

www.raisecom.com

ISCOM21XXEA-MA Configuration 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.

Copyright ©2011 Raisecom. All rights reserved.

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 ISCOM21XXEA-MA 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 ISCOM21XXEA-MA specification, instead of the web page above, please send comments to:

export@raisecom.com

We hope to hear from you!

CONTENTS

Chapter 1	Product Overview -----	1
Chapter 2	How to Use the Command Line-----	2
2.1	Introductions to commands line -----	2
2.2	Brief configuration -----	2
2.2.1	Commands line mode configuration-----	2
2.2.2	Getting help-----	3
2.2.3	Properties of editing-----	4
2.2.4	Commands history-----	4
2.2.5	The command-line Error -----	5
Chapter 3	System Function Configuration -----	6
3.1	File Management-----	6
3.1.1	Profile Management-----	6
3.1.2	BOOTROM file management-----	6
3.1.3	System File Management-----	7
3.1.4	Backup and update-----	7
3.1.5	Typical application -----	8
3.2	Switch Management-----	9
3.2.1	Console Management-----	9
3.2.2	telnet management-----	10
3.2.3	SSH management-----	11
3.2.4	Cluster rcommand Management-----	13
3.2.5	NMS Management-----	13
3.2.6	User Logging Management-----	14
3.3	Keepalive Function-----	15
3.3.1	The Introduction To Keepalive Principle-----	15
3.3.2	Keepalive Default Configuration-----	15
3.3.3	Keepalive Configuration-----	15
3.3.4	Monitoring And Maintenance-----	16
3.3.5	Typical application -----	16
3.4	Task Scheduling Function-----	17
3.4.1	The Introduction To Task Scheduling Function Principle-----	17
3.4.2	Task Scheduling Configuration-----	17
3.4.3	Monitoring and maintaining-----	17
3.4.4	Typical Configuration-----	17
3.5	Fault Location-----	18
3.5.1	Basic principle -----	18
3.5.2	Memory -----	18
3.5.3	Buffer-----	18
3.5.4	UP/DOWN history-----	18
3.5.5	show tech-support -----	18
3.5.6	syslog in specified packet-----	18
3.5.7	Discard/ Recover specified packet -----	19
3.5.8	Device statistics -----	20
3.6	Ping-----	21
3.6.1	Ping Principle -----	21
3.6.2	Ping Configuration-----	21
3.6.3	Typical application -----	21
3.7	tracerout-----	22
3.7.1	traceroute Principle-----	22
3.7.2	traceroute configuration-----	23
3.7.3	Typical Configuration Example-----	23
3.8	telnet-----	24
3.8.1	telnet Principle -----	24
3.8.2	telnet Default Configuration -----	24
3.8.3	telnet Configuration-----	24
3.8.4	Typical Configuration Example-----	25
3.9	Watchdog-----	25
3.9.1	Watchdog Principle -----	25
3.9.2	Configure Watchdog-----	26
3.9.3	Typical Configuration Example-----	26

3.10 MTU Function	26
3.10.1 MTU Instruction -----	26
3.10.2 MTU Configuration -----	26
3.10.3 Monitoring and maintenance -----	27
3.10.4 Typical Configuration Example-----	27
Chapter 4 CPU Monitoring Configuration Guide -----	28
4.1 Introduce CPU Monitoring-----	28
4.2 CPU monitoring configuration -----	28
4.2.1 Default configuration of CPU monitoring -----	28
4.2.2 Configure CPU monitoring function -----	29
4.2.3 Monitoring and Maintenance -----	29
4.2.4 Typical configuration examples-----	32
Chapter 5 Radius Accounting-----	34
5.1 Overview-----	34
5.2 Default configuration -----	34
5.3 Radius accounting configuration -----	34
5.3.1 Enable/disable Radius accounting function -----	34
5.3.2 Configure Radius accounting server IP address and UDP port number -----	34
5.3.3 Configure the shared key that communicate with the Radius Accounting server-----	35
5.3.4 The strategy of Radius accounting configuration fail-----	35
5.3.5 Configure Radius accounting strategy-----	35
5.4 Monitoring and Maintenance -----	36
5.5 Typical configuration example-----	36
Chapter 6 Mirror Function-----	37
6.1 Local Port Mirror Function Principle-----	37
6.2 Local Port Mirror Function Configuration-----	37
6.2.1 The Default Configuration-----	37
6.2.2 Local Port Mirroring Function configuration -----	38
6.2.3 Monitoring And Maintaining-----	38
6.2.4 Typical Configuration Example-----	39
6.3 Monitoring and Maintaining -----	39
6.4 Typical Configuration Example -----	39
Chapter 7 Port Rate Limiting and Shaping -----	41
7.1 Port rate limiting and shaping principle-----	41
7.2 Line rate and TS based on port-----	42
7.2.1 The default configuration-----	42
7.2.2 Port speed limitation and reshaping function -----	43
7.2.3 Monitoring and maintaining-----	44
7.2.4 Typical configuration example-----	44
7.3 Speed limitation and reshaping function based on VLAN configuration -----	45
7.3.1 The default configuration-----	45
7.3.2 Speed limitation and reshaping function based on VLAN configuration -----	45
7.3.3 Monitoring and maintaining-----	46
7.3.4 Typical configuration example-----	46
Chapter 8 MAC Address Transmission Table Management -----	49
8.1 Brief introduction-----	49
8.1.1 MAC address transmission table-----	49
8.1.2 MAC address learning -----	49
8.1.3 MAC address table management-----	50
8.2 MAC address transmission table management configuration-----	50
8.2.1 The default MAC address transmission table configuration-----	50
8.2.2 Static MAC address configuration -----	51
8.2.3 MAC address aging time configuration -----	51
8.2.4 MAC address learning enable/disable -----	52
8.2.5 Clear MAC address table -----	52
8.2.6 Monitoring and maintaining-----	53
8.2.7 Typical configuration example-----	53
8.3 MAC address number limit -----	54
8.3.1 Configure the default MAC address number limit-----	55
8.3.2 Configure the MAC address number-----	55
8.3.3 Monitoring and maintaining-----	55
8.3.4 Typical configuration example-----	55
Chapter 9 Physical Layer Interface -----	57
9.1 Physical ports features -----	57
9.2 The default values -----	57

9.3	Rate and duplex mode	57
9.4	IEEE 802.3X flow control	59
9.5	Auto-MDIX	62
9.6	mtu	63
9.7	Add description for interfaces	64
9.8	Open and close physical layer port	64
9.9	Clear interface statistics	65
9.10	Dynamic statistics time	66
9.11	Monitoring and maintaining	66
9.12	Typical configuration	67
Chapter 10 Storm Control		70
10.1	Brief introduction	70
10.2	The default configuration	70
10.3	Storm control function configuration	70
10.3.1	Enable/disable storm control function	70
10.3.2	Storm control number	70
10.4	Monitoring and maintaining	71
10.5	Typical configuration example	71
Chapter 11 Layer-two Protocol Relay		72
11.1	Brief principle	72
11.2	Basic configuration	72
11.2.1	Default configuration	72
11.2.2	Relay configuration	73
11.2.3	Layer-two protocol transparent transmission speed limit configuration	74
11.2.4	Layer-two protocol transparent transmission message statistics clear	75
11.2.5	Monitoring and maintaining	75
11.2.6	Typical configuration example	75
Chapter 12 Layer-3 Interface Configuration		77
12.1	Layer-3 interface overview	77
12.2	Layer-3 interface configuration	77
12.3	Layer-3 interface description information configuration	78
12.4	Configuration of layer-3 interface management message COS value	78
12.5	Acquisition of layer-3 interface statistics information	79
12.6	Acquisition of layer-3 interface COS value	79
12.7	Monitoring and maintenance	79
12.8	Typical configuration example	79
12.9	Layer-3 interface configuration trouble shooting	80
Chapter 13 Link Aggregation		81
13.1	Basic principle	81
13.2	LACP aggregation function	81
13.3	Classification	82
13.4	Manual aggregation	82
13.4.1	Default configuration	82
13.4.2	Manual aggregation configuration	82
13.5	Static LACP aggregation function	83
13.5.1	Default configuration	84
13.5.2	Configure static LACP aggregation	84
13.6	Trunk min-active links	85
13.6.1	Default configuration	85
13.6.2	Function configuration	85
13.7	Monitoring and maintenance	85
13.8	Typical configuration example	87
13.8.1	Manual aggregation	87
13.8.2	Static LACP aggregation	89
Chapter 14 STP Configuration Guide		90
14.1	STP/RSTP principle introduction	90
14.1.1	STP purpose	90
14.1.2	STP related protocol and standard	90
14.2	Configure STP	90
14.2.1	Default STP configuration	90
14.2.2	Root configuration	91
14.2.3	Port priority configuration	91
14.2.4	Switch priority configuration	91

14.2.5	Path-cost configuration-----	92
14.2.6	Transmit-limit configuration -----	92
14.2.7	STP timer configuration -----	92
14.3	Configure edge port -----	93
14.3.1	STP mcheck -----	93
14.3.2	STP/MSTP mode -----	94
14.3.3	link-type -----	94
14.3.4	clear statistics -----	95
14.3.5	Monitoring and maintaining -----	95
14.3.6	Typical configuration instance -----	95
14.4	MSTP configuration-----	96
14.4.1	The default MSTP configuration -----	96
14.4.2	Configuration of MSTP region-----	97
14.4.3	The max-hop configuration of MSTP region-----	97
14.4.4	Configuration of root/secondary root -----	98
14.4.5	Configuration of port priority -----	99
14.4.6	Configuration of switch priority -----	99
14.4.7	Configuration of bridge-diameter -----	100
14.4.8	Configuration of path-cost -----	100
14.4.9	Configuration of transit-limit-----	101
14.4.10	Configuration of STP timer-----	102
14.4.11	Configuration of edge port-----	102
14.4.12	Configuration of STP mcheck -----	103
14.4.13	Configuration of STP/MSTP mode -----	104
14.4.14	Configuration of link type -----	104
14.4.15	Configuration of rootguard -----	105
14.4.16	Configuration of loopguard -----	105
14.4.17	Configuration of statistics clear -----	105
14.5	Monitoring and maintenance-----	106
14.6	Typical configuration instance-----	106

Chapter 15 DHCP Configuration ----- 109

15.1	DHCP client configuration-----	109
15.1.1	DHCP client overview -----	109
15.1.2	Configure DHCP Client-----	109
15.1.3	Monitoring and maintenance -----	113
15.1.4	Typical configuration example-----	114
15.1.5	DHCP Client trouble shooting -----	115
15.2	DHCP Snooping configuration-----	115
15.2.1	DHCP Snooping principle -----	116
15.2.2	DHCP Snooping configuration -----	118
15.2.3	Monitoring and maintenance -----	120
15.2.4	Straight-through topology configuration example -----	122
15.2.5	Ethernet loop topology configuration example -----	124
15.2.6	DHCP Snooping trouble shooting -----	127
15.3	DHCP Server Configuration-----	127
15.3.1	DHCP Server principle overview-----	127
15.3.2	DHCP Server configuration -----	128
15.3.3	Monitoring and maintenance -----	138
15.3.4	Typical configuration example-----	140
15.3.5	DHCP Server trouble shooting -----	144
15.4	DHCP Relay Configuration-----	144
15.4.1	DHCP Relay principle overview-----	144
15.4.2	Configure DHCP Relay-----	146
15.4.3	Monitoring and maintenance -----	151
15.4.4	Typical configuration example-----	153
15.4.5	DHCP Relay trouble shooting -----	155
15.5	DHCP OPTION configuration-----	155
15.5.1	DHCP OPTION principle -----	155
15.5.2	DHCP OPTION configuration -----	155
15.5.3	Monitoring and maintenance -----	157
15.5.4	Typical configuration example-----	157

Chapter 16 RMON Function Configuration----- 159

16.1	RMON principle overview-----	159
16.2	RMON configuration-----	159
16.2.1	Default configuration -----	159
16.2.2	RMOB statistics group configuration -----	159
16.2.3	RMON history statistics group configuration-----	160
16.2.4	RMON alarm group configuration -----	161

16.2.5	RMON event group configuration -----	161
16.3	Monitoring and maintenance -----	162
16.4	Typical configuration example -----	162
16.4.1	Network demand-----	162
16.4.2	Network picture -----	163
16.4.3	Configuration Steps -----	163
Chapter 17	ARP Management Configuration -----	164
17.1	ARP principle overview -----	164
17.2	ARP configuration-----	164
17.2.1	ARP default configuration -----	165
17.2.2	Add static ARP address table entry -----	165
17.2.3	Set the timeout of ARP dynamic address mapping table entry -----	165
17.2.4	Set ARP dynamic learning mode -----	166
17.2.5	Empty ARP address mapping table -----	166
17.3	Monitoring and maintenance -----	167
17.4	Typical configuration example -----	167
17.4.1	Network demand-----	167
17.4.2	Configuration steps -----	167
Chapter 18	SNMP Function Configuration -----	168
18.1	SNMP principle overview -----	168
18.1.1	SNMP overview -----	168
18.1.2	SNMP V1/V2 overview -----	168
18.1.3	SNMPv3 interview -----	169
18.2	SNMPv1/v2/v3 management configuration -----	169
18.2.1	Default SNMP configuration -----	169
18.2.2	SNMPv1/v2 configuration -----	170
18.2.3	SNMPv3 configuration -----	171
18.2.4	SNMP v1/v2 TRAP configuration -----	173
18.2.5	SNMPv3 Trap configuration-----	173
18.2.6	Other SNMP configuration -----	174
18.3	Monitoring and maintenance -----	175
18.4	Typical configuration example -----	175
Chapter 19	Time Management Function Configuration -----	179
19.1	Time management overview -----	179
19.2	Time configuration function -----	179
19.2.1	Default time function configuration -----	179
19.2.2	Time setting function configuration-----	179
19.2.3	Timezone management function configuration-----	180
19.2.4	Summer time function configuration -----	180
19.2.5	Monitoring and maintenance -----	181
19.2.6	Typical configuration example -----	181
19.3	SNTP function configuration -----	182
19.3.1	SNTP protocol default configuration -----	182
19.3.2	SNTP protocol function configuration-----	182
19.3.3	Monitoring and maintenance -----	182
19.3.4	Typical configuration example -----	183
19.4	NTP configuration -----	183
19.4.1	NTP principle overview-----	183
19.4.2	NTP configuration -----	185
19.4.3	Monitoring and maintenance -----	187
19.4.4	Typical configuration example -----	188
19.4.5	NTP trouble shooting -----	190
Chapter 20	Loopback Detection Configuration Guide -----	191
20.1	Loopback detection introduction -----	191
20.2	Loopback detection default configuration -----	191
20.3	Loopback detection function configuration -----	191
20.3.1	Open or close port loopback detection function -----	191
20.3.2	Configure destination MAC address and VLAN Function -----	192
20.3.3	Configure cycle loopback detection function -----	192
20.3.4	Configure loop detection automatically release the blocked port time -----	192
20.3.5	Configure other receiving device loop detection the message approach -----	193
20.3.6	Manually open the port blocked-----	193
20.3.7	Clear loop detection statistics -----	194
20.4	Monitoring and maintenance -----	194
20.5	Typical configuration examples -----	194
Chapter 21	VLAN Configuration -----	197

21.1 VLAN Principle overview-----	197
21.2 Switch VLAN Function Configuration -----	197
21.2.1 VLAN based on port -----	198
Chapter 22 QinQ Configuration -----	204
22.1 QinQ principle overview-----	204
22.1.1 Basic QinQ -----	204
22.1.2 Flexible QinQ -----	204
22.1.3 VLAN conversion -----	205
22.2 Basic QinQ configuration-----	206
22.2.1 Default configuration-----	206
22.2.2 Basic QinQ function configuration-----	206
22.2.3 Monitoring and maintenance -----	206
22.2.4 Typical configuration example-----	206
22.3 Configure flexible QinQ -----	209
22.3.1 Configure flexible QinQ function-----	209
22.3.2 Monitoring and maintenance -----	209
22.3.3 Typical configuration -----	210
22.4 Configure VLAN conversion -----	212
22.4.1 Configure VLAN conversion function-----	212
22.4.2 Monitoring and maintenance -----	214
22.4.3 Typical configuration example-----	214
Chapter 23 Multicast -----	221
23.1 Multicast Overview-----	221
23.1.1 The confusion of unicast/broadcast-----	221
23.1.2 Information transmission in unicast -----	221
23.1.3 Transmitting information in broadcasting-----	222
23.1.4 Information transmission in multicast-----	222
23.1.5 The advantage of multicast is:-----	223
23.2 IGMP Snooping Configuration-----	223
23.2.1 About IGMP Snooping protocol-----	223
23.2.2 IGMP snooping configuration-----	224
23.2.3 Monitoring and maintenance -----	229
23.2.4 Typical configuration example-----	230
23.2.5 IGMP snooping trouble shooting-----	230
23.3 MVR Configuration-----	231
23.3.1 MVR principle-----	231
23.3.2 IGMP filtration introduction-----	232
23.3.3 MVR configuration-----	232
23.3.4 MVR monitoring and maintaining-----	235
23.3.5 IGMP filter configuration-----	236
23.3.6 IGMP filter monitoring and maintenance-----	239
23.3.7 Typical configuration example-----	240
23.3.8 MVR and IGMP filter trouble shooting-----	242
Chapter 24 ACL Function Configuration-----	243
24.1 Configuration Description-----	243
24.2 ACL Introduction-----	243
24.3 IP ACL Configuration-----	243
24.3.1 IP ACL Default Configuration-----	243
24.3.2 IP ACL Configuration-----	243
24.3.3 Monitoring and Maintenance -----	244
24.3.4 Specific Configuration Example-----	244
24.4 MAC ACL Function-----	245
24.4.1 MAC ACL Default Configuration-----	245
24.4.2 Monitoring and Maintenance -----	246
24.4.3 Specific Configuration Examples-----	246
24.5 MAP ACL Function-----	246
24.5.1 MAP ACL Default Configuration-----	247
24.5.2 MAP ACL Configuration-----	247
24.5.3 Monitoring and Maintenance -----	253
24.5.4 Specific Configuration Example-----	253
24.6 Application Configuration Based on Hardware ACL-----	253
24.6.1 Application Default Configuration Based on Hardware ACL-----	254
24.6.2 Monitoring and Maintenance -----	256
24.6.3 Specific Configuration Examples-----	256
24.7 Configuration Function Based on Software IP ACL-----	257
24.7.1 Layer-3 Interface Protect Configuration Based on IP ACL-----	257
24.7.2 Monitoring and Maintenance -----	258

24.7.3	Specific Configuration Example-----	258
Chapter 25 QoS Configuration -----	259	
25.1 Configuration Description-----	259	
25.2 QoS Introduction-----	259	
25.2.1	Introduction-----	259
25.2.2	Classification-----	261
25.2.3	Policy and Marking -----	263
25.2.4	Bit-Rate Limitation and Reshaping-----	263
25.2.5	Mapping Table -----	264
25.2.6	Queueing and Scheduling-----	264
25.2.7	QoS Default Configuration -----	265
25.3 QoS Enable and Disable -----	266	
25.3.1	QoS Start and Stop Default Configuration-----	266
25.3.2	QoS Start and Close Default Configuration-----	266
25.3.3	Monitoring and Maintenance -----	266
25.3.4	Configuration Examples -----	266
25.4 Classification Function Configuration -----	267	
25.4.1	Classification Default Configuration-----	267
25.4.2	Flow Classification Configuration Based on Port TRUST Status-----	267
25.4.3	Configuring Flow Classification on ACL/class-map-----	270
25.4.4	Monitoring and Maintenance -----	273
25.4.5	Typical Configuration Examples -----	274
25.5 Policy and Marking Function Configuration -----	275	
25.5.1	Policy and Marking Default Configuration-----	275
25.5.2	Policy and Marking Configuration -----	275
25.5.3	Monitoring and Maintenance -----	280
25.5.4	Specific Configuration Examples:-----	282
25.6 Bit-Rate Limitation and Reshaping Function Configuration -----	283	
25.6.1	Configuration Based on Bit-Rate and Reshaping of Data Flow-----	283
25.6.2	Monitoring and Maintenance -----	284
25.6.3	Specific Configuration Examples -----	284
25.7 Map Function Configuration -----	285	
25.7.1	Map Default Configuration -----	285
25.7.2	CoS-localpriority map List Configuration -----	285
25.7.3	DHCP-localpriorityMap List Configuration -----	286
25.7.4	tos-localpriority List Configuration -----	288
25.7.5	Set Ports Based on smac, dmac, vlan's Frame Priority and Priority Override Function-----	289
25.7.6	Monitoring and Maintenance -----	290
25.8 Queue and Adjust Function Mode -----	291	
25.8.1	Queue and Adjust Default Configuration-----	291
25.8.2	SP Configuration-----	291
25.8.3	WRR Configuration -----	292
25.8.4	DRR Configuration -----	292
25.8.5	WFQ Configuration-----	292
25.8.6	Monitoring and Maintenance -----	293
25.8.7	Specific Configuration Examples -----	293
25.9 QoS Trouble Shoot-----	294	
25.10 QoS Command Reference-----	294	
Chapter 26 Dynamic ARP Inspection Configuration-----	296	
26.1 Dynamic ARP inspection principle overview-----	296	
26.2 Configure Dynamic ARP Inspection-----	297	
26.2.1	Default Dynamic ARP Inspection configuration-----	297
26.2.2	Global Dynamic ARP Inspection configuration-----	297
26.2.3	DAI Protection VLAN Configuration-----	298
26.2.4	Configure port ARP trust-----	299
26.2.5	Configure static Dynamic ARP Inspection-----	299
26.2.6	ARP Packets Rate-limit Default Configuration-----	300
26.2.7	ARP Packets Rate-limit Port Configuration-----	300
26.2.8	ARP Packets rate-limit global configuration-----	301
26.3 Monitoring and maintenance-----	302	
26.4 Typical configuration example-----	303	
Chapter 27 IP Source Guard Configuration-----	305	
27.1 IP Source Guard principle overview-----	305	
27.2 Configure IP Source Guard-----	305	
27.2.1	Default IP Source Guard configuration-----	305
27.2.2	Enable/disable global stable binding function-----	305
27.2.3	Enable/disable global dynamic binding function-----	306

27.2.4	Configure port credit state-----	306
27.2.5	Configure stable binding relationship-----	307
27.2.6	Transfer dynamic binding relationship to static binding-----	307
27.2.7	Enable/disable auto-update to static binding-----	308
27.3	Monitoring and maintenance -----	308
27.4	Typical configuration example -----	309
27.5	IP Source Guard command list -----	310
Chapter 28	Unicast Router Configuration Guide -----	311
28.1	Routing Overview-----	311
28.1.1	Overview-----	311
28.2	Static Routing Configuration -----	312
28.2.1	Static routing overview-----	312
28.2.2	Configure static routing-----	312
28.3	Monitoring and maintenance -----	313
Chapter 29	802.3ah OAM Function Configuration-----	315
29.1	802.3ah OAM Principle Introduction -----	315
29.1.1	OAM mode and discovery-----	315
29.1.2	OAM loop-back-----	315
29.1.3	OAM events-----	315
29.1.4	OAM mib-----	316
29.2	802.3ah OAM Mode Configuration -----	316
29.3	802.3ah OAM Active Mode Function -----	317
29.3.1	OAM default configuration-----	317
29.3.2	OAM enable/disable configuration function-----	317
29.3.3	Run OAM loop-back function-----	318
29.3.4	Opposite OAM event alarm function-----	320
29.3.5	View opposite IEEE 802.3 Clause 30 mib-----	320
29.3.6	OAM statistics clear function-----	321
29.3.7	Monitoring and maintenance-----	321
29.3.8	Configuration example -----	322
29.4	802.3ah OAM Passive Function -----	323
29.4.1	OAM default configuration-----	323
29.4.2	OAM enable/disable configuration -----	323
29.4.3	Response/ignore opposite OAM loop-back configuration function-----	325
29.4.4	OAM link monitor configuration function-----	325
29.4.5	OAM fault indication function-----	327
29.4.6	Local OAM event alarm function-----	327
29.4.7	IEEE 802.3 Clause 30 mib support-----	328
29.4.8	OAM statistics clear function-----	329
29.4.9	Monitoring and maintenance-----	330
29.4.10	Configuration example -----	330
Chapter 30	Extended OAM Configuration-----	332
30.1	Extended OAM principle overview-----	332
30.2	Extended OAM management -----	332
30.2.1	Default extended OAM configuration-----	332
30.2.2	Extended OAM configuration mode-----	333
30.2.3	Remote equipment system configuration-----	333
30.2.4	Configure extended OAM protocol-----	334
30.2.5	Configure remote equipment port-----	335
30.2.6	Upload/download files from remote equipment-----	338
30.2.7	Configure remote equipment to network management enabled equipment-----	342
30.2.8	Save remote equipment configuration information to local end-----	344
30.2.9	Reset remote equipment-----	345
30.2.10	Extended OAM statistic clear function-----	345
30.2.11	Monitoring and maintenance-----	346
30.2.12	Typical configuration example-----	346
Chapter 31	Optical Module Digital Diagnoses -----	348
31.1	Optical Module Digital diagnoses principle -----	348
31.2	Optical module digital diagnostic configuration-----	349
31.2.1	Optical module digital diagnostic default configuration-----	349
31.2.2	Optical module digital diagnostic able/disable configuration-----	349
31.2.3	Optical module parameter abnormal alarm configuration-----	350
31.2.4	Optical module digital diagnostic parameters monitoring and maintenance-----	350
Chapter 32	802.1x Configuration -----	351
32.1	802.1x principle overview-----	351
32.2	Configure 802.1x-----	352

32.2.1	Default 802.1x configuration -----	352
32.2.2	Basic 802.1x configuration -----	352
32.2.3	802.1x reauthorization configuration-----	354
32.2.4	Configure 802.1x timer -----	354
32.2.5	802.1x statistics cleanup-----	356
32.2.6	Maintenance -----	356
32.2.7	Configuration example -----	356
Chapter 33	Auto-update Configuration-----	359
33.1	Principle of auto-update function -----	359
33.2	Default Auto-update configuration -----	360
33.3	Auto configuration and load function configuration -----	360
33.3.1	Enable auto-update -----	360
33.3.2	Configure TFTP server address -----	361
33.3.3	Configure file name rule -----	361
33.3.4	Configure the filename -----	364
33.3.5	Configure the switch of covering local configuration-----	365
33.3.6	Set auto-update TRAP switch -----	365
33.3.7	Set Auto-update file version-----	366
33.4	Monitoring and maintenance -----	366
33.5	Typical configuration example-----	367
33.5.1	Destination -----	367
33.5.2	The topology structure -----	367
33.5.3	The configuration steps on Cisco 3750:-----	367
33.5.4	Configure PC1-----	369
33.5.5	Configure PC2-----	369
33.5.6	Devices Auto-update Finish-----	369
33.5.7	Auto-update erratum-----	370
Chapter 34	Function Configuration of Ethernet Ring-----	371
34.1	Overview-----	371
34.2	Default configuration list of Ethernet ring-----	372
34.3	Function configuration of Ethernet ring-----	372
34.3.1	Create and delete ring-----	372
34.3.2	Configure ring switch-----	373
34.3.3	Configure sending interval of Hello message-----	373
34.3.4	Configure fault-delay-----	373
34.3.5	Configure bridge priority information-----	373
34.3.6	Configuration ring description information-----	374
34.3.7	Configure ring port aging time-----	374
34.3.8	Configure ring protocol vlan-----	374
34.3.9	Clear ring port static-----	374
34.3.10	Configure upstream-group-----	375
34.4	Monitoring and maintenance -----	375
34.4.1	Ethernet ring information monitoring-----	375
34.4.2	Ethernet ring port information monitoring-----	376
34.5	Typical configuration illustration-----	377
34.5.1	Ethernet ring typical application-----	377
34.5.2	Configuration illustration of single ring -----	378
34.5.3	Tangent dual ring networking application-----	384
34.5.4	Non-Raisecom Upstream Device-----	385
34.5.5	Typical application of looped network dual-link protection-----	386
34.5.6	Typical application of dual homing topology-----	389
Chapter 35	Failover Configuration-----	391
35.1	Overview of failover -----	391
35.2	Failover configuration -----	392
35.3	Monitoring and maintenance -----	392
35.4	Typical configuration illustration-----	393
35.4.1	Failover group application based on port-----	393
35.4.2	Failover group application based on MEP fault-----	395
Chapter 36	TACACS+ Configuration-----	397
36.1	TACACS+ Theory -----	397
36.2	TACACS+ Function Configuration-----	397
36.2.1	TACACS+ Function Default Configuration-----	397
36.2.2	TACACS+ function configuration-----	398
36.2.3	Monitoring and Maintenance -----	398
36.2.4	Typical Configuration Illustration-----	398
Chapter 37	GVRP Configuration Guide-----	400

37.1 GVRP overview	400
37.1.1 Brief introduction of GARP	400
37.1.2 Brief introduction of GVRP	403
37.1.3 Protocol specification	403
37.2 Configuration of GVRP	403
37.2.1 Default configuration	403
37.2.2 Configuration guide	404
37.2.3 Configure GVRP	404
37.3 Monitoring and Maintenance	406
37.4 Typical configuration illustration	406
37.4.1 Networking demand	406
37.4.2 Figure of networking	407
37.4.3 Configuration steps	407
Chapter 38 PPPoE Configuration Guide	410
38.1 Function principle of PPPoE+	410
38.2 Function default configuration of PPPoE+	410
38.3 Function configuration of PPPoE+	410
38.3.1 Enable or disable PPPoE+ function	410
38.3.2 Configure function of trusted port	411
38.3.3 Configure add/modify message information of PPPoE+	411
38.3.4 Clear statistics	414
38.4 Monitoring and maintenance	414
38.5 Typical configuration illustration	414
Chapter 39 CFM Configuration	416
39.1 CFM Introduction	416
39.1.1 CFM Modules	416
39.1.2 CFM Basic Function	417
39.2 CFM Default Configuration List	418
39.3 CFM Configuration Constraint and Limitation	418
39.4 CFM Configuration List and Specification	419
39.4.1 Configure CFM Maintenance Domain MD	419
39.4.2 Configure Service Instance MA	420
39.4.3 Configure MIP	421
39.4.4 Configure MEP	421
39.4.5 Configure CC Protocol Switch	423
39.4.6 Configure Sending Interval of CCM Message	423
39.4.7 Configure Archive Time of Error CCM Message in MEP CCM Database	424
39.4.8 Launch Loopback Protocol	425
39.4.9 Launch Linktrace Protocol	426
39.4.10 Configure Linktrace Database Switch Status	427
39.4.11 Configure Linktrace Database Archive Time	428
39.4.12 Configure Linktrace Database to Store Data Entries	428
39.4.13 Fault Indication	429
39.4.14 Configure Enable/Disable CFM Protocol in Global Mode	430
39.4.15 Configure Enable/Disable CFM Protocol in Port Mode	430
39.5 Monitoring and Maintenance	431
39.5.1 Display Route Trace Information Studied in LinkTrace Database	431
39.5.2 Display local MP Configuration Information, include MEP and MIP	432
39.5.3 Display Error CCM Database Information	432
39.5.4 Display Indicated Maintenance Domain Configuration Information	433
39.5.5 Display Remote MEP Information	433
39.5.6 Display Particular Information of Remote MEP	433
39.5.7 Display CFM Protocol Configuration	434
39.5.8 Clear Error CCM Database Indicated Information	434
39.5.9 Clear Archive Route Trace Information in Linktrace Database	435
39.5.10 Clear Indicated Remote MEP Information	435
39.6 Typical Configuration Illustration	435
Chapter 40 Y.1731 Configuration	440
40.1 Functional overview of Y.1731	440
40.1.1 Components of Y.1731	440
40.1.2 Basic function of Y.1731	441
40.2 Default configuration list of Y.1731	442
40.3 CFM configuration constraints and limitations	443
40.4 CFM configuration list and instruction	444
40.4.1 Configure overall functional switch of Y.1731	444
40.4.2 Configure ports functional switch of Y.1731	445

40.4.3	Configure maintenance domain-----	446
40.4.4	Configure service instance-----	447
40.4.5	Configure VLAN mapping in service instance-----	447
40.4.6	Configure MEP -----	449
40.4.7	Configure a static remote MEP -----	451
40.4.8	Configure CCM transmitting switch -----	452
40.4.9	Configure CCM transmitting interval-----	452
40.4.10	Configure CCM transmitting mode -----	453
40.4.11	Configure dynamic import function for remote learning-----	454
40.4.12	Configure cc check function of remote MEP-----	454
40.4.13	Configure aging time for remote MEP-----	455
40.4.14	Configure client VLAN for Y.1731 OAM message-----	455
40.4.15	Configure priority for Y.1731 OAM message-----	456
40.4.16	Configure hold time for error CCM batabase-----	457
40.4.17	Configure CFM fault alarm level -----	458
40.4.18	Execute layer-2 ping operation (fault reset)-----	459
40.4.19	Execute layer-2 traceroute operation (fault isolation)-----	460
40.4.20	Configure switch status for LT database-----	462
40.4.21	Configure data holding time in LT database-----	462
40.4.22	Configure data entries can be stored in database LT-----	463
40.5	Monitoring and maintenance -----	464
40.5.1	Show LT database traceroute information-----	464
40.5.2	Show local MEP configuration information-----	465
40.5.3	Show discovery information of remote MEP-----	465
40.5.4	Show error CCM database information-----	466
40.5.5	Show configuration information of maintenance domain and service instance-----	466
40.5.6	Show information of static remote MEP-----	466
40.5.7	Show global configuration information of Y.1731-----	467
40.5.8	Show the measurement results of previous RFC2544 throughput-----	467
40.5.9	Clear information of database LT-----	467
40.5.10	Clear information of remote MEP database-----	468
40.6	Typical configuration -----	468
40.7	Appendix -----	474
Chapter 41	SLA Configuration-----	475
41.1	SLA overview -----	475
41.1.1	SLA modules-----	475
41.1.2	Basic function of SLA-----	475
41.2	SLA default configuration list -----	476
41.3	SLA configuration guide and limit -----	476
41.4	SLA configuration list and instruction -----	477
41.4.1	Configure SLA y1731-echo -----	477
41.4.2	Configure SLA y1731-jitter -----	477
41.4.3	Configure SLA icmp-echo -----	478
41.4.4	Configure SLA icmp-jitter -----	479
41.4.5	Configure SLA schedule information and enable schedule-----	479
41.5	Monitoring and maintenance -----	480
41.5.1	Show configuration information related to operation-----	480
41.5.2	Show the latest test information of operation-----	481
41.5.3	Show statistic information of operation schedule-----	482
41.6	Typical configuration applications -----	485
Chapter 42	LLDP Configuration-----	490
42.1	Overview of LLDP -----	490
42.2	LLDP default configuration list -----	491
42.3	Configuration constraints and limitations of LLDP-----	491
42.4	Configuration list and item-by-item description of LLDP-----	491
42.4.1	Configure the LLDP global enable -----	491
42.4.2	Configure LLDP port enable -----	492
42.4.3	Configure LLDP sending delay timer -----	494
42.4.4	Configure LLDP aging coefficient-----	495
42.4.5	Configure cycle transmission timer of LLDP-----	495
42.4.6	Configure the LLDP alarm notification delay timer-----	496
42.4.7	Configure LLDP alarm enable-----	497
42.5	Monitoring and maintenance -----	498
42.5.1	Clear statistics of LLDP -----	499
42.5.2	clear neighbor information of LLDP -----	500
42.5.3	Show local configuration information -----	501
42.5.4	Show local system and port information-----	502

42.5.5	show neighbor information -----	503
42.5.6	Show statistics of system and ports -----	504
42.6	typical configuration illustration -----	506
Chapter 43	Port Backup Configuration Guide -----	509
43.1	Overview-----	509
43.1.1	Switch port backup -----	509
43.1.2	port backup based on VLAN-----	510
43.2	Configure port backup-----	510
43.2.1	Default configuration -----	510
43.2.2	Configuration guide -----	510
43.2.3	Configure port backup-----	511
43.3	Monitoring and maintenance -----	513
43.4	Typical configuration illustration-----	514
43.4.1	Networking requirement -----	514
43.4.2	Networking structure -----	514
43.4.3	configuration steps -----	515

Release Notes

Date of Release	Manual Version	Software Version	Revisions	Translator
20110905	201106		First release	Dorothy, Lily, Karen, Lucas

Preface

About This Manual

This manual introduces primary functions of the configuration management software for Raisecom ISCOM21xxEA-MA 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 ISCOM21xxEA-MA series device, this is also a recommended document.

