RAISECOM

www.raisecom.com

ISCOM2924GF-4GE_4C Maintenance Guide

Legal Notices

Raisecom Technology Co., Ltd makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. **Raisecom Technology Co., Ltd** shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty.

A copy of the specific warranty terms applicable to your Raisecom product and replacement parts can be obtained from Service Office.

Restricted Rights Legend.

All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of **Raisecom Technology Co., Ltd.** The information contained in this document is subject to change without notice.

Copyright Notices.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in Writing from **Raisecom Technology Co., Ltd.**

Trademark Notices

RAISECOM is the trademark of Raisecom Technology Co., Ltd.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows® XP is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of
Microsoft Corporation.

Contact Information

Technical Assistance Center

The Raisecom TAC is available to all customers who need technical assistance with a Raisecom product, technology, or, solution. You can communicate with us through the following methods:

Address: Building 2, No. 28 of the Shangdi 6th Street, Haidian District, Beijing 100085

Tel: +86-10-82883305

Fax: +86-10-82883056

World Wide Web

You can access the most current Raisecom product information on the World Wide Web at the following URL:

http://www.raisecom.com

Feedback

Comments and questions about how the ISCOM2924GF-4GE_4C system software works are welcomed. Please review the FAQ in the related manual, and if your question is not covered, send email by using the following web page:

http://www.raisecom.com/en/contact-us.html.

If you have comments on the ISCOM2924GF-4GE_4C specification, instead of the web page above, please send comments to:

export@raisecom.com

We hope to hear from you!

CONTENTS

Preface

About This Manual

This manual introduces primary functions of the configuration management software for RC series products.

Who Should Read This Manual

This manual is a valuable reference for sales and marketing staff, after service staff and telecommunication network designers. For those who want to have an overview of the features, applications, structure and specifications of ISCOM2924GF-4GE_4C device, this is also a recommended document.

Relevant Manuals

ISCOM2924GF-4GE_4C Configuration Guide

ISCOM2924GF-4GE_4C Hardware Description

Organization

This manual is an introduction of the main functions of ISCOM2924GF-4GE_4C. To have a quick grasp of the using of the ISCOM2924GF-4GE_4C, please read this manual carefully. The manual is composed of the following chapters

Chapter 1 Safety Introduction

Chapter 2 Routine Maintenance

Chapter 3 Troubleshooting

Chapter 4 System Management Troubleshooting

Chapter 5 Interface Troubleshooting

Chapter 6 Layer-2 Network Troubleshooting

Chapter 7 IP Forward and Route Troubleshooting

Chapter 8 Service Troubleshooting

Chapter 9 Common Maintenance Command

Chapter 10 Maintenance Record

Appendix A Terms

Appendix B Abbreviation

Compliance

The RC series products developed by Raisecom are strictly complied with the following standards as well as ITU-T, IEEE, IETF and related standards from other international telecommunication standard organizations:

YD/T900-1997 SDH Equipment Technical Requirements - Clock

YD/T973-1998 SDH 155Mb/s and 622Mb/s Technical conditions of optical transmitter module and receiver module

YD/T1017-1999 Network node interface for the Synchronous Digital Hierarchy (SDH)

YD/T1022-1999 Requirement of synchronous digital hierarchy (SDH) equipment function

YD/T1078-2000 SDH Transmission Network Technique Requirements-Interworking of Network Protection Architectures

YD/T1111.1-2001 Technical Requirements of SDH Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Receiver Modules

YD/T1111.2- 2001 Technical Requirements of SHD Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Transmitter Modules

YD/T1179- 2002 Technical Specification of Ethernet over SDH

G.703 Physical/electrical characteristics of hierarchical digital interfaces

G.704 Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels

G.707 Network node interface for the synchronous digital hierarchy (SDH)

G.774 Synchronous digital hierarchy (SDH) - Management information model for the network element view

G.781 Synchronization layer functions

G.783 Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks

G.784 Synchronous digital hierarchy (SDH) management

G.803 Architecture of transport networks based on the synchronous digital hierarchy (SDH)

G.813 Timing characteristics of SDH equipment slave clocks (SEC)

G.823 The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy

G.825 The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)

G.826 End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections

G.828 Error performance parameters and objectives for international, constant bit-rate synchronous digital paths

G.829 Error performance events for SDH multiplex and regenerator sections

G.831 Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)

G.841 Types and characteristics of SDH network protection architectures

G.842 Interworking of SDH network protection architectures

G.957 Optical interfaces for equipments and systems relating to the synchronous digital hierarchy

G.691 Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers

G.664 Optical safety procedures and requirements for optical transport systems

I.731 ATM Types and general characteristics of ATM equipment

I.732 ATM Functional characteristics of ATM equipment

IEEE 802.1Q Virtual Local Area Networks (LANs)

IEEE 802.1p Traffic Class Expediting and Dynamic Multicast Filtering

IEEE 802.3 CSMA/CD Access Method and Physical Layer Instruction

Chapter 1 Safety Introduction

This chapter describes the safety precautions in ISCOM2924GF switch maintenance.

- Safety statement
- Safety symbols
- Electrical safety
- Radiation safety
- Mechanical safety
- Device safety
- Dangerous operation

1.1 Safety statement

⚠Caution :

Please carefully read the statement to prevent personal injury or equipment damage during the operation.

In order to avoid accident, the chapter serves as a general guide for the safe installation and operation of Raisecom products

Only qualified and authorized service personnel should carry out adjustment and maintenance.

The device maintenance should comply with local security specifications strictly. Safety matters mentioned in the manual is supplementary. Raisecom shall not be liable for the accident caused by violating general safety operation requirements and the safety standard of design, production and usage.

1.2 Safety symbols

The common safety symbols in equipment maintenance are shown in Table 1-1, which are used to prompt the user to comply with safety precautions.

Table 1-1 safety symbols types and meanings:

Symbols	Meanings
⚡	Danger of high voltage!
ESD	Electrostatic symbol, indicating that the equipment is sensitive to static electricity.
⏚	Earth connecting symbol, indicating that the equipment should be connected to the earth.

Symbols	Meanings
☢	Danger of electromagnetic radiation!
⚠	Danger of microwave radiation!
⚠	Danger of laser!

1.3 Electrical safety

1.3.1 High voltage safety

During maintenance, make sure the working environment and staff comply with high voltage safety rules so as to avoid personal injury and equipment damage.

The high voltage safety rules are as below:

- Operation & maintenance personnel must have related qualification.
- The maintenance of ac power device must comply with local regulations.
- The operation must use special tools.
- Prohibit wearing watches, bracelets, rings, and other conductive objects.
- Avoid the device from damping when operating in wet environment. Turn off power supply immediately if the cabinet is damp.

⚠Warning: High voltage power provides power for the operation, so direct contact or indirect contact through the wet object will lead to fatal danger.

1.3.2 Power cord safety

During maintenance, make sure the power cord complies with safety rules so as to avoid personal injury and equipment damage.

The power cord safety rules are as below:

- Turn off or disconnect the power before maintaining and removing power cord.
- Make sure the power cord label displays correct before connection.
- Only power cords meeting the specifications are allowed.

⚠Warning: Prohibit installing and removing the power cord in electrical conditions. The core of power cord conductors will produce electric arc or spark once touching the conductor, which may result in fire or eye injuries.

1.3.3 Thunder-and-lightning safety

During a lightning storm, the atmosphere will produce a strong electromagnetic field. Therefore, in order to prevent possible damage, the device should be timely taken thunder-and-lightning protection work.

Warning: In a thunderstorm, the operations under high voltage, AC power, iron tower, as well as mast homework are strictly forbidden.

1.3.4 Electrostatic safety

In equipment maintenance, take the anti-static measure to avoid device damage.

Antistatic rules are as below:

- The equipment should be grounded properly in accordance with requirements.
- To prevent body electrostatic from damaging the equipment, working staff must wear ESD wrist before contacting equipment or components and make sure the other side of ESD wrist connects the ground correctly.
- To guarantee anti-static wrist in working condition, the system resistance should be at the range of 0.75MΩ-10MΩ. If the resistance is not enough, change a new anti-static wrist in time.

Note:

- Any time contacting equipment or components, working staff must wear ESD wrist. ESD wrist should contact with the skin, and insert the plug to ESD socket on the equipment.
- Avoid any contact between components and clothes because the ESD wrist can't prevent the components from producing electrostatic when contacting with clothes.

1.4 Radiation safety

1.4.1 Electromagnetic exposed security

For antenna maintenance in a tower or mast, contact related working staff to close antenna radiation firstly.

Before entering into the electromagnetic radiation over proof area, the working staff should confirm the position of radiation over proof areas and turn down transmitter.

Warning: High strength radio frequency signal is harmful to human body.

1.4.2 Laser safety

Laser transceiver is used for optical transmission systems and related test. Bare fiber or connector interface will launch the invisible laser with high power density. The eyes may be burnt if looking at the laser output interface with naked eyes.

Please comply with the following requirements to prevent laser radiation hazard:

- Only authorized personnel with related training can take operation.
- Wear goggles in operation.
- Power off before disconnect optical fiber connectors.
- Cover optical interface in use and the connected fiber-optical splice with dust cap to protect eyes when pulling out the fiber.
- In an uncertain power status, forbid to watch bare optical fiber or connector.
- Measure optical power by optical power meter to make sure that the optical source has turned

off.

- Pay attention to avoid the laser radiation before opening the front door of optical fiber transmission system.
- Prohibit the use of microscope, magnifier, loupe and other optical instruments to watch the fiber connectors or the ends of fiber.

Please obey the following requirement for operations on optical fiber:

- Only trained personnel can cut and weld optical fiber.
- Before cutting or welding fiber optical, disconnect the fiber with optical source. Then use fiber caps to protect all the fiber connectors.

1.5 Mechanical safety

1.5.1 Drilling

Please comply with the following requirements for cabinet drilling:

- At first, remove cables in the cabinet.
- Wear goggles to avoid injury caused by sprayed metal particles.
- Wear protective gloves during drilling.
- Strictly prevent metal particles from falling into the cabinet. After drilling, clean it up carefully.

Warning: Users are not allowed to drill in the cabinet on their own. Drilling without meeting the requirements may destroy the electromagnetic shielding performance of cabinet and damage internal cables. Metal particles generated by drilling into the cabinet will lead to short-circuit boards.

1.5.2 Carrying chassis

Please wear protective gloves during manual lifting so as to avoid scratching.

Grasp the handle or hold up the bottom edge of chassis when moving or lifting the chassis instead of the handles of installed components inside the chassis (such as power modules, fan modules).

Note:

- Take good preparation for load-bearing and avoid being crushed or sprained.
- When pulling out the chassis, please pay more attention to the unstable and heavy devices on cabinet so as to avoid being crushed or sprained.

1.6 Device safety

Too low temperature or violent vibration and oscillation may lead to the brittle plastic skin cracking. To ensure the construction safety, the device should meet the following requirements:

- All cables are laid down above zero centigrade.
- Keep the cables in ambient temperature for more than 24 hours before maintenance operation if the cable storage environment is below zero.
- Carry the cables gently to avoid nonstandard operation of pushing them down the lorry directly, especially in low temperature construction environment.

To ensure safety, if you have any questions, please contact RAISECOM office or technical support.

1.7 Dangerous operation

Dangerous operation refers to the operations lead to abnormal work or service interruption. Therefore, in the daily maintenance, avoid the dangerous operations, which are used by professional maintenance staff only in certain circumstances.

1.7.1 Hardware dangerous operation

Prompt	**Consequence**
Prohibit altering power switch randomly	Power off and service interruption

1.7.2 Command dangerous operation

Command	**Consequence**
reboot	Reboot and service interruption

Chapter 2 Routine Maintenance

Routine maintenance introduces preventive routine maintenance method, also known as preventive maintenance, or periodic maintenance. This chapter describes the maintenance purposes and contents of ISCOM2924GF switch routine maintenance.

- ✧ Maintenance purposes
- ✧ Operating environment
- ✧ Hardware maintenance
- ✧ Software maintenance
- ✧ Service maintenance
- ✧ Data backup and recovery

⚠Caution: Please read "*1.1 Safety statements*" carefully to ensure the personal and device safety in maintenance.

2.1 Maintenance purposes

In order to keep the normal working of ISCOM2924GF switch, it needs to detect and eliminate the hidden faults in time to ensure the best operation state and meet users' service requirements.

Routine maintenance cycle is divided into day, week, month, quarter and year.

2.2 Operation environment

Good working environment is the foundation for the long-term stability of ISCOM2924GF device. Refer to following table for maintenance.

Item	Cycle	Method	Standards and description
Environment temperature	Week	Thermometer	Normal value: -10℃～60℃
Environment humidity	Week	Hygrometer	Normal value: 5% RH～95% RH, no condensation
Operating pressure	Week	Barometer	86kPa～106kPa
Grounding	Week	Ground wire	Check whether the ground wire connection is normal.

2.3 Hardware maintenance

2.3.1 Indicator inspection

Through the indicator status, make a preliminary judge for possible failure.

The meanings of indicators on ISCOM2924GF-4GE main board panel are shown as below:

Indicator	Status	Description
LINK/ACT Port 1～Port 28	Green	Line indicator ON: The line is connected properly. Flickering: There is data transmitting OFF: The line is disconnected or the connection is abnormal.
SPEED Port 1～Port 24 (SFP optical module interface)	Green	Optical interface work rate indicator ON: The interface works in the rate of 1000Mbit/s OFF: The interface works in the rate of 100Mbit/s, or power off
SPEED Port 25～Port 28 (COMBO interface)		
PWR1/2	Green	Power indicator ON: The power works normally OFF: The device is powered off or the power module is installed abnormally
FAN1/2	Green	Fan indicator ON: The fan works normally Flickering: The fan works abnormally OFF: No fan module is installed
SNMP	Green	SNMP interface indicator ON: SNMP interface connection is normal Flickering: There is database transmitting OFF: SNMP interface is disconnected or the connection is abnormal
SYS	Green	System indicator Flickering: The system works normally OFF/ON: The system works abnormally

The meanings of indicators on ISCOM2924GF-4C main board panel are shown as below:

Indicator	Status	Description
LINK/ACT Port 1～Port 28	Green	Line indicator ON: The line is connected properly. Flickering: There is data transmitting OFF: The line is disconnected or the connection is abnormal.

Indicator	Status	Description
SPEED Port 1～Port 24 (SFP optical module interface)	Green	Optical interface work rate indicator ON: The interface works in the rate of 1000Mbit/s OFF: The interface works in the rate of 100Mbit/s, or power off
SPEED Port 25～Port 28 (SFP+ optical module interface)	Green	Optical interface work rate indicator ON: The interface works in the rate of 10Gbit/s OFF: The interface works in the rate of 1000Mbit/s, or power off
PWR1/2	Green	Power indicator ON: The power works normally OFF: The device is powered off or the power module is installed abnormally
FAN1/2	Green	Fan indicator ON: The fan works normally Flickering: The fan works abnormally OFF: No fan module is installed
SNMP	Green	SNMP interface indicator ON: SNMP interface connection is normal Flickering: There is database transmitting OFF: SNMP interface is disconnected or the connection is abnormal
SYS	Green	System indicator Flickering: The system works normally OFF/ON: The system works abnormally

Note : If indicator is abnormal, please take troubleshooting based on the indicator status.

2.3.2 Hardware state inspection

Generally speaking, it is unnecessary to take hardware appearance inspection if the ISCOM2924GF switch is placed in a fixed place and there is no alarm. For equipment operating under long runtime (years), or tough work environment (higher dusty/humidity), please check the working state of power and fan modules. Hardware working state maintenance should comply with the standards in the following table:

Item	Cycle	Method	Standards and description
Temperature	Day	**show environment**	The normal temperature range is 5℃~80℃, otherwise it will have temperature alarm.

Item	Cycle	Method	Standards and description
AC voltage	Day	**show environment**	The rated voltage of AC power is 220V, the voltage fluctuation range is 100V~240V (50Hz/60Hz).
DC voltage	Day	**show environment**	The rated voltage of DC power is -48V, the voltage fluctuation range is -36V~-72V. The rated voltage of DC power is +24V, the voltage fluctuation range is +18V~+36V.
Fan status	Day	**show fan-monitor status**	No noise and normal speed.
Power status	Day	**show environment**	The power is stable and normal.
CPU utilization	Day	**show cpu-utilization**	Lower than 80%. If not, check the equipment and find out the reason.
Interface Up/Down statistics	Week	**show interface port** [*port-id*] **statistics**	Check physical layer interface statistics.
Interface configuration and status	Week	**show interface ip** **show vlan** **show interface port**	Check whether the IP address configuration, VLAN, and interface No. are correct.

2.3.3 Replace power module

Caution:

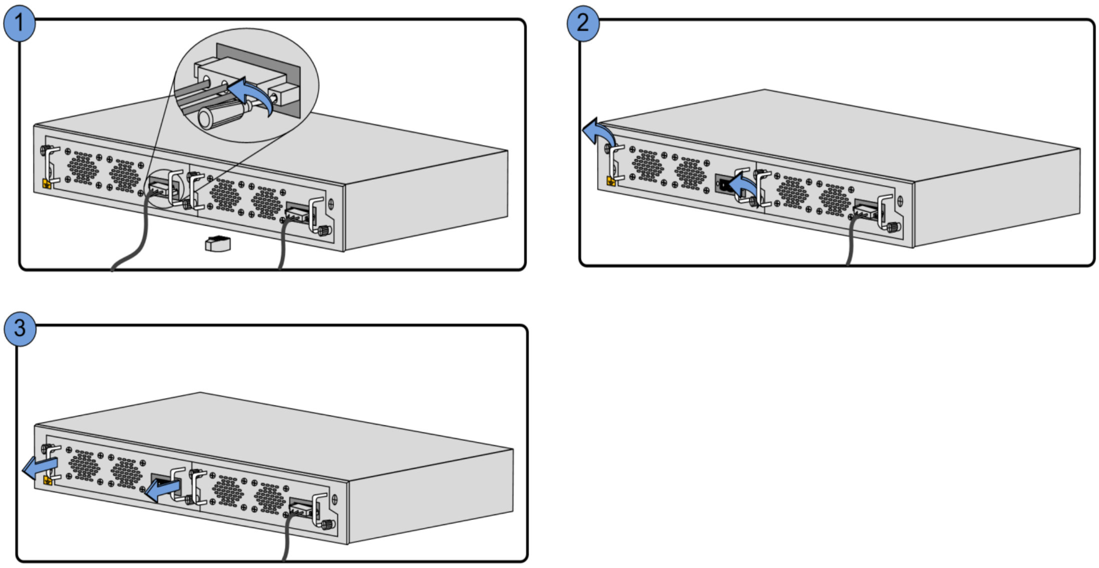
- Please do not removal and install power modules with power on.
- Turn off the switch corresponding to power distribution box, unplug the power cord when replacing power module.
- Connect power cord and rack power distribution box to power on the device after installing power module correctly.
- Wear antistatic wrist strap in removal and installation operation.

The specific steps are as follows:

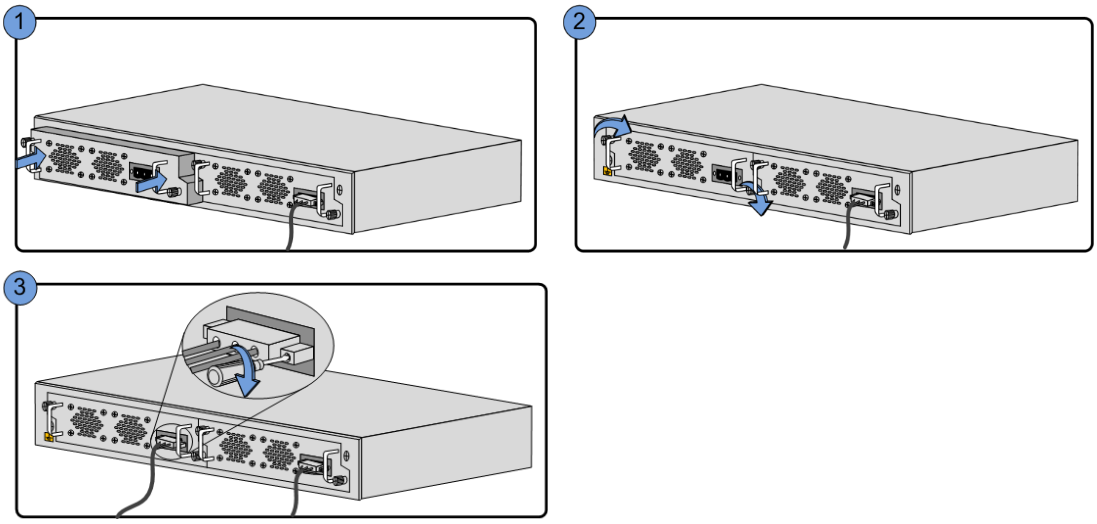
Note:

- ISCOM2924GF-4GE/4C device power configuration is in support of dual DC, dual AC, or mixed power (1 DC+1AC) configuration. Here, take DC power module replacement as an example.
- If replacing the AC power module, it needs to open power card buckle when removing power module and close it after connecting the power cord. Other operations are the same to DC power module replacement.

1. Make sure the power module location to replace. Turn off the switch corresponding to power distribution box, power off the device.
2. Remove power cord for the power module to replace, as shown in the following Figure (1).
3. Loosen the captive screws at both ends of power module, as shown in Figure (2) below.
4. Pull out the power module to replace, seize power module handle at both ends, gently remove the power module from the device, as shown in Figure (3) below.



5. Plug the standby power module in device, hold the handle on both ends and gently plug power module into the slot until it is connected to the device in a good condition, as shown in the following Figure (1).
6. Fix the captive screws at both ends of the power module, as shown in Figure (2) below.
7. Connect power cord on power module, as shown in Figure (3) below.
8. Connect the power cord to the corresponding position of original power module on power distribution box, turn on the related switch and power on the device.



Check device indicator to make sure the power module works normally.

2.4 Software maintenance

Item	Cycle	Method	Standards and description
Alarm	Day	**Real-time monitor alarms**	Normal for no alarm. Record and analyze alarm if there is alarm information.

Item	Cycle	Method	Standards and description
Log	Day	**show logging** Command: **show logging file**	Normal for no lots of repeated logs. If there is, analyze and deal with it immediately processing it. Note: The commands of **show logging** and **show logging file** can only see the system logs in a period of time, if you need to check all the log information, please enter log server.
Operating configuration	Week	**show running-config**	Make sure the system configuration is correct.
Startup file	Week	**show startup-config**	Make sure the startup file is correct
System time	Week	**show clock**	Make sure the system time is correct
License	Week	EMS enquiry	Inquiry results should be as expected.
Ping & Traceroute	Week	**ping** and **traceroute**	Test for network nodes passed by, and analyze the network fault point.
Features	Week	Refer to *ISCOM2924GF-4GE&4C Configuration Guide*	Each feature should be in line with the requirements.
Software Version	Month	**show version**	Normally, displayed system software version No. should be as expected.
User Management	Month	**show user**	User information should be consistent with the requirements.
SNMP TRAP configuration	Month	**show snmp config**	Check the SNMP Trap state. When the device monitors anomalies of the fans speed and temperature, it will produce the alarm and send Trap.

2.5 Service maintenance

The service maintenance of ISCOM2924GF switch contains Ethernet features, network reliability, OAM features, security features, Qos features and system feature maintenance.

2.5.1 Ethernet features maintenance

User can take Ethernet feature maintenance for the device as below:

Command	Description
Raisecom(config)#**clear mac-address-table** { **all** | **blackhole** | **dynamic** | **static** }	Clear MAC address
Raisecom(config-port)#**spanning-tree clear statistics**	Clear interface spanning-tree statistics
Raisecom(config-port)#**clear loopback-detection statistic**	Clear loopback-detection statistics

Command	Description
Raisecom(config)#**clear relay statistics** [**port-list** *port-list*]	Clear transparent transmission messages statistics
Raisecom#**show mac-address-table static** [**port** *port-id* | **vlan** *vlan-id*]	Show static unicast MAC address
Raisecom#**show mac-address-table multicast** [**vlan** *vlan-id*] [**count**]	Show layer-2 multicast address
Raisecom#**show mac-address-table l2-address** [**count**] [**vlan** *vlan-id* | **port** *port-id*]	Show all layer-2 unicast addresses and learned MAC address count
Raisecom#**show mac-address-table threshold** [**port-list** { **all** | *port-list* }]	Show the learnt MAC address count threshold
Raisecom#**show mac aging-time**	Show MAC address aging time
Raisecom#**show vlan** [*vlan-list* | **static**]	Show VLAN configuration
Raisecom#**show interface port** [*port-id*] **switchport**	Show interface VLAN configuration
Raisecom#**show switchport qinq**	Show basic QinQ configuration
Raisecom#**show interface port** [*port-id*] **vlan-mapping add-outer**	Show flexible QinQ configuration
Raisecom#**show interface port** *port-id* **vlan-mapping** { **ingress** | **egress** } **translate**	Show 1:1 VLAN mapping configuration
Raisecom#**show spanning-tree**	Show basic STP configuration
Raisecom#**show spanning-tree port** *port-list*	Show STP configuration at interface
Raisecom#**show spanning-tree** [**instance** *instance-id*] **port** *port-list* [**detail**]	Show STP configuration at interface
Raisecom#**show spanning-tree region-operation**	Show MST region configuration
Raisecom#**show loopback-detection** [**port-list** *port-list*]	Show interface loopback detection configuration
Raisecom#**show loopback-detection block-vlan** [**port-list** *port-list*]	Show the blocked VLAN information by loopback detection
Raisecom#**show switchport protect**	Show interface protection configuration
Raisecom#**show mirror**	Show interface mirror configuration
Raisecom#**show relay** [**port-list** *port-list*]	Show transparent transmission configuration and status
Raisecom#**show relay statistics** [**port-list** *port-list*]	Show transparent transmission messages statistics

2.5.2 Network reliability maintenance

User can take network reliability maintenance for the device as below:

Command	Description
Raisecom(config)#**clear ethernet line-protection** [*line-id*] **statistics**	Clear protection line statistics
Raisecom(config)#**clear ethernet ring-protection** *ring-id* **statistics**	Clear protection ring statistics
Raisecom(config)#**clear ethernet ring** *ring-id* **statistics**	Clear ring interface statistics
Raisecom#**show lacp internal** [**detail**]	Check local system LACP protocol interface status, mark, interface priority, management key, operation key and interface status machine state
Raisecom#**show lacp neighbor** [**detail**]	Check neighbor LACP protocol information, including mark, interface priority, device ID, Age, operation key, interface No. and interface status machine state
Raisecom#**show lacp statistics** [**port-list** *port-list*]	Check interface LACP protocol statistics, including total number of receiving and sending LACP messages, Market messages, Market Response messages and error messages
Raisecom#**show lacp sys-id**	Check local system LACP protocol global enabling situation, device ID, including LACP protocol priority and system MAC address
Raisecom#**show link-aggregation**	Check whether the current system enables aggregation link, link aggregation load-balancing mode, current group member interface set by all aggregation group and current effective members interface
Raisecom#**show switchport backup**	Check interface backup status information, including restore delay time, restore mode and interface backup group information, which contains master interface, standby interface and their status (Up/Down/Standby) and VLAN list.
Raisecom#**show ethernet line-protection** [*line-id*]	Check whether protection line configuration is correct
Raisecom#**show ethernet line-protection** [*line-id*] **statistics**	Check protection line statistics
Raisecom#**show ethernet line-protection** [*line-id*] **aps**	Check APS protocol information
Raisecom#**show ethernet ring-protection**	Check whether ERPS ring configuration is correct
Raisecom#**show ethernet ring-protection status**	Check whether the ERPS ring status is correct
Raisecom#**show ethernet ring-protection statistics**	Check ERPS ring statistics
Raisecom#**show ethernet ring** [*ring-id*]	Check Ethernet ring information
Raisecom#**show ethernet ring port**	Check Ethernet ring interface information
Raisecom#**show ethernet ring port statistic**	Check Ethernet ring interface messages statistics

2.5.3 OAM maintenance

User can take OAM maintenance for the device as below:

Command	**Description**
Raisecom(config-port)#**clear oam statistics**	Clear EFM OAM interface link statistics
Raisecom(config)#**clear ethernet cfm errors** [**level** *level*]	Clear CCM error database information
Raisecom(config)#**clear ethernet cfm remote-mep** [**level** *level*]	Clear remote MEP
Raisecom(config)#**clear ethernet cfm traceroute-cache**	Clear Traceroute Cache database
Raisecom(config)#**clear ethernet lmi statistics port-list** { **all** | *port-list* }	Clear interface E-LMI statistics
Raisecom#**show oam** [**port-list** *port-list*]	Check EFM basic configuration
Raisecom#**show oam loopback** [**port-list** *port-list*]	Check EFM remote loopback configuration
Raisecom#**show oam notify** [**port-list** *port-list*]	Check OAM link monitoring and fault indication configuration
Raisecom#**show oam statistics** [**port-list** *port-list*]	Check OAM statistics
Raisecom#**show oam trap** [**port-list** *port-list*]	Check OAM event alarm configuration
Raisecom#**show oam event** [**port-list** *port-list*] [**critical**]	Check local serious fault information detected by interface
Raisecom#**show oam peer event** [**port-list** *port-list*] [**critical**]	Check local serious fault information sent from peer device
Raisecom#**show ethernet cfm**	Check CFM global configuration
Raisecom#**show ethernet cfm domain** [**level** *level*]	Check maintenance domain and service instance configuration
Raisecom#**show ethernet cfm errors** [**level** *level*]	Check error CCM database information
Raisecom#**show ethernet cfm lck** [**level** *level*]	Check Ethernet lock signal
Raisecom#**show ethernet cfm local-mp** [**interface port** *port-id* | **level** *level*]	Check local MEP configuration
Raisecom#**show ethernet cfm remote-mep** [**static** [**level** *level*]]	Check static remote MEP information
Raisecom#**show ethernet cfm remote-mep** [**level** *level* [**service** *name* [**mpid** *local-mep-id*]]]	Check remote MEP information
Raisecom#**show ethernet cfm suppress-alarms** [**level** *level*]	Check CFM alarm suppression function configuration

Command	Description
Raisecom#**show ethernet cfm traceroute-cache**	Check fault location database traceroute information
Raisecom#**show sla** { **all** | *oper-num* } **configuration**	Check SLA configuration
Raisecom#**show sla** { **all** | *oper-num* } **result**	Check the latest test operation information
Raisecom#**show sla** { **all** | *oper-num* } **statistic**	Check operation scheduling statistics letter. The same operation (distinguished by operation No.) can record a maximum of 5 group statistics information, if the number is above 5, the oldest statistics will be aged (subject to the starting time of scheduling)
Raisecom#**show ethernet lmi config port-list** { **all** | *port-list* }	Check interface E-LMI configuration
Raisecom#**show ethernet lmi statistics port-list** { **all** | *port-list* }	Check interface E-LMI statistics
Raisecom#**show ethernet lmi uni port-list** { **all** | *port-list* }	Check UNI configuration
Raisecom#**show ethernet lmi evc** *evc-number*	Check EVC status
Raisecom#**show ethernet lmi evc map port-list** { **all** | *port-list* }	Check EVC and CE-VLAN mapping information
Raisecom#**show ethernet lmi evc map oam**	Check EVC mapping OAM protocol information

2.5.4 Security feature maintenance

User can take security feature maintenance for the device as below:

Command	Description
Raisecom(config)#**clear filter statistics** [*filter-number*]	Clear filter statistics
Raisecom#**clear tacacs statistics**	Clear TACACS+ statistics
Raisecom#**show ip-access-list** [*acl-list*]	Check IP ACL configuration
Raisecom#**show ipv6-access-list** [*acl-list*]	Check IPv6 ACL configuration
Raisecom#**show mac-access-list** [*acl-list*]	Check MAC ACL configuration
Raisecom#**show access-list-map** [*acl-number*]	Check MAP ACL configuration
Raisecom#**show filter** [*filter-number-list*]	Check filter configuration
Raisecom#**show radius-server**	Check RADIUS server configuration

Command	Description
Raisecom#**show tacacs-server**	Check TACACS+ server configuration
Raisecom#**show storm-control**	Check storm suppression configuration

2.5.5 QoS feature maintenance

User can take Qos feature maintenance for the device as below:

Command	Description
Raisecom(config)#**clear service-policy statistics** [**egress** | **ingress** | **port**] *port-list* [**class-map** *class-map-name*]	Clear QoS messages statistics
Raisecom(config)#**clear rate-limit statistics vlan** [*vlan-id*]	Clear VLAN rate-limit packet loss statistics
Raisecom#**show mls qos priority** [**port** *port-id*]	Check interface priority trust rule configuration
Raisecom#**show mls qos**	Check QoS configuration
Raisecom#**show class-map** [*class-map-name*]	Check specified traffic classification rule configuration
Raisecom#**show mls qos policer** [*policer-name* | **aggregate-policer** | **class-policer** | **single-policer**]	Check specified rate limit rule configuration
Raisecom#**show policy-map** [*policy-map-name* [**class** *class-map-name*] | **class** *class-map-name* | **port** *port-id*]	Check specified traffic policy configuration
Raisecom#**show service-policy statistics** [**port** *port-id*]	Check the applied policy statistics
Raisecom#**show mls qos mapping** { **cos** | **dscp** | **localpriority** }	Check specified priority mapping relation configuration
Raisecom#**show mls qos queue**	Check queue scheduling configuration

2.5.6 System feature maintenance

User can take system feature maintenance for the device as below:

Command	Description
Raisecom(config)#**clear lldp statistic** [**port** *port-id*]	Clear LLDP statistics
Raisecom(config)#**clear lldp remote-table** [**port** *port-id*]	Clear LLDP neighbor information
Raisecom(config)#**clear rmon**	Clear all RMON configuration
Raisecom#**show snmp access**	Show SNMP access group configuration

Command	Description
Raisecom#**show snmp community**	Show SNMP community configuration
Raisecom#**show snmp config**	Show basic SNMP configuration, including local SNMP engine ID, administrator logo and contact method, switch location, and TRAP switches status
Raisecom(config)#**show snmp group**	Show the mapping relationship between SNMP users and access group
Raisecom(config)#**show snmp host**	Show Trap destination host information
Raisecom(config)#**show snmp statistics**	Show SNMP statistics
Raisecom(config)#**show snmp user**	Show SNMP users information
Raisecom(config)#**show snmp view**	Show SNMP view information
Raisecom#**show keepalive**	Show KeepAlive configuration
Raisecom#**show rmon**	Show RMON related information
Raisecom#**show rmon alarms**	Show RMON alarm group information
Raisecom#**show rmon events**	Show RMON event group information
Raisecom#**show rmon statistics**	Show RMON statistics group information
Raisecom#**show rmon history** { **port** *port-id* | **ip** *if-number* }	Show RMON history group information
Raisecom#**show lldp local config**	Show LLDP local configuration
Raisecom#**show lldp local system-data** [**port** *port-id*]	Show LLDP local system information
Raisecom#**show lldp remote** [**port** *port-id*] [**detail**]	Show LLDP neighbour information
Raisecom#**show lldp statistic** [**port** *port-id*]	Show LLDP messages statistics
Raisecom#**show logging**	Show system log configuration
Raisecom#**show logging buffer**	Show system log buffer information
Raisecom#**show logging discriminator**	Show filter information
Raisecom#**show logging file**	Show system log file content
Raisecom#**show logging history**	Show system log history list information
Raisecom#**show alarm management** [*module_name*]	Show current alarm parameters configuration information, including alarm suppression, alarm reverse mode, alarm delay, alarm storage mode, the maximum alarm number stored in alarm buffer and the maximum number stored in alarm log.

Command	Description
Raisecom#**show alarm log**	Show system log alarm statistics
Raisecom#**show alarm management statistics**	Show alarm management module statistics
Raisecom#**show alarm**	Show global hardware monitoring alarm configuration information, including global alarm Syslog output, global sending Trap, power off alarm, temperature alarm and voltage alarm.
Raisecom#**show alarm port-list** *port-list*	Show interface status alarm
Raisecom#**show alarm currrent**	Show hardware monitoring current alarm
Raisecom#**show alarm history**	Show hardware monitoring history alarm
Raisecom#**show environment** [**power** | **temperature** | **voltage**]	Show current device power, temperature, voltage alarm and environment information
Raisecom#**show fan-monitor information**	Show fan monitoring configuration
Raisecom#**show fan-monitor status**	Show current fan status
Raisecom#**show cpu-utilization**	Show CPU utilization and related configuration
Raisecom#**show version**	Show device running version information
Raisecom#**show running-config**	Show current configuration
Raisecom#**show clock**	Show system time
Raisecom#**show power-card**	Show power type and serial No.

2.6 Data backup and recovery

In the daily maintenance, for the safety of the data, users can take data backup regularly. Data backup usually contains system boot file ("z" for the suffix), configuration file (".cfg" for the suffix), system alarms and system log files backup.

System boot files and configuration files backup are used for system data recovery after equipment failure. System alarms and system logs backup are used for technical personnel to take fault location.

Note : System boot files and configuration files are required for backup before the upgrade.

Suggest backup system boot file every quarter through the command of **upload system-boot** on FTP/TFTP.

2.6.1 Backup alarm and log

2.6.1.1 Backup alarm

- Alarm files for alarm backup on server and device should be the same completely.
- Alarms backup should operate on EMS platform.
- Inspect it by EMS every quarter.

2.6.1.2 Backup log

- The device will make the key information, debugging information, error information from system generate system log, output log files and transmit them to log host, Console interface, monitor console or Flash memory, so that users can check and position the faults. The backup log files on server and device should be the same completely.
- System log backup should be taken once a quarter manually, which can be copied to either maintenance terminal device or log server.
- Use network management software for examination once a quarter.

2.6.2 Backup configuration file

The configuration file, in suffix of ".cfg", is loaded when equipment startup, which can be open by notepad function in Microsoft's Windows series operating system.

Configuration file backup is a kind of data safety measure; user can save current running configuration file to safe position at any time, for the benefit of data recovery after data corruption.

The configuration file backup needs to operate manually. Better to backup it after each modification.

2.6.2.1 Copy to screen

In the debug tool interface, executive configuration commands and copy and paste the display information to a txt file so as to backup configuration file to the terminal hard disk.

2.6.2.2 Backup on TFTP

The steps are as follows:

1. Configure IP address, which must be in the same network segment with TFTP server.

2. Start TFTP server. Through the network to connect ISCOM2924GF switch and TFTP server, then by **upload** command backup configuration file in Flash memory to TFTP server.

3. Executive command: **upload startup-config tftp** *10.0.0.1* **config**

The result:

```
Raisecom#upload startup-config tftp 10.0.0.1 config
  Waiting...Start
  Uploading 1K/1K
  Success
```

Note: User can set the IP address parameters according to the network environment.

2.6.2.3 Backup on FTP

The steps are as follows:

1. Configure IP address and start FTP server.

2. Through the network to connect ISCOM2924GF switch and FTP server, then by **upload** command backup configuration file in Flash memory to FTP server. It needs to input user name and password in configuration.

3. Executive command: **upload startup-config ftp** *10.0.0.1* **raisecom raisecom config**

The result:

```
Raisecom#upload startup-config ftp 10.0.0.1 raisecom raisecom config
    Waiting...
```

Note: User can set the IP address parameters according to the network environment. The user name and password can be set based on FTP server. The user name and password in example are both raisecom.

2.6.3 Recover configuration file

2.6.3.1 Recover backup configuration file on PC through TFTP

The steps are as follows:

1. Configure IP address.

2. Start TFTP server. Through the network to connect ISCOM2924GF switch and TFTP server, then by **download** command recover configuration file backup in TFTP server to Flash memory.

3. Executive command: **download startup-config tftp** *10.0.0.1* **config**

The result:

```
Raisecom# download startup-config tftp 10.0.0.1 config
  Waiting...Start
  Downloading 1K
  Success
```

Note : User can set the IP address parameters according to the network environment.

4. Transmit configuration files and set configuration files for next startup.

TFTP adopts the backup and recovery without any safety authentication, which make it easy for other people to snooping.

2.6.4.1 Recover backup configuration file on PC through FTP

The steps are as follows:

1. Configure IP address.

2. Start FTP server. Through the network to connect ISCOM2924GF switch and FTP server, then by **download** command recover configuration file backup in FTP server to Flash memory.

3. Executive command: **download startup-config ftp** *10.0.0.1* **raisecom raisecom config**

The result:

Raisecom# **download startup-config ftp** *10.0.0.1* **raisecom raisecom config**

Waiting...

Note : User can set the IP address parameters according to the network environment. The user name and password can be set based on FTP server. The user name and password in example are both raisecom.

4. Transmit configuration files, and set configuration files for next startup.

FTP protocol is available to pass through multiple segments, as long as providing destination routing information. Therefore, it is easy to realize the remote backup and recovery and facilitate network management.

Chapter 3 Troubleshooting

This chapter contains the following information:

- ✧ Troubleshooting instructions
- ✧ Troubleshooting process
- ✧ Fault removal process
- ✧ Common methods for fault localization
- ✧ Requirements on maintenance staff
- ✧ Raisecom technical support

3.1 Troubleshooting instructions

The guide focuses on introducing the fault classification according to network position and network application of the device, common typical problem and fault phenomenon. The common fault of ISCOM2924GF series products can be classified as below:

- ✧ System management troubleshooting
- ✧ Interface troubleshooting
- ✧ Layer-2 network troubleshooting
- ✧ IP forward and route troubleshooting
- ✧ Service troubleshooting

The above classification is mainly based on the simple common fault, some in reality maybe the combination of fault classifications.

When the device is at fault, please check related chapter according to fault phenomenon, deal with the problem refers to fault diagnosis process, troubleshooting processing steps and the cases.

3.2 Troubleshooting process

3.2.1 Fault information collection

This section focuses on introducing the source, necessity and content of fault information collection.

3.2.1.1 The source of fault information

The fault information generally origins from the following ways:

- ➢ Users fault report
- ➢ Fault report gave by maintenance personnel of adjacent device;
- ➢ Device alarm output
- ➢ Information collected from maintenance tool
- ➢ Daily maintenance or inspection found in the abnormal.
- ➢ Syslog

3.2.1.2 The necessity of fault information collection

It is necessary to collect fault information when fault happens. The main reasons are as below:

- The expanding network size and increasingly complex network environment make the fault causes more complex and increase the difficulty of fault localization. So it is the key to collect information effectively and completely for fault localization.
- The fault phenomenon is generally collected by telephone when fault happens, but this kind of feedback cannot collect comprehensive and integrated content which may not respond the essence of fault directly.
- For summarizing fault reasons and preventing the same fault, it needs to collect detailed fault information to find the fundamental cause.

3.2.1.3 The content of fault information collection

The following table shows partial content of fault information collection:

Table fault information collection

Collection item	**Note**
Fault phenomenon	
Fault time and rate	
Operation before the fault	
Issue tracking when fault happens	
Output information when fault happens	
Alarm information when fault happens	
Log information when fault happens	
Operation after the fault	
Networking situation	
Software and hardware version information of fault device and related devices	
Configuration information of fault device and related devices	

3.2.2 Fault judgment

Judge according to fault information and related product knowledge and confirm the fault scope and category. That is, make sure the occurred range, group and type of fault.

3.2.3 Fault localization

The occurrence of fault has its oneness in a specific time. That is to say, in many possible reasons, only one leads to the fault. This basic principle determines the basic method for fault localization.

Fault localization means the process to find the correct reason from many possible reasons. Through a series of methods and skill, analyze the possible reasons, eliminate the impossible factors and finally make sure the real cause for fault.

The fault localization method also provides guidance and reference for troubleshooting.

3.2.4 Fault removal

After the correct fault localization, start the most important step: fault removal.

Fault removal refers to the process to remove the fault and recover the normal work of system through right methods (such as check and maintain the line, replace the veneer, modify the configuration, replace the system, reset the machine and etc.) after correct fault localization.

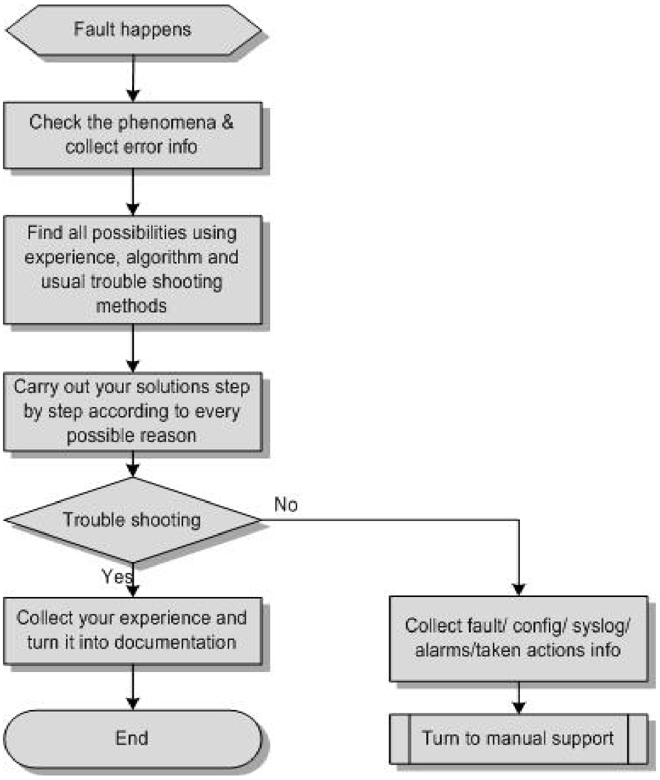
3.2.5 Fault summary

The final step for troubleshooting is experience summary. The experience summary is a documented process for troubleshooting. It is very necessary for the following reasons:

- The document is the precious experience summary and important reference material for the future troubleshooting.
- The document has taken a record of all operation and configuration changes in the process of troubleshooting and provides related proof for the next fault localization.

3.3 Fault removal process

Flow chart of fault removal:


Fault happens
Check the phenomena & collect error info
Find all possibilities using experience, algorithm and usual trouble shooting methods
Carry out your solutions step by step according to every possible reason
Trouble shooting
No
Yes
Collect your experience and turn it into documentation
End
Collect fault/ config/ syslog/ alarms/taken actions info
Turn to manual support

Flow chart of fault removal

3.4 Common methods for fault localization

3.4.1 Alarm analysis

Alarm means the simple and clear alarm information output from ISCOM2924GF alarm system to maintenance personnel, usually in the form of voice, screen and etc. It is one of the principal means for fault localization.

Note: See *ISCOM2924GF-4GE/4C Alarm Reference* for specific alarm information.

The device fault often causes a large number of alarms. Analyze the alarms to judge the fault type and location.

Obtain the alarm by the following methods:

- Obtain the current and historic alarm of device by checking network management.
- The indicator light state on device panel
- Log document of device

The characteristics to locate fault from fault information are as follows:

- Comprehensive: Network management alarm information contains all the device information.
- Accurate: Network management alarm information contains alarm type, alarm time and related historic alarm.
- The communication fully depended on network management computer and device is normal. Once the communication breaks down, the ability to obtain fault information by this way will be lowered greatly or even lost fully.

3.4.2 Indicator light analysis

Indicator light analysis refers to locate the fault from the indicator light state of device. Check the indicator state to judge the work state of following units:

- Interface work state
- Power work state

Generally, it needs to locate the fault together with the alarm analysis because indicator light can only provide seldom information.

Note: Please see *2.3.1 Indicator check* for the specific meaning of ISCOM2924GF panel indicator.

3.4.3 Signal flow analysis

Signal flow analysis refers to check every part of device point-by-point according to service orientation, which can locate the fault quickly.

3.4.4 Instrument test

Instrument test means to test and verify the fault by instrument directly. The main features are:

- Check the fault by direct test.
- Higher requirement to maintenance staff
- There is part limitation to fault localization. It needs to configure professional instrument and

can only check the work state of some units.

Note: The common instruments are: light power meter, multi-meter, BER tester, network analyzer, cable tester, etc.

3.4.5 Performance analysis

Analyze the performance index of fault service by performance statistics method and check fault reasons.

The fault localization needs to understand the system performance statistics information. Based on different fault type, the maintenance personnel need to check different statistics information, make familiar with system structure and operation mechanism, check what kind of statistics information the system can provide and how to check and analyze statistics information.

For example: use **show interface port** [*port-id*] **statistics** command to check Ethernet interface statistics information in physical layer interface mode so as to judge whether the device runs normally. If wrong CRC message increases quickly, it shows that the link may be abnormal, interface negotiation may be wrong or physical interface may appear fault. If there is plenty of loss of packet, it shows that the flow sent by butting device outweighs the receiving capacity of interface.

3.4.6 Switchover/Reset

Pay close attention to the following items with switchover and reset methods:

- Backup the configuration in advance to prevent service configuration lost caused by reset.
- Switchover and reset will give rise to the interruption of service, even system paralysis with incorrect operation.

Switchover refers to switch the work manually between master device and minor device, that is to say, switch the service from master device to minor device. The service can be switched to minor device when the master device appears fault which cannot be ruled out in case of emergency.

Reset means to restart the running device manually. In extreme cases, the fault can be eliminated by reset. Reset operation may lose some data and information related to the fault and has no advantages to fault localization and removal, so this method should be avoided as far as possible.

Compared to other methods, switch and reset cannot make accurate localization to the fault reasons. However, they may cover the essence of fault and cause hidden danger to the safe and stable operation o f device. Therefore, they can only be a kind of emergency measures and used in extreme cases cautiously.

3.4.7 Replacement

Replacement refers to locate fault using normal units to replace trouble units when fault happens. Replacement is the commonly used fault localization method and can locate the fault on a certain unit quickly. Generally, it is only applied to the simple occasion with single fault reason.

Replacement is the most efficient method for hardware fault. It can remove fault and restore service very quickly. Be noted that, replacement is dangerous some times, for example: the optical interface module is damaged by over-strong optical power, after replacing a new one, it may be damaged again. Thus to perform replacement must try to avoid new fault.

3.5 Requirements on maintenance staff

3.5.1 Professional quality and skill

Here are the basic quality requirements on profession knowledge on maintaining and troubleshooting staff:

- Master the basic concepts and principles of data communication and optical communication;
- Master the basic concepts and principles of switch technology;
- Master the solutions of dealing with common alarms.

3.5.2 Familiar with system and networking

The staff to maintain and remove fault on the device must know general structure of the device locating network, including but not only the below items:

- Familiar with the device layer in network and the upper/down interconnected devices;
- Familiar with the interface property setting of interfaces;
- Familiar with direction of service flow;
- Familiar with device operation condition.

3.5.3 Basic operation on device

The maintenance staff must be familiar with the most basic and common operation methods:

- Understand the basic operation of device;
- Understand the basic operation of NMS.

3.5.4 Common using on the meters and instruments

The maintenance staff must know how to use the meters and instruments. Refer to the related user manuals for each meter and instrument for detail using.

3.6 Raisecom technical support

If user cannot solve the fault problem, please contact Raisecom technical support.

- Telephone: 400-890-1001, 8610-82883110 (7x24 hours)
- Contact the local office.
- E-mail address: help@raisecom.com
- Fax: 8610-82885200, 8610-82884411

Chapter 4 System Management Troubleshooting

This chapter focuses on introducing the system fault location methods and processing steps.

- Telnet login problem
- SSH login fault

4.1 Telnet login problem

4.1.1 Fault phenomenon

Administrator cannot login the device through Telnet.

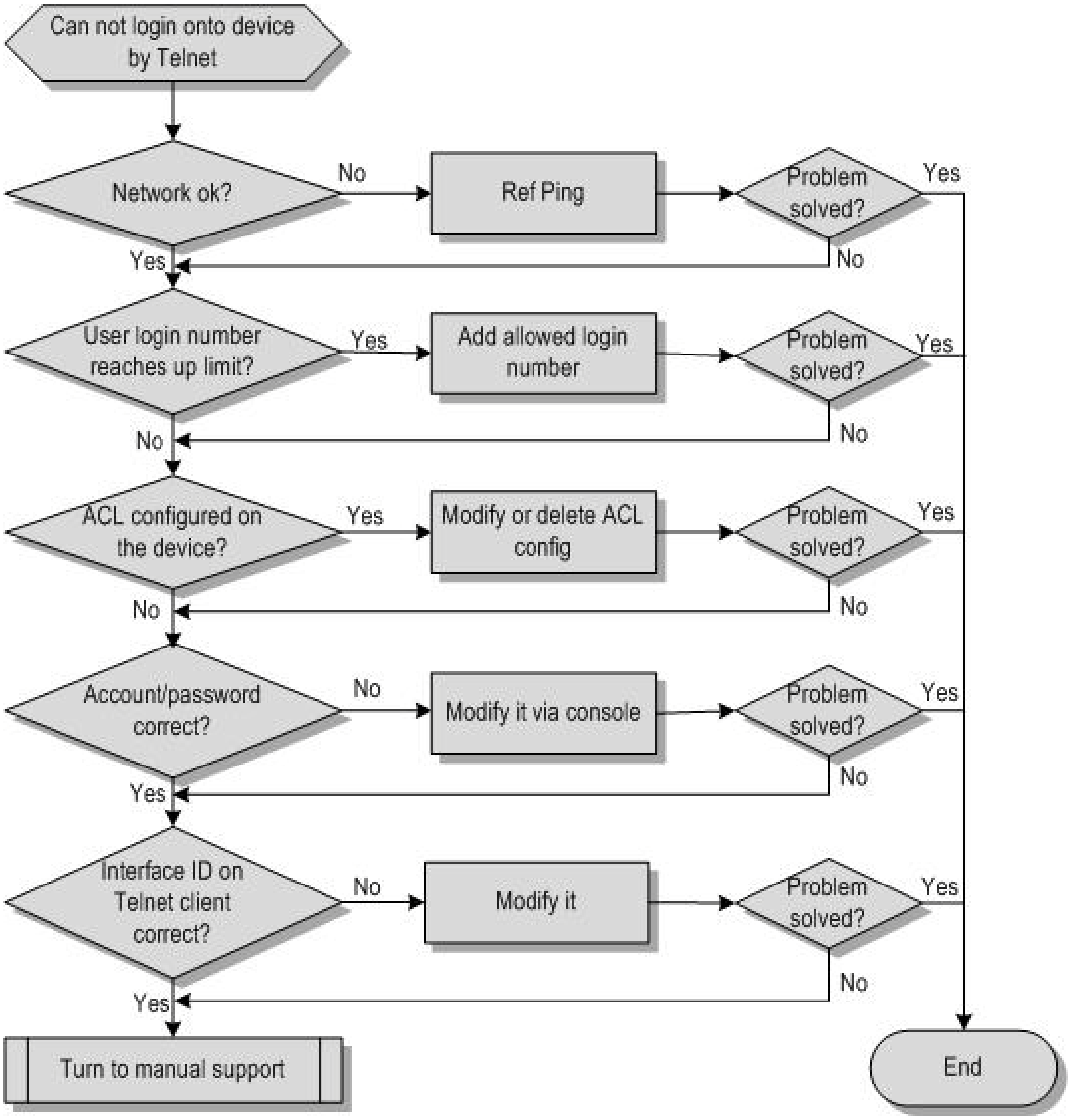
4.1.2 Possible reasons

The telnet login problem may be caused by the following reasons:

- Route blocked, unable to establish TCP connection.
- Login users reach the upper limit.
- Device has been configured ACL.
- User name and password configuration error.
- Telnet client is set incorrectly.

4.1.3 Fault diagnosis process

Flow chart of fault diagnosis:



Flow chart of fault diagnosis for telnet login fault

4.1.4 Troubleshooting processing steps

Note: Please save the executive results of following steps so as to gather and feedback information quickly when failed to solve the problems.

- Check the network connectivity.

Check whether there is unstable network connection, for example loss of packets, login/logoff and etc.

Use **ping** command to check the network connection status between telnet client and device. If Ping the connection unsuccessfully, the telnet connection will also fail, see “Ping error” continue to position so that the telnet client can ping the device.

Start step 2 if the network is connective.

- Check whether the device is in support of Telnet function.

Telnet connection cannot be established if user-located interface is not in support of Telnet function.

Login the device from Console port and use the command of **telnet-server accept port-list** *port-list* to configure the Telnet function interface.

Raisecom#**show telnet-server**

```
Max session: 5
Accept port-list: 1-8
Using session-list: 1
```

Start step 3 if the user-located interface is in support of Telnet function.

- Check whether login users reach the upper limit.

Login the device from Console port; carry out **show user** command to check the current user number. By default, allow a maximum of 5 users to login.

Raisecom#**show user**

```
  Username              Priority       Server
-------------------------------------------
  Raisecom1              15              Local
  raisecom2              15              Local
```

Start step 4 if login users haven't reach upper limit.

- Check whether the device is configured ACL.

Login the device from Console port, use **show filter** command to check whether the device is configured ACL. If it is configured ACL, please use **show ip-access-list** or **show access-list-map** command to check whether there is deny client IP address or telnet TCP port protocol rules. If yes, cancel the corresponding rules.

Start step 5 if the device isn't configured ACL or the ACL is configured correct.

- Check whether the user name and password are correct.

By default, the user name and password are both *raisecom*.

Login the device from Console port, use **user name** *user-name* **password** *password* command to create or modify the user name and password under Privileged EXEC mode.

Start step 6 if user name and password are both correct.

- Please collect the following information and contact Raisecom technical support if the above steps cannot solve problems.
  - The executive results of above steps
  - Device configuration files, log information and alarm information

4.2 SSH login fault

4.2.1 Fault phenomenon

Users cannot login the device through SSH.

4.2.2 Possible reasons

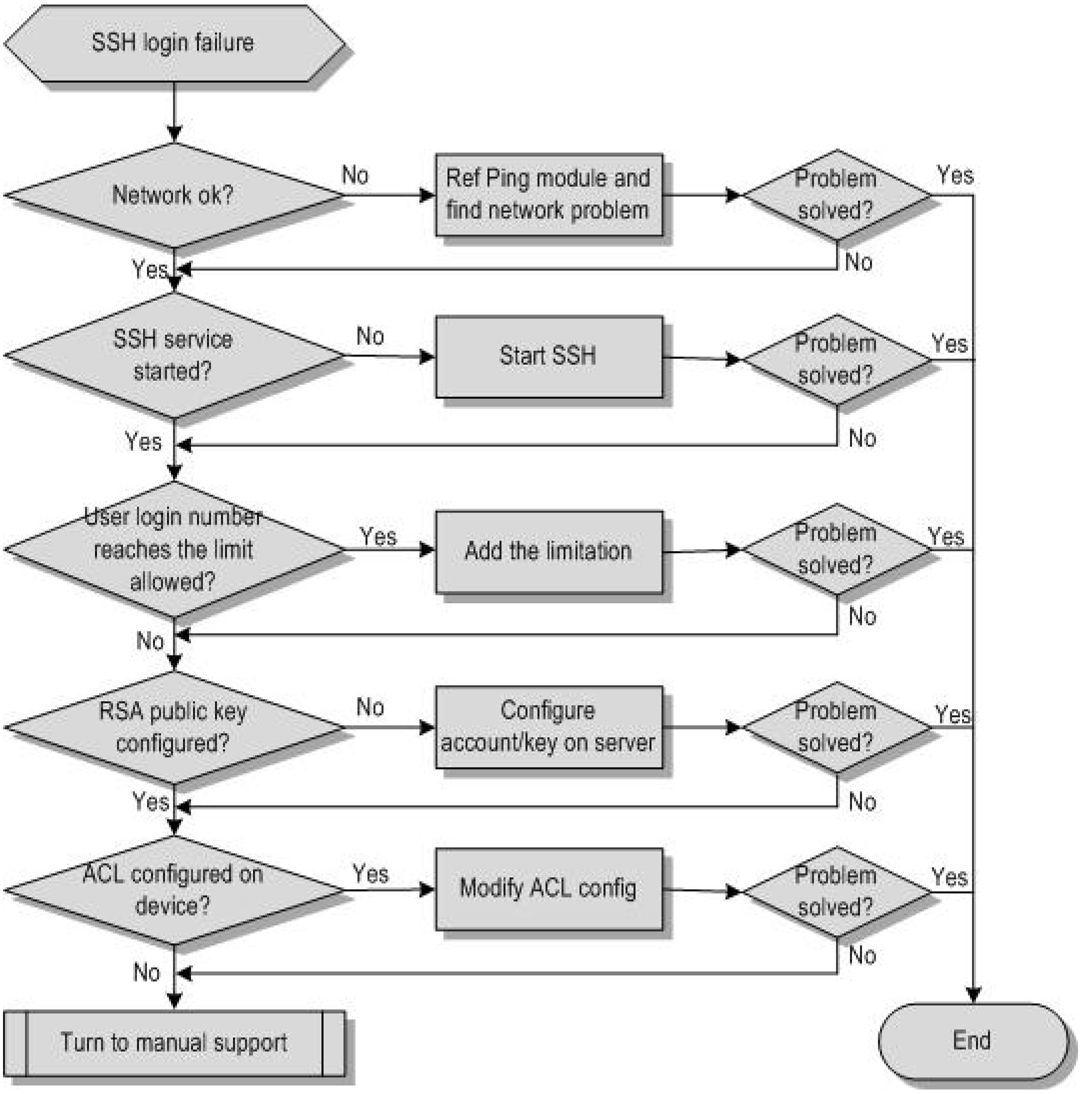
The SSH login fault may be caused by the following reasons:

- Route blocked, unable to establish TCP connection.

- ➢ The SSH version of server and client are inconsistent.
- ➢ Haven’t started SSH service.
- ➢ Haven’t configured SSH server and client RSA public key.
- ➢ Login users reach the upper limit.
- ➢ The device has been configured ACL.

4.2.3 Fault diagnosis process

Flow chart of fault diagnosis:



Flow chart of fault diagnosis for SSH login fault

4.2.4 Troubleshooting processing steps

Note: Please save the executive results of following steps so as to gather and feedback information quickly when failed to solve the problems.

- ➢ Check network connectivity.

Use **ping** command to check the network connection status. If Ping the connection unsuccessfully, the SSH connection will also fail.

Start step 2 if the network is connective.

- Check whether there is unstable network connection, for example loss of packets, login/logoff continued and etc. If the network is not connective, see "Ping error" continue to position so that the SSH client can Ping the device.

Start step 3 if the network is stable.

- Check the SSH version client information.

The clients need to switch over to SSHv2 because ISCOM2924GF only supports this version.

Start step 4 if SSH version is correct.

- Check whether the SSH service is enabled.

Login the device from Console port, and use the command of **show ssh2 server** to check SSH servicer port configuration information.

Raisecom#**show ssh2 server**

```
SSH server information:
------------------------------------------------------------------
State:    Enable
Version:    ssh-2
Authentication method(default:local user-password ):    local user-password
Authentication timeout(default 600):    600s
Authentication retries(default 20):    20
Max client count(default 5):    5
Current    client count:    0
Current    channel count:    0
Listen port on (default 22):    22
```

SSH servicer enable/disable can be seen through above display information. Only when the system enables SSH service, users can login. The following command can make SSH server enable.

Raisecom#**config**

Raisecom(config)#**ssh2 server**

Start step 5 if SSH service is enabled.

- Check whether login users reach the upper limit.

The device can allow a maximum of 5 SSHv2 client ports. It will no longer accept new connection when users logged in are more than 5.

Login the device from Console port, and carry out the command of **show ssh2 session** to check whether the SSH channel is occupied fully.

Raisecom#**show ssh2 session**

```
ID   Ver Cipher(IN/OUT)        Con-Time     State            UserId          Ip
----------------------------------------------------------------------
 0   2.0 aes/aes              0h:0m:13s   OK(1channels) raisecom      10.169.0.9
 1   2.0 --/--                --          Closed          --              --
 2   2.0 --/--                --          Closed          --              --
 3   2.0 --/--                --          Closed          --              --
 4   2.0 --/--                --          Closed          --              --
```

Start step 6 if login users haven't reach upper limit.

- Check whether the device has been configured RSA public key.

The device must be configured local public key as SSH servicer.

If not, please login the device from Console port, use **generate ssh-key** *length* command to create.

Start step 7 if the device has been configured RSA public key.

- Check whether the device has been configured ACL.

Log onto the device from Console port, use **show filter** command to check whether the device is configured ACL. If it is configured ACL, please use **show ip-access-list** or **show access-list-map** command to check whether there is deny client IP address or SSH TCP port protocol rules. If yes, cancel the corresponding rules.

Start step 8 if the device hasn't configured ACL.

- Please collect the following information and contact Raisecom technical support if the above steps cannot solve problems.
  - The executive results of above steps
  - Device configuration files, log information and alarm information

Chapter 5 Interface Troubleshooting

This chapter focuses on introducing the interface fault location methods and processing steps.

- ✧ The Ethernet interface physical layer cannot Up
- ✧ Ethernet interface Up/Down frequently
- ✧ Link aggregation interface cannot forward
- ✧ Troubleshooting cases

5.1 The Ethernet interface physical layer cannot Up

5.1.1 Fault phenomenon

The Ethernet physical interface status remains Down after connecting cable to the device.

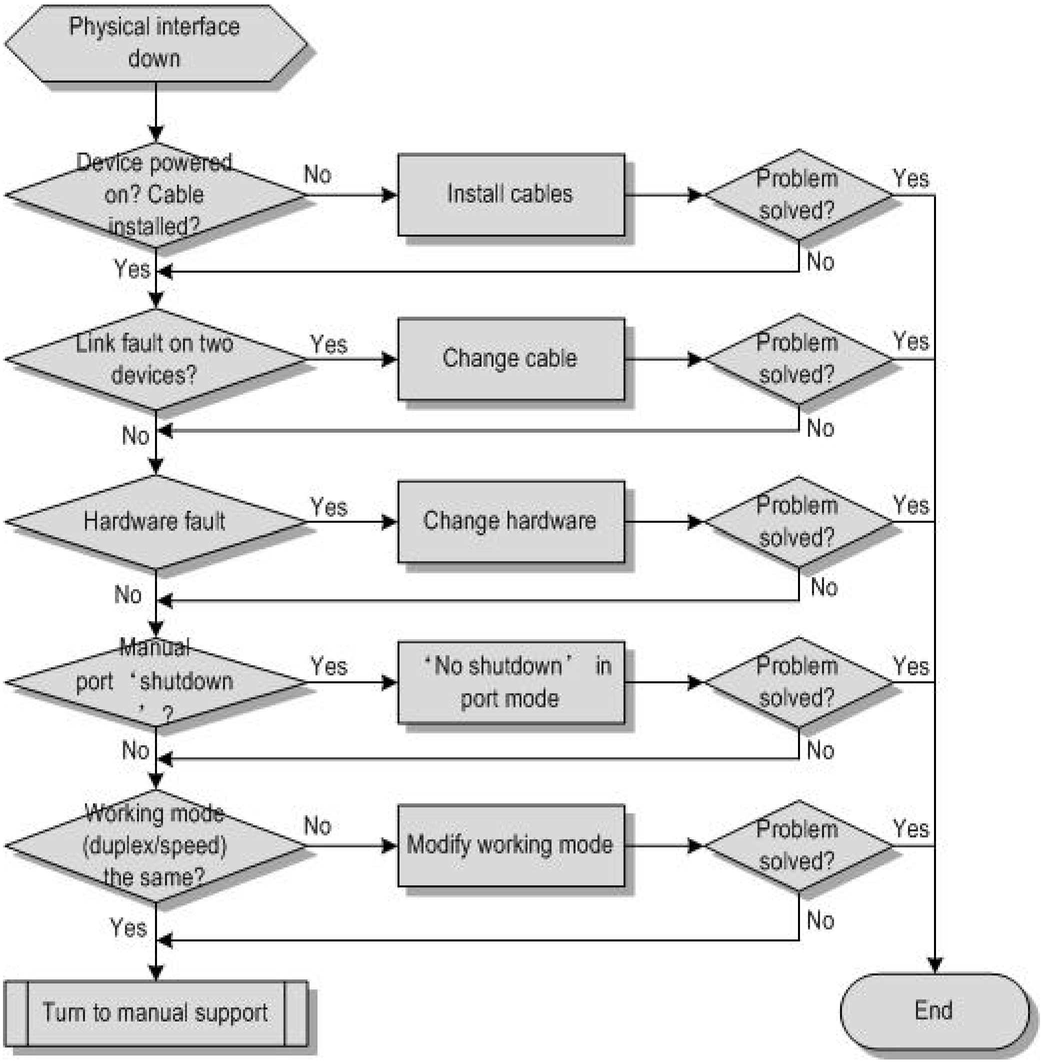
5.1.2 Possible reasons

That Ethernet physical interface layer cannot Up may be caused by the following reasons:

- ➢ The device doesn’t power on or the cable isn’t connected.
- ➢ Twisted pair pin arrangement is wrong, connector type does not match, link is too long or link loss is too much.
- ➢ The interface, interface module or device fault.
- ➢ The interface is set to Shutdown state.
- ➢ The interface duplex or rate negotiation mode is inconsistent.

5.1.3 Fault diagnosis process

Flow chart of fault diagnosis:



Flow chart of fault diagnosis that Ethernet interface Up fault

5.1.4 Troubleshooting processing steps

Note: Please save the executive results of following steps so as to gather and feedback information quickly when failed to solve the problems.

- Check whether the local and opposite devices power on and whether cable and module are connected well.

Start step 2 if the interface state still remains Down after powering and connecting cable to device.

- Check the link on both ends and interface module

Check the following items if the device is connected by twisted pair:

Item	Standard	Follow-up Operation
Test whether twisted pair appear fault with a tester.	The tester shows that twisted pair is normal.	Change cable if cable is teated out fault.

Item	Standard	Follow-up Operation
Check whether the length of twisted pair among devices meet requirement.	The cable length among devices is less than 100m。 10/100/1000M electrical interface uses RJ-45 connector, and interface cable adopts CAT-5/CAT-5+ twisted pair. The transmission distance is 100m.	Do the following operations if the length is more than 100m: • Shorten the distance among devices so as to reduce the length of twisted pair. • The devices can be interconnected with Repeater, HUB or Switch if it is unable to change the distance.
Check whether the pin arrangement type of twisted pair is correct.	Straight through cable can connect router to Ethernet switch or PC to Ethernet switch. Crossover cable can connect routers or router to PC.	Correct the twisted pair type if it is wrong.
Check whether the electrical interface modules on both sides are normal.	The electrical interface modules are normal.	Try to change the electrical interface modules on both sides.

Check the following items if the device is connected by optical fiber:

Item	Standard	Follow-up Operation
Check the corresponding relation between optical module and optical fiber.	Check whether the type of optical fiber is correct. Please see *ISCOM2924GF-4GE/4C Hardware Description*.	Please change optical module or optical fiber accordingly if the corresponding relation is wrong.
Check whether the length of optical fiber matches the transmission distance of optical module.	The length of optical fiber is less than the transmission distance of optical module. Please see *ISCOM2924GF-4GE/4C Hardware Description* for the transmission distance of optical module.	Shorten the length of optical fiber according or change the other optical module with longer transmission distance.
Test signal attenuation with a tester in a reasonable range.	Please see *ISCOM2924GF-4GE/4C Hardware Description* for the optical signal attenuation range.	Please change optical fiber if the attenuation is too large; shorten the length of optical fiber if it still cannot meet the requirement.
Check whether the both ends of optical fiber link are normal with a tester or physical loopback method.	The tester shows normal in receiving and dispatching. The interface state shows Up with physical loopback method.	Please change cable if it appear cable fault; try to change optical interface modules on both ends if it remains fault.

Start step 3 if the interface state still remains Down.

- Check whether the hardware of local and opposite devices is normal.

Try to connect the cable to other interface and start step 4 if it remains fault.

- Check whether the interface state of local and opposite devices is set to Shutdown manually.

Use **show interface port** [*port-id*] command to check whether the interface state is set to Shutdown.

If yes, please execute the **no shutdown** command under physical interface layer configuration mode.

Note: If the device is configured failover function and the checked interface is downstream interface in the failover group, then the Down state upstream interface will make the downstream interface Down, at this time, please remove the Down fault of upstream interface at first.

Start step 5 if the interface state still remains Down.

- Check whether the interface duplex or rate negotiation mode on both ends is consistent.

Use **show interface port** [*port-id]* command on both ends of device respectively to check the interface duplex and rate negotiation mode information.

- Please use **speed** command to adjust the interface to consistent in the physical interface configuration mode if the interface duplex on both ends is inconsistent under non-automatic negotiation mode.
- Please use **duplex** command to adjust the interface to consistent in the physical interface configuration mode if the interface duplex on both ends is inconsistent the non-automatic negotiation mode.

Start step 6 if the interface state still remains Down.

- Please collect the following information and contact Raisecom technical support if the above steps cannot solve problems.
  - The executive results of above steps
  - Device configuration files, log information and alarm information

5.2 Ethernet interface Up/Down frequently

5.2.1 Fault phenomenon

Ethernet interface Up/Down frequently

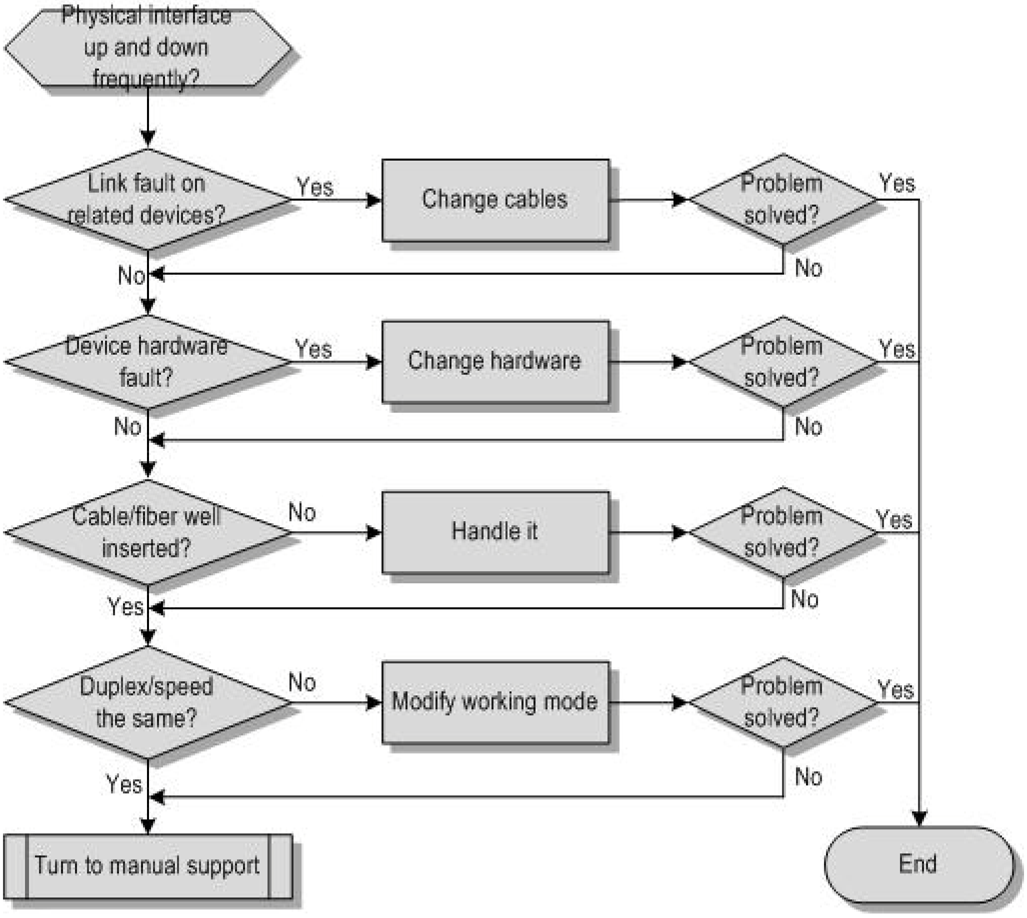
5.2.2 Possible reasons

That Ethernet interface Up/Down frequently may be caused by the following reasons:

- The cable is connected poorly.
- The interface, interface module or device fault.
- Twisted pair or cable is too long, link loss is too much.
- The interface duplex or rate negotiation mode is inconsistent.

5.2.3 Fault diagnosis process

Flow chart of fault diagnosis:



Flow chart of fault diagnosis that Ethernet interface Up/Down frequently

5.2.4 Troubleshooting processing steps

Note: Please save the executive results of following steps so as to gather and feedback information quickly when failed to solve the problems.

- Check whether the cable and module of local and opposite devices are normal.

Start step 2 if the interface state still Up/Down frequently after checking the cable and module.

- Check whether the link on both ends and interface module are normal.

Check the following items if the device is connected by twisted pair:

Item	Standard	Follow-up Operation
Test whether twisted pair appear fault with a tester.	The tester shows that twisted pair is normal.	Change cable if cable is teated out fault.

Item	Standard	Follow-up Operation
Check whether the length of twisted pair among devices meet requirement.	The cable length among devices is less than 100m。 10/100/1000M electrical interface uses RJ-45 connector, and interface cable adopts CAT-5/CAT-5+ twisted pair. The transmission distance is 100m.	Do the following operations if the length is more than 100m: ● Shorten the distance among devices so as to reduce the length of twisted pair. ● The devices can be interconnected with Repeater, HUB or Switch if it is unable to change the distance.
Check whether the electrical interface modules on both sides are normal.	The electrical interface modules are normal.	Try to change the electrical interface modules on both sides.

Check the following items if the device is connected by optical fiber:

Item	Standard	Follow-up Operation
Check the corresponding relation between optical module and optical fiber.	Check whether the type of optical fiber and its corresponding relation with optical module are correct.	Please change optical module or optical fiber accordingly if the corresponding relation is wrong.
Check whether the length of optical fiber matches the transmission distance of optical module.	The length of optical fiber is less than the transmission distance of optical module.	Shorten the length of optical fiber according or change the other optical module with longer transmission distance.
Test signal attenuation with a tester in a reasonable range.	The signal attenuation should happen in an allowable range.	Please change optical fiber if the attenuation is too large; shorten the length of optical fiber if it still cannot meet the requirement.
Check whether the both ends of optical fiber link are normal with a tester or physical loopback method.	The tester shows normal in receiving and dispatching. The interface state shows Up with physical loopback method.	Please change cable if it appear cable fault; try to change optical interface modules on both ends if it remains fault.

Start step 3 if the interface state still Up/Down frequently.

➢ Check whether the hardware of local and opposite devices is normal.

Try to connect the cable to other interface and start step 4 if it remains fault.

➢ Check whether the interface duplex or rate negotiation mode on both ends is consistent.

Start **show interface port** [*port-id]* command on both ends of device respectively to check the interface duplex and rate negotiation mode information.

Try to change interface to non-automatic negotiation mode to force interface duplex or rate consistent if the interface state still Up/Down frequently under non-automatic negotiation mode.

- Please use **speed** command to adjust the interface to consistent in the physical interface configuration mode if the interface duplex on both ends is inconsistent under non-automatic negotiation mode.
- Please use **duplex** command to adjust the interface to consistent in the physical interface configuration mode if the interface duplex on both ends is inconsistent under non-automatic negotiation mode.

Start step 5 if the interface state still remains Up/Down frequently.

- Please collect the following information and contact Raisecom technical support if the above steps cannot solve problems.
  - The executive results of above steps
  - Device configuration files, log information and alarm information

5.3 Link aggregation interface cannot forward

5.3.1 Fault phenomenon

Link aggregation interface cannot forward

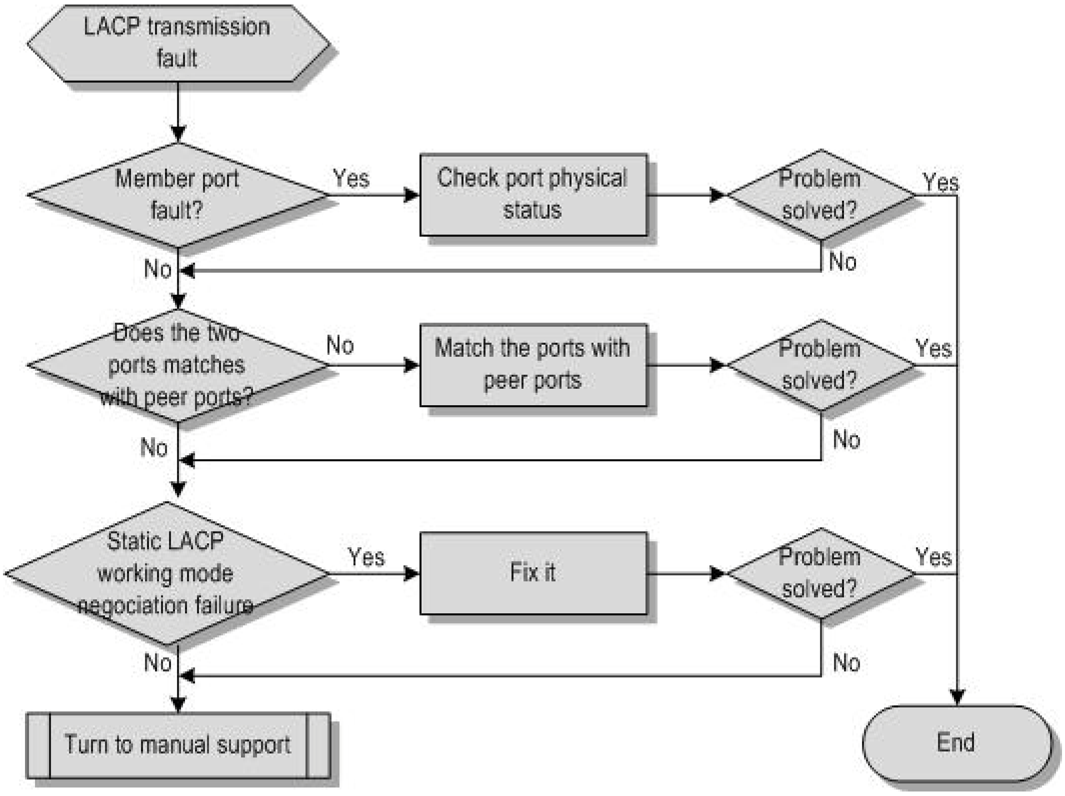
5.3.2 Possible reasons

That link aggregation interface forward fault may be caused by the following reasons:

- Link aggregation member interface fault
- The link aggregation member interface configuration on both ends of device is inconsistent.
- The number of Up member interface is less than the lower limit.
- The link aggregation member interface of static LACP mode is negotiated unsuccessfully.

5.3.3 Fault diagnosis process

Flow chart of fault diagnosis:



Flow chart of fault diagnosis that link aggregation interface cannot forward

5.3.4 Troubleshooting processing steps

Note: Please save the executive results of following steps so as to gather and feedback information quickly when failed to solve the problems.

- Check whether link aggregation member interface is normal.

Execute **show link-aggregation** command to check related link aggregation member interface state.

- If member interface state remains Down, please firstly remove interface Down fault according to Ethernet physical interface layer unable Up localization mentality.
- If member interface state is Up, please make sure both ends each cable have connected to correct corresponding device and interface. Start step 2 if it remains fault.

- Check link aggregation member interface information on both ends of device.

Execute **show link-aggregation** command to check link aggregation member interface information.

- If the number of link aggregation member interface is inconsistent, please add the physical interface to link aggregation group correctly.
- Start step 3 if the number of member interface is consistent.

- Check whether the link aggregation is configured the minimum active links value.

Execute the command of **show link-aggregation** on both ends of device to check the “MinLinks” information.

- If the link aggregation is configured minimum active links value and “MinLinks” is larger than “UpLinks”, please use the command of **link-aggregation group** *group-id* **min-active links** *value* to configure the minimum active links value in global configuration mode.
- Start step 4 if the link aggregation hasn’t configured minimum active links value.

- Check whether link aggregation is in static LACP mode.
  - If link aggregation is configured static LACP mode and member interface is free from selection, then LACP is negotiated unsuccessfully. The reasons are as below:

- Member interface fault makes the LACP protocol message negotiation overtime. Please try to connect cable to other free interface and add the interface to link aggregation group simultaneously.

- The static LACP mode is only configured on one end of device; please configure the link device on both ends correctly.

Start step 5 if LACP still negotiates unsuccessfully after troubleshooting.

- Start step 4 if the link aggregation isn’t configured static LACP mode.

- Please collect the following information and contact Raisecom technical support if the above steps cannot solve problems.
  - The executive results of above steps
  - Device configuration files, log information and alarm information

5.4 Troubleshooting Cases

Part of users cannot visit network normally through link aggregation access mode.

5.4.1 Fault phenomenon

Part of users cannot visit network normally through link aggregation access

5.4.2 Network environment

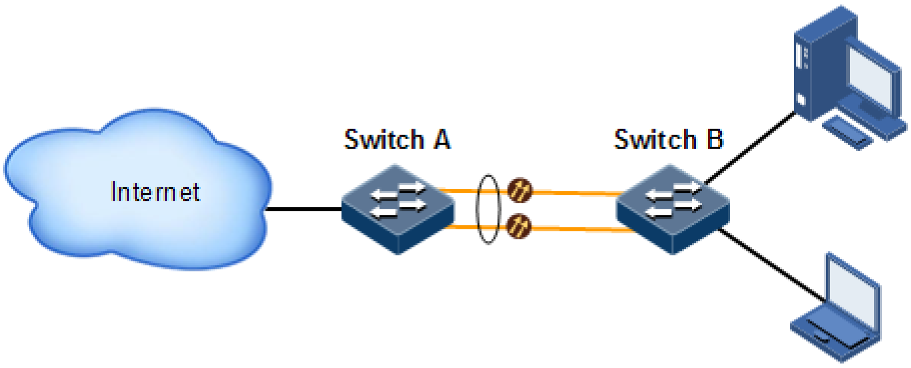


Figure of link aggregation access networking

5.4.3 Fault description

The above figure shows the link aggregation configuration between Switch A and Switch B; users access to network through Switch B. After a period of time, some of them will fail to access the network, and these users are relatively decentralized, but not concentrated in one place.

5.4.4 Fault analysis

- ➢ Check fault users MAC address, which is relatively decentralized and hasn't obvious common characteristics and remove the possibility to limit these users on device.
- ➢ Start **show interface port** [*port-id]* command on Switch A and Switch B and find that the physical interface state of link aggregation member is Up.
- ➢ Start **show interface port** [*port-id]* **statistics** command on Switch A and Switch B and find that the message statistics from one member interface doesn't increase all the way. The middle transmission link fault still fails to transmit data even if the physical interface state shows Up.
- ➢ Start **show link-aggregation** command on Switch A and Switch B and find that the load sharing mode of link aggregation is original MAC address. The member link of link aggregation shares the flow through Hash algorithm. Using original MAC address to transmit interface, the MAC address will be distributed to one fixed link according to constant Hash algorithm. Therefore, users were distributed on the same fault link will fail to visit normally.

5.4.5 Operation steps

The following methods can be used to remove the fault:

- Change the fault link between Switch A and Switch B.
- Use shutdown command to close the fault link so that the link aggregation group makes response to the fault and shift flow to normal link.

⚠Caution: Under global configuration mode, it is impossible to use **link-aggregation load-sharing mode** {smac | **dmac** | **sxordmac** | **sip** | **dip** | **sxordip** | **sportxorsxordmac**} command to solve the problem. The pocket loss problems happen even if users access the network successfully.

5.4.6 Case summary

- Check whether user attribute is regular when users in concentrated physical region cannot connect to the network normally (e.g. Users MAC address is relatively concentrated); if so, please check as below:
  - Check whether the link closed to user is normal.
  - Check whether the device is configured to limit users to visit.
- Check the link aggregation when users in non-concentrated physical region cannot connect to the network normally; if so, please check member interface and see whether the flow hashed to the interface can be transmit normally.
- Give full consideration to the load sharing algorithm features of member link in checking link aggregation fault.
- If the above operations fail to solve the problem, check whether other protocols has influenced the link aggregation, such as home or opposite terminal is configured loopback function.

Chapter 6 Layer-2 Network Troubleshooting

This chapter focuses on introducing the layer-2 network fault location methods and processing steps.

- ✧ The device fails to set correct dynamic MAC address table entry.
- ✧ VLAN users cannot visit each other.
- ✧ The service cannot be connected successfully after configuring QinQ

6.1 The device fails to set correct dynamic MAC address table entry

6.1.1 Fault phenomenon

Layer-2 data cannot forward, device fails to set correct dynamic MAC address table entry.

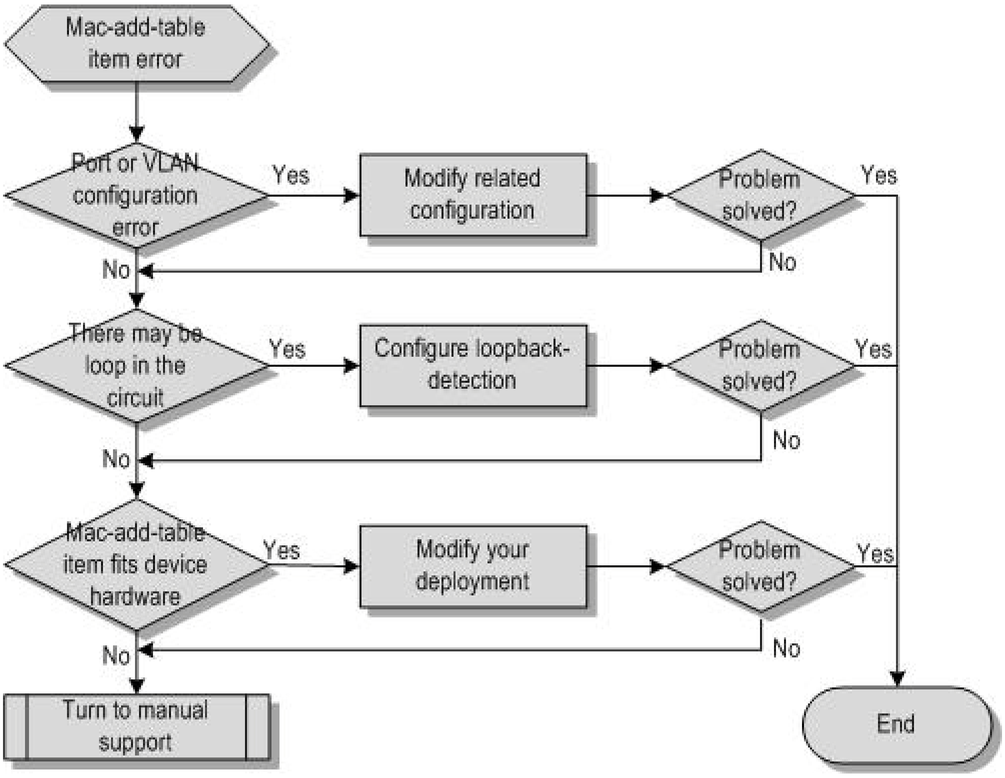
6.1.2 Possible reasons

That the device fails to set correct dynamic MAC address table entry may be caused by the following reasons:

- ➢ Wrong configuration leads to wrong MAC address learning.
- ➢ Network loop makes MAC address refresh constantly.
- ➢ The quantity of MAC address table entry reaches the maximum specification of device.

6.1.3 Fault diagnosis process

Flow chart of fault diagnosis:


Mac-add-table item error
Port or VLAN configuration error
Yes
Modify related configuration
Problem solved?
Yes
No
No
There may be loop in the circuit
Yes
Configure loopback-detection
Problem solved?
Yes
No
No
Mac-add-table item fits device hardware
Yes
Modify your deployment
Problem solved?
Yes
No
No
Turn to manual support
End

Flow chart of fault diagnosis that the device fails to set correct dynamic MAC address table entry

6.1.4 Troubleshooting processing steps

Note: Please save the executive results of following steps so as to gather and feedback information quickly when failed to solve the problems.

- Check whether wrong configuration leads to wrong MAC address learning.

Execute **show mac-address-table l2-address** command to check whether the corresponding relation among MAC address, VLAN and device interface is correct.

  - Bind VLAN and device interface again if there is mistake between them.
  - Start step 2 if the configuration between VLAN and device interface is correct.

- Check whether there is loop network broadcasting storm and dynamic MAC table entry oscillation.
  - The loop can be removed by configuring loop detection function on the related interface, please see *ISCOM2924GF-4GE/4C Configuration Guide* for the detailed configuration information.
  - Start step 3 if there is no loop.
- Check whether the quantity of MAC address table entry reaches the maximum specification of device.

Execute **show mac-address-table l2-address count** command to check whether the quantity of dynamic MAC address learning reaches the maximum specification of device.

  - It is unable to set MAC address table entry continuously if the current quantity of dynamic MAC address learning reaches the maximum specification of device. Then start **show mac-address-table l2-address** command to check MAC address learning list.

- The interface connection network may refresh the MAC address table entry maliciously if MAC address learning quantity far outweighed the real network operation devices' number;

Contact the lower network administrator to solve the problem of network attack.

- The access devices' number outweighed the maximum specification of device if MAC address learning quantity is less than the real network operation devices' number; please adjust network design.

- Start step 4 if the quantity of MAC address learning doesn't reach the maximum specification of device.

➢ Please collect the following information and contact Raisecom technical support if the above steps cannot solve problems.

- The executive results of above steps
- Device configuration files, log information and alarm information

6.2 VLAN users cannot visit each other

6.2.1 Fault phenomenon

VLAN users cannot visit each other

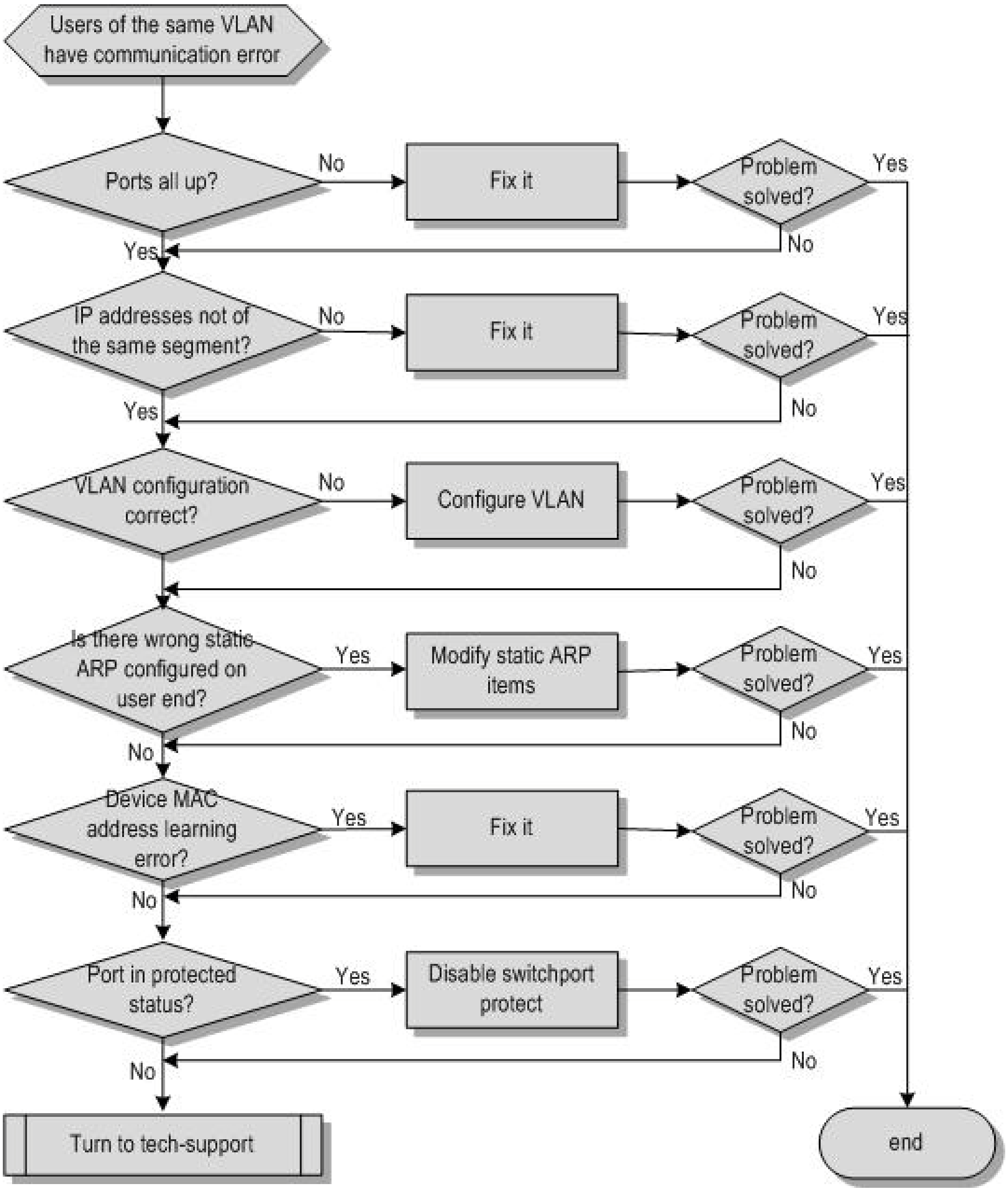
6.2.2 Possible reasons

That VLAN users cannot visit each other may be caused by the following reasons:

➢ The physical interface state remains Down.
➢ User terminal IP address is not in the same subnet.
➢ VLAN configuration error
➢ The host has configured wrong static ARP.
➢ MAC address learning error
➢ The device is configured interface protection.

6.2.3 Fault diagnosis process

Flow chart of fault diagnosis:


Users of the same VLAN have communication error
Ports all up?
No
Fix it
Problem solved?
Yes
No
Yes
IP addresses not of the same segment?
No
Fix it
Problem solved?
Yes
No
Yes
VLAN configuration correct?
No
Configure VLAN
Problem solved?
Yes
No
Is there wrong static ARP configured on user end?
Yes
Modify static ARP items
Problem solved?
Yes
No
No
Device MAC address learning error?
Yes
Fix it
Problem solved?
Yes
No
No
Port in protected status?
Yes
Disable switchport protect
Problem solved?
Yes
No
No
Turn to tech-support
end

Flow chart of fault diagnosis that VLAN users cannot visit each other

6.2.4 Troubleshooting processing steps

Note: Please save the executive results of following steps so as to gather and feedback information quickly when failed to solve the problems.

- Check whether the VLAN intercommunication interface Up.

Execute **show interface port** [*port-id]* command to check the intercommunication interface state.

- If member interface state remains Down, please firstly remove interface Down fault according to Ethernet physical interface layer unable Up localization mentality.
- Start step 2 if member interface state remains Up.

- Check whether user intercommunication terminal IP address is in the same subnet. If not, please shift to the same subnet. Start step 3 if it remains fault.

- Check whether VLAN configuration is correct.

Execute **show vlan** command to check the following information:

Check whether the intercommunication interface VLAN has been created, if not, please start **create vlan** *vlan-id* **active** or **vlan** *vlan-id* command to create VLAN in global configuration mode.

Execute **create vlan** *vlan-id* **active** command in global configuration mode or **state active** command in VLAN configuration mode to activate VLAN if VLAN has been created and remains suspend.

Check whether the intercommunication interface has joined VLAN, if not, please joins the interface to designated VLAN.

The interface contains two types: Access interface and Trunk interface. Access interface is mostly used for user terminal access, while Trunk interface is used for layer-2 device interconnection. The type of interface needs to match the network planning, otherwise, the interface will fail to connect, see *ISCOM2924GF-4GE/4C Configuration Guide* for detailed information.

Note: Check whether intercommunication device interface gives the green light to designated VLAN if intercommunication interface is not in the same device.

Start step 4 if users still cannot visit each other with correct VLAN configuration.

- Check whether the user terminal device is configured wrong static ARP table entry, if yes, please correct it. Start step 5 if it remains fault.
- Check whether MAC address learning table entry is correct.

Execute **show mac-address-table l2-address** command to check whether MAC address learning table entry is correct.

  - Please firstly remove the fault according to device fails to set correct MAC address table entry localization mentality.
  - Start step 6 if MAC address table entry is correct.
- Check whether the device is configured interface protection.

Execute **show switchport protect** command to check whether the device is configured interface protection, if yes, use **no switchport protect** command to cancel interface protection in the corresponding mode.

Start step 7 if the device hasn’t configured interface protection.

- Please collect the following information and contact Raisecom technical support if the above steps cannot solve problems.
  - The executive results of above steps
  - Device configuration files, log information and alarm information

6.3 The service cannot be connected successfully after configuring QinQ

6.3.1 Fault phenomenon

The service cannot be connected successfully after configuring QinQ

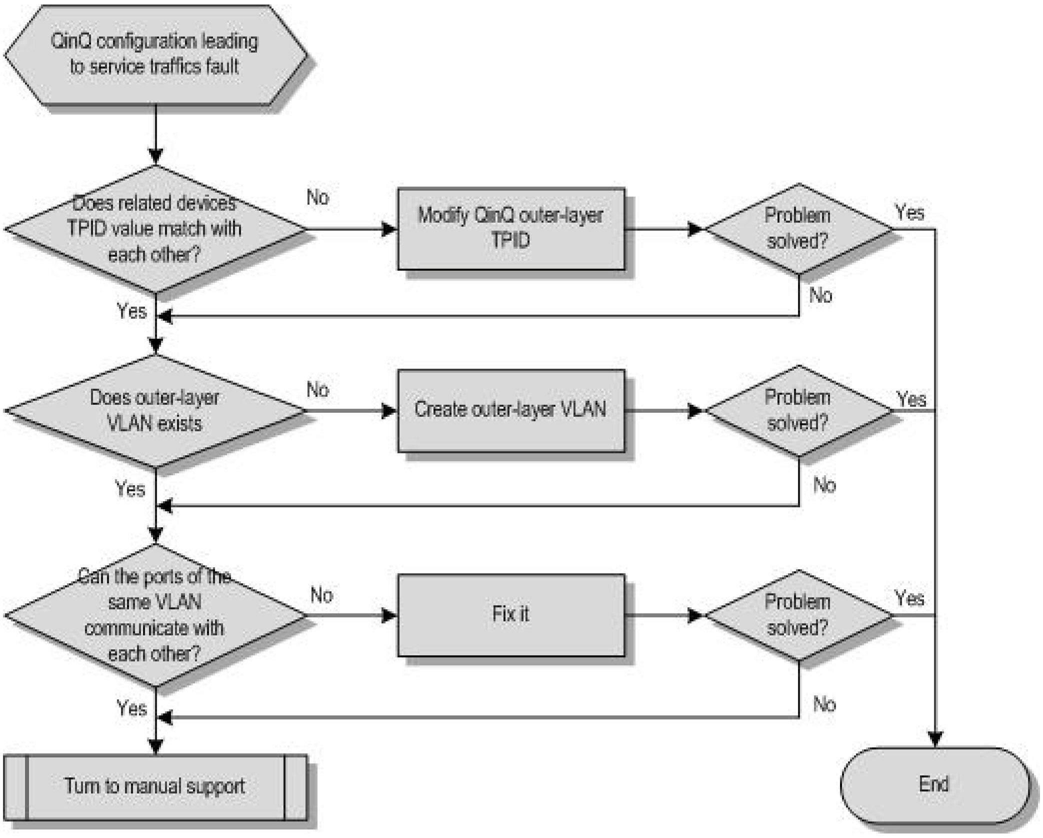
6.3.2 Possible reasons

That the service cannot be connected successfully after configuring QinQ may be caused by the following reasons:

- The outer QinQ TPID value cannot be identified by the other conjoint device.
- The interface cannot join VLAN without creating outer VLAN.
- The device is configured flexible QinQ, but can’t identify it because the reported user VLAN Tag messages are not in the specified range.
- VLAN interface fails to interconnect.

6.3.3 Fault diagnosis process

Flow chart of fault diagnosis:


QinQ configuration leading to service traffics fault
Does related devices TPID value match with each other?
No
Modify QinQ outer-layer TPID
Problem solved?
Yes
No
Yes
Does outer-layer VLAN exists
No
Create outer-layer VLAN
Problem solved?
Yes
No
Yes
Can the ports of the same VLAN communicate with each other?
No
Fix it
Problem solved?
Yes
No
Yes
Turn to manual support
End

Flow chart of fault diagnosis that The service cannot be connected successfully after configuring QinQ

6.3.4 Troubleshooting processing steps

Note: Please save the executive results of following steps so as to gather and feedback information quickly when failed to solve the problems.

- Check whether the outer QinQ TPID value can be identified by the other conjoint device.

Start **show switchport qinq** command to check the outer QinQ TPID value, which is 0x8100 by default.

- If the outer QinQ TPID value of all the devices is different, please use **mls double-tagging tpid** *tpid* command to modify them to the same one in global configuration mode.
- Start step 2 if the outer QinQ TPID value of all the devices is the same.

- Check whether there is outer VLAN.

Start **show vlan** command to check whether there is outer VLAN. If not, the device will fail to add

VLAN Tag to outbound interface message.

If there isn’t VLAN, Please use **create vlan** *vlan-id* { **active** | **suspend** }or **vlan** *vlan-id* command to create VLAN in global configuration mode.

Start step 3 if there is VLAN.

- When deploying flexible QinQ, check whether user side message VLAN Tag is within the added outer VLAN configuration.

Execute the command of **show interface port** *port-id* **vlan-mapping add-outer** to check the user VLAN range needing to add outer VLAN configured on interface and compare with the VLAN Tag with user side message.

  - If user side message VLAN Tag is not within the range, please use the command of **switchport vlan-mapping cvlan** *vlan-list* **add-outer** *vlan-id* to set again in interface configuration mode.
  - Start step 4 if it is within the range.

- Check whether the interface in VLAN can intercommunicate.

Check whether the interface can intercommunicate by means of connecting all interfaces in VLAN to terminal device or to Ping the opposite device.

  - If the interface in VLAN can intercommunicate, please see *the localization mentality that VLAN user cannot visit each other* to solve the problem.
  - Start step 5 if the interface in VLAN can intercommunicate.

- Please collect the following information and contact Raisecom technical support if the above steps cannot solve problems.
  - The executive results of above steps
  - Device configuration files, log information and alarm information

Chapter 7 IP Forward and Route Troubleshooting

This chapter focuses on introducing IP forward and route fault location methods and processing steps.

- Fail to learn opposite ARP table entry
- Ping error
- Traceroute error

7.1 Fail to learn opposite ARP table entry

7.1.1 Fault phenomenon

Connect ISCOM2924GF to opposite device and find that ARP table entry cannot be learnt.

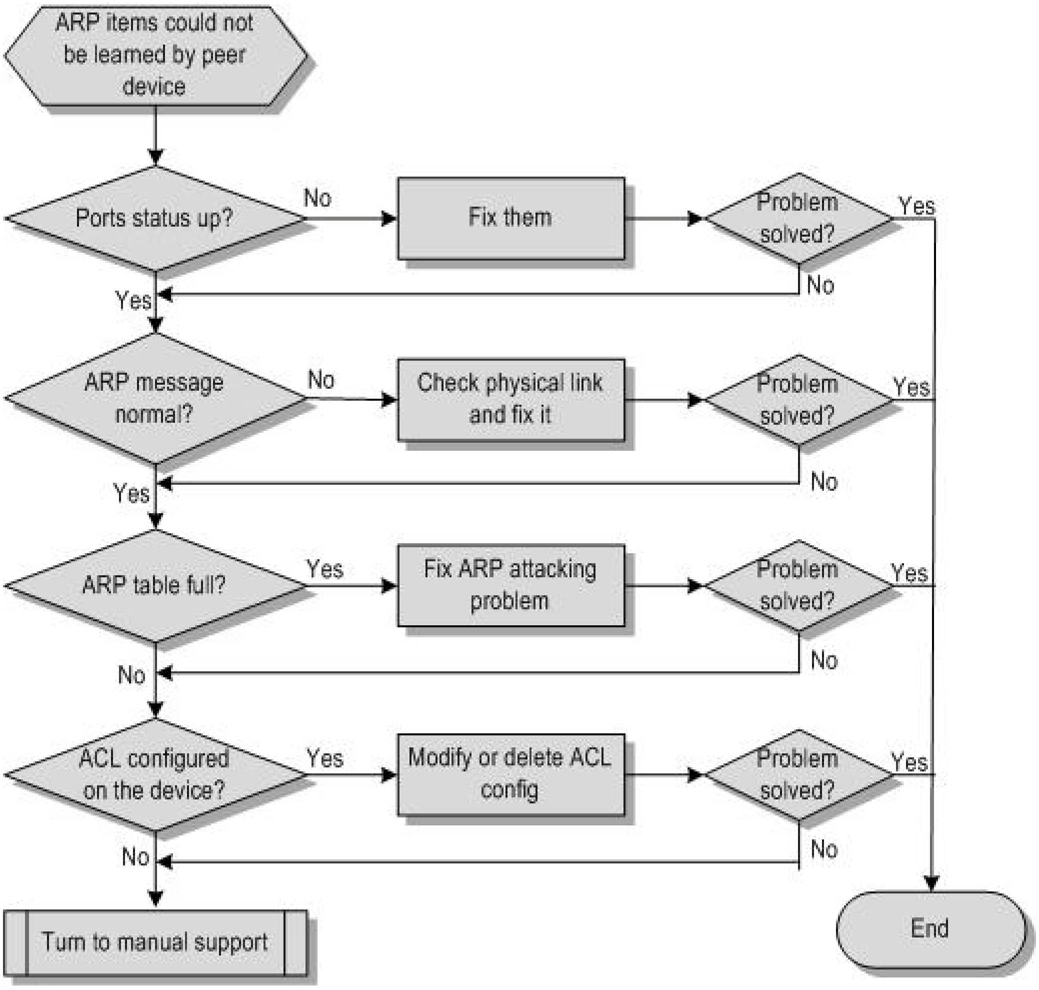
7.1.2 Possible reasons

The opposite ARP table entry learning fault may be caused by the following reasons:

- Physical interface layer cannot Up normally.
- The device is attacked by ARP.
- The link transmission is unstable or optical power is insufficient.
- The device is configured ACL.

7.1.3 Fault diagnosis process

Flow chart of fault diagnosis:



Flow chart of fault diagnosis for opposite ARP table entry learning fault

7.1.4 Troubleshooting processing steps

Note: Please save the executive results of following steps so as to gather and feedback information quickly when failed to solve the problems.

- Start **show interface port** [*port-id]* command to check the physical interface layer state.
  - If it displays as Down, please deal with according to Ethernet physical interface layer unable Up localization mentality.
  - Start step 2 if it displays as Up.
- Check whether ARP message can forward normally.

Login the device from Console port and configure ARP message statistic function on both ends, check whether it is normal for the device to receive and dispatch the ARP request and response. Please Ping IP address of opposite device in local device firstly so as to trigger local device to dispatch ARP request message. Please see *ISCOM2924GF-4GE/4C Configuration Guide* for the detailed configuration of message statistics function.

- Please check the link quality of device if the ARP message is received and dispatched abnormally, for example, whether there is unstable link transmission or insufficient optical power.
- Start step 3 if it is normal.

- Check whether the quantity of ARP mapping table entry reaches the maximum specification.

Execute **show arp** command to check whether the current quantity of ARP table entry reaches the maximum specification.

- ARP table entry may be attacked by ARP or the unused dynamic ARP table entry hasn't been aged if the quantity reaches the maximum specification. At this time, contact network administrator to handle ARP attack or use **arp** *ip-address mac-address* command to configure ARP table entry in global configuration mode so as to add ARP table entry of opposite device to ISCOM2924GF manually.
- Start step 4 if the quantity doesn't reach the maximum specification.

➢ Check whether the device is configured ACL.

Login the device from Console port, use **show filter** command to check whether the device is configured ACL. If it is configured ACL, please use **show ip-access-list** or **show access-list-map** command to check whether there is deny client IP address or telnet TCP port protocol rules. If yes, cancel the corresponding rules.

Start step 5 if the device isn't configured ACL.

➢ Please collect the following information and contact Raisecom technical support if the above steps cannot solve problems.

- The executive results of above steps
- Device configuration files, log information and alarm information

7.2 Ping error

7.2.1 Fault phenomenon

Fail to Ping opposite device

7.2.2 Possible reasons

The Ping error may be caused by the following reasons:

➢ Link fault

➢ Inconsistent IP interface VLAN

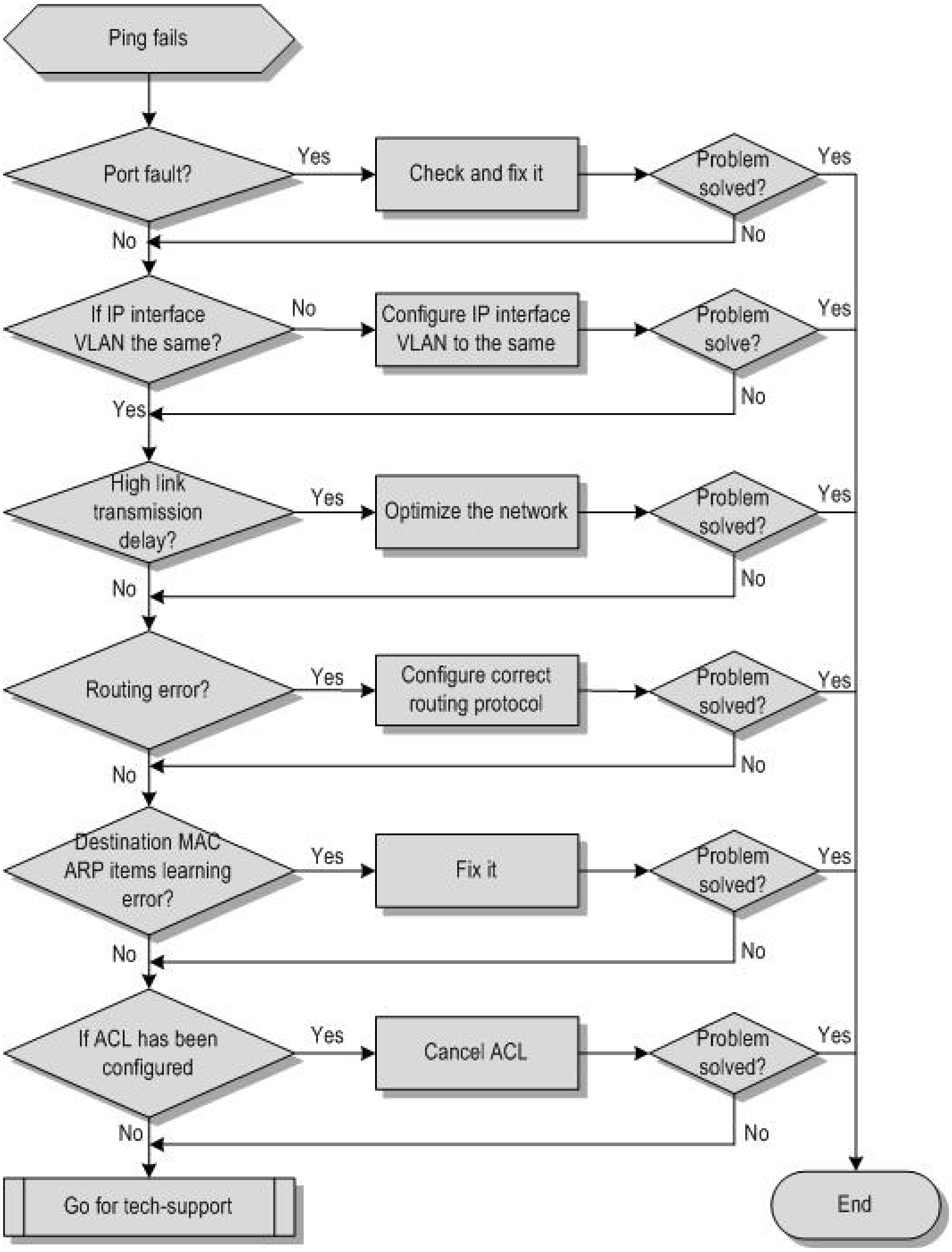
➢ Route fault

➢ ARP table entry learning fault

➢ ACL makes ICMP message be discarded.

7.2.3 Fault diagnosis process

Flow chart of fault diagnosis:



Flow chart of fault diagnosis for Ping error

7.2.4 Troubleshooting processing steps

Note: Please save the executive results of following steps so as to gather and feedback information quickly when failed to solve the problems.

- Execute **show interface port** *port-id* command to check the interface physical layer state.
  - If it displays as Down, please deal with according to Ethernet physical interface layer unable Up localization mentality.
  - Start step 2 if it displays as Up.
- Check whether the Ping IP interfaces on both ends belong to the same VLAN.

Execute **show interface ip** command to check whether the Ping IP interfaces on both ends belong to the same VLAN.

- If the IP interfaces belong to different VLAN, start **ip-address** *ip-address* [*ip-mask*] [*vlan-list*] command to add IP interfaces on both ends to the same VLAN.
- Start step 3 if the IP interfaces on both ends belong to the same VLAN.

➢ Check whether the longer link transmission time leads to Ping error.

The principle of Ping process is that it can Ping as receiving response message in the specific time, otherwise, it will display as Ping impassability. So the reason for Ping error may be loss of packets caused by longer link transmission time.

Execute **ping** *ip-address* **waittime** *value* command to set the idle timeout waiting for message response of opposite device in order to check whether the longer link transmission time leads to Ping error. The Default value is 3s.

- Link forward time is too long if it can Ping after setting **waittime** for the more value (the maximum value is 60s); try to optimize transport network.
- Start step 4 if it still displays as Ping error.

➢ Check the route.

Ignore the route if both sides of Ping are in the same network; otherwise, check the route. (Including routes from client to gateway and from gateway to opposite device)

Execute **show ip route** command to check whether there are unbroken roundtrip routes in the route tables.

- Check whether the route protocol configuration is correct without finding the corresponding route table entry after finishing the above command.
- Start step 5 if the corresponding route table entry information is found.

➢ Check whether the ARP destination address table entry is learnt.

Execute **show arp** *ip-address* command to check whether the ARP destination address table entry is learnt.

- Please firstly remove the fault according to “unable to learn ARP table entry of opposite device” localization mentality if the ARP destination address table entry isn’t learnt.
- Start step 6 if the ARP destination address table entry isn’t learnt.

➢ Check whether the device is configured ACL.

Execute **show filter** command to check whether the device is configured ACL. If it is configured ACL, please use **show ip-access-list** or **show access-list-map** command to check whether there is deny client IP address or ICMP protocol rules. If yes, cancel the corresponding rules.

Start step 7 if the device isn’t configured ACL.

➢ Please collect the following information and contact Raisecom technical support if the above steps cannot solve problems.
- The executive results of above steps
- Device configuration files, log information and alarm information

7.3 Traceroute error

7.3.1 Fault phenomenon

Fail to Traceroute opposite device

7.3.2 Possible reasons

The Traceroute error may be caused by the following reasons:

- The reason is the same as Ping error; please see “Ping error” for detailed information.
- UDP message is limited.

7.3.3 Fault diagnosis process

Ellipsis

7.3.4 Troubleshooting processing steps

Note: Please save the executive results of following steps so as to gather and feedback information quickly when failed to solve the problems.

- Check the same steps as “Ping error”.

See “Ping error” localization mentality for detailed steps.

- Check whether the device is configured ACL rules to prohibit UDP message.

The message sent by Traceroute is UDP message, and the port number is above 30000. Traceroute error also happens when the related devices prohibit the delivery of UDP message.

Start **show filter** command to check whether the device is configured ACL. If it is configured ACL, please use **show ip-access-list** or **show access-list-map** command to check whether there is UDP protocol prohibition rules. If yes, cancel the corresponding rules.

Start step 3 if the device isn’t configured ACL.

- Please collect the following information and contact Raisecom technical support if the above steps cannot solve problems.
  - The executive results of above steps
  - Device configuration files, log information and alarm information

Chapter 8 Service Troubleshooting

This chapter focuses on introducing service fault location methods and processing steps.

- ACL unavailable fault
- Users cannot receive multicast message

8.1 ACL unavailable

8.1.1 Fault phenomenon

ACL configuration cannot filter user flow normally.

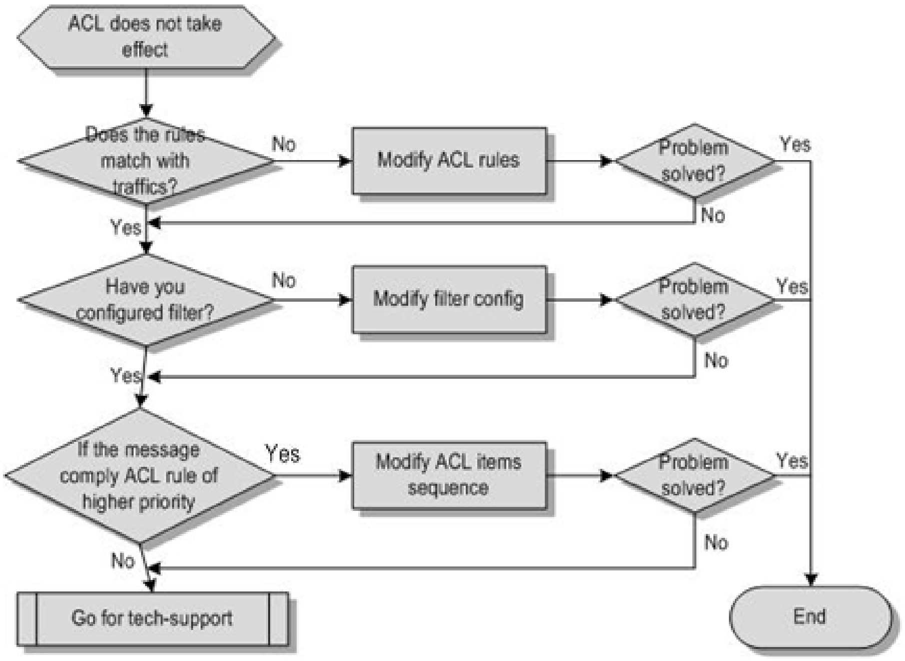
8.1.2 Possible reasons

ACL unavailable fault may be caused by the following reasons:

- The message and user-defined ACL rule are inconsistent.
- Filter application is incorrect. (The application mode fails to meet the service requirement and application orientation is wrong.)
- The message has matched other ACL rules with higher priority.

8.1.3 Fault diagnosis process

Flow chart of fault diagnosis:



Flow chart of fault diagnosis for ACL unavailable fault

8.1.4 Troubleshooting processing steps

Note: Please save the executive results of following steps so as to gather and feedback information quickly when failed to solve the problems.

- Check whether the message and user-defined ACL rule are inconsistent.

Execute **show ip-access-list**, **show ipv6-access-list**, **show mac-access-list** or **show access-list-map** command to check user-defined ACL rule, capture and check message, analyze the message information (IP address, MAC address, DSCP value, VLAN ID, 802.1p value and etc.) and see whether it is matched with user-defined rule.

  - Change user-defined ACL rule to match the message if they are inconsistent, see *ISCOM2924GF-4GE_4C Configuration Guide* for detailed configuration information.
  - Start step 2 if they are matched.
- Check whether ACL is joined to filter correctly.

Join ACL to filter to make ACL available on device. Start **show filter** command to check the filter configuration information and note that whether ACL application mode (based on device, VLAN, interface or the flow from ingress to egress interface) and service requirement is consistent, whether the application orientation is correct (whether **ingress** and **egress** interfaces are configured correctly and whether the flow orientation is correct).

  - If the filter configuration is incorrect, see *ISCOM2924GF-4GE_4C Configuration Guide* to configure filter again according to service requirement.
  - Start step 3 if the filter configuration is correct.
- Check whether the message has matched other ACL rules with higher priority.

The filter can be joined to many ACL matching rules to form many filter rules. The added sequence of ACL matching rules determines the priority in configuring filter, the later, and the higher. Take higher priority rule as the final confirmation if these rules conflict with each other in configuration calculation.

Execute **show filter** [*filter-number-list*] command to check the sequence of filter ACL rules.

  - If the added sequence of ACL matching rules cannot meet service requirement, see *ISCOM2924GF-4GE_4C Configuration Guide* to configure filter again according to service requirement.
  - Start step 4 if the added sequence is correct.
- Please collect the following information and contact Raisecom technical support if the above steps cannot solve problems.
  - The executive results of above steps
  - Device configuration files, log information and alarm information

8.2 Users cannot receive multicast message

8.2.1 Fault phenomenon

Device of the same user VLAN cannot receive multicast message after configuring IGMP Snooping.

8.2.2 Possible reasons

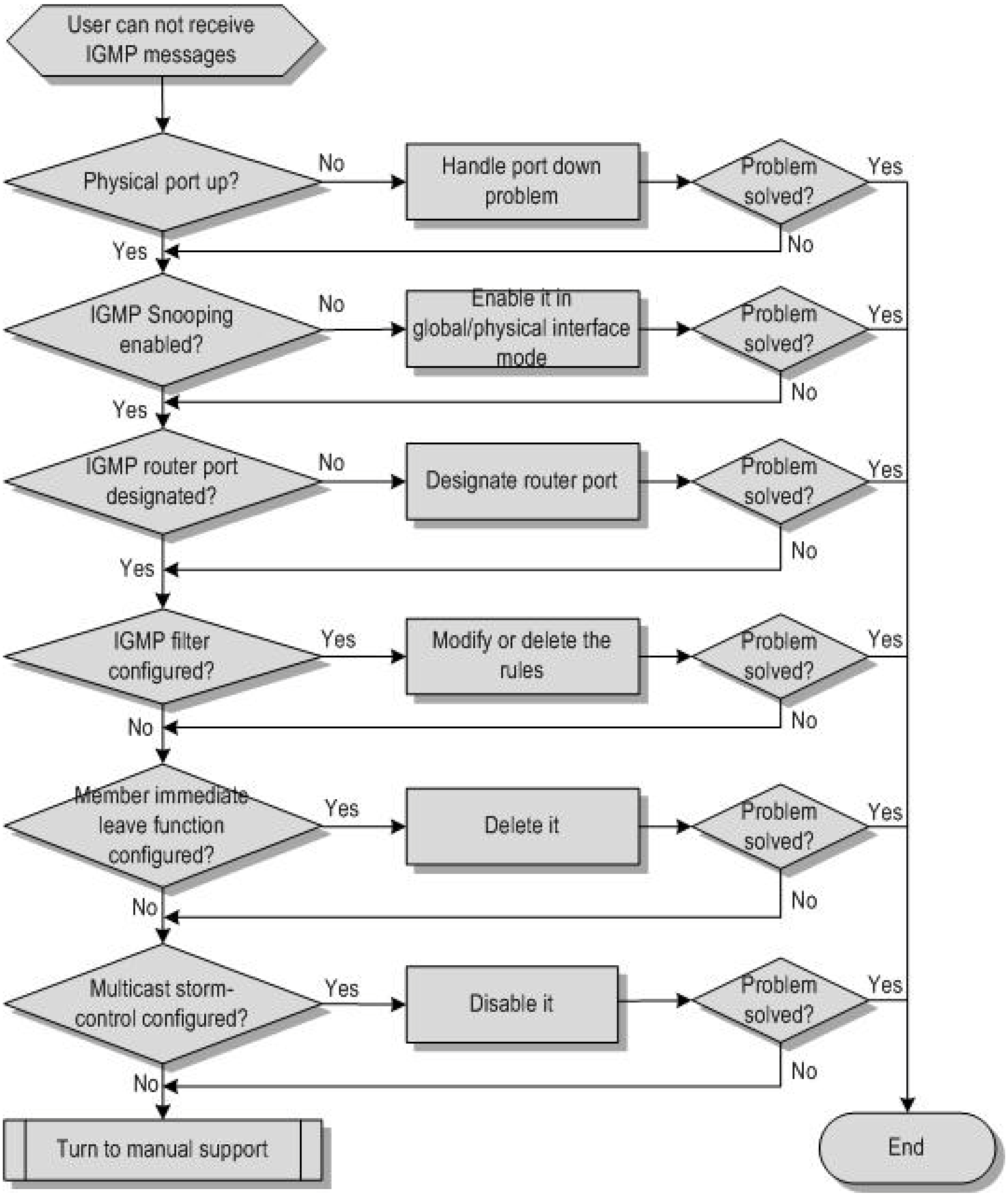
That users cannot receive multicast message may be caused by the following reasons:

- Link fault

- IGMP Snooping disable fault
- Fail to designate multicast router interface
- Configured immediate-leave function
- Configured IGMP filter function
- Configured multicast flow control function

8.2.3 Fault diagnosis process

Flow chart of fault diagnosis:



Flow chart of fault diagnosis that users cannot receive multicast message

8.2.4 Troubleshooting processing steps

Note: Please save the executive results of following steps so as to gather and feedback information quickly when failed to solve the problems.

- Check whether the physical interface state displays as Up.

Execute **show interface port** *port-id* command to check the operating state of upstream and downstream interfaces.

  - If it displays as Down, please remove the fault according to Ethernet interface physical layer unable Up localization mentality.
  - Start step 2 if it displays as Up.

- Check whether IGMP Snooping is enabled in global configuration mode and VLAN configuration mode.

By default, IGMP Snooping is disabled in global configuration mode; by default, all VLAN can enable IGMP Snooping function when IGMP Snooping is globally enabled.

Execute **show ip igmp snooping** command to check IGMP Snooping configuration information.

  - If IGMP Snooping is disabled in global configuration mode or related VLAN configuration mode, please use **ip igmp snooping** command to enable IGMP Snooping.
  - Start step 3 if IGMP Snooping is enabled in global configuration mode or related VLAN configuration mode.

- Check whether the multicast router interface is designated.

ISCOM2924GF can designate multicast router interface automatically (transmit downstream multicast report, leave message and etc.) through IGMP query message only if multicast router protocol is enable on upstream multicast router. The multicast message will not be transmitted normally if the device isn't designated multicast router interface, so it suggests configure the device manually.

Execute the command of **show ip igmp snooping mrouter** to check the multicast router interface configuration.

  - Execute the command of **ip igmp snooping mrouter vlan** *vlan-id* **port** *port-id* in global configuration mode if the device isn't designated multicast router interface.
  - Start step 4 if the multicast router port is designated.

- Check whether the device is configured IGMP filter function.

Execute **show ip igmp filter** command to check whether the device is configured IGMP filter function.

  - If the device is configured IGMP filter function, please use **show ip igmp filter** [*port-id*], **show ip igmp filter vlan** [*vlan-id*] and **show ip igmp profile** [*profile-number*] commands to confirm whether the filter rules are conflicted to user service requirement. If yes, see *ISCOM2924GF-4GE_4C Configuration Guide* to configure filter rules again.
  - Start step 5 if the device isn't configured IGMP filter function or the filter rules are conflicted to user service requirement.

- Check whether the device is configured immediate-leave function for member interface.

The immediate-leave function can be configured when there is only one member device under the interface. If the VLAN is configured immediate-leave function for member interface with more than one receiver device and the device cannot transmit specific query message as receiving IGMP leave message from member interface, please delete the interface forward table entry immediately from the device multicast forwarding table and make multicast flow of other devices unconnected.

Execute **show ip igmp filter vlan** [*vlan-id*] command to check whether the immediate-leave function is enabled under VLAN configuration mode.

  - If yes, please execute **no ip igmp snooping immediate-leave** command in VLAN configuration mode or **no ip igmp snooping vlan** *vlan-list* **immediate-leave** command in global configuration mode to cancel immediate-leave function of member interface.

- Start step 6 if the immediate-leave function is disabled.

➢ Check whether the device is configured multicast flow storm control function.

The multicast flow will be controlled partly if multicast flow storm control function is enabled, which may make partial multicast data forward unsuccessfully.

Execute **show storm-control** command to check whether multicast flow storm control function is enabled.

- If yes, please execute the command of **storm-control multicast disable port-list** *port-list* in global configuration mode to disable this function.
- Start step 7 if multicast flow storm control function is disabled.

➢ Please collect the following information and contact Raisecom technical support if the above steps cannot solve problems.

- The executive results of above steps
- Device configuration files, log information and alarm information

Chapter 9 Common Maintenance Command

Command	**Function**
Raisecom#**show ip-access-list** Raisecom#**show mac-access-list**	Show related access-list configuration information
Raisecom#**show clock**	Show current system time
Raisecom#**show cpu-utilization**	Show CPU utilization
Raisecom#**show hardware**	Show hardware environment information
Raisecom#**show interface port** [*port-id*] **statistics**	Show device interface information
Raisecom#**show process**	Show all tasks states information
Raisecom#**show running-config**	Show current system configuration
Raisecom#**show clock** [**summer-time recurring**]	Show current time, time zone and daylight saving time configuration
Raisecom#**show sntp**	Show SNTP configuration
Raisecom#**show ntp status**	Show NTP configuration
Raisecom#**show ntp associations**	Show NTP connection information
Raisecom#**show startup-config**	Show start-up configuration stored in the system.
Raisecom#**show switchport qinq**	Show interface QinQ basic configuration.
Raisecom#**show version**	Show system version information
Raisecom#**show vlan**	Show VLAN configuration
Raisecom（config）#**clear mac-address-table**	Clear MAC address
Raisecom(config)#**search mac-address**	Search MAC address
Raisecom(config-port)#**spanning-tree clear statistics**	Clear interface spanning-tree statistics
Raisecom(config-port)#**clear loopback-detection statistic**	Clear loopback-detection statistic
Raisecom(config)#**clear relay statistics**	Clear transparent transmission message statistics.
Raisecom(config)#**clear ethernet line-protection statistics**	Clear protection link statistics, including number of transmitting and receiving APS messages, the recent switching time and recent state switching time.
Raisecom(config)#**clear ethernet ring-protection** *ring-id* **statistics**	Clear protection ring statistics

Raisecom(config-port)#**clear oam statistics**	Clear EFM OAM interface link statistics
Raisecom(config)#**clear ethernet cfm errors**	Clear information in CCM error database
Raisecom(config)#**clear ethernet cfm remote-mep**	Clear remote MEP
Raisecom(config)#**clear ethernet cfm traceroute-cache**	Clear traceroute cache database
Raisecom(config)#**clear filter statistics**	Clear filter statistics
Raisecom(config)#**clear service-policy statistics** [**egress** | **ingress** | **port**] *port-list* [**class-map** *class-map-name*]	Clear QoS message statistics
Raisecom(config)#**clear lldp statistic**	Clear LLDP statistics
Raisecom(config)#**clear lldp remote-table**	Clear LLDP neighbor information
Raisecom(config)#**clear rmon**	Clear RMON configuration

Chapter 10 Maintenance Record

10.1 Routine maintenance record

CO Name:

Maintenance time:

Responsible person:

Item	Result	Description
	□Normal □Abnormal	
	□Normal □Abnormal	
	□Normal □Abnormal	
	□Normal □Abnormal	
	□Normal □Abnormal	
	□Normal □Abnormal	
	□Normal □Abnormal	
	□Normal □Abnormal	
	□Normal □Abnormal	
	□Normal □Abnormal	
Remarks: (Problems, Process and Pending task)		
Signature		

10.2 Emergency maintenance record

Complainant		**Telephone**	
Complaint-time		**Response-time**	
CO site		**Address**	
Model		**Version**	

Description
Trouble-shooting
Treatment ☐Phone guidance ☐Remote management ☐Onsite **Process**
Results
Pending task

Troubleshooting time	
Contacts	
Signature	

Appendix A Terms

L	
Connectivity Fault Management（CFM）	A standard defined by IEEE. It defines protocols and practices for OAM (Operations, Administration, and Maintenance) for paths through 802.1 bridges and local area networks (LANs). Used to diagnose fault for EVC (Ethernet Virtual Connection). Cost-effective by fault management function and improve Ethernet maintenance.
Link Aggregation	A computer networking term which describes using multiple networks cables/ports in parallel to increase the link speed beyond the limits of any one single cable or port, and to increase the redundancy for higher availability.
Q	
802.1Q in 802.1Q	QinQ is (also called Stacked VLAN or Double VLAN) extended from 802.1Q, defined by IEEE 802.1ad recommendation. Basic QinQ is a simple layer-2 VPN tunnel technology, encapsulating outer VLAN Tag for client private packets at carrier access end; the packets take double VLAN Tag passing through trunk network (public network). In public network, packets only transmit according to outer VLAN Tag, the private VLAN Tag are transmitted as data in packets.
Y	
Ethernet Ring Protection Switching（ERPS）	An APS (Automatic Protection Switching) protocol based on ITU-T G.8032 Recommendation to provide backup link protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer.
Ethernet Linear Protection Switching（ELPS）	A protocol based on ITU-T G.8031 APS (Automatic Protection Switching) to protect an Ethernet connection. It is a kind of end-to-end protection technology. Including two linear protection modes: linear 1:1 protection switching and linear 1+1 protection switching.

Appendix B Abbreviation

A	
ACL	Access Control List
APS	Automatic Protection Switching
C	
CCM	Continuity Check Message
CFM	Connectivity Fault Management
CoS	Class of Service
D	
DoS	Deny of Service
DRR	Deficit Round Robin
DSCP	Differentiated Services Code Point
E	
EFM	Ethernet in the First Mile
ELPS	Ethernet Linear Protection Switching
ERPS	Ethernet Ring Protection Switching
EVC	Ethernet Virtual Connection
F	
FTP	File Transfer Protocol
G	
GARP	Generic Attribute Registration Protocol
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GVRP	GARP VLAN Registration Protocol
I	
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force

IP	Internet Protocol
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector
L	
LACP	Link Aggregation Control Protocol
LBM	LoopBack Message
LBR	LoopBack Reply
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LTM	LinkTrace Message
LTR	LinkTrace Reply
M	
MA	Maintenance Association
MAC	Medium Access Control
MD	Maintenance Domain
MEG	Maintenance Entity Group
MEP	Maintenance associations End Point
MIB	Management Information Base
MIP	Maintenance association Intermediate Point
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
N	
NNM	Network Node Management
O	
OAM	Operation, Administration and Management
P	
PC	Personal Computer
Q	
QoS	Quality of Service

R	
RADIUS	Remote Authentication Dial In User Service
RMON	Remote Network Monitoring
RMEP	Remote Maintenance association End Point
RNC	Radio Network Controller
RSTP	Rapid Spanning Tree Protocol
S	
SFP	Small Form-factor Pluggables
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SSHv2	Secure Shell v2
STP	Spanning Tree Protocol
T	
TACACS+	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service
V	
VLAN	Virtual Local Area Network
W	
WRR	Weight Round Robin

瑞斯康达科技发展股份有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: Building 2, No. 28 of the Shangdi 6th Street, Haidian District, Beijing. Postcode: 100085 Tel: +86-10-82883305 Fax: +86-10-82883056 Email: export@raisecom.com http://www.raisecom.com