VLAN

IEM7110-3G supports based on 802.1Q VLAN. It deals with messages based on Tag of recognized message(including 802.1p priority and VLAN ID, etc.).

Frames with 802.1q add 4 byte Tag based on Ethernet frames, including 2 byte TPID, 3 byte Priority, 1 byte CFI and 12 byte VLAN ID.



TPID: a 16-bit field set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame.

Priority: It indicates the frame priority level. Values are from 0 (best effort) to 7 (highest); 1 represents the lowest priority.

CFI: a 1-bit field. If the value of this field is 1, the MAC address is in non-canonical format. If the value is 0, the MAC address is in canonical format.

VLAN ID: a 12-bit field specifying the VLAN to which the frame belongs. The hexadecimal values of 0x000 and 0xFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4,094 VLAN.

1. The type of port's Line

IEM7110-3G support 2 type port line:
Access: Port belongs to 1 VLAN, normally, it used for connecting user device, default all port is access port.

Trunk: Port belongs to some VLAN, can transmit and receive some VLAN message, normally, it used for connection of network device.

2. Deal with transmit and receive message

Type	**Receive message**	
	Message did not take Tag	**Message take Tag**
Access	Put the VLAN tag point to Port default VLAN ID for message	Put the VLAN tag point to Port default VLAN ID for message
Trunk	Put the VLAN tag point to Port default VLAN ID for message	Keep up VLAN ID, no need replace

Type	**Transmit message**
Unmodify	Did not modify when transmit, the data packet is the same as enter into switch
Untagged	Did not take the mark when transmit
Tagged	Take the mark when transmit

Unmodify: No need to modify original VLAN mark
Untagged: It is a normal Ethernet message
Tagged: Added a 4 bytes VLAN information after original MAC address and destination MAC address

3. Parameter item description

Item	**Description**
PVID	Port's LAN ID, value range : 1～4094
VID	VLAN ID number, value range: 1～4094

Item	Description
Power type	Include Access and Trunk
Member type	Unmodify, Untagged, Tagged
Modify all	Quickly modify the type of all members at the same time
Add	Add the configurated VLAN into VLAN table
Delete	Choice one VLAN in the table, knock<Delete>, delete VLAN

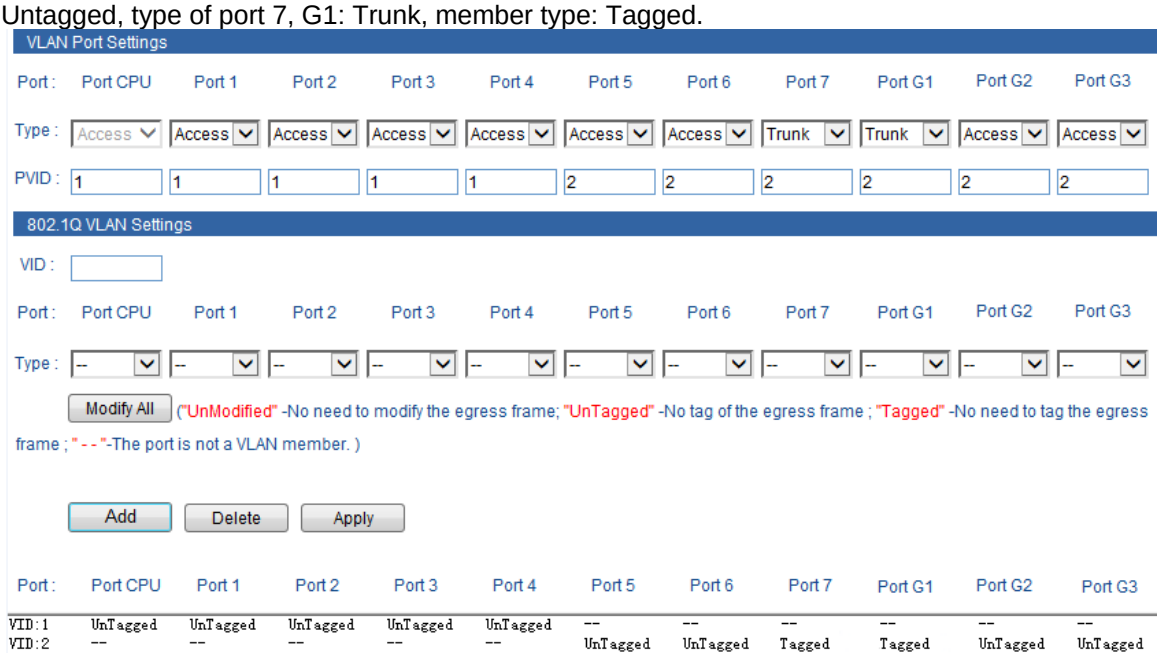
The default VLAN, all port are Access, PVID: 1, all belong to the members of VLAN1

4. Create VLAN

The step is as follows:

1. Enter into VLAN configuration interface, firstly select port type, Access or Trunk;
2. Input the default PVID of the port in [PVID] text box;
3. Input appointed VLAN into [VID] text box;
4. Set up members' type of each port: Unmodified, Untagged, Tagged
5. Click [Add] button, add VLAN items into the table and click [Apply] and reboot the device. Then creating new VLAN is finished.

As follow figure 5.5.1, create VLAN1, port type: Access, member type: Untagged, member included CPU port and port 1~4. Create VLAN2, type of port 5, 6: Access, member type: Untagged, type of port 7, G1: Trunk, member type: Tagged.



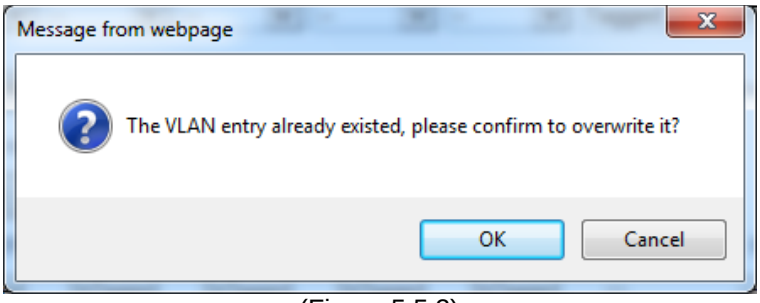
(Figure 5.5.1)

We can know as the figure, the type of port 7, G1 is Trunk, can allow the data of VLAN 1 and VLAN 2 pass.

5. Modify VLAN

It can re-configure existing VLAN including modifying member's type and quantity of the port. Steps are as follows:

1. Enter into VLAN configuration interface, firstly select VLAN items which need to modify in VLAN item table, like as VLAN 1.
2. Member's type of VLAN1 shows in current VLAN item setting and set up member's type of the port according to the steps for creating new VLAN.
3. Click [Add] button, select [OK] when reminds whether overwrite it as shown in Figure 5.5.2. Add new VLAN items into table and click [Apply] and reboot the device. Modify VLAN finished.

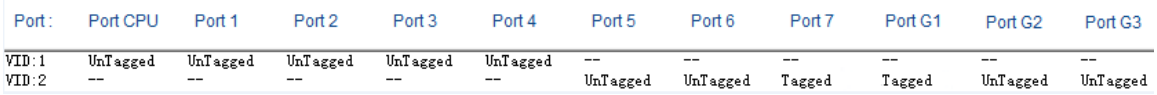


(Figure 5.5.2)

6. Delete VLAN

Steps of remove VLAN are as follows:

1. Firstly select VLAN items which need to remove, like as VLAN2;
2. After selected, click [Delete], then [Apply]. As shown in Figure 5.5.3:

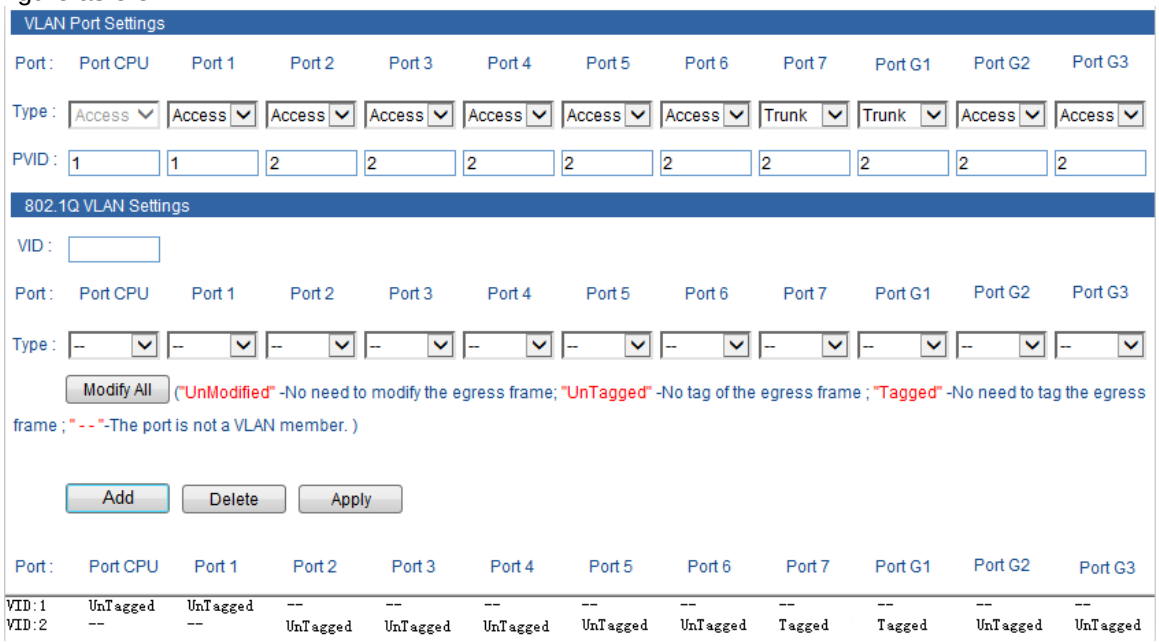


Port :	Port CPU	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port G1	Port G2	Port G3
VID:1	UnTagged	UnTagged	UnTagged	UnTagged	UnTagged	--	--	--	--	--	--
VID:2	--	--	--	--	--	UnTagged	UnTagged	Tagged	Tagged	UnTagged	UnTagged

(Figure 5.5.3)

7. VLAN Configuration of Single Ring

1. Need to set one port as managed port, managed port and CPU port must in a same VLAN, figure as 5.5.4, port 1 is managed port.
2. The port that already set in ring network port, the VLAN port type must Trunk and take Tag, figure as 5.5.4.



(Figure 5.5.4)

8. Typical VLAN Configuration

Suppose switch's port 3, 4, 5 satisfied to the requirements as follows: port 3 can intercommunicate with Port 5, Port 4 can intercommunicate with Port 5, Port 3 can's intercommunicate with Port 4, How to set VLAN? (Not consider the configuration of other VLAN)

Let's analyse at first, port 3 can intercommunicate with Port 5, the port must belong to a same member of VLAN, the same, Port 4 can intercommunicate with Port 5, the port must belong to a same member of VLA, port 3 and port 4 belongs to different VLAN, figure as 5.5.5

1. Port 3's PVID: 2, Port 4's PVID: 3, Port 5's PVID: 4, port type are both Access.

2. Add VLAN2, VLAN3, VLAN4, the member is 3 and 5, 4 and 5, 3, 4 and 5. Port type is Untagged.



(Figure 5.5.5)

:

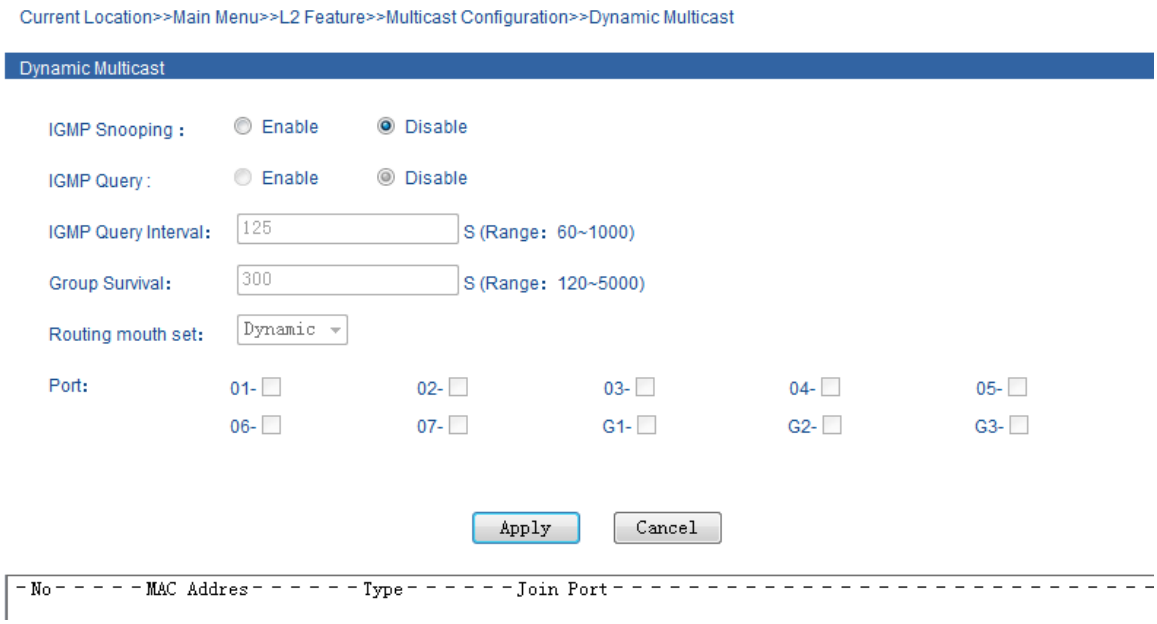
The switch VLAN maximum support 64 VLAN item, VID value range:1~4094
Managed port is the port that manage and configure switch, it must in a same VLAN as CPU port

5.5.2 Dynamic Multicast

IP host applies to join (or leave) multicast group to the neighboring router through IGMP (Internet Group Management Protocol) protocol. IGMP Snooping is multicast constraining mechanism. It manages and controls multicast group by snooping and analysis of the IGMP messages between the host and the multicast device.

Work process of IGMP Snooping: the switch snoops messages between the host computer and the router and tracks multicast information and the port applied for. When the switch snoops IGMP Report message sent from the host computer to the router, the switch would add this port to multicast forwarding list; when the switch snoops IGMP Leave message sent by the host computer, the router will send Group-Specific Query message of this port. If other hosts need this multicast, then the responses IGMP Report message. If the router doesn't get any reply from the hosts, the switch would delete this port from the multicast forwarding list. The router will send IGMP Query message regularly, the switch will deletes the port from the multicast forwarding list if it doesn't get the IGMP Report message from the host.

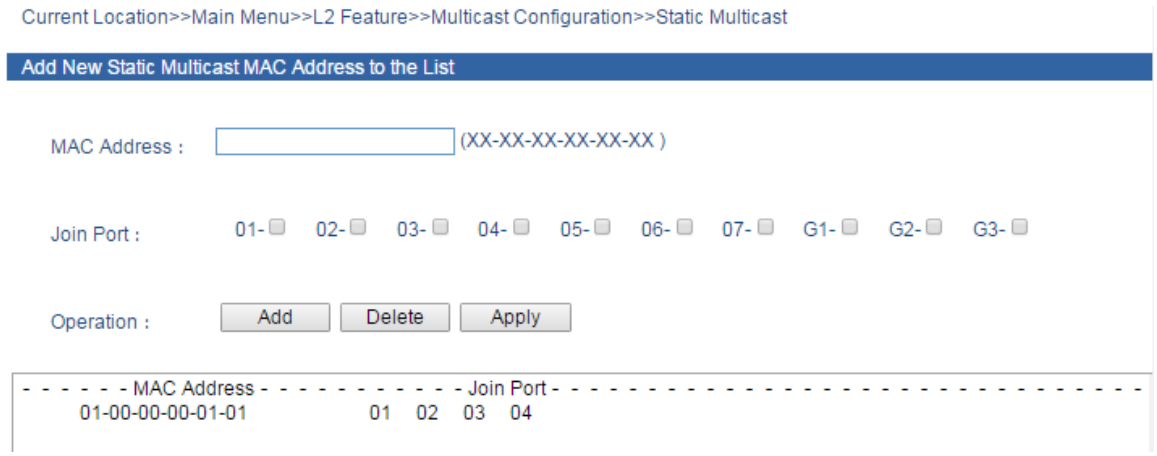
IGMP Snooping: Enable or disable IGMP snooping function
IGMP Query: Enable or disable IGMP query function
IGMP Query Interval: after enabling IGMP Query, the interval to check existing multicast members.
MAX Age: the maximum existing time of the members



(Figure 5.5.6)

5.5.3 Static Multicast FWD

The device provides the function of static MAC address forwarding. The destination address includes the data packets with static MAC address which will be transferred to the appointed port. Embedded forwarding address list in the switch chip can learn and support 2,000 MAC addresses and 15 multicast forwarding ports list. Static MAC address carry out transmit function, it did not accept the arrangement of aging.