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 Product Overview

The Switch can be managed through the Switch's serial port, Telnet, or the Web-based management agent. The Command Line Interface (CLI) can be used to configure and manage the Switch via the serial port or Telnet interfaces. This manual provides a reference for all of the commands contained in the CLI. Configuration and management of the Switch via the Web-based management agent is discussed in the Manual. Configuration and management of the Switch via the Web-based management agent is discussed in the User's Guide.

Accessing the Switch via the Serial Port

The Switch's serial port's default settings are as follows:

- 9600 baud
- no parity
- 8 data bits
- 1 stop bit

ISCOM21XXEA-MA series have three kinds: ISCOM2110EA-MA, ISCOM2126EA-MA, and ISCOM2128EA-MA. ISCOM2110EA-MA has 8 100MBASE-T ports and 2 COMBO 100/1000MSFP ports. ISCOM2126EA-MA has 24 100MBASE-T ports and 2 COMBO 100/1000MSFP ports. ISCOM2128EA-MA has 24 100MBASE-T ports and 4 COMBO 100/1000MSFP ports. All of them have the same User and password raisecom.

Chapter 2 How to Use the Command Line

2.1 Introductions to commands line

Commands Line is the channel for the communication between subscribers and switches. In the commands lines, subscribers is able to monitor, control and manage the switches through configuring the corresponding commands. For better convenience, subscribers can edit shortcuts to use the commands, by the same time subscribers can examine the used commands through transferring the history. The commands line mode confines the way different subscribers use commands lines, where various commands line modes are offered. Subscribers can make certain configuration only in the corresponding mode.

2.2 Brief configuration

2.2.1 Commands line mode configuration

Mode	Description	Access	Prompt	Exit
User EXEC mode	Subscriber is allowed to configure the basic information and the parameter shown on the switch.	Login the switch and enter the user's name and password.	Raisecom>	Exit Withdraw from the current mode.
Privileged EXEC mode	Subscriber is allowed to configure the basic information of the switch, like system time and the name of the switch, except the operation information.	From universal subscriber mode, type enable and password.	Raisecom#	Exit Withdraw from the current mode.
Global configuration mode	Subscriber is allowed to configure all the operation parameters.	From subscriber privilege mode, type config	Raisecom(config)#	Exit Withdraw from the current mode.
Physical interface configuration	Subscriber is allowed to configure the Ethernet physical interface of the switch.	From global configuration mode, type interface port portid .	Raisecom(config-port)#	Exit Withdraw from the current mode.
Physical interface bulk configuration	Subscriber is allowed to range configure the parameter of the switch's Ethernet physical interface.	From global mode, type interface port portid .	Raisecom(config-range)#	Exit Withdraw from the current mode.
Layer-3 interface configuration	Subscriber is allowed to configure the switch's three-tier Ethernet interface.	From global mode, type interface port ip id .	Raisecom(config-ip)#	Exit Withdraw from the current mode.

VLAN configuration	Subscriber is allowed to configure the VLAN operation parameters.	Enter vlan	Raisecom(config-vlan)#	Exit Withdraw from the current mode.
Class Map configuration	Subscriber is allowed to configure the given data flow.	From global configuration mode, type class-map class-map-name [match-all match-any] command.	Raisecom(config-cmap)#	Exit Withdraw from the current mode.
Policy Map configuration	Subscriber is allowed to classify and package the data flow defined by class-map.	From global configuration mode, type policy-map policy-map-name command.	Raisecom(config-pmap)#	Exit Withdraw from the current mode.
Traffic classification configuration	Subscriber is allowed to configure the action of the date flow.	From policy map exec mode, type class-map class-name command.	Raisecom(config-pmap-c)#	Exit Withdraw from the current mode.
The cluster configuration mode	Subscriber is allowed to configure the cluster.	From global configuration mode, type cluster command.	Raisecom(config-cluster)#	Exit Withdraw from the current mode.
ACL mapping table configuration	Subscriber is allowed to configure the access control list mapping table.	From global configuration mode, type access-list-map <0-399> {permit / deny} command.	Raisecom(config-aclmap)#	Exit Withdraw from the current mode.
Subscriber network mode	Subscriber is allowed to configure three-tier network setting, show the users' network information and network tools.	Form global configuration mode, type user-network diagnostics.	Raisecom(config-usenet)#	Exit Withdraw from the current mode.
RIP configuration mode	Subscriber is allowed to configure RIP.	Forom global configuration mode, type router rip.	Raisecom(config-router-rip) #	Exit Withdraw from the current mode.
OSPF configuration mode	Subscriber is allowed to configure OSPF.	From global configurationiom mode, type router ospf.	Raisecom(config-router-ospf) #	Exit Withdraw from the current mode.

2.2.2 Getting help

Command	Function Description
help	Obtaining a brief description (in Chinese or English) from the help system.

abbreviated-command-entry?	Obtaining a list of commands that begin with a specified string (abbreviated-command-entry): Example: Raiscom> en? enable <i>enable</i>
abbreviated-command-entry<Tab>	Supplementing an unfinished command line. Example: Raiscom # show ser<TAB> Raiscom # show sersion
?	List all commands of the current mode. Example: Raiscom #?
command?	List all keywords and optional items for a specified command line and give brief help information of the command line. Example: Raiscom # show?
command keyword ?	List related commands: Raiscom(config)# ip? ip <i>IP setting</i> ip-access-list <i>Define IP access control list</i>

2.2.3 Properties of editing

- <**up arrow**>: the command last entered
- <**down arrow**>: the command entered next
- <**left arrow**>: move left by a character
- <**right arrow**>: move right by a character
- <**Backspace**>: delete the character before the cursor
- <**CTRL+d**>: delete the character after the cursor
- <**CTRL+a**>: move the cursor to the head of the row
- <**CTRL+e**>: move the cursor to the tail of the row
- <**CTRL+k**>: delete all the characters after the cursor
- <**CTRL+x**>: delete all the characters left to the cursor
- <**CTRL+z**>: quit the current unprivileged user mode and enter Privileged EXEC mode.

2.2.4 Commands history

By default, 20 historical commands will be temporarily saved in the buffer of the system. Users can

set up the number of historical commands to be saved under User EXEC mode:

Raisecom# **terminal history <0-20>**

Users can also user the command **history** to display all historical commands.

2.2.5 The command-line Error

Error	Description	Getting help
Unknown command or inaccurate For example Raisecom# sh co %" co " Unknown command.	Review the command needed.	
The command is not confirmed: For example Raisecom# sh r %" r " Unconfirmed command	Input the order that can not be recognized by the switch from the commands.	Add ? for annotation and command. For example: Raisecom# sh r rate-limit: Rate control rmon: RemoteNetwork Monitoring (RMON) configuration rndp:RNDP configuration rtdp:RTDP configuration running-config: Running system configuration information
Command incomplete For example Raisecom# show %" show " Incomplete command.	The switch can not recognize the operation form the command, command that can be recognized is needed.	Add ? for command and annotation. For example: Raisecom# sh r rate-limit: Rate control rmon: RemoteNetwork Monitoring (RMON) configuration rndp:RNDP configuration rtdp:RTDP configuration running-config: Running system configuration information

Chapter 3 System Function Configuration

3.1 File Management

3.1.1 Profile Management

The default configuration storage file name of the system is: **startup_config.conf**. The configuration storage file could be written into the flash file system through the command **write**, and the configuration information will be re-configured automatically the next time. By the command of **erase** to delete the file. The configuration information file **startup_config.conf** could be uploaded to the server or downloaded to the system to replace the original configuration information, through FTP protocol with the command **upload** and **download**. Use **show startup-config** to show the configuration information in storage. Use **show running-config** to show the current configuration information in the system.

Command	Description
write	Write the configuration file into the flash file system, and the configuration information in storage will be re-configured automatically after the system rebooting
erase	Delete the file
show startup-config	Show the configured information in storage
show running-config	The configuration information in the current system

3.1.2 BOOTROM file management

BOOTROM, boot of the switch, initialize the switch. User can upgrade BootROM file through FTP. BootROM file system is called **bootrom** (or **bootromfull**) in default cases. With the command **ftp file-name**, user can set these file system names.

When powered, the switch will run **BootROM** file first. When ‘Press space into Bootrom menu...’ is shown, user can enter **Bootrom** menu bar by pressing ENTER, and carry out the following operation:

- ‘?’ show all the commands available
- ‘h’ show all the commands available
- ‘v’ show the version of **Bootrom**
- ‘b’ quick start executive command
- ‘T’ download configuration file through the switch ports
- ‘N’ set the MAC address
- ‘R’ reboot the switch

3.1.3 System File Management

The documents that keep the equipment running, like host software and configuration files, are kept in the storage devices. For the convenience and efficiency of user's managing the equipment, the equipment manages the documents in the way of Document System. The function of the document system contains catalog's creating and deleting, document's copying and display, and so on.

In default cases, the document system will remind user for confirmation if the command may lose any data (like deleting or recovering files).

- With the command **upload** and **download**, program files could be uploaded to the server or downloaded to the system through the TFTP protocol or FTP protocol;
- Use **dir** to look over the system FLASH files;
- Use **show version** to look over the software version;
- Use **clock** to set system time;
- Use **logout** to exit the current system.

Command	Description
dir	To look over the system files
show version	To look over the software version
clock	To set system time
logout	Exit the system

3.1.4 Backup and update

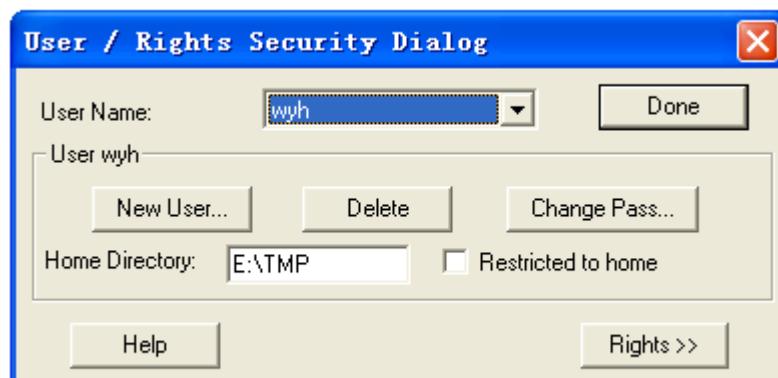
ISCOM switches may use upload command for backup and download command for update.

Command	Description
Upload {system-boot startup-configure remote-fpga } ftp A.B.C.D username password filename	Files are uploaded to server through FTP protocol A.B.C.D:IP destination address <i>username</i> : server user name <i>password</i> : user's password <i>filename</i> : filename(o.0)
download {system-boot startup-configure bootstrap remote-fpga} ftp A.B.C.D username password filename	By FTP protocol the files are downloaded to the system and replace the files before. A.B.C.D:IP destination address <i>username</i> : server user name <i>password</i> : user's password <i>filename</i> : filename(o.0)
upload {system-boot startup-configure remote-fpga } tftp A.B.C.D filename	Files are uploaded to server through FTP protocol A.B.C.D: IP destination address <i>filename</i> : filename
download {system-boot startup-configure remote-fpga } tftp A.B.C.D filename	Files are uploaded to server through FTP protocol A.B.C.D: IP destination address

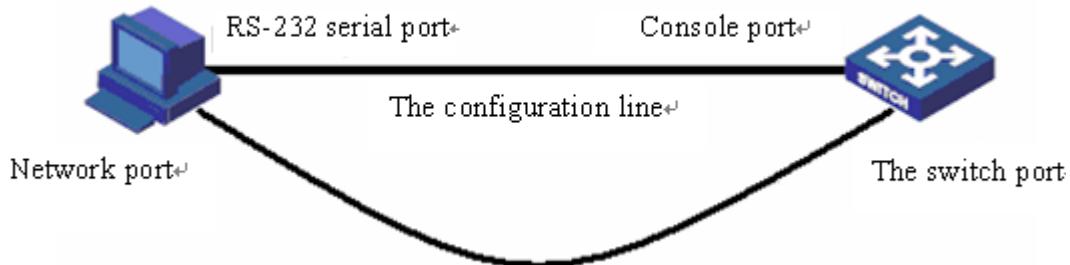
filename: filename

3.1.5 Typical application

When subscribers have configuration files or new upgrade files, he/she can download the configuration files into the switch. To make it, subscriber should open the FTP software, like wftpd32.exe, and set user name, password and file path. As shown below, user name is wyj, password for 123, the path of the configuration file is E:\TMP.



User uses serial line to connect the switch and PC, and connect the line to the switch port, as shown below. Open the terminal emulation program, such as **SecureCRT 5.1**. Take Console management as reference when using Console interface.



User can also use **upload**, **download** to upload and download files from FTP. The connection line is shown as figure.

For example:

Using FTP to download system file **ROS_4.3.313.ISCOM2128EA-MA.31.20080602** to the switch, user should set the switch IP address: 20.0.0.10 first, then open the FTP software **wftpd32.exe** and set user name, password, and file path. Input **download** and select **system-boot**, input the host IP address: 20.0.0.10, user name, password of the FTP software, and all the process is done.

Raisecom#config

Raisecom(config)#interface ip 0

Raisecom(config-ip)#ip address 20.0.0.10 1

Set successfully

```
Raisecom(config-ip)#exit
RaiseCom(config)#exit
RaiseCom#download      system-boot      ftp      20.0.0.221      wyh      123
ROS_4.3.313.ISCOM2128EA-MA.31.20080602

Waiting....Start
Getting from source ...Done
Writing to destination...Size 1754K / 1754K
Success!

When the files in switch need to be uploaded to the host, user can use TFTP to upload startup-config to the host. To do this, user should set the IP address 20.0.0.10 of the switch, then open the TFTP software Cisco TFTP Server to set the file path, input upload, host IP address 20.0.0.221, and upload the generated file name WW.

RaiseCom#config
RaiseCom(config)#interface ip 0
RaiseCom(config-ip)#ip address 20.0.0.10 1
Set successfully
RaiseCom(config-ip)#exit
RaiseCom(config)#exit
RaiseCom#upload startup-config tftp 20.0.0.221 ww

Waiting....Start
Getting from source ...Done
Writing to destination...Size 1K / 1K
Success!
```

3.2 Switch Management

3.2.1 Console Management

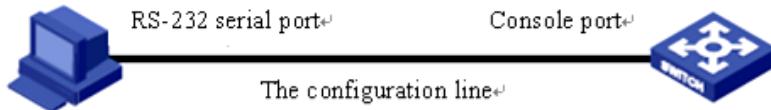
Local control port management means using a console port of a terminal or a PC that is running terminal simulation program to configure and manage the switch. This management approach is out-of-band management, and needs no network for communication. Thus the console port can configure and manage the switch even if the network is not going on well.

Local management manages the switch by connecting the terminal and console program inside the switch.

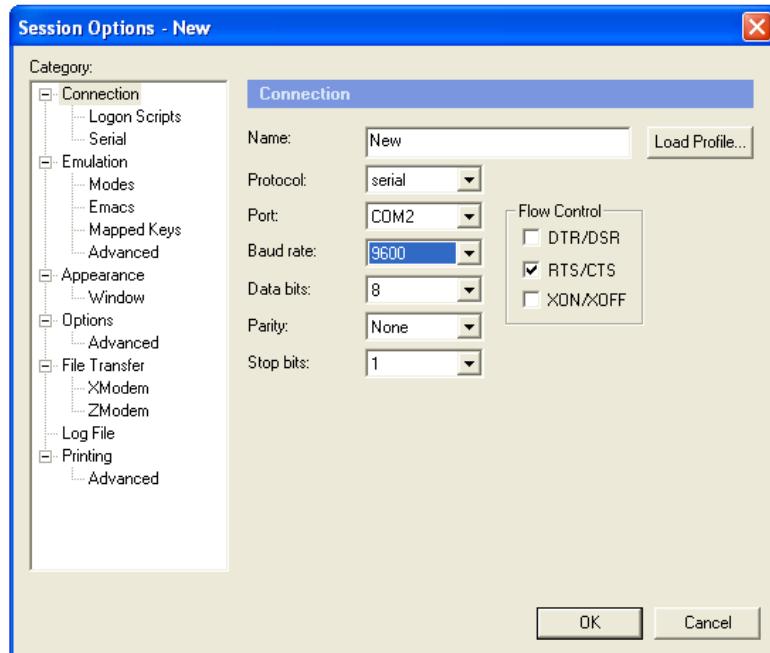
To login in the Ethernet switch through the console port, the user's terminal communication parameter configuration and the configuration of switch's console port should be consistent. The default configuration of the switch's console port is shown below:

- 9600 baud
- no parity
- 8 data bits
- 1 stop bit

First, connect the switch console port and the serial port of PC, and keep the PC online. As shown below,



Then, run the terminal simulation program on PC, such as **SecureCRT 5.1**, as is shown below. Select the serial port connected with the switch port, and configure the terminal communication parameter as: baud rate 9600 bit/s, 8 data bits, 1 stop bit, no parity and flow control, serial interrupted default value 100ms.



At last, download the system files to the switch and run it through console port. The calculation of the switch data can also be observed and controlled by computer.

3.2.2 telnet management

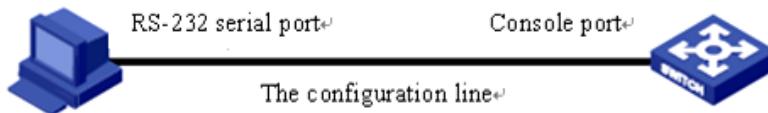
The TELNET protocol aims at offering a communication mechanism which is generally universal, two-way and 8 byte available. Its main objective is letting terminal interface device and the process for terminal interact. In addition, as you can see, the protocol could be used in terminal communication (connection) and process to process communication (distributed computing).

A general thought: a telnet connection is a connection which is used to transfer TCP that contains TELNET control data.

TELNET protocol base on the following 3 ideas mainly: first, virtual network terminals; second, the principle of negotiating options; third, viewing the terminal and process as a balanced approach.

User can make remote management and maintenance through Telnet. Both switch client and telnet client need corresponding configuration so that user can login in the switch by Telnet.

When user login on a switch, the picture following shows the detail:



User can start TELNET services by command.

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 0	Enter IP port mode
3	ip address A.B.C.D [A.B.C.D] <1-4094>	Configure the IP address A.B.C.D: IPaddress [A.B.C.D]: subnet mask <1-4094>: vlan number
4	exit	Exit global configuration mode and enter enable mode
5	telnet-server {accept/close/max-session} port-list	Set telnet services port-list port list
6	show telnet-server	Show telnet configuration

3.2.3 SSH management

3. 2. 3. 1 SSH Function Instruction

SSH (Secure Shell) is a protocol which is used for providing a secure remote login and other secure network services on the non-secure network. When the user makes a telnet to network devices through non-secure network environment, each time before sending data, SSH will automatically encrypt data. When the data arrive at their destination, SSH automatically decrypts the encrypted data, thus providing secure information safeguards to protect the network device from interception and other attacks, such as clear-text passwords. In addition, SSH provides strong authentication to protect against such a "middleman" and other attacks. SSH uses a client - server model. SSH server accepts the connection of SSH Client and provides authentication, SSH client establishes SSH connection with SSH server so that it can achieve to the SSH server through the SSH login.

In addition, SSH also supports other features, such as the transmission of data can be compressed, thus speeding up the transfer speed. They can replace Telnet, or FTP, Pop and even PPP. It provides a secure 'channel'.

3. 2. 3. 2 SSH Default value

Function	Default
SSH server status	stop
SSH V2 key	N/A

SSH V2 server Authentication timeout	600 second
Allowed authentication-retries	20 times
SSH V2 server monitoring port number	22
SSH V2server Session functions	enable
SSH V2 server authentication method	Use local user-password
SSH V2 RSA public key	N/A

3. 2. 3. 3 SSH Configuration

Step	Command	Description
1	config	Enter the global configuration mode
2	generate ssh-key	Generate SSH server key.
3	SSH2 server authentication-timeout <i>time</i>	Set SSH V2 sever authentication timeout (by seconds).
4	SSH2 server authentication-retries <i>retry</i>	Set SSH V2 server's authentication retries, at the range of 1-100.
5	ssh2 server port <i>port</i>	Set SSH V2 server monitoring port number
6	ssh2 server session { <i>sessionlist</i> } { <i>enable /disable</i> }	Enable or disable SSH V2 server session.
7	ssh2 server authentication { <i>password / rsa-key</i> }	Set ssh2 server authentication
8	SSH2 server authentication public-key	Enter rsa public key. It can open the client generated RSA public key host file by Text editing software, then run the command line, copy the key file to the console, type ctrl + s to save the input.
9	ssh2 server	Start SSH V2 server
10	exit	Return to global configuration
11	show ssh2 session	Show information of SSH V2 server

3. 2. 3. 4 Monitoring and Maintenance

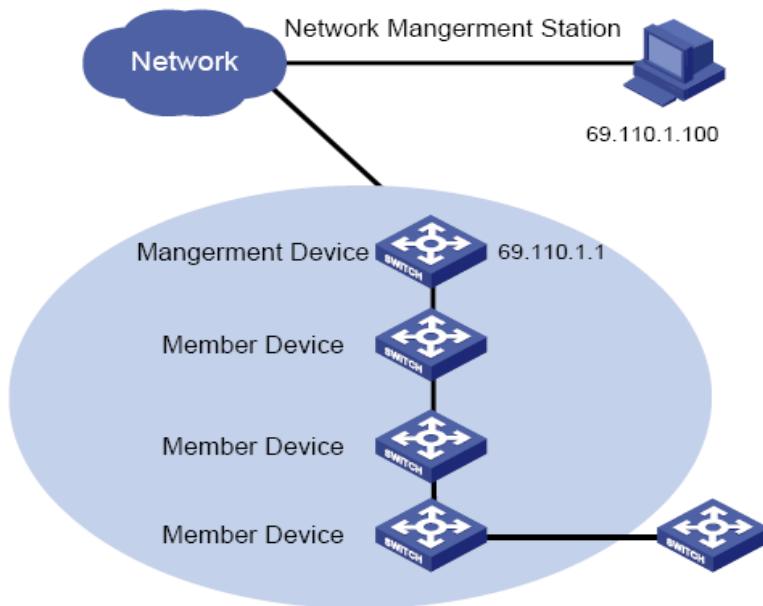
Command	Description
show SSH2 public-key	Show public key information
show SSH2 server	Show server configuration
show SSH2 session	Show session information

show ssh2 public-key rsa Show ssh2 rsa public-key

show ssh2 public-key dss Show ssh2 dss public-key

3.2.4 Cluster rcommand Management

Using Raisecom cluster management function, network administrator is able to manage several switches through a registered IP address of the main switch. The main switch is command facility, while the other switches that are under administration will be member equipments. Member equipment needs not IP address setting usually, it is managed and maintained by manage equipment's redirection. The typical using environment is shown below:



Cluster management contains three protocols: RNDP (Raisecom Neighbor Discover Protocol), RTDP (Raisecom Topology Discover Protocol) and RCMP (Raisecom Cluster Management Protocol). RNDP see to the facility neighbor discovery and information collection, RTDP see to collecting and handling all the network topology information, while RCMP see to the cluster member's joining, validation, deletion and so on. Among them, RTDP and RCMP communicate in cluster VLAN. So, appropriate configuration to VLAN2 is needed to make sure that RTDP and RCMP communicate normally, when there be facility that does not support Raisecom cluster management function between the two facilities that need cluster management.

Different roles form by the different degrees and functions of each switch in the cluster, but user can constitute a certain switch's role form configuration. The roles in cluster include supervisory unit, member unit and alternate unit.

The **rcommand** command, like telnet, can login member switch on the command-line interface of the supervisor switch. Consult cluster management function about configuration and commands of cluster management.

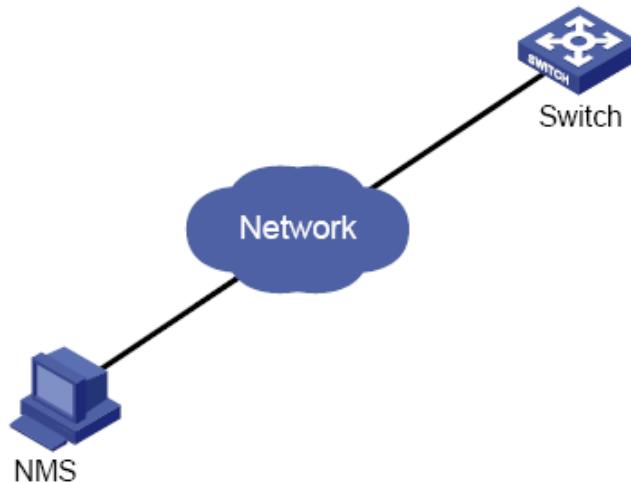
3.2.5 NMS Management

NMS is short for Network Management System. It has 5 functions: alarming, performance,

configuration, safety and accounting. In SNMP, NMS is the workstation running the client program. IBM NetView and Sun NetManager are the usual NMS stations in use. When SNMP Agent receives the query message Get-Request, Get-Next-Request, Get-Bulk-Request about MIB from NMS, Agent carry out **read** or **write** to MIB according to the message style, then create **Response** message according to the operation result and sent it to NMS as response.

On the other side, once SNMP Agent receives any change on facilities like normal/hot booting or anything unusual it will create a **Trap** message and report it to NMS actively.

User can login the switch through NMS, manage and configure the switch by the Agent process on the switch. As shown below.



3.2.6 User Logging Management

User can login, configure and manage the switch by the following way:

- Local login from Console port;
- Local or remote login using Telnet through Ethernet port;
- Login from NMS port

User's name and password is needed when logging, by default username is **raisecom**, password for **raisecom**.

Step	Command	Description
1	user USERNAME password { no-encryption md5 } PASSWORD	User login USERNAME: username; PASSWORD: password;
2	user USERNAME privilege <1-15>	User login privileges; USERNAME: username; <1-15>: user privileges grade.
3	write	Save configuration information
4	show user	Show user information

3.3 Keepalive Function

3.3.1 The Introduction To Keepalive Principle

To find out the facility out of order in time, user needs to acquire the facility information periodically to see if the facility is available and the basic facility information. Users can receive the state of **Keepalive Trap** information collection facility from NMS periodically without any operation. Keepalive module send TRAP periodically to NMS about the basic information of facilities, including facilities' name, facilities' OID, the hardware and software version, MAC address and IP address.

Keepalive module sends **keepalive trap** that contains the basic information of the switch to the network administration station, so that the network administration station could find the switch in a short time.

3.3.2 Keepalive Default Configuration

Function	Default value
keepalive trap switch	On
Keepalive alternation	300 seconds

3.3.3 Keepalive Configuration

By default, KEEPALIVE is open on the switch, and the switch send KEEPALIVE trap periodically. By carrying out the following command in global configuration mode, KEEPALIVE can be set OPEN, CLOSE and PAUSE. If it is CLOSE, the configuration can be loaded. And if it is PAUSE, the configuration can not be saved; the configuration is still default after reboot.

Step	Command	Description
1	config	Enter configuration mode
2	interface ip 0	Enter IP port mode
3	ip address A.B.C.D [A.B.C.D] <1-4094>	Configure the IP address of the switch A.B.C.D: IP address [A.B.C.D]: subnet mask <1-4094>: vlan number
4	exit	Quit global configuration mode and enter privileged EXEC mode
5	snmp-server host A.B.C.D version 3 {noauthnopriv / authnopriv} NAME [udpport <1-65535>] [bridge] [config] [interface] [rmon] [snmp] [ospf]	Configure SNMPv3 Trap the destination host A.B.C.D: IP address NAME: SNMPv3 team name <1-65535>: the UDP port number which the destination use to receive TRAP

6	snmp-server keepalive-trap interval <120-28800>	Set he interval time fo the switch sending KEEPALIVE-TRAP to SNMP network administration station <120-28800>: the interval range, the unit is second
7	snmp-server keepalive-trap {enable/disable/pause}	Start, close, pause sending keepalive trap
8	exit	Return to privileged EXEC mode
9	show snmp config	Show basic SNMP configuration

3.3.4 Monitoring And Maintenance

Show is used to show switch the operation and configuration for maintenance and monitoring. To do this, the following **show** command is available:

Command	Description
show snmp config	Show the basic configuration of SNMP

3.3.5 Typical application



As is shown above, set the IP address as 20.0.0.10 first, then configure the SNMPv2c Trap destination host address: add a **host_1** host address, username public, SNMP version v2c, all trap, set the interval time 500S of the switch sending **keepalive-trap** to SNMP network administration station, open **keepalive trap**, show basic SNMP information at last.

```
Raisecom#config
RaiseCom(config)# int ip 0
RaiseCom(config-ip)#ip address 20.0.0.10 1
RaiseCom(config-ip)#exit
RaiseCom(config)#snmp-server host 20.0.0.221 version 2c public
RaiseCom(config)#snmp-server keepalive-trap interval 500
RaiseCom(config)#snmp-server keepalive-trap enable
RaiseCom(config)# show snmp config
```

3.4 Task Scheduling Function

3.4.1 The Introduction To Task Scheduling Function Principle

The function is to carry out certain command periodically and maintain the switch configuration function seasonally. By configuring time list a time attribution list could be found, including start time, periodically time and end time. There are two kinds of time attribution, one begins when the switch starts, which is relative time; the other is the normal time, including year, month, day and so on, which is absolute time.

3.4.2 Task Scheduling Configuration

1. Setting task schedule:

Step	Command	Description
1	config	Enter global configuration mode
2	schedule-list list-no start { up-time days time [every days time [stop days time]] date-time date time [every { day / week / days time } [stop date time]] }	Add or modify schedule-list table. The command set the beginning time and end time of scheduling task, and the cycling interval. list-no: the range of scheduling list number<0-99>; days time: from the start-up time start, it is relative time; input format days: <0-65535>, time: HH:MM:SS such as 3 3:2:1 date time: the calculation of time is in accordance with the system data, it is absolute time; input format: MMM-DD-YYYY HH:MM:SS like jan-1-2003 or 1-1-2003, the range of YYYY is from 1970 to 2199.
3	command-string schedule-list list-no	Add the commands that support schedule-list to the scheduling list. command-string: command string. list-no: list number range <0-99>
4	show schedule-list	Show schedule-list configuration.

3.4.3 Monitoring and maintaining

Command	Description
show schedule-list	Show schedule-list configuration

3.4.4 Typical Configuration

First, add a **schedule-list** table, **List number:** 1, the beginning time is Feb-2-2004 0:0:0 according to system date, and perform every six days, while the terminal time is Feb-2-2005 0:0:0. Then, add the commands that support **schedule-list** to schedule list, and show the **schedule-list** configuration at

last.

Raisecom#**config**

```
Raisecom(config)#schedule-list 1 start date-time Feb-2-2004 0:0:0 every 6 0:0:0 stop Feb-2-2005
0:0:0
```

```
Raisecom(config)#mac-address-table learning disable port-list 1 schedule-list 1
```

```
Raisecom(config)#storm-control dlf schedule-list 1
```

```
Raisecom(config)#exit
```

```
Raisecom# show schedule-list
```

3.5 Fault Location

3.5.1 Basic principle

When anything abnormal happened in the system, fault location can be carried out by examining the facilities' running information.

3.5.2 Memory

Command	Description
show memory	Show the memory state

3.5.3 Buffer

Command	Description
show buffer [port <1-26>]	Show information of the port buffer <1-26>: port range

3.5.4 UP/DOWN history

Command	Description
show diags link-flap	Show the UP/DOWN statistics

3.5.5 show tech-support

Command	Description
show tech-support	Show tech-support information.

3.5.6 syslog in specified packet

After syslog enabled, EMS supporter can view specified packets. It should run according to

following step:

Step	Command	Description
1	debug driver	Debug driver module
2	config	Enter global configuration mode
3	logging console debug	Console logging Leveldebug
4	driver {receive-packet send-packet} [ethertype-classify { Arp/dhcpsnooping /dot1x/etherent-ring/gvrp/igmpsnooping/ip/loopbackdetect/mstp/oam/pppoeagent/ relay-dot1x/relay-gmrp/relay-gvrp/relay-lacp/relay-stp/rndp/rcmp/rtdp/sla-cfm/sla-ip/other}] syslog {enable/disable} [port-list port-list]	Open/Close logging specified type sending/receiving packets <i>enable: enable</i> <i>disable: disable</i>
5	exit	Back to global configuration mode
6	show device statistics	Show device statistics

It will not logging any packet in default situation.

Typical configuration:

Open port 1 Eth type is stp receiving syslog

Raisecom # **debug driver**

Set successfully

Raisecom # **config**

Raisecom(config)#**logging console debugging**

Set console logging information successfully

Raisecom (config)# **debug driver receive-packet ethertype-classify stp syslog enable port-list 1**

3.5.7 Discard/ Recover specified packet

Discard/ Recover specified receiving/sending packet should be according to the following step:

Step	Command	Description
1	config	Enter global configuration mode
2	driver {receive-packet send-packet} [ethertype-classify { Arp/dhcpsnooping /dot1x/etherent-ring/gvrp/igmpsnooping/ip/loopbackdetect/mstp/oam/pppoeagent/ relay-dot1x/relay-gmrp/relay-gvrp/relay-lacp/relay-stp/rndp/rcmp/rtdp/sla-cfm/sla-ip/other}] discard {enable/disable} [port-list port-list]	Discard/ Recover specified receiving/sending packet <i>enable: enable</i> <i>disable: disable</i>
3	exit	Back to global configuration mode
4	show device statistics	Show device statistics

Typical Configuration Example:

Discard port 1 Eth type stp receiving packet

Raisecom # **config**

Raisecom (config)# driver receive-packet ethertype-classify *stp* discard *enable* port-list *1*

3.5.8 Device statistics

Command	Description
show device statistics	Show device statistics
clear device statistics	Clear device statistics

Typical Configuration

Show receiving packet statistics on port 1

Raisecom#**show device statistics port 1 SvcName**

<i>RcvStat</i>	<i>SndStat</i>	
-----	-----	-----
<i>ip</i>	0	0
<i>arp</i>	0	0
<i>loopbackdetect</i>	0	0
<i>relay-stp</i>	0	0
<i>relay-dot1x</i>	0	0
<i>relay-lacp</i>	0	0
<i>relay-gmrp</i>	0	0
<i>relay-gvrp</i>	0	0
<i>rndp</i>	0	0
<i>rtdp</i>	0	0
<i>mstp</i>	0	0
<i>rcmp</i>	0	0
<i>oam</i>	0	0
<i>dot1x</i>	0	0
<i>gvrp</i>	0	0
<i>sla-cfm</i>	0	0
<i>sla-ip</i>	0	0
<i>ethernet-ring</i>	0	0
<i>dhcpsnooping</i>	0	0
<i>pppoeagent</i>	0	0
<i>igmpsnooping</i>	0	0
<i>other</i>	0	0

3.6 Ping

3.6.1 Ping Principle

Ping is the most frequently-used command for troubleshooting, which is usually used to test if the link between the two hosts works. **Ping** is carried out by ICMP ECHO messages usually. It is made of ICMP reply and questioning messages, and if the network works well a reply messages will be received.

Ping can also be carried out through other paths, such as UDP, TCP and SNMP. In general, almost all the requests/replies can be used to acquire reply time. Usually, the ways except ICMP ECHO is used to settle the problem that some routers' no response or low response priority leads to the wrong answering time.

3.6.2 Ping Configuration

Test if the remote host is accessible.

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 0	Enter ip port mode
3	ip address A.B.C.D [A.B.C.D] <1-4094>	Configure the ip address on the switch A.B.C.D: IP address [A.B.C.D]: subnet mask <1-4094>: vlan number
4	exit	Exit global configuration mode and enter privileged EXEC mode.
5	exit	Exit privileged EXEC mode.
6	ping Ipaddress [count NumPktsRe] [size SizeofIcmpeChPkt] [waittime PktTimOut]	Test if the remote host is accessible. Ipaddress: test the IP address A.B.C.D. NumPktsRe: Number of packets to receive specify the package number before the ping program ends <1-65535>. SizeofIcmpeChPkt: Size of icmp echo packet specify the size of the ICMP answering message<1-4096>. PktTimOut: Packet timeout in seconds specify the time-out time of ping waiting for answer <1-100>, the unit is milliseconds.

3.6.3 Typical application

As is shown below, the host connects the switch with cable. User can confirm if the connection works through the command **ping**, while the switch is also able to transfer data to the host through **ping**.



1 Set the switch IP address as 20.0.0.10, the connection IP address as 10.168.0.221, the number of messages sent is 3, the message size is 100, waiting time 3. Because the destination IP address goes against the PC IP, the connection does not work.

Raisecom#**config**

```
Raisecom(config)# int ip 0
```

```
Raisecom(config-ip)#ip address 20.0.0.10 1
```

```
Raisecom(config-ip)#exit
```

```
Raisecom(config)#exit
```

```
Raisecom#ping 10.168.0.221 count 3 size 100 waittime 3
```

Type CTRL+C to abort.

Sending 3, 108-byte ICMP Echos to 10.168.0.221 , timeout is 3 seconds:

UUU

no answer from 10.168.0.221

Ping unsuccessfully

2 Connect PC, the IP address is 20.0.0.221, set the switch IP 20.0.0.10, connect success will be shown.

Raisecom#**config**

```
Raisecom(config)# int ip 0
```

```
Raisecom(config-ip)#ip address 20.0.0.10 1
```

```
Raisecom(config-ip)#exit
```

```
Raisecom(config)#exit
```

```
Raisecom#ping 20.0.0.10 count 3 size 100 waittime 3
```

Type CTRL+C to abort.

Sending 3, 108-byte ICMP Echos to 20.0.0.221 , timeout is 3 seconds:

!!!

Success rate is 100 percent(3/3)

round-trip (ms) min/avg/max = 0/10/32

3.7 tracerout

3.7.1 traceroute Principle

Traceroute, like **ping**, is a useful way of network management, which is used to find the route that the router s and lines that the message actually passes.

L3 Traceroute is carried out by sending a group of incremental TTL probe packets. Probe packets work in the form of UDP or ICMP Echo. If only TTL>0, or a ICMP will be returned per hop to the destination. From this message the RRT of per hop on the way to destination.

3.7.2 traceroute configuration

Before L3 Traceroute is used, the IP address and default gateway of the switch need configuration first.

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 0	Enter IP configuration mode
3	ip address A.B.C.D [A.B.C.D] <1-4094>	Configure the IP address of the switch A.B.C.D: IP address [A.B.C.D]: subnet mask <1-4094>: vlan number
4	exit	Quit global configuration mode and enter privileged EXEC mode
5	ip default-gateway A.B.C.D	Configure the default gateway A.B.C.D: gateway number
6	show int ip	Show IP configuration
7	show running	Show default gateway configuration
8	traceroute A.B.C.D [firstTTL <1-255>] [maxTTL <1-255>] [port <1-65535>] [waittime <1-60>] [count <1-10>]	traceRoute show the route to destination A.B.C.D: IP address firstTTL: initialize TTL value maxTTL: maximize TTL value <1-255>: TTL value range <1-65535>: Port number range <1-60>: waiting time range <1-10>: count value

3.7.3 Typical Configuration Example

Example: set the IP address as 10.0.0.8, default gateway 10.100.0.1, trace the route to 58.63.236.42(www.sina.com.cn)

Raisecom#**config**

Raisecom(config)# **int ip 0**

Raisecom(config-ip)#**ip address 10.0.0.8 1**

Raisecom(config-ip)#**exit**

```
Raisecom(config)#ip default-gateway 10.100.0.1
```

```
Raisecom(config)#exit
```

```
Raisecom#tracing the route to 58.63.236.42
```

Type *ctrl+c* to abort.

1	10.0.0.1	10 ms	10 ms	10 ms
2	192.168.101.5	3 ms	3 ms	73 ms
3	192.168.101.5	10 ms	10 ms	10 ms
4	202.96.4.81	18 ms	16 ms	19 ms
5	202.106.228.177	9 ms	5 ms	12 ms
6	202.106.228.5	10 ms	8 ms	9 ms
7	202.96.12.25	7 ms	8 ms	5 ms
8	219.158.11.66	24 ms	20 ms	10 ms
9	202.97.15.57	101 ms	101 ms	126 ms
10	202.97.60.185	218 ms	222 ms	205 ms
11	202.97.40.58	119 ms	112 ms	113 ms
12	219.136.246.134	118 ms	142 ms	131 ms
13	219.136.246.6	138 ms	135 ms	110 ms
14	58.63.232.46	103 ms	115 ms	105 ms
15	58.63.236.42	199 ms	205 ms	197 ms

Trace complete.

3.8 telnet

3.8.1 telnet Principle

Telnet is the standard protocol and main way of remote login, which offers the ability of working on the local machine for remote host. The telnetd module in ROS4.0 implements the function of telnet server, letting telnet remote client login the facility so that it could be logged in and managed by telnet client.

3.8.2 telnet Default Configuration

Function	Default value
Telnet server up-link limit	5
telnet server link physical port	All the ports

3.8.3 telnet Configuration

1 Close telnet configuration

Step	Command	Description
1	config	Enter global configuration mode
2	telnet-server close terminal-telnet <1-5>	Telnet server close <1-5> end telnet dialog number
3	exit	Return to privileged EXEC mode
4	show telnet-server	Show current telnet server configuration

2 Set the telnet server linking upper-limit

Step	Command	Description
1	config	Enter global configuration mode
2	telnet-server max-session <0-5>	Set the telnet server linking upper-limit. <0-5> linking number
3	telnet-server accept port-list (all/{1-MAX_PORT_STR})	Set the available port of the telnet server port-list: port list all: all the ports MAX_PORT_STR: port upper limit
4	exit	Return to privileged EXEC mode
5	show telnet-server	Show the current configuration of the telnet server
6	Show information port	Show information port

3.8.4 Typical Configuration Example

1 Set the linking upper limit of the telnet server as 3, open the available ports of Telnet server and show the current configuration.

Raisecom#**config**

Raisecom(config)#**telnet-server max-session 3**

Set successfully

Raisecom(config)#**telnet-server accept port 28**

Raisecom(config)#**exit**

Raisecom#**show telnet-server**

Max session: 3

Accept port-list: 28

3.9 Watchdog

3.9.1 Watchdog Principle

By configuring the watchdog software, the system program going into endless loop can be avoided,

and the system stability will be better.

3.9.2 Configure Watchdog

Enable and Disable watchdog

Step	Command	Description
1	watchdog {enable/disable}	<i>enable</i> : open watchdog <i>disable</i> : close watchdog
2	show watchdog	Show watchdog state

3.9.3 Typical Configuration Example

Open watchdog and show the state

Raisecom#**watchdog enable**

Set successfully

Raisecom#**show watchdog**

Watchdog function: Enable

3.10 MTU (Maximum transferred unit) Function

3.10.1 MTU Instruction

MTU-Maximum transferred unit, which is system allowed the maximum length of forwarding packets. When the length of forwarding packets longer than the maximum allowed by the system, the system will discard the packet.

3.10.2 MTU Configuration

Set system that allows maximum length of forwarding packets

Step	Command	Description
1	config	Enter global configuration mode
2	[no]system mtu PKTS-MAX-LEN	Set or recover maximum length of forwarding packets that systme allows <i>PKTS-MAX-LEN</i> :maximum length of forwarding packets(bytes)
3	show system mtu	Show maximum length of forwarding packets that the current system allows

Note:

The maximum length packet and the length of the echo may be different, because the device is different. Some devices are only allowed to select several fixed length, so when setting the maximum

length of the packet, it will be judged according to the input parameters. The closest optional length which is greater than input parameter is set to the maximum length that the system allows to forward packets. Therefore, the maximum length of echo is different from the set. But it also indicates that set successfully.

3.10.3 Monitoring and maintenance

Command	Description
show system mtu	Show maximum length of forwarding packets that current system allows

3.10.4 Typical Configuration Example

Set system that allows forwarding packets maximum length as 1522, shows the current system that allows maximum length of forwarding packets:

```
Raisecom(config)#system mtu 1522
```

Actual max frame length: 1522

```
Raisecom(config)#show system mtu
```

System MTU size: 1522 bytes

Chapter 4 CPU Monitoring Configuration Guide

4.1 Introduce CPU Monitoring

CPU monitoring module can provide the necessary relevant information of operations for administrators and developers, which is a strong support for the system performance or diagnostic failure. Main features include the following points:

1) CPU-utilization calculation and display

Calculate CPU holding-time and utilization in each cycle (1 second, 5 seconds, 1 minute, 10 minutes, or 2 hours) of occupancy time and, including CPU holding-time and utilization in each task and total CPU holding-time and utilization.

Show information of tasks statistics and utilization in each task.

Show total tCPU utilization in each cycle.

2) CPU utilization alarm

When CPU utilization in interval-time exceeds a rising-threshold or below a falling-threshold, system will send trap accompanied by top five tasks and their CPU utilization in a recent one cycle (5 seconds, 1 minute, or 10 minutes).

3) Stack monitoring

When task stack low (less than 10%), prompt Informational-level syslog message;

When task stack overflow, prompt Critical-level information;

4) Show process dead

5) Show cpu-utilization

6) Show process TASKNAME.

4.2 CPU monitoring configuration

4.2.1 Default configuration of CPU monitoring

Function	Default value
CPU-utilization alarm	disable
Rising-threshold	100
Falling-threshold	1
Interval-value	60s

4.2.2 Configure CPU monitoring function

4.2.2.1 Enable or disable CPU utilization Trap

This configuration is used to enable or disable CPU utilization Trap. Default CPU utilization Trap disable.

Step	Command	Description
1	config	Enter into global configuration mode.
2	snmp-server traps {enable/disable} cpu-threshold	Configure CPU utilization and Trap enable or disable.

4.2.2.2 Configure CPU rising-threshold and falling-threshold as well as interval-time

Step	Command	Description
1	config	Enter into global configuration mode.
2	cpu rising-threshold rising-threshold-value [falling-threshold falling-threshold-value] [interval interval-value]	Configure CPU rising-threshold and falling-threshold as well as interval-time <i>rising-threshold-value</i> : rising-threshold value, range in 1-100, default as 100; <i>falling-threshold-value</i> : falling-threshold value, range in 1-100, default as 1; <i>interval-value</i> : interval-value, range in <5-36000>, unit of seconds, default as 60;
3	show cpu-utilization	Show CPU utilization and configuration information.

When implementation of **no cpu rising-threshold**, restore rising-threshold-value to the default 100;

When implementation of **no cpu falling-threshold**, restore falling-threshold-value to the default 100;

When implementation of **no cpu interval**, restore interval-value to the default 60 seconds;

Note: Rising-threshold-value must be greater than falling-threshold-value.

4.2.3 Monitoring and Maintenance

Command	Description
show process [sorted (normal-priority process-name)]	View status information of each task.
show process cpu [sorted [1min / 10min / 5sec / invoked]]	View operating status information of each task.
show process TASKNAME	View status information of specified task in detail.
show cpu-utilization [dynamic]	View total CPU utilization in each cycle.
show cpu-utilization history (5sec / 1min / 10min / 2hour)	View cpu-utilization history.
show process dead	View process dead information.

4. 2. 3. 1 show process

Raisecom(config)#**show process**

```

Number of processes:          94
Last 5 seconds CPU utilization:   13 %
Last 1 minute CPU utilization:    1  %
Last 10 minutes CPU utilization:  2   %

READY      / Task is not waiting for any resource other than the CPU.
PEND       / Task is blocked due to the unavailability of some resource.
DELAY      / Task is asleep for some duration.
SUSPEND    / Task is unavailable for execution (but not suspended, delayed, or pended).
DELAY+S    / Task is both delayed and suspended.
PEND+S    / Task is both pended and suspended.
PEND+T    / Task is pended with a timeout..
PEND+S+T / Task is pended with a timeout, and also suspended.
state+I   / Task has inherited priority (+I may be appended to any string above).
DEAD      / Task no longer exists.

```

PNo	Priority	Status	PC	ErrorNo	Stack	ProcessName
				(Size /Use /Max)		
1	0/ 0	PEND	5177D4	3D0001	7984/ 224/ 380	tExcTask
2	0/ 0	PEND	5177D4	0	4984/ 216/ 280	tLogTask
3	10/ 10	DELAY	4F5D98	0	4184/ 144/ 288	tTaskM
4	50/ 50	PEND	4F13AC	0	9984/ 192/ 1596	tNetTask
.....						

4. 2. 3. 2 show process cpu

Raisecom(config)#**show process cpu**

```

Last 5 seconds CPU utilization:   18 %
Last 1 minute CPU utilization:    1  %
Last 10 minutes CPU utilization:  2   %
Last 2 hours CPU utilization:    2   %

```

PNo	CPURunTime	Invoked	CPUUtilization	ProcessName
(Sec.uSec)		(5sec/1min/10mins)		

16	96.901411	13454	0.08%/ 0.50%/ 0.46%	<i>tPortStats</i>
7	62.516049	1132594	0.25%/ 0.31%/ 0.30%	<i>linksan</i>
17	41.530019	18982	0.22%/ 0.21%/ 0.20%	<i>tLinkTrap</i>
64	35.116337	22008	0.00%/ 0.18%/ 0.16%	<i>tIpBind</i>
95	28.42222	18980	0.14%/ 0.14%/ 0.13%	<i>tCPUMon</i>
84	18.558805	20210	18.56%/ 0.79%/ 0.38%	<i>tScrnBg_0</i>
29	18.351982	18980	0.08%/ 0.09%/ 0.08%	<i>tCcom</i>

4. 2. 3. 3 show process TASKNAME

Raisecom(config)#show process **tCcom**

<i>Process ID:</i>	<i>B5BA30</i>
<i>Process name:</i>	<i>tCcom</i>
<i>Create time:</i>	<i>0h:0m:9s</i>
<i>Entry:</i>	<i>4489B0</i>
<i>Status:</i>	<i>PEND</i>
<i>Error number:</i>	<i>0</i>
<i>Program counter:</i>	<i>5177D4</i>
<i>Delay(ticks):</i>	<i>0</i>
<i>Total invoked times:</i>	<i>19121</i>
<i>Semaphore waiting for:0</i>	
<i>CPU use time(Sec.uSec):</i>	<i>18.488418</i>
<i>Normal priority/Current priority:</i>	<i>150/150</i>
<i>Stack size/Stack use/Max stack use: 16376/240/496</i>	
<i>Stack begin/Stack pointer/Stack end:B5BA30/B5B940/B57A30</i>	

Statistics for Period:

<i>Period</i>	<i>CPURunTime</i>	<i>Invoked</i>	<i>CPU-Utilization</i>
			<i>(Sec.uSec)</i>

<i>5seconds</i>	<i>0.4819</i>	<i>5</i>	<i>0%</i>
<i>1minute</i>	<i>0.52988</i>	<i>55</i>	<i>0%</i>
<i>10minutes</i>	<i>0.561054</i>	<i>580</i>	<i>0%</i>

4. 2. 3. 4 show cpu-utilization

<i>CPU threshold trap enable:</i>	<i>Enable</i>
<i>Rising threshold:</i>	<i>80</i>
<i>Falling threshold:</i>	<i>50</i>

Trap transfer observation interval(second): 10
Last 1 second CPU utilization: 28%
Last 5 seconds CPU utilization: 19%
Last 1 minute CPU utilization: 1%
Last 10 minutes CPU utilization: 2%
Last 2 hours CPU utilization: 2%
Total CPU utilization: 2%

4.2.3.5 show cpu-utilization history

Raisecom(config)#**show cpu-utilization history 10min**

Cpu utilization history table size:60

CPU-utilization:

2%	2%	2%	2%	2%	2%	2%	2%	2%	2%	2%	2%	2%	2%
2%	2%	2%	2%	2%	2%	2%	2%	2%	2%	2%	2%	2%	2%
2%	2%	2%	2%										

4.2.3.6 show process dead

Raisecom(config)#**show process dead**

<i>Entry</i>	<i>Priority</i>	<i>ErrorNo</i>	<i>MaxStackSize</i>	<i>DeadTimes</i>	<i>TimeDel</i>	<i>CurStatus</i>	<i>ProcName</i>
15654	250	0	6504	1	0h:0m:18s	DEAD	tRosApp
3f4fc	200	0	872	1	0h:1m:20s	DEAD	tColdTrap

4.2.3.7 Typical configuration examples

Configure snmp-server, enable CPU-utilization Trap, rising-threshold as 80, falling-threshold as 20, interval-time as 10s; vies configuration information and total CPU-utilization in each cycle.

Raisecom# **snmp-server host 11.22.33.44 version 2c public udpprt 162**

Raisecom# snmp-server traps *enable* cpu-threshold

Raisecom# cpu rising-threshold 80 falling-threshold 20 interval 10

Raisecom(config)#**show cpu-utilization**

CPU threshold trap enable: Enable
Rising threshold: 80
Falling threshold: 20
Trap transfer observation interval(second): 10
Last 1 second CPU utilization: 7%
Last 5 seconds CPU utilization: 13%
Last 1 minute CPU utilization: 1%
Last 10 minutes CPU utilization: 2%

Last 2 hours CPU utilization: 2%

Total CPU utilization: 2%

Chapter 5 Radius Accounting

5.1 Overview

Radius accounting function is mainly for the user that is doing Radius authentication in certification stage. When the user is logging on, a message that enables accounting function will be sent to Radius accounting server; during the time that user is landed, accounting updating message will be sent to the server according to the accounting strategy; and when the user is logging out, a message to stop accounting will be sent to the server, which contains the landing time. With these messages, the server can be clear when and who have ever log in the OLT, the logging time and even the operation.

5.2 Default configuration

By default Radius accounting is disabled.

5.3 Radius accounting configuration

5.3.1 Enable/disable Radius accounting function

The configuration is to enable or disable Radius accounting function. By default the function is disabled.

Step	Command	Description
1	aaa accounting login {enable / disable}	Enable or disable Radius accounting
2	show aaa accounting	Show Radius accounting configuration

5.3.2 Configure Radius accounting server IP address and UDP port number

The configuration is to configure the IP address and UDP port number of Radius accounting server. By default the IP address is 0.0.0.0, port number is 1813.

Step	Command	Description
1	radius accounting-server A.B.C.D [acct-port]	Configure the IP address and UDP port number of Radius accounting server. A.B.C.D: is the IP address of accounting server Acct-port: is the UDP port number of accounting server, range is 1-65535. The configuration is an optional option, the current value is the default value. Use no radius accounting-server to restore the IP address and port number to default value.
2	show radius-server	Show Radius configuration

5.3.3 Configure the shared key that communicate with the Radius Accounting server

This command is used to configure the key which communicates with the Radius accounting server, the key must be corresponding with Radius accounting server key, or they will charge fail. Key is empty by default.

Step	Command	Description
1	radius accounting-server <i>key WORD</i>	Configure the key which communicates with the Radius accounting server. <i>WORD</i> : shared key and should be configured to a string with length not more than 255 characters. Command of no radius accounting-server <i>key</i> can restore shared key to the default value.
2	show radius-server	Show Radius configuration information.

5.3.4 The strategy of Radius accounting configuration fail

When Radius accounting is enabled, user who passed Radius certification will be charged, but if the accounting fails (disconnected with the server or when shared key is different from the one on the server), there are two way, one is to allow user login, the other is to deny. By default it is to allow.

Step	Command	Description
1	aaa accounting fail { <i>online / offline</i> }	Configure the strategy of accounting fail <i>online</i> : accounting fail permits login <i>offline</i> : accounting fail not permits login
2	show aaa accounting	Show Radius accounting configuration

5.3.5 Configure Radius accounting strategy

There are two strategies, one is to send one accounting enable message to accounting server when user is logging on, and send one accounting ending message to the server; the other way is to add accounting update messages periodically besides the two kinds of messages above, the period is changeable. By default the first way will be taken.

Step	Command	Description
1	aaa accounting update < <i>0-300</i> >	Configure accounting update message period. < <i>0-300</i> >: the period of accounting update message sent, unit is minute, if it is configure 0, the message will not be sent. Use no aaa accounting update to restore the accounting strategy to default value.
2	show aaa accounting	Show Radius accounting configuration.

5.4 Monitoring and Maintenance

Command	Description
show aaa accounting	Show Radius accounting configuration.
show radius-server	Show Radius configuration.

5.5 Typical configuration example

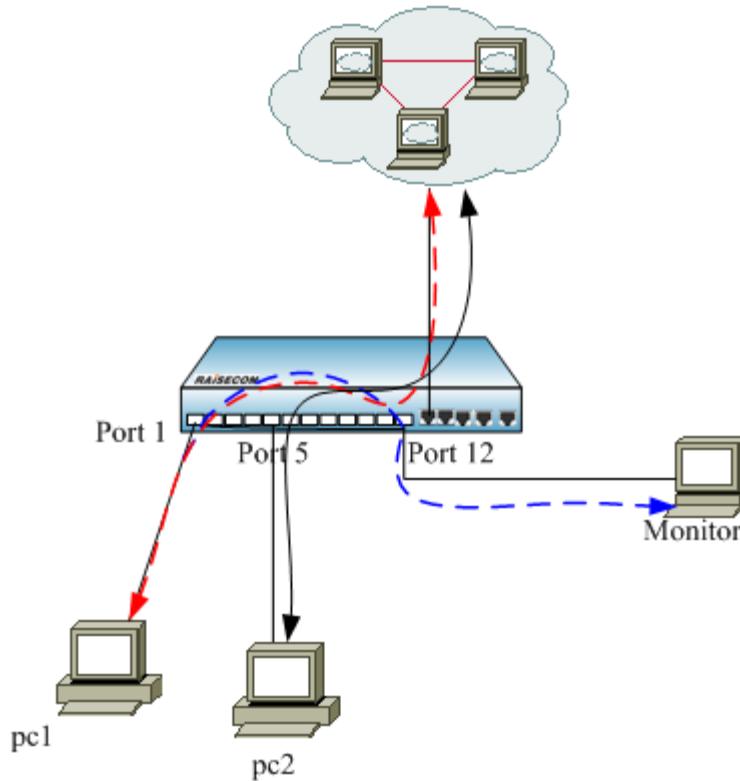
Example 1: enable Radius accounting function, configure the IP address of accounting server to 20.20.20.20, port number is 6000, shard key is hello, the accounting fail strategy is offline, the accounting strategy is to send a accounting update message per 10 minutes.

```
Raisecom# aaa accounting login enable  
Raisecom# radius accounting-server 20.20.20.20 6000  
Raisecom# radius accounting-server key hello  
Raisecom# aaa accounting fail offline  
Raisecom# aaa accounting update 10
```

Chapter 6 Mirror Function

6.1 Local Port Mirror Function Principle

Mirror function is to copy some messages the appointed destination port from the appointed source port, while the normal message transmission works well. With this function, exchange equipment user can monitor the message delivering and receiving of a certain port, and analyse the network situation or defaults.



Mirror Function

PC1 and PC2 connect internet through port 1 and port 5 of the exchange equipment. When we need to monitor the data from PC1, we need to appoint the port 1 of the facility on connection as the mirror source port, and enable the mirror function of the receiving port message, then appoint monitoring port 12 as the destination port. When the data message from PC1 enters the exchange equipment, it will transfer the message and copy the message to the mirroring destination port (port 12). The monitoring equipment connected with the mirror destination port can receive the messages that are mirrored and make analysis.

6.2 Local Port Mirror Function Configuration

6.2.1 The Default Configuration

Function	Default value
----------	---------------

Port mirroring	Disable
Mirror source port	N/A
Mirror destination port	Port 1

6.2.2 Local Port Mirroring Function configuration

The traffic of source port will be copied to monitor port, so that network administrators can analyze the network.. Port 1 is monitor port by default, the source port and the monitor can not be same port.

When the mirror function go into effect, the message from I/O mirror ports will be copied to the monitoring port. The mirroring rules are set when the mirror ports are configured: both, ingress and/or egress. Also, the port can not be set as mirror port when it has already been set as monitoring port.

Only after the mirror function is enabled can the other configurations go into effect.

Step	Command	Description
1	config	Enter global configuration mode
2	mirror { enable / disable }	Enable/disable the mirror function
3	mirror monitor-port <i>port_number</i>	Set the monitor port. <i>port_number</i> is physical port number, range is 1-26.
4	mirror source-port-list{ both <i>port-list</i> /ingress <i>port-list</i>/ egress <i>port-list</i> /ingress <i>port-list</i> egress <i>port-list</i>}	Set source port list, and appoint the corresponding ingress/egress <i>port-list</i> is the physical port list, use ‘,’ and ‘-’ to carry out multi-port input.
5	exit	Quit global configuration mode and enter privileged EXEC mode.
6	show mirror	Show mirror configuration

Notice:

- The mirroring messages also comply with the VLAN configuration transmission rules of the port.
- There can be more than one mirroring port, but only one monitoring port is allowed. Mirror function is disabled by default.

With configuration command **no mirror source-port-list**, the mirroring port that has been configured can be deleted.

With configuration command **no mirror all**, all of the mirroring configurations can be deleted.

6.2.3 Monitoring And Maintaining

The command to show the port mirroring function

Command	Description
---------	-------------

show mirror	Show the port mirroring function
--------------------	----------------------------------

6.2.4 Typical Configuration Example

Set port 26 as the monitoring port, **ingress** port 5-8, **egress** port 7-12

Raisecom #config

Raisecom (config)#mirror enable

Raisecom (config)#mirror monitor-port 26

Raisecom (config)#mirror source-port-list ingress 5-8 egress 7-12

Raisecom (config)#exit

Raisecom #show mirror

Mirror: Enable

Monitor port: 26

-----the ingress mirror rule-----

Mirrored ports: 5-8

-----the egress mirror rule-----

Mirrored ports: 7-12

6.3 Monitoring and Maintaining

Show the commands of mirror function

Command	Description
show mirror	Show mirror configuration

6.4 Typical Configuration Example

To the figure, if there is too many data for port 1 to receive, and reducing the packets number for the monitoring facility is needed, it is supposed to do the following configuration:

Raisecom #config

Raisecom (config)#mirror enable

Raisecom (config)#mirror monitor-port 12

Raisecom (config)#mirror source-port-list ingress 1

Raisecom (config)# mirror ingress divider 200

Raisecom (config)#exit

Raisecom #show mirror

Mirror: enable

Monitor port: 12

Non-mirror port: Not block

-----the ingress mirror rule-----

Mirrored ports: 1

Filter rule: All

Divider: 200

MAC address: 0000.0000.0000

-----the egress mirror rule-----

Mirrored ports: --

Filter rule: All

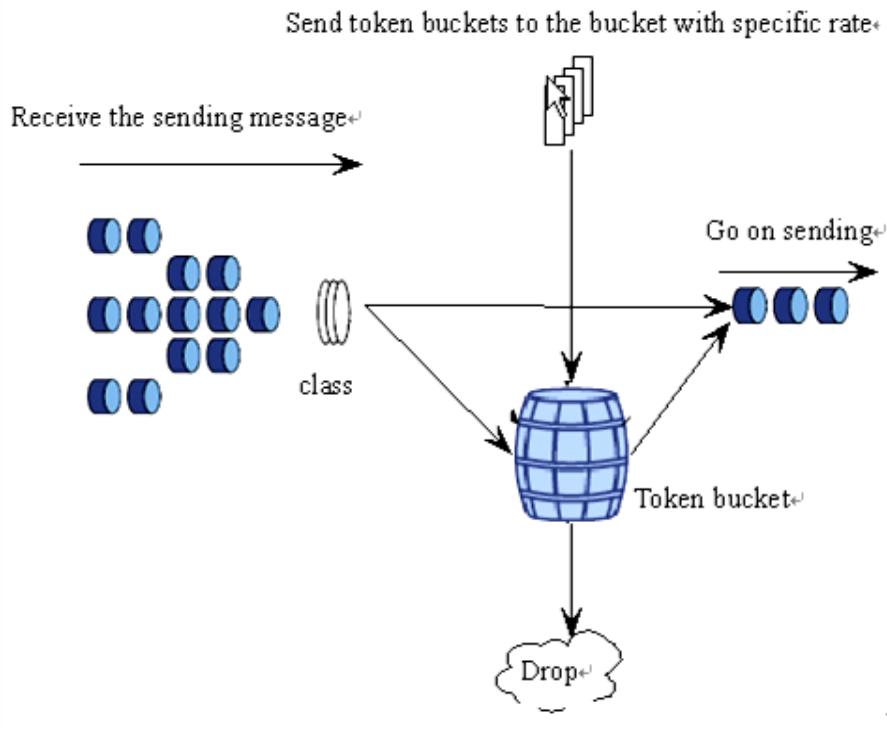
Divider: 1

MAC address: 0000.0000.0000

Chapter 7 Port Rate Limiting and Shaping

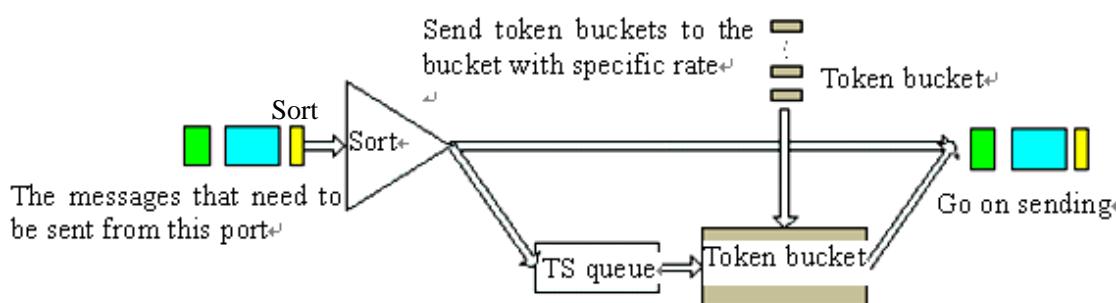
7.1 Port rate limiting and shaping principle

Line rate means rate limiting based on ports, which restricts the overall rate of the ports' receiving and sending messages. Line rate uses token bucket to control the rate. If some port of the facility is in rate limit, all the messages received or sent by the port need to be handled by token bucket. If there is enough token in token bucket, then messages can be received or sent, or it will be abandoned.



Line limit process

Traffic shaping (TS) is used typically in confining the rate and limit of one stream in the output-network, so that this kind of message can be sent out steadily. Stream shaping is usually carried out by buffer and token bucket. When some groups' rate is too high, the message will be stored in buffer first, and then it will be sent into the groups steadily.



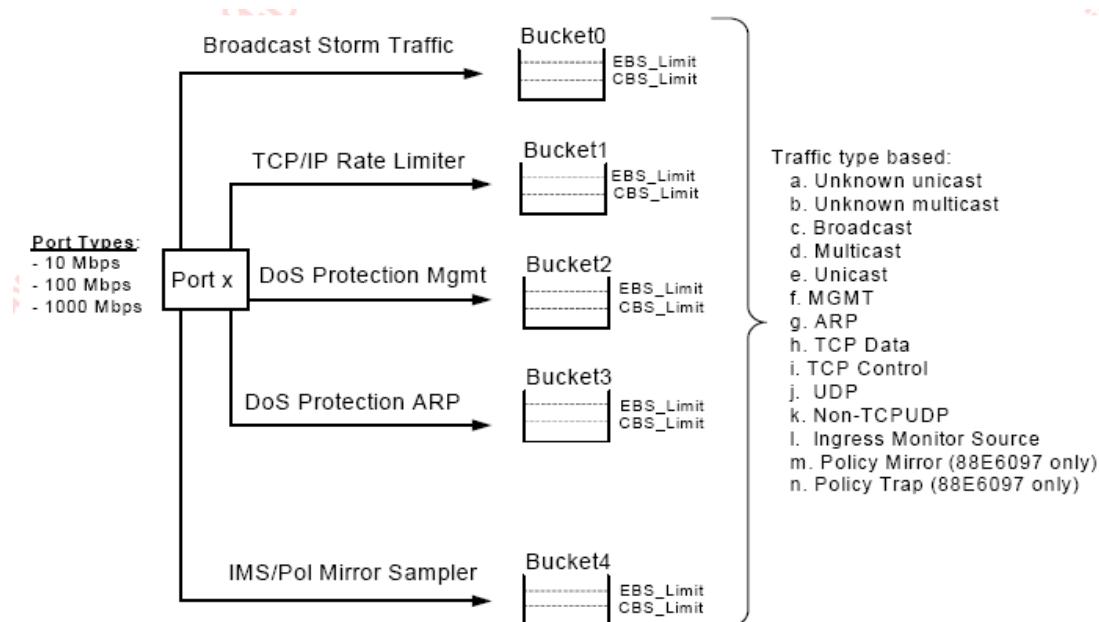
TS processing

TS can reshape given group stream or all the groups. When the groups come, it is classified first, and then continues transmission if there is no need for TS and token bucket. If TS is needed, the group

will be compared with the token in token bucket. The token bucket put token in the bucket according to the rate that users set. If there is enough token for sending, the group will be sent, while the token number decreases according to the group length. When the token is the bucket is not enough for sending, the group will be stored in TS line. When there is group in the TS line, TS pick up one group and send it out periodically. Each sending will be compared with the token in the token bucket, until the token is not enough for the group in the line being sent out or all the groups in the line have been sent out.

For some purpose the bandwidth of the ports or VLAN needs to be confined. In this situation the bandwidth function needs to be configured that the port or VLAN bandwidth be confined in a range, the data that is over the bandwidth will be abandoned. By default, the ports and VLAN rate is auto negotiated, which need not to be confined.

On ingress port, the speed limit may base on specific packets and priority queue. PIRL (Port Based Ingress Rate Limiting) module makes MV6097 chip for instance, which shows the speed limiting process. The chip on each port supports five rate limiting resources (0-4), occupied by global storm-control, packet types, and queue priority. The rate limiting is available in bucket.



Steps: 64 Kbps for 64 Kbps-1 Mbps, 1Mbps for 1 Mbps ~ 100 Mbps; 100 Mbps for 100 Mbps ~ 1000 Mbps.

The speed limit is focus on ARP, TCP Data, Tcp Ctrl, UDP, and Non-TCPUDP packet, in priority queue for 0-4. When a transmitting speed exceeds the rate limit, it will be discarded or dealed with by flow control.

7.2 Line rate and TS based on port

7.2.1 The default configuration

Function	Default value
The ingress port resource speed limitation message type, line priority calculation.	Or calculation relationship

When ingress port resource exceed the given speed limit	Drop drop
MAC no-speed limitation	Disabled
Port no-speed limitation function based on smac, dmac	Disabled

7.2.2 Port speed limitation and reshaping function

1. Configure the ingress port bandwidth and burst:

Step	Command	Description
1	config	Enter global configuration mode Set the physical port bandwidth limit <i>port-list</i> physical port, ranging from 1 to the maximum number, use ‘,’ and ‘-’ for multi-port input:
2	rate-limit port-list {all / port-list} ingress rate [burst]	<i>rate</i> means the bandwidth, the unit is kbps, from 1 to 1048576. <i>burst</i> the burst,unit Kbps,can be set from 1 to 512. The actual value may be different from the value setting; <i>ingress</i> the ingress direction
3	exit	Quit global configuration mode and enter EXEC privileged mode
4	show rate-limit port-list [port-list]	Show port bandwidth limitation. <i>port-list</i> : accord with the meaning above.

2. Configure the ingress port bandwidth and burst:

Step	Command	Description
1	config	Enter global configuration mode
2		Configure the rate limiting. <i>port-list</i> : physical port number, range is 1-26, use “,” and “-” for multiple ports’ rate limiting.
	rate-limit port-list {all / port-list} egress rate [burst]	<i>rate</i> : stands for the maximum bandwidth allowed to be transmitted, unit is kbps, range is 1-1048576. (The actual value may be a little bit different from the configured value because it can only be the exponential of 2). <i>burst</i> : the configured bandwidth. Unit is KBps, the available value is 1-512. The real value can be different with the configured value. <i>egress</i> : the out traffic
3	exit	Exit from global configuration mode and enter privileged EXEC mode.
4	show rate-limit port-list [port-list]	Show the rate limiting of the port <i>port-list</i> : physical port number, range is 1-26,use “,” and

“-“ for multiple ports configuration.

To delete port speed limitation, use global configuration command **no rate-limit port-list {all/port-list} {both | ingress | egress}**

3. Configure the ingress/egress port bandwidth and burst:

Step	Command	Description
1	config	Enter global configuration mode
2		Configure the rate limiting. <i>port-list</i> physical port number, range is 1-26, use “,” and “-“ for multiple ports’ rate limiting.
	rate-limit port-list {all / port-list} both rate	<i>rate</i> stands for the maximum bandwidth allowed to be transmitted, unit is kbps, range is 1-1048576. (The actual value may be a little bit different from the configured value because it can only be the exponential of 2). <i>burst</i> : the configured bandwidth. Unit is KBps, the available value is 1-512. The real value can be different with the configured value.
3	exit	Exit from global configuration mode and enter privileged EXEC mode.
4	show rate-limit port-list [port-list]	Show the rate limiting of the port <i>port-list</i> physical port number, range is 1-26,use “,” and “-“ for multiple ports configuration.

7.2.3 Monitoring and maintaining

Use **show** to look over the switch’s configuration and states of port speed limitation and PIRL function for the convenience of monitoring and maintaining. The relative command is show below:

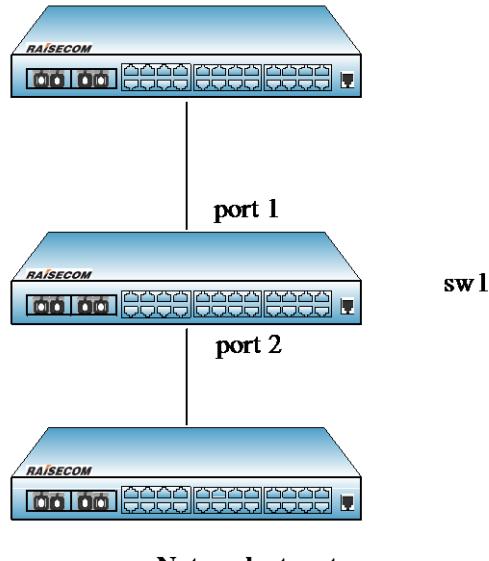
Command	Description
	Show the port bandwidth limitation
show rate-limit port-list [port-list]	<i>port-list</i> strands for physical port number, range is 1-26, use ‘,’ and ‘-’ for multi-port ingress

7.2.4 Typical configuration example

➤ Aim

Configure the uplink bandwidth of the sw1 port 1 as 1000kbps, burst 64kbps, so that the switch could manage the network traffic.

➤ Network structure:

**Network structure**

➤ Configuration step:
Raisecom#**config**

Raisecom(config)# **rate-limit port-list 1 ingress 1000 64**

Set successfully

Actual ingress rate of FE port: 1000

Actual ingress burst of FE port: 64

Raisecom(config)#**exit**

Raisecom# **show rate-limit port-list 1**

I-Rate: Ingress Rate

I-Burst: Ingress Burst

E-Rate: Egress Rate

E-Burst: Egress Burst

Port	I-Rate(Kbps)	I-Burst(KBps)	E-Rate(Kbps)	E-Burst(KBps)
1	1000	64	0	0

Port	I-Rate(Kbps)	I-Burst(KBps)	E-Rate(Kbps)	E-Burst(KBps)
1	1000	64	0	0

7.3 Speed limitation and reshaping function based on VLAN configuration

7.3.1 The default configuration

By default, there is no bandwidth limit based on VLAN.

7.3.2 Speed limitation and reshaping function based on VLAN configuration

1. Configure speed limitation based on VLAN:

Step	Command	Description
1	config	Enter global configuration mode
2	rate-limit vlan	Set the traffic limitation based on VLAN.

	<i><1-4094> rate burst[statistics]</i>	<i><1-4094>:VLANID;</i> <i>Rate</i> strands for the bandwidth limitation based on VLAN, the unit is kbps, range is 1-1048576. The actual value may be different from the configured one. <i>burst</i> configured burst, the unit is Kbps, the value can be set from 1 to 512; <i>statistics</i> : statistics of packet drop
3	exit	Exit from global configuration and enter EXEC privileged mode
4	show rate-limit vlan	Show the port speed limitation

2. configure the bandwidth and burst based on QinQ VLAN

Step	Command	Description
1	config rate-limit double-tagging-vlan outer {<1-4094> any} inner {<1-4094> any} rate burst[statistics]	Enter global configuration mode Configure the bandwidth limit based on QinQ VLAN; outer {<1-4094>/any} outer layer VLAN, <i>any</i> strands for any outer layer VLAN; inner {<1-4094>/any} lining VLAN, <i>any</i> strands for any outer layer VLAN;
2		<i>rate</i> strands for the configured bandwidth value, the unit is kbps, range is 1-1048576, the actual value may be different from the configured value. <i>burst</i> the configured burst, the unit is kbps, the value can be set from 1 to 512. The actual value may be different from the configured value. <i>statistics</i> : statistics of packet drop
3	exit	Exit from global configuration mode and enter EXEC privileged mode.
4	show rate-limit vlan	Show the port bandwidth limitation.

Notice: The outer and inner VLAN can not be assigned at the same time.

7.3.3 Monitoring and maintaining

Using **show**, the switch's VLAN speed limit configuration and state can be shown for the convenience of monitoring and maintaining. The related command is shown below:

Command	Description
show rate-limit vlan	Show the port bandwidth limitation.

7.3.4 Typical configuration example

➤ Aim

Set the switch's VLAN 5 bandwidth as 2048kbps, the burst is 128kbps, with statistics of drop packets.

Set the outer layer VLAN as 6, inner VLAN as 10, the bandwidth 1024kbps, the burst 64kbps, with statistics of drop packets.

Set the outer layer VLAN as any, inner VLAN as 8, the bandwidth 4096kbps, the burst 256kbps, with statistics of drop packets.

➤ Configuration step:

Step 1:

Raisecom#**config**

Raisecom(config)# **rate-limit vlan 5 2048 128 statistics**

Set successfully

Actual rate: 2048

Actual burs: 128

Raisecom(config)# **rate-limit double-tagging-vlan outer 6 inner 10 1024 64 statistics**

Set successfully

Actual rate: 1024

Actual burs: 64

Raisecom(config)# **rate-limit double-tagging-vlan outer any inner 8 4096 256 statistics**

Set successfully

Actual rate: 4096

Actual burs: 256

Raisecom(config)#**exit**

Raisecom# **show rate-limit vlan**

CVLAN: Customer VLAN(inner VLAN)

SPVLAN:Service provider VLAN(outer VLAN)

CVLAN: Customer VLAN(inner VLAN)

SPVLAN:Service provider VLAN(outer VLAN)

StatisHw:Statistics Hardware

Inp: Inprofile

OutP:Outprofile

Type	CVLAN	SPVLAN	Rate(Kbps)	Burst(KB)	StatisHw	Inp(Pkts)	Outp(Pkts)
single	5	--	2048	128	YES	41,135	1,323
double	10	6	1024	64	YES	32,324	1,235
double	8	any	4096	256	YES	16,132	1,034

Step 2: Clear vlan5 statistics

Raisecom(config)# **clear rate-limit statistics vlan 5**

Raisecom(config)#**exit**

Raisecom# **show rate-limit vlan**

CVLAN: Customer VLAN(inner VLAN)

SPVLAN:Service provider VLAN(outer VLAN)

StatisHw:Statistics Hardware

Inp: Inprofile

OutP:Outprofile

Type	CVLAN	SPVLAN	Rate(Kbps)	Burst(KB)	StatisHw	Inp(Pkts)	Outp(Pkts)
------	-------	--------	------------	-----------	----------	-----------	------------

single	5	--	2048	128	YES	0	0
double	10	6	1024	64	YES	32,324	1,235
double	8	any	4096	256	YES	16,132	1.034

Step 3: Clear statistics of CVLAN 10 and SPVLAN 6

```
Raisecom(config)# clear double-tagging-vlan statistics outer 6 inner 10
```

```
Raisecom(config)#exit
```

```
Raisecom# show rate-limit vlan
```

CVLAN: Customer VLAN(inner VLAN)

SPVLAN:Service provider VLAN(outer VLAN)

StatisHw:Statistics Hardware

Inp: Inprofile

OutP:Outprofile

Type	CVLAN	SPVLAN	Rate(Kbps)	Burst(KB)	StatisHw	Inp(Pkts)	Outp(Pkts)
------	-------	--------	------------	-----------	----------	-----------	------------

single	5	--	2048	128	YES	0	0
double	10	6	1024	64	YES	0	0
double	8	any	4096	256	YES	16,132	1.034

Chapter 8 MAC Address Transmission Table Management

8.1 Brief introduction

8.1.1 MAC address transmission table

The Ethernet switch's main function is to transmit message in data link layer that is to transmit messages to the corresponding port according to the destination MAC address. MAC address transmission table is a two-ply table that contains MAC address and transmission port matchup, which is the base of the Ethernet switch transmitting layer-2 messages.

MAC address transmission table contains the following information:

- The destination MAC address;
- The VLAN ID belongs to the port;
- The transmission egress port number of the local equipment;

When the Ethernet switch is transmitting messages, according to the MAC address table information, the following way is available:

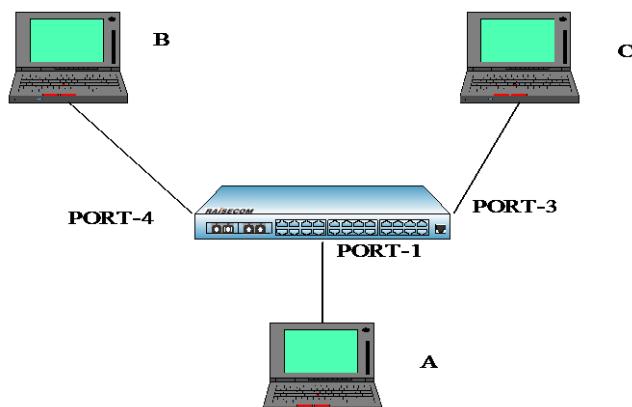
- Unicast: when there is table item that fits the message destination MAC address in the MAC address transmission table, the switch will transmit it directly from the transmission egress port of the table item;
- Broadcast: when the messages that the switch received from the destination address are all F, or when there is no table item that is accord with the message destination MAC address in the MAC address transmission table, the switch will use broadcast and transmit the message to all the ports except the receive ports.

8.1.2 MAC address learning

The table item in MAC address table can be upgraded and maintained through the following two ways:

- Manual configuration
- MAC address learning

Usually, most MAC address is created and maintained by the MAC address function. The Ethernet switch learning MAC address process is shown below:



Mac address learning

When User A need to communicate with User B in the same VLAN1, the message need to be sent to the switch's port 1, while the switch record the message's source MAC address, or User A's address 'MAC-A', to its own MAC address transmission table.

When the learning process is done, the switch will transmit the message. Because there is no MAC address and port table item, the switch will transmit the message to all the port except port 1 to confirm that User B could receive the message;

Because the switch use broadcast to transmit the message, both User B and User C will receive the message, while User C is not the destination equipment, so he will not process it. Normally, User B will respond User A by sending messages. When the response message is sent to port 4, the switch will use the same MAC address learning way and save User B's address and port corresponding relationship in the MAC address transmission table.

By this time there will be two table items in the switch's transmission table. When transmitting response message, because there has already been the table item that the destination is 'MAC-A' in the MAC address transmission table, the switch will no longer use broadcast, but send the message directly to User A through port 1 to accomplish the message interaction.

The way above is independent MAC address learning, or IVL, while there is another way for learning MAC address, that is share-VLAN MAC address learning, or SVL. By default, the switch use IVL mode, and SVL mode needs to be set in some cases.

8.1.3 MAC address table management

1. MAC address transmission table aging mechanism:

The switch MAC address transmission table has limitation in capacity, so it use aging mechanism to refresh the MAC address transmission table to make full use of the address transmission table resource. That is, the system open the aging timer when it is creating one table item dynamically, and if there is no more messages received from the MAC address of the table item in the aging time, the switch will delete the MAC address table item.

Notice:

- When 'destination MAC address refresh' function is enabled, if the switch transmits a message which the destination is one MAC address in the aging time, the MAC table item will be refreshed, and restart aging;

- MAC address aging mechanism is valid only to dynamic MAC address table item.

2. MAC address table sorts and features:

- Static MAC address table item: or 'permanent address', it is added or deleted by user, without aging. For a network in which the equipments change rarely, manually adding static address table item can reduce the network broadcast traffic.
- Dynamic MAC address table item: it stands for the MAC address table item that ages according to the aging time that user set. The switch could add dynamic MAC address table item through MAC address learning mechanism or user handwork.

8.2 MAC address transmission table management configuration

8.2.1 The default MAC address transmission table configuration

Function	Default value
----------	---------------

MAC address aging time	300s
MAC address learning feature	Enable
Static MAC address privilege	-1 (N/A in command lines)
Static MAC address MAC strategy	Transmit normally
Static MAC address no-speed-limit	enable

8.2.2 Static MAC address configuration

Step	Command	Description
1	config	Enter global configuration mode Set the static MAC address.
2	mac-address-table static unicast <i>HHHH.HHHH.HHHH vlan vlan_id port port-number</i>	<i>HHHH.HHHH.HHHH</i> : the static MAC address which will be set; format is hex, dotted notation for every four characters. <i>vlan_id</i> : range is 1-4094. <i>port_number</i> : the physical port number. Set the static MAC address.
3	mac-address-table static multicast <i>HHHH.HHHH.HHHH vlan vlan_id port port-list</i>	<i>HHHH.HHHH.HHHH</i> : is the static MAC address which will be set; format is hex, dotted notation for every four characters. <i>Vlan_id</i> range is 1-4094. <i>port_number</i> : the physical port number, use ',' or '-' to input the port list.
4	exit	Exit global configuration mode and enter privileged EXEC mode
5	show mac-address-table static <i>[port port-number vlan vlan_id]</i>	Show (port or VLAN) static address. <i>port_number</i> : physical port. <i>vlan_id</i> : range is 1-4094.

Notice:

- The switch MAC address, multicasting address, FFFF.FFFF.FFFF and 0000.0000.0000 can not be configured as the static MAC address.
- At present configurable static unicast MAC address amount are different on the devices.

8.2.3 MAC address aging time configuration

The dynamic source MAC address that the switch has learned will age when it is not in use. The aging time can be changed, and the MAC address aging can be disabled. By default, the aging time is 300s.

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode
2	mac-address-table aging-time {0 time}	Set the aging time of MAC address table. 0 stands for MAC address will not be aged <i>time</i> : the target MAC address aging time, unit is second, range is 10-1000000, and default value is 300.
3	exit	Quit global configuration mode and enter privileged EXEC mode
4	show mac aging-time	Show MAC address aging time

To restore the default value, use the command no: no mac-address-table aging-time.

8.2.4 MAC address learning enable/disable

Sometimes disable/enable a certain physical port learning MAC address is needed, which can be achieved by configuring the switch of MAC address learning ability. By default, every physical port can be allowed to learn MAC address.

Step	Command	Description
1	config	Enter global configuration mode.
2	mac-address-table learning {enable disable} port-list {all {1-MAX_PORT_NUM}}	Enable or disable the MAC address learning function of physical port. enable enable MAC address learning function. disable disable MAC address learning function. <i>MAX_PORT_NUM</i> the maximum port number that the equipment support
3	exit	Exit from global configuration mode to privileged EXEC mode.
4	show interface port [port-number]	Show port status. <i>port_number</i> physical port,range is 1-MAX_PORT_NUM.

8.2.5 Clear MAC address table

Clear layer-2 MAC address table entries of the switch, includes static and dynamic MAC address. The command can be used in global configuration mode.

Step	Command	Description
1	clear mac-address-table {all/dynamic/static}	<i>all</i> : delete all lay-2 MAC addresses in the MAC address table <i>dynamic</i> : delete dynamic lay-2 MAC addresses in the MAC address table <i>static</i> : delete static lay-2 MAC addresses in the MAC address table

8.2.6 Monitoring and maintaining

Use **show** to look over MAC address transmission table configuration:

Command	Description
show mac aging-time	Show MAC address aging time
show mac-address-table l2-address port port-number	Show the switch port MAC address <i>Port_number</i> physical port, range is 1~26
show mac-address-table l2-address vlan vlan_id	Show the switch port MAC address <i>vlan_id</i> VLAN ID, range is 1~4094
show mac-address-table l2-address count port port-number	Show the switch port MAC address number Count stands for the MAC address number related to the statistics <i>port_number</i> physical port number, range is 1~26.
show mac-address-table l2-address count	Show mac-address-table count
show mac-address-table l2-address count vlan vlan_id	Show the switch VLAN MAC address Count stands for the MAC address number related to the statistics <i>vlan_id</i> VLAN ID, range is 1~4094
show mac-address-table static	Show the switch static MAC address configuration information

Especially, the command for searching the information of a certain MAC address is in the switch.

Command	Description
	Search for MAC address
search mac-address HHHH.HHHH.HHHH	static MAC address which <i>HHHH.HHHH.HHHH</i> is to be set, format is hex, dotted notation for every four characters.

8.2.7 Typical configuration example

Note: RC551 device doesn't support this configuration.

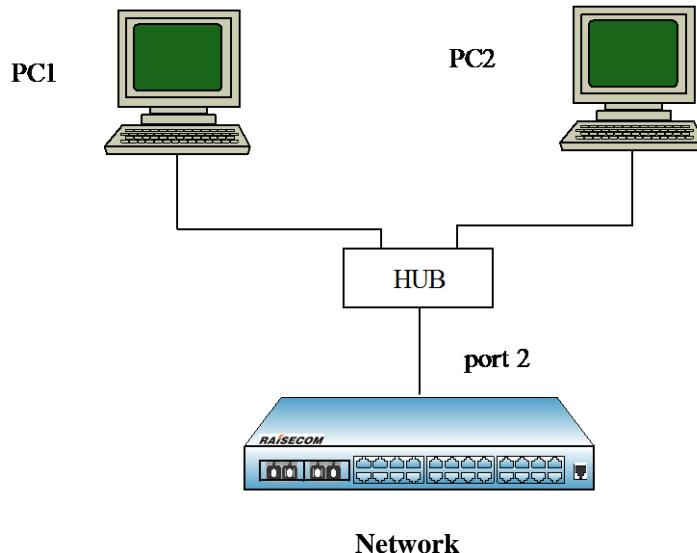
➤ Destination:

Enable all the ports' MAC address learning function of the switch;

Configure a static unicast MAC address 1234.1234.1234 in port 2, VLAN 10;

Set the aging time 100s, and observe the switch MAC address learning and aging situation.

➤ Network figure



➤ Configuration step

Step 1:

Enable all the ports' MAC address learning function

```
Raisecom(config)#mac-address-table learning enable port-list all
```

Step 2:

Set static unicast MAC address 1234.1234.1234.1234 in port 2, VLAN 10

```
Raisecom(config)#interface port 2
```

```
Raisecom(config-port)#switchport access vlan 10
```

```
Raisecom(config)#mac-address-table static unicast 1234.1234.1234 vlan 10 port 2
```

Step 3:

Set the aging time as 100s

```
Raisecom(config)#mac-address-table aging-time 100
```

We can notice that the switch can learn 2 dynamic MAC address through port 2, which age 100s later, then restart learning, while static MAC address will no age.

8.3 MAC address number limit

With MAC address learning function, the Ethernet switch can get the MAC address within the same network segment. To the message that is sent to the MAC addresses, the Ethernet switch use hardware for transmission through looking for MAC address transmission table to raise the transmission efficiency. If the MAC address transmission table is much too large, the time of looking for the corresponding transmission table item may be prolonged, and the switch transmission function will drop. By configuring the maximum MAC address number that the Ethernet port can learn, the administrator is able to control the MAC address transmission table item number that the Ethernet switch maintains. When the MAC address count that the port has learned rises to the maximum value that user set, the port will no longer learn MAC address.

Ethernet switches specify MAC-address-table threshold on a port, and don't limit other VLAN messages.

8.3.1 Configure the default MAC address number limit

By default, the MAC address learning number has no upper limit.

8.3.2 Configure the MAC address number

Note: RC551 device doesn't support this configuration.

Step	Command	Description
1	config	Enter global configuration mode
2	interface { port line client} <1-MAX_PORT_NUM>	Enter Ethernet physical port mode
3	mac-address-table threshold <PORT_MAC_MAX_THRESHOLD_STR>	Configure the MAC address learning upper limit <i>PORT_MAC_MAX_THRESHOLD_STR</i> value lower limit
4	no mac-address-table threshold	Configure mac-address-table upper limit as default value.
5	exit	Quit global configuration mode and enter privileged EXEC mode
6	show mac-address-table threshold port-list {1-MAX_PORT_NUM}	Show mac address table threshold value

8.3.3 Monitoring and maintaining

Command	Description
show mac-address-table threshold port-list {1-MAX_PORT_NUM}	Show mac address table threshold value
show mac-address /2	Show interface MAC address number that has been learned

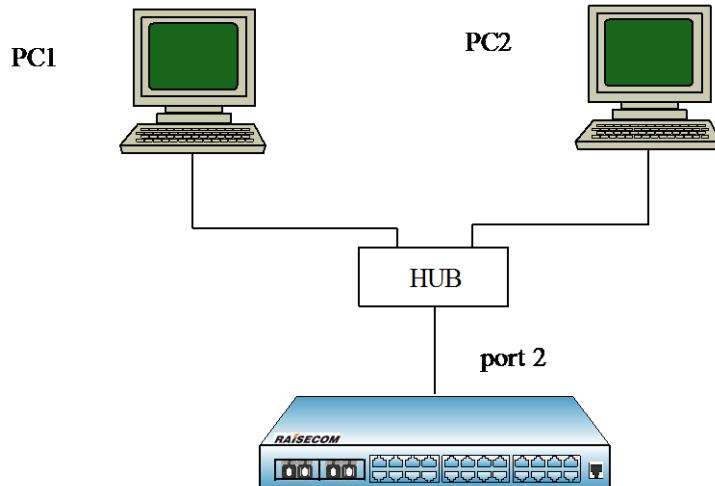
8.3.4 Typical configuration example

Note: RC551 device doesn't support this configuration.

➤ Destination

Configure the MAC address learning threshold of the switch port as 1, and the switch won't learn the dynamic MAC address that extend the threshold value.

➤ Network



Networking

- Configuration step

Step 1:

The upper limit of port 2 learning MAC address is 1

```
Raisecom(config)#interface port 2
```

```
Raisecom(config-port)#mac-address-table threshold 1
```

Step 2:

Show interface MAC address learning number:

```
Raisecom# show mac-address-table l2-address count port 1
```

Port 2 shows only 1 dynamic MAC is learned.

Step 3:

Cancel the MAC learning confirmation of port 2

```
Raisecom(config-port)#no mac-address-table threshold
```

Show MAC address learning count:

```
Raisecom# show mac-address-table l2-address count port 2
```

There are 2 dynamic MAC that has been learned on port 2.

Chapter 9 Physical Layer Interface

9.1 Physical ports features

For a switch, whatever the equipment is, physical interface is necessary for connection. And physical ports have many features, any message that is entering or leaving the switch needs physical ports to transmit, so the function of physical port is relatively more difficult, which is also very important; to some of the function manual configuration is available, like port rate, duplex mode, negotiation mode, crossover cable automatic recognition and system maximum transmission unit, all of which are the features of the physical ports. To the certain use, the corresponding setting is needed for the physical port to receive or transmit messages.

9.2 The default values

By default, the physical port commands are shown below:

Command	Default value
Rate configuration	The rate of electronic port and 100M optical port is auto negotiated, 100M optical port rate is 100M by default
Duplex mode configuration	The rate of electronic port and 100M optical port is auto negotiated, 100M optical port in duplex is full duplex
Rate control configuration	Physical port rate control function is off
Crossover Ethernet cable auto-recognition and straight Ethernet cable function	Normal mode
Port maximum transmission unit	2048 byte
Interface description	port <i>port-number</i>
Interface on/off configuration	on
Dynamic statistical refresh frequency	2s

9.3 Rate and duplex mode

Gigabit port is always working in 1000Mbps and full duplex mode. When auto negotiation function is enabled, the duplex mode (speed) will be set according to the result auto negotiation. In default situation, auto negotiation is enabled for all the electronic ports and 1000M optical port, only the default value of 100M optical port is 100M/FD.

Rate and duplex mode configuration step is shown below:

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode.
2	interface port <i>port-number</i>	Enter Ethernet physical interface configuration mode or physical interface range configuration mode.
2	interface range <i>port-list</i>	<i>port_number</i> is the physical interface, range is 1-26. <i>port-list</i> range is 1-26, use “,” and “-“for multiple interfaces configuration.
3	speed { <i>auto/10/100/1000</i> }	Set the speed and duplex mode of the port.
3	duplex { <i>full/half</i> }	<i>auto</i> : represents that both the speed and duplex are set according to the result of auto negotiation. <i>10</i> : represents that the speed is set to 10Mbps. <i>100</i> : represents that the speed is set to 100Mbps. <i>1000</i> : represents that the speed is set to 1000Mbps. <i>full</i> : set the duplex mode to full duplex. <i>half</i> : set the duplex mode to half duplex.
4	exit	Exit from Ethernet physical interface configuration mode to global configuration mode.
5	exit	Exit from global configuration mode to privileged EXEC mode
6	show interface port <i>port-number</i>	Show the status for the port. <i>port_number</i> physical port, range is 1-26.

Note:

- Using the Ethernet interface configuration mode **speed auto**, the rate and duplex mode will be restored to auto negotiation by default.
- Different ports fit different rate and duplex mode. 100M electronic ports can not be set to 1000M, 100M optical port can be set to 100M/FD only, 1000M optical port can be only configured 1000M/FD/auto, while extended card port can not be configured rate and duplex mode when the extended card does not exist.

Example 1: Set the speed of port 15 to 10Mbps in full-duplex mode.

Raisecom#**config**

Raisecom (config)#**interface port** *15*

Raisecom (config-port)#**speed** *10*

Raisecom (config-port)# **duplex** *full*

Raisecom (config-port)#**exit**

Raisecom (config)#**exit**

Raisecom#**show interface port** *15*

R: Receive Direction

S: Send Direction

<i>Port</i>	<i>Admin</i>	<i>Operate</i>	<i>Speed/Duplex</i>	<i>Flowcontrol(R/S)</i>	<i>Mac-learning</i>
-------------	--------------	----------------	---------------------	-------------------------	---------------------

<i>15</i>	<i>enable</i>	<i>down</i>	<i>10/full</i>	<i>off/off</i>	<i>enable</i>
-----------	---------------	-------------	----------------	----------------	---------------

Example 2: Set the rate of 100M optical port to 10Mbps in half-duplex mode.

Raisecom#**config**

Raisecom(config)#**interface port 1**

Raisecom(config-port)#**speed 10**

Port 1 only supports 100M/FD!

Raisecom(config-port)# **duplex half**

Port 1 only supports 100M/FD!

Example 3: Set 1000M optical port P2 to 100Mbps in half-duplex mode

Raisecom#**config**

Raisecom(config)#**interface port 2**

Raisecom(config-port)#**speed 100**

Port 2 only supports 1000M/FD or auto-negotiation!

Raisecom(config-port)# **duplex half**

Port 2 only supports 1000M/FD or auto-negotiation!

Example 4: Set 100M electronic port P3 to 1000Mbps

Raisecom#**config**

Raisecom(config)#**interface port 3**

Raisecom(config-port)#**speed 1000**

Port 3 does not support 1000M!

Example 5: Set extended card P25 to 1000Mbps

Raisecom#**config**

Raisecom(config)#**interface port 25**

Raisecom(config-port)#**speed 1000**

Port 25 is unavailable.

9.4 IEEE 802.3X flow control

In ISCOM2128EA-MA product, receive and send cannot be set separately.

The flow control function of Raisecom series switches is set on both RX and TX direction separately. By default, flow control function is disabled on all ports. For the sub-card ports, if no sub-card, flow control command fails.

Step	Command	Description
1	config	Enter global configuration mode

		Enter Ethernet physical interface configuration mode or range configuration mode.
2	interface port <i>port-number</i>	<i>port_number</i> physical ports, range is 1-26.
	interface range <i>port-list</i>	<i>port-list</i> , range is 1-26, use “;” and “-“ for multiple ports.
		Enable/disable the flow control function on RX and TX direction.
3	flowcontrol { <i>on/off</i> }	<i>on</i> : enable the flow control function of the port. <i>off</i> : disable the flow control function of the port.
4	exit	Exit from the physical interface configuration mode and enter global configuration mode.
5	exit	Exit from global configuration mode and enter privileged EXEC mode.
6	show interface port <i>port-number</i>	Show the traffic control of the port. <i>port_number</i> physical port number, range is 1-26.

Example 1: Set port 10 flow control function on.

Raisecom#config

```
Raisecom(config)# interface port 10
Raisecom(config-port)#flowcontrol receive on
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show interface port 10
```

R: Receive Direction

S: Send Direction

Status: Forwarding status

<i>Port</i>	<i>Admin</i>	<i>Operate</i>	<i>Speed/Duplex</i>	<i>Flowctr(R/S)</i>	<i>Maclearn</i>	<i>Status</i>
10	enable	down	auto	on/on	enable	Forward

Example 2: Set port 25 (no sub-card) flow control function on.

Raisecom#config

```
Raisecom(config)#interface port 25
```

Raisecom(config-port)# **flowcontrol on**

Port 25 is unavailable!

The flow control function on both RX and TX direction is set separately. By default, flow control function is disabled on all ports.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>port-number</i>	Enter Ethernet physical interface configuration mode

	interface range <i>port-list</i>	or range configuration mode.
		<i>port_number</i> physical ports, range is 1-26.
		<i>port-list</i> , range is 1-26, use ‘,’ and ‘-’ for multiple ports.
		Enable/disable the flow control function on RX and TX direction.
3	flowcontrol {receive/send}{on/off}	Send represents the traffic control function at TX direction. <i>receive</i> : represents the traffic control function at RX direction. <i>on</i> : enable the flow control function of the port. <i>off</i> : disable the flow control function of the port.
4	exit	Exit from the physical interface configuration mode and enter global configuration mode.
5	exit	Exit from global configuration mode and enter privileged EXEC mode.
6	show interface port <i>port-number</i>	Show the traffic control of the port. <i>port_number</i> physical port number, range is 1-26.

Example 1: Set the flow control for port 10.

```
Raisecom#config
```

```
Raisecom (config)# interface port 10
```

```
Raisecom (config-port)#flowcontrol receive on
```

```
Raisecom (config-port)#exit
```

```
Raisecom (config)#exit
```

```
Raisecom#show interface port 10
```

R: RX Direction

S: tx Direction

Port	Admin	Operate	Speed/Duplex	Flowcontrol(R/S)	Mac-learning	Status
------	-------	---------	--------------	------------------	--------------	--------

10	enable	down	auto	on/off	enable	Forward
----	--------	------	------	--------	--------	---------

For some equipments, the flow control situation of the ports' receiving direction and sending direction is configured respectively, but the result take effect at the same time, that is to say, changing the flow control setting of any direction will effect the flow control configuration of both side, on or off at the same time. By default all the ports' flow control is off.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>port-number</i> interface range <i>port-list</i>	Enter physical port mode or interface range configuration mode. <i>port_number</i> physical port number, range is 1-26 <i>port-list</i> port list, range is 1-26, use ‘,’ and ‘-’ for

		multiple setting.
		Configure physical port flow control function on/off
3	flowcontrol <i>{receive/send}{on/off}</i>	send strands for the flow control function of the sending direction; receive strands for flow control function of the receiving direction; on enable interface flow control function; off disable interface flow control function
4	exit	Quit physical port configuration mode and enter global configuration mode
5	exit	Quit global configuration mode and enter privileged EXEC mode
6	show interface port <i>port-number</i>	Show interface flow control state; <i>port_number</i> physical port number.

For example: set port 10 flow control function on receiving direction to on.

Raisecom#**config**

Raisecom(config)# **interface port 10**

Raisecom(config-port)#**flowcontrol receive on**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show interface port 10**

R: Receive Direction

S: Send Direction

Status: Forwarding status

Port	Admin	Operate	Speed/Duplex	Flowctr(R/S)	Maclearn	Status
10	enable	down	auto	on/on	enable	Forward

9.5 Auto-MDIX

The function of Auto-MDIX is to auto-recognize crossover Ethernet cable and straight Ethernet cable.
The configuration step is show below:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>port-number</i> interface range <i>port-list</i>	Enter physical port mode or interface range configuration mode; <i>port_number</i> physical interface number; <i>port-list</i> port list, use ‘,’ and ‘-’ for multiple setting.
3	mdi (<i>auto /normal /across</i>)	Configure port MDI mode;

		auto linear ordering auto reserve mode
		normal normal mode
		across cross mode
4	exit	Quit physical port configuration mode and enter global configuration mode
5	exit	Quit global configuration mode and enter privileged EXEC mode
6	show mdi [<I-MAX_PORT_STR>]	Show port MDI state <I-MAX_PORT_STR>: physical port

For example: Set Auto-MDIX function to auto mode on port 8.

```
Raisecom#config
Raisecom(config)# interface port 8
Raisecom(config-port)#mdi auto
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show mdi 8
```

Port 8 MDI mode :auto Current status :across

9.6 mtu

Step	Command	Description
1	config	Enter global configuration mode
2	system mtu <1522-9000>	Set maximum transmission unit;
	system mtu <MIN_FRAME_LEN_STR-MAX_FRAME_LEN_STR>	<1522-9000> system maximum transmission unit range; Delete maximum transmission unit configuration
3	exit	Quit global configuration mode and enter privileged EXEC mode
4	show system mtu	Show system maximum transmission unit configuration

The command of **no system mtu** is used to delete maximum transmission unit configuration.

For example: Set system maximum transmission unit to 5000.

```
Raisecom#config
Raisecom(config)# system mtu 5000
Raisecom(config)#exit
Raisecom#show system mtu
System MTU size: 5000 bytes
```

9.7 Add description for interfaces

Description of the Physical port can be added. The command of **no description** can restore the default configuration.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>port-number</i> interface range <i>port-list</i>	Enter physical layer port configuration mode or volume configuration mode <i>port_number</i> : physical port number, range is 1-26
3	[no]description <i>WORD</i>	Add physical port or IP interface description <i>WORD</i> : specify class-map description. 64 character the most, can not be separated by space.
4	exit	Quit physical layer port configuration mode and enter global configuration mode.
5	exit	Quit global configuration mode and enter privileged EXEC mode.
6	show interface port [<1-MAXPORT>] description	Show port description <1-MAXPORT> port number.

Example 1: add description for physical port 8.

```
Raisecom#config
Raisecom(config)# interface port 8
Raisecom(config-port)# description this-is-a-port
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show interface port 8 detail
Port      Description
-----
8        this-is-a-port
```

9.8 Open and close physical layer port

Sometimes, for a certain intention, to close physical ports is needed, and configuring the ports' on/off is necessary. By default all the ports are on. To extended card port, physical ports on/off commands are invalid when the card is not inserted.

Step	Command	Description
1	config	Enter global configuration
2	interface port <i>port-number</i> interface range <i>port-list</i>	Enter physical layer port configuration mode or volume configuration mode. <i>port_number</i> physical port number.

		<i>port-list</i> port list, use ‘,’ and ‘-’ to make multi-port input.
3	{shutdown no shutdown}	Close or open physical port. shutdown stands for closing physical port. no shutdown stands for opening physical port.
4	exit	Quit physical layer interface configuration mode and enter global configuration mode
5	exit	Quit global configuration mode and enter privileged EXEC mode.
6	show interface port <i>port-number</i>	Show port state <i>port_number</i> physical port number.

Example 1: Close port 20.

Raisecom#**config**

Raisecom(config)# **interface port 20**

Raisecom(config-port)#**shutdown**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show interface port 20**

R: Receive Direction

S: Send Direction

<i>Port</i>	<i>Admin</i>	<i>Operate</i>	<i>Speed/Duplex</i>	<i>Flowctr(R/S)</i>	<i>Maclearn</i>	<i>Status</i>
-----	-----	-----	-----	-----	-----	-----
20	<i>enable</i>	<i>down</i>	<i>auto</i>	<i>off/off</i>	<i>enable</i>	<i>Forward</i>

Example 2: Close extended card port P25 (not extended card inserted)

Raisecom#**config**

Raisecom(config)#**interface port 25**

Raisecom(config-port)# **shut down**

Port 25 is unavailable!

9.9 Clear interface statistics

Step	Command	Description
1	config	Enter global configuration
2	clear interface {port <i>port-num/ client / line } statistics</i>	Cear interface statistics <i>port-num:</i> port number

Example 1: Clear statistica on port 8.

Raisecom#**config**

Raisecom(config)**clear interface port 8 statistics**

Set successfully

9.10 Dynamic statistics time

Dynamic statistics time is defaulted to 2s.

Step	Command	Description
1	config	Enter global configuration
2	dynamic statistics time <2-300>	Set dynamic statistics time
3	exit	Quit global configuration mode
4	show interface port <i>portid</i> statistics dynamic	Show dynamic statistics on the ports

The command of **no dynamic statistics time** can restore the default value (2s).

9.11 Monitoring and maintaining

Use **show** to show port state.

Step	Command	Description
1	show interface port <i>port-number</i>	Show port state <i>port_number</i> physical port number.
2	show interface port [<1-MAXPORT>] description	Show port information. <1-MAXPORT> port number.
3	show interface port [<1-MAXPORT>] statistics	Show interface statistics
4	show interface port <i>portid</i> statistics dynamic [detail]	Show interface dynamic statistics

For example: Show port 8 state.

Raisecom#**show interface port 8**

R: Receive Direction

S: Send Direction

Status: Forwarding status

Port	Admin	Operate	Speed/Duplex	Flowctr(R/S)	Maclearn	Status
------	-------	---------	--------------	--------------	----------	--------

8	enable	down	auto	off/off	enable	Forward
---	--------	------	------	---------	--------	---------

Raisecom#**show interface port 8 descriptor**

<i>Port</i>	<i>Description</i>
<hr/>	
8	<i>this-is-a-port</i>

9.12 Typical configuration

1. Show Port 9 statistics.

Raisecom#show interface port 9 statistics

<i>Port</i>	<i>9</i>
<hr/>	
<i>Input Normal Statistics:</i>	
<i>InOctets:</i>	15,960
<i>InUcastPkts:</i>	183
<i>InMulticastPkts:</i>	0
<i>InBroadcastPkts:</i>	10
<i>Input Error Statistics:</i>	
<i>DropEvents(Pkts):</i>	0
<i>CRCAccAlignErrors(Pkts):</i>	0
<i>UndersizePkts:</i>	0
<i>OversizePkts:</i>	0
<i>Fragments(Pkts):</i>	0
<i>Jabbers(Pkts):</i>	0
<i>Collisions(Pkts):</i>	0
<i>Output Normal Statistics:</i>	
<i>OutOctets:</i>	12,846
<i>OutUcastPkts:</i>	164
<i>OutMulticastPkts:</i>	0
<i>OutBroadcastPkts:</i>	1
<i>Output Error Statistics:</i>	
<i>OutputError(Pkts):</i>	0
<i>OutputDiscard(Pkts):</i>	0
<i>Abort(Pkts):</i>	0
<i>Differred(Pkts):</i>	0
<i>LateCollisions(Pkts):</i>	0
<i>NoCarrier(Pkts):</i>	0
<i>LostCarrier(Pkts):</i>	0
<i>MacTransmitError(Pkts):</i>	0
<i>Bit Statistics:</i>	
<i>Ingress Bits:</i>	127,680
<i>Egress Bits:</i>	102,768

2. Set dynamic statistics time as 10s on port 5.

Raisecom#config

```
Raisecom(config)#dynamic statistics time 10
Raisecom(config)#exit
Raisecom#show interface port 5 statistics dynamic
  Dynamic statistics period: 10 seconds
    Port      5
    -----
    Input Normal Statistics:
      InOctets:          15,960
      InUcastPkts:       183
      InMulticastPkts:   0
      InBroadcastPkts:   10
    Output Normal Statistics:
      OutOctets:          12,846
      OutUcastPkts:       164
      OutMulticastPkts:   0
      OutBroadcastPkts:   1
    Bit Statistics:
      Ingress Bits:       127,680
      Egress Bits:        102,768
    Speed during 10 seconds Statistics:
      Ingress Speed(bps): 12700
      Egress Speed(bps):  10270
      Ingress Speed(pps): 18
      Egress Speed(pps):  15
Please press <Ctrl+C> to stop.
```

3. Restore dynamic statistics time to default value on port 12.

```
Raisecom#config
Raisecom(config)#no dynamic statistics time
Raisecom(config)#exit
Raisecom#show interface port 12 statistics dynamic detail
  Dynamic statistics period: 2 seconds
    Port      12
    -----
    Input Normal Statistics:
      InOctets:          15,960
      InUcastPkts:       183
      InMulticastPkts:   0
      InBroadcastPkts:   10
    Input Error Statistics:
      DropEvents(Pkts):   0
      CRCAlignErrors(Pkts): 0
      UndersizePkts:      0
```

<i>OversizePkts:</i>	0
<i>Fragments(Pkts):</i>	0
<i>Jabbers(Pkts):</i>	0
<i>Collisions(Pkts):</i>	0
<i>Output Normal Statistics:</i>	
<i>OutOctets:</i>	12,846
<i>OutUcastPkts:</i>	164
<i>OutMulticastPkts:</i>	0
<i>OutBroadcastPkts:</i>	1
<i>Output Error Statistics:</i>	
<i>OutputError(Pkts):</i>	0
<i>OutputDiscard(Pkts):</i>	0
<i>Abort(Pkts):</i>	0
<i>Differred(Pkts):</i>	0
<i>LateCollisions(Pkts):</i>	0
<i>NoCarrier(Pkts):</i>	0
<i>LostCarrier(Pkts):</i>	0
<i>MacTransmitError(Pkts):</i>	0
<i>Bit Statistics:</i>	
<i>Ingress Bits:</i>	127,680
<i>Egress Bits:</i>	102,768
<i>Speed during 2 seconds Statistics:</i>	
<i>Ingress Speed(bps):</i>	63800
<i>Egress Speed(bps):</i>	51300
<i>Ingress Speed(pps):</i>	93
<i>Egress Speed(pps):</i>	82

Please press <Ctrl+C> to stop.

Chapter 10 Storm Control

10.1 Brief introduction

A packet storm occurs when a large number of broadcast, unicast, or DLF packets are received on a port. Forwarding these packets can cause the network to slow down or to time out. Storm control is configured for the switch as a whole but operates on a per-port basis. By default, storm control is enabled.

Under storm-control, the largest flow of various packets must be the same. AS long as one packet threshold is changed, other packets threshold will also be changed.

10.2 The default configuration

By default, storm control is enabled for unicast DLF packets, broadcast packets and mulicast packets.

10.3 Storm control function configuration

10.3.1 Enable/disable storm control function

The configuration is to enable/disable storm control

Step	Command	Description
1	config	Global configuration mode
2	storm-control {broadcast / multicast / dlf / all} {enable / disable}	Enable/disable broadcast packet, multicast packet and DLF packet Broadcast DLF broadcast packet Multicast DLF multicast packet Dlf DLF packet All broadcast, multicast and DLF unicast packets.
3	exit	Quit global configuration mode and enter privileged EXEC mode
4	show storm-control	Show storm control state

10.3.2 Storm control number

Configure storm control threshold, unit is pps (packet per second).

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode
2	storm-control bps value	Set storm control threshold. Value: kbit number that is allowed to pass per second.
3	exit	Quit global configuration mode and enter privileged EXEC mode.
4	show storm-control	Show storm control state.

10.4 Monitoring and maintaining

Command	Description
show storm-control	Show storm control state.

10.5 Typical configuration example

Example 1: Disable storm control to broadcast packet

```
Raisecom#config
Raisecom(config)# storm-control broadcast disable
Raisecom(config)#exit
Raisecom#show storm-control
  Broadcast: Disable
  Multicast: Enable
  Unicast destination lookup failed(DLF): Enable
  Threshold: 1024 pps
```

Example 2: Set storm control threshold to 200kbps.

```
Raisecom#config
Raisecom(config)# storm-control bps 200
Raisecom(config)#exit
Raisecom#show storm-control
  Broadcast: Disable
  Multicast: Enable
  Unicast destination lookup failed(DLF): Enable
  Threshold: 200Kbps
```

Chapter 11 Layer-two Protocol Relay

11.1 Brief principle

QinQ offers a relatively simple layer-two VPN tunnel, by packaging outer layer VLAN Tag of user's private network message, so that the message is able to go through the operator's backbone network with layer-two Tag. Based on this, with layer-two protocol transparent transmission function, the layer-two protocol of the user's network can go through the operator's network, so that the same user network of the different places can run layer-two protocol in uniform.

Usually layer-two protocol transparent transmission is carried out by the operator's network edge switch. Transparent transmission function starts on the port that connects the operator's network edge switch and user network. The port exchange mode is access mode or dot1 q-tunnel mode, while the user switch port that is connected with it is trunk mode or hybrid mode. User network's layer-two protocol message, coming from the transparent transmission port, enters operator's network after being packaged by operator edge switch (message input interface). Then decapsulation will be done by the edge switch and the message will be transmitted to user network.

Transparent transmission function includes message packaging and decapsulation, the basic principle is shown below:

- Message encapsulation: in the message input side, the equipment will change the destination MAC address of layer-two protocol message from user network into special broadcast MAC address (default value 010E.05E00.0003). In operator network, the modified message will be transmitted in the user's VLAN as data message.
- Message decapsulation: in the message output side, the equipment will recognize the message that the destination MAC address is special broadcast MAC address (default value is 010E.5E00.0003), and revert the destination MAC address to the source destination MAC address of layer-two protocol message, then send the message to the given user network.

Layer-two protocol transparent transmission function can run with QinQ function or work respectively. But in actual, after the protocol message MAC address being modified, it still need to be covered with outer Tag to go through the operator network.

11.2 Basic configuration

Layer-two transparent transmission configuration includes: transparent transmission protocol enable/disable, transparent transmission message destination MAC address, COS value, the specified VLAN, the specified output port, message lost limit and port off limit. Configuring specified VLAN can make the transparent transmission message be transmitted by the specified VLAN, not the input VLAN; configuring the specified output port, can make the transparent transmission message being transmitted by only the given output port.

11.2.1 Default configuration

Function	Default value
----------	---------------

Enable/disable relay	Disable
Message destination MAC address	010E.5E00.0003
Message COS	5
Specified VLAN	No specified VLAN
Specified output port	No specified output port
Message package lost limit	No limit
Message port disabled limit	No limit

11.2.2 Relay configuration

By the following step, transparent transmission message destination MAC address, message COS value, the specified output port and VLAN can be configured, and enable/disable layer-two protocol transparent transmission function is available.

Step	Command	Description
1	config	Enter global configuration mode
2(optical)	relay destination-address HHHH.HHHH.HHHH	Configure transparent transmission message destination MAC address, transparent transmission message destination MAC address must be broadcast address, and can not take 0x0180C2 or 010E.5E00.0003 as front
3 (optional)	relay cos <0-7>	Set transparent transmission COS value, range is 0-7
4	interface port portid	Enter Ethernet physical port mode
5	relay port portid	Set transparent transmission specified output port, range is 1-MAX port number.
6	relay vlan <1-4094>	Set transparent transmission message specified VLAN, range is 1-4094.
7	relay {stp/ dot1x / lacp / all}	Enable/disable port layer-two transparent transmission function, all stands for all layer-two protocols that support transparent transmission.
8	exit	Return to global configuration mode
9	exit	Return to privileged EXECmode
10	show relay	Show transparent transmission function configuration and state
11	write	Save current system configuration

The command of **no relay destination-address** reverts relay destination MAC address to default value 010E.5E00.0003. Via **no relay cos** clears transparent transmission message specified VLAN,

that is the not specified VLAN. By **no relay{stp/dot1x/lacp/gmrp/gvrp/all}** closes layer-two protocol transparent transmission function.

Notice:

- Transparent transmission message input equipment and output equipment need to configure the same transparent transmission message destination MAC address, that is to say, to cooperate with other manufacturers, it is needed to keep the equipment transparent transmission message destination MAC address to stay the same. Transparent transmission message destination MAC address must be broadcast address, and can not begin with 0x0180c2 or 0x010E5E, but can be set to 010E.5E00.0003.
- Transparent transmission message COS value range is 0-7. Usually, transparent transmission protocol message PRI should be higher than ordinary data message.
- Transparent transmission specified output port can be any port of the equipment (except source port). User needs to make sure port VLAN attribution correct by configuration, or the message transparent transmission will fail.
- Transparent transmission specified VLAN value range is 1-4094. If this VLAN has not been created, transparent transmission message real-time transmission fails. So, when configuring specified VLAN, it is necessary to create and enable the VLAN on the equipment.
- To start layer-two protocol transparent transmission, it is needed to disable the corresponding protocols. To enable STP transparent transmission, closing STP protocol is needed.
- On the same equipment, when both the protocol message input port and output port transparent transmission function is enabled, the destination MAC address of protocol message will not be modified.

11.2.3 Layer-two protocol transparent transmission speed limit configuration

To configure transparent transmission message lost threshold and port off threshold, follow the steps below:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter Ethernet physical port mode
3	relay drop-threshold {stp / dot1x / lacp } <1-4096>	Set transparent packet drop-threshold, value range is 1-4096 PDUs/sec.
4	relay shutdown-threshold {stp / dot1x / lacp } <1-4096>	Set transparent packet shutdown-threshold, value range is 1-4096 PDUs/sec.
5	exit	Return to global configuration mode
6	exit	Return to privileged EXEC mode
7	show relay	Show transparent transmission configuration and state
8	write	Save the current configuration of the system

no relay drop-threshold{stp/dot1x/lacp}: revert transparent transmission protocol packet lost default configuration. **no relay shutdown-threshold{stp/dot1x/lacp}:** revert transparent transmission protocol port close threshold to default configuration, use **no relay shutdown** to enable the port.

Notice:

- Transparent transmission message packet lost threshold and port close threshold value range is 1-4096, usually, packet lost threshold should be less than port close threshold.
- After port transparent transmission function is enabled, if message receiving rate exceeds port close threshold, or if the port receives the message of specified destination MAC address, the

port will be closed. When the port is closed because of transparent transmission function, use **no relay shutdown** to enable the port.

11.2.4 Layer-two protocol transparent transmission message statistics clear

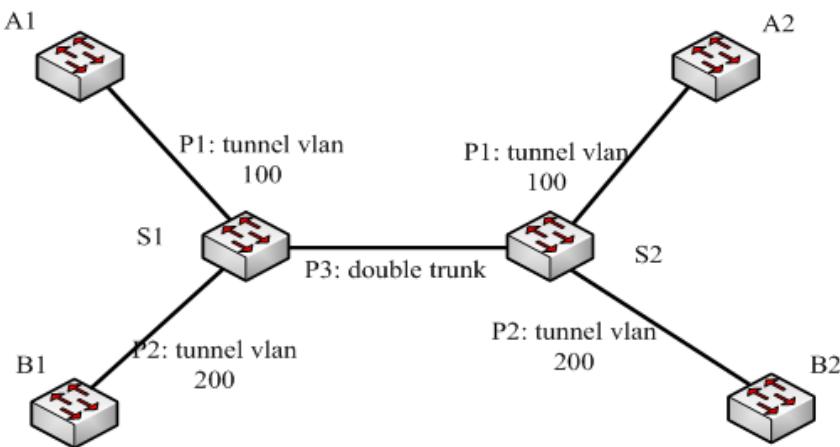
Follow the step below to clear transparent transmission message statistics

Step	Command	Description
1	config	Enter global configuration mode
2	clear relay statistics [port-list <i>port-list</i>]	Clear relay statistics
3	exit	Return to privileged EXEC mode
4	show relay statistics	Show transparent transmission stat. information.

11.2.5 Monitoring and maintaining

Command	Description
show relay [port-list <i>port-list</i>]	Show transparent transmission configuration and state
show relay statistics [port-list <i>port-list</i>]	Show transparent transmission message stat. information
show relay transparent	Show BPDUs transparent information.

11.2.6 Typical configuration example



Transparent transmission basic function configuration

S1, S2 configuration is the same. S1 configuration is shown below:

- 1) Create VLAN

Raisecom(config)#**create vlan 100 active**

Raisecom(config)#**create vlan 200 active**

2) Set port 1 to access mode, ACCESS VLAN to 100, enable STP protocol relay and set STP relay drop-threshold to 1500.

```
Raisecom(config)# interface port 1  
Raisecom(config-port)#switchport mode access  
Raisecom(config-port)#switchport access vlan 100  
Raisecom (config-port)#relay stp  
Raisecom(config-port)#relay drop-threshold stp 1500  
Raisecom (config-port)#exit
```

3) Set port 2 to access mode, ACCESS VLAN to 200, enable STP protocol relay and set STP relay drop-threshold to 1000.

```
Raisecom(config)# interface port 2  
Raisecom(config-port)#switchport mode access  
Raisecom(config-port)#switchport access vlan 200  
Raisecom (config-port)#relay stp  
Raisecom(config-port)#relay drop-threshold stp 1000  
Raisecom (config-port)#exit
```

4) Set port 3 to trunk mode.

```
Raisecom(config)# interface port 3  
Raisecom(config-port)# switchport mode trunk  
Raisecom (config-port)#exit
```

Chapter 12 Layer-3 Interface Configuration

This chapter focuses on introducing how to configure and maintain layer-3 interface in the switch, including the following contents:

- ❖ Layer-3 interface overview
- ❖ Layer-3 interface configuration
- ❖ Layer-3 interface description information configuration
- ❖ Monitoring and maintenance
- ❖ Typical configuration example
- ❖ Layer-3 interface configuration trouble shooting

12.1 Layer-3 interface overview

Layer-3 interface of ISCOM switch is virtual interface configuration based on VLAN and used for network device management. The VLAN with routing function can be configured a connected virtual layer-3 interface. The layer-3 interface shows up in the form of IP address, every layer-3 interface has an IP address and connects at least one VLAN.

12.2 Layer-3 interface configuration

At present, layer-2 ISCOM series switch can be configured 15 virtual layer-3 interfaces within the limits of 0-14; layer-3 ISCOM series switch can be configured 63 virtual layer-3 interfaces within the limits of 0-62.

The steps to create layer-3 interface and configure IP address are shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	Interface ip <0-ifNum>	Enter Ethernet layer-3 interface configuration mode
3	ip address ip-address [ip-mask] vlanlist	Configure the IP address of layer-3 interface and connected static VLAN ID
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface ip	Show the IP address of layer-3 interface, subnet mask and static VLAN ID configuration information

Use the command **no interface ip A.B.C.D** to delete the IP address configuration of layer-3 interface in IP interface configuration mode.

12.3 Layer-3 interface description information configuration

Users can set designated layer-3 interface description information through **description** command. The steps to add interface description information in layer-3 interface configuration mode are as below:

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip <0-ifNum>	Enter Ethernet layer-3 interface configuration mode
3	description WORD	Configure layer-3 interface description information
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface ip <0-ifNum> description	Show designated layer-3 interface description information

Note: Layer-3 interface description information allows a maximum length of 64 characters and cannot be separated by spaces.

Use the command **no description** to delete the configured interface description information in layer-3 interface configuration mode and return to the default configuration.

12.4 Configuration of layer-3 interface management message COS value

Configure management message priority (modify the cos value in layer-3 management message with tag, such as arp message, SNMP message and trap message):

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip <0-ifNum>	Enter Ethernet layer-3 interface configuration mode
3	Ip COS <0-7>	Configure layer-3 interface management message COS value
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip <0-ifNum> cos	Show designated layer-3 interface COS value information

Note: Default value: 0.

12.5 Acquisition of layer-3 interface statistics information

Users can check the designated layer-3 interface statistic information through **show interface ip <0-MAX_SW_STR> statistics** command.

Step	Command	Description
1	show interface ip <0-MAX_SW_STR> statistics	Acquire IP interface statistic information in privileged EXEC mode

Note: Part of layer-3 interface statistic information is related to RMON module, when RMON is close, the abnormal input data value will be incorrect.

12.6 Acquisition of layer-3 interface COS value

Users can check the designated layer-3 interface COS value through **show ip <0-MAX_SW_STR> cos** command.

Step	Command	Description
1	show ip <0-MAX_SW_STR> cos	Acquire IP interface cos value in privileged EXEC mode

12.7 Monitoring and maintenance

Use the command **show interface ip** to show layer-3 interface configuration information in privileged EXEC mode. Users can check the configuration effect through the information.

Command	Description
show interface ip	Show the configuration information of IP address, subnet mask and static VLAN ID for layer-3 interface
show interface ip description	Show layer-3 interface description information
Show ip <0-MAX_SW_STR> cos	Show COS configuration information

12.8 Typical configuration example

The configured IP address of ISCOM switch IP interface 1 is 20.0.1.4, subnet mask is 255.255.255.0. Connecting to VLAN1 and set interface description information as interface-No1, COS value is 5.

Raisecom #config

Raisecom (config)#**interface ip 1**

Raisecom (config-ip)#**ip address 20.0.1.4 255.255.255.0 1**

Raisecom (config-ip)#**description interface-No1**

Raisecom (config-ip)#**ip cos 5**

12.9 Layer-3 interface configuration trouble shooting

Fault: ISCOM switch failed to ping the straight-connected host.

Fault removal:

Step 1: Check whether the switch configuration is correct. Use **show arp** command to check whether there is ARP table entry of host in the switch ARP table.

Step 2: Check to the VLAN of switch port that is connected to host, whether it belongs to configured IP interface and whether the IP address and host IP are in the same network segment.

Step 3: If the configuration is correct, try to open ARP debug switch to check whether the switch transmits and receives ARP message correctly. There is something wrong with the Ethernet physical layer if the switch can only transmit ARP message but failed to receive.

Chapter 13 Link Aggregation

13.1 Basic principle

Link aggregation is to combine several physical Ethernet port into a logical aggregation group. Use the upper class entity of link aggregation service to take the physical links in the same aggregation group as a logical link.

Link aggregation is able to achieve egress/ingress load-sharing among the aggregation member port to increase bandwidth. At the same time, the member ports of the same aggregation group will dynamically backup each other, which increase the connection stability.

In the same link aggregation, members group able to achieve egress/ingress load-sharing must have a consistent configuration. These configurations include STP, QoS, QinQ, VLAN, port attributes, MAC address learning and so on, as following table shows:

Classification	Details
STP configuration consistent	Port STP enable / disable status, the link attributes connected to the port (such as point-to-point or not-point-to-point), the port traceroute cost, STP priority, message transmitting rate limit, loopback protection configuration or not, Root protection configuration or not, the edge port or not.
QoS configuration consistent	Flow control, flow shaping, congestion avoidance, port speed-limit, SP queues, WRR queue scheduling, WFQ queues, port priority, port trust mode.
QinQ configuration consistent	Port QinQ function enable/ disable status, the added outer-layer VLAN Tag, the strategy to add outer layer VLAN Tag for different inner layer VLANID
VLAN configuration consistent	Port allowed VLAN, port default VLAN ID, port link type (i.e., Trunk, Hybrid, and Access type), sub-net VLAN configuration, protocol VLAN configuration, VLAN packet with a Tag or not
Port Property configuration consistent	Whether to join the isolation group on port, port speed, duplex mode, and up / down status.
MAC address learning configuration consistent	Whether have the MAC address learning function, whether the port with restrictions to number of the greatest learning MAC addresses, whether to continue forwarding control. after MAC table

13.2 LACP aggregation function

LACP (Link Aggregation Control Protocol, Link Aggregation Control Protocol) is a standard protocol based on IEEE802.3ad. LACP protocol has interactive information with peer end through LACPDU (Link Aggregation Control Protocol Data Unit). Enable a port LACP protocol, the port will notify peer-end system LACP protocol priority by transmitting LACPDU, the system MAC, port LACP protocol priority, port ID and operation Key. After Receipt of LACPDU on peer-end, will compare one of the information with other ports information received to select the port can be in

Selected state and thus both sides can agree on **Selected** state. When operation Key is the link aggregation, the aggregation control depending on port configuration (i.e., rate, duplex mode, up / down status, basic configuration and other information) automatically generates a configuration combination. In link aggregation the port in **Selected** status has the same operation Key.

In a static aggregation group, the port may be in two states: active or standby: both active port and standby port can transmit and receive lacp protocol, but standby ports cannot forward the user messages.

In a static aggregation group, the system set the port in active or standby status in accordance with the following principles:

System according to whether they found a neighbor, port rate, port priority, port ID priority, choose the highest priority port as the default port, the default port is in active state, with the same rate of the default port, peer-end equipment and operation key ports on peer-end equipment are also in active state. Other ports are in a standby state.

13.3 Classification

In accordance with the different aggregation methods, link aggregation can be divided into two categories:

- manual aggregation
- static LACP aggregation

13.4 Manual aggregation

13.4.1 Default configuration

Function	Default
Link aggregation function	Enable
Link aggregation group	Does not exist, need to configure manually
Loading-sharing mode	Source, destination MAC address logic OR result selects the forwarding port

13.4.2 Manual aggregation configuration

13.4.2.1 Trunk group

Users can configure the link aggregation function as the following steps:

Step	Command	Description
1	config	Enter global configuration mode
2	trunk group <i>trunk-group-id portlist</i>	Add a aggregation group <i>trunk-group-id</i> : created aggregation ID, range in 1-6. <i>portlist</i> : The physical port ID list, using ‘,’ and ‘-’ to

		do multi-port input.
3	trunk {enable/disable}	Enable or disable link aggregation
4	exit	Exit global configuration mode and enter the privileged user mode
5	show trunk	Show enable link aggregation or not at present, load balancing mode of link aggregation, group member ports set by all of current trunk groups and the member port currently in effect.

Use **no trunk group *trunk-group-id*** to delete specified aggregation.

13.4.2.2 Loading-sharing mode

There are six kinds of link aggregation load-sharing mode:

mac: select the forward port based on source MAC address.

dmac: select the forward port based on destination MAC address.

sxordmac: select the forward port based on the result of logical operation “or” of source MAC address, destination MAC address.

sip: select the forward port based on source IP address.

dip: select the forward port based on target IP address.

sxordip: select the forward port based on the result of logical operation “or” of source MAC address, destination MAC address.

Step	Command	Description
1	config	Enter global configuration mode
2	trunk loading-sharing mode {smac / dmac / sxordmac / sip / dip / sxordip}	Configure loading-sharing mode for all link aggregation.
3	exit	Exit global configuration mode
4	show trunk	Show enable link aggregation or not at present, load balancing mode of link aggregation, group member ports set by all of current trunk groups and the member port currently in effect.

Use **no trunk loading-sharing mode** to restore the default mode of link aggregation loading-sharing.

Note: This command is only supported in part of the equipment; the specific circumstances need to refer to the command manual.

13.5 Static LACP aggregation function

Note: ISCOM2128EA-MA products are not in support of lacp command.

13.5.1 Default configuration

Function	Default value
Link aggregation	On
Link aggregation group	Does not exist, manual configuration is needed
Loading-sharing mode	Source, destination MAC address logic OR result selects the transmission port

13.5.2 Configure static LACP aggregation

Follow the following step to configure link aggregation:

Step	Command	Description
1	config	Enter global configuration
2	lacp system-priority <i>system-priority</i>	Configure the system LACP protocol priority
3	trunk group <i>trunk-group-id portlist</i>	Create a static LACP aggregation group; <i>trunk-group-id</i> : the created aggregation group number, range is 1-6; <i>portlist</i> : physical port number list, use ‘,’ and ‘-’ to do multi-interface input
4	interface interface-type interface-number	Enter Ethernet port view
5	lacp port-priority <i>port-priority</i>	Configure the port LACP protocol priority
6	lacp mode <i>{active/passive}</i>	Configure the port LACP protocol mode
7	trunk {enable/disable}	Enable/disable link aggregation
8	show trunk	Show if link aggregation is on, link aggregation load balancing mode, the group member port configured by all the aggregation groups and the effective member port
9	show lacp sys-id	Shows device ID of local-end system, including the system LACP protocol priority and system MAC address.
10	show lacp internal	Show configuration and status of local-end system LACP protocol port
11	show lacp neighbor	Show port LACP protocol neighbor information
12	show lacp statistics	Show port LACP protocol statistics information

Use **no trunk group** *trunk-group-id* to delete the specified aggregation group.

13.6 Trunk min-active links

13.6.1 Default configuration

Feature	Default Value
Trunk min-active link	On
The min-active links	1
Trunk group	No exist, configured by manually
Load-sharing	The port number is computed by the last three bits of message source MAC and destination MAC address XOR result.

13.6.2 Function configuration

Step	Command	Description
1	config	Enter global configuration
2	trunk group trunk-group-id min-active links threshold	Configure min-active links to threshold

13.7 Monitoring and maintenance

Note: ISCOM2128EA-MA products are not in support of lacp command.

Use **show** to look over link aggregation configuration.

Command	Description
show trunk	Show enable link aggregation or not at present, load balancing mode of link aggregation, group member ports set by all of current trunk groups and the member port currently in effect.
show lacp sys-id	Shows device ID of local-end system, including the system LACP protocol priority and system MAC address.
show lacp internal	Show configuration and status of local-end system LACP protocol port
show lacp neighbor	Show port LACP protocol neighbor information
show lacp statistics	Show port LACP protocol statistics information

Use **show trunk** to show if link aggregation is enabled, link aggregation load-sharing mode, all the group member port that is configured by aggregation group and the current effective member port. The current effective member port is the port list that the port state is UP in the configured group member ports. The example below is echo in the actual result:

Raisecom#**show trunk**

Trunk: Enable

Loading sharing mode: SXORDMAC

Loading sharing ticket algorithm: :

<i>Trunk Group</i>	<i>Member Ports</i>	<i>Efficient Ports</i>
3	1,4-6,8	1,4

Use **show lacp sys-id** shows LACP protocol global enabled situation as well as Device ID including LACP priority and system MAC addresses.

Raisecom#**show lacp sys-id**

Global LACP function: Enabled

32768, 000E.5E3D.3C79

Use **show lacp internal** display LACP protocol port configuration and status in local-end system.

Show LACP protocol neighbor information, flag, port priority, device ID, Age, operation keys, peer port ID, status of peer port state machine.

There are two kinds port status: Active and standby.

Active indicates that the port has been selected to participate in transmitting. Standby indicates that the port is not selected, and does not participate in forwarding.

Signs are expressed by two letters, the meaning are as following:

S - Device is requesting Slow LACPDU

F - Device is requesting Fast LACPDU

A - Device is in Active mode

P - Device is in Passive mode

Admin Key port and operation key port are belonged to same trunk group number.

Status of the port state machine is composed by 8 bit: bit 0 is in the lowest position.

Bit 0: LACP is enabled flag. 1: enable; 0: disabled

Bit 1: LACP flag of the timeout. 1 indicated a short time-out; 0 indicates a long time-out

Bit 2: that the port where the sender whether the link aggregation. 1: yes; 0: no

Bit 3: Transmitting end considers port link is in synchronization status or not. 1: yes; 0: no

Bit 4: Transmitting end considers port link is in the collection status or not. 1: yes; 0: no

Bit 5: Transmitting end considers port link is in distribution state. 1: yes; 0: no

Bit 6: Receiver state machine in transmitting end is in default status. 1: yes; 0: o

Bit 7: Receiver state machine in transmitting end is in timeout status. 1: yes; 0: no

Raisecom#**show lacp internal**

Flags:

S - Device is requesting Slow LACPDU

F - Device is requesting Fast LACPDU

A - Device is in Active mode

P - Device is in Passive mode

<i>Port State</i>	<i>Flags Port-Pri</i>	<i>Admin-key Oper-key Port-State</i>
-------------------	-----------------------	--------------------------------------

.....

1	<i>standby</i>	SA	32768	0x1	0x1	0x7D
2	<i>active</i>	SA	32768	0x1	0x1	0x3D
3	<i>standby</i>	SA	32768	0x1	0x1	0x7D
4	<i>standby</i>	SA	200	0x1	0x1	0x7D

Use **show lacp neighbor** display port LACP protocol neighbor information.

LACP protocol neighbor information in showing port, concluding flag, port priority, device ID, age, operation key, peer port ID and peer port state machine state.

Age refers to time of the port received the final LACP protocol message to the present time.

The meaning of Flag and port state machine state is the same as command **show lacp internal**

Raisecom#**show lacp neighbor**

Flags:

S - Device is requesting Slow LACPDU

F - Device is requesting Fast LACPDU

A - Device is in Active mode

P - Device is in Passive mode

	<i>Port</i>	<i>Flags</i>	<i>Port-Pri</i>	<i>Dev-ID</i>	<i>Age</i>	<i>Oper-key</i>	<i>Parter-Port</i>	<i>Port-State</i>
<hr/>								
1	SP	0		0000.0000.0000	0s 0x0	0x0	0x8	
2	SA	32768		000B.4634.9580	26s 0x1	0x2	0x3D	
3	SP	0		0000.0000.0000	0s 0x0	0x0	0x8	
4	SP	0		0000.0000.0000	0s 0x0	0x0	0x8	

show lacp statistics is used to show port LACP protocol statistics, including the total transceiver number of LACP message, transceiver number of Marker message, transceiver number of Marker Response message and the number of error messages.

Raisecom#**show lacp statistics**

LACPDU *Marker* *Marker Response LACPDU*

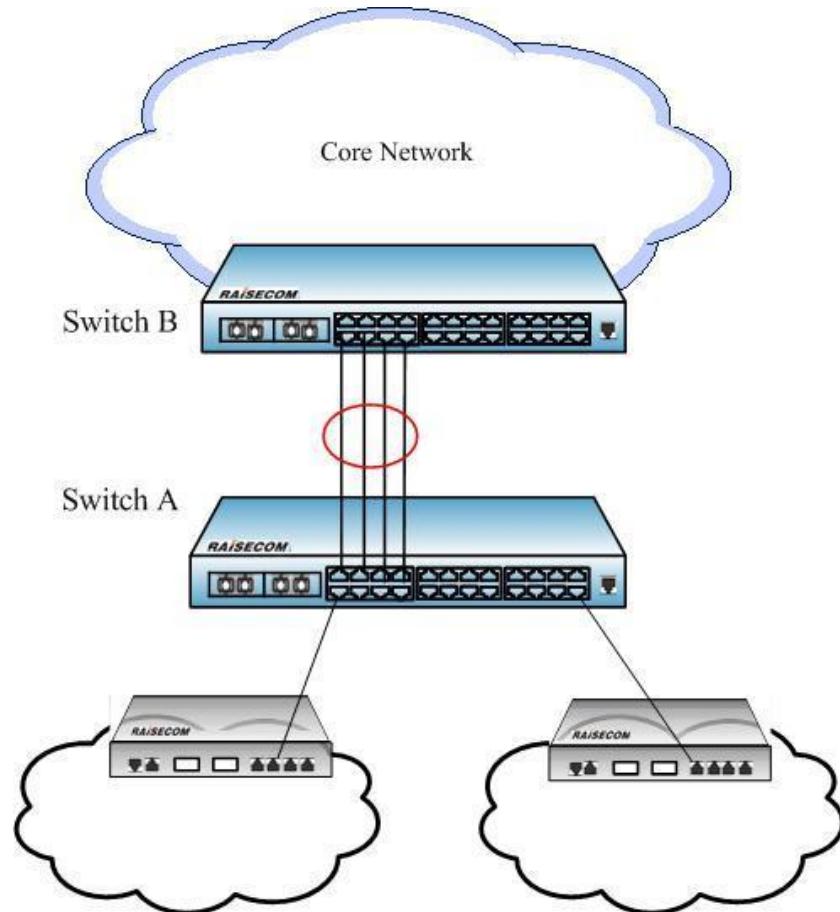
	<i>Port</i>	<i>Send</i>	<i>Recv</i>	<i>Send</i>	<i>Recv</i>	<i>Send</i>	<i>Recv</i>	<i>Pkts Err</i>
<hr/>								
1	89	0	0	0	0	0	0	0
2	90	102	0	0	0	0	0	0
3	89	0	0	0	0	0	0	0
4	89	0	0	0	0	0	0	0

13.8 Typical configuration example

Note: ISCOM2128EA-MA products are not in support of static LACP.

13.8.1 Manual aggregation

Switch A uses 4 ports aggregation to access Switch B, through which egress/ingress load can be shared between the members. Switch A access ports are port1~port 4.



Switch A configuration step

1) Configure aggregation group, join the port into the aggregation group:

Switch A #config

Switch A (config)#trunk-group 1port 1-4

2) Configure the load-sharing mode of trunk link aggregation:

Switch A (config)#trunk loading-sharing mode smac

3) Enable link aggregation function:

Switch A (config)#trunk enable

Switch A (config)#exit

Switch A #show trunk

Trunk: Enable

Loading sharing mode: SMAC

Loading sharing ticket algorithm: :

<i>Trunk Group</i>	<i>Member Ports</i>	<i>Efficient Ports</i>
--------------------	---------------------	------------------------

.....

1

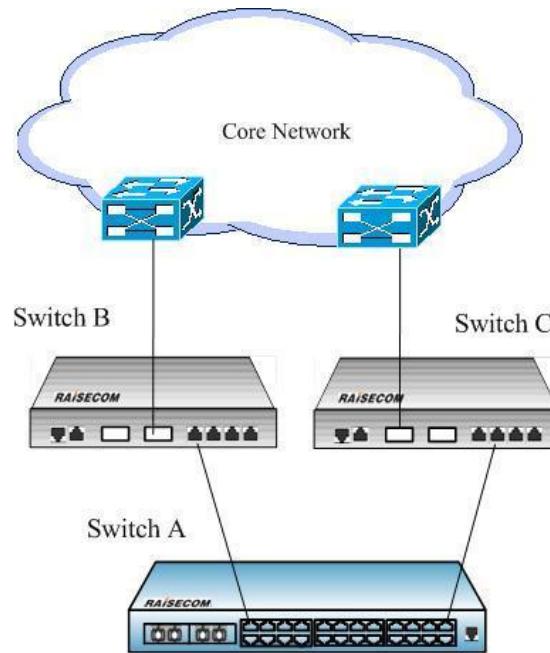
1-4

1-4

SwitchB has the same configuration with Switch A.

13.8.2 Static LACP aggregation

Static LACP has the typical Dual-homing application topology as below, on Switch A configures trunk group, in the mode of static LACP. The SwitchB and SwitchC, without supporting LACP, may realize redundancy backup for high reliability.



The following steps are only for Switch A because SwitchB and Switch C need not the configuration

Configuration step

1) Configure static LACP aggregation group, join the port into the trunk group:

Switch A #**config**

Switch A (config)#**trunk-group 1 port 1,24 lacp-static**

2) Enable trunk function:

Switch A (config)#**trunk enable**

Switch A (config)#**exit**

Switch A #**show trunk**

Trunk: Enable

Loading sharing mode: SMAC

Loading sharing ticket algorithm: :

<i>Trunk Group</i>	<i>Member Ports</i>	<i>Efficient Ports</i>
--------------------	---------------------	------------------------

.....

I

1,24

I

Chapter 14 STP Configuration Guide

14.1 STP/RSTP principle introduction

14.1.1 STP purpose

STP (Spanning Tree Protocol) is founded according to 802.1D created by IEEE association, which is used for deleting data link layer physical loop protocol in local area network. The equipments that is running the protocol find loop in the network through exchanging message, and stop some ports selectively, then cut the loop network structure into tree network without any loop, which stop message breeding and looping endlessly, and avoid the host's message handling ability to decline because of receiving the same message.

STP has two meanings, narrowly-defined STP stands for the STP protocol defined in IEEE 802.1D, broadly-defined STP stands for the STP protocol defined in IEEE 802.1D and the modified spanning tree protocols based on it.

14.1.2 STP related protocol and standard

The related protocol includes:

- IEEE 802.1D: Spanning Tree Protocol;
- IEEE 802.1w: Rapid Spanning Tree Protocol;
- IEEE 802.1s: Multiple Spanning Tree Protocol.

14.2 Configure STP

14.2.1 Default STP configuration

Function	Default
Global STP function	Disable
Port STP function	Enable
STP and port priority	128
STP and system priority	32768
Network diameter	7
Usually according to the physical feature the default value is shown below:	
Port cost	10Mbps: 2000000
	100Mbps: 200000
	1000Mbps: 20000
	10Gbps: 2000

The maximum package number every hello time	3
max-age timer	20s
hello-time timer	2s
forward-delay timer	15s

14.2.2 Root configuration

Step	Command	Description
1	config	Enter global configuration mode
2	spanning-tree root {primary, secondary}	Set the switch to root switch or back-up root switch for spanning tree
3	exit	Return to privileged EXEC mode
4	show spanning-tree	Show STP configuration

14.2.3 Port priority configuration

Step	Command	Description
1	config	Enter global configuration
2	interface port <1-MAX_PORT_NUM>	Enter Ethernet physical port mode
3	[no] spanning-tree priority <0-240>	Set port priority for spanning tree
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show STP configuration

14.2.4 Switch priority configuration

Step	Command	Description
1	config	Enter global configuration mode
2	[no] spanning-tree priority <0-61440>	Set the switch priority for spanning tree. 0-61440: the switch priority
3	exit	Return to privileged EXEC mode
4	show spanning-tree	Show STP configuration

14.2.5 Path-cost configuration

Note: RC551 series devices are not in support of this function, ISCOM2128EA-MA products are not in support of path-cost.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <1-MAX_PORT_NUM>	Enter Ethernet physical port mode <i>1-MAX_PORT_NUM</i> : the equipment port number
3	[no] spanning-tree path-cost <0-200000000>	Set port inner path cost for spanning tree <i>0-200000000</i> : port inner path cost
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show STP configuration

14.2.6 Transmit-limit configuration

Use this command to configure the maximum BPDU number that is allowed to be sent every Time. The parameter is a relative value, without any unit. The larger the parameter is set, the larger the message number that is allowed to be sent every Hello Time, and the more switch resource will be cost. Like time parameter, the configuration will take effect only in the root switch. By default, the value is 3. The configuration step is show below:

Step	Command	Description
1	config	Enter global configuration mode
2	[no] spanning-tree transit-limit <1-10>	Set the switch maximum sending rate
3	exit	Return to privileged EXEC mode
4	show spanning-tree	Show MSTP configuration

14.2.7 STP timer configuration

- The switch has three time parameter: Forward Delay, Hello Time and Max Age:
 - Hello Time: the time interval of the switch sending the bridge configuration information (BPDU), which is used for the switch to detect if there is default with the link. Every Hello Time, the switch will send hello message to the switches around to make sure if there is default with the link.

The default value is 2s, user can change the value according to the network situation. When there are frequent changes in the network links, the value can be shortened to enhance the spanning tree protocol stability. Contrarily, enlarging the value will reduce the resource occupancy rate to system CPU of STP.

- Forward Delay: confirm the time parameter of the switch's state transplant. Link fault will bring the network re-computing the spanning tree, and the STP structure will change accordingly, but the new configuration information by computing will not spread all through the network. If the newly selected root port and the specified port start data transmission immediately, provisional route cycle may happen. To prevent this, the protocol take a state transplant mechanism: the root port and designated port will have to go through a betweenness before data transmission, and only when the betweenness goes through Forward Delay can the ports enter transmission state. This delay confirms that the new configuration information has spread all through the network.

The default value is 15s, user can change it according to the situation, increase the value when the network topology change is not frequent, and decrease it on the contrary.

- Max Age: the bridge configuration information that STP uses has lifecycle to judge if the configuration information is out of time. The switch will drop the outdated configuration information. When the bridge configuration information is out of time, the spanning tree protocol will re-compute the spanning tree.

The default value is 20s, a smaller value will result in the spanning tree re-computing much too frequent, while a value that is much too large will lead to the spanning tree protocol unfitness to the network topology structure change.

Step	Command	Description
1	config	Enter global configuration mode
2	[no] spanning-tree hello-time <1-10>	Set the switch time parameter Hello Time
3	[no] spanning-tree forward-delay <4-30>	Set the switch time parameter Forward Delay
4	[no] spanning-tree max-age <6-40>	Set the switch time parameter Max Age
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

14.3 Configure edge port

14.3.1 STP mcheck

There are two working modes on the switch that supports MSTP: STP compatible mode and MSTP mode. If in a network the port of the switch that is running MSTP is connected with the switch that is running STP, the port will change into STP compatible mode automatically. But if the switch that is running STP is removed, the port cannot change into MSTP mode automatically, but still works in STP compatible mode. Of course, if the port receives new STP message later, the port will return to STP compatible mode. The configuration step is shown below:

Step	Command	Description
1	Config	Enter global configuration mode
2	interface port <1-MAX_PORT_NUM>	Enter Ethernet physical port mode <i>MAX_PORT_NUM</i> the maximum port number that the equipment supports.

3	spanning-tree mcheck	Force the port to move back to MSTP mode
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

14.3.2 STP/MSTP mode

Step	Command	Description
1	config	Enter global configuration mode
3	spanning-tree mode{stp/ mstp}	Configure spanning tree work mode
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

14.3.3 link-type

The two ports that are connected by point to point link can move to transmission state rapidly through transmitting synchronal message, which decreases unnecessary transmission delay time. By default, MSTP sets the link type of the port according to duplex state. Full duplex port is thought to be point to point link, while half duplex is thought to be shared link.

Users can configure by hand to force the current Ethernet ports and point-to-point link connected, but if the link point-to-point link is not a problem in the system would, under normal circumstances, the proposed user of this configuration is set automatically, by Automatic port discovery is linked with point-to-point link. Reverse order no spanning-tree link-type link state port to restore the default values. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <1-MAX_PORT_NUM>	Enter Ethernet physical port mode <i>MAX_PORT_NUM</i> : the maximum port number that the equipment supports
3	spanning-tree link-type {auto/ point-to-point / shared}	Set the port's link type
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration.

14.3.4 clear statistics

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <1-MAX_PORT_NUM>	Enter Ethernet physical port mode <i>MAX_PORT_NUM</i> : the maximum port number that the equipment supports.
3	spanning-tree clear statistics	Clear the port stat. information.
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

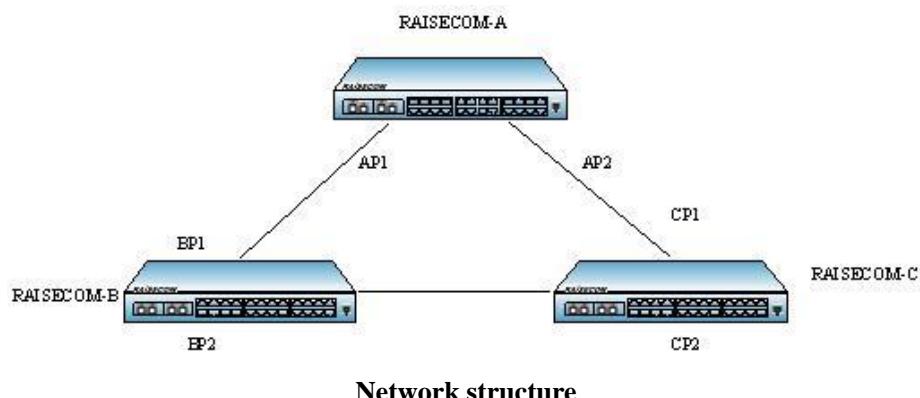
14.3.5 Monitoring and maintaining

Command	Description
show spanning-tree	Show the basic information of spanning tree.
show spanning-tree detail	Show the detailed information of the spanning tree.
show spanning-tree port-list [portlist]	Show the basic information of the spanning tree port list.
show spanning-tree port-list [portlist] detail	Show the detailed information of the spanning tree port list.

14.3.6 Typical configuration instance

There are 3 RAISECOM switch, A, B, C increase according to the equipment MAC address. Configure the switch priority to select the root bridge to A or B freely so that the topology can be changed.

Network structure figure:



Configuration steps:

Open A, B, C global STP:

Raisecom(config)#**spanning-tree enable**

Set the STP working mode of port AP1, AP2, BP1, BP2, CP1, CP2 to RSTP;

By default, check out the stable topology structure:

Raisecom#**show spanning-tree**

Switch A is the root bridge, switch B and C assigned switch A as root.

Show spanning tree configuration of port 1, 2 on switch A, B, C:

Raisecom#**show spanning-tree port 1-2**

A: the switch's AP1, AP2, as the designated port is in normal transmission state;

The BP1of switch B and CP1 of switch C, as the root port, are in normal transmission state, while BP2 and CP2, one is in normal state, the other is in block state;

Set the priority of B to 4096, and repeat the above step:

Raisecom(config)#**spanning-tree priority 4096**

When the topology is stable the root bridge will change into switch B, the port AP2, BP1 between A and C will be blocked.

14.4 MSTP configuration

14.4.1 The default MSTP configuration

Function	Default value
Global MSTP function	Disabled
PORT MSTP function	Enabled
Max jump number of MST region	20
The priority of STP port	128
The system priority of STP	32768
Network diameter	7
Port cost	According to the physical features, the usual situation by default is show below: 10Mbps: 2000000 100Mbps: 200000 1000Mbps: 20000 10Gbps: 2000
Max packet sent out number every	3

Hello Time	
max-age timer	20s
hello-time timer	2s
forward-delay timer	15s
MST region modifying priority	0

14.4.2 Configuration of MSTP region

When the switch running in MSTP mode, the switch can be configured the region information where it belongs to. Which MST region a switch belongs to is determined by the region name, VLAN mapping table and MSTP modification configuration. By the following steps user can put the current switch into a special MST region.

Note 1: MST region configuration view is used here. To configure MST region name, modification class and the relationship between VLAN and instances, it is needed to enter MST region view. If the configuration is not enabled, then the configuration information will only be recorded but not activated. The configuration is shown below:

Note 2: ISCOM2128EA-MA products are not in support of active.

Step	Command	Description
1	config	Enter global configuration mode
2	spanning-tree region-configuration	Enter MST region configuration mode
3	[no] name name	Set MST region name
4	[no] revision-level level	Set MST region modification class; <i>level</i> : modification class, range is 0-65535, the default value is 0
5	instance <0-4095> vlan <1-4094>	Set mapping relationship from VLAN to instances for MST region. <i>0-4095</i> : the instance number; <i>1-4094</i> : VLAN ID
6	exit	Return to global configuration mode
7	exit	Return to privileged EXEC mode
8	show spanning-tree region-configuration	Show MST region configuration information.

14.4.3 The max-hop configuration of MSTP region

MST region maximum hop number confines the scope of MST region. Only when the configured switch is the region root, can the configured maximum hop number be taken as MST region maximum hop number, while other not-region root switches configuration is not valid on it.

From the root switch of the spanning tree in the region, BPDU in the region hop number will

decrease by 1 when transmitted by one switch, and the switch will drop the configuration information that receives 0 hop number. It will make the switch that is out of the max hop number not being able to take part in the spanning tree calculation, which confines the scope of MST region.

For instance: if the maximum hop number of the region root switch is set to 1, the spanning tree function in the region is not available, because only this switch takes part in the spanning tree computing. By default, the maximum hop number is 20, or to hop down 19 steps along the spanning tree path from the region root. The configuration is shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	[no] spanning-tree max-hops <1-40>	Set the maximum hop number of the switch MST region
3	exit	Return to privileged EXEC mode
4	show spanning-tree	Show MSTP configuration

14.4.4 Configuration of root/secondary root

On the one hand, MSTP can configure the switch priority, and then after a spanning tree calculation, to determine the root of the tree root switch to back up or exchange; On the other hand, the user can also specify the order directly. It should be noted that if the root switch designated direct way, then the whole network, users can not modify the proposed switch to any of the priority; otherwise, the root cause designated switch or switch back up the root is invalid.

At the same time, the user can not be designated as an instance of spanning tree two or more root switch; On the contrary, the user can specify multiple spanning tree with a back-up roots. Under normal circumstances, the proposal for a user to specify a spanning tree roots and a number of back-up roots.

When the root switch failure or shutdown, the switch can replace the backup root switch into the corresponding instance of the root switch. However, at this time if the user has set up a new root switch, then switch back up the root will not be a root switch. If a user to configure a number of instances spanning tree root switch back up, when the root switch fails, MSTP will choose the smallest of the MAC address of the switch as a backup root switch.

By default, the switch cannot be taken as the root switch of the spanning tree or the back-up root switch of the spanning tree. Use **no spanning-tree [instance instance-id] root** revert command to restore the default configuration. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	spanning-tree [instance instance-id] root {primary, secondary}	For a certain spanning tree instance, set the switch as the root switch or back-up root switch. <i>instance-id</i> instance number, range is 0-4095
3	exit	Return to privileged EXEC mode

4	show spanning-tree	Show MSTP configuration
----------	---------------------------	-------------------------

14.4.5 Configuration of port priority

Spanning tree protocol spanning tree calculation, the elections need to root port (root port) and designated ports (designated port), in the path of the port costs in line under the premise of the port-side ID of the smaller ports more vulnerable to root for the election or designated port. Users can set up port priority, to reduce port ID, and then there's the purpose of controlling spanning tree protocol to choose a specific port to become the root port or the designated port. With the same priority, the port that has smaller number has higher priority.

Same with the priority of configuring the switch, port priority is independent in different cases. Users can use **instance** instance-id parameter to determine the configuration of port-priority case. If the instance-id value is 0 or parameters **instance** instance-id is omitted, it is configured for the CIST port priority.

Note: The value of priority must be a multiple of 16, such as 0,16,32,48 and so on, the default value of 128. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <1-MAX_PORT_NUM>	Enter Ethernet physical port mode; <i>MAX_PORT_NUM</i> : the maximum port number that the equipment supports
3	[no] spanning-tree [instance instance-id] priority <0-240>	Set port priority for a certain spanning tree instance <i>instance-id</i> : instance number, range is 0-4095 <i>0-240</i> : port priority value
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

14.4.6 Configuration of switch priority

Bridge ID switch determines if the size of this switch can be selected as the root of the tree. Through the allocation of a smaller priority, the smaller switches Bridge ID can be got so that a certain switch can be the spanning tree root. Priority same, small MAC address for the small roots.

Same with the configuration root and backup root, the priority is independent with each other in different instance configurations. Users can use **instance** instance-id parameter to determine the priority allocation of instance. If the instance-id value is 0, or when the parameters **instance** instance-id is omitted, it is configured for the CIST bridge priority.

Note: The value of priority must be in multiples of 4096, such as 0, 4096, 8192, and so on, the default value is 32,768. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode.
2	[no] spanning-tree [instance <i>instance-id</i>] priority <0-61440>	Set port priority for a certain spanning tree instance. <i>instance-id</i> : instance number, range is 0-4095. <i>0-61440</i> : port priority value.
3	exit	Return to privileged EXEC mode.
4	show spanning-tree	Show MSTP configuration.

14.4.7 Configuration of bridge-diameter

RSTP in the agreement, the network diameter refers to the number of switches in the network to exchange up to the path that, switch the number of nodes. MSTP in the agreement, the network diameter settings only effective CIST for example MSTI invalid. And in the same region, no matter how many nodes path, just as a computing node. This fact, the network should be defined as the diameter across the region up to that path, the number of regions. If the network has only one region, then running network diameter is 1.

MST with the region of the largest jump a few similar, if and only if the switch configuration for the CIST root switch, configure the entry into force.

Comparison of the MST's largest region is used to jump a few region characterization of the size of the network diameter is the characterization of the entire network of the size of a parameter. Network that the greater the diameter of a larger network.

When the user switches to configure the network parameters in diameter, MSTP through the switch will automatically calculate the Hello Time, Forward Delay, and Max Age three times to set the parameters for a better value.

Default network with a diameter of 7, the corresponding three times are their default values respectively. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	[no] spanning-tree bridge-diameter <2-7>	Set the diameter of the switch network
3	exit	Return to privileged EXEC mode
4	show spanning-tree	Show MSTP configuration

14.4.8 Configuration of path-cost

Note: RC551 series devices are not in support of this function.

When STP is computing the spanning tree, it is needed to vote root port and designated port, the less the port patch costs, the easier the port be voted as root port or designated port. Users can use

instance instance-id parameter to determine the instance of the port inner path cost of the configured port. If the instance-id value is 0, or when the parameters **instance** instance-id is omitted, it is configured for the CIST inner patch cost.

Usually port cost depends on the physical features, the default case is:

- 10Mbps is 2000000;
- 100Mbps is 200000;
- 1000Mbps is 20000;

Specific configuration is as follows:

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical interface mode. <i>MAX_PORT_NUM</i> : the maximum port number that the equipment supports.
3	[no] spanning-tree [instance <i>instance-id</i>] inter-path-cost <i><0-200000000></i>	Set the port inner patch cost for a certain spanning tree instance. <i>instance-id</i> : instance number, range is 0-4095. <i>200000000</i> : the maximum patch cost value.
4	exit	Return to global configuration mode.
5	exit	Return to privileged EXEC mode.
6	show spanning-tree	Show MSTP configuration.

14.4.9 Configuration of transit-limit

Use the command to configure the maximum BPDU number that is allowed to be sent every Hello Time for MSTP. This parameter is a relative value, not units, the configuration parameters have been greater, each with Hello Time allowed to send the message, the more the number, but also will take up more resources to switch. With the same parameters of the time, only the root switch configuration comes into force.

By default, this value is 3. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode.
2	[no] spanning-tree transit-limit <i><1-10></i>	Set the switch port maximum sending rate.
3	exit	Return to privileged EXEC mode.
4	show spanning-tree	Show MSTP configuration.

14.4.10 Configuration of STP timer

- There are three time parameter: Forward Delay, Hello Time and Max Age:
 - Hello Time: the time interval of the switch's sending BPDU, which is used to determine if there is fault in the link. Every Hello Time the switch will send hello message to the switches nearby to make sure if there is fault with the link.

The default value is 2s, user can change the value according to the network state. If there is frequent change in network links, the value can be shortened in a certain degree to enhance STP stability. On the opposite, enlarging the value will decrease STP resource taken rate to the system CPU.

- Forward Delay: to make sure the time parameter of the switch state safe transformation. Link fault will bring in the re-computing of the spanning tree and the corresponding change of the network structure, but the new configuration information that is re-computed cannot spread all through the network. If the newly elected root port and designated port started immediately transmit the data, may cause a temporary path of the loop. To this end an agreement to adopt a state transfer mechanism: the root port and designated port will go through a betweenness before data re-transmission (state of learning), a state in the middle Forward Delay after delay of time before they can enter the state forward. The delay to ensure that the new configuration information has been spread throughout the network.

Default value is 15 seconds, the user can adjust the value of the actual situation, when the network topology changes frequently are not able to reduce the value, increasing the contrary.

- Max Age: the bridge configuration information that is used by the spanning tree protocol has life cycle to determine whether the configuration information is out of date. The switch will discard the configuration information out of date. When the bridge configuration information expired, spanning tree protocol will be re-spanning tree.

Default is 20 seconds, the value is too small will lead to weight spanning tree calculation too often, too much will lead to spanning tree protocol in a timely manner cannot adapt to the network topology.

The entire network to exchange all of the switches used CIST root switch on the three parameters of the time, only in the root switch configuration on the entry into force. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	[no] spanning-tree hello-time <1-10>	Set the switch time parameter Hello Time
3	[no] spanning-tree forward-delay <4-30>	Set the switch time parameter Forward Delay
4	[no] spanning-tree max-age <6-40>	Set the switch time parameter Max Age
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

14.4.11 Configuration of edge port

Edge port: the port that has no direct connection to the switch or indirect connection to any switch through the network.

Configure the edge port so that the port state can transform into transmission state rapidly, without waiting for; for Ethernet port that is has direct connection with user's terminal equipment, it is supposed to be set to edge port for rapid transformation to transmission state.

If a port is set to edge port auto detection (auto), then the attribution of the edge port is decided by the actual situation. If a port is set to edge port (force-true), when the port receive BPDU the actual running value will become not-edge port, which will keep the state until the configuration is changed.

By default, all the network switch ports will be set to auto-detect. The reverse command **no spanning-tree edged-port** restores the default value of the edge port attribution. Specific configuration is as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical port mode <i>MAX_PORT_NUM</i> : the maximum port number that the equipment supports
3	spanning-tree edged-port <i>{auto / force-true / force-false}</i>	Set the edge port attribution.
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

14.4.12 Configuration of STP mcheck

Switch port in support of MSTP has two work modes: STP compatibility mode and MSTP mode. Supposed that in a network switch-port running MSTP connecting a switch operating STP, the port will be automatically moved to STP compatibility mode. But if switch running STP remove, the port cannot automatically moved to MSTP mode, and still work in STP compatibility mode. At this time McHeck operation force it to the MSTP mode. Of course, if this port receive new STP message, the port will return to STP compatibility mode. The specific configurations are as follows:

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical port mode. <i>MAX_PORT_NUM</i> : the maximum port number that the equipment supports.
3	spanning-tree mcheck	Force the port to MSTP mode.
4	exit	Return to global configuration mode.
5	exit	Return to privileged EXEC mode.
6	show spanning-tree	Show MSTP configuration.

14.4.13 Configuration of STP/MSTP mode

When STP is enabled, two spanning tree mode is supported: STP compatible mode and MSTP mode.

- STP compatible mode: do not implement the rapid transformation from alternate port to root port. Only STP configuration BPDU and topology change notice (STP TCN BPDU) will be sent out. The un-identified part will be dropped when MST BPDU is received.
- MSTP mode: sending MSTP BPDU. If the opposite end of the local switch port is running STP, the port will move to STP compatible mode. If the opposite end of the local switch port is running RSTP, the local will keep MSTP and take it only as our region information.

The steps to configure the switch spanning tree mode are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	spanning-tree mode {stp / mstp}	Set the spanning tree running mode
3	exit	Return to privileged EXEC mode
4	show spanning-tree	Show MSTP configuration

14.4.14 Configuration of link type

By transmitting synchronal message the two ports that is connected by point to point link can move to transmission state rapidly, which reduces the unnecessary transmission delay. By default, MSTP set the link type of the port according to duplex state. Full duplex port is seen as point to point link, while half duplex port is seen as shared link.

Users can configure by hand to force the current Ethernet ports and point-to-point links connected, but the system will get into trouble if the link is not point to point link, usually it is supposed that this configuration is set to be auto so that the system will find out if the ports are connected with point to point link. Reverse command **no spanning-tree link-type** recovers the default value of the link state of the port. Specific configuration is as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <1-MAX_PORT_NUM>	Enter Ethernet physical port mode <i>MAX_PORT_NUM</i> the maximum port number that the equipment supports
3	spanning-tree link-type {auto point-to-point shared}	Set the link type of the port
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

14.4.15 Configuration of rootguard

Reselect when the bridge received a packet in higher priority, but the new elections weak network connectivity, and consumes CPU resources. As for the network with MSTP enabled, if someone send higher-priority BPDU message to attack, networks would be instable caused by continual election. But generally speaking, each bridge priority has been configured in the network planning stage, the more edge, the lower priority. Therefore, down streaming port generally will not receive the highest priority packet than that of the bridge, unless of malicious attacks. For these ports, users can open rootguard, and refuse to deal with the packet with high priority than bridge. If received higher-priority packet, it will block ports for a period of time, to prevent more attacks against upper link.

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <1-MAX_PORT_NUM>	Enter Ethernet physical port mode <i>MAX_PORT_NUM</i> the maximum port number that the equipment supports.
3	spanning-tree rootguard {enable / disable}	Set rootguard.
4	show spanning-tree port-list detail	Show MSTP configuration.

14.4.16 Configuration of loopguard

Spanning tree module would periodically exchanged messages, if in a certain time didn't receive a message that regard it as link failures. Then take the election, freeing the backup port. But in practical applications, it may not caused by link failures. In this case, if release the backup port , it will bring a loop back .

The loopguard will not selection when the port in a certain period of time doesn't receive a message, , keep original condition.

Note: The loopguard and link backup are opposite, i.e. they will not take effect at the same time.

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <1-MAX_PORT_NUM>	Enter Ethernet physical port mode. <i>MAX_PORT_NUM</i> the maximum port number that the equipment supports.
3	spanning-tree loopguard {enable/disable}	Set loopguard.
4	show spanning-tree port-list detail	Show MSTP configuration.

14.4.17 Configuration of statistics clear

MSTP counts each MSTP port BPDU message number of the following types: ingress STP message, ingress RSTP message, ingress MSTP message, egress STP configuration message, egress SRTP message (to the switch that is running MSTP, it will be zero forever), egress MSTP message.

The steps to clear MST port statistics are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <1-MAX_PORT_NUM>	Enter Ethernet physical port mode <i>MAX_PORT_NUM</i> the maximum port number that the equipment support
3	spanning-tree clear statistics	Clear the port statistics to zero
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

14.5 Monitoring and maintenance

Command	Description
show spanning-tree region-configuration	Show MST region configuration information
show spanning-tree [instance instance-id]	Show the basic information of multi-spanning tree instance
show spanning-tree [instance instance-id] detail	Show the detailed information of multi-spanning tree instance
show spanning-tree [instance instance-id] port-list [portlist]	Show the basic information of multi-spanning tree instance port list
show spanning-tree [instance instance-id] port-list [portlist] detail	Show the detailed information of multi-spanning tree instance port list

14.6 Typical configuration instance

Note: ISCOM2128EA-MA products are not in support of active.

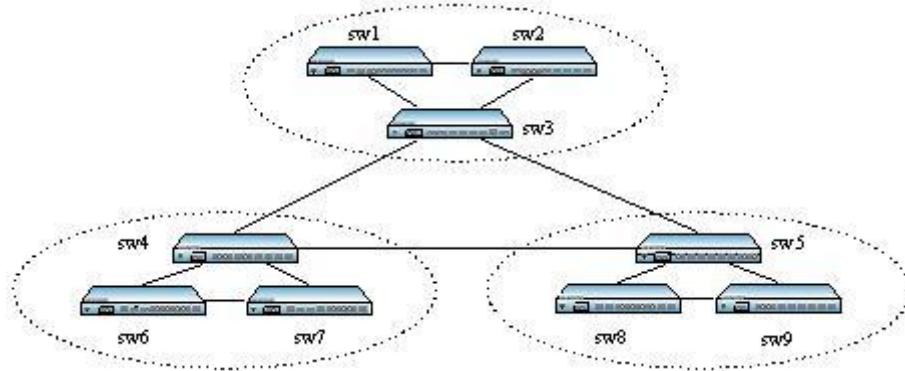
➤ Destination:

Set sw1, sw2, sw3 to the same MST region MST1, modification class to 2, and map VLAN1 to instance 1, VLAN2 to instance 2, other VLAN to CIST;

Set MST2, MST3 to contain sw4/sw6/sw7, sw5/sw8/sw9, the correspondence that VLAN map to instance is similar to MST1.

Show the final spanning tree voting; configure the CIST that take sw3/sw4/sw5 as switch.

➤ Network figure



➤ Configuration step:

Step 1:

Configure MST region configuration information, the region name is MST, modification class is 2, map VLAN2 to instance 2, others to CIST, and enable the configuration information

Raisecom#**config**

```
Raisecom(config)#spanning-tree region-configuration
Raisecom(config-region)#name MST1
Raisecom(config-region)#revision-level 2
Raisecom(config-region)#instance 1 vlan 1
Raisecom(config-region)#instance 2 vlan 2
Raisecom(config-region)#exit
```

Step 2:

Configure MST2 and MST3 in the same way.

Step 3:

To look over the spanning tree configuration information, instance 1 information:

```
Raisecom#show spanning-tree region-configuration
Raisecom#show spanning-tree instance 1
```

MST1, MST2, MST3 form as complete single spanning tree.

Step 4:

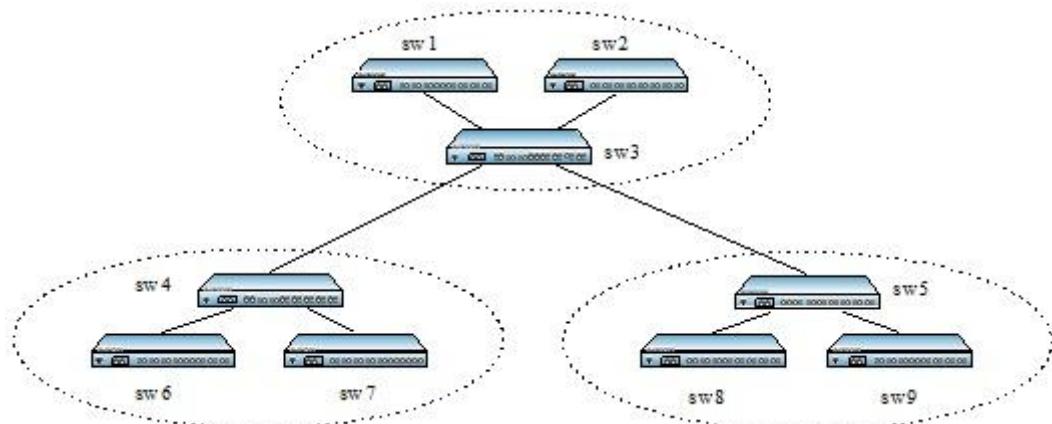
Set the electric physical port on MST1, MST2, MST3 region to the member port of VLAN1;

In MST1 region configure the bridge priority of sw3 to 4096, the priority of other switches larger than 4096;

In MST2 region configure the bridge priority of sw4 to 8192, the priority of other switches larger than 8192;

In MST3 region configure the bridge priority of sw5 to 8192, the priority of other switches larger than 8192;

There is only one MST1 in MST1/MST2/MST3 region, sw3/sw4/sw5 is thought to be root, and the topology picture is as follows:



Chapter 15 DHCP Configuration

15.1 DHCP client configuration

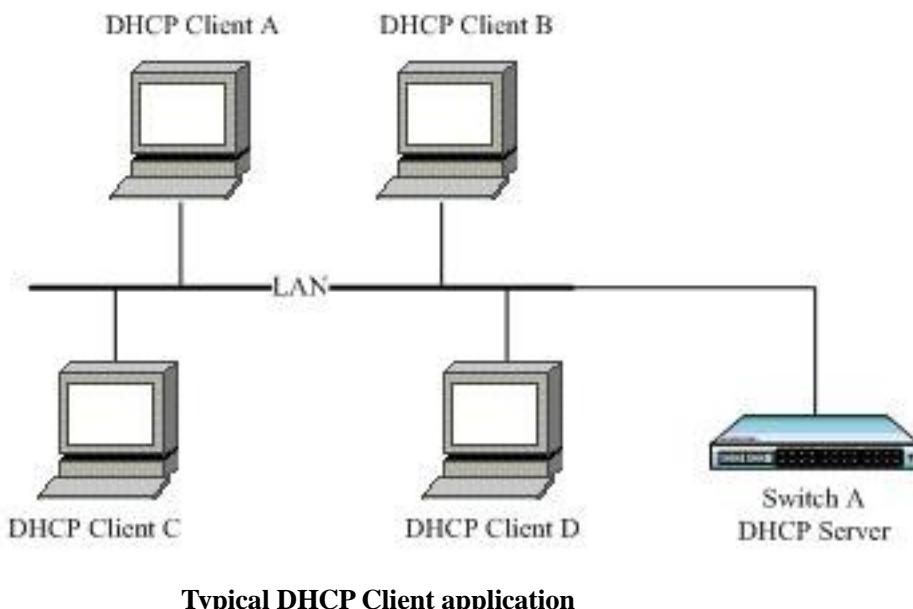
15.1.1 DHCP client overview

DHCP (Dynamic Host Configuration Protocol) is a protocol to offer client device the configuration information. Based on BOOTP, it adds some function like assigning available network address automatically, network address reuse and other extension configuration. The two protocols can do some interoperation with some mechanism. DHCP offers configuration parameters to the network host, which can be divided into two basic parts: one is offering specific configuration information not network host, the other part is assigning network address to the host. DHCP is based on client/server mode, where the designated host offers network address and configuration information to the needed host. The designated host is called server.

Usually, DHCP server is used to accomplish IP address assignation in the following situations:

- Large network scale, it is much too verbose for manual configuration, and cluster management is difficult.
- In the network the host number is larger than supported IP address number, the system cannot offer a static IP address for each host, and the user number access to the network is also limited (for example, Internet service provider is of the situation), lot of users must use DHCP service to get IP address.
- Only a few hosts need static IP addresses, most hosts do not need that.

There are usually one host and multiple clients (like PC and portable devices) in a typical DHCP application.



Typical DHCP Client application

15.1.2 Configure DHCP Client

The part is about how to configure DHCP Client on the switch, concluding the following

configuration information:

- ❖ Default DHCP Client configuration
- ❖ DHCP Client configuration guide
- ❖ Configure IP port 0 applying IP address by DHCP
- ❖ DHCP Client renewal
- ❖ DHCP Client release IP address
- ❖ Configure hostname/class-id/client-id

Note: To ISCOM serious devices, the commands related to DHCP Client is under IP port; when it comes to RC551 devices, they are in global configuration mode.

15.1.2.1 Default DHCP Client configuration

Function	Default value
hostname	raisecomFTTH
class-id	raisecomFTTH-ROS_VERSION
client-id	raisecomFTTH-SYSMAC- IF0
The IP port acquiring IP address by DHCP	N/A
DHCP Client renew	N/A
DHCP Client release IP address	N/A

15.1.2.2 DHCP Client configuration guide

- Make sure that DHCP Server or DHCP Relay is not enabled on the switch.
- To a switch, only IP port 0 supports DHCP Client function.

When DHCP Client is enabled, DHCP Server or DHCP Relay cannot be enabled on the switch

Before using the command, you should make sure that the designated VLAN has been created manually, and the port that IP port lays in has joined the VLAN, while DHCP server has been configured. Or IP address will not be acquired successfully by DHCP.

If IP port 0 has been configured acquiring IP address from DHCP, then it allows configuring IP address manually under the port.

If IP port 0 has acquired IP address form DHCP, run **ip address dhcp {1-4094} [server-ip ip-address]**, and if the acquired address is different from the designated VLAN or DHCP Server IP address, then the port will release the acquired IP address and start a new application.

To port 0, the IP address acquired from DHCP and the manually configured one can cover each other.

- If IP port 0 has acquired IP address by DHCP, then it will start IP address renewal automatically.
- If the client goes through multiple Relay to acquire IP address from DHCP server, make sure that each device is connected and configured correctly. The number of DHCP Relay between the client and server should not exceed 16 in RFC1542, and it is usually recommended not to pass 4.
- After switches enabled, if the local has no configuration files, then switches will start DHCP

client and apply IP address in VLAN1.

15.1.2.3 Configure IP port 0 applying IP address by DHCP

In IP port 0 (only IP port 0), enable DHCP Client, and the device will acquire IP address and requested parameters in the designated VLAN. The parameters includes: gateway address (option 3), TFTP server name (option66), TFTP server address (option 150), configured filename (option 67), root path (option 17), NTP server (option 42).

If DHCP server does not support option 150, then you can configure TFTP server address in option 66, which is also supported by DHCP Client.

If one IP address has been configured to IP port 0, then no matter if default gateway configuration successes or not, DHCP Client is thought to have acquired IP address successfully from the server.

The configuration steps are shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 0	Enter IP port 0 configuration mode
3	ip address dhcp 1	Configure IP port 0 acquiring IP address by DHCP
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp client	Show DHCP Client configuration and the acquired information (run the command when the application ends)

Note:

- If DHCP Server or DHCP Relay has been enabled on the switch, DHCP Client cannot longer be enabled.
- If DHCP Client has been enabled on the switch, then DHCP server or DHCP Relay cannot be enabled.

15.1.2.4 DHCP Client renewal

In IP port 0, if IP address has been acquired through DHCP, then you can use the command to renew.

When renewing, the result will be shown in the command lines automatically. If renew successes will be typed out by SYSLOG.

The steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 0	Enter IP port 0 configuration mode
3	ip dhcp client renew	DHCP Client renew

4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp client	Show DHCP Client configuration and the acquired information (execute the command when renewal ends)

Note: The command is available only when IP port 0 has acquired IP address through DHCP.

15.1.2.5 DHCP Client release IP address

In IP port 0, the steps to release the IP address and other information (like gateway address, TFTP server host name, TFTP server IP address and configured filename) are shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 0	Enter IP port 0 configuration mode
3	no ip address dhcp	DHCP Client release IP address
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp client	Show DHCP Client configuration information and the acquired information

Note: Only when DHCP Client has been enabled in IP port 0 can the command takes effect.

15.1.2.6 Configure hostname/class-id/client-id

In IP port 0, configure hostname, class-id and client-id for DHCP Client, which will be used when DHCP Client is sending out messages. Take configuring hostname for example, it is similar when configuring class-id and client-id.

The steps are shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 0	Enter IP port 0 configuration mode
3	ip dhcp client hostname myhost	Configure hostname to myhost
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp client	Show DHCP Client configuration and acquired information

Note: No matter if DHCP Client has been enabled, hostname, class-id or client-id can be configured. When IP port 0 applies IP address by DHCP Client, current hostname, class-id or client-id is used; when DHCP Client renews, hostname, class-id or client-id should be the same with the one when it is applying IP address.

15.1.3 Monitoring and maintenance

Use different **show** to show DHCP Client running state and configuration. All the listed **show** commands are shown below:

Command	Description
show ip dhcp client	Show DHCP Client configuration and the acquired information

Use **show ip dhcp client** to show the configuration and acquired information of DHCP Client. The configuration includes: hostname, class-id and client-id. The acquired information includes: the acquired IP address, subnet mask, default gateway, lease length, lease starting and ending time, server address, TFTP server hostname, TFTP server IP address and the configuration filename.

Raisecom#show ip dhcp client

Feedback 1: IP port 0 has acquired IP address through DHCP:

<i>Hostname:</i>	<i>raisecomFTTH</i>
<i>Class-ID:</i>	<i>raisecomFTTH-ROS_4.9.771</i>
<i>Client-ID:</i>	<i>raisecomFTTH-000e5e034be5-IF0</i>
<i>Assigned IP Addr:</i>	<i>20.0.0.1</i>
<i>Subnet mask:</i>	<i>255.0.0.0</i>
<i>Default Gateway:</i>	<i>--</i>
<i>Client lease Starts:</i>	<i>Jan-01-2000 12:47:19</i>
<i>Client lease Ends:</i>	<i>Jan-01-2000 13:17:19</i>
<i>Client lease duration:</i>	<i>1800(sec)</i>
<i>DHCP Server:</i>	<i>20.0.0.10</i>
<i>Tftp server name:</i>	<i>--</i>
<i>Tftp server IP Addr:</i>	<i>20.0.0.110</i>
<i>Startup_config filename:</i>	<i>/raisecom/config/0906081</i>
<i>NTP server IP Addr:</i>	<i>20.0.0.110</i>
<i>Root path:</i>	<i>/raisecom/image/2109A#0906053#0906054;2924GF##0906122</i>

Feedback 2: IP port 0 is acquiring IP address through DHCP:

<i>Hostname:</i>	<i>raisecomFTTH</i>
<i>Class-ID:</i>	<i>raisecomFTTH-ROS_4.9.771</i>
<i>Client-ID:</i>	<i>raisecomFTTH-000e5e034be5-IF0</i>
<i>DHCP Client is requesting for a lease.</i>	

Feedback 3: Disable DHCP Client on IP interface 0 :

<i>Hostname:</i>	<i>Raisecom</i>
<i>Class-ID:</i>	<i>Raisecom-3.5.856</i>
<i>Client-ID:</i>	<i>Raisecom-000e5e48e596-IF0</i>

DHCP Client is disabled.

Feedback 4: applying IP address fails, no available lease information:

<i>Hostname:</i>	<i>Raisecom</i>
<i>Class-ID:</i>	<i>Raisecom-3.5.856</i>
<i>Client-ID:</i>	<i>Raisecom-000e5e48e596-IF0</i>

No lease information is available.

15.1.4 Typical configuration example

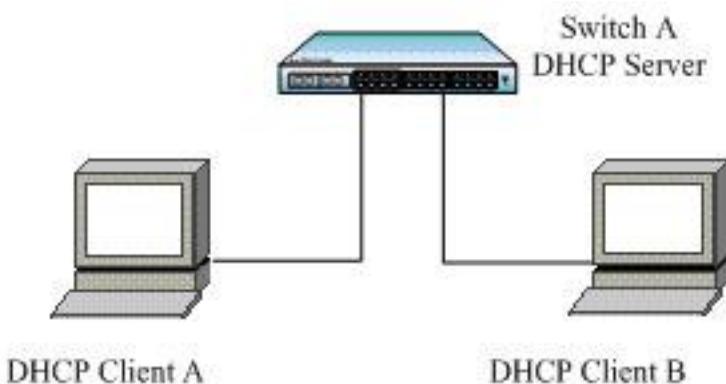
The example is simple but classical on the process of configuring DHCP Client.

1.Configuration instruction

The two DHCP clients connect DHCP server by port 2 and 3 respectively.

- Configure direct ip pool on DHCP Server, and enable DHCP Server globally.
- Configure the two DHCP client acquiring IP address and other configuration information by DHCP.

2.Topology



3.The configuration steps

Only the configuration steps of Client A are listed here, the steps of the other one is the same and will not be listed.

Configure IP port 0 acquiring IP address by DHCP:
Raisecom(config)# interface ip 0

Raisecom(ip-config)#ip address dhcp 1

4. Show result

On DHCP Client, use **show ip dhcp client** to show the client IP address applied from DHCP and other configuration information.

Raisecom(config)# **show ip dhcp client**

<i>Hostname:</i>	<i>raisecomFTTH</i>
<i>Class-ID:</i>	<i>raisecomFTTH-ROS_4.9.771</i>
<i>Client-ID:</i>	<i>raisecomFTTH-000e5e034be5-IF0</i>
<i>Assigned IP Addr:</i>	<i>20.0.0.1</i>
<i>Subnet mask:</i>	<i>255.0.0.0</i>
<i>Default Gateway:</i>	<i>--</i>
<i>Client lease Starts:</i>	<i>Jan-01-2000 12:47:19</i>
<i>Client lease Ends:</i>	<i>Jan-01-2000 13:17:19</i>
<i>Client lease duration:</i>	<i>1800(sec)</i>
<i>DHCP Server:</i>	<i>20.0.0.10</i>
<i>Tftp server name:</i>	<i>--</i>
<i>Tftp server IP Addr:</i>	<i>20.0.0.110</i>
<i>Startup_config filename:</i>	<i>/raisecom/config/0906081</i>
<i>NTP server IP Addr:</i>	<i>20.0.0.110</i>
<i>Root path:</i>	<i>/raisecom/image/2109A#0906053#0906054,2924GF##0906122</i>

15.1.5 DHCP Client trouble shooting

- Make sure that DHCP server is able to support option 1, option 3, option 66, option 67, option 150, option 17, and option 42. If some option is not supported, DHCP cannot get information of this kind, but still can get IP address.
- If the device as DHCP Client starts DHCP Snooping as well, make sure the port it uses to connect DHCP server is the trusted port. Or DHCP Client cannot get IP address.

15.2 DHCP Snooping configuration

The part is about how to configure and maintain DHCP Snooping on the switch, concluding the following contents:

- ❖ DHCP Snooping principle
- ❖ DHCP Snooping configuration
- ❖ Monitoring and maintenance
- ❖ Typical configuration example
- ❖ DHCP Snooping trouble shooting

15.2.1 DHCP Snooping principle

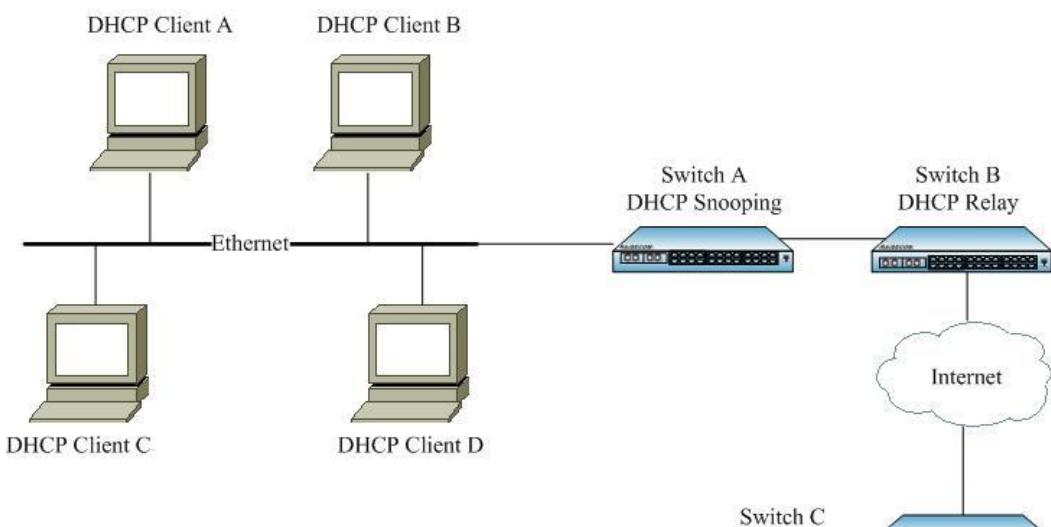
15.2.1.1 Basic Introduction

If there is private DHCP server in the network, user may get wrong IP address. DHCP Snooping is a safe feature of DHCP, it provides network safety by filtrating the unbelievable DHCP message and establishing and maintaining a DHCP Snooping binding database (or DHCP Snooping binding table). To let user get IP address from valid DHCP server, DHCP Snooping safety mechanism allows the port to be set to creditable port and untrust port. It divides creditable port from untrust port on the switch, filtrates the untrust DHCP response message to insure the network safety. It is like firewall between untrust host and DHCP server.

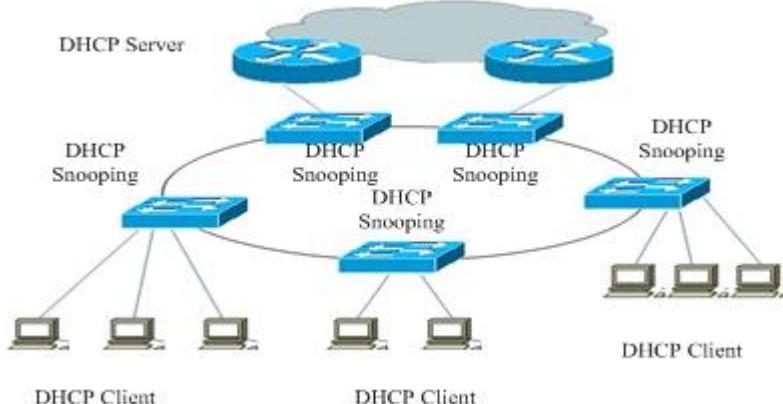
Untrust DHCP message is the message that the host received from the network or outside the firewall. When DHCP Snooping is used in the network that provides network services, untrust message is from other network which does not belong to the server network, like user switch. The messages that are from unknown equipments may be attacking source, so it is untrust. Meanwhile, for the network safety, network administrator may need to record the users' IP address to make sure the corresponding relation between IP address acquiring from DHCP server and MAC address of users' devices. DHCP Snooping receives DHCP ACK broadcasting message by monitoring DHCP Request and trust port and records the DHCP client port MAC address and IP address so as to realize the above function.

In the network that provides services, the creditable port is connected with DHCP server; the untrust port is connected with client side, or with other equipments in the network. The untrust port will drop the DHCP-ACK, DHCP-NAK and DHCP-OFFER message that is received from DHCP response (because these equipments that are connected with untrust ports should not make any response to DHCP server); while the response message received by the creditable port will be transmitted normally, which will prevent pseudo-server deception and make sure that user can get the correct IP address.

The figures below are typical network applications of DHCP Snooping:



DHCP Snooping typical network structure



DHCP Snooping Ethernet loop typical network structure

15.2.1.2 Option 82 overview

Option 82 is the Relay Agent Information option of DHCP message, which is identified in request document RFC3046. When DHCP Client sent request message to DHCP Server, if it is needed to cross DHCP Snooping, DHCP Snooping will add Option 82 to request message. Option 82 contains much sub-option. The option 82 introduced here support sub-option 1 and sub-option 2:

sub-option 1: circuit ID is defined in it

sub-option 2: remote ID is defined in it

sub-option 1: sub-option 1 is a sub-option of Option 82, which is circuit ID sub-option. A sub-option is usually configured on DHCP Snooping equipment or repeaters, which defines the port number of the switch port that needs to carry DHCP client when transmitting messages and the port's VLAN number. Usually sub-option1 and sub-option 2 need to be used together to note the information of DHCP source port.

Sub-option 2: it is also a sub-option of Option 82, which is Remote ID. This sub-option is usually also configured on DHCP repeater, which defines the MAC address information of the equipments that carry Snooping or repeater equipment. Usually sub-option 1 needs to be used together to note DHCP source port information.

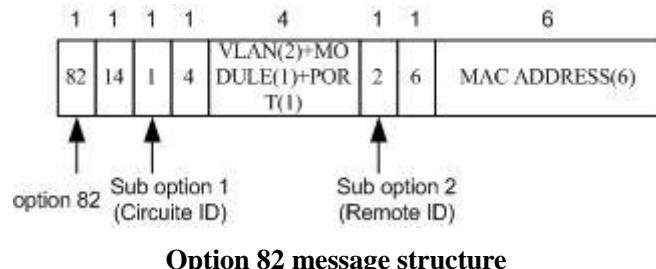
Option 82 actualize the address information of DHCP client and DHCP snooping equipment or repeater equipment's record on DHCP server, with the help of other software it could actualize DHCP distribution restriction and billing function. For example, combined with IP Source Guard, the reception of IP address + MAC address can be defended effectively.

15.2.1.3 Option 82 handling actions

- 1: When the switch receives a request message without Option 82 words, if it supports Option 82, Option 82 will be added and transmitted.
- 2: When the switch receives a request message without Option 82 words, if it supports Option 82, Option 82 will be transmitted; if not, the message will be dropped.
- 3: When the switch receives a request message without Option 82 words, if it supports Option 82, Option 82 will be deleted and transmitted; if not, the message will be dropped.

15.2.1.4 The structure of Option 82 message

Option 82 obeys ‘TLV’ option format, fig 1-2 shows its message structure:



15.2.2 DHCP Snooping configuration

The part is about how to configure DHCP Snooping on the switch, concluding the following configuration information:

- ❖ Default DHCP Snooping configuration
- ❖ DHCP Snooping configuration guide
- ❖ Configure global DHCP Snooping
- ❖ Configure port DHCP Snooping
- ❖ Configure port trust
- ❖ Configure DHCP Snooping supporting Option 82

15.2.2.1 Default DHCP Snooping configuration

Function	Default value
Global DHCP Snooping state	Disabled
Port DHCP Snooping state	Enabled
Port trust state	Untrusted
DHCP Snooping supporting Option 82	Disabled

15.2.2.2 DHCP Snooping configuration guide

- Make sure that the switch DHCP Server or DHCP Relay is not enabled;
- Global DHCP Snooping must be enabled;
- If DHCP Snooping is not enabled on the port, DHCP Snooping cannot be available on the switch;
- After DHCP Snooping is on, DHCP Server or DHCP Relay cannot be started on the switch;
- If only DHCP Snooping is enabled, while DHCP Snooping supporting Option 82 is not, the switch will not insert Option 82 in the message nor handle the message that contains Option 82;
- Make sure the port that connects DHCP server is trust, while the port that connects client side is untrust.

15.2.2.3 Configure global DHCP Snooping

By default, global DHCP Snooping is off. Only when global DHCP Snooping is enabled can the switch DHCP Snooping take effect. To enable global DHCP Snooping, take the following steps:

The configuration step is shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp snooping	Enable global DHCP Snooping
3	exit	Return to privileged EXEC mode
4	show ip dhcp snooping	Show DHCP Snooping configuration

Note: If the switch enables DHCP Server or DHCP Relay, global DHCP Snooping cannot be started. On the opposite, if the switch enables DHCP Snooping, DHCP Server or DHCP Relay cannot be started.

Use global configuration command **no ip dhcp snooping** to disable global DHCP Snooping.

15.2.2.4 Configure port DHCP Snooping

By default, DHCP Snooping is on, use **no ip dhcp snooping port-list** to close port DHCP Snooping.

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp snooping port-list 4-9	Enable DHCP Snooping on port 4-9
3	exit	Return to privileged EXEC mode
4	show ip dhcp snooping	Show DHCP Snooping configuration

15.2.2.5 Configure port trust

Untrust port will drop DHCP-ACK, DHCP-NAK, DHCP-OFFER message received from DHCP server response (because these equipments connected by untrust ports should not make any DHCP server response). While the DHCP server response message received by credible port will be transmitted normally.

Note: By default, all the ports' DHCP Snooping of the switch is on. But until global DHCP Snooping is on can they be available. That is to say, if global DHCP Snooping is off, and only port DHCP Snooping is on, DCHP Snooping cannot take effect.

Trust port connects DHCP server or the ports of others switches, while untrust port connects user or network, which keeps away from server deception, and makes sure user can get the correct IP address.

Follow the steps below to set the designated port to credit port.

Step	Command	description
1	config	Enter global configuration mode
2	interface port 15	Enter port configuration mode
3	ip dhcp snooping trust	Configure credit port
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp snooping	Show DHCP Snooping configuration

Note: Only when port trust is started in global DHCP Snooping and the port has also started DHCP Snooping can it take effect. Use **no ip dhcp snooping trust** to set the port to untrust port.

In port configuration mode use no ip dhcp snooping trust to set the port to untrust port and delete it from trust port list.

15.2.2.6 Configure DHCP Snooping supporting Option 82

Following the steps below, user can enable DHCP Snooping supporting Option 82, and the switch will add Option 82 option into the DHCP request message that receives Option 82; delete Option 82 in the DHCP response message that contains Option 82. The received DHCP request message that contains Option 82 will be handled according to the configured strategy and transmitted, while to the response message that don't contain Option 82 option, the switch will not take any action and transmit it directly.

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp snooping information option	Enable DHCP Snooping supporting Option 82
3	exit	Return to privileged EXEC mode
4	show ip dhcp snooping	Show DHCP Snooping configuration

Note: DHCP Snooping supporting Option 82 function is global, but it reacts on the port. It can be enable only in global DHCP Snooping, and only when the port starts DHCP Snooping can Option 82 take effect on the port.

Use global configuration command no ip dhcp snooping information option to stop DHCP Snooping supporting Option 82.

15.2.3 Monitoring and maintenance

Use the command **show** to look over the switch DHCP Snooping running state and configuration state and help monitoring and maintenance.

Command	Description
show ip dhcp snooping	Show DHCP Snooping configuration information
show ip dhcp snooping binding	Show DHCP Snooping binding table information

Use **show ip dhcp snooping** to show DHCP Snooping configuration information, including global DHCP Snooping state, if Option 82 is supported, port DHCP Snooping state and port trust. Specific steps are as follows:

Raisecom#**show ip dhcp snooping**

DHCP Snooping: Enabled

Option 82: Enabled

Port	Enabled Status	Trusted
1	<i>enabled</i>	<i>no</i>
2	<i>enabled</i>	<i>no</i>
3	<i>enabled</i>	<i>no</i>
4	<i>enabled</i>	<i>no</i>
5	<i>enabled</i>	<i>no</i>
6	<i>enabled</i>	<i>no</i>
7	<i>enabled</i>	<i>no</i>
8	<i>enabled</i>	<i>no</i>
9	<i>enabled</i>	<i>no</i>
10	<i>enabled</i>	<i>no</i>
11	<i>enabled</i>	<i>no</i>
12	<i>enabled</i>	<i>no</i>
13	<i>enabled</i>	<i>no</i>
14	<i>enabled</i>	<i>no</i>
15	<i>enabled</i>	<i>yes</i>
16	<i>enabled</i>	<i>no</i>
17	<i>enabled</i>	<i>no</i>
18	<i>enabled</i>	<i>no</i>
19	<i>enabled</i>	<i>no</i>
20	<i>enabled</i>	<i>no</i>
21	<i>enabled</i>	<i>no</i>
22	<i>enabled</i>	<i>no</i>
23	<i>enabled</i>	<i>no</i>
24	<i>enabled</i>	<i>no</i>
25	<i>enabled</i>	<i>no</i>
26	<i>enabled</i>	<i>no</i>

Use **show ip dhcp snooping binding** to show DHCP Snooping binding table information, current binding number and the maximum binding number. The binding table information contains binding IP address, binding MAC address, binding VLAN and binding port. Specific steps are as follows:

Raisecom#show ip dhcp snooping binding

Ip Address	Mac Address	Lease(sec)	Type	VLAN	Port
20.168.0.3	000E.5E00.91E0	1650	dhcp-snooping	1	17

Current Binding: 1

History Max Binding: 1

15.2.4 Straight-through topology configuration example

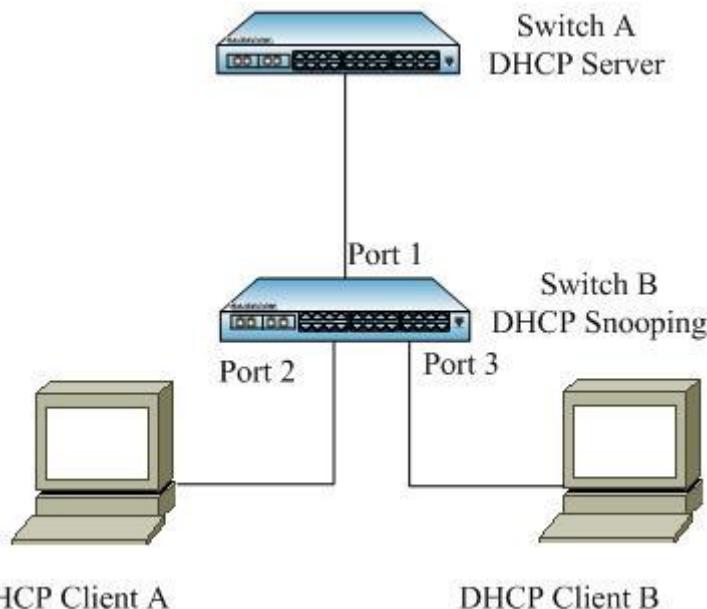
This part gives an introduction to an example that a DHCP client connects DHCP server and get IP address dynamically through DHCP Snooping, it shows the typical configuration of DHCP Snooping.

1.Configuration explanation

This example is a simple and typical DHCP configuration, the two DHCP clients use DHCP port 2, 3 respectively to connect DHCP server.

- Configure the correct address pool on DHCP Server, and enable DHCP Server function globally.
- Enable DHCP Snooping function globally on DHCP Snooping equipment, and enable DHCP Snooping on the port, set port 1 to trust port, and configure DHCP Snooping supporting Option 82, use the default strategy Replace to handle the request messages from client side.

2.Topology picture



Typical DHCP Snooping straight-through topology configuration

3.Configuration step

Configure DHCP Snooping:

- Enable global DHCP Snooping:

Raisecom#**config**

Raisecom(config)#**ip dhcp snooping**

- Port enable DHCP Snooping:

Raisecom(config)# **ip dhcp snooping port-list 1-3**

- Set port 3 to DHCP Snooping trust port:

Raisecom(config)# **interface port 1**

Raisecom(config_port)# **ip dhcp snooping trust**

- Enable DHCP Snooping supporting Option 82:

Raisecom(config)#**ip dhcp snooping information option**

4. Show the result

On ISCOM switch use command **show ip dhcp snooping** to look over the switch DHCP Snooping running state and configuration state, on the client side use **show ip dhcp client** to show client IP address application. Specific contents are as follows:

Raisecom#**show ip dhcp snooping**

DHCP Snooping: Enabled

Option 82: Enabled

<i>Port</i>	<i>Enabled</i>	<i>Status</i>	<i>Trusted</i>
-------------	----------------	---------------	----------------

1	<i>enabled</i>	<i>yes</i>	
2	<i>enabled</i>	<i>no</i>	
3	<i>enabled</i>	<i>no</i>	

...

...

...

Raisecom#**show ip dhcp client**

Hostname: raisecomFTTH

Class-ID: raisecomFTTH- 3.6.1025

Client-ID: raisecomFTTH-000e5e8a0798-IF0

Assigned IP Addr: 10.0.0.5

Subnet mask: 255.0.0.0

Default Gateway: 10.0.0.1

Client lease Starts: Jan-01-2007 08:00:41

Client lease Ends: Jan-11-2007 11:00:41

Client lease duration: 874800(sec)

DHCP Server: 10.100.0.1

Tftp server name: --

Tftp server IP Addr: 10.168.0.205

Startup_config filename: 2109.conf

15.2.5 Ethernet loop topology configuration example

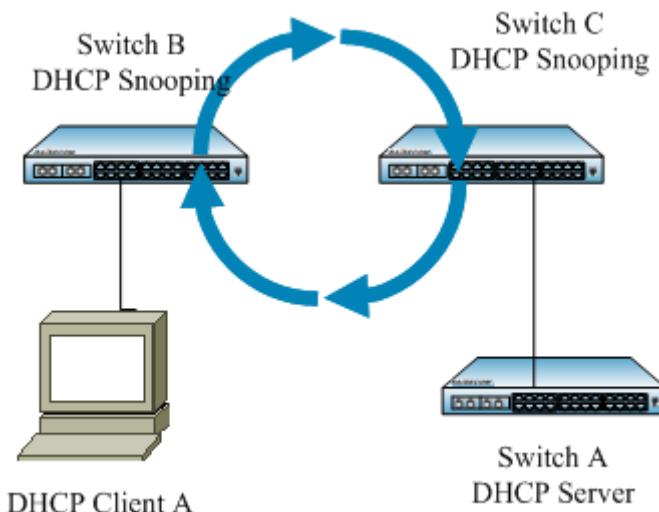
This part gives an introduction to an example that a DHCP client connects DHCP server and get IP address dynamically through Ethernet loop, it shows the typical configuration of DHCP Snooping.

1.Configuration explanation

Network topology is the Ethernet loop composed by two sets of ISCOM2128EA-MA, enable DHCP Snooping function on loop device and configure loop port and device connection port for trust ports.

- Configure the correct address pool on DHCP Server, and enable DHCP Server function globally.
- Enable DHCP Snooping function globally on DHCP Snooping equipment, and configure loop port and DHCP Server connection port for trust ports.

2.Topology picture



Typical DHCP Snooping Ethernet loop topology configuration

3.Configuration step

Switch B

- Configure Ethernet loop


```
Raisecom#config
Raisecom(config)#interface port 13
Raisecom(config-port)# ethernet ring 1 23
Raisecom(config)# ethernet ring 1 enable
```
- Configure DHCP Snooping


```
Raisecom#config
Raisecom(config)# ip dhcp snooping
Raisecom(config)#interface port 13
Raisecom(config-port)# ip dhcp snooping trust
```

```
Raisecom(config-port)# interface port 23
Raisecom(config-port)# ip dhcp snooping trust
➤ Configure loop port mode
Raisecom(config)#interface port 13
Raisecom(config-port)# switchport mode trunk
Raisecom(config-port)# interface port 23
Raisecom(config-port)# switchport mode trunk
```

Switch C

```
➤ Configure Ethernet loop
Raisecom#config
Raisecom(config)#interface port 9
Raisecom(config-port)# ethernet ring 1 21
Raisecom(config)# ethernet ring 1 enable
➤ Configure DHCP Snooping
Raisecom#config
Raisecom(config)# ip dhcp snooping
Raisecom(config)#interface port 9
Raisecom(config-port)# ip dhcp snooping trust
Raisecom(config-port)# interface port 21
Raisecom(config-port)# ip dhcp snooping trust
Raisecom(config-port)# interface port 15
Raisecom(config-port)# ip dhcp snooping trust
➤ Configure loop port mode
Raisecom(config)#interface port 9
Raisecom(config-port)# switchport mode trunk
Raisecom(config-port)# interface port 21
Raisecom(config-port)# switchport mode trunk
```

Client A

➤ Connect to Switch B port 17, apply for IP address

Switch A

➤ Connect to Switch C port 15, configure DHCP Server

```
Raisecom(config-ip)# ip address 20.0.0.10 255.0.0.1
Raisecom(config-ip)# ip dhcp server
```

Raisecom(config)# **ip dhcp server**

Raisecom(config)#**ip dhcp server ip-pool pool 20.0.0.1 20.0.0.200 255.0.0.0 ip 0**

4.Show the result

Switch A

Raisecom#**show ip dhcp server lease**

<i>IP Address</i>	<i>Hardware Address</i>	<i>Lease Expiration</i>	<i>IP Interface</i>
20.0.0.1	00:0E:5E:03:8A:23	Jan-01-2000 10:10:24	0
20.0.0.110	00:1E:58:49:42:BD	Jan-01-2000 10:09:34	0
20.0.0.2	00:0E:5E:03:70:DE	Jan-01-2000 10:09:21	0

Total: 3

Switch B

Raisecom#**show ip dhcp snooping binding**

<i>Ip Address</i>	<i>Mac Address</i>	<i>Lease(sec)</i>	<i>Type</i>	<i>VLAN</i>	<i>Port</i>
20.0.0.110	001E.5849.42BD	1615	<i>dhcp-snooping</i>	1	17

Current Binding: 1

History Max Binding: 1

Switch C

Raisecom#**show ip dhcp snooping binding**

<i>Ip Address</i>	<i>Mac Address</i>	<i>Lease(sec)</i>	<i>Type</i>	<i>VLAN</i>	<i>Port</i>

Current Binding: 0

History Max Binding: 0

Client A

R:\ros>**ipconfig /all**

Windows IP Configuration

Host Name : RCYF-1235

Primary Dns Suffix : soft2.raisecom.com

Node Type : Unknown

IP Routing Enabled. : No

WINS Proxy Enabled. : No

DNS Suffix Search List. : soft2.raisecom.com

raisecom.com

Ethernet adapter Local connection-2:

```

Connection-specific DNS Suffix . :
Description . . . . . : D-Link DFE-530TX PCI Fast Ethernet Adapter (rev.C)
Physical Address . . . . . : 00-1E-58-49-42-BD
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address. . . . . : 20.0.0.110
Subnet Mask. . . . . : 255.0.0.0
Default Gateway. . . . . :
DHCP Server . . . . . : 20.0.0.10
Lease Obtained. . . . . : Sept. 7, 2009 Monday 16:25:09
Lease Expires . . . . . : Sept. 7, 2009 Monday 16:55:09

```

15.2.6 DHCP Snooping trouble shooting

If DHCP client cannot get network address normally through DHCP Snooping, it may be one of the following situations:

- If global DHCP Snooping and port DHCP Snooping are enabled at the same time;
- If DHCP Snooping do not open Option 82 option, when DHCP Snooping receives the message that contains Option 82 it will be dropped directly;
- If DHCP Snooping Option 82 option is enabled, and the request message handling strategy is set to be DROP, then the messages that contain Option 82 will be dropped;
- If the port is not configured as DHCP Snooping trust port, all the response messages to the ports mentioned above will be dropped.

If above configuration cannot make it running, check if Route enabled on device opened DHCP Snooping and DHCP server IP is correct.

15.3 DHCP Server Configuration

Note: ISCOM 2128EA-MA products are not in support of dhcp server.

The part is about how to configure and maintain DHCP Server on the switch, concluding the following contents:

- ❖ DHCP Server principle overview
- ❖ DHCP Server configuration
- ❖ Monitoring and maintenance
- ❖ Typical configuration example
- ❖ DHCP Server trouble shooting

15.3.1 DHCP Server principle overview

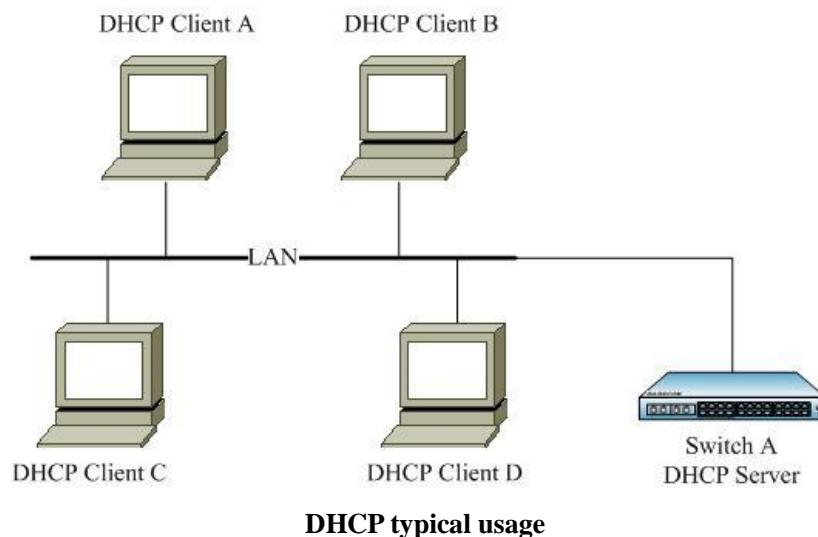
Dynamic Host Configuration Protocol (DHCP) let the client acquire configuration information protocol in TCP/IP network, which is based on BOOTP protocol, and adds the function of automatic

distribution useful network address and so on based on BOOTP protocol. The two protocol can make interoperability through some mechanism. DHCP offers the network hosts configuration parameters, which are made of two parts: one is to transmit special configuration information to network hosts, the other one is to assign network addresses to the hosts. DHCP is based on client/server mode, in this mode specific host assigns network addresses and transmits network configuration parameters to network hosts, the designated hosts are called server.

Usually, in the following situations DHCP server will be used to accomplish IP address distribution:

- When the network scope is too large for manual configuration or centralized management to the whole network.
- When the network host number is larger than the IP address number that the network supports, and cannot give each host a stable IP address; there is also user number limit who can get into the network at the same time (for example, Internet access service provider belongs to the situation), lots of users have to acquire their own IP address dynamically from DHCP server.
- When there is not so many hosts who need stable IP address, and most hosts have no the need for stable IP address.

In typical DHCP application, there is usually one DHCP server and several client ports (like PC and portable machine), the typical DHCP application is shown below:



15.3.2 DHCP Server configuration

The part is about how to configure DHCP Server on the switch, concluding the following configuration information:

- ❖ Default DHCP Server configuration
- ❖ DHCP Server configuration guide
- ❖ DHCP Server global configuration
- ❖ IP port DHCP Server configuration
- ❖ IP-pool configuration
- ❖ TFTP server address configuration
- ❖ Boot filename configuration
- ❖ Option 82 state configuration
- ❖ User custom options configuration

- ✧ Lease table timeout configuration
- ✧ Relay-ip address configuration

Note: Only ISCOM3000 serial switches support border upon surrogate IP address configuration.

15.3.2.1 Default DHCP Server configuration

Function	Default value
Global DHCP Server state	Disabled
IP port DHCP Server state	Disabled
Address pool	N/A
Lease table timeout	Maximum timeout: 10080 minutes Least timeout: 30 minutes Default timeout: 30 minutes
Neighbor proxy address	N/A

15.3.2.2 DHCP Server configuration guide

- Make sure that DHCP Snooping on the switch is not on; Global DHCP Server must be enabled;
- If DHCP Server is not enable in IP port, DHCP Server does not take effect on this IP port;
- When DHCP Server is on, DHCP Snooping cannot be started either on the switch;
- Make sure that the connection to DHCP Relay and DHCP server is correct. DHCP server must be ISCOM3000 serious products. The IP port address and the corresponding address pool range is correct;
- If the client connect DHCP server through DHCP Relay, DHCP server must be ISCOM3000 serial switches. Except making sure IP port address and address pool configuration correct, correct configuration to neighbor proxy address and DHCP Relay.

15.3.2.3 DHCP Server global configuration

By default, global DHCP Server is disabled. Only when global DHCP Server is enabled, the switch DHCP Server can take effect. User can follow the steps below to start global DHCP Server:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp server	Enable global DHCP Server
3	exit	Return to privileged EXEC mode
4	show ip dhcp server	Show DHCP Server configuration

Note:

- If DHCP Snooping has been started on a switch, global DHCP Server cannot be started any more.

- On the opposite, if global DHCP Server has been started, DHCP Snooping or DHCP Client cannot be started.

Use global configuration command **no ip dhcp server** to close global DHCP Server.

15.3.2.4 IP port DHCP Server configuration

By default, IP port DHCP Server function is disabled as well, user can use IP port command **ip dhcp server** to start IP port DHCP Server function. To close IP port DHCP Server, use IP port command **no ip dhcp server**.

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 4	Enter IP port 4 configuration mode
3	ip dhcp server	Enable DHCP Server
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp server	Show DHCP Server configuration

Note: When global DHCP Server is off, user can start DHCP Server beforehand on a certain IP interface, but only when global DHCP Server starts, can the DHCP Server started from the IP port take effect.

Use IP port configuration command **no ip dhcp server** to close IP port DHCP Server.

15.3.2.5 Ip-pool configuration

DHCP server selects and distributes IP address and other parameters from the address pool for the client. When the equipment that is selected as DHCP server receives a DHCP request from the client, it will select proper address pool by configuration, and then pick out a free IP address, which will be sent out to the client together with other parameters (like DNS server address, address lease limit). Lots of standard configuration option is identified in RFC2132, where more detailed information can be got there. But most DHCP configurations use only a few options of the rules.

Following the steps below user can configure address pool:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp sever ip-pool WORD start-ip-address end-ip-address mask-address ip <0-14> [gateway ip-address] [dns ip-address] [secondary-dns ip-address]	Configure the address pool
3	exit	Return to privileged EXEC mode

4	show ip dhcp server ip-pool	Show configuration information of DHCP server
----------	------------------------------------	--

Note:

- The command can configure one address pool to IP interface once. If IP interface does not exist when configuring, still the address pool can be successfully configured, but it will not take effect until the IP port is created and the IP address is configured. If the IP port is changed or deleted, the configured address pool can still be kept. Once the IP port is re-created, the configured address pool will take effect again.
- If the client and the server is in the same subnet, when configuring IP address pool, the network section that the address pool is in should be the same with the network section that of IP port address's, that is to say, address pool's network address is the same with the port's network address; if the client connects the server through DHCP Relay, then the server's address and relay-ip should be within the same network section. Otherwise, DHCP Server will not distribute IP address for DHCP client.

Use global configuration command **no ip dhcp server ip-pool** ip-pool to delete the configured address pool. If the IP address pool that is to be deleted does not exist, returned value is fault.

Here, the maximum IP address pool number that can be configured for each IP port is 4, the maximum IP address number that the switch supports is 2500. Address pool take the name as the only mark.

Configuration example:

Raisecom#**config**

Raisecom(config)#**ip dhcp server ip-pool pool1 192.168.1.100 192.168.1.200**

255.255.255.0 ip 4 gateway 192.168.1.1 dns 192.168.1.1 secondary-dns 10.168.0.1

Raisecom(config)#**exit**

Raisecom#**show ip dhcp server ip-pool**

The result is shown below:

Name of ip pool table : pool1
Status of IP pool table: active
IP address range: 192.168.1.100 - 192.168.1.200
Mask: 255.255.255.0
Including IP Interface: 4
IP address of gateway: 192.168.1.1
IP address of DNS server: 192.168.1.1
IP address of secondary DNS server: 10.168.0.1

Valid IP pool count : 1
Valid IP address count : 12
Allotted IP address count : 0

Gateway and dns is optional, if they are not used, default gateway and DNS will not be selected for

the client.

15.3.2.6 TFTP server address configuration

In practical application, the remote client is required to start the automatic acquisition configuration files and loading and complete automatic configuration process. After launching the empty configuration, the client needs to request DHCP Server IP address and DHCP Server needs to provide other necessary configuration parameters for automatic configuration. After obtaining the IP address and corresponding configuration parameters distributed by the server, the client needs to acquire and execute the configuration file in designated server so as to complete automatic configuration.

If the request message Option 55 contains the corresponding parameters of DHCP Option150, then DHCP Server has configured TFTP server address while assigning IP address for client. The client can acquire related configuration file in the designated TFTP Server to perform automatic configuration process.

The configuration step is as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp sever tftp-server <i>ip-address ip-pool WORD</i>	Configure TFTP server address
3	exit	Return to privileged EXEC mode
4	show ip dhcp server ip-pool	Show configuration information of DHCP server

Note:

- Before performing the command to configure TFTP server address for client, make sure that the DHCP server has already configured designated IP address pool.
- If performing this command in the same address pool for many times, the new configuration needs to cover the previous TFTP server address configuration.
- If the server has configured TFTP server address and the request message only request Option 66 but not Option 150, then server can transmit TFTP server address to client by response message.
- Delete the address pool with TFTP server address and the corresponding TFTP server configuration information.

Use the global configuration command **no ip dhcp server tftp-server ip-pool *ip-pool*** to delete TFTP server configuration in the current address pool. Return the error if designated ip address pool is absent.

Configuration example:

Raisecom#**config**

Raisecom(config)#**ip dhcp server tftp-server 192.168.0.1 ip-pool pool 1**

Raisecom(config)#**exit**

Raisecom#**show ip dhcp server ip-pool**

The result is shown below:

Name of ip pool table : pool1
Status of IP pool table: active
IP address range: 192.168.1.100 - 192.168.1.200
Mask: 255.255.255.0
Including IP Interface: 4
IP address of gateway: 192.168.1.1
IP address of DNS server: 192.168.1.1
IP address of secondary DNS server: 10.168.0.1
IP address of TFTP server: 192.168.0.1
Boot-file name: --

Valid IP pool count : 1
Valid IP address count : 101
Allotted IP address count : 0

15.3.2.7 Boot filename configuration

Boot file contains client boot image, which is the loading operating system. So in the process of client automatic configuration, in addition to the configuration of TFTP server IP address or a host name, still need to be designate the boot filename, acquire and execute designated boot image in designated server so as to complete automatic configuration.

If the request message Option 55 contains the corresponding parameters of Option67, then the server will transmit boot filename to client by response message while assigning IP address for client. The client can acquire designated configuration file in the TFTP Server to perform automatic configuration.

The configuration step is as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp sever bootfile <i>filename ip-pool WORD</i>	Configure boot filename
3	exit	Return to privileged EXEC mode
4	show ip dhcp server ip-pool	Show configuration information of DHCP server

Note:

- Before performing the command to configure boot filename for client, make sure that the DHCP server has already configured designated IP address pool.
- If performing this command in the same address pool for many times, the new configuration needs to cover the previous boot filename configuration.
- The length of boot filename is 1-63 characters. Beyond the scope of length, the configuration will fail.
- Delete the address pool with boot filename and the corresponding boot filename configuration information.

Use the global configuration command **no ip dhcp server bootfile ip-pool ip-pool** to delete boot filename configuration in the current address pool. Return the error if designated ip address pool is absent.

Configuration example:

Raisecom#**config**

Raisecom(config)#**ip dhcp server bootfile configuration ip-pool pool1**

Raisecom(config)#**exit**

Raisecom#**show ip dhcp server ip-pool**

The result is shown below:

```
-----
Name of ip pool table : pool1
Status of IP pool table: active
IP address range: 192.168.1.100 - 192.168.1.200
Mask: 255.255.255.0
Including IP Interface: 4
IP address of gateway: 192.168.1.1
IP address of DNS server: 192.168.1.1
IP address of secondary DNS server: 10.168.0.1
IP address of TFTP server: 0.0.0.0
Boot-file name: configuration
-----
Valid IP pool count : 1
Valid IP address count : 101
Allotted IP address count : 0
```

15.3.2.8 Option 82 state configuration

Option 82 refers to relay agent information option, which records client's position information and makes it convenient to localize the client and achieve server safety and billing control for client. In addition, the DHCP server enabled Option to 82 can formulate more flexible address allocation strategies according to options contents.

If the DHCP server is in support of Option 82, then when it receives the request message with Option 82, carry Option 82 information while configuring IP address in the response message.

If the DHCP server isn't in support of Option 82, then when it receives the request message with Option 82, need to configure IP address only for client and not carry Option 82 information in the response message.

User can configure DHCP Server nonsupport Option 82 according to the following steps:

Step	Command	Description
1	config	Enter global configuration mode

2	no ip dhcp sever relay information option	Configure DHCP Server nonsupport Option 82
3	exit	Return to privileged EXEC mode
4	show ip dhcp server	Show configuration information of DHCP server

By default, DHCP Server is in support of Option 82, use global configuration command **ip dhcp server relay information** to restore default setting.

Configuration example:

Raisecom#**config**

```
Raisecom(config)#no ip dhcp server relay information option
Raisecom(config)#exit
Raisecom#show ip dhcp server
```

The result is shown below:

DHCP Server: Enabled

IP Interface Enabled: 4

Total Number: 1

Option 82: Disabled

Max lease time: 1440 m

Min lease time: 40 m

Default lease time: 60 m

15.3.2.9 User custom options configuration

DHCP protocol provided the mechanism to transmit configuration parameters for the client through TCP/IP network and store configuration parameters and other control information in the option domain of DHCP message. Some of the options function or options content in DHCP protocol haven't make unified regulation in the RFC, to these DHCP options without any function limit in the RFC, the manufacturer can customize DHCP server function, and provide information designated by the manufacturer while assigning IP address to the client. In addition, the RFC limit for some DHCP options may no longer be able to meet the current demand and need to expand content options or use custom options to meet the demand. Because some of the DHCP option functions and contents are strictly limited by RFC, not all the options are in support of support custom. By default, except the Option 150, Option 67 and Option 82 mentioned above, there aren't other user custom options configured in the server.

The configuration step is as follows:

Step	Command	Description
1	config	Enter global configuration mode

2	ip dhcp sever option number { ascii ascii-string hex string ip-address ip-address} ip-pool WORD	Configure user custom options
3	exit	Return to privileged EXEC mode
4	show ip dhcp server ip-pool	Show configuration information of DHCP server

Note:

- Before performing the command to configure user custom options for client, make sure that the DHCP server has already configured designated IP address pool.
- If performing this command in the same address pool for many times, the new configuration needs to cover the previous user custom options configuration.
- At present, the supportive scope for user custom options is Option 2-254, not concluding Option 3, 50-56, 62, 63, 66, 67, 82, and 150.
- Every address pool can configure a maximum of 10 user custom options.
- Delete the address pool with user custom options and the corresponding user custom options configuration information.

Use the global configuration command **no ip dhcp server option number ip-pool ip-pool** to delete user custom options configuration in the current address pool. Return the error if designated ip address pool is absent.

Configuration example:

Raisecom#config

```
Raisecom(config)#ip dhcp server option 32 ascii configuration ip-pool pool1
Raisecom(config)#exit
Raisecom#show ip dhcp server ip-pool
```

The result is shown below:

```
-----
Name of ip pool table : pool1
Status of IP pool table: active
IP address range: 192.168.1.100 - 192.168.1.200
Mask: 255.255.255.0
Including IP Interface: 4
IP address of gateway: 192.168.1.1
IP address of DNS server: 192.168.1.1
IP address of secondary DNS server: 10.168.0.1
IP address of TFTP server: 0.0.0.0
Boot-file name:
DHCP Vendor-specific option 32: configuration
-----
Valid IP pool count : 1
Valid IP address count : 101
Allotted IP address count : 0
```

15.3.2.10 Lease table timeout configuration

When distributing IP address for the client, it is needed to designate the lease time of the IP address. By default the system lease time is:

- Default lease time: 30 minutes (usually it will not be used);
- The maximum lease time: 10080 minutes (7days), when the lease time that the client requests is larger than this value, the larger value will be used.
- The least lease time: 30 minutes, when the lease time that the client requests is smaller than this value, least lease time will be used; otherwise, according to the request time, if the client does not designate lease time, use the least lease time for distribution.

If the administrator needs to modify the least lease time, manual configuration is needed.

The configuration step is as follows:

Step	Command	Description
1	config	Enter global configuration mode
2 (optional)	ip dhcp sever default-lease <i>timeout</i>	Configure the IP address pool default lease time for DHCP server
3 (optional)	ip dhcp sever max-lease <i>timeout</i>	Configure the IP address pool maximum lease time for DHCP serve
4 (optional)	ip dhcp sever min-lease <i>timeout</i>	Configure the IP address pool least lease time for DHCP serve
5	exit	Return to privileged EXEC mode
6	show ip dhcp server	Show DHCP server configuration

Note: The lease time configured here is used for all the IP address of the address pool. At the same time, the maximum lease time cannot be shorter than least rent time, default lease time must be between maximum and least lease time.

Use global command **no ip dhcp server default**, **no dhcp-server max-lease**, **no dhcp-server min-lease** to cancel the current setting, and restore system default lease time setting.

Configuration example:

```
Raisecom#config
Raisecom(config)#ip dhcp server default-lease 60
Raisecom(config)#ip dhcp server max-lease 1440
Raisecom(config)#ip dhcp server min-lease 45
Raisecom(config)#exit
Raisecom#show ip dhcp server
```

The result is shown below:

```
DHCP Server: Enabled
IP Interface Enabled: 4
Total Number: 1
```

Max lease time: 1440 m

Min lease time: 40 m

Default lease time: 60 m

15.3.2.11 Relay-ip address configuration

When the client is connected with the server by DHCP Relay, DHCP server must know the neighbor DHCP Relay IP address, which needs the administrator's manual configuration as well.

The configuration step is shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp sever relay-ip ip-address ip-mask	Configure neighbor proxy IP address
3	exit	Return to privileged EXEC mode
4	show ip dhcp server relay-ip	Show DHCP server configuration

Note: Only ISCOM3000 serious switches support the command **ip dhcp server relay-op**. Here the configured neighbor proxy IP address is actually the port address that is connected with the client, as is shown in the typical example. The maximum number of neighbor proxy IP address is 8.

Use global configuration command **no ip dhcp server relay-ip ip-address** to delete neighbor proxy IP address configuration.

Configuration example:

```
Raisecom#config
Raisecom(config)#ip dhcp server relay-ip 192.168.1.1 255.255.255.0
Raisecom(config)#exit
Raisecom#show ip dhcp server relay-ip
```

The result is shown below:

index	IP address	IP Mask	Status
1	192.168.1.1	255.0.0.0	active

15.3.3 Monitoring and maintenance

Use different **show** commands to show the switch DHCP Server running and configuration situation for monitoring and maintaining. All the show commands are listed below:

Command	Description
---------	-------------

show ip dhcp server	Show DHCP Server configuration and static information
show ip dhcp server ip-pool	Show DHCP Server address pool information
show ip dhcp server relay-ip	Show the configured neighbor DHCP proxy address information
show ip dhcp server lease	Show the designated IP address and the corresponding information

Note:

- Only ISCOM3000 serial switches supports the command **show ip dhcp server relay-ip**
- Before using **show ip dhcp server lease**, the system time should better be configured accurately, because lease time limit is computed according to the system date absolute time.

Use **show ip dhcp server** command to look over the configuration information, like global or IP port configuration information, static information or so.

Raisecom#**show ip dhcp server**

DHCP Server: Enabled

IP Interface Enabled: 4

Total Number: 1

Option 82: Enabled

Max lease time: 1000 m

Min lease time: 32 m

Default lease time: 300 m

Statistics information:

Running time: 0 hours 7 minutes 33 seconds

Bootps: 0

Discover: 0

Request: 0

Release: 0

Offer: 0

Ack: 0

Nack: 0

Decline: 0

Information: 0

Unknowns: 0

Total: 0

Use the command **show ip dhcp server ip-pool** to show the configured address pool information:

Raisecom#**show ip dhcp server ip-pool**

Name of IP pool table: dhcp

Status of IP pool table: active

IP address range: 11.1.1.33 - 11.1.1.44

Mask: 255.255.255.0

Including IP Interface: 4

*IP address of gateway: 0.0.0.0
 IP address of DNS server: 0.0.0.0
 IP address of secondary DNS server: 0.0.0.0
 IP address of TFTP server: 100.0.0.1
 Boot-file name: config
 DHCP Vendor-specific option 32: 10.100.0.1*

*Valid IP pool count: 1
 Valid IP address count: 12
 Allotted IP address count: 0*

Use the command **show ip dhcp server relay-ip** to show the configured neighbor proxy address information:

Raisecom#**show ip dhcp server relay-ip**

In English:

<i>Index</i>	<i>IP Address</i>	<i>IP Mask</i>	<i>Status</i>
1	11.1.1.34	255.255.255.0	active

Use the command **show ip dhcp server lease** to show the configured neighbor proxy address information.

Raisecom#**show ip dhcp server lease**

<i>IP Address</i>	<i>Hardware Address</i>	<i>Lease Expiration</i>	<i>IP Interface</i>
172.16.1.11	00:a0:98:02:32:de	Feb-01-2006 11:40:00	1
172.16.3.254	02:c7:f8:00:04:22	Jul-01-2006 23:00:00	1

Character instruction:

- IP Address: the client IP address;
- Hardware Address: the client MAC address
- Lease Expiration: lease timeout limit
- IP Interface: IP interface number

Lease timