MIEN6024/MIEN6026 Series

Managed Rack-Mounting Industrial Ethernet Switch

User Manual

(Edition: V5.0)

Wuhan Maiwe Communication Co., Ltd.

Trademark

Maiwe This trademark is owned by Wuhan Maiwe Communication Co., Ltd.

Mwring is the trademark used for link redundancy and self-recovery technology, owned by Wuhan Maiwe Communication Co., Ltd.

Microsoft and **Windows** is registered trademark owned by Microsoft.

Clarification

The user manual is applicable to MIEN6024/6026 series managed rack-mounting managed industrial Ethernet switches.

Please read the following license agreement carefully before using this manual. The products described in this manual can be used only if you agree on the following license agreement.

Important Statement

Any information provided by our company in this manual does not represent for corresponding authorization on these information.

Our company attempts to ensure the accuracy and applicability for the information provided in this manual, however our company does not assume any responsibility for the use of these information, and does not assume any joint responsibility for the use of these information. There may be a few technical or typographical errors in the product and manual. The company reserves the right to change all or part of this manual without prior notice.

Statement

Due to continuous update and improvement of products and technology, the contents of this document may not be completely consistent with the actual products, appreciate for your understanding. If necessary to inquiry the updates of the product, please check our official website or contact our representative directly.

Revision history:

Version	Date	Reason
V3.1.1		Create file
V3.1.2	2012.02	Content revision
V3.1.3	2012.08	VLAN part content revision
V4.0	2014.06	Product upgrade
V5.0	2015.04	Product upgrade

Safe Use Instruction

This product performance is excellent and reliable in the designed range of use, **but it's necessary to avoid man-made damage or destroy for the equipment**.

- Read the manual carefully and keep this manual for reference if need afterwards.
- Do not put the device close to the water sources or damp places.
- Do not put anything on the power cable, it should be placed out of reach.
- To avoid causing fire, do not knot or wrap the cable.
- Power connector and other device connectors should be firmly connected with each other, frequently inspection is needed.
- Please keep the fiber socket and plug clean. Do not look directly at the fiber section when the equipment is working.
- Please keep the equipment clean and wipe it with a soft cotton cloth if necessary.
- Please do not repair the equipment by yourself, unless there is clear instructions in the manual.

Under the following circumstances, please cut off power immediately and contact us.

- Equipment water damage.
- The equipment is broken or the casing is broken.
- The equipment works abnormally or the performance has completely changed.
- The equipment produces odor, smoke or noise.

Statement: Information requiring explanation in use of the managed software.
Attention: Matters requiring specific attention in the use of the managed software.

Catalogue

1. System Introduction

1.1. Product Introduction

Managed Industrial Ethernet Switch manufactured by Wuhan Maiwe Communication Co., Ltd, is specifically designed and developed for industrial high-speed network communication application. The managed switch provides a high-end industrial Ethernet communication solutions for flexible industrial application requirements, making the industrial communication more reliable, smother and faster, meeting the constantly innovation requirements for customers in terms of added value application.

To satisfy different requests, MAIWE brand managed series of switches can be used for Plug and Play simple application mode and complicated Web-management method. All TX ports support adaptive-negotiation mode, 10/100Mbps half-duplex and full-duplex work mode, flow control, auto-MDI/MDI-X connection. MAIWE brand managed series of switches provide advanced management function thru Web management or SNMP network management, such as Mwring, VLAN, Trunk, QoS, GMP Snooping, Flow control, Port mirroring, Static MAC address forwarding table, Network fault diagnosis, Email/Relay failure alarms, Fireware online upgrade and other advanced network management functions. MAIWE brand managed series of switches provide both dual redundancy power supply and full range ADC input voltage. In terms of installation structure, MAIWE brand managed series of switches are a type of compact and small footprint switch with rack mounting installation.

The **Mwring** technique is designed and developed for industrial application by Wuhan Maiwe Communication Co., Ltd. It supports self-recovery function for Ethernet communication link down and the recovery time is less than 20ms. MAIWE brand managed series of switches can construct the ring network by any common 100MBased port so as to provide faster restoration speed and communication bandwidth.

MIEN6024 managed industrial Ethernet switch is equipped with 24*100MBased ports, MIEN6026-2S/M switch is equipped with 26*100MBased ports, which all support 802.1Q VLAN, minimum rate limitation of 62.5Kbps, switch bandwidth 8.8Gbps and 8K MAC table size.

1.2. Product Characteristic

1.2.1. Industrial Network Performance

- Link redundancy self-recovery technology based on Mwring technology.
- Embedded Web server, support browser remote management and

configuration.

- Trunk.
- Real-time monitoring of broadcast storm control.
- Online firmware update.
- Dynamic IGMP Snooping supporting, multicast traffic filtering.
- Optional different distances and types of 100Base-FX port.
- Store and forward mechanism, switch bandwidth 8.8Gbps
- Adaptive 10/100MBased FX port, full/half duplex, MDI/MDIX adaptive mode.
- Full-duplex flow control and half duplex back pressure flow control.
- Port VLAN and IEEE 802.1Q VLAN.
- Support QoS, IEEE802.1P and ToS/Diff-serve, improve the communication quality.
- Support SNMP V1/V2C different levels network management.
- Redundant dual power input meets the requirements of high availability.
- Meet trouble-free working requirement under strong electromagnetic interference environment.
- Support private MIB, effective remote data monitoring and management capability.

1.2.2. Industrial Application Design

- Redundant dual power input design
- Rack mounting installation
- Bandwidth management, avoid unpredictable network problems
- Backup and restore system configuration parameters
- User-friendly graphical interface, one key to restore factory default
- Port mirroring for online debugging
- Effective network diagnostic tool
- Relay power-down alarms
- Fast connection recovery after change of cable
- Real-time network time synchronization
- Restrict access to IP, manage switch in the network

1.2.3. Remote Management Configuration

- Manage configuration thru Web page, Console applications or Windows applications
- Support standard SNMP management protocol

1.3. Packing List

Packing list of MAIWE Brand Managed Switch is listed as below. If any item in the list is lost or damaged, please contact the distributor or MAIWE

customer service center, they will assist you to make replacement or complement.

Items	Quantity
MAIWE Brand Managed Series Switch	1
User manual	1
CD (network management software, excluded in the standard configuration)	1
RS-232 serial cable	1
Product quality certificate and warranty card	1

1.4. Performance Specifications

MAIWE Brand Managed Series Switch is capable of completing Ethernet information interchange, users must choose the suitable model and use properly by referring to below information, so that switch can performance good industrial characteristic and network interchange capability.

Technique parameters:

IEEE Standard: 802.3, 802.3 u, 802.3x, 802.1P, 802.1Q, 802.1D/W

Exchange: Store and forward

Backplane Bandwidth: 8.8Gbps

Flow control: Full-duplex flow control, half duplex back pressure control

MAC Address: 8K

Transmission distance: Twisted pair 100m, fiber cable with options 20, 40, 60 and 80 km.

Management: Web Management and SNMP

Redundancy recovery: Recovery time is less than 20ms

Broadcast storms suppression: Real-time monitoring and control

Firmware Upgrade: Web online upgrade

Management functions: System information settings, 802.1Q VLAN (4K items), Trunk, QoS, 802.1P/1Q, ToS/DiffServe, IGMP Snooping, broadcast storm control, rate limiting, port mirroring, static MAC address forwarding (including unicast address and multicast address), SNMP V1/V2C

Diagnostics function: Relay power-down alarm, traffic statistics, Syslog

EMC Standard：

EN61000-4-2 static defend (ESD): ±8kVcontact discharge, ±15kV air discharge

EN61000-4-3 electromagnetic: 10V/m (80-1000MHz)

EN61000-4-4 instantaneous high voltage (burst): ±4kV power cable, ±2kV

signal cable

EN61000-4-5 surge voltage: ±4kV (line/earth), ±4kV (line/line) power cable, ±2kV signal cable

EN61000-4-6 conduction defend: 3V 10 kHz~150 kHz), 10V (150 kHz~80 MHz)

EN55022: EN55022 Class A

2. Hardware Installation & Networking

2.1. Hardware Structure

2.1.1. System Structure

System hardware is mainly inclusive of several components as below:

●Industrial Ethernet controller adapts high performance ASIC chip technology, support 2-layer wire-speed packet forwarding

●FX port adapts integrated optical transceiver module, with stable performance.

●Use of industrial grade power supply with overcurrent, overvoltage and EMC protection.

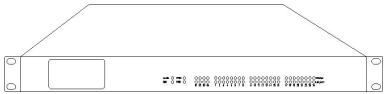
●All data ports have EMC protection.

2.1.2. Housing Structure

The housing is 19''U rack-mounting structure, as below picture 2.1. The housing is six-sides sealed. The housing's left and right panel which is made of single rib type aluminum alloy is part of the cooling system. By abandoning the traditional flow fan heat dissipation mode, it reduces the machine's power consumption as well as improve the system stability.

MIEN6024, MIEN6024-4/8S/M and MIEN 6026-2S/M switch's external dimensions (W×H×D): 482.6mm×44mm×210mm

The housing design is as below picture 2-1:



Picture 2-1 Casing House

MIEN6024-12/16/24S/M housing design is as below picture 2-2, the external dimensions (W×H×D) is 482.6mm×44mm×315mm

Picture 2-2 Casing House

The indicator lights of the front panel indicate the current working status of the switch, The specific description is shown in below table 2-1:

Table 2-1 Front Panel Indicator Light Instruction

PWR1 PWR2	ALARM		RUN	LINK/ACT		10/100M	
Red light on	Green light off	Green light flashes	Green light periodically flashes	Green light on	Green light flashes	Green light on	Green light off
Power supply normal	No alarm	Alarm	System work normally	Link established	Data transmission	100M	10M

100MBased FX port

The product is equipped with multiple 100Base-FX full-duplex single-mode/multi-mode FX port, with optional port SC, ST or FC. The FX port needs to be used in pair (TX and RX are in pair), the TX port is the fiber transmitting end, connecting with the fiber receiving end RX of the other remote switch FX port. The RX port is the fiber receiving end, connecting with the fiber transmitting end TX of the other remote switch FX port. Two redundant 100Base-FX ports can be used to establish a fiber redundant ring network. If system fails, the ring network redundancy recovery time is less than 20ms, which can effectively improve the reliability of network operation.

100MBased FX port mainly has three type of port: SC, ST and FC, refer to below picture 2-3.

Picture 2-3 SC/ST/FC Port SFP Module

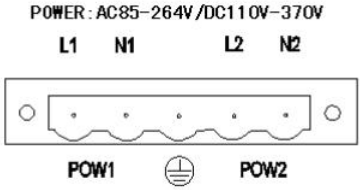
Ethernet RJ45 Port

The product is equipped with multiple 10Base-T/100Base-TX Ethernet ports. Each RJ45 port with adaptive function, supporting auto MDI/MDI-X connection, can connect the switch with terminal equipment, servers, hubs or other switches via straight line/cross-over cable. Each RJ45 port supports IEEE802.3x adaptive function, so the optimum transmission mode (half or full duplex) and data rate (10 Mbps or 100Mbps) can be automatically selected (the other connected equipment must meet this feature). If the equipment which is connected to these ports does not support adaptive function, the port will force itself to work at the same rate as the other parties, avoiding full/half duplex mismatch, the transferring mode will be default as half-duplex mode, and the flow control will be automatically disabled.

Power Input Terminal:

The standard configuration of the series rack-mounting industrial Ethernet

switch is using dual redundant AD220V power supply. The terminal blocks of MIEN6024, MIEN6024-4/8S/M and MIEN 6026-2S/M use 7.62mm pitch terminals to connect two power inputs, the terminal blocks of MIEN6024-12/16/24S/M use 5.08mm pitch terminals to connect two power inputs. The power consumption is less than 25W. The power input terminal is as below picture 2-4.



Picture 2-4 Power Input Terminal

Switch Power Supply Requirements as below Table 2-2.

Table 2-2 Switch Power Supply Requirements

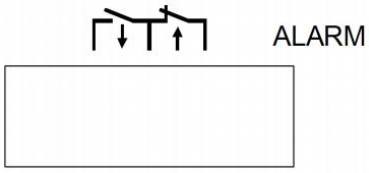
Power	Voltage Range	Operating Temperature	Storage Temperature	Humidity
DC24V	18~36VDC	-40°C~85°C	-40°C~85°C	5~95%
DC48V	36~72VDC	-40°C~85°C	-40°C~85°C	5~95%
AD220	85~264VAC 47-63Hz/ 110~370VDC	-40°C~85°C	-40°C~85°C	5~95%

Attention:

The supported power specifications of the equipment is 24VDC, 48VDC and 220VAC/DC. Please confirm whether the power supply is compliance with the requested power specification printed on the label of the device before power on, so as not to damage the device.

The alarm relay's one side port is NO, the other side port is NC, refer to below picture 2-5, the middle port is the public end, the left two terminals are NO relay, and the right two terminals are NC relay. If the switch is on normal work condition, the NO relay is closed, NC relay is open. If the system is power

off, dual power supplies is power failure, port link is down or network storm occurs, the NO relay is open and the NC relay is closed. The relay recommended switch load capacity is 1A (24VDC).



Picture 2-5 Alarm Relay

Relay Type	Power On	Power Off	Function
NO relay	Closed	Open	Power on alarm
NC relay	Open	Closed	Power down, line down or storm alarm

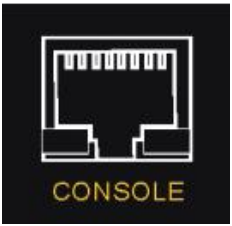
Table 2-3 Alarm Relay Instruction

Serial Network Management Port (CONSOLE)

CONSOLE port is a RJ45 port, as below picture 2-6. Please use MAIWE brand serial extension cable to connect with PC serial port. It is a standard 3 wire RS-232 cable.

Serial communication parameters are as follows:

Baud Rate: 9600; Data bits: 8; Parity: None; Stop bit: 1; Flow Control: None.



Picture 2-6 RJ45 serial port

2.2. Hardware Installation

2.2.1. Installation Requirements

The Industrial Ethernet Switch is a kind of single unit structure that fits rack-mounting installation. Before installing, first confirm suitable working environment for installation, including power requirements, sufficient space, being closed to other network equipment to be connected. Please confirm the following installation requirements.

●Power requirements: The standard product is charged by AD220 power supply. For other power supply methods, please refer to the product label printed on the housing and related user manual.

●Environmental requirements: Temperature -40 °C ~ 70 °C, relative humidity 5 ~ 95% (no condensation).

●Grounding resistance requirement: <5Ω

●According to the contract configuration requirements, check whether the fiber cables are in place, fiber optic connectors are appropriate.

●Avoid direct sunlight and away from heat sources or areas with strong electromagnetic interference.

●Standard 19'' U rack-mountable installation. Check for suitable cables and connectors.

Attention:

Make sure the power cable is disconnected before installing or connecting Ethernet switch. Calculate Max current of each power cable and public cables, observe all electric information so as to obtain allowed Max current of wires in different width. If exceeding the Max current, wires will overheat, causing serious damage to the equipment.

Meanwhile MUST pay attention on the following items:

Separate the power cable and other cables, if the two paths have to cross, MUST make sure that the intersection of these cables are vertical. Signal wires or communication wires and power cables cannot be laid in the same pipe. To avoid interference, wires with different signal characteristics should be separated. We can use the type of signal transmitted in a line to determine which wires should be separated. The rule of thumb is that wires with the same electrical characteristics can be bundled together. Separate the input and output wires. It is highly recommended that all equipment wires in the system should be labeled when necessary.

The switch should be connected to the protection ground: Grounding

and laying wires will effectively suppress the effects of noise caused by electromagnetic interference. A ground connection should be made before connecting the equipment, from the ground screw to the ground surface.

2.2.2. Mainframe Installation

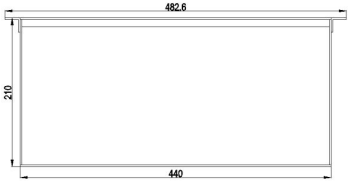
For most industrial applications, it is very convenient to install in a 19-inch rack. Check the rack installation before mainframe installation, including the following two items:

- Is there enough room for installing this product?
- Is there a power supply suitable for this product?

Firstly confirm the right place of installation, match the hole of switch and the hole of rack mounting, and then fix it with M5X14 type screw (recommended).

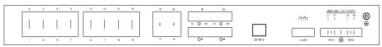
All different switch model detailed installation picture as below:

1.MIEN6024 and MIEN 6026-2S/M switch's installation dimensions refers from picture 2-7 to 2-11.

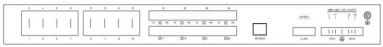


Picture 2-7 MIEN6024 and MIEN 6026-2S/M Switch Front Pannel

Picture 2-8 MIEN6024 Switch Rear Panel



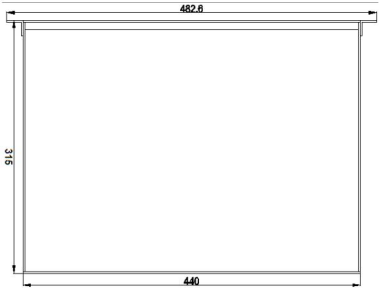
Picture 2-9 MIEN6024-4S/M Switch Rear Pannel



Picture 2-10 MIEN6024-4S/M Switch Rear Pannel

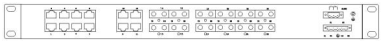
Picture 2-11 MIEN6026-2S/M Switch Rear Pannel

2.MIEN6024-12/16/24S/M switch's installation dimensions refers from picture 2-12 to 2-15



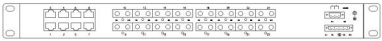
Picture 2-12 MIEN6024-12/16/24S/M Switch Rear Pannel

Picture 2-13 is MIEN6024-12S/M Switch (12*100M TX port+12*100M FX port) Rear Pannel



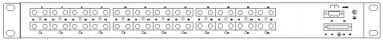
Picture 2-13 MIEN6024-12S/M Switch (12*100M TX port+12*100M FX port) Rear PPannel

Picture 2-14 is MIEN6024-16S/MSwitch (8*100M TX port+16*100M FX port) Rear Pannel



Picture 2-14 MIEN6024-16S/M Switch (8*100M TX port+16*100M FX port) Rear Pannel

Picture 2-15 is MIEN6026-24S/M Switch (24*100M FX port) Rear Pannel



Picture 2-15 MIEN6026-24S/M Switch (24*100M FX port) Rear Pannel

2.2.3. Cable Connection

After the correct installation, the cable can be installed and connected, mainly including cable connection of the following ports.

●Data transmission interfaces

The terminal equipment ports provided by the product is 10Base-T/100Based-TX Ethernet RJ45. Connect the terminal equipment with

straight line cable, connect the network equipment with cross-over cable.

●CONSOLE port

The CONSOLE port of the product can be connected to the serial port of the control computer.

●Power connection

After all other cables have been connected, connect the power supply that meets the product specifications.

2.2.4. Fiber Connection

MIEN6026-2S/M is equipped with 2*100Base-TX single-mode/multi-mode FX port, the type of FX port is selected with options of SC, ST and FC according to different requirements.

Attention：

This switch uses laser to transmit signals over fiber cable. Laser is compliance with Class 1 laser standard, normal operation will not harm the eyes. But if the equipment is power on, please DO NOT stare directly at the fiber port and fiber terminal section.

Follow up the below steps to connect insertable SFP module:

●Remove and retain the rubber bush of SC/FC/ST port, re-install the rubber bush to protect the fiber terminator when not in use.

●Check whether the fiber terminator is clean or not. Slightly wipe the cable plug with clean and wet tissue or cotton ball. Soiled fiber terminator will lower the quality of optical transmission and affect the ports performance.

●Connect the one end of fiber cable with Ethernet switch FX port, connect the other end of fiber cable with another equipment FX port.

●After connection, please check the FX port LNK/ACT indicator lights of switch front panel. If lights on, connection is available.

2.2.5. Laying Cables

Laying cables should be compliance with the following items:

●Check whether the specifications, model and quantity of all cables are consistent with the construction drawing design and contract requirements before laying the cables.

●Before the cable is laid, check whether the cable is damaged, whether there are quality certificates such as the factory record and quality assurance.

●The specifications, quantity, routing direction, and placement position of the required laying cables should meet the construction drawing design requirements. The laying length of each cable should be determined according to the actual location.

●User cable and power cable should be placed separately.

●There MUST be no disconnection in the middle of the laying cable, or a connector in the middle.

●The cable should be straight and neatly discharged in the aisle, and the curve should be even, smooth and straight.

●The cable should be straight in the channel, and should not exceed over the channel, block other access holes, and should be tied and fixed at the cable exit channel or cable bend.

●When the cables power cables and ground cables are placed in the same slot, the three types of cables cannot overlap and mix. If cable is too long, the cable grounding plate must be placed in the middle of the cable tray, and it cannot be pressed on other cables.

●Prevent the cable from knotting, reduce the bend and avoid small bend radius when laying the fiber on the tail. The lashing should be tight and not too tight. When placed on the cable tray, it should be placed separately from other cables.

●The two ends of the cable should have corresponding identifiers. The content of the identification should be concise and easy to maintain.

Attention:

When laying the fiber on the tail, it is necessary to prevent the cable from being knotted, reduce the bend and avoid small bend radius. If the bend radius is too small, the link optical signal will be seriously depleted and also it will affect the quality of communication.

2.3. Simple Test

2.3.1. System Self-examination

All indicator lights of the front panel will flash once at the moment the equipment is power on, it means the equipment is working well. And the Power indicator light is on afterwards. Run indicator light (system operating status indicator lights) will flash at 1s interval.

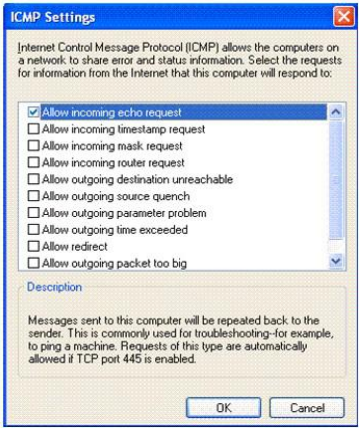
2.3.2. TX Port Test

As below picture 2-16, power on the equipment, connect two TX ports with Ethernet ports of two testing computers with straight-line network cable, sent Ping command to each other, if each side could receive command and does not loss packet, it means the hardware of these two tested TX ports is working normally.

Picture 2-16 TX Port Test

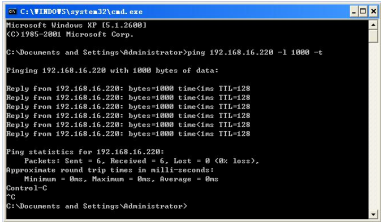
PING Command Example:

IP address of the No.1 testing computer is 192.168.0.10, IP address of the No.2 testing computer is 192.168.0.11, make sure to choose the first row of two computer's fireware local connection ICMP setting Allow Incoming Echo Request, the operation method is to open the advanced setting page of windows fireware, as below picture 2-17.



Picture 2-17 ICMP Settings Page

Please sequentially click START and RUN of No.1 testing computer, input cmd or command (cmd used for win2000/XP system, command used for win98/ 95 system), pop up control window, send ping 192.168.0.11—1 1000-t, (-1 means sending data packet bits, -t means constantly sending data packet), follow the same method for No. 2 testing computer, and run ping 192.168.0.11---1 1000 –t. If No.1 testing computer return to reply from 192.168.0.11: bytes=1000 times<10ms TTL = 128, and No.2 testing computer return to reply from 192.168.0.10: bytes=1000 times<10ms TTL = 128, use CTL+C command count packet loss rate as 0 after running is over 10mins, it means the equipment is on normal working status, as below picture 2-18.



Picture 2-18 Testing Computer Returned Page after Input Ping in CMD

2.3.3. FX Port Test

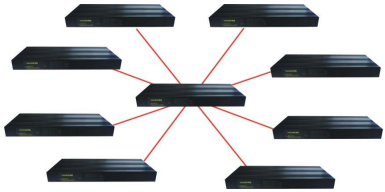
Use two equipment to construct an optical chain network as below picture 2-19. Connect any one TX port of each equipment with testing computer, sent Ping command to each other, if each side could receive command and does not loss packet, it means the hardware of these two tested TX ports is working normally, and LINK/ACT light of corresponding FX port should be on, it means the hardware of these two tested TX ports is working normally, and use the same method to test other FX ports.

Picture 2-19 FX Port Test

2.4. Network Topology

The series of Switches are capable of networking flexibly, and there are basically seven kinds of topology structure: Star Type, Chain Type, Single Ring, Inter-Ring One-Way Coupling, Inter-Ring Double-Way Coupling, Tangent Ring Coupling.

2.4.1. Star Type Network

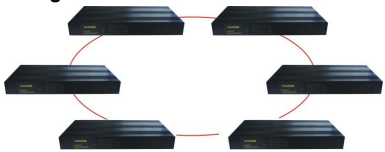


Picture 2-20 Star Type

2.4.2. Chain Type Network

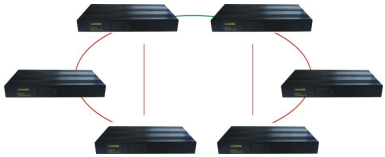
Picture 2-21 Chain Type

2.4.3. Single Ring Network



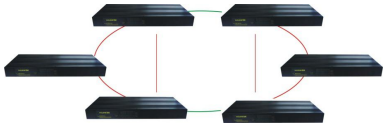
Picture 2-22 Single Ring

2.4.4. Inter-Ring One-Way Coupling



Picture 2-23 Inter-Ring One-Way Coupling

2.4.5. Inter-Ring Double-Way Coupling



Picture 2-24 Inter-Ring Double-Way Coupling

2.4.6. Tangent Ring Coupling

Picture 2-25 Tangent Ring Coupling

3. Serial Port Console Configure Basic Parameters

MAIWE Brand managed switches support Web access, Web configuration and Web management. Before conducting the specific operations, ensure that http user network equipment and switch that are visited are in the same network segment.

3.1. Setup Managed Switches IP Address via Super Terminal

Connect the MAIWE Brand managed switch console port with PC serial port with a serial cable offered by us, open the PC's super terminal, windows users can find the super terminal thru the path: Start-Application-Attachment-Communication. You need to establish a new link once open the super terminal and then need to select the communication port connected with switch using the below configuration parameters:

Baud Rate: 9600; Data bits: 8; Parity: None; Stop bit: 1; Flow Control: None.

3.1.1. User Account and Password

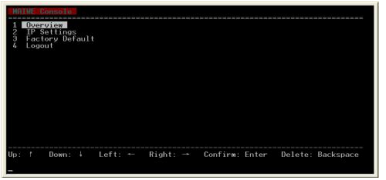
After successfully configuring the super terminal, click Enter, you will see the page as below picture 3-1.

Picture 3-1. User Account and Password Setting Page

Input user account and password, the default user account and password are both: admin, it's needed to click Enter each time finishing typing, after login you will access to console application.

3.1.2. Console Menu

Console menu is inclusive of four functions: 1. Basic information, 2. IP setting, 3. Recovery factory default setting, 4. Return to log-in page, as below picture 3-2. Make selections by moving the upward or downward arrows, click Enter and go to sub-module function.



Picture 3-2. Console Menu Page

Overview: Check system basic information

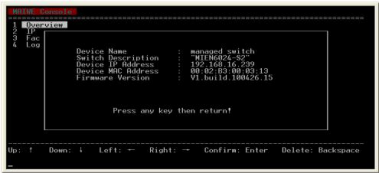
IP settings: DHCP server automatically assign one IP address or appoint one fixed IP address.

Factory Default: Recovery factory default parameters.

Logout: Logout the console application and return to login page.

3.1.3. Overview

In the page of Overview subitem, some system information of the switch are listed, such as switch name, description, IP address, MAC address and fireware version. Details see below picture 3-3.



Picture 3-3. Overview Page

Device Name: User can revise via web management.

Switch Description: Device model, different model has different description, which user cannot revise.

Device IP Address: It's allowed for user to revise.

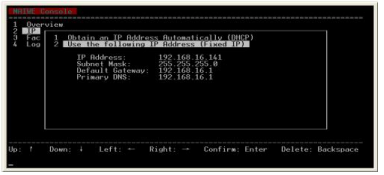
Device MAC Address: It's not allowed for user to revise.

Fireware Version: It's allowed for user to revise.

Press any key then return: Return to console main menu page.

3.1.4. IP Settings

Choose IP Settings while setup IP address via console application, prompting as below picture 3-4.



Picture 3-4 Settings Page

Setup a new IP address for the switch. While selecting Obtain an IP Address Automatically (DHCP), the switch will be automatically assigned one IP address thru DHCP server, while selecting Use the Following IP Address (Fixed IP), IP address, Subnet Mask, Default Gateway, Primary DNS these four items can be edited to setup a fixed network parameters.

IP address and Gateway should be in same network segment, as well as the IP address of network equipment that accesses to Web administrator. Consult the network administrator while setup IP address or other network parameters to avoid that web administrators cannot login due to faulty settings. After successfully setting the IP address, it's allowed to access the switch's web page by using the IP address.

3.1.5. Factory Default

This function will recover all configuration parameters to factory default.

Attention:

After successful recovery, the switch will automatically restart the software, but it's still suggested to power on the switch again to remove some contents in the RAM. Noted that the current IP address is 192.168.16.253, user needs to correct corresponding network parameters first and then accesses to web management.

3.1.6. Logout

This function will logout the console application of MAIWE Brand managed switches. To avoid to inadvertently revise some core functions of the switch, it will only return to login page after logout console application, but not really logout console application and enter the switch's background operation system CLI.

4. WEB Management Function

Statement:

All the functions interface and configuration introduced below are prevail in kind.

MAIWE Brand managed switches is embedded with web server, provide a user-friendly method to access and configure the switch. User can access the series of switched via IE, Firefox or other browsers (Note: better to use IE browsers to upgrade system).

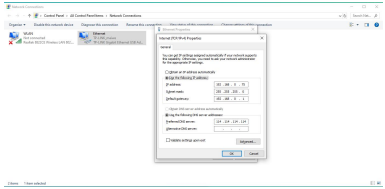
Both switch and PC's IP address should be in the same network segment if accessing the switch via Web. Correct PC's IP address to ensure its IP and switch's IP in the same LAN, Windows user refers to the following operation steps:

Start→ Control→ Network and Internet Connect→ Network Connect→ Local Connect→ Property→ Internet（TCP/IP）

MAIWE Brand managed switch default IP: 192.168.16.253. PC IP: 192.168.16.X (X is any number from 2~254, except for 253).

After modifying PC's IP address, it's allowed to use default IP address: 192.168.16.253, accessing the switch via Web and setting related configuration operation.

Specific windows system operation page see below picture 4-1.



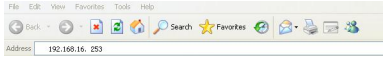
Picture 4-1 IP Settings Page in Windows

After changing the IP address of the PC, you can use the default IP address: 192.168.16.253 to access this series of switches through the Web and perform related configuration operations.

This manual selects the MIEN6026 model for description. The different models of the same series only differ in the number of optical ports and electrical ports. Most of the functions are the same, and the operation methods are the same, so they will not be described separately.

4.1. WEB Login

Open the browser, input default IP address of the series of switches in the address bar, as below picture 4-2.

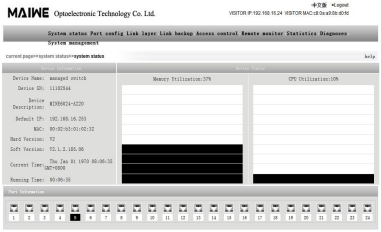


Picture 4-2. Input IP address in Address Bar

Click Enter, it will pop up a form, prompting user to input account and password, as below picture 4-3.

Picture 4-3 Input User Account and Password

Default user name and password are both: admin. If user name or password are input incorrectly, the managed switch's Web Server will provide three chances in total to input user name and password, if user fails three times, and the browser will show 401 Unauthorized error. Input correct user name and password, it's allowed to enter Web server main page if the identification is okay, as below picture 4-4.



Picture 4-4 Web Server Main Page

Attention:

1.Users can use IE, Firefox, Google and other browsers to visit Web server, there are maybe some difference in display page between different browsers. If it effects the normal usage, please change to IE, Firefox or Google.

2.The series of switches have been tested significant times with IE, Firefox, Google and other browsers, and all can be used normally, it's suggested to use IE browser while upgrade kernel program to avoid problems.

4.2. System Status

4.2.1. Equipment Information

The equipment information is inclusive of the device name, description, IP address, MAC address, fireware version. See below picture 4-5.

Picture 4-5 Equipment Information

●Equipment Name: Switch model name in the marked network, can be modified by user.

●Equipment Number: Number description defined by switch manufacturer.

●Equipment Description: A brief introduction of the switch.

●MAC Address: the Switch managed system MAC address.

●Hardware Version: Switch current hardware version.

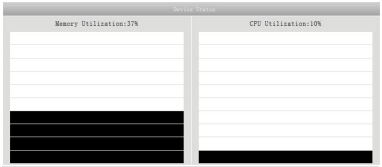
●Software Version: Switch current Firmware Version.

●Current Time: When the switch is power on, it is 1970 Linux time, user can modify it, if using ntp, switch can connect with internet and auto synchronize with server clock.

●Running Time: Time running starts since switch power on. When the switch resets or cuts off and restart, time running will restart from zero.

4.2.2. Equipment Status

In the form of equipment status, black stripe stands for system memory and CPU usage, as below picture 4-6.



Picture 4-6 Equipment Status

Memory usage: The internal CPU of the equipment has extension of external SDRAM, memory usage reflects how many space has CPU used the external SDRAM.

CPU usage: Switch is embedded with a high-performance CPU inside, CPU usage reflects the how busy the CPU is.

4.2.3. Port Information

Port total numbers differ from different model of switches. If the port's connection is normal, the port background color is black green. If the port's connection is abnormal, the port background color is white, as below picture 4-7. It will auto display every time if there is new connection status changes, it's no need to manually refresh the page.

Picture 4-7 Port Information

4.2.4. Menu and Auxiliary Function

The webpage menu is system status, port setting, two layer characters, link back up, access control, remote monitoring, ports statistics, network diagnosis, system management. See below picture 4-8.

Picture 4-8 Menu and Auxiliary Function

The functions are listed as below table 4-1.

Menu	Page	Function
System status	Equipment information	Name, number, software version, IP address, etc
	Equipment status	CPU utilization, etc
	Port information	Port numbers, etc
Port setting	Port setting	Configure switch ports basic information, such as: speed mode, flow control status
	Bandwidth management	Switch rate management
	Broadcast storm suppression	Set the type of storm suppression and inhibition rate
Lay 2 characters	QoS	Setup 802.1p, port priority and DSCP priority, etc
	VLAN	Display the table of 802.1q VLAN and VLAN port and set configuration and management, VLAN TRUNK is existed in the advanced settings of 802.1Q VLAN
	IGMP Snooping	Set IGMP, Enable Query, query intervals, etc
	Static multicast	Set the static multicast, MAC address and its corresponding ports
Link backup	Fast ring network	Set fast ring network port and ring type
	Trunk	Set port trunk group
	Rapid Spanning Tree	Set Rapid Spanning Tree detailed information

Access control	User password	User authorization and password management
	Login control	Modify the system's firewall to limit access to client IP address
	Port authentication	Separate business and authentication
	Authentication database	Add or delete the stored user name and password in the database
	MAC port locking	MAC address and other one port bound setting
Remote monitoring	SNMP	SNMP agent provided to manage switch equipment
	Email log	Periodically sent syslog to appointed users via E-mail
	Relay alarm	Set alarm type and display the alarms
Port statistics	Frame receive statistics	Various frame statistics, such as unicast, multicast, etc
	Frame send statistics	Various frame statistics, such as unicast, multicast, etc.
	Total frame statistics	Various frame statistics, such as unicast, multicast, etc
	MAC table address	Display the MAC table address
Network diagnostics	Port mirroring	Set port mirroring and port collection
	Network diagnostics	network failures analyzes, network testing, or problem solving
System configuration	Time setting	Setup system time
	Address setting	Setup IP address
	System information	Equipment model, CPU and other related parameters or review
	Log information	Display log information and manage it

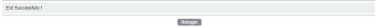
	Document management	Switch software upgrade, obtaining, saving or switch configuration recovery.

Table 4-1 Menu Function Description Table

The right side of menu is help-link, click Help at any page, it will pop up the help page of current page function, as below picture 4-9.

Picture 4-9 Help Page

Every page top right corner has Logout link, at any time user can click Logout, prompting as below picture 4-10.



Picture 4-10 Exit Login Page

Click Login Again and then you will enter identification from.

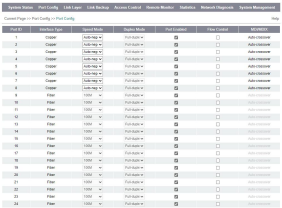
The top right of the menu is Access IP Address: 192.168.16.45 MAC Address: bc:5f:f4:5d:69:f6, which is current PC's IP address and MAC address while accessing the switch's web server.

4.3. Port Configuration

Port setting is inclusive of three submenu: port setting, broadband management and broadcast storm suppression.

4.3.1. Port Setting

Port setting page as below picture 4-11.



Picture 4-11 Port Setting

Port setting in the picture is default setting, every configuration item statement is as below:

Port ID: Display the switch's all ports, 26 ports in total as the picture.

Port Type: Display every communication port media type, such as RJ45 port or FX port, the FX port and TX port in above picture is only related with communication but not related with port type.

Baud Rate Mode: Multiple options button, including three kinds mode, auto-negotiation, 10M, and 100M rate. Auto-negotiation is default, supporting communication port auto-negotiating with the connected equipment via IEEE802.3u protocol, selecting the best rate to communicate. 10M and 100M rate is enforcing mode, requiring the port to communicate with the same rate. As auto-negotiation is default mode, the connected network equipment should also use auto-negotiation mode, or the switch will default setup the port as half-duplex mode if auto-negotiation fails.

Duplex Mode: Including full duplex and half duplex two options, only start the enforcing rate mode while auto-negotiation mode is invalid.

Port Activation: When the option is selected, it will enable the port. The port will be disabled if the option is not selected.

Flow Control: Flow control is used to manage data transmission of two nodes PC network, two nodes must support flow control so that it works, if connected network equipment does not support flow control, it's suggested to shut down the function because overmuch pause frame or conflict signal will cause communication problem. If data flow is discarding, flow mechanism performances very clear, it can be enabled or disabled, the default setting is disabled.

Polar Transformation: MDI (Medium Dependent Interface) , MDIX("X" is cross line), it is a connection method of Ethernet port connecting with router, HUB and switch. The series only use Auto-MDI/MDIX, supporting auto-flip function, which cannot be revised by user.

As for port configuration, a brief conclusion is as below table 4-2.

Table 4-2 Port Configuration Information

Setting Item	Description	Default
Port Type	Media port type, RJ45 or FX port	Factory default
Mode	Transmission mode of two node points	Auto-negotiation
Flow Control	Data transmission	Disabled

	management of two node points	
Polar Transformation	Media port cable type	Auto flip
Port Activation	Enable port configuration	Enabled

Statement

MAIWE Brand managed switches provide Web page to configure, all configuration parameters in the page will be submitted to switch after clicking Setting, all modification made by user will be cancelled if user does not click Setting first and exits the page. Clicking Cancel will not submit user's all modification and recover the settings as it used to be.

The others are the same except for the special ones, settings will be saved after click setting.

Attention:

1.Auto-negotiation mode are all TX port default mode, while TX ports are auto-negotiation mode, the connected network equipment should also use auto-negotiation mode, or the switch will default setup the port as half-duplex mode if auto-negotiation fails.

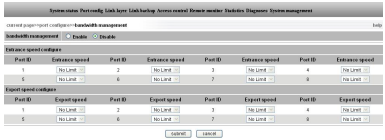
2.Flow control is used to manage data transmission of two node points PC network, two node points must support flow control so that it works, if connected network equipment does not support flow control, it's suggested to shut down the function.

3.Flow control can be enabled or disabled, default setting is disabled mode. Using flow control will generate many pause frame, overmuch frame may cause pause frame storm, so please be careful to use flow control function.

4.3.2. Bandwidth Management

The equipment supports rate-based port limitation, including entrance and exist rate limitation. As below picture 4-12, user can limit each port's communication rate or cancel port rate limitation. User can choose a fixed rate in the scope of 64Kbps ~ 100Mbps, the minimum granularity is 64Kbps. The type of port limitation includes PC all unicast packet, multicast packet and broadcast packet. The equipment provide dual-direction rate limitation. Entrance rate is the real rate when PC and other equipment flows to switch's port. The exit rate is the real rate when switch's port flows to connected equipment. If the entrance and exit rate of two equipment's port are limited, the

real rate will be the minimum figure of the two.



Picture 4-12 Bandwidth Management Page

Attention

1.If the port is up to appointed rate, switch will not limit the rate immediately because there is a 128K data buffer for both enter and exit, only if the buffer has been running out , it will start to limit the rate.

2.If connected equipment all enable flow control in the use of port rate limitation, the rate change between equipment will be a steady curved line. Switch will determine whether or not abandon the exceeded flow message based on whether or not start flow control.

3.If both use flow control in the use of port rate limitation, packet should not be discarding. The representation of packet loss is that sometimes the transformation rate is fast sometimes is slow.

4.Port rate limitation requires high-quality network cables, otherwise there will be a lot of conflict packet and broken packet.

4.3.3. Storm Suppression

There will be broadcast storm if host system responses to a constantly recurring packet, or try to response to an unanswerable system on the internet. Request or response packet will constantly produce in order to change the status, which will result in worse situation. With the increasing amount of network packet, discarding will occur, which will lower the network performance or even lead to network breakdown. Network storm is a kind of breakdown of network discarding resulting from snowball effect in the very beginning period, right now the majority regard network discarding or breakdown due to constant overmuch broadcast as broadcast storm.

There are various reasons for network storm, for example, a redundancy or incorrect disconnection generates the ring network between switches, broadcast packet and multicast packet transmit to other ports via switch, these ports that receive broadcast and multicast packet will constantly recur broadcast, which will cause broadcast storm. Broadcast storm can stop others'

malicious attacks in some conditions, such as DOS (Denial of Service) attack, DOS send ICMP request to other broadcast address thru one host, resulting in other mainframes response to the broadcast address, which will cause broadcast storm due to DOS attack.

We use RSTP or Mwring private protocol to prevent ring network generation, the network storm suppression mentioned here mainly aim to network discarding due to constant recurring overmuch broadcast. If enabling storm suppression function, this kind of attack will be prevented. As for the type of network storm, our equipment is capable of examining four kinds of broadcast packet:

1. Broadcast packet: Target address is FF-FF-FF-FF-FF-FF data frame.

2. Multicast packet: MAC address is the least order of the most significant byte is odd data frame.

3. MAC Control Frame: If the length and type area of Ethernet is 0x8808, it means the data frame is MAC control frame.

4. Destination locating failure frame: The MAC address of the data frame does not exist in the internal index table, then send the data to all ports.

Storm suppression configuration as below picture 4-13

Picture 4-13 Storm Suppression Configuration Page

Max Rate : 5 levels in total, 3%, 5%, 10%, 20% and 30% in separate, the basic rate of 100M port is 100Mbps.

All configuration parameters in the page will be submitted to switch after clicking Setting, all modification made by user will be cancelled if user does not click Setting first and exits the page. Clicking Cancel will not submit user's all modification and recover the settings as it used to be.

Attention:

1.The Max length of Ethernet data frame is 1518 Bytes, each 64Kb data communication traffic includes approx. 6 Ethernet data frames of 1518 bytes. The minimum length of Ethernet data frame is 64 Bytes, each 64Kb data communication traffic includes approx. 128 Ethernet data frames of 64 bytes. In network broadcast packet is more than 800pc/s, network delay is relatively obvious, while broadcast flow usually is 64 Bytes data frame in network; it's suggested to setup 3% based on above theory, the 64 bytes data frame is more than 5000pc/s while using other settings.

2.Storm suppression and bandwidth management is based on same logic, suppressing the storm is to limit rate correspondingly, so the suppression percentage is effected by R/T buffer, the rate change is a fluctuant curved line.

3.Destination address is multicast address but unrecorded multicast packet in multicast table which belongs to destination address locating failure packet.

4. Please be careful to use MAC control frame and destination locating failure frame, it's suggested to enable MAC control frame storm suppression while using flow control function for constructed-ring ports in the ring network.

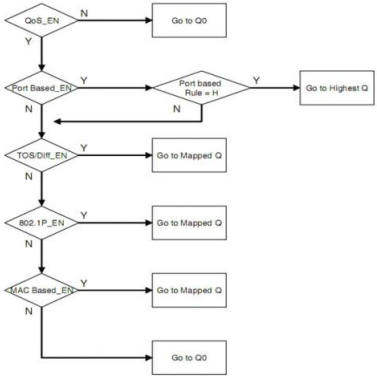
4.4. Layer 2 Characters

Layer 2 characters are inclusive of QoS, VLAN, IGMP Snooping and Static multicast.

4.4.1. QoS

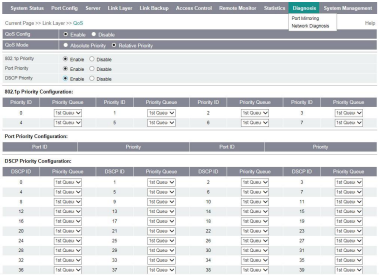
QoS(Quality of Service)is conducted by exchange chip's 4 interior priority queues, the packet's staying duration of the switch at advanced priority queue is shorter, supporting shorter latency for some delayed sensitive communication traffic, the data packet at lower priority queues is on the contrary. MAIWE brand managed switches can classify the data packets to the corresponding level according to port ID, MAC address, 802.1P priority label, DiffServ and IP TOS. QoS operation mechanism's actual scheduling at full speed is conducted based on advantaged method and advanced priority queues mixed mode.

Each port provides 4 queues at most when dealing with packets in different priority, after enabling the function, QoS mechanism will transfer the received packet to the suitable exit queue according to the principle as attached picture 4-14.



Picture 4-14 QoS Mechanism Flow Chart

QoS configuration page as picture 4-15



Picture 4-15 QoS Configuration Page

When QoS is disabled, all the options below are disabled, it's no need to enable the priority, so all packets are at lowest priority queues, and select the option Enable first and then setup QoS, as below picture 4-16.

Picture 4-16 QoS Setting Page

The second step is to choose and use absolute priority or relative priority. When selecting the absolute priority, switch will deal with the advanced priority

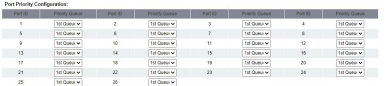
queues firstly and then lower priority queues. As for relative priority, switch will deal with the advanced priority queues firstly but at the same time juggle with data of lower priority queues. 4 queues forwarding rate from high to low are 8:4:2:1, as below picture 4-17.

Picture 4-17 QoS Control Type Page

Priority settings has three kinds of methods: 802.1P priority, port priority and DSCP priority. Any kind of priority can be enabled, port priority has privilege among the three kinds of priority configuration, as below picture 4-18.

Picture 4-18 Three Kinds of Priority Setting Page

Port priority only can use the highest and lowest two queues of switch's 4 priority queues, if one port uses the highest priority queues, the packets which sent from all ports will enter the switch's highest priority queues regardless of IEEE 802.1P and DSCP priority settings, this is to say port priority has absolute privilege right comparing with other two priority settings. Port priority configuration see below picture 4-19.



Picture 4-19 Port Priority Configuration Page

802.1P is expanding protocol of IEEE802.1Q (VLAN Label technology) standard, they work cooperatively. It provides an executive QoS mechanism in layer 2 MAC (Media Access Control) in essence, VLAN Label have two parts, VLAN ID (12bit) and priority (3bit). IEEE802.1Q VLAN standard does not define and use priority filed, while 802.1P defines the filed, so there are 8 valid IEEE802.1P priority grade (3 bits), and IEEE802.1Q label have 3 filed as user's priority. See below picture 4-20.

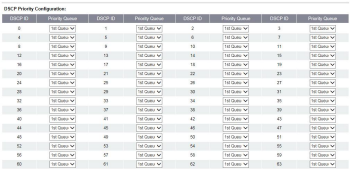
Picture 4-20 802.1P Priority Configuration Page

Priority 0 is Default Value, and it will be auto without setting other priority value. Priority 0 and priority 1 reflects to the first queue in the equipment

default settings, which is the lowest priority queue. Priority 2 and priority 3 reflects to the second queue, priority 4 and priority 5 reflects to the third queue, priority 6 and priority 7 reflects to the highest priority queue with fastest transmitting speed.

DiffServ is differentiated service, is assigned with a simple, upgradable, rough-divided computer network system, in the modern IP network, layer 3 is used for network communication management and providing service quality guarantee. For example, DiffServ supports to provide relatively shorter reflecting time to ensure the key network data such as audio and video pass through successfully, and provide simple, best-effort communication guarantee for non-key data communication such as web communication or file transferring.

DiffServ is a kind of layer 3 solution by using DSCP area in IP header to store priority information, it uses 6 bits among the 8 bits of IP header TOS area, so there are 64 types of priority division in total, as well as compatible with TOS. DSCP uses 64 values to reflect the user definition service level, supporting to establish more control operations in network communication. DSCP is an advanced intelligent method to distinguish the priority with different types of communication traffic. Based on the DSCP (DiffServ Code Point) value in IP header, the series of switches can classify the communication packet service level. The switch supports IPv4 and IPv6 of DSCP. If the DSCP priority is enabled, the switch will classify the communication traffic level based on DSCP value. DSCP configuration as below picture 4-21.



Picture 4-21 DSCP Priority Configuration Page

Attention:

1. Switch inside only has 4 transmitting priority queues, so although 802.1P and DSCP each have 8 and 64 priority, but finally need to be carried out thru switch, so the priority of 802.1P and DSCP are at same transmitting queue in default settings, all packets in the same transmitting queue have same priority in term of hardware despite that they could be setup as different priority in term of software.

2. As for absolute priority, switch will deal with the data at the fastest priority queue firstly and then deal with the data at lower priority queue. As for relative priority, switch will deal with the data at the fastest priority queue but at the same time juggle with data of lower priority queue. 4 queues transmitting percentage from high to low are 8: 4: 2: 1;

3. If three types of priority are enabled at the same time, priority ranks from high to low is port>DSCP>802.1P.

4. Port priority only has two kinds, the highest and the lowest; port priority has the privilege in the three types of priority, which only means the switch will unconditionally deal with the data of the port at the highest priority regardless of the settings of 802.1 and DSCP. If the port priority is setup as the lowest priority, 802.1and DSCP still can change its priority.

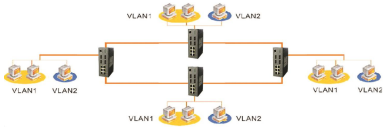
5. 802.1P is extension of 802.1Q, priority identification is placed in VLAN Tag, which is only valid for VLAN packet of 802.1Q.

6. DSCP priority identification is placed in IP header, which is only valid for IP data packet; IP data frame priority can pass through the whole internet. DSCP is compatible with IPv4 TOS, supporting to use layer 3 equipment with TOS priority solution to conduct operation.

4.4.2. VLAN

VLAN refers to Virtual Local Area Network technology, VLAN is a method to establish independent logic network from the real physical network, in which several VLANs can be existed in the same physical network in the meanwhile. VLAN can effectively minimum the broadcast scope for easy network management via data-incommutable and separate logic network segment (such as company department). In actual, if a router is added among these different virtual network segment, they can still exchange the data via the router. It's effective to suppress the broadcast storm via VLAN.

MAIWE brand managed switches support port VLAN and IEEE 802.1Q VLAN, but they cannot be used in the same time, the default settings is to enable the port VLAN. As for IEEE 802.1Q VLAN, please refer to below picture 4-22.



Picture 4-22 IEEE 802.1Q VLAN Network Topology

Port VLAN

Port VALN provides a solution that can divide the switch's ports into different virtual private areas. It's not allowed to exchange the data between different virtual private areas, so it's relatively safe to maintain data in respective private area.

MAIWE brand managed switches provide flexible VLAN configuration for each port, VLAN port filters the communication traffic out of scope of the private area as a filter. Enable the port VLAN in default settings, add one default table among it, and put all ports in the VLAN, as below picture 4-23.

Picture 4-23 VLAN Item and Port Page

User can configure port VLAN via web page based on self-requirements, see below picture 4-24, advanced setting buttons are only valid under 802.1Q VLAN, current status is hidden status.

Picture 4-24 VLAN Port Configuration Page

Steps as follow:

●Delete default table first before add own VLAN, or all ports are still at least in one same VLAN, which cannot separate the communication data. Select default in the table and then click Delete Table.

●Input added VLAN name in group name frame, name must be the combination of numbers or letters, such as group1.

●Select port of added VLAN the in the port list, it's convenient for user to choose required port with the right two buttons Choose Used Port and Select All, there will be a switch for two options of Select All and Cancel Select All after clicking Select All.

●Click Add Table so as to add VLAN into the table after selecting the port.

●Add new VLAN group with same method.

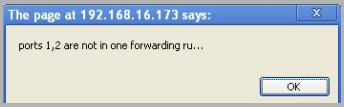
●If there are still some rest of ports not being added into any VLAN, it's needed to add these ports into new VLAN.

●Fill in the VLAN name in group name, click Choose Unused Port and add it to table.

Attention

1. Delete default table first, or all ports are still at least in one same VLAN, which cannot separate the communication data.

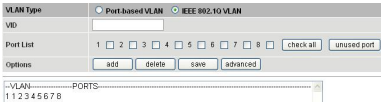
2. All ports must be added into any group of VLAN, such as port 1,2 is not added to any VLAN, then chick Save Setting, popping up the below prompting picture:



3. Any one port can be added into several groups of VLAN, this port can communicate with all added VLAN members.

802.1Q VLAN

MAIWE brand managed switches also support IEEE 802.1Q VLAN. VLAN can span multiple switches to be partitioned by IEEE802.1Q. The switch supports standard IEEE802.1Q, and it is compatible with other switches supporting IEEE802.1Q standard, as well as supports revision of 802.1Q label and connects with equipment no matter what it can identify 802.1Q label or not. It's very convenient to use the series of switches to configure IEEE802.1Q VLAN. IEEE802.1Q VLAN can be configured via web page as below picture 4-25.



Picture 4-25 IEEE802.1Q VLAN Configuration Page

The method of how to add 802.1Q VLAN of VLAN table is same as port VLAN, it's necessary to emphasis that VID value must be the figure in the scope of 1~4094. There is one default table with VID value 1, all ports is in this VLAN, see below picture 4-26.

Picture 4-26 IEEE802.1Q VLAN Item and Port Page

Setting steps as below:

●Delete default table with VID value 1 first and then added own VLAN, or all ports are still at least in one same VLAN, which cannot separate the communication data. Select 1 in the table and then click Delete Table.

●Input added VID in VID figure frame, the value must be the integer and in the scope of 1~4094.

●Select port of added VLAN the in the port list, it's convenient for user to choose required port with the right two buttons Choose Used Port and Select All, there will be a switch for two options of Select All and Cancel Select All after clicking Select All.

●Click Add Table so as to add VLAN into the table after selecting the port.

●Add new VLAN group with same method.

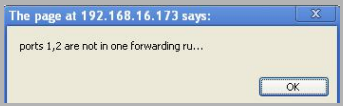
●If there are still some rest of ports not being added into any VLAN, it's needed to add these ports into new VLAN.

●Input added VID in VID figure frame, click Choose Unused Port and add it to the table.

Attention:

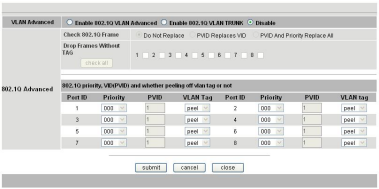
1. Delete default table with VID value 1 first, or all ports are still at least in one same VLAN, which cannot separate the communication data.

2.All ports must be added into any group of VLAN, such as port 1,2 is not added to any VLAN, then chick Save Setting, popping up the below prompting picture:



3. Some ports can be added into several 802.1Q VLAN, but it's not recommended to do so.

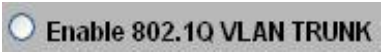
In above VLAN configured Web page , when selecting IEEE802.1Q VLAN , Advanced Setting button is enabled, it's hidden in port VLAN , click Advanced Setting, popup advanced setting page as below picture 4-27.



Picture 4-27 IEEE802.1Q Advanced Setting Page

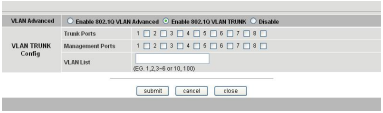
Advanced setting is default as disabled, all following options in grey are in

disabled status, click Enabled so as to setup. User can have smaller operation for VLAN function via the settings in this page, detailed explanation for settings as below.



:

VLAN trunk function makes multiple switches can partition VLAN after constructing the network. The web page is as below picture 4-28.



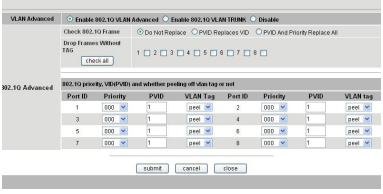
Picture 4-28 Enable 802.1Q VLAN Trunk Web Page

Trunk port list: Assigned trunk list

Port list management: It's only needed to set one list for one network to manage the switches in the network.

VLAN List: List VLAN ID of requiring to use trunk port.

Enable 802.1Q VLAN Advanced Rule, as below picture 4-29.

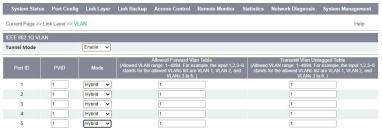


Picture 4-29 Enable 802.1Q VLAN Advanced Rule Page

802.1Q frame checking: VID refers to group ID when adding VLAN, the scope is 1~4094; PVID is port vid, same with below "port VID", PVID can be setup by user, as well as the priority. Replaced function is to replace the VLAN tag of received VLAN packet from the port with PVID or priority, non-replacement means non-execution of the order.

Discarding of non-TAG frame: If assigned one port receives packet of VLAN non-TAG, discard the packet. Please be careful to use this function.

Method used for configuring port PVID, priority and VLAN Tag is as below picture 4-30.



Picture 4-30 Port-based 802.1Q Priority, Port VID (PVID) and VLAN Tag handing method Configuration Page

Priority: Setup port default priority part, 3 bits in total, 8 kinds of priority is optional, currently the purpose of setting is only for replacement.

Port VID: Setup port default VID, currently the purpose of setting is only for replacement.

VLAN tag: It's an operation that VLAN packet sent from this port strip out or save its VLAN Tag. Striping out function is generally used when the connected port is terminal network, such as PC.

So that PC usually cannot receive the packet with VLAN Tag.

Attention:

1.It's necessary to delete the default VLAN group before modify VLAN settings because it covers all ports.

2.IEEE 802.1Q VLAN packet process: Data enter into the port---check if need to add or replace VLAN tag---check if forwarding table is allowed to transmit or discard---check if need to remove VLAN Tag---data exits from the port

3.IEEE 802.1Q VLAN have one more process of adding and removing VLAN tag comparing with port VLAN. As for this kind of VLAN, it's only allowed that the port is up-connect-port or terminal port.

4.If 802.1Q VLAN is enabled, PVID will auto update and be consistent with VLAN VID.

4.4.3. IGMP Snooping

MAIWE brand managed switches provide internet multicast management protocol, with function of auto snooping IGMP data packet, auto checking multicast members and maintaining a multicast forwarding table based on multicast group dynamic information. See below picture 4.31.

Picture 4.31 IGMP Snooping Configuration Page

IGMP Snooping function is default as disabled, selecting Enable first if it's needed to use IGMP function, setting parameters instructions is as below:

IGMP Query. Choosing whether to enable multicast members query function, IGMP query packet is used for checking existing multicast group, user can setup query interval. Each time multicast members will response a report after receiving the query packet, switch will update multicast table after receiving the members response report and recalculate the member's existing time if switch does not receive the members response report after many times checking, the switch will auto delete the multicast group members after exceeding the member's existing time.

The function can make switch work as IGMP state machine if there is no router or router does not support multicast in the network. If there is existing other IGMP query equipment, the query function can be disabled. Disabling the option will not periodically query multicast members, so as to reduce network load.

The function is default as disabled.

IGMP query intervals: The option will only be enabled after IGMP query option is enabled, it's to setup the interval of sending IGMP query. The interval settings cannot be too short, short interval will increase the network load, in the meanwhile the interval settings cannot be too long, overlong interval will cause slow multicast dynamic update.

Interval setting scope is 60~1000s, the default setting is 125s. It is software running time and not very accurate but within the range of allowed error.

Members existing time: Multicast group members existing time, it will recount each time there is member joining in the multicast group or switch receives the member's report packet, the member will be deleted in the multicast group if exceeds the time. Time settings cannot be too long or too short, it can be setup from 120 to 5000s, default setting is 300s.

Members can join in multiple multicast groups, it will count independently in each multicast group, it's software running time and not very accurate but within the range of allowed error.

Switch will send from all ports by default if it receives unknown multicast group packet.

After IGMP Snooping function is enabled, switch will dynamically maintain a multicast forwarding table, as below picture 4-32.

Picture 4-32 Unknown Multicast Group Forwarding List

The second item is dynamic maintained multicast address forwarding table, the first item is manually added static multicast table which will be stated afterwards, the type is fixed. Each time open Web page, contents in table 4-3 will refresh once.

Table 4-3 IGMP Setting Description Table

Setting Item	Description	Default Setting
IGMP Snooping function	Enable IGMP Snooping	Disabled
IGMP Query function	Enable switch IGMP query configuration	Enabled
IGMP Query Intervals	Switch query intervals	125s(protocol standard time)
Members Existing Time	Switch multicast address aging time	300s

Attention

1.If PC is one network port with multiple IP address, Windows system always responses with use of the bottom IP address, which perhaps will cause problem..

2. It's not suggested to exist multiple IGCP query, it may waste sources.

3. If the relations of unknown multicast groups is not certain, please select all ports.

4.4.4. Static Multicast Table

This switch supports manually add/delete MAC multicast address forwarding function, as below picture 4-33.

Picture 4-33 Static Multicast Forwarding Table Configuration Page

The statics multicast table and the IGMP Snooping dynamic multicast table use same multicast table, which is placed in the forwarding address table of switch's chip, not only keep the learning function, but also support MAX 4k multicast MAC address and 256 multicast forwarding port table, the difference is IGMP Snooping dynamically add/delete multicast table based on IGMP protocol, when aging counting is enabled, it will delete the outdated multicast group and its members, but static multicast table provides user to manually add/delete multicast table, which is defined as static in multicast table, static

MAC address performance forwarding function but is not dominated by aging operation, the packet of static MAC address included in destination address will be forwarded to assigned port, setting parameters instruction is as below:

Static multicast MAC address: Fill in the added MAC multicast address in this frame, the format is XX-XX-XX-XX-XX-XX, the first 3 bytes of multicast address are 6 binary 01-00-5E, the following multicast address is reserved by the switch, please do not use.

01-00-5E-00-00-XX (reserved multicast managed MAC address)

01-80-C2-XX-XX-XX (reserved Ethernet bridge managed MAC address)

Port Table: Select destination address as the forwarding port of the multicast MAC address, tick the port you are going to forward.

Processing Table: The table is used for operating multicast table, button Add and Delete is used to add/delete static MAC address. Existing static multicast table will be displayed in the below frame. It will update each time user open the web page or execute add/delete operation. There is added static multicast forwarding address (01-00-5e-01-02-05) as below picture 4-34.

Picture 4-34 Static Multicast Forwarding Address Table

Attention:

1. Add/Delete operation will be invalid immediately, it's no need to click Save like other pages.

2. Please do not use unicast as input address.

3. Please do not input reserved multicast MAC address, such as 01-00-5E-00-00-XX (reserved multicast management MAC address), 01-80-C2-XX-XX-XX (reserved Ethernet bridge management MAC address).

4.5. Link Backup

Link backup function setting: Mwring fast ring network, Trunk, and RSTP.

4.5.1. Fast ring network

Switches can be connected with other with redundancy link via Mring, when one of connection is cut off, the other one connection could fast auto recover, it has capability of link redundancy and fast recovery when network is cut off or breakdown. Mwring technology is developed by Wuhan Maiwe Communication Co., Ltd, is specially designed for high-reliable industrial control network application.

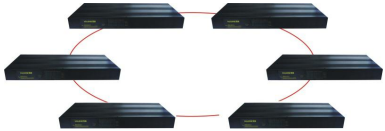
Network self-recovery time is less than 20ms in the multiple-ring network generated by switches with Mwring technology. Mwring technology allows user to take switches' some ports as ring network redundancy port to connect with other switches. When one of connection is cut off, Mwring redundancy

mechanism enables the backup link to fast recover the network communication. Table 4-4 based on comparison of redundancy technology recovery time is only for reference.

Table 4-4 Self-recovery time based on Redundancy technology

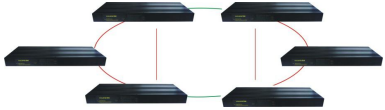
Redundancy technology	Mwring	RSTP	STP
Self-recovery time	<20ms	>5s	>30s

Normally, Miring technology can generate a ring network by three switches or above. Below picture 4-35 is a typical application demo based on Mwring technology.



Picture 4-35 Typical Application Based on Mwring Technology

Mwring technology could fast generate two types of ring network: single ring, inter-ring one-way coupling. Single ring is a basic unit made of two ports of switch, see above picture. Inter-ring one-way coupling is used to access two or more several single rings, and access the single rings in separate to generate ring network with one network cable as below picture 4-36.



Picture 4-36 Double-ring Connection

It's allowed that one or multiple rings exist in the same network for Mwring technology, but it must be equipped with unique ID for each ring, this ID is shared with the switches in the ring network. Web page of fast ring network is as below picture 4-37.

Picture 4-37 Fast Ring Network Configuration Page

Ring network group: Each switch supports four group of ring network at

most, three single ring and one double ring, any of which can be enabled. It's suggested to use less enabled ring network group, do not enable two single rings as well as double ring network to add complexity if one single ring meets the requirement.

Network identification: The ring ID mentioned above is integer within the scope of 1-254, each ring must has unique ID and ID should be shared with all switches that construct the ring, that is to say all switches access to the ring must use the ID to make network identification.

Port table: Select which ports will be connected to the ring, two ports are needed to be connected to the single ring, only one port is needed to be connected the inter-ring coupling.

Saving configuration parameters after finishing settings, Mwring function will be activated. A brief sum of configuration parameters instructions is as below table 4-5.

Table 4-5 Mwring Configuration Parameter Description

Setting Item	Describe	Default
Network identification	Identify different rings	250/251/252/4
Port table	Assign different port for different type of ring	25, 26/25, 26/25, 26/1
Type of ring network	Ring type of connecting switch (single ring, inter-ring coupling)	Single ring network
Active	Active Mwring technology	Active

Attention:

1)Mwring is MAIWE private protocol, it's only used for MAIWE brand same series of switches and not compatible with other company's switches.

2)Mwring and RSTP cannot be enabled at the same time, when user enables Mwring, RSTP will automatically close, when user enables RSTP, Miring will automatically close.

3)When Mwring is enabled, there is a short time for all switches to exchange packets to avoid redundancy link, and then ring network will be in steady status temporarily, as same as the situation when the main link is cut off for self-recovery, in this temporary steady status there could be packet loss but duration is very short (<20ms).

4)It's suggested to use less enabled ring network group, do not enable two single rings as well as double ring network to add complexity if one

single ring meets the requirement..

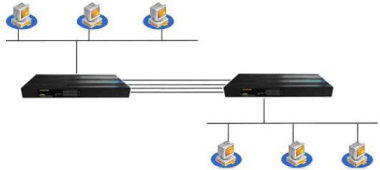
5)The recovery time of ring network is related to the number of switches that generates the ring network and the complexity of ring network, the recovery time less than 20ms is tested with 8 units of switches or below generating a single ring.

6)Please do not use function of trunk, port mirroring and rate limitation for entrance/exit of bandwidth management for ports which take part in constructing ring network.

7)Setup the third group of the ring network as enabled by default, default ring is 25 and 26 port, ID is 252, please do not select the wrong network port when generating the ring, or it will produce storm.

4.5.2. Trunk

The main function of trunk is bond multiple physical ports (normally 2-4) as a logic path, so as to work like a path. After bonding multiple physical link, it will not only increase the whole network bandwidth but also the data can be transferred via bonded multiple physical link at the same time, supporting link redundancy function. The rest of links are still working if the network is breakdown or one or several link is cut off. It's a very helpful and often used function when Trunk is generating redundancy network, as well as it's simple to use. Picture 4-38 below is an application case of using Trunk.



Picture 4-38 Application Case Supporting Trunk

The two switches in above picture generate a computer network via a Trunk group, the two switches are connected with four ports to improve bandwidth and achieve link redundancy.

MAIWE brand 100MBased managed switches support Trunk function, which authorizes two groups of Trunk in total and each group of trunk includes 2-4 ports as single logic link to improve bandwidth and link redundancy. When one of the physical link cannot be communicated or is failure, the other links in

the group of trunk will immediately take over and stay communication, in this case it can provide a fast recovery mechanism after one communication is cut off. Configuration of trunk function is based on the web page of below picture 4-39.

Picture 4-39 Trunk Configuration Page

Trunk group: The switch supports two group of trunk at most.

Port table: Choose assigned port in each group of trunk, each group of trunk can be assigned 2-4 100MBased ports, except for port 1, others can be added into trunk group (port 1 cannot be used for trunk). One port cannot exist in two groups of trunk at the same time.

Enable: Choose whether to enable this group of Trunks, and it will be enabled when you tick it. When using Trunk, you must enable it first, and then make a physical connection

Attention:

1.The switch supports two group of trunk at most, each group of trunk can be assigned 2-4 100MBased ports.

2.Port 1 cannot be used for trunk, that is to say port 1 does not support trunk function and cannot be added into any group of trunk.

3.One port cannot exist in two group of trunk at the same time.

4.Enable the trunk first and then proceed physical connection when use it.

5.The improvement of bandwidth is not just simple multiple relations concerned with the number of ports, whereas the bandwidth of trunk does not increase in most cases, which is determined by the forwarding mechanism of exchange chip.

6.Self-recovery time of trunk is very short, it will not loss packet with 100MBased rate.

RSTP (Rapid Spanning Tree Protocol)

STP:

STP is a kind of layer 2 management protocol, it can eliminate the network layer 2 ring path thru alternatively discarding network redundancy link, as well as support link backup function.

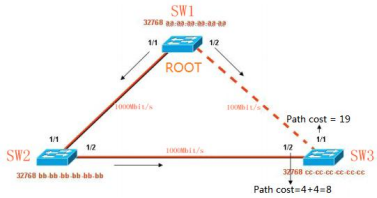
STP is not well known like router protocol because it is relatively small, but it controls the port forwarding. The real situation is indeed so, especially

running with other protocols. STP could stop the forwarding path of other protocols, causing different kinds of strange phenomenon.

802.1D defines the STP, its basic principle is very simple, there's no ring path for trees grown in the nature, as well if the network grow like a tree. Thus, STP defines the concepts of Root Bridge, Root Port, Designated Port and Path Cost, so as to cut redundant ring path and obtain link backup and path optimization by a method of generating a nature tree. The method of generating the tree is called SPA, Spanning Tree Algorithm.

To obtain these functions, switches (network bridge) must communicate some information, these information unit is called BPDU (Bridge Protocol Data Unit). BPDU is a kind of layer 2 packet, targeted MAC is multicast address 01-80-C2-00-00-00. All network bridge supporting STP will receive and deal with BPDU packet, the packet's data zone carries all useful information for STP calculation.

The working process of STP is to select Bridge Root firstly, the basis of selection is switch (network bridge) priority and switch (network bridge) MAC address combined Bridge ID, switch with minimum Bridge ID will be the Bridge Root in the network. In the network each switch (network bridge) is default as enabled, on the condition that switch (network bridge) priority is the same (default priority is 32768), switch (network bridge) with minimum MAC address will be the Bridge Root, all ports will be the assigned port and get into forwarding status. As below picture 4-40, SW1 is the Bridge Root when priority is the same.



Picture 4-40 Bridge Root Selection

The next, other switch (network bridge) will choose the strongest branch as the path to Bridge Root, corresponding port role will be the root port. As above picture 4-40, the link between SW1 and SW3 is 100M FE link, the default value of path cost of SW3 from port 1 to Bridge Root is 19, but the path cost of SW2 from port 2 to Bridge Root is 4+4=8, so port 2 is the root port, getting into the forwarding status. Similarly, if SW2 port 1 is the root port, then

port 2 is the assigned port and gets into the forwarding status.

A tree generates after Bridge Root and root port is confirmed, as the solid line in the picture. The next task is to cut redundant ring network, which is the dotted line, it's finished by discarding the corresponding port of non-bridge root, for example, if SW3 port 1 role is disabled port and gets into discarding status.

After Spanning Tree is stable over a period (30s by default), all ports get into forwarding status or discarding status. STP BPDU still will be sent from assigned port of each network bridge periodically to maintain the link status. If network topology changes, Spanning Tree will recalculate and port status will change as well.

RSTP

At the beginning of the century, IEEE came up with 802.1w standard, as the complement of 802.1D standard. It defines RTSP (Rapid Spanning Tree Protocol) in IEEE 802.1w. RTSP has three points of great improvement to get faster convergences rate (within 1s at fastest speed).

The first point of improvement is to setup two characters used for fast switch Alternate Port and Backup Port for Root Port and Designated Port, when Root Port/Designated Port is invalid, Alternate Port/Backup Port will get in the forwarding status without delay. All network bridge in above picture all run RSTP, SW1 is Root Bridge, supposed SW3 is Root Port of port 2, port 1 will identify this kind of topology, become the Alternate Port of Root Port, and get into discarding status. When port 1 is in the case that all links are invalid, port 2 will immediately get into forwarding status and no need to wait for double Forward Delay time.

The second point of improvement is to assign that port can get into forwarding status without delay only requiring a handshake with downstream network bridge in the point-to-point link of two exchange ports are connected. If three or more shared links of network bridge are connected, downstream bridge will not response to the handshake request sent from upstream assigned port and it's needed to wait double Forward Delay time to get in the forwarding status.

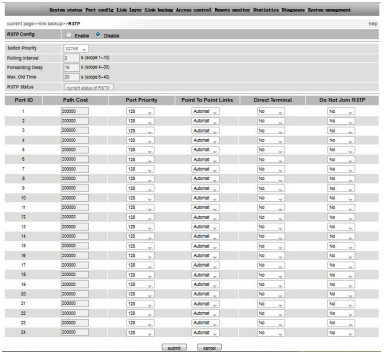
The third point of improvement is directly connect with the terminal end but not defines the other port of network bridge as Edge Port. Edge Port can directly get into forwarding status without delay. It requires man-configuration because network cannot get to know whether the port has been directly connected with terminal end or not.

As we can see, RSTP has a great improvement compared with STP. In order to support these improvement, the format of BPDU has made certain

revision, RSTP is still compatible with STP and two of the protocols can be constructed hybrid ring.

RSTP configuration instruction

Fast click RST submenu in Menu, popup the configuration page as below picture 4-41.



Picture 4-41 RSTP Configuration Page

RSTP configuration: Enable/Disable RST function, the default setting is disabled, RST and Mwring function cannot be enabled in the same time. When RSTP is enabled, RSTP will enable all ports, some ports will be discarded until convergence period is over, web server will not response in this period, after convergence is over and network tree is generated, web server can be used again. See attached picture 4-42.

Picture 4-42 RSTP Web Server Page

Switch priority: Setup the priority of switch (network bridge), switch priority and MAC address are combined into the bridge ID. Switch (network bridge) with minimum bridge ID will be the Root Bridge in the network. The smaller the ID is, the highest the priority is, and the more likely it becomes Root Bridge, the default value is 32768.

Query interval: Setup how long it will take the switch send BPDU packet once a time, small interval will fasten the RSTP convergence rate but increase the network workload, overlarge interval will increase the RSTP convergence

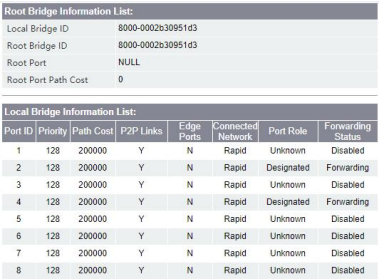
rate. The default value is 2, the scope is integer from 1-10 and measured in seconds.

Forwarding delay: Switch ports status maintains a time of forward delay during transition of learning and listening, and is measured in seconds. The default value is 15, the scope is integer from 4-30.

Maximum aging time: It refers to the validity of the packet after one switch receives a BPDU packet from other switch, and it's measured in seconds. The default value is 15, the scope is integer is 6-40.

Time setting value must meet the below formula: 2*(forwarding delay-1)>=Max aging time

RSTP status information: Click RSTP and find out RSTP status information, see below picture 4-43.



Root Bridge Information List:	
Local Bridge ID	8000-0002b30951d3
Root Bridge ID	8000-0002b30951d3
Root Port	NULL
Root Port Path Cost	0

Local Bridge Information List:

Port ID	Priority	Path Cost	P2P Links	Edge Ports	Connected Network	Port Role	Forwarding Status
1	128	200000	Y	N	Rapid	Unknown	Disabled
2	128	200000	Y	N	Rapid	Designated	Forwarding
3	128	200000	Y	N	Rapid	Unknown	Disabled
4	128	200000	Y	N	Rapid	Designated	Forwarding
5	128	200000	Y	N	Rapid	Unknown	Disabled
6	128	200000	Y	N	Rapid	Unknown	Disabled
7	128	200000	Y	N	Rapid	Unknown	Disabled
8	128	200000	Y	N	Rapid	Unknown	Disabled

Picture 4-43 RSTP Status Information Page

The page demos the switch under current network and MAC address 00-02-b3-02-02-02 is Root Bridge switch not this switch (the switch MAC address is 00-02-b3-02-002-09), the port of the switch is 2, so the status of port 2 is forwarding, and the port 3 is assigned port under forwarding status, but port 6 is discarding, which it means port 6 is redundancy link. The page information demos the current status of RSTP, RSTP is under dynamically monitoring and auto-negotiation status, each time refreshing the page, the latest status is shown but the information is probably different.

Forwarding status refers to the running status of the port, there are 4 kinds in total:

Disabled: It stands for the port is disconnected, disconnected port is under this status.

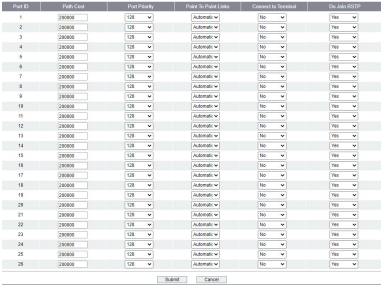
Discarding: During this status the BPDU packet can be received, if BPDU packet is not received during the period and changing into learning status, port

will be under discarding status at the moment the link is just connected.

Learning: During this status packet can be received, the switch stops max age=20s under discarding status at the moment is link is connected, determine whether it is possible the port of the switch will be the root port or assigned port, and finish RST root selection, construction and the direction of port status during the period of sending and receiving BPDU packet. If it is determined to be root port or assigned port, then stopping a time of forward delay=15s, and continue to calculate and determine whether it is possible to be the root port or assigned port, and currently there is supporting function of learning MAC address. If it is root port or assigned port then changes into forwarding status, if not then changes into discarding status.

Forwarding: At the moment the port can send and receive packet normally.

In order to fasten RSTP the self-recovery process and decrease the network load, user can configure the port in detailed according to the below page picture 4-44.



Picture 4-44 RSTP Port Information Configuration Page

Port Path Cost: Combining with port priority to generate port ID for comparison, link cost is decided by network physical link, user should modify the value based on the specific physical link. The default 100MBased port cost is 200000.

Port priority: The priority in the port of network bridge, combing with port link cost to generate port ID for comparison, the smaller the ID is, the higher the priority is. The default value is 128.

Point-to-point network connection: If there is only direct connection between different switches port, the port is point-to-point connection. RSTP uses auto-negotiation mechanism aiming to point-to-point link, which will

enable fast change of port status.

Direct connection with terminals: Switch in the network edge is generally connected with terminals, such as PC and working station. Configuring these ports that are connected with terminal equipment as Edge Port, which enables the fast change of port status. Without the transition process of discarding, learning and forwarding.

Participation of RST construction: Assigning the port to run with RSTP so as to decrease the number of ports and RSTP running complexity, which will shorten the RSTP self-recovery time.

Attention:

1.RSTP defines in the standard of 802.1w, is public standard protocol. MAIWE brand RSTP protocol is compatible with other brand network equipment that supports standard RSTP.

2.RSTP and Mwring function cannot be enabled at the same time.

3.When RSTP is enabled, RSTP will disable all ports, and it will discard some ports till the convergence period is over, during this period Web server will not response, webserver can be restarted after convergence is over (above 10s) and network tree is generated.

4.Each time link changes, there is a new convergence process with different length of time, but it will probably cause webserver cannot be visited till the convergence is over.

5.After RSTP is enabled, each unit of switch will periodically send query packet from every connected port based on the packet interval setup by user, which will cause network load.

6.Max aging time and forwarding delay must meet the below condition: 2*(forward delay-1)>=Max aging time.

7.It's suggested to setup port information and decrease the number of ports so as to reduce the complexity network calculation and convergence time. Decreasing the forwarding delay and Max aging time can fasten the RSTP self-recovery time.

4.6. Access Control

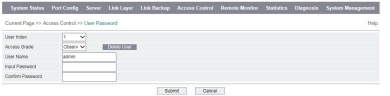
Access control function settings: Account password, login control, port authentication, database authentication and MAC port locking.

4.6.1. User Password

Switch's webserver provides three different groups of user account and password, each group can choose two levels to protect access to webserver. It's only allowed to login webserver via user account and password and managing switch. User account and password can be added, deleted and

modified by changing user index. The user account and password of factory default settings are both: admin, the access level is administrator.

User account and password must be legal characters, which can be formed by letters (case sensitive) and numbers, the max length of user account and password is 32 bytes. If current login user account and password is modified not same as before, it will prompt to retype user account and password if accessing to webserver again, as below picture 4-45.



Picture 4-45 User Password Setting Page

User index: User account and password group index, number 1-3, three groups in total.

Access level: It's divided into two levels, administrator and guest. Administrator has the right to check and modify all settings, guest can only check the settings. It only can be set as administrator mode for the first group.

User account: Setup account name of the group, the account name can be formed by letters (case sensitive) and numbers, empty user account is not allowed, and the max length is 32 bytes.

Input password: Setup the account password of the group, account password can be formed by letters (case sensitive) and numbers, empty password is allowed, and the max length is 32 bytes.

Confirm password: Retype the password to avoid to input wrong password.

Attention:

1.The first group can only be set as administrator mode to guarantee one group of administrator mode at least.

2.User account and password can be formed with letters and numbers, it's not suggested to use Chinese.

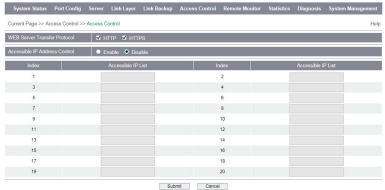
3.For safety, it's suggested for administrator to modify default user account and password of the first group after first time login.

4.Each time after user login the webserver, webserver will invalidate the login after spare 5mins, user will be requested to re-login if user operates the Web page currently, which is to prevent others' faulty operation for web when administrator is not presence. The time is calculated by software and not extreme accurate.

5.User can click Exit at the right top corner at any time to exit Webserver, actively invalidate the latest login, any web operation afterwards will reactivate login authentication.

4.6.2. Login Control

Login control can limit the accessed client IP address thru modifying system firewall so as to limit the access to webserver, see below picture 4-46.



Picture 4-46 Login Control Setting Page

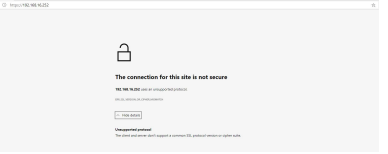
Web server transfer protocol: It's used to support web server transfer protocol, the default setting is supporting http and https, it's not suggested for user to modify it.

HTTP: It's abbreviation of Hyper Text Transfer Protocol, and used to transfer data in WWW mode, please refer to RFC2612 about the details of HTTP. HTTP uses Request/Response mode. Client send a request to server, Request includes the method of request, URL, protocol version, requested modifiers, client information and message structure in which contents is similar with MIME. Server response in a status row, the corresponding contents include message protocol version, correct or wrong codes plus server information, entitles metadata and possible metadata contents.

User directly input http://192.168.16.253 in the browser address so as to use HTTP to access to webserver.

HTTPS: HTTPS is security version of HTTP, which is developed for confidentiality, and its security basis is SSL protocol. SSL is located between TCP/IP and other application layer protocols, providing security support for data communication. SSL can be divide into two layers, SSL Record Protocol and SSL Handshake Protocol. SSL Record Protocol is based on transfer protocol such as TCP, providing data encapsulation, data compression, data encryption and other basic functions support for higher layer protocol. SSL Handshake Protocol is based on SSL Record Protocol and used for communication both sides identify authentication, negotiating encryption calculation and exchanging encryption keys before actual data transferring.

User directly input http://192.168.16.253 in the browser address and click Enter, which is to access webserver via HTTPS, it will probably prompt warning as below picture 4-47.



Picture 4-47 Warning Page

Click Continue to Browser the Website, sometimes it probably shows the main page is abnormal when it's the first time to login because of abnormal webpage script application running. It will be back to normal after refreshing several times.

Login IP address control: Switch provides advanced communication filter function thru modifying system fireware. When the function is enabled, only PC with assigned IP address can access to the equipment, all other unlisted IP address is not allowed to access to the web server of the switch.

Allowed accessed IP address list: Input network equipment IP address which is allowed to access to web in the frame, 20 records is allowed in total, user can use several records but at least setup one IP address list, the address cannot be the switch's own address, or the webserver cannot be shut down.

Attention:

1.HTTP and HTTPs must be enabled at least one access protocol.

2.Sometimes individual browser probably shows the main page is abnormal when it's the first time to login because of abnormal webpage script application running. It will be back to normal after refreshing several times.

3.Accessed IP address must be a legal IP address, at least there is one address and equipment IP in the same network segment, or the equipment will identified that the settings is invalid.

4.It's allowed accessed IP address in address list, but not accessed IP address without permission. At least it's needed to setup one valid address if enabling it, or the web server of the switch cannot be accessed.

5.Do not use switch's own address, webserver cannot be accessed if only this address is used by mistake.

4.6.3. Port Authentication

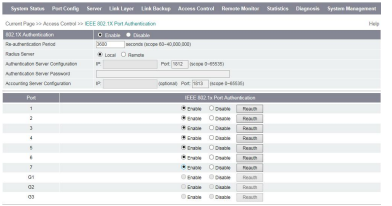
IEEE 802.1X authentication system structure uses logic function of

controllable port and uncontrollable port so as to separate the business and authentication. Separation of Business flow and authentication flow after use passes authentication has no special requirement for packets handling afterwards. Business can be very flexible especially there is a great advantage when conducting bandwidth multicast types of business, all business are not limited by authentication style.

802.1X structure is mainly inclusive three parts:

- Applicant: User or client wants authentication.
- Authentication server: Typical example is RADIUS server.
- Authentication: Wireless access point, switch, and etc.

Our equipment can be played as two roles of authentication server and authenticator, as well as using external authentication server and supporting external billing system. The page of port authentication is as below picture 4-48.



Picture 4-48 IEEE 802.1X Authentication Setting Page

On-time update authentication: It's re-authentication period of 802.1X. If it's beyond this time, the latest authentication is invalid and re-authentication is needed in order to enhance the security of authentication. The setting scope is 60-40000000s, the default value is 3600s, which is re-authentication is needed per hour.

Radius server: It's to setup RADIUS authentication server, there are Local and Remote two options.

Local: The switch is regarded as the RADIUS authentication server with in-built Radius server, applicant can only use internal user account and password of Radius database in the switch, the following three items are disabled:

Remote: The switch local port is authenticated by switch's external Radius authentication server, external Radius authentication server refers to switch's nom-in-built Radius server, the switch's in-built Radius server cannot be used

as other switch's remote authentication server. After the item is enabled, the following three items will be enabled, billing server is optional, other options are necessary items.

Authentication server settings: It's only be used after selecting Remote server, and fill in the shared password characters string of the switch access remote authentication server.

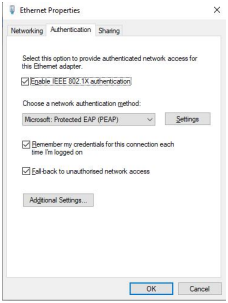
Billing server settings: it's only be used after selecting Remote server and as optional settings, the function of billing server is billing, IP address you set must be accessed by the switch, the default port is 1813, billing server faulty settings will cause that applicant cannot pass identify authentication, it's no needed to setup if without billing server.

It's used to setup enable/disable 802.1X authentication function of corresponding ports in below picture 4-49, the port will be in invalid status before pass authentication if enabling it, and changes into normal forwarding status after pass authentication. Click Re-authenticate will invalidate the latest authentication, and it's needed to authenticate the port again.

Picture 4-49 Corresponding Port IEEE 802.1X Authentication Configuration Page

Attention:

1.In windows system, open network connection first and then open the property page.



If there is no identify authentication label, please select Control Panel-Management Tool-Components Service-Service, enable Wireless Zero Configuration and Wired AutoConfig service. In the options of Select the Method of Network Identify Authentication, please choose MD5-Query, other methods are not supported, as above picture.

2.If 802.1X authentication function is enabled, and user account and password of authentication database is set, it will shows the below authentication dialog box when connecting the network in windows system.

Input user account and password you setup and then pass the authentication.

3.If the switch's port that user uses to access to web server enables the authentication function, once the function is enabled, user cannot access to web server normally and needs to pass authentication to access to web server again, which is normal situation, not the failure behavior.

4.All up-link ports, down-link ports and billing server ports must pass mandatory authentication, which is disabling to use authentication, or remote server cannot be used, unless to use internal authentication server.

5.Faulty billing server settings will also cause that applicant cannot pass identify authentication, it's no need to setup if there is no billing server.

6.Administrator must confirm the equipment can access to remote server while using remote server, which it means the network gateway is set correctly in Equipment Address, DNS must be setup correctly if use domain name.

7.The switch's in-built authentication server cannot be used as other

switch's remote authentication server.

8.If there is no any user account and password in authentication database, all ports will auto pass authentication.

4.6.4. Authentication Database

RADIUS is Remote Authentication Dial in User Service, RADIUS uses UDP as its transferring protocol to transfer authentication, authorization and configuration information system between Network Access Server and Shared Authentication Server. Besides, RADIUS is responsible for transferring the billing information between Network Access Server and Shared Authentication Server.

RADIUS authentication database as the part of 802.1X authentication and authorization protects multiple groups of user account and password used for authentication. User can add or delete the user account and password reserved in the database via the page. Any applicant's user account and password is compliance with database match rules, the authentication system of the equipment is authorized to this applicant. RADIUS authentication database configuration is as below picture 4-50.

Picture 4-50 RADIUS Authentication Database Setting Page

Login account: Setup new authentication user account, it's formed by numbers and letters (case sensitive) with 16 characters at most.

Account password: New account password, it's also formed by numbers and letters (case sensitive) with 16 characters at most.

Handling list: Click Add User and Delete User to add/delete user account and password in the below frame, all add/delete operation must click Save Settings to submit to the switch, and it will trigger database update and whole 802.1X re-authentication process. All modifying parts will be cancelled if exit the page before click Save Settings.

Attention:

1)When click Add Account and Delete Account, added table in the frame shows it has been changed but not been saved, only click Save Setting these changes will be submitted to switch and trigger update of database and restart of whole 802.1X authentication.

2)Please use standard 802.1X login tool like windows own tool, tools such as H3C 802.1X login tool with a bite custom filed cannot be used in the

switch.

3)Total numbers of user account should not be over 128.

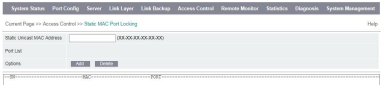
4)Database contents is invalid in actual if Radius authentication is not enabled.

5)If authentication database does not have any user account and password, all ports will pass authentication automatically.

4.6.5. MAC Port Locking

MAC port locking refers to manually add a static MAC address in forwarding table of switch, all data that are planned to the address will only be forwarded to the assigned port, which is also called MAC address bound.

Static MAC address differs from dynamic MAC address by learning, dynamic address will be deleted after exceeding max aging time, while static MAC address is not limited to aging time once it's added, and it will exist all the time if no one manually delete it. One MAC address in static table corresponds to one port, which is bounding static address with one port, the purpose of bound is to limit the movement of computer. If computer MAC is bound with port, the computer cannot be communicated if it moves to other unlocked port. If other computer moves to the bound port, then it still can communicate. Bound is aimed at MAC address, so the opposite of limitation of computer is port protection, the configuration page of the function is as below picture 4-51.



Picture 4-51 Static MAC Locking Configuration Page

The configuration page of MAC port locking is very similar with static multicast table, as well as operation method, the only one difference is the former is one-to-one relationship, which it means one MAC address only corresponds one port, but the latter is one-to many relationship.

Static Unicast MAC address: Add static MAC unicast address in the frame, the format is XX-XX-XX-XX-XX-XX, single address start with 00 of hexadecimal notation.

Port list: Select the bound forwarding port of the unicast MAC address packet, only one port is allowed to tick here.

Handling list: The item is used to operate unicast table, Add and Delete button is used to add/modify and delete static MAC address. Existing static address table will be displayed in the following frame, the frame will be updated

each time user open Web page or execute operation of Add or Delete.

Attention:

1. Add and Delete operation will be valid immediately, which does not need to click Save Setting like other pages.

2. The function is a kind of security mechanism, please be careful to confirm settings.

3. Please do not use multicast table as input address.

4. Please do not input reserved MAC address, such as the switch own MAC address.

4.7. Monitoring Alarm

Monitoring alarm function settings: SNMP configuration, Email log, Relay alarm.

4.7.1. SNMP

Simple Network Management Protocol (SNMP) is defined by internet engineering group, which is a part of internet protocol. Using SNMP to monitor network devices by network management system on the condition of observing one network equipment. SNMP is composed by a series of standard network management, application layer protocol, database and data objects. SNMP can display management total numbers via the forms of management system, such as system description configuration. The configuration can be checked or setup via a management application supporting SNMP. SNMP is based on TCP/IP protocol and usually exists in network equipment by using UDP port 161 (SNMP) and 162 (SNMP-Trap), and SNMP Agent and uses standard MIBs (information specific to the device) as equipment interface, these network equipment can be monitored or controlled via agent. When a Trap event happens, the message is transmitted by SNMP Trap, at that time an available Trap receiver can receive this Trap message. SNMP configuration page is as below picture 4-52.

Picture 4-52 SNMP Configuration Page

SNMP Configuration: Enable or Disable SNMP, the default setting is disabled.

Read-only community name: Use one string to name SNMP community,

the group only has authority of Get operation, is default as public.

Read-Write community name: Use one string to name SNMP community, the group has authority of Get and Set operation, is default as private.

SNMP TRAP gateway: when Agent sends abnormal alarm message, SNMP TRAP receives the IP address of the equipment.

Statement:

MAIWE brand managed series switches support SNMP V1/V2C. SNMP V1 and V2C both use public character string to match authentication, which it means SNMP server allows read-only style and read-write style to access all objects by using public or private string. SNMP Community uses one string, which is called Community Name. SNMP Community Name is used to define the relationship of SNMP manager and SNMP agent. Community Name works like password, in order to limit SNMP manager to access SNMP Agent of Ethernet Switch.

Attention:

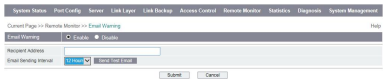
1.The Switch's SNMP supports SNMP Trap function, SNMP Trap uses public UDP port 162.

2.The Switch's SNMP Agent supports a part of standard MIB-2 and RMON, and only supports Get operation. It also supports our company private MIBs, this part of MIBs supports both Get and Set operation to simply configure the switch, but private MIBs only supports Web managed function, it's not suggested for user to use.

3.Please note the authority of Read and Write in SNMP browser, please check Community Name you used if Read and Write is abnormal.

4.7.2. Email Log

The function periodically sends syslog to user appointed mailbox via email, as below picture 4-53.



Picture 4-53 Email Log Configuration Page

Email Log: Enable or disable function, is default as disabled.

Receiver address: Input mail address that receives the email log, which can be SOHU, SINA and other normal mailbox, user needs to setup the mailbox in order to avoid the email log is mistook as trash mail. The sender address of email is maiweso@sohu.com, which will not be changed. User can setup email filter based on it.

Email Interval: It refers to the interval of sending email log, the default

period is 12hrs, value scope is 1-24hrs, measured unit is hour, time is calculated by computer software and not very accurate.

After all parameter settings are finished, user can click Send System Testing Email, wait for one minute, if receiving the email as below picture 4-44, which it means testing is okay and email system is working normally.

Dear Users:
Thanks for using email log system! If you've read this email, it means the system will meet your needs. The system can provide you periodical email log support, send you all syslog including broadcast storm or other alarm messages in form of email.
You can define the system yourself, please directly contact with us via our company official website WWW.MAIWE.COM.
Please do not response to this email.

Sincerely.

Wuhan Maiwe Communication Co., Ltd.

Picture 4-54 System Testing Email

Attention:

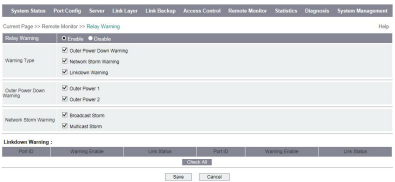
1.If user cannot receive email, please check mailbox settings to avoid email log is mistook as trash email and being deleted.

2.Only click Send System testing Email means the setting value is saved, which it means Send System Testing Email is Setting plus send testing email.

4.7.3. Relay Alarm

There is one NC alarm relay equipped in the switch, the system is running an event supervisory, for example, when some ports user defines is power failure alarm or port is link down, event supervisory can drive relay to send alarm signal, but will not send alarm signal for ports link down upon initialization.

The switch monitors power supply failure alarm, network storm alarm and port link down alarm, the page configures corresponding items to monitor these alarm events, the default setting is not monitoring all alarm events. Relay alarm function configuration page is as below picture 4-55.



Picture 4-55 Relay Alarm Page

Relay Alarm: Enable or disable relay alarm function, is default as disabled.

Alarm enable type: Including power supply failure alarm, network storm alarm, port link down alarm three kinds, all items are controlled by relay alarm Enable/Disable.

Power Supply Failure Alarm: Monitoring Power 1 and Power 2 status, tick the corresponding item of enabling monitoring. When Power 1 and Power 2 corresponding item is ticked and power failure, alarm message is displayed after the corresponding item (marked in RED).

Network storm alarm: monitors whether broadcast storms and multicast storms occur. When the corresponding items of broadcast storm and/or multicast storm are checked and a storm occurs, the alarm information is displayed behind the corresponding item (displayed in red).

Port link down alarm: Monitoring whether switch each port is link down, choose to monitor one or multiple ports, only one port is link down, there will be an alarm (marked in RED). Link down will not alarm without monitoring port, corresponding port only shows the actual connection status.

Attention:

1. After alarm function setting is finished, there will be an alarm whatever any type alarm is triggered, alarm will be cancelled until recovery.

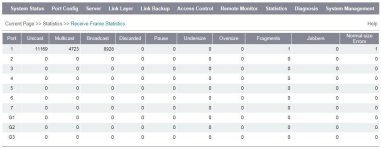
2. The font color of corresponding place is marked with RED in the page if there is an alarm.

4.8. Port Statistics

Port Statistics Function Settings: frame receive statistics, frame send statistics, total frame statistics, MAC table address.

4.8.1. Frame Receiving Statistics

The switch automatically monitors each port, statistics all network packet, display these statistics in Web page, as below picture 4-56.These statistics is all network packet since switch is power on, when switch is soft reset or restart after power off, these data will be all zeroing.



Picture 4-56 Frame Receiving Statistics Page

Unicast packet: The number of port received unicast address packet

Multicast packet: The number of port received multicast address packet

Broadcast packet: The number of port received broadcast address packet

Discarding packet: The number of port received normal but discarding packet due to safety reason.

Pause Frame: Port received Ethernet control frame of 0x8808 protocol, under full-duplex status, the packet is used to control the frequency of port sending data.

Ultra-short Frame: The number of port received packet with length less than 64 bytes, including FCS.

Jumbo Frame: The number of port received packet with length more than 1512 or1522 (enable VALN) bytes, including FCS.

Incorrect Ultra-short Frame: The number of port received packet with length less than 64 bytes, with incorrect FCS or incomplete string.

Incorrect Jumbo Frame: The number of port received packet with length more than 1512 bytes, with incorrect FCS or incomplete string.

Incorrect Normal Frame: The number of port received packet with length between 64 and 1512 bytes, with incorrect FCS or incomplete string and detected invalid string.

4.8.2. Frame Sending Statistics

Frame Sending Statistics page is as below picture 4-57.

Picture 4-57 Frame Sending Statistics Page

Unicast packet: The number of port received unicast address packet

Multicast packet: The number of port received multicast address packet

Broadcast packet: The number of port received broadcast address packet

Discarding packet: The number of port received normal but discarding packet due to insufficient resource or unmatched analytical conditions (exclude conflict discarding packet).

Pause Frame: Port received Ethernet control frame of 0x8808 protocol, under full-duplex status, the packet is used to control the frequency of port sending data.

Conflict Detection: The number of conflict when port sends data.

Multiple conflict: The number of packets that the number of conflict is more than once when port sends data but data is still send successfully.

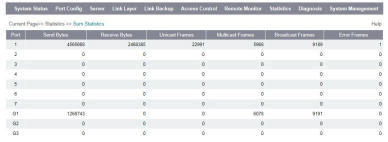
Short Frame Conflict: The number of detected conflict packets with transmission less than 64 bytes.

Conflict Discarding: The number of discarding packet due to more than 16 conflicts.

Resource Busy Discarding: The number of discarding (lots of data with lower priority after enabling QoS) packets due to being lack of resource in pop queue.

4.8.3. Total Frame Statistics

Total frame statistics page is as below picture 4-58.



Picture 4-58 Total Frame Statistics Page

Sending total bytes: Total number of bytes of port sending all packets.

Receiving total bytes: Total number of bytes of port receiving all packets.

Unicast packet: The number of port transmitted and received unicast address packet

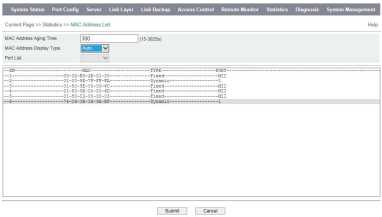
Multicast packet: The number of port transmitted and received multicast address packet

Broadcast packet: The number of port transmitted and received broadcast address packet

Incorrect packet: The number of port transmitted and received incorrect packet due to all different reasons.

4.8.4. MAC Address

MAC (Media Access Control) address is hardware identification of network equipment, switch forwards packet based on MAC address, MAC address' uniqueness guarantee the accuracy of forwarding packet. Each switch maintains a MAC address as below picture 4-59. In this table, MAC address is one-to-one corresponded with switch's ports. When switch receives frame, it will determine to filter or forward to switch's corresponding port based on MAC address. MAC address is the basis of precondition of switch fast forwarding.



Picture 4-59 MAC Address Table Page

Address Display Type: Appoint the sort type of MAC address, Auto and Port two sort types are optional. All port's all MAC address will be listed if choose Auto, corresponding port's MAC address will be listed if choose Port.

Port List: Choose displayed corresponding port's MAC address, the item only works when Address Display Type is selected as Port, all ports MAC will be displayed if selected as Auto.

The switch MAC address is divided as three kinds:

Dynamic MAC address

This type of address filed in MAC address list is Dynamic, dynamic MAC address is obtained in switch network by frame learning and it will be deleted if exceeding the aging time. If equipment connected switch's port changes, the corresponding relations of related MAC address and port in MAC address list will change. Dynamic MAC address will disappear after switch power off and restart and need to be obtained again by learning.

Static MAC address

This type of address filed in MAC address list is Static, static MAC address is generated thru configuring MAC port locking and not limited by switch aging time. Whatever the equipment connected switch's port changes, the corresponding relations of related MAC address and port in MAC address list will not change. Static MAC address will disappear after switch power off and restart.

Permanent Static MAC address

This type of address filed in MAC address list is Curing, permanent MAC address is also generated by configuration and not limited by switch aging time. Whatever the equipment connected switch's port changes, the corresponding relations of related MAC address and port in MAC address list will not change. Permanent MAC address will disappear after switch power off and restart.

Attention:

1. The equipment address is based on the calculation and index of switch's MAC address, so VLAN value in all MAC display is 0.

2. Static address can be configured in above static MAC address port list, corresponding table needs to be revised if port changes.

3. Multicast address table is displayed in IGMP Snooping list, address tables here are all unicast table.

4. The default aging time of MAC address is 300s (5 minutes), and can be setup via web management.

4.9. Network Diagnostics

Network diagnostics function settings: port mirroring and network ping diagnostics.

4.9.1. Port Mirroring

Port mirroring function is coping all sent/received data of one port or multiple ports to other assigned port. With assigning one port as other port's mirroring port, all sent/received data other port can be observed by the port. Port mirroring function is to diagnose, debug and analyze network failure.

MAIWE brand managed switches port mirroring function provides multiple mirroring rules, user can capture all data of entrance and exit. Port mirroring is copying data of monitored port to other assigned monitored port and analyzing and monitoring data. Many-to-one mirroring is supported, which is copying packet of multiple ports to other one monitored port. User can assign the direction of monitored packet, for example only monitoring assigned port's forwarding packet. The equipment configure port mirroring function in the way of port mirroring groups. Each port mirroring group includes one monitored port and one group of monitored ports. The configuration page of the function is as below picture 4-60.

Picture 4-60 Port Mirroring Configuration Page

Port Mirroring: Enable or disable the port mirroring function, is default as disabled.

Duplicated port: it refers to port in which data are collected, or port in which sent/received data will be copied in terms of port mirroring function, setting multiple port is available.

Mirroring Port: It refers to port in which data are collected, or port in which collected data will be copied in terms of port mirroring function, setting only one port is available, that is to say there is only existing one mirroring port at meanwhile.

Port Mirroring Mode: It refers to the direction options of collecting data, it is entrance data or exit data, or both. The concept of entrance and exit is defined aiming to switch's chip, not from the aspect of mirroring port.

Attention:

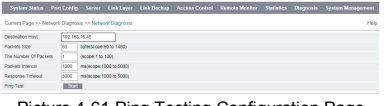
1. The function must be closed in normal use, or all advanced management functions based on ports cannot be used normally, such as RSTP and IGMP Snooping.

2. Port mirroring function can only deal with FCS normal packet, exclusive of all faulty frames.

3. The direction options of collecting data is entrance or exit data, or both. The concept of entrance and exit is defined aiming to switch's chip, not from the aspect of mirroring port.

4.9.2. Network Diagnostics

MAIWE brand managed switches support diagnostics function, such as network failure analyzing, network testing or problem solving. Configuration page is as below picture 4-61.



Picture 4-61 Ping Testing Configuration Page

Ping function uses simple ping command, offer user a simple and effective network problem diagnostics tool, the special place of the function is that user can input a ping command in the web page, switch itself send a ping command and output result in web page. In this way, user can easily control switch to send ping command and output result.

Ping function all settings items are as below table 4-6.

Table 4-6 Ping Function Settings Description Table

Setting item	Description	Default value
Targeted mainframe	Ping IP address	Blank
Packet size	Length of Ping packet	60
The number of Packet	The number of sending Ping packet	1

Packet intervals	Intervals of sending Ping packet	1000
Response timeout	Ping overflow time	5000

Attention:

1. Please ensure the first item Allow Incoming Echo Request in targeted mainframe windows firewall local connection ICMP setting is ticked before using Ping network diagnostics function, or the target mainframe cannot passed by ping.

2. Domain name of the targeted mainframe does not support unlimited extension, only support third level domain name, such as mial.sina.com.

3. If prompt of Request timeout appears, it means the opposite's network card is not working normally or network line is failure.

4. If Ping domain name appears prompt message of unknown host name, it means DNS configuration is faulty.

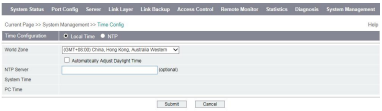
5. If Ping domain name appears prompt of Request timeout, it means the gateway settings is faulty.

4.10. System Management

System management function settings: time configuration, address setting, system information log information and file management.

4.10.1. Time Configuration

Set up switch's system time via time configuration setting function. The switch does not have backup battery reserved system time value, system time will lost when it power off. The switch's system time is Linux time 1st July 1970 after restart. Please synchronize the switch time after each time restart the switch. Time configuration page is as below picture 4-62.



Picture 4-62 Time Configuration Page

Time configuration: The switch provides two different time configuration options; Local Time and Using NTP.

Local time: It's time set by user. Generally it's PC time when it access the page, when user choose the item and click Setting, Update Time To Switch will be displayed at the bottom, after clicking, accessing PC time will be updated to switch.

Using NTP: It refers that the switch auto syncs time with time server of

internet, NTP (The Network Time Protocol) is a network time sync protocol, using UDP and 123 port. NTP can resist unstable network responding time so as to improve accuracy of time correction.

World Time Zone: The division of World Time Zone takes standard of prime meridian. From west diameter 7.5 degrees to east diameter 7.5 degrees (Longitude interval is 15 degrees), it is Zero Zone. From two boundaries of Zero Zone to the west and east separately, each longitude interval of 15 degrees is divided as a zone, there are separate 12 zones in west and east. West 12 zones are coincide with east 12 zones, there are 24 zones in global. Each zone takes solar time of central longitude line as standard time. Closed two zones standard only has one hour difference. Zone boundary is divided based on geography in principle, but always based on all every country's administration boundary or nature boundary in the concrete implementation for easy use.

User can choose related zone according to typical territory in the equipment. User can auto adjust internal time migration based on selected zone.

Auto adjustment of DST: DST is one hour earlier than standard time. For example, during the period of implementing DST, standard time 10am becomes DST 11am. DST is called Daylight Saving Time, a kind of region time system set by man for saving energy. There are around 110 countries in global implementing DST at present, when choosing special area, if the area allows for DST, the option is available, or it's invalid.

NTP server: Provide mainframe name or IP address of NTP time service.

System Time: Equipment itself current system time, it is 0:00:10 Thursday on 1st Jan. 1970. User can manually update local time to switch or auto use NTP update.

PC time: PC system time when access to web server, when select Local Time, prompt of Update Time To Switch will appear, clicking the button will update the time to switch.

Attention:

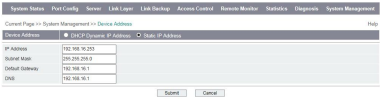
1. When Using NTP, NTP server cannot be empty, switch needs to connected with internet , using public internet NTP server.
2. Update Time to Switch button only pops up when user choose Local Time and click Setting, when user shift to Using NTP, it will disappear after clicking Setting.
3. Only administrator has authority to manually configure equipment time.

4. Time Zone and DST must be configured whatever to use Local Time or NTP Time.

5. NTP server or visitor's PC time configuration may cause abnormal display, user can change Time Display format to adjust display.

4.10.2. Address Setting

The function will assign one IP address to the series of switch. In general there are two ways of assignation: DHCP or appointing one IP address. The factory default setting of the switch is using fixed address, IP address is 192.1687.16.253. Configuration page is as below picture 4-63.



Picture 4-63 Equipment Address Configuration Page

DHCP Dynamic IP address: Using DHCP protocol to dynamically assign one IP address from DHCP server. It needs DHCP server in network, it's not suggested for user to use it because accessing web server needs to know clear switch IP address, but dynamic IP address cannot be confirmed before assigning IP address, and a new IP address may will be assigned after each time restart.

Static IP address: Manually setup a fixed static IP address, it's suggested for user to use the option, manual setting one fixed IP address is easy to use web management, and there is no conflict for IP address settings.

IP address: IP address is a 32 bytes address which is assigned to equipment connected with internet. IP address is composed by two fields: net-id and host-id. IP address is assigned by America National Defense Data Grid Network Information Centre. In order to easily manage IP address, IP address is divided as five categories. See as below:

Network Type	Address Scope	Available IP network scope for user
A	0.0.0.0-127.255.255.255	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	192.0.0.0-233.255.255.255	192.0.0.0-223.255.254.0
D	244.0.0.0-239.255.255.255	NONE
E	240.0.0.0-247.255.255.255	NONE

Other address 255.255.255.255

Category A, B and C address is unicast address, category D address is multicast address. Category E address is retained address for special use in

future. At present IP address for large use belongs to category A, B and C.

IP address takes decimal to record. Each IP address is represent as 4 decimal integers separated by decimal point. Each integer corresponds to a byte, such as 10.110.50.101.

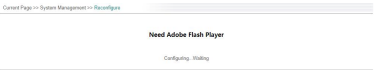
Subnet Mask: Mask is an IP address corresponding to 32 bytes number, some numbers are 1, other are 0. In principle these 1 and 0 can be combined in any way, but in general when mask is designed, setup the consecutive the first several numbers as 1. Mask can divide IP address as two parts: subnet address and host address. IP address and corresponding parts with mask bytes 1 is subnet address, other bytes is host address. Category A address corresponding mask is 255.0.0.0, category B address mask is 255.255.0.0, category C address mask is 255.255.255.0.

Using mask can divide category A network with 16000 thousand hosts or category B network with 60 thousand hosts into many small network, each small network is called subnet.

Default Gateway: default gateway in the host is called default route in general. Default route is selected route by router when other routes cannot be found in targeted address in IP packet. All packets in which targeted address is not in the route list of router will use default route. The route will connect with other router in general, and the router will deal with packet as well, if knowing how to route this packet, the packet will be forwarded to known router, or packet will be forwarded to default route and arrive at other router.

DNS address: the function of DNS (Domain Name Server) is resolving the domain for our easy memory to IP address that internet can identify. If our equipment needs to access some host name, so we need to take advantage of this server to resolve to IP address.

User needs to click Saving each time after modifying address settings so that it will be submitted to switch and shift to a waiting page as below picture 4-64.



Picture 4-64 Waiting Page after User Modify Address

After the page shut down, switch will use new IP address and restart web server.

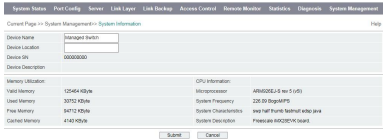
Attention:

1. IP address scope we can setup should be 192.168.x.x, 172. [16-31].x.x or 10.x.x.x.

2. NTP and Email will use DNS service, if use these two services, please fill in correct DNS address.

4.10.3. System Information

User can get to know switch system related information and setup switch' name thru the page shown in below picture 4-65.



Picture 4-65 System Information Configuration Page

Equipment Name: It's to name for each switch in marked network so as to distinguish them. Switch name does not exceeds 16 bytes at most.

Equipment Number: It describe switch factory numbers, set by factory and cannot be modified by user.

Equipment Description: It's switch model, decided by hardware and cannot be modified by user. User can search and find this information via a SNMP Client software or upper computer management.

Memory Usage: It describes switch's system RAM usage.

CPU Information: It describes switch system main CPU basic information.

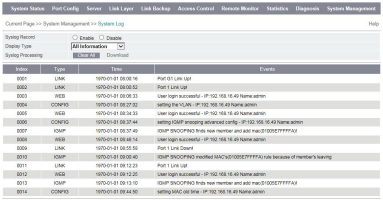
Equipment Power Supply: it displays power supply for the equipment, ON: Power on/OFF: power off.

4.10.4. Log Information

Equipment provides log information for user conference possible setting problems. When the function is enabled, switch will record happened related events and reserve to log information files, log function reserves all records to SDRAM, 2000 records at most. Previous records will be deleted and new record will be added if exceeding 2000 records. The following events will be reserved to log files:

- System Restart
- Port Link Down/UP
- Login information
- Broadcast Storm Occurs
- System Operation Record
- NTP Time Sync Information
- Other System Information

Log information is as below picture 4-66.



Picture 4-66 Log Information Configuration Page

Log Record: Enable or disable log record function, is default as enable. Log contents will not be deleted after log function is disabled, but just new log information will not be added.

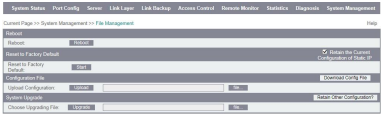
Display Type: Display some type of information, can be shift between All information, Operation Information and Connecting Information.

Delete All Information: Click the button is to delete all log information.

Download Information: Click the button is to download log information from web server and reserved to access PC, file name is syslog.cfg. Please use browser to download it directly, web server of the switch does not support multithread download tool like XUNLEI.

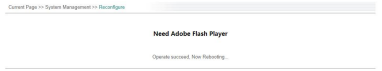
4.10.5. File Management

File Management page is as below picture 4-67. The page is some unconventional operation for switch, please be careful to use it. Improper operation may damage the switch. Only administrator is allowed to do these operation.



Picture 4-67 File Management Page

Restart Switch: The operation is used to restart switch, the switch will not work and forward any packet before the switch completely restarts, this kind of restart differs from hardware reset by powering on, it's like windows operating system warm boot. The best advantage of the function is to provide a function of remote restarting switch, user can remote restart the switch only user can remote access it. Click Restart and it will go to a waiting page as below picture 4-68.



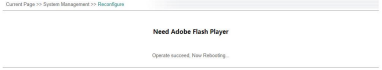
Picture 4-68 Waiting Page of Restarting Equipment

When the page shuts down, the switch software finish reset.

Factory Default Recovery: The operation is used to recover the switch as factory default and auto restart switch in the meanwhile, the switch does not work and cannot forward any packet before the switch restart successfully. The function is to recover factory default when switch is working abnormally due to faulty parameters set by user.

When switch recovers factory default, it's default to click and reserve current static IP setting, which it means Switch's IP address, subnet mask, default gateway and DNS address reserves previous static setting after factory default recovery. User can choose not to click reserve settings too, in this way the switch recovers the factory default IP address 192.168.16.253 after switch successfully recovers factory default. User needs this IP address to access web server.

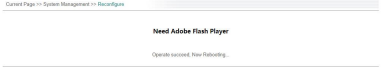
Click Start, then it goes to a waiting page as below picture 4-69.



Picture 4-69 Waiting Page of Factory Default Recovery

When the page shuts down, the switch finish factory default recovery and restart.

Configuration file: The operation allows user to reserve the switch's current all configuration as one file, the configuration file can be used to backup and recover switch's all configuration. The function allows user easily configure multiple switches with one configuration file. Click Download Configuration File, then user can download the configuration file to access PC, the file name is switchcfg.cfg, the switch does not support multithread download tool like XUNLEI, please use browser to download directly. Click Browser first to select a file when uploading a configuration file, please do not select non-configuration file of the switch, uploading wrong file may damage the switch, click Upload, then it goes to a waiting page as below picture 4-70.



Picture 4-70 Waiting Page of Equipment Reset

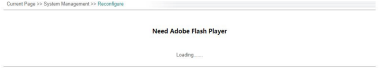
When the page shuts down, the switch uses new configuration to setup and restart. Switch cannot power down during the operation process, or it may damage the switch.

System Upgrade: The operation is used to upgrade system once for core application of switch, user can obtain switch's upgrade application by email or our company official website, please note to match equipment model with correct version, use unmatched upgrade application may cause switch's permanent damage.

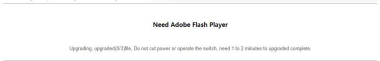
It's default to recover factory default and restart after mirroring upgrade, and it reserves previous static IP setting before upgrade under this factory configuration. User can click Whether to Reserve Current Other Settings? to choose whether to reserve previous fast ring network setting, RSTP setting or VLAN setting. Click options you want to reserve and click Reserve, as below picture 4-71.

Picture 4-71 Whether to Reserve Current Other Settings

Click Browser to choose upgrade application after user obtains upgrade application, and then click Start Upgrade, then it will go to the download page. It starts to upgrade after successfully downloading, download is divided as three steps in detailed, switch finishes upgrade after three steps pages update over, switch will auto recover factory default and restart after upgrade. Please note switch cannot power down during the whole upgrade process, or it may damage the switch.

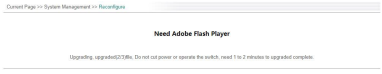


Picture 4-72 Download and Waiting Page

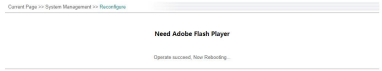


Picture 4-73 Upgrade Process the First Step Page

Picture 4-74 Upgrade Process the Second Step Page



Picture 4-75 Upgrade Process the Third Step Page



Picture 4-76 Factory Default Recovery and Restart after Finish Upgrade

File management page ticking options statement:

1. Reserve static IP setting: It refers to reserve the previous static IP setting during some operations process.

2. Factory Setting Recovery: It refers to auto recover factory default after some operations.

3. Reserve current fast ring network setting: It refers to reserve pervious switch fast ring network function setting during some operation process.

4. Reserve current RSTP setting: It refers to reserve pervious switch RSTP function setting during some operation process.

5. Reserve current VLAN setting: It refers to reserves previous switch VLAN function setting before some operation.

Attention:

1. Factory setting recovery will result in switch all function settings are recovered to the original status, if Reserve Current Static IP setting is not ticked, switch's IP address will be recovered as static IP 192.168.16.253 after factory default recovery. User needs the IP to access web server, it's suggested for user to modify switch's IP address after factory default recovery to avoid conflict and abnormal use.

2. Please do not select non-configuration file of the switch during the process of uploading configuration file, uploading wrong file may damage the switch.

3. It cannot power down during uploading configuration file, or it may damage the switch.

4. If new configured static IP is not in the same network segment during uploading configuration file, which will result in that switch cannot re-login web server and refresh the network page.

5. If dynamic IP setting is used in new configuration but there is no DHCP server in network segment during uploading configuration file, which will result

in IP related parts will not update.

6. Please note equipment model needs to match the version during upgrade, using unmatched upgrade application may cause switch permanent damage.

7. It cannot power down during the whole upgrade process, power down may cause switch permanent damage. Please send switch back to our company immediately to seek for possible solution if it power down during the upgrade.

8. If switch setting is chaos, please consider to reset switch after factory default recovery.

5. Maintenance and Service

Since the date of shipment, Wuhan Maiwe Communication Co., Ltd. provides five years warranty. Within the warranty period, if there is any failure or operation fails, our company will repair or replace the product for free based on our company product specification. But above commitment does not cover damage casued by improper use, accidents, natural disasters, improper operation or improper installation.

To ensure that consumers benefit from Maiwe Brand products, user can get help and solve problem by the following several ways:

- Internet services.
- Call our technical support office.
- Product repair or replacement.

5.1. Internet Service

User can get more useful information and usage tips on the technical part of official website of Wuhan Maiwe Communication Co., Ltd.

5.2. Technical Support Call Services

User can call to technical support office of Wuhan Maiwe Communication Co., Ltd, our company has professional technicians to answer your questions to help you solve the problem in use of the product at the first time.

5.3. Product Repair or Replacement

First please confirm with technicians of Wuhan Maiwe Communication Co., Ltd before product repairing, replacement or refund, and then contact with sales person of Wuhan Maiwe Communication Co., Ltd and solve the problem. User should follow Wuhan Maiwe Communication Co., Ltd handling procedures, and negotiate with technicians and sales person of Wuhan Maiwe Communication Co., Ltd to finish product repairing, replacement or refund.

.

WUHAN MAIWE COMMUNICATION CO.,LTD
Add.:Building 2, Area E, Phase ii, Optical valley core center, No.52, Liufang road, East Lake Hi-tech Development Zone,Wuhan,China
Phone: 027-87170215/16
Fax: +86-027-87170217
www.maiwe.com