(Figure 5.5.7)

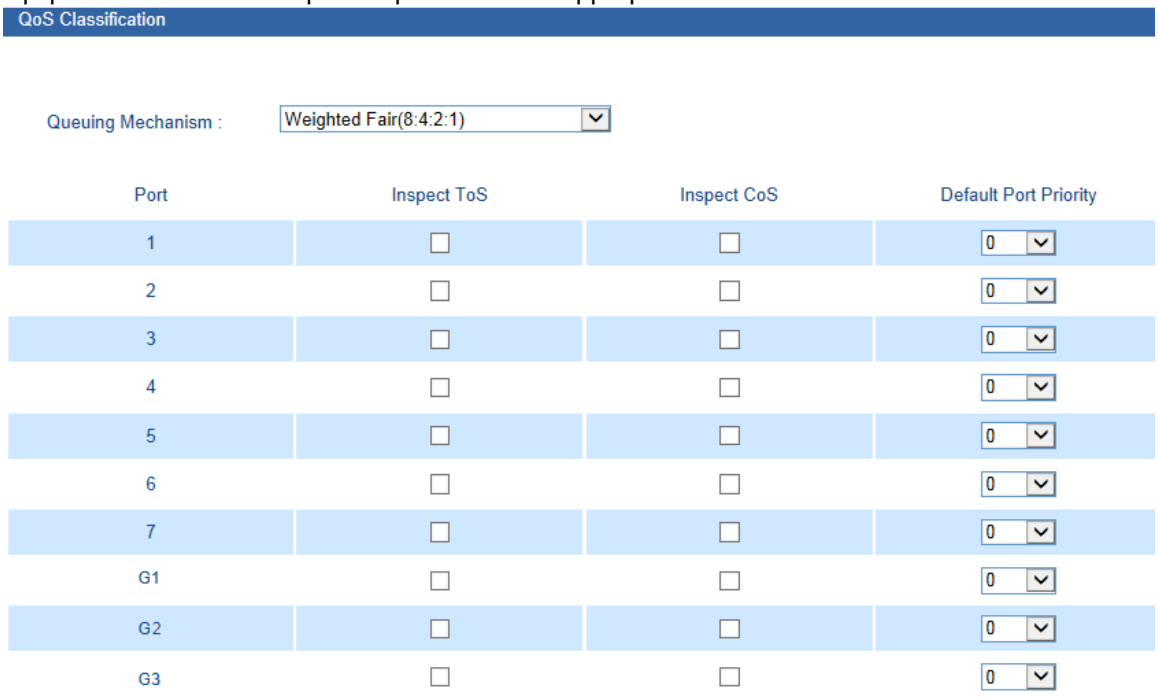
Button [Add/Edit], [Delete] were used for add/delete static Multicast MAC address. Join port is used to choice the transmit port of static MAC address, can point to 1 or more transmit port. Knock[Add], [Delete], static MAC address will be updated. For example, add MAC address “01-00-00-00-01-01” member is port 1, 2, 3, 4. Multicast MAC address is 1 of highest byte’s low byte. All none multicast address did not allow to add in this table and the format must according to XX-XX-XX-XX-XX-XX, did not have space or other illegal character, otherwise, will be display warning information.

1. This function has great impact on forwarding multicast, unless you can make sure the address is no problem, otherwise, please use it with caution.
2. The following multicast addresses are reserved for the device or protocol, please don't use them: 0180C20000xx, 01005E0000xx.
3. IGMP dynamic learning will not update the multicast address, static multicast forwarding is a kind of safety mechanism.

5.6 QOS

5.6.1 QOS Classification

QoS provides four internal queues, each queue supports four different levels of traffic, shorter persistence time of high-priority data packets in the switch, supports lower latency for certain delay-sensitive traffic. According to port ID, MAC address, 802.1p priority tags and IP TOS, equipment can be able to put the packets to an appropriate level.



(Figure 5.6.1)

Users can select the QOS priority queue mechanism, the queue mechanism in two ways: weighted Fair mode and strict mode.

5.6.2 COS

IEEE P802.1p is the name of a task group active during 1995–98 responsible for adding traffic class expediting and dynamic multicast filtering to the IEEE 802.1D standard. Essentially, they provided a mechanism for implementing Quality of Service (QoS) at the media access control (MAC) level. The group's work with the new priority classes and Generic Attribute Registration Protocol (GARP) was not published separately but was incorporated into a major revision of the standard, IEEE 802.1D-1998. It also required a short amendment extending the frame size of the Ethernet standard by four bytes which was published as IEEE 802.3ac in 1998.

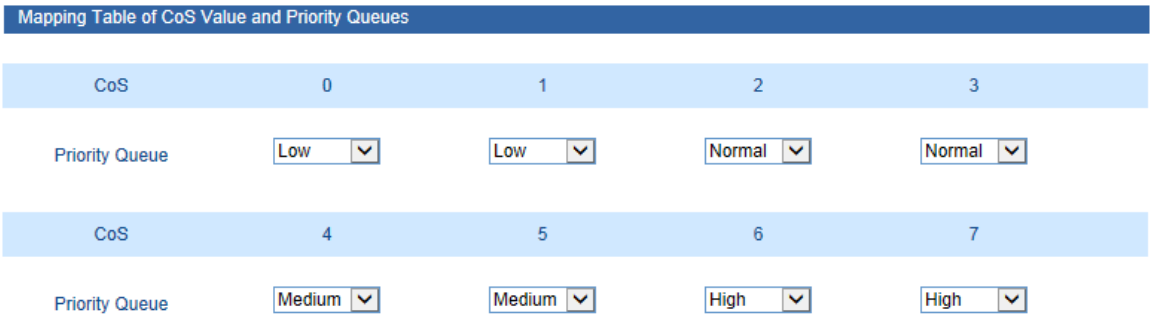
The QoS technique developed by the working group, also known as class of service (CoS), is a 3-bit field called the Priority Code Point (PCP) within an Ethernet frame header when using VLAN

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. Although this technique is commonly referred to as *IEEE 802.1p*, there is no standard or amendment by that name published by the IEEE. Rather the technique is incorporated into IEEE 802.1Q standard which specifies the tag inserted into an Ethernet frame.

Priority levels

Eight different classes of service are available as expressed through the 3-bit PCP field in an IEEE 802.1Q header added to the frame. The way traffic is treated when assigned to any particular class is undefined and left to the implementation. The IEEE however has made some broad recommendations:

PCP	Priority	Acronym	Traffic Types
1	0 (lowest)	BK	Background
0	1	BE	Best Effort
2	2	EE	Excellent Effort
3	3	CA	Critical Applications
4	4	VI	Video, < 100 ms latency and jitter
5	5	VO	Voice, < 10 ms latency and jitter
6	6	IC	Internetwork Control
7	7 (highest)	NC	Network Control



5.6.3 DSCP

DiffServ architecture provides each transport packets in the network are classified into different categories, classified information is contained in the IP packet header, DiffServ architecture using the first 6 bits of IP packet header TOS(Type of Service) to carry the packets' classified information. This definition is only for the lower 6 bits, one number does not exceed 63. This definition supports both IPv4 (ToS field) and IPv6 (Traffic Class field). DSCP has 64 priority values (0-63), the lowest priority 0 and the highest priority 63. In fact, the DSCP field is a superset of the IP precedence field, DSCP field definition is backward-compatible with IP precedence field.
So far, the defined DSCP with default DSCP, the value is 0; class selector DSCP defined as the backward-compatible with IP precedence, the value(8,16,24,32,40,48,56); Expedited Forwarding (EF), generally used for low latency service, the recommended value is 46 (101110); identified by forwarding (AF) defines four service levels, each service level has 3 down process, so spent 12 DSCP values ((10,12,14), (18,20,22), (26,28,30), (34,36,38)).
The priority value of the device (1-16) is defined as the lowest priority, as the first queue. Priority value (17-32) is defined as the second queue, the priority value (33-48) is defined as the third queue, the priority value (49-64) is defined as the fastest queue, the highest priority.

Mapping Table of ToS (DSCP) Value and Priority Queues

ToS(DSCP)	Level	ToS(DSCP)	Level	ToS(DSCP)	Level	ToS(DSCP)	Level
0x00(01)	Low	0x04(02)	Low	0x08(03)	Low	0x0C(04)	Low
0x10(05)	Low	0x14(06)	Low	0x18(07)	Low	0x1C(08)	Low
0x20(09)	Low	0x24(10)	Low	0x28(11)	Low	0x2C(12)	Low
0x30(13)	Low	0x34(14)	Low	0x38(15)	Low	0x3C(16)	Low
0x40(17)	Normal	0x44(18)	Normal	0x48(19)	Normal	0x4C(20)	Normal
0x50(21)	Normal	0x54(22)	Normal	0x58(23)	Normal	0x5C(24)	Normal
0x60(25)	Normal	0x64(26)	Normal	0x68(27)	Normal	0x6C(28)	Normal
0x70(29)	Normal	0x74(30)	Normal	0x78(31)	Normal	0x7C(32)	Normal
0x80(33)	Medium	0x84(34)	Medium	0x88(35)	Medium	0x8C(36)	Medium
0x90(37)	Medium	0x94(38)	Medium	0x98(39)	Medium	0x9C(40)	Medium
0xA0(41)	Medium	0xA4(42)	Medium	0xA8(43)	Medium	0xAC(44)	Medium
0xB0(45)	Medium	0xB4(46)	Medium	0xB8(47)	Medium	0xBC(48)	Medium
0xC0(49)	High	0xC4(50)	High	0xC8(51)	High	0xCC(52)	High
0xD0(53)	High	0xD4(54)	High	0xD8(55)	High	0xDC(56)	High
0xE0(57)	High	0xE4(58)	High	0xE8(59)	High	0xEC(60)	High
0xF0(61)	High	0xF4(62)	High	0xF8(63)	High	0xFC(64)	High



1. Port priority is the highest level, don't need to check other QoS attributes is discharged into the highest priority queue if you set the port priority as 1.
2. DSCP priority comes second, unless we do not set DSCP, therefore will check 802.1p priority, otherwise it will line up according to the DSCP settings.
3. As above, the three priorities can be used alone, can also be used at the same time, queuing according to the above rules.

5.7 Redundancy

5.7.1 Rapid Ring

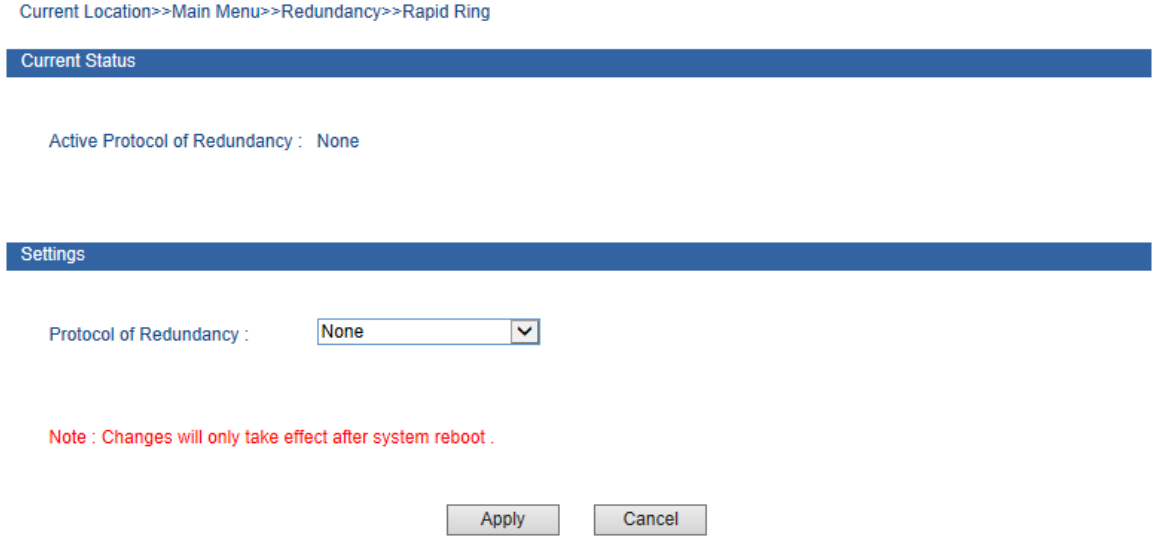
Ring technology provides auto-recovery and reconnection mechanism for broken network. When network is broken, it has link redundancy and self-recovery capability and self-recovery time is less than 20ms. Ring is the patented technology of 3onedata Co., Ltd. designed for industrial control network requiring high reliability.

Ring technology support maximum 250 pieces switches, in which the **Ring** its self-recovery time is <20ms.

Each port of IEM7110-3G can be Ring Port to connect other switches. When network is broken, relay for failure alarm will be activated. Redundant organization of **Ring** enable backup link to recover network instantly.

Self-developed patented technology for Ring network can realize the intelligent redundancy for industrial Ethernet switch, which can make you easily and conveniently establish redundant Ethernet, and can facilitate the quick recovery of any network section of automatic system

disconnected from the network. IEM7110-3G supports maximum 4 ring groups. Each group set up 2 ports as Ring Port and a port cannot belong to several rings.
Hello_time setting is time interval of sending detecting packet to network at regular time. The unit is ms. Its main purpose is to detect network connection. It sends a detecting packet to next door devices by CPU. If they receive it, then reply a confirm packet to ensure network connection is active. If this setting will influence self-recovery time, we suggest advanced users can use it.
Basic interface of Rapid Ring as shown in figure 5.7.1:

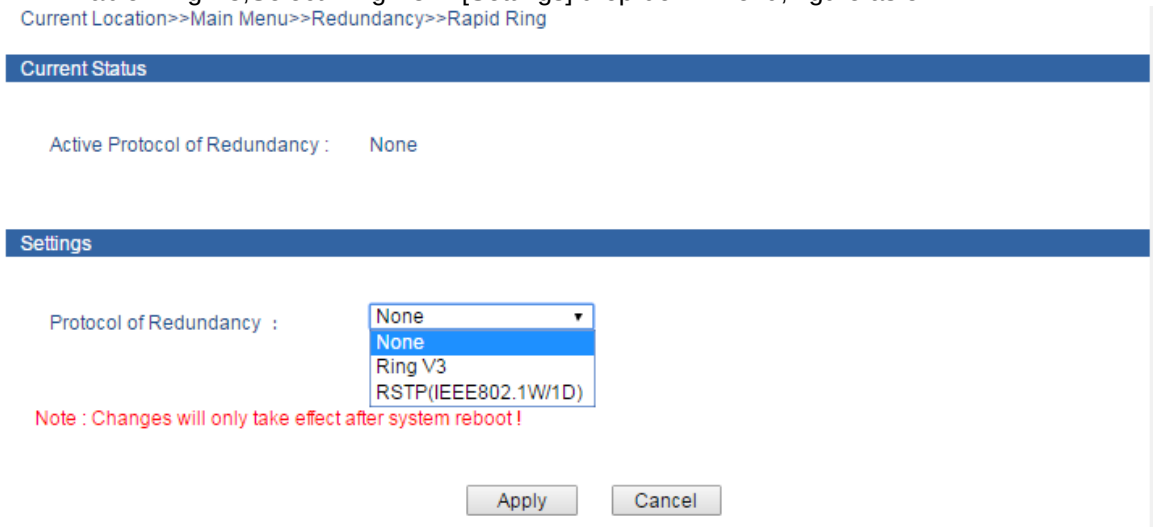


(Figure 5.7.1)

Initial interface display redundancy protocol is none, can configure it through [Settings]. There has 2 type Ring arithmetic: Ring V3 and RSTP), Ring V3 Single ring, coupling ring, chain ring and Dual_homing.

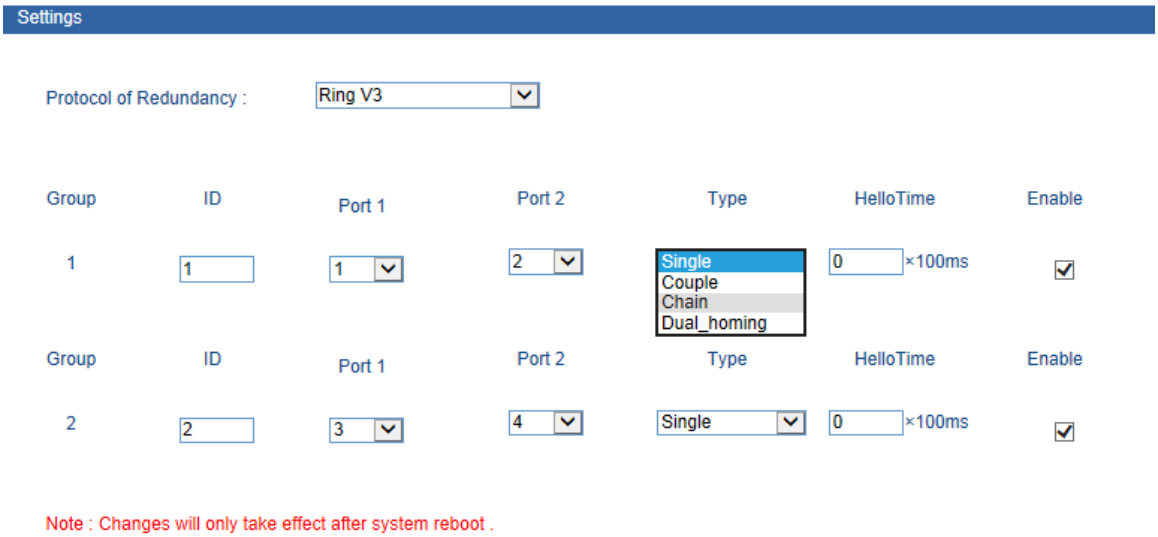
Method to enable Ring V3

1. Enable Ring V3,Select Ring V3 in [Settings] drop-down menu, figure as 5.7.2



(Figure 5.7.2)

2. After select Ring V3, Configuration interface is as figure 5.7.3, we can see Ring V3 support 4 different ring group: Single, Coupling, Chain and Dual_homing.



(Figure 5.7.3)

3. Enable Ring Group 1(or Group 2), and enter into Network ID(support 0-255 number only).Select Ring Port between Port 1 and Port 2.

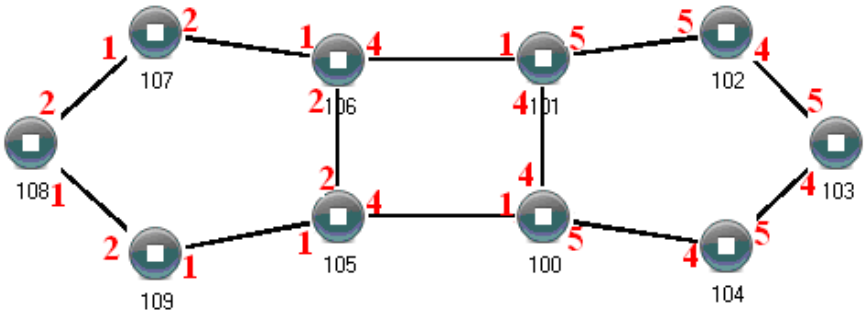
"Chain" refers to strengthen user's capability of making any type of redundant topological structure with flexibility by taking an advanced software technology. In fact, Chain is to cascade several switches already set up to Ring and both sides of chain access to network.

"Dual Homing" refers to a fact that two Rings connect the same switch. This type of configuration is ideal choice for centralized management of several Rings.

Method to enable Chain and Dual Homing is similar to that to enable Single Ring and Coupling Ring. It only needs to select corresponding items in [Type].

1. Method to enable Ring V3 coupling ring

The architecture of coupling ring as figure 5.7.4



Coupling(Figure 5.7.4)

Operation method:

1. Select Ring V3, enable ring group 1 and 2. (Hello_time can be disable, if enable, time of sending Hello packet could not be very fast, it will influence CPU operate speed);
2. Set 105, 106 device's ring port as port 1 and port 2 in ring group 1, network ID: 1, type: single ring. Set ring port as port 4 in ring group 2, Coupling ctrl port: 2, network ID: 3, type: coupling ring, figure as 5.7.5.

Group	ID	Port 1	Port 2	Type	HelloTime	Enable
1	1	1	2	Single	0 ×100ms	☑

Group	ID	Coupling Port	Coupling Ctrl Port	Type	HelloTime	Enable
2	3	4	2	Couple	0 ×100ms	☑

(Figure 5.7.5)

3. Set 100, 101 device's ring port as port 4 and port 5 in ring group 1, network ID: 2, type: single ring. Set ring port as port 1 in ring group 2, Coupling ctrl port: 4, network ID: 3, type: coupling ring, figure as 5.7.6.

Group	ID	Port 1	Port 2	Type	HelloTime	Enable
1	2	4	5	Single	0 ×100ms	☑

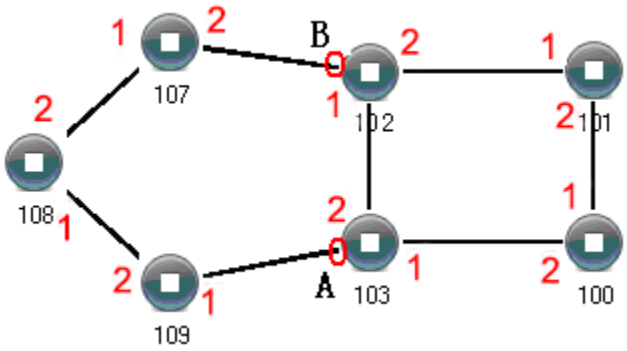
Group	ID	Coupling Port	Coupling Ctrl Port	Type	HelloTime	Enable
2	3	1	4	Couple	0 ×100ms	☑

(Figure 5.7.6)

4. Set 107, 108, 109 device's ring port as port 1 and port 2 in ring group 1, network ID: 1, type: single ring. Set 102, 103, 104 device's ring port as port 4 and port 5 in group 1, network ID: 2, type: single ring.
5. Connect 100-104 device's port 4 and port 5 with network cable. Connect 105-79 device's port 1 and port 2 with network cable, Connect 101 device's port 1 to 106 device's port 4 with network cable, Connect 100 device's port 1 to 105 device's port 4 with network cable.

2. Method to enable Ring V3 Chain ring

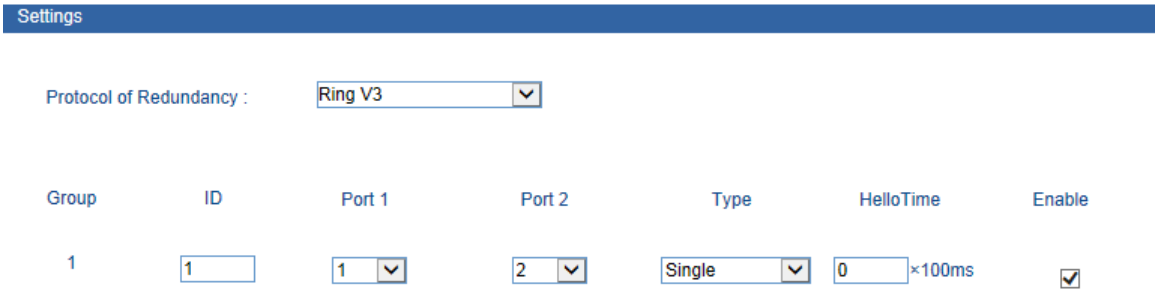
The structure of Chain ring as figure 5.7.7



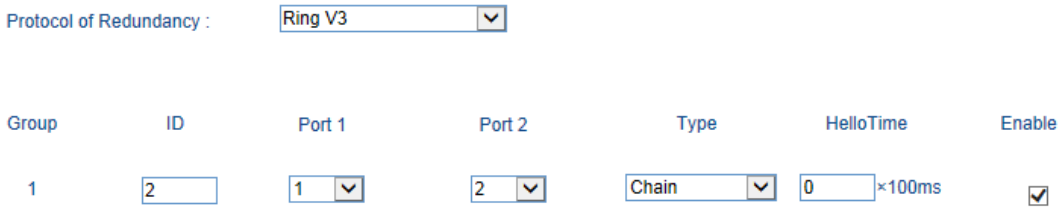
Chain (Figure 5.7.7)

Operating method:

1. Enable Ring Group 1: Hello time can be disable too, if it enable, time of sending Hello packet could not be very fast, or it will influence CPU dealing speed.
2. Set up Port 1 and 2 of Device 100, 101, 102 and 103 to be Ring Port in Ring Group 1, Network ID is1, Ring Type is Single; as shown in figure 5.7.15. Set up Port 1 and 2 of Device 107, 108 and 109 to be Ring Ports in Ring Group 2, Network ID is 2. Ring Type is Chain; as shown in figure 5.7.9.



(Figure 5.7.8)



(Figure 5.7.9)

3. Use a wire to connect Port 1 and 2 of Device 107-109 in turn to make a chain. Use a wire to connect Port 1 and 2 of Device 100-103 in turn to make a Single Ring, Then use a wire to connect Port 2 of Device 107 and Port 1 of Device 109 to normal port of Device 102 and 103. Chain is finished.

1. Port cannot be trunking setting when it is already Ring port.
2. In the same single ring, identity must be consistent, otherwise it will not built a ring and cannot communicate.
3. All ring ports in the VLAN settings must be TRUNK tagged VLAN member, otherwise cannot communicate.
4. To form tangent ring or other complex rings, should pay attention to the ring identity whether is it consistent, different single ring identification must be different.

5.7.2 RSTP

The first spanning tree protocol was invented in 1985 at the Digital Equipment Corporation by Radia Perlman. In 1990, the IEEE published the first standard for the protocol as 802.1D, based on the algorithm designed by Perlman. Subsequent versions were published in 1998 and 2004, incorporating various extensions.

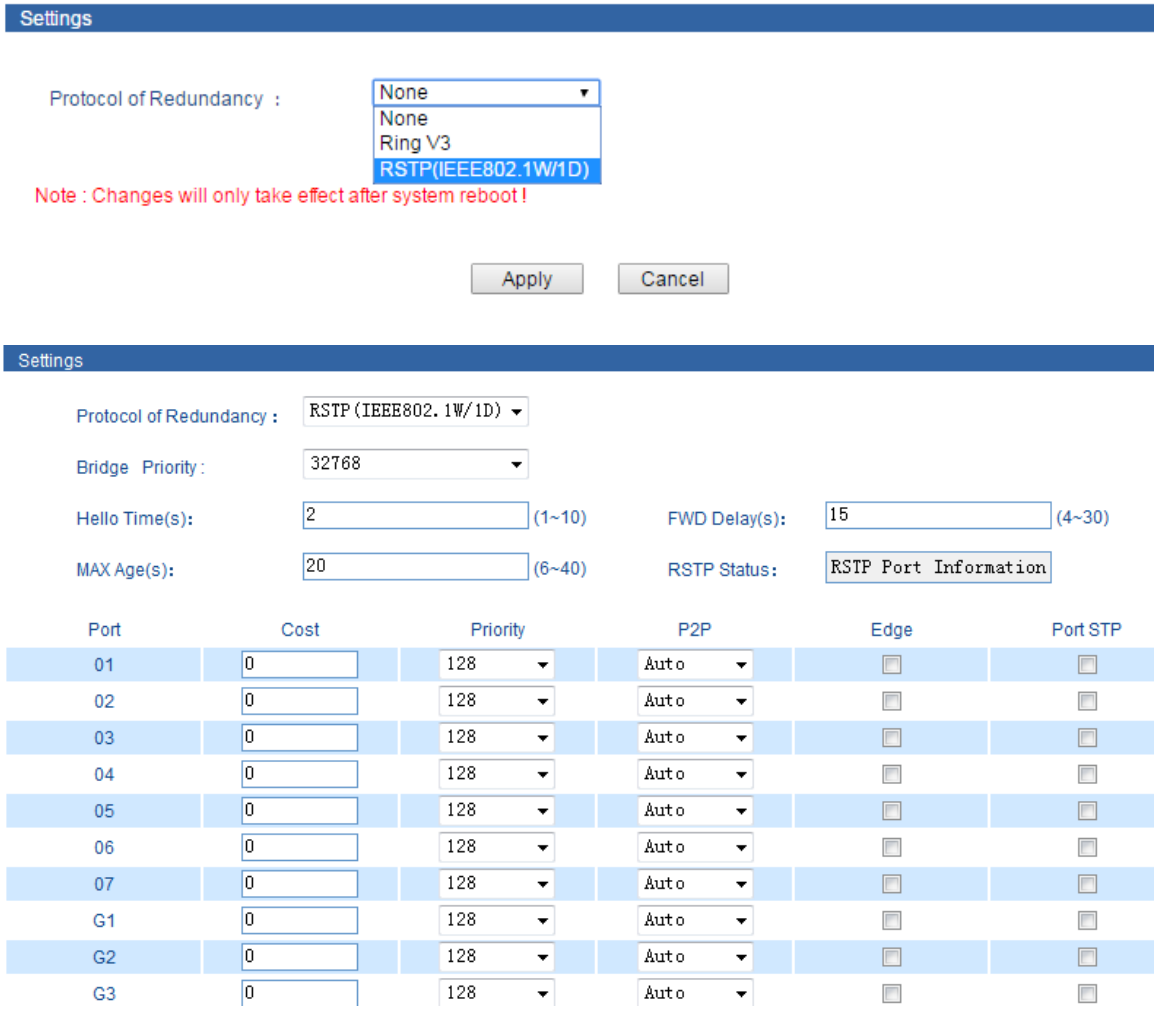
Although the purpose of a standard is to promote interworking of equipment from different vendors, different implementations of a standard are not guaranteed to work, due for example to differences in default timer settings. The IEEE encourages vendors to provide a "Protocol Implementation Conformance Statement", declaring which capabilities and options have been implemented, to help users determine whether different implementations will interwork correctly.

Also, the original Perlman-inspired Spanning Tree Protocol, called DEC STP, is not a standard and differs from the IEEE version in message format as well as timer settings. Some bridges implement both the IEEE and the DEC versions of the Spanning Tree Protocol, but their interworking can create issues for the network administrator, as illustrated by the problem discussed in an on-line Cisco document.

Rapid Spanning Tree Protocol

In 2001, the IEEE introduced Rapid Spanning Tree Protocol (RSTP) as 802.1w. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this. RSTP was designed to be backwards-

compatible with standard STP.While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within 3 × Hello times (default: 3 times 2 seconds) or within a few milliseconds of a physical link failure. The so-called Hello time is an important and configurable time interval that is used by RSTP for several purposes; its default value is 2 seconds. Standard IEEE 802.1D-2004 incorporates RSTP and obsoletes the original STP standard Select RSTP function in rapid ring network interface as follows:



（Figure 5.7.10）

Rapid Spanning Tree of concepts:

Switch priority: As the bridge priority, the bridge priority and bridge MAC address combine bridge ID, the smallest ID Bridge will become the root bridge on the network.

Polling interval: how often send BPDU packet at one time.

Forwarding delay: the port state of switch remain a forward delay time over the listening and learning.

The maximum aging time: after one switch receive a packet from other switches, how long the packet is valid.

The port concepts of RSTP**:**

Port path overhead: port link cost compared with port priority and port ID.

Port priority: port priority among the net bridge compared with port priority and port ID

Point to point network connection: directly connect with switches port each other, the port is P2P, which adopted negotiation mechanism, RSTP can achieve port state rapid conversion RSTP

Directly connect terminal: connect the edge of network switch with terminal devices with **configuration Edge port**, which can achieve port state rapid conversion without the processing Discarding, Learning, and Forwarding
Don't join RST structure: don't participate in RSTP running

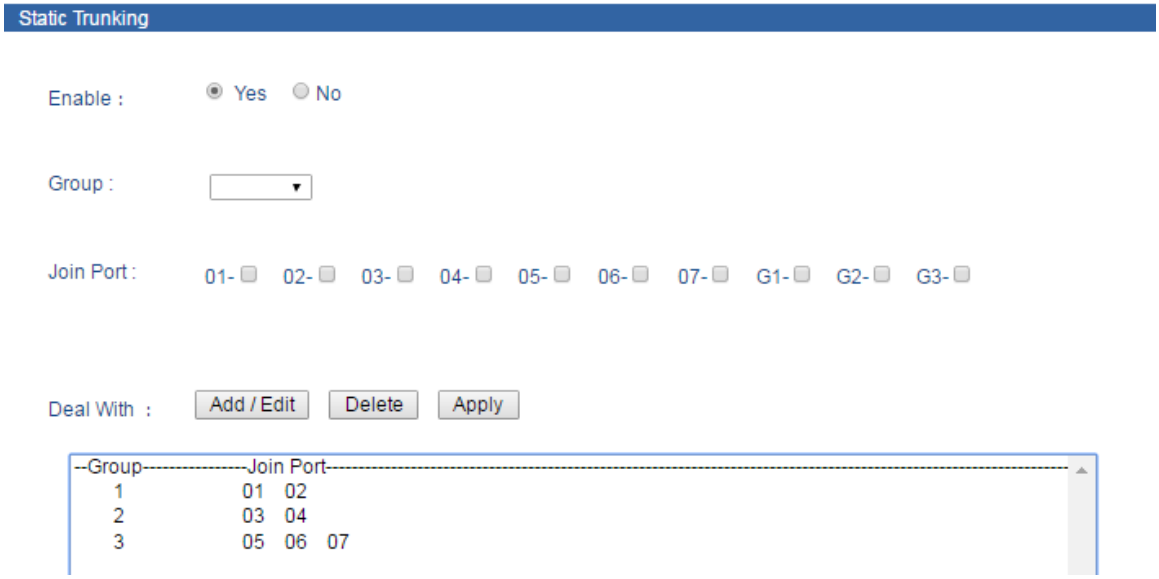
RSTP switch port states:

1. **Blocking**- A port that would cause a switching loop if it were active. No user data is sent or received over a blocking port, but it may go into forwarding mode if the other links in use fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state. Prevents the use of looped paths.
2. **Listening**- The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state. It does not populate the MAC address table and it does not forward frames.
3. **Learning**- While the port does not yet forward frames it does learn source addresses from frames received and adds them to the filtering database (switching database). It populates the MAC Address table, but does not forward frames.
4. **Forwarding**- A port receiving and sending data, normal operation. RSTP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.

The example of Configuration: The priority of network bridge is "32768", If there did not have network ID less than itself, itself is root network bridge. There did not have same network ID in network. Every 2 seconds, the network bridge will transmit BPDU message to all appoint port. If did not receive BPDU message more than 20 seconds, it realized port invalid, will calculate the status of network bridge again. Each status exchange for each other if need to transmit, need to wait 15 seconds.

5.7.3 Port Trunking

In telecommunications, trunking is a method for a system to provide network access to many clients by sharing a set of lines or frequencies instead of providing them individually. This is analogous to the structure of a tree with one trunk and many branches. Trunking, is set by the configuration software, the two or more physical ports get together into a logical path to increase the bandwidth between the switch and the network node. Trunking is a packaging technology, it is a peer to peer link, both ends of the link are switches, it can be a switch and a router, and also can be a host, switch or router. Based on port trunking function that allows between two or more ports between switches, switches and routers, hosts the switch or router connected in parallel to provide for the simultaneous transmission of higher bandwidth and greater throughput, significantly entire network capacity. Trunking is more economical to increase the bandwidth between the switch and network device, such as servers, routers, workstations, or other switches. Trunking function is to integrate more than one physical port (typically 2-4) to a logical channel.



(Figure 5.7.11)

Device supported 3 trunking group, operate method: choice apply, choice the port need to trunking the port list, Choice setting, available after reboot. If the port already set to Ring port, it cannot set to trunking port. Each trunking group at least have 2 port member, at more 4. 1 port cannot exit in 2 trunking group.

1. The trunking groups require all the attributes can be the same, including speed, duplex, STP state etc.
2. If you do not confirm the STP state, please disable RSTP function, or close others, leaving only one STP channel.
3. Port 1 as the system reserved, cannot be used as trunking.
4. The ports of having been set to the port aggregation that cannot be set to ring ports.

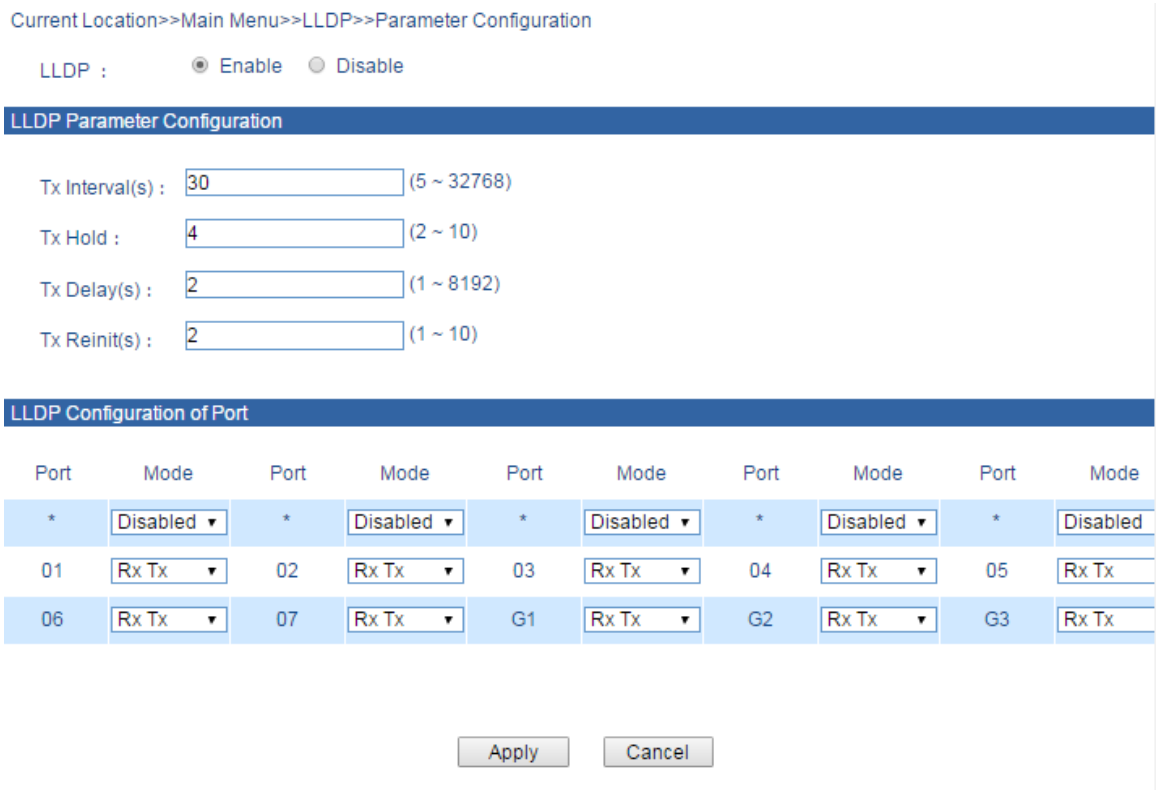
5.8 LLDP

5.8.1 Parameter Configuration

LLDP is a second layer topology discovery protocol, the basic principle is: network equipment to the adjacent equipment issued its notice of state information, and each port of all equipment are stored with their own information, if a local device state changes, also can with its directly connected neighbor devices to send updated information to that neighbor devices will be the information stored in the standard SNMP-MIB library. Network management system can query from the SNMP-MIB Library of the current second layer connection. It should be noted that LLDP is only a remote device status information discovery protocol, it can't complete the network device configuration and port control and other functions.

Configuration item	meaning
Disable	The switch will not send the LLDP message, and will reduce the LLDP message received from the neighbor.
Enable	The switch will send the LLDP message, which will analyze the LLDP message received from the neighbor.
TX interval	The switch status is not changed, the device periodically to the neighbor nodes to send LLDP packets, the interval time is called to send LLDP message **interval**.
RX	Switch will not send out the LLDP information, but the information from the vicinity of the unit LLDP analysis.

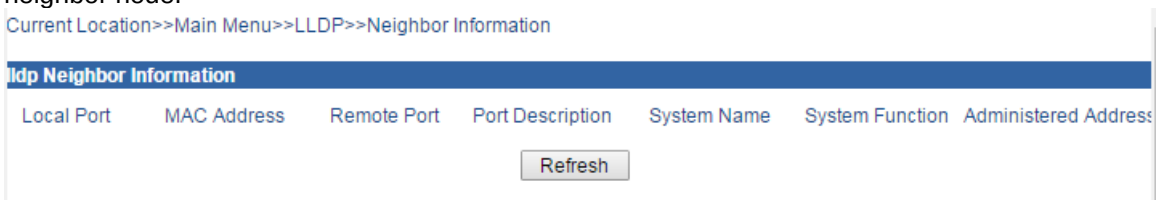
TX	Will reduce the LLDP information received from the neighbors, but will send LLDP information.



(Figure 5.8.1)

5.8.2 Neighbor Information

LLDP management address is the address of the network management system identification and management. Management address can clearly identify a device, it is conducive to the network topology, network management, network management. The management address is encapsulated in the Management Address TLV field of the LLDP message and is sent to the neighbor node.



(Figure 5.8.2)

5.9 Access Control

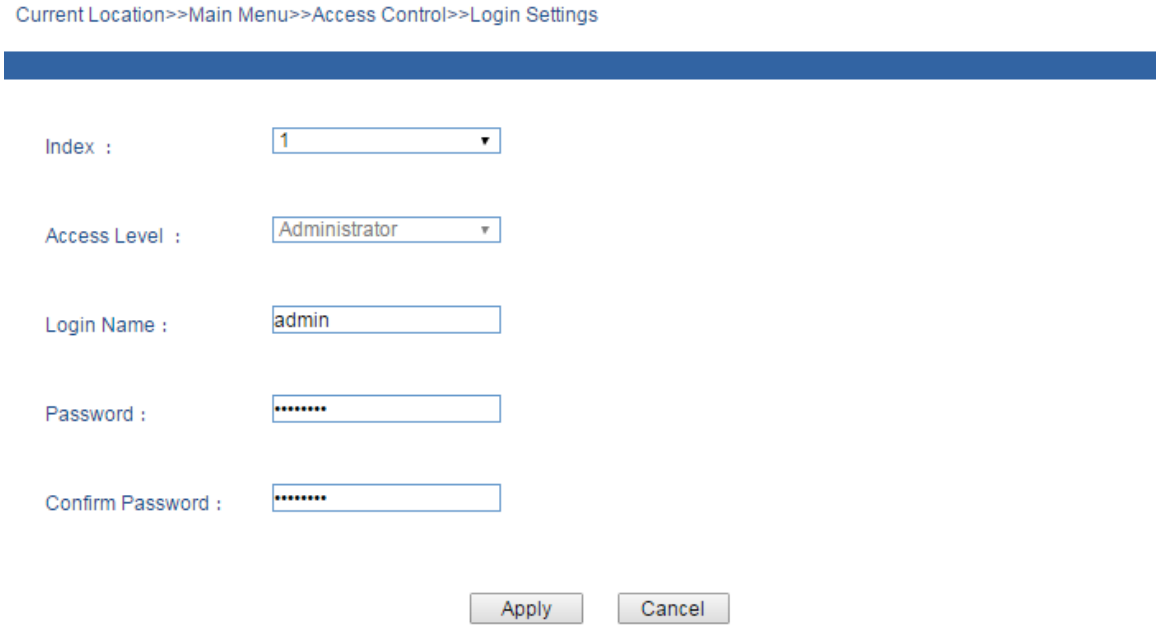
5.9.1 User Password

Enterprise usually required two different person to monitor device and manage system/ network. The authority need to separate. Monitor person was in charge of monitor work, system/network person was in charge of system/work management. The switch provided classification management: Administrator authority and Observer authority. Observer just had authority to check the status of switch. Administrator had the authority to configure the parameters of the switch.

Index

User index indicates which group of users. There are three user indexes in drop-down list.

Access level:
Administrator: have the right to check and configure all settings
Observer: have the right to check all settings merely
Login name
The identity of visitor with the letter combination is no more than 16 bytes
Password:
Visitor use password, user authority allows the letter combination no more than 16 bytes
Confirm password
Make sure the last time input password is correct.



(Figure 5.9.1)

5.10 Remote monitoring

5.10.1 SNMP

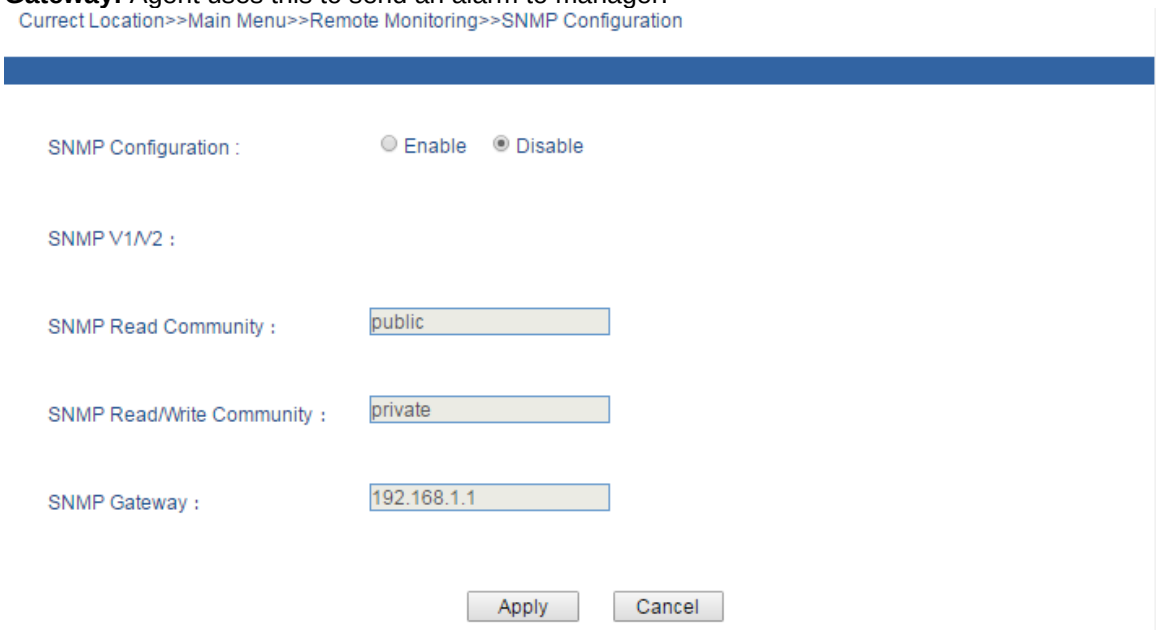
1. Introduction of SNMP
SNMP (Simple Network Management Protocol) is an internet-standard protocol for managing devices on IP networks. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

2. Work Mechanism of SNMP
SNMP includes 2 parts: NMS and Agent:
NMS: Network Management Station. Software runs on the manager. The common management platforms are "Quid View", "Sun Net Manager" and "IBM Net View". Agent is the software of the server running in the network device.
NMS can send "Get Request", "Get Next Request" and "Set Request" message to Agent. After Agent gets those messages, it will read or write according to the message type to create Response message and send the Response message back to NMS. Agent will also send Trap message to NMS when the device is abnormal.

3. SNMP Version
Currently SNMP Agent of the device supports SNMP V3 and it is also compatible with SNMP V1and SNMP V2C. It is authenticated by user name and password in SNMP V3.
SNMP V1 and SNMP V2C adopt authentication of Community Name. The SNMP message of the community name which is not authenticated will be discarded. SNMP community name defines

the relationship of SNMP NMS and SNMP Agent. User can choose the following one or more features related to community name.
1. Defines MIB view of community name.
2. Setup visit privilege of MIB objective is Write or Read. Community name with Read privilege can check the device information only. Community name with Write privilege can configure the device.
3. Setup appointed basic visit control list of the community name.
IEM7110-3G supports SNMP V1/V2c. Both SNMP V1 and V2c use public character strings for match authentication.
SNMP usually uses UDP Port 161(SNMP) and 162 (SNMP-traps) based on TCP/IP protocol. SNMP protocol agent is existed in network device. MIB (information specific to the device) is uses as device connector. These network devices can be monitored or controlled through the agent. When trap event happens, a message is transmitted by SNMP Trap, an available trap receiver can get this trap information.

SNMP supports 3 kinds of basic operating in total:
Read: Manager can use this to get some variable value of Agent.
Read/Write: Manager can use this to set up some variable value of Agent.
Gateway: Agent uses this to send an alarm to manager.



(Figure 5.10.1)

5.10.2 Relay Alarm

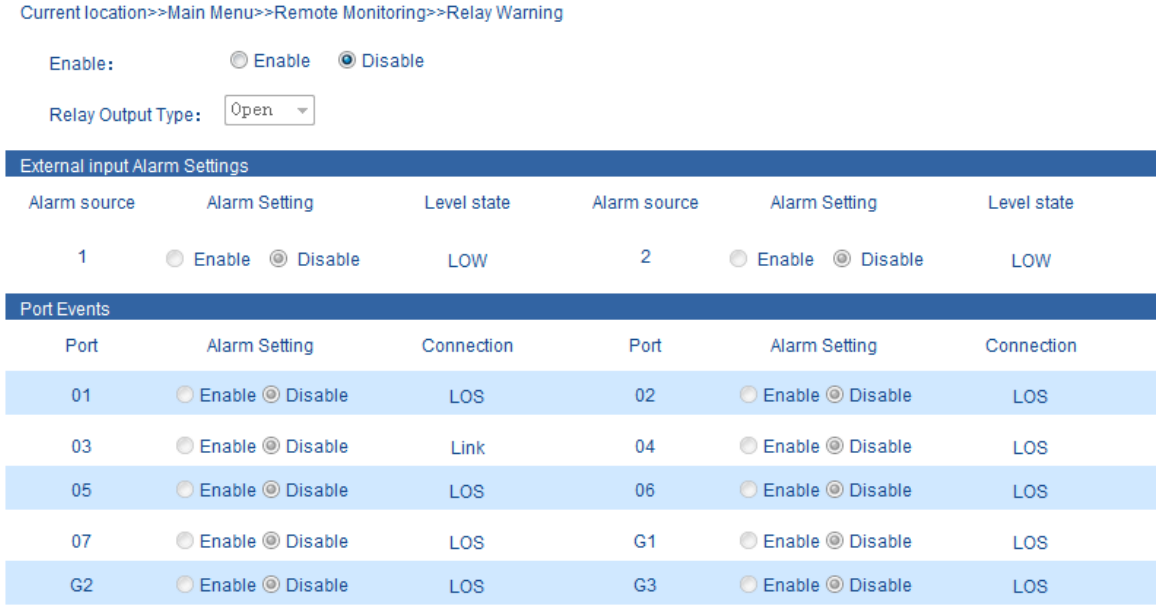
Warning had 2 types: Power alarm, port alarm. Main function: once the devices were in unusual status, can inform administrator in time and repair the status of device quickly, can avoid more lose
Relay warning input type: Close/Open. Once select close, the light will be bright when have alarm. Relay will be in open status.

Power alarm

IEM7110-3G provided dual DC power supply (single power supply did not have alarm), if one power supply had problem, another will support power supply immediately, dual power supply hot back-up. Select to enable power alarm, if power supply was in unusual status, device will send alarm signal, inform power supply work unusual.

Port Alarm

Alarm when port disconnect. Enable port alarm, if port was in unusual status (Connect or disconnect), device will output a signal, inform the device work unusual.



(Figure 5.10.2)

The product supports two channel alarm input and output.

ALARM_IN[1:2] Default level	Relay output default state	ALARM_IN[1:2] level	ALARM_OUT2 level state	Dynamic relay status	ALARM_OUT1 level state
L	open	L	H	close	L
		H	L	open	H
L	close	L	L	open	L
		H	H	close	H

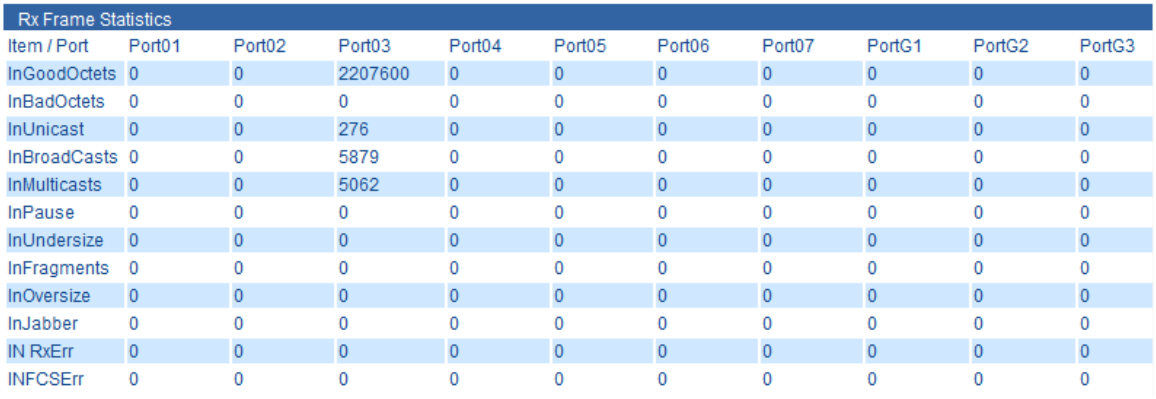
In default status, the type of relay output is open, the alarm light is OFF, have no alarm, relay always open.
When the device have alarm, the light is ON, relay close

5.11 Traffic Statistics

The function of traffic Statistics is to calculate the data packets in a fixed time, included transmit and receive data packets.

Operate method: Start to calculate after select clear

5.11.1 RX frame statistics



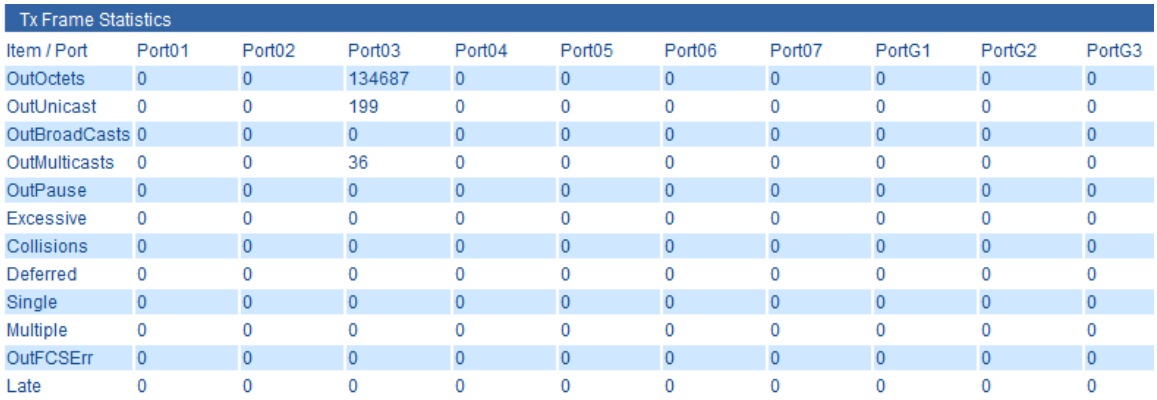
Rx Frame Statistics

Item / Port	Port01	Port02	Port03	Port04	Port05	Port06	Port07	PortG1	PortG2	PortG3
InGoodOctets	0	0	2207600	0	0	0	0	0	0	0
InBadOctets	0	0	0	0	0	0	0	0	0	0
InUnicast	0	0	276	0	0	0	0	0	0	0
InBroadCasts	0	0	5879	0	0	0	0	0	0	0
InMulticasts	0	0	5062	0	0	0	0	0	0	0
InPause	0	0	0	0	0	0	0	0	0	0
InUndersize	0	0	0	0	0	0	0	0	0	0
InFragments	0	0	0	0	0	0	0	0	0	0
InOversize	0	0	0	0	0	0	0	0	0	0
InJabber	0	0	0	0	0	0	0	0	0	0
IN RxErr	0	0	0	0	0	0	0	0	0	0
INFCSErr	0	0	0	0	0	0	0	0	0	0

(Figure 5.11.1)

Frame Name	Description
InGoodOctets	Number of valid received data byte (including FCS)
InbadOctets	Number of invalid received data byte (including FCS)
InUnicasts	Valid Unicast Data Frames
InBroadcasts	Valid Broadcast Data Frames
InMulticasts	Valid multicast excluding InBroadcasts
InPause	Number of Valid Flow Control Pause frames
InUndersize	Number of valid data frames less than 64 bytes
InFragments	Fragments (less than 64 bytes, invalid FCS)
InOversize	Valid oversized frames received (more than 1518 or 1522)
InJabber	Invalid oversized frames received (more than 1518 or 1522)
InRxErr	Receive error frame
InFCSErr	Number of FCS checkout error frames (completed data)

5.11.2 TX frame statistics



Tx Frame Statistics

Item / Port	Port01	Port02	Port03	Port04	Port05	Port06	Port07	PortG1	PortG2	PortG3
OutOctets	0	0	134687	0	0	0	0	0	0	0
OutUnicast	0	0	199	0	0	0	0	0	0	0
OutBroadCasts	0	0	0	0	0	0	0	0	0	0
OutMulticasts	0	0	36	0	0	0	0	0	0	0
OutPause	0	0	0	0	0	0	0	0	0	0
Excessive	0	0	0	0	0	0	0	0	0	0
Collisions	0	0	0	0	0	0	0	0	0	0
Deferred	0	0	0	0	0	0	0	0	0	0
Single	0	0	0	0	0	0	0	0	0	0
Multiple	0	0	0	0	0	0	0	0	0	0
OutFCSErr	0	0	0	0	0	0	0	0	0	0
Late	0	0	0	0	0	0	0	0	0	0

(Figure 5.11.2)

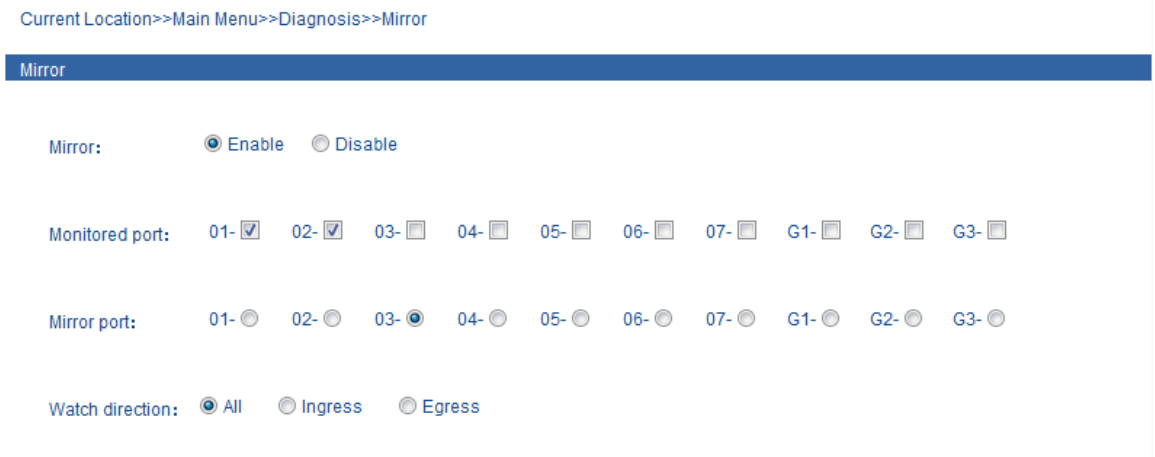
Frame Name	Description
OutOctets	Number of output bytes(including FCS)
OutUnicasts	unicast data frames output
OutBroadcasts	Broadcast data frames output
OutMulticasts	Multicast data frames output
OutPause	Number of output flow control pause frames
Excessive	Number of unsuccessful output frames(trying more than 16 times with

	half duplex flow control)
Collisions	Number of collision in output
Deferred	Number of successful output frames(the receiver is busy, but It sends successfully after a delay)
Single	Number of successful output frames(collision happens in 1 time only)
Multiple	Number of successful output frames(collision more than 1 time)
OutFCSErr	Output invalid FCS frame
Late	Number of collision after frames output 64 bytes

5.12 Diagnosis

5.12.1 Mirror

Port mirroring refers to copy data from the port which need to be monitored to appointed monitoring port for analysis and monitoring. Ethernet switch supports many-for-one mirror which means messages from several ports can be copied to a monitored port. User can appoint the direction of monitored message, such as only monitoring of transmitted messages of appointed port. The device configures port mirroring function through port mirroring group. Each group includes a monitored port and a group of mirror ports. Total bandwidth of mirroring is not more than that of monitored port. It is good to monitor and manage its internal network data when using port mirroring in a company. It is also good to locate the failure when network is cut up.
Example as figure: Port 3 collect all of the data from port 1 and port 2



(Figure 5.12.1)

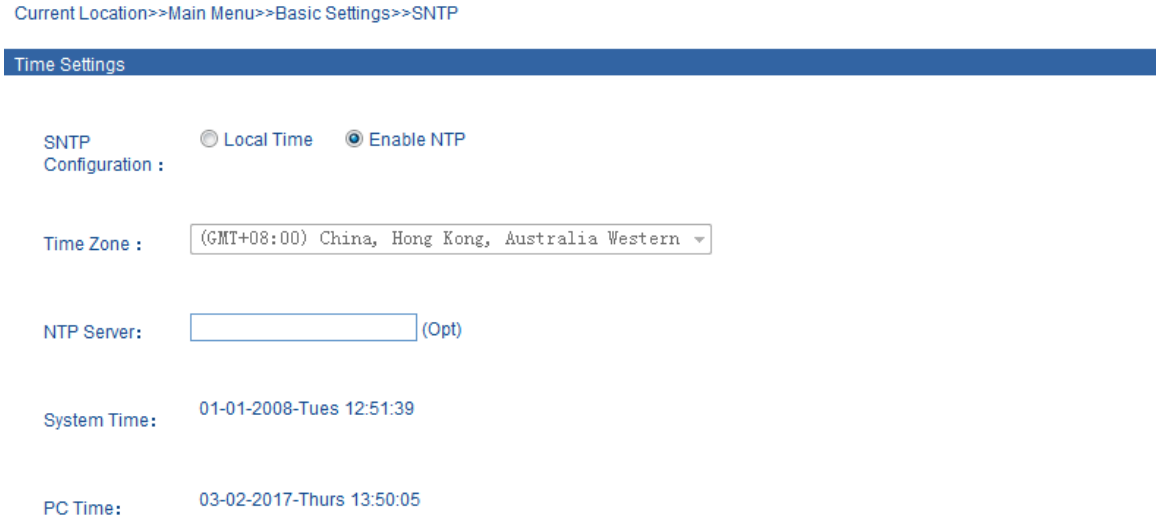
Mirror Port
It defines a group of ports which are needed to be monitored. The device collects data from these ports.
Monitored Port
It defines a group of ports which are used to monitor other ports. The device outputs the data through these ports.
Watch direction
This parameter indicates the direction of the data. It includes 3 kinds of choices: "All", "Ingress" and "Egress".

1. This function is not often used. Otherwise other port-based higher management function like RSTP,IGMP SNOOPING
2. Port mirroring function can only deal with the normal FCS packets. It cannot deal with error data frames.

5.13Basic settings

5.13.1 SNTP

NTP (Network Time Protocol) is a protocol and software implementation for synchronizing the clocks of computer systems over packet-switched data network. It provides coordinated universal time including scheduled adjustments. No information about time zones or daylight saving time is transmitted; this information is outside its scope and it must be obtained separately.



（Figure 5.13.1）

Local Time
To configure the time by hand to undated the time of the device

Enable NTP
To update the time of the device by using NTP protocol

Time Zone
Standard time zones could be defined by geometrically subdividing the Earth's spheroid into 24 lines. The local time in neighboring zones would differ by one hour. And the variation in the position of the sun from one end of the zone to the other (east vs. west) would be at most 1/24 of the sky. Most of the 25 nautical time zones (specifically UTC−11 to UTC+11) are indeed defined this way, and are 15° of longitude wide. An hourly zone in the central Pacific Ocean is split into two 7.5°-wide zones (UTC±12) by the 180th meridian, part of which coincide with the International Date Line.

NTP Server
It provides host name or IP address of NTP timing.

System Time
Device time

PC Time
Visitor's own PC, display and switch itself does not matter.

1. NTP server can be empty, the device using the own server update, but must use the correct DNS and gateway.
2. NTP server must have a valid host name or a valid IP address.
3. Only the Administrators have permission to manually configure the device time.
4. Time zones must be configured; either uses the "local time" or "NTP time.
5. The configuration of the NTP server or PC can cause the display is not normal, you can change the time display format to adjust the display.

5.13.2 Network & Reboot

Device configuration support two modes, DHCP and static IP address, can get the device's IP address via client when the DHCP function is running, if you need NTP that need to connect internet, please enter the available and correct gateway and DNS address.

IP Address

IP address is a address of 32 bits length which is assigned to the device on the internet. The IP address consists of two fields: the network number field (net-id) and the Host ID field (host-id). For can conveniently manage IP address, IP addresses are divided into five categories. As blow:

Network type	Address range	Available IP network range
A	0.0.0.0～126.255.255.255	1.0.0.0～126.0.0.0
B	128.0.0.0～191.255.255.255	128.0.0.0～191.254.0.0
C	192.0.0.0～223.255.255.255	192.0.0.0～223.255.254.0
D	224.0.0.0～239.255.255.255	Non
E	240.0.0.0～246.255.255.255	Non
Others	255.255.255.255	255.255.255.255

A, B, C class address is unicast address; D class address is multicast address; E class address is reserved to prepare for the future for special purposes.

IP address using dotted decimal. Each IP address is represented as four decimal integers separated by decimal points, each integer corresponds to a byte, such as, 10.110.50.101.

Subnet Mask

Mask is corresponding 32 bits number of IP address. Some are 1, the others are 0. These 1 and 0 can be combined arbitrary in principle, but the first continuous bits are 1 when designing subnet mask. IP address can be divided into 2 parts by subnet mask: subnet address and host address. 1 in IP address and subnet corresponds to subnet address, other bits are host address. A type of address corresponding mask is 255.0.0.0; mask of B type address is 255.255.0.0; mask of C type address is 255.255.255.0.

Default Gateway

Default gateway in the host PC is generally called default route. Default route refer to a kind of router that destination address of IP data packet will choose when it don't find other existing route. All data packets of destination address which don't exist in the list of router will choose default route.

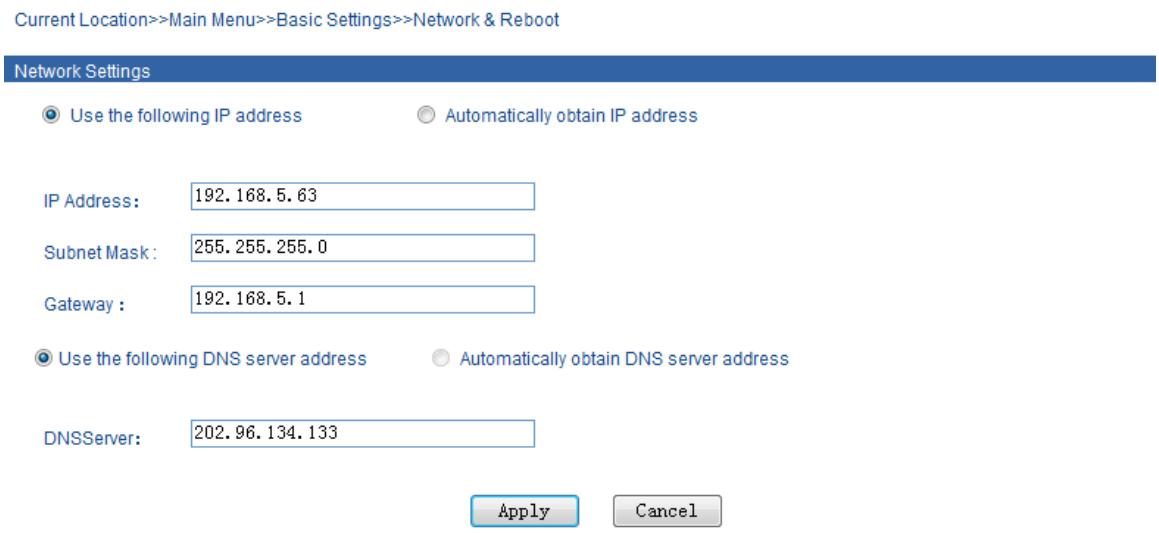
DNS Address

DNS (Domain Name Server) is for us to analyze domain to IP address of the Internet. If our equipment needs to access a host, you need to use this server to resolve an IP address.

Device reboot

Can reboot the switch remote. Knock [Basic settings/Network&reboot] menu, Enter into reboot interface, Figure as 5.13.2.

Knock<Reboot> button, after confirmation, device will be reboot. After 20 seconds, know menu bar and back to WEB managed login interface.

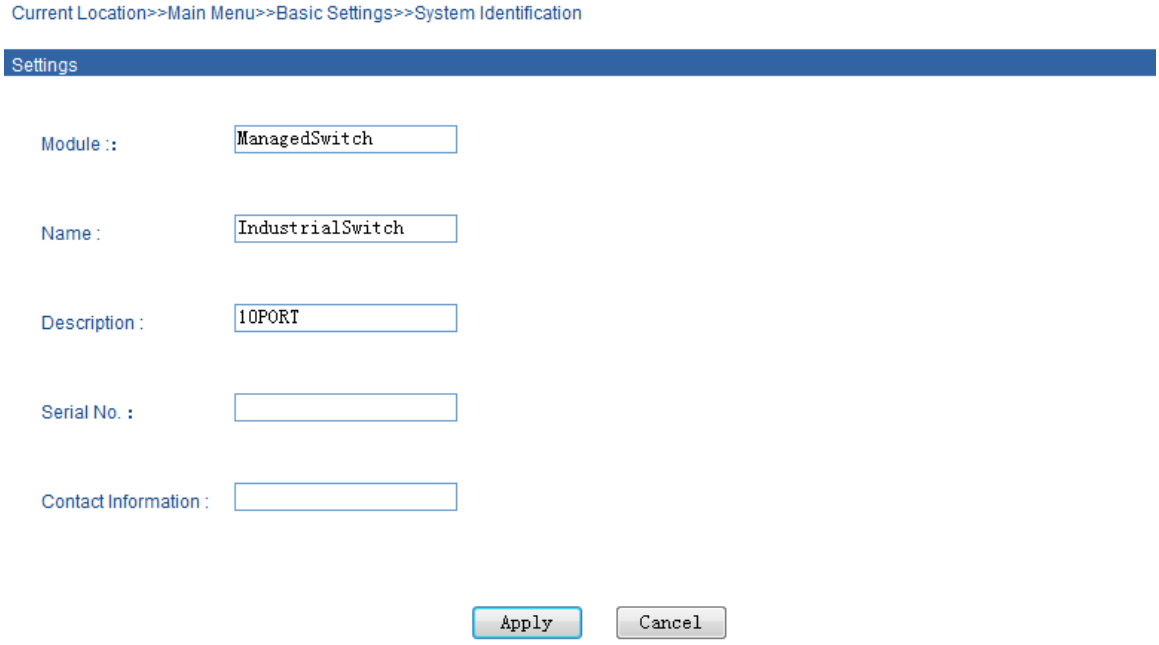


(Figure 5.13.2)

Before reboot, please save all configurations. Otherwise, all configuration will be lost

5.13.3 System identification

In System Identification interface we can see Model, Name, Description, Serial NO., and Contact Information. We can modify these above items by this function. It will take effect after system reboot. Figure 5.13.3 is initial device settings of the switch.



(Figure 5.13.3)

Module
To give a module to each device, length is not more than 16 bytes.

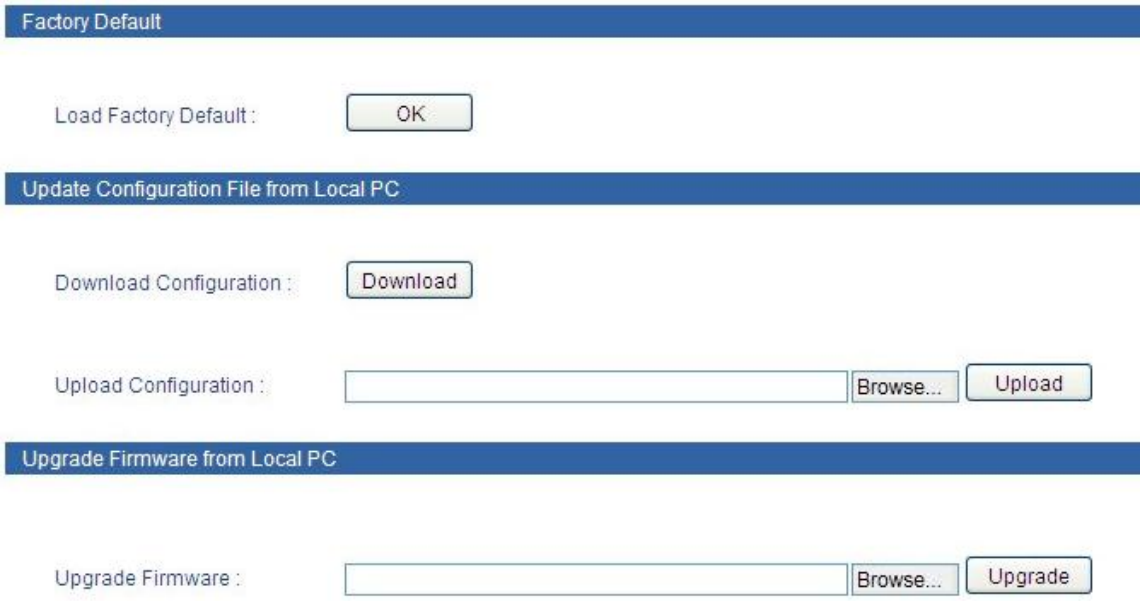
Name
To give a name to each device, length is not more than 16 bytes.

Description
A brief description to a device, the length is not more than 16 bytes.

Serial No.
Display Installation Location of the device, the length is not more than 30 bytes.

5.13.4 System File Upgrade

The menu included 5 functions: Factory default, Download Configuration, up load configuration, upgrade firmware.



(Figure 5.13.4)

1. Factory Default
If you know the IP address of the device, user name and password:
Use IE to login Web interface.
Click "System Management"
Click "System File Update"
Choose "Factory Default"
Click "OK"
Notice: the IP address will be "192.168.1.254".
Open a new interface, input "192.168.1.254" to make a new configuration.

2. Download Configuration
If you know the IP address of the device, user name and password:
Use IE to login Web interface.
Click "System Management"
Click "System File Update"
Choose "Download Configuration"

Click "Download"
Choose the name of the file and the place to save.

3. Upload Configuration
If you know the IP address of the device, user name and password:
Use IE to login Web interface.
Click "System Management"
Click "System File Update"
Choose "Upload Configuration"
Click "Upload"

4. Upgrade Firmware
If you know the IP address of the device, user name and password:
Use IE to login Web interface.
Click "System Management"
Click "System File Update"
Choose "Upgrade Firmware"
Click "Browse" and find the place of uploading the file.
Click "Upgrade"
A suggestion" interruption of power is not allowed during uploading", confirm it.

1. Load factory default will result in all status be in factory default settings, the IP could be static IP address "192.168.1.254".
2. Upload the configuration file, in the new configuration if static IP is not in the same network segment, the website will not be opened.
3. Use dynamic IP settings, but there is no DHCP server on the network segment, that will result in the relevant part of the IP will not be updated in the new configuration when upload configuration.

5.13.5 Logout

As shown in Figure 5.13.5, logout functionality for the system interfaces.



（Figure 5.13.5）

System Logout
Click the <OK> button, the interface would be returned to the login screen, configuration does not have to be changed.

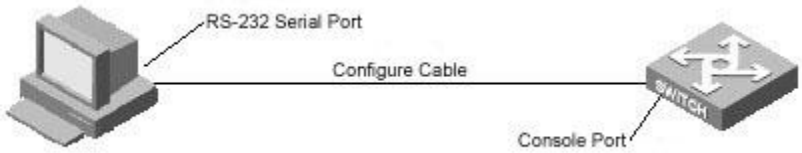
Chapter 6 CLI Command

6.1 Login Ethernet Switch

Build configuration environment by Console port

1. Connect switch to configuration terminal

As shown in figure 6.1.1, build local configuration environment, only need to connect serial port of PC to Console port of switch.



(Figure 6.1.1)

2. Configure terminal parameter

1) Turn on PC, in Windows interface click [start/(all)files/attachment/communication], run Hyper Terminal to make a new connection. As shown in figure 6.1.2, in "Name" Text-box input name of new connection, click OK.



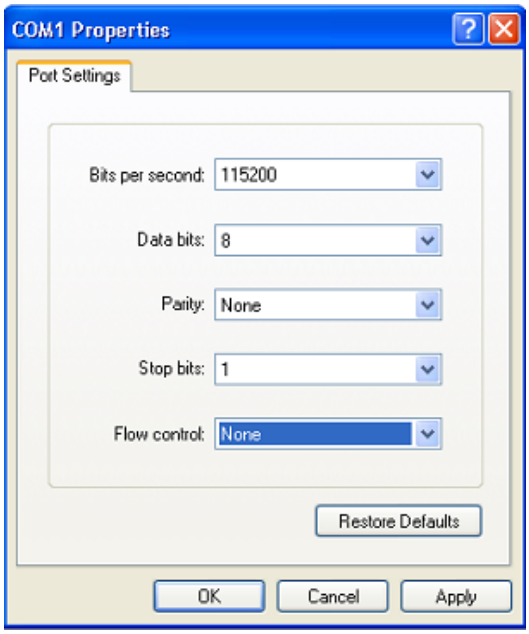
(Figure 6.1.2)

2) Select port connected to. As figure 6.1.3, select port in dropdown list of "Connect Using" (the port selected must exist in connecting ports), click <OK>.



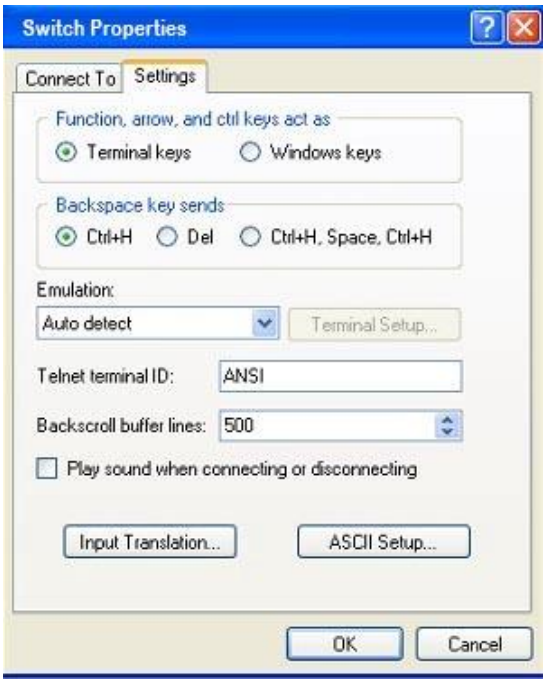
(Figure 6.1.3)

3) Port Setting. Setup Bits per second 115200bit/s in dialog box of port properties. Data bits is 8, Parity is None, Stop bits is 1, Flow control is None. Click <OK>, enter into [Hyper Terminal] window. As shown in figure 6.1.4.



(Figure 6.1.4)

4) Configuration of Hyper terminal properties. Select [Files/properties/settings] in [Hyper Terminal] window, enter into properties settings as shown in figure 6.1.5. Select VT100 or auto detect as terminal emulation type. Click <OK>, back to [Hyper Terminal] window.



(Figure 6.1.5)

5) Supply power to the switch, after power supply, displays auto detect information of Ethernet switch in super terminal. After auto detection, “Enter”, till command line single <user name> appears, input right username and password to enter into switch system mode. Detailed configuration command, please refer to following chapters in this book.

If connecting port is not COM1, then choose corresponding COM in second step. Bits per second must be 115200 in the third step, or it will not display normally.

Build configuration environment by Telnet

It needs to possess the following factors telnet to Ethernet switch through terminal:

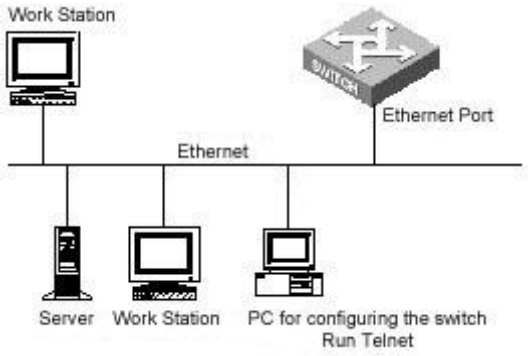
1. Correctly configure IP address of device in Ethernet switch (use IP command in view of system management);

2. If the port of terminal and it’s corresponding connecting port of switch are in the same LAN, then IP address must be configured in the same segment, or terminal and switch must be connected by routers.

It can telnet to Ethernet switch by meeting these two points above. Then configure Ethernet switch.

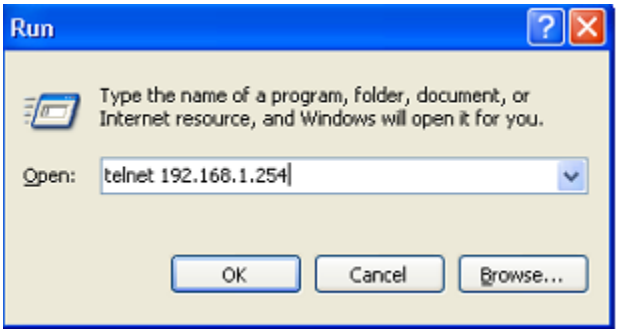
1) Before telnet to Ethernet switch it is needed to input telnet password, the default is admin.

2) As shown in figure 6.1.6, to build a configuration environment need to connect PC to Ethernet switch by LAN.



(Figure 6.1.6)

3) Run Telnet program in PC, input IP address of connecting Ethernet port of Ethernet switch and PC. As shown in figure 6.1.7:



(Figure 6.1.7)

4) Type into Enter until it shows “password” in terminal, it asks to input password. After correct password it shows command prompt.(such as Switch#).

5) Command configures Ethernet switch or check status of Ethernet switch. Input “?”, when help is needed. Detailed configurable commands please refer to the following chapters.

6.2 Agreement

1. Format agreement of command lines

Format	Description
Bold	Key words of the command show by bold type.
italic	Parameter of the command show *italic type.*
[ ]	It shows part in “[]” is optical when command configuration is need.
{ x | y | ... }	It shows to pick up one from two or more items.
[x | y | ...]	It shows to pick up one or no one from two or more items.
{ x | y | ... }	It shows to pick up one at least, all at most from two or more items.

2. Format agreement of figure interface

Format	Description
< >	“< >” shows press name, like ”click<OK>”
[ ]	“[ ]” shows windows name, menu name and data list. like “eject [create user]window”
/	Multilevel is separated by “/”. Like [file/create/folder] means[create] a [folder] under the menu of [file]

6.3 Command lines Port

IEM7110-3G can provide command lines port and its configuration for user’s easy configuration and management. Command lines port includes the following features:
1. Local configuration through Console port;
2. Supports history command saving which means it can save 10 pieces. History commands can be selected by up and down key.
3. User can type in “help” or “?” to get some help;
4. Supports intelligent complement with Tab when commands input;
5. Command interpreter take the method of partial matching. User can type in conflict-free key words, such as config command, only need to type in conf.

- **View of Command Lines**

IEM7110-3G’s view of command lines aim at configuration of different functions. After connecting IEM7110-3G, the view of user is entered to. It need to type in user name and password to enter into view of system. Under the view of system, corresponding view appears after typing indifferent commands.

Command lines provide the following views:

View	Function	Prompt	Enter	Quit
System	-	Switch#		Quit and return to user login
Device Information	Show or modify device information, like software version, IP address, etc.	Device_information#	**Information**	Exit and return to the view of system
Port Setting	Show or modify port information, like duplex mode, port enable.	Port_config#	**Port**	
Bandwidth Management	Show or modify bandwidth information, like ingress and egress bandwidth configuration.	Bandwidth#	**Bandwidth**	
IGMP	Igmp snooping	IGMP#	**IGMP**	
LLDP	LLDP setting	LLDP#	**LLDP**	
VLAN	Show or modify information of VLAN, like add Vlan, pvid, port type, etc.	Vlan_config#	**Vlan**	

Static Multicast Filtering	Show or modify static multicast address, like add static multicast address.	Multicast_filters#	**Multicast**	
QoS	Show or modify value of Qos, Tos, like Qos, Tos etc.	QoS_config#	**QoS**	
Ring	Show or modify Ring information, like Ring id,Ring port, etc.	Ring#	**Ring**	
Trunking setting	Show or modify port trunking information, like trunking information.	Port_Trunk#	**Trunk**	
SNMP	Snmp setting	SNMP#	**SNMP**	
Alarm Setting	Show or modify alarm information, like power alarm, port alarm, etc.	Alarm_config#	**Alarm**	
Port Mirror	Show or modify port mirroring information	Port_mirror#	**Mirror**	
System Management	Show or modify configuration information, like IP address, subnet mask, default gateway and password, etc.	System_manage#	**Manage**	
Time	Enter time zone setting menu	Time#	**TIme**	

➢ **Command lines Online help**

Command lines port provides the following online help:

- ✧ Total help;
- ✧ Partial help;

1. Total help

1)Type in <?> to get all commands and their description.

Example:

```
Switch# ?
  List                --List commands of current menu
  Help                --Help commands of current menu
  Quit                --Quit from CLI
  Exit                --Exit from current menu
  Reboot              --Reboot switch
  Port          <dir> --Enter port setting menu
  Bandwidth     <dir> --Enter bandwidth management menu
  Igmp          <dir> --Enter igmp snooping menu
  Lldp          <dir> --Enter lldp setting menu
  Vlan          <dir> --Enter vlan menu
  QoS           <dir> --Enter QoS menu
  Ring          <dir> --Enter Ring menu
  Trunk         <dir> --Enter Trunking setting menu
```

```
Snmp          <dir>    --Enter snmp setting menu
Alarm         <dir>    --Enter alarm setting menu
Statistics    <dir>    --Enter statistics menu
Mirror        <dir>    --Enter port mirror menu
Manage        <dir>    --Enter system manage menu
Multicast     <dir>    --Enter static multicast filters menu
Information   <dir>    --Enter device information menu
Time          <dir>    --Enter time zone setting menu
```

2)Type in a command and "?", between there is a space, if key word is in this location, then type in all keywords and descriptions.

Switch(information)# **show ?**

```
mac                --Device MAC Address
version            --Device version
others             --Device type,name,etc
```

2. Partial help

1) Type in a character string with <?>. It can show all commands beginning with this character string.

Switch# **r?**

```
Reboot             --Reboot switch
Ring          <dir>    --Enter Ring menu
```

2) Type in a command, a character string and<?>. It can show all key words of commands beginning with this character string.

Switch# **m?**

```
Mirror        <dir>    --Enter port mirror menu
Manage        <dir>    --Enter system manage menu
Multicast     <dir>    --Enter static multicast filters menu
```

3) Type in former letters of some key word of the command, press<Tab> key. If the letters are unique, it can show the completed key word.

Switch# **inf** press <Tab> key

Switch# **information**

Frequent Incorrect Information of Command Lines

All commands typed by users, if it is certificated by grammar, it can run correctly, or users will be sent incorrect information. Frequent incorrect information is as below:

Incorrect information	Reason
Fault Command	Command cannot be found.
	Key word cannot be found.
	The type of parameter is wrong.
	The parameter is beyond the border.
Incomplete Command	Command is not completed.
Too many parameters	Parameter is too much.

History Command

Command lines port can provides the function similar to Dos key. It automatic save command lines that users types in, and users can use these history commands. Detailed operating is shown as below:

Operating	Key	Result
Visit previous history command	Up < ↑ >	If it exists earlier command, it is taken out.
Visit next history command	Down < ↓ >	If it exists later command, it is taken out.

6.4 Device Information

Device information includes Device Type, Hardware Version, Device Name, Software Version, Device Description, Serial number and Contact Way. Among them, Hardware Version and Software Version can be only read, not modified.

Enter into the view of device information

Command of entering into the view of device information:

Operating	Command	Description
Enter into the view of device information	**Information**	Run in the view of system

Show Device Information

Command of showing device information:

Operating	Command	Description
Show system version	**show version**	Run in the view of device information
Show MAC address of device	**show mac**	Run in the view of device information
Show Device Type, Name, etc.	**show others**	Run in the view of device information

Example: Show Device Type, Name, etc.

Switch(information)# **show others**

Device type ManagedSwitch
Device name IndustrialSwitch
Description 10PORT
Serial number
Contact way

Configuration of Device Information

Command of configuration of device information, including Device Type, Name, Serial Number, Description and Contact Way:

Operating	Command	Description
Configure Device Type	**config –t** *type*	type:configurable type,the length is between 1～17 characters

Operating	Command	Description
Configure Device Name	**config -n** *name*	name:configurable name, the length is between 1～17 characters
Configure Serial Number	**config -m** *number*	number: configurable number, the length is between 1～30 characters
Configure Device Description	**config -p** *description*	description: configurable description, the length is between 1～17 characters
Configure Contact way	**config -c** *contact*	Contact: Configure Contact way 1-30 bytes
Clean Device information	**Clean** <*options*>	-t: Clean Device Type -n: Clean Device Name -m: Clean Serial Number -p: Clean Device Description -c: Clean Contact way

Switch(information)# **config ?**
<options>
-t --Set device type
-n --Set device name
-m --Set serial number
-p --Set device description
-c --Set contact way

Config <options> <string>

Switch(information)# **clean ?**
<options>
-t --Clean device type
-n --Clean device name
-m --Clean serial number
-p --Clean device description
-c --Clean contact way

Clean <options>

6.5 Port Configuration

Port information includes link state (link or loss) of port, port state (full or half), speed (auto-negotiation, 10Mbps
, 100Mbps), type of connector (Ethernet or Fiber), flow control and port enable.

Introduction of the Port

IEM7110-3G support the following features of Ethernet port:
10/100Base-Tx Ethernet port can work in the mode of full/half duplex, auto-negotiation. It supports MDI/MDIX auto connection and negotiates with other Ethernet device. It chooses suitable work mode and speed by itself to simplify configuration and management of the system. 100Base-FX port, the speed is 100Mbps. It works in the mode of full duplex and flow control is not configurable.

Enter into the view of port configuration

Command of entering into the view of port configuration:

Operating	Command	Description
Enter into the view of port configuration	**port**	Run in the view of system

Show configurable information of port
Command of showing configurable information:

Operating	Command	Description
Show state information of the port	**Show state** *<portlist>*	<portlist>: 1,3,5-10 or all
Show configurable information of the port	**Show config** *<portlist>*	<portlist>: 1,3,5-10 or all

Example: show state information of Port3 and 4.
Switch(Port)# **show state 3, 4**

	Speed	Port_status	Link_status	Interface_type
port 3	100M	FULL	Link	TX
port 4	10M	HALF	LOS	TX

Switch(Port)# **show state all**

	Speed	Port_status	Link_status	Interface_type
port 1	10M	HALF	LOS	TX
port 2	10M	HALF	LOS	TX
port 3	100M	FULL	Link	TX
port 4	10M	HALF	LOS	TX
port 5	10M	HALF	LOS	TX
port 6	10M	HALF	LOS	TX
port 7	10M	HALF	LOS	TX
port 8	10M	HALF	LOS	TX
port 9	10M	HALF	LOS	TX
port10	1000M	FULL	LOS	FX

Port Configuration
Port configuration includes:
1. Enable or disable the port;
2. Configuration of port speed and duplex mode;
3. Configuration of flow control of the port;
4. Clean frames statistics information of the port;;

Enable or Disable the Port
User can use the following command to enable and disable. The default state is to enable.
Command of enabling or disabling the port:

Operating	Command	Description
Disable the port	**switch** *<portlist>* **disable**	<portlist>the value is 1, 3, 5-10 or all
Enable the port	**switch** *<portlist>* **enable**	<portlist>the value is 1, 3, 5-10 or all

Example: Disable Port 3, 4, 6
Switch(Port)# **switch 3-4,6 disable**
[OK]

➢ **Configuration of Port Speed and Duplex Mode**

Command of configuration of port speed and duplex state:

Operating	Command	Description
Configuration of port speed and duplex mode	**Mode** *<portlist>* {10h|10f|100h|100f|auto}	<portlist>: 1,3,5-10 or all Mode: 10h, 10Mbps half duplex 10f, 10Mbps full duplex 100h, 100Mbps half duplex 100f, 100Mbps full duplex Auto: auto-negotiation

Example: configure speed of Port 3, 4, 5 is 100Mbps, full duplex.
Switch(Port)# **Mode 3-5 100f**
[OK]

Switch(Port)# **mode ?**
<portlist> --Portlist Example:1,3,5-10 or all

Mode <portlist> <rate>
Switch(Port)# **mode 8 ?**
<rate>
10h --10M half duplex
10f --10M full duplex
100h --100M half duplex
100f --100M full duplex
1000f --1000M full duplex
auto --Auto

Mode <portlist> <rate>

Configuration of Flow Control of the Port

Command of enabling or disabling flow control of the port:

Operating	Command	Description
Enable flow control	**Flow-con** *<portlist>* enable	<portlist>: 1,3,5-10 or all
Disable flow control	**Flow-con** *<portlist>* disable	<portlist>: 1,3,5-10 or all

Example: Enable flow control of Port 3, 4, 5
Switch(Port)# **flow-con 3,4,5 enable**
[OK]

6.6 Bandwidth Management

Enter into the View of Bandwidth Management

Bandwidth configuration includes:
1. Configuration of ingress bandwidth;
2. Configuration of egress bandwidth;
3. Configuration of type of ingress limited packets;
4. Show bandwidth configuration information;

Command of entering into the view of bandwidth management:

Operating	Command	Description
Enter into the view of bandwidth management	**bandwidth**	Run in the view of system

Configuration of Egress Bandwidth

The default egress bandwidth is unlimited.
Command of configuration of egress bandwidth:

Operating	Command	Description
Configuration of egress bandwidth	**Config egrate** <*portlist*> < bw >	<portlist>: 1,3,5-10 or all <bw>: 128k, 256k, 512k, 1M, 2M, 4M, 8M 0 --unlimited

Example: Configure the egress bandwidth of Port 1, 2 is 8M
Switch(Bandwidth)# **config egrate 1,2 8M**
[OK]

Example: configure unlimited egress bandwidth of Port 1.
Switch(Bandwidth)# config egrate 1 0 0 0 0
[OK]

Configuration of Ingress Bandwidth

The default ingress bandwidth is unlimited.
Command of configuration of ingress bandwidth:

Operating	Command	Description
Configuration of ingress bandwidth	**Config inrate** <*portlist*> <*low_bw*> <*normal_bw*> <*medium_bw*> <*high_bw*>	<portlist>: 1,3,5-10 or all <Lbw>/l (128k, 256k, 512k, 1M, 2M, 4M, 8M) 0 --unlimited

Example: Configure ingress bandwidth of Port 1, 2, low priority is 1M, normal priority is 2M, medium priority is 4M and high priority is 8M.
Switch(Bandwidth)# **config inrate 1,2 1M 2M 4M 8M**
[OK]

Example: configure unlimited priority of Port 1
Switch(Bandwidth)# **config inrate 1 0 0 0 0**
[OK]

Configuration of Type of ingress limited packets
The default ingress limited packets is broadcast packets only.
Command of configuration of ingress limited packets:

Operating	Command	Description
Configuration of type of ingress limited packets	**Config intype** <*portlist*> {0|1|2|3}	<portlist>: 1,3,5-10 or all {0|1|2|3}: type of limited packets 0 means limitation of all packets; 1means limitation of broadcast, multicast and flooding unicast; 2 means limitation of broadcast and multicast; 3 means the limitation of broadcast.

Example: Configure ingress limited packets of Port 1, 2 is "limitation of all packets".
Switch(Bandwidth)# **config intype 1,2 0**
[OK]

Show Configuration Information of Bandwidth
Command of showing configuration information of bandwidth:

Operating	Command	Description
Show type of ingress limit packets	**Show intype** <*portlist*>	<portlist>: Port 1, 2, 3-10
Show information of ingress port bandwidth	**Show inrate** <*portlist*>	<portlist>: Port 1, 2, 3-10
Show information of egress port bandwidth	**Show egrate** <*portlist*>	<portlist>: Port 1, 2, 3-10

Example: show ingress limit packets of Port 1 and 2.
Switch(Bandwidth)#**show intype 1,2**
port1 Limit packets:Broadcast only
port2 Limit packets:Broadcast only

6.7 VLAN

Introduction of VLAN
VLAN (Virtual Local Area Network) is a kind of new data exchange technology for logically dividing LAN into many segments and making many virtual work groups. This technology mainly allows that switch can limit broadcast when LAN interconnects. This technology can divide a LAN into several logical LAN——VLAN. Each VLAN is a broadcast domain and hosts in VLAN can communicate just like in the same LAN. But it cannot interconnect between VLAN. So broadcast message is limited in VLAN.
IEM7110-3G supports 802.1q VLAN and Port-based VLAN

VLAN Configuration
VLAN configuration includes:
1、add Vlan;
2、delete Vlan;
3、configure type of Pvid;
4、configure port type (trunk | access);

5、show information of Vlan;

Enter into configurable view of VLAN
Command of enter into configurable view of VLAN:

Operating	Command	Description
Enter into configurable view of VLAN	**Vlan**	Run in the view of system

Switch# **vlan**
Switch(Vlan)# **?**
List --List commands of current menu
Help --Help commands of current menu
Quit --Quit from CLI
Exit --Exit from current menu
Reboot --Reboot switch
Show vlantype --Show current VLAN type
Enable --VLAN Enable
PVLANSetting <dir> --Enter based on Port VLAN setting menu
QVLANSetting <dir> --Enter IEEE 802.1Q VLAN setting menu

Port VLAN configuration

Operating	Command	Description
Enter the Vlan information view	**Show vlantype**	To perform the operation in the system.
Select the Vlan type	**Enable {0|1}**	0: Port based on VLAN 1: 802.1Q based on VLAN
Select the port based Vlan	**PVLANSetting**	Based on Port VLAN setting menu
Based on the 802.1Q Vlan	**QVLANSetting**	IEEE 802.1Q VLAN setting

Switch(Vlan)# **show vlantype**
802.1Q VLAN is enable!
Switch(Vlan)# **enable 0**
Based on port VLAN is enable!
[OK]
Switch(Vlan)# **show vlantype**
Based on port VLAN is enable!

Operating	Command	Description
Show port vlan	**Show vlan***<items>*	*<items>:*Port vlan items
Add port Vlan	**Add** *<item>* *<portlist>*	<vid>: VLAN ID:1-4094 <portlist>: 1, 3, 5-10 or all 0 --CPU port
Delete port Vlan	**Delete** *<vidlist>*	<vidlist>: 1,4,5-4094 or all

Switch# **vlan**
Switch(Vlan)# **pVLANSetting**
Switch(PVlan)# **add 2 1,2**
[OK]

Switch(PVlan)# **show vlan all**
VID PORT
1 1 2 3 4 5 6 7 8 9 10
2 1 2

Switch(PVlan)# **delete 2**
[OK]

802.1Q VLAN
Add/Delete Vlan
Command of add/delete VLAN:

Operating	Command	Description
Add QVlan	**Add** <*vid*> <*portlist*> <*typelist*>	<vid>: VLAN ID:1-4094 <portlist>: 1, 3, 5-10 or all 0 --CPU port <typelist>: Unmodified | Un-tagged | Tagged
Delete QVlan	**Delete** <*vidlist*>	<vidlist>: 1,4,5-4094 or all

Example: Add vlan 2, Port members include Port 2, 5, 6, port types are untagged, tagged, Unmodified

Switch(QVlan)# add 2 2,5,6 u,t,m
VID : 2
Port_cpu : ----
port 1 : ----
port 2 : UnTagged
port 3 : ----
port 4 : ----
port 5 : Tagged
port 6 : UnModified
port 7 : ----
port 8 : ----
port 9 : ----
port10 : ----
[OK]
Tip: This configuration will be validated after restarting

- **Pvid and Port Type Configuration**

Configure pvid and port type:

Operating	Command	Description
Pvid configuration	**config pvid** <*portlist*> <*pvid*>	<portlist>: 1,3,5-10 or all ; 0 --CPU port <pvid>: 1,3,5-10 or all ; 0 --CPU port
Port type configuration	**config type** <*portlist*> {Trunk|Access}	<portlist>: 1,3,5-10 or all

Example: configure Pvid of Port 2, 3, 4 is 1
Switch(QVlan)# **config pvid 2-4 1**
[OK]
Tip: This configuration will be validated after restarting

Show Information of Vlan

Command of showing information of Vlan:

Operating	Command	Description
Show information of vlan	**Show vlan** <vidlist>	<vidlist>: 1,4,5-4094 or all
Show Pvid of port	**Show pvid** <*portlist*>	<portlist>: 1,3,5-10 or all 0 --CPU port
Show port type	**Show type** <*portlist*>	<portlist>:1,3,5-10 or all 0 --CPU port

Example: Show information of vlan 1.

```
Switch(QVlan)# show vlan 1
        Port_cpu     P1   P2   P3    P4    P5    P6    P7    G1   G2   G3
 VID:   1     UT     UT   UT   UT   UT   UT   UT   UT   UT   UT   UT

Switch(QVlan)# show pvid all
  Port_cpu  PVID: 1
  Port 1    PVID: 1
  Port 2    PVID: 1
  Port 3    PVID: 1
  Port 4    PVID: 1
  Port 5    PVID: 1
  Port 6    PVID: 1
  Port 7    PVID: 1
  Port 8    PVID: 1
  Port 9    PVID: 1
  Port10    PVID: 1
Switch(QVlan)# show type all
  Port_cpu  type: Access
  port 1    type: Access
  port 2    type: Access
  port 3    type: Access
  port 4    type: Access
  port 5    type: Access
  port 6    type: Access
  port 7    type: Access
  port 8    type: Access
  port 9    type: Access
  port10    type: Access
```

6.8 QoS

- **Enter into configurable view of QoS**

QoS configuration includes:

1. Enable Tos, Cos
2. Qos queue mechanism settings(8:4:2:1, high priority first)
3. Cos/Tos value mapping
4. Default port priority
5. Show configuration information of QoS

Enter into configurable view of Qos:

Operating	Command	Description

Operating	Command	Description
Enter into configurable view of Qos	**QoS**	Run in the view of system

➢ **Enable Tos、Cos**

User can use the following command to setup Tos, Cos.
Check Tos/Cos:

Operating	Command	Description
Check Tos/Cos	**check** <*portlist*> {0|1|2|3}	<portlist>: Port 1, 2, 3-7 0: Forbid; 1: use ToS; 2: use CoS; 3: all use

Example: Use CoS of Port 1, 3, 4, 6.
Switch(QoS)# **check 1,3,4,6 2**
[OK]
Example: Use ToS of Port 2, 3, 5, 6.
Switch(QoS)# **check 2,3,5,6 1**
[OK]

➢ **QoS Queue Mechanism settings**

User can use the following command to setup QoS queue mechanism.
QoS queue mechanism:

Operating	Command	Description
QoS queue mechanism	**Queuingm** {0|1}	0: Weight proportion(8:4:2:1)1: higher priority first

Example: setup weight proportion of QoS queue mechanism is(8:4:2:1)
Switch(QoS)# **queuingm 0**
[OK]

➢ **Cos/Tos Value Mapping**

User can use the following command to configure Cos/Tos value mapping.
Cos/Tos value mapping configuration command:

Operating	Command	Description
Cos value mapping configuration	**Config cos** <*coslist*> <*classlist*>	<coslist>: CoS mapping value, 0, 1, 2-7 <classlist>: priority queue low, normal, medium, high
Tos value mapping configuration	**Config tos** <*dscplist*> <*classlist*>	<dscplist>: ToS mapping value, 1, 2, 3-64 <classlist>: queue low, normal, medium, high

Example: Setup CoS value 0, 2, 5, 7 correspond to the priority queue of Low, Normal, Medium, High
Switch(QoS)# **config cos 0,2,5,7 l,n,m,h**
[OK]

➢ **Default Port Priority Configuration**

User can use the following command to configure default port priority.

Default port priority configuration:

Operating	Command	Description
Default port priority configuration	**Default priority** <*portlist*> <*classlist*>	<portlist>: Port1, 2, 3-10 <classlist>: priority queue low, normal, medium, high

Example: setup default priority of Port 1, 3, 4, 6 correspond to Low, Normal, Medium, High
Switch(QoS)# default priority 1,3,4,6 1
[OK]

➢ **Show Configuration Information of Qos**

User can use the following command to check information of QoS.
Command of showing information of Qos:

Operating	Command	Description
Show QoS queue mechanism	**Show queuingm**	
Show CoS value mapping	**Show cos** <*coslist*>	<coslist>: cos mapping value, 0, 1, 2-7
Show ToS value mapping	**Show tos** <*dscplist*>	<dscplist>: tos mapping value, 1, 2, 3-64
Show state of ToS/CoS	**Show state** <*portlist*>	<portlist>: Port 1, 2, 3-10 or all
Show default port priority	**Show default** <*portlist*>	<portlist>: Port 1, 2, 3-10 or all

6.9 Ring Configuration

➢ **Enter into view of Ring Configuration**

Ring configuration includes:
1. Ring3 configuration;
2. RSTP configuration;
3. Show Ring information;

Enter into view of Ring configuration:

Operating	Command	Description
Enter into view of Ring configuration	**Ring**	Run in the view of system

```
Switch(Ring)# ?
  List              --List commands of current menu
  Help               --Help commands of current menu
  Quit              --Quit from CLI
  Exit              --Exit from current menu
  Reboot             --Reboot switch
  Show ring           --Show current ring config
  Enable            --Enable Ring
  Disable           --Disable Ring
  Modify ring3        --Modify Ring III parameter
```

Config ring3 --Config Ring III
Modify rstp_state --Modify RSTP State parameter
Config rstp_state --Config RSTP State
Modify rstp_port --Modify RSTP Port parameter
Config rstp_port --Config RSTP Port
rstp status --Show rstp status informaiton

Ring network state information view
Into the show ring network state information view:

Operating	Command	Description
Enter the ring network state information view	**Show ring**	To perform the operation in the system.

Switch(Ring)# **show ring**
Ring closed !

To enable or disable the ring
Users can use the following command to set the ring network enabled, ring network to set command:

Operating	Command	Description
Ring opening	**Enable** {3|4}	3: open ring3；4: open RSTP
Ring close	**Disable** {0|3|4}	0: Disable all ring； 3: Disable Ring3；4: Disable RSTP

Example: open RING3
Switch(Ring)# **enable 3**
[OK]
Tip: This configuration will be validated after restarting

The Ring3 configuration
Ring3 enabled, can use the following command to set the Ring3.
Table 9.4.1 Ring3 to set and modify:

Operating	Command	Description
Configuration Ring3	**Config ring3** {1|2} <id> <LoopType> <port> <hellotime>	{1|2} : 1 ring group 1, 2 ring group 2 <id>: Said the ring network identification, value of [0-255] <LoopType>: 0--Single, 1--Couple, 2--chain, 3--Daul_homing <portlist>: Ring network port <hellotime>: value of [0-300]

Operating	Command	Description
Modify ring3	**Modify ring3** {1|2} <options> <parameter>	{1|2} : 1 ring group 1, 2 ring group 2 <options>: h--modify Hello time Range [0-300]*100ms i--modify Ring III ID Range [0-255] t--modify Ring III LoopType {0|1|2|3} p--modify Ring III port s--modify Ring III state {enable or disable} <parameter>: And the parameter matching -h|-i|-p

Example: the allocation of port 7, 8 to first groups in Ring3 ring, ring ID is 1, hellotime is 0, the ring type Couple
Switch# **ring**
Switch(Ring)# **enable 3**
[OK]
Tip: This configuration will be validated after restarting
Switch(Ring)# **config ring3 1 1 1 7,8 0**
[OK]
Tip: This configuration will be validated after restarting
Switch(Ring)# **show ring**
Ring III Enable
Group:1 ID: 1 port:7,8 type: Couple Hello_time: 0*100ms state:Enable
Group:2 ID: 2 port:3,4 type: Single Hello_time: 0*100ms state:Disable

The RSTP configuration
RSTP enabled, can use the following command to set the RSTP.

Operating	Command	Description
Display current configuration RSTP	**Show rstp_p** *<portlist>*	*<portlist >* *1,3,5-10or all*
Modify the RSTP port	**Modify rstp_port**< *portlist* > <options><parameter>	< *portlist* >: *1,3,5-10 or all* Options: -c --modify pathcost Range [0-200000000] -p --modify portpriority {0|16|32|48|64|80|96|112|128|144|160|176|192|208|224|240} -t --modify p2p {no|yes|auto} -e --modify edge {no|yes} -a --modify enable {no|yes}
Modify the RSTP state	**Modify rstp_state** <options> <parameter>	Options: -p The switch priority (0,4096,8192,12288,16384,20480,24576, 28672,32768,36864,40960,45056,49152, 53248,57344,61440) -h The polling interval（1~10s） -d Forwarding delay time（4~30s） -m The survival time.（6~40s）

Operating	Command	Description
The configuration of RSTP port	**Config rstp_port** <port> <pathcost> <portpriority> <p2p> <edge> <enable>	<port> --RSTP Port <pathcost> --Port pathcost Range [0-200000000] <portpriority> --Port portpriority {0|16|32|48|64|80|96|112|128|144| 160|176|192|208|224|240} <p2p> --Port p2p {no|yes|auto} <edge> --Port edge {no|yes} <enable> --Port enable {no|yes}
The configuration of RSTP state	**Config rstp_state** <priority> <hellotime> <delaytime> <maxage>	<priority> --RSTP priority {0|4096|8192|12288|16384|20480|24576| 28672|32768|36864|40960|45056|49152|53248|57344| 61440} <hellotime> --RSTP hellotime Range [1-10]s <delaytime> --RSTP delaytime Range [4-30]s <maxage> --RSTP maxage Range [6-40]s

Example: RSTP port configuration
Switch(Ring)# **config rstp_port 1 20000 224 yes yes yes**
[OK]
Tip: This configuration will be validated after restarting

Display the current state of the Rstp information
The configuration of Rstp, can use the following command to view the Rstp current status information.
Table 9.7.1 view the Rstp information about the current configuration command:

Operating	Command	Description
Display the current state of the RSTP information	**RSTP Status**	To perform the operation in the system.

Example: the ring network configuration information for the current view
Switch(Ring)# **show Status**
This ID : Root ID :
Root Port : Root port path cost :

Port	Priority	Path cost	P2P	Edge	Network	Roles	Forwarding
1	128	0	Y	Y	Rapid	Disabled	Disabled
2	128	0	Y	Y	Rapid	Disabled	Disabled
3	128	0	Y	N	Rapid	Disabled	Disabled
4	128	0	Y	N	Rapid	Disabled	Disabled
5	128	0	Y	N	Rapid	Disabled	Disabled
6	128	0	Y	N	Rapid	Disabled	Disabled
7	128	0	Y	N	Rapid	Disabled	Disabled
8	128	0	Y	N	Rapid	Disabled	Disabled
9	128	0	Y	N	Rapid	Disabled	Disabled
10	128	0	Y	N	Rapid	Disabled	Disabled

6.10 Port Trunking

- **Enter into view of port trunking**

Port trunking configuration includes:
1、Port trunking configuration;
2、Clean port trunking information;
3、Check port trunking information;
Enter into view of port configuration command:

Operating	Command	Description
Enter into view of port trunking configuration	trunk	Run in view of system

➢ **Port Trunking Configuration/Cleaning**

User can use the following commands to configure/delete port trunking.
Port trunking configure/clean command:

Operating	Command	Description
Port trunking configuration	**Config** <trunkgroup><*portlist*>	{1|2|3|4}: Trunking group 1, 2, 3, 4 <portlist>: trunking port 1, 2, 3-10 or all
Clean port trunking	**Clean** <trunkgroup>	<trunkgroup> --Trunking group 1 ,2 ,3 ,4or all

Example: Setup 1, 2, 4 as trunking group 1
Switch(Trunk)# **config 1 1,2,4**
[OK]

➢ **Show Port Trunking Configuration Information**

User can use the following command to check port trunking configuration information.
Command of showing port trunking configuration:

Operating	Command	Description
Show port trunking configuration	**Show** <trunkgroup>	<trunkgroup>: Trunking group 1, 2, 3; 4 all: All trunking groups

Switch(Trunk)# show all
Group: 1 state: Disable Port: ---
Group: 2 state: Disable Port: ---
Group: 3 state: Disable Port: ---
Group: 4 state: Enable Port: 1, 2

6.11 Alarm Configuration

➢ **Enter into view of alarm information**

Alarm configuration includes:
1. Power Alarm;
2. Port Alarm;
3. Delete alarm information;
4. Check alarm information;

Enter into view of alarm configuration command:

Operating	Command	Description
Enter into view of alarm configuration	**Alarm**	Run in view of system

➢ **Alarm Configuration/Cleaning**

User can use the following commands to configure alarm.
Alarm configuration command:

Operating	Command	Description
Enable port relay	**Port relay** <*portlist*> **enable**	<portlist>: Alarm Port 1, 2, 3-10
Disable port relay	**Port relay** <*portlist*> **disable**	<portlist>: Alarm Port 1, 2, 3-10
Enable power relay	**Power relay** {1|2|all} **enable**	{1|2|all}: which power alarm 1: the first power 2: the second power
Disable power relay	**Power relay** {1|2|all} **disable**	{1|2|all}: which power alarm 1: the first power; 2: the second power
type of Relay output configuration	**Type** {0|1}	{0|1}: type of relay output 0: OFF; 1: ON
Clean alarm information	**Clean alarm**	Run in view of alarm

Example: Enable Port1, 3, 5, 7 alarm
Switch(Alarm)# **port relay 1,3,5,7 enable**
[OK]

Example: Disable the first power alarm
Switch(Alarm)# **power relay 1 disable**
[OK]

- **Show Alarm Information**

User can use the following commands to check alarm information.
Command of checking alarm information:

Operating	Command	Description
Show power alarm information	**Show power** {1|2|all}	{1|2|all}: which power alarm 1: the first power; 2: the second power
Show port alarm information	**Show port** <*portlist*>	<portlist>: Alarm Port 1, 2, 3-10
Show alarm output type	**Show type**	Run in view of alarm

Example: Check all ports alarm information settings

```
Switch(Alarm)# show port all
  Port 1  Alarm status: Disable     [LOS ]
  Port 2  Alarm status: Disable     [LOS ]
  Port 3  Alarm status: Disable     [Link]
  Port 4  Alarm status: Disable     [LOS ]
  Port 5  Alarm status: Disable     [LOS ]
  Port 6  Alarm status: Disable     [LOS ]
  Port 7  Alarm status: Disable     [LOS ]
  Port 8  Alarm status: Disable     [LOS ]
  Port 9  Alarm status: Disable     [LOS ]
  Port10  Alarm status: Disable     [LOS ]
```

6.12 Port Mirroring

- **Enter into view of port mirroring**

Port mirroring configuration includes:

1. Port mirroring configuration;
2. Delete port mirroring;
3. Check port mirroring;

Enter into port mirroring configuration command:

Operating	Command	Description
Enter into view of port mirroring configuration	**Mirror**	Run in system view

➢ **Port Mirroring Configuration/Closing**

User can use the following commands to configure/delete port mirroring.
Port Mirroring configuration/deleting:

Operating	Command	Description
Port mirroring configuration	**Config** {0|1|2} <mirror_port> <port>	{0|1|2}: collected data type; 0 --all data 1 --Ingress data only 2 --Egress data only < Mirror port>: 1, 2, 3-10 <port>: collect port
Close mirroring information	**Close mirror**	Run in view of port mirroring

Example: Configure Port 3 to collect all data from both Port 1 and 2.
Switch(Mirror)#config 0 3,7,9 1
[OK]

➢ **Show Information of Port Mirroring**

Command of showing mirroring information:

Operating	Command	Description
Show Mirroring information	**Show mirror**	Run in view of port mirroring

6.13 Static Multicast Configuration

➢ **Enter into configurable view of static multicast filtration**

Static multicast configuration includes:
1. Add static multicast address; 2. Delete multicast address 3. Check multicast address;
Enter into view of static multicast command:

Operating	Command	Description
Enter into view of static multicast	**Multicast**	Run in view of system

➢ **Add /Delete static multicast address**

User can use the following commands to add/delete static multicast address.
Multicast address add/delete command:

Operating	Command	Description
Add multicast address	**Add** <*macaddress*> <*portlist*>	<macaddress>: multicast address, format is XY-XX-XX-XX-XX-XX, X is any hex number <portlist>: Port 1,2,3-10 or all
Delete multicast address	**Delete** <*macaddress*>	

Example: Add multicast address 01-22-33-44-55-66, its port members are Port 1, 2, 3.
Switch(Multicast)# **add 01-22-33-44-55-66 1,2,3**
MAC : 01-22-33-44-55-66 Port: 1,2,3
[OK]

- **Configuration of showing static multicast address**

User can use the following commands to check static multicast address.
Chart 11.3.1 shows static multicast address command:

Operating	Command	Description
Show static multicast filtrated address	**Show multicast**	Run in view of multicast

6.14 System Management

- **Enter into view of system manage configuration**

System manage configuration includes:
1. System time-out setting;
2. Default gateway and IP address setting;
3. Host name and password setting;
4. Device IP address, subnet mask and default checking;
5. Restore factory setting;
6. Upload and download configurable files setting;
7. System upgrade;

Enter into view of system manage configuration

Operating	Command	Description
Enter into view of system manage	**Manage**	Run in view of system

- **System time-out setting:**

User can use following command to setup system time-out
System time-out setting command:

Operating	Command	Description
System time-out setting	**Set** <*time_out*>	<time_out>: system time-out time, value is [0-9999], unit is minute, default is 5 minutes.

Example: setup system time-out time is 10 minutes.
Switch(Manage)# # **set 10**
[OK]

System time-out defines the time with no operating when entering into CLI configuration mode. When time out, system will auto-jump to user mode and recertify host name and password.

➢ **IP Address and Default Gateway Setting**

User can use the following commands to setup Device IP address and default gateway address.
Device IP address and default gateway address setting:

Operating	Command	Description
Device IP address setting	**IP** *<A.B.C.D>* *<A1.B1.C1.D1>*	<A.B.C.D>: IP address <A1.B1.C1.D1>: Subnet Mask
Default gateway setting	**Gateway** *<A.B.C.D>*	<A.B.C.D>: Gateway address

Example: configure Device IP address to 192.168.1.254, subnet mask to 255.255.255.0, default gateway to 192.168.1.1
Switch(Manage)# ip 192.168.1.254 255.255.255.0
[OK]
The Switch is rebooting.Please waiting.....

➢ **Host name and Password Setting**

User can set up host name and password by following commands.
Host Name and Password setting:

Operating	Command	Description
Host name configuration	**Hostname** *<hostname>*	<hostname>: hostname character string
Password configuration	**Password** *<password>* *<password>*	<password>: password character string

➢ **Show Device IP Address, Subnet Mask and Default Gateway**

User can check Device IP address, subnet mask and default gateway.
Check Device IP address, subnet mask and default gateway.

Operating	Command	Description
Display Device IP address, subnet mask and default gateway	**show net_address**	Run in view of System Manage.

Example: Check Device IP address, subnet mask and default gateway address.
Switch(Manage)# **show net_address**
Device gateway : 192.168.1.1
Device mask address : 255.255.255.0
Device IP address : 192.168.1.254

➢ **Restore Factory Setting**

User can use following command to restore device to factory setting.
Restore Factory Setting:

Operating	Command	Description

Operating	Command	Description
Restore factory setting	**Restore**	Run in view of System manage

Example: Restore the device to Factory setting.
Switch(Manage)# **restore**
Restore Settings or not ? [yes/no]: yes // < Y>
Please waiting.....

- **DNS Setting**

DNS Setting:

Operating	Command	Description
DNS setting	**DNS <Server>**	<Server> --DNS Server such as 202.96.134.133

- **DHCP Setting**

DHCP Setting:

Operating	Command	Description
DHCP setting	DHCP {enable|disable}	Run in view of System manage

6.15 Frame statistics

Enter into view of frame statistics
Frame include:
1. View frame statistics;
2. Clear all port frame statistics;

Operating	Command	Description
Enter into view of frame statistics	**Statistics**	Run in view of Frame System

View frame statistics
Users can use this command to view the statistics of a port frame

Operating	Command	Description
View frame statistics	**Show frames** *<port>*	<port>:por 1, 2, 3-10 Note: only one port can be viewed at a time.

View port 6 frame statistics,show frames 6
Switch(Statistics)# show frames 6

InGoodOctets	0	OutOctets	0
InbadOctets	0	OutUnicast	0
InUnicasts	0	OutBroadCasts	0
InBroadcasts	0	OutMulticasts	0
InMulticasts	0	OutPause	0
InPause	0	Excessive	0
InUndersize	0	Collisions	0
InFragments	0	Deferred	0

InOversize	0	Single	0
InJabber	0	Multiple	0
IN RxErr	0	OutFCSErr	0
INFCSErr	0	Late	0

Clear all port frame statistics
Users can use this command to clear the number of frames for all ports

Operating	Command	Description
Clear all port frame statistics	Clean frames	Run in view of Frame System

Example: Delete frame statistics for all ports
Switch(statistics)# clean frames
[OK]

6.16 LLDP
Enter into view of LLDP

Operating	Command	Description
Enter into view of LLDP	**LLDP**	Run in view of System

Operating	Command	Description
Set lldp enable	**Lldp** {enable|disable}	Run in view of LLDP System
Show the configuration of LLDP	**Show**	Show the configuration of LLDP
Set the Configuration of sending LLDPDU	**Config** <TxInterval> <TxHold> <TxDelay> <TxReinit>	<TxInterval> --Tx Interval[5-32768] <TxHold> --Tx Hold[2-10] <TxDelay> --Tx Delay[1-8192 and <= TxInterval/4] <TxReinit> --Tx Reinit[1-10]
Config port mode type	**Set** <portlist> {0|1|2|3}	<portlist> --Portlist Example:1,3,5-10 or all {0|1|2|3} 0 --Disabled 1 --Rx Tx 2 --Tx only 3 --Rx only
Print remote machine's infomation	**Print neighbors**	Run in view of LLDP System
Print lldp statistics local counters	**print local**	
Clear lldp statistics local counters	**clear**	

6.17 SNMP
Configure the view into the SNMP
The Snmp configuration including:
1. Close the Snmp

2. To view the Snmp configuration information
3. The Snmp configuration
Enter the Snmp managed view:

Operating	Command	Description
enter the Snmp view	**Snmp**	To perform the operation in the system

Enable the SNMP information
Enter the Snmp command information and configuration view:

Operating	Command	Description
Show Snmp information	**Show**	To perform the operation in the system
Close snmp	**Close**	Turn off the snmp
Set the snmp	**Config** <orcomm> <rwcomm> <snmpgw>	<orcomm> --only read community name such as public <rwcomm> --read or write community name such as private <snmpgw> --gateway address such as 192.168.1.1

Switch(Snmp)# config 1 1 192.168.5.1
[OK]
Switch(Snmp)# show
The only read community name :1

The read or write community name:1

The SNMP gateway :192.168.5.1

6.18 IGMP

Enter the IGMP managed view:

Operating	Command	Description
enter the IGMP view	**IGMP**	To perform the operation in the system

Switch# igmp
Switch(Igmp)#

Operating	Command	Description
IGMP Snooping set	**Set igmp** {enable|disable}	To perform the operation in the system
IGMP Snooping query set	**Set query** {enable|disable}	Enable or disable igmp query function
Query time set	**Query** <time>	<time> --Range [60-1000] seconds
Show MAC address table	**Show MAClist**	Show MAC address table

Switch(Igmp)# set igmp enable
[OK]
Switch(Igmp)# set query enable

```
  [OK]
Switch(Igmp)# query 100
  [OK]
Switch(Igmp)# show MAClist
  IGMP Snooping query time 100 seconds
  [  1] MAC List: 01-00-5E-00-00-73  Port: 03
  [  2] MAC List: 01-00-5E-00-00-09  Port: 03
  [  3] MAC List: 01-00-5E-2D-12-58  Port: 03
  [  4] MAC List: 01-00-5E-40-98-8F  Port: 03
  [  5] MAC List: 01-00-5E-7B-0C-01  Port: 03
  [  6] MAC List: 01-00-5E-7F-FF-FA  Port: 03
  [  7] MAC List: 01-00-5E-00-00-FB  Port: 03
  [  8] MAC List: 01-00-5E-00-00-FC  Port: 03
  [  9] MAC List: 01-00-5E-4D-EC-DE  Port: 03
  [ 10] MAC List: 01-00-5E-00-00-02  Port: 03
  [ 11] MAC List: 01-00-5E-00-00-FD  Port: 03
  [ 12] MAC List: 01-00-5E-00-00-64  Port: 03
```

6.19 Time

Enter the time view:

Operating	Command	Description
Enter the time view	**Time**	To perform the operation in the system

```
Switch(Igmp)# exit
Switch# time
Switch(Time)# ?
```

Operating	Command	Description
Close the time configuration	**close**	Close the time configuration
Show the time	**show**	Show the time
Set the time zone	**Zone** {-12|-11|-10|-9|-8|-7, 1|-7, 2|-6, 1|-6, 2|-5,1|-5,2|-4,1|-4,2|-3,1|-3,2|-2|-1|+0,1|+0,2|+1,1|+1,2|+2,1|+2,2|+3|+4|+5|+6|+7|+8,1|+8,2|+9|+10,1|+10,2|+11|+12, 1|+12,2}	Set the time zone
Set NTP server address	**Server** <serveraddr>	<serveraddr> --the NTP server address such as www.3onedata.com

```
Switch(Time)# zone +8,1
  [OK]
Switch(Time)# show
Time Configuration:Enable
The World TimeZone:(GMT+08:00) China, Hong Kong, Australia Western
    The NTP server:www.3onedata.com
   The system time:2017-3-2,17:33:58, Thu
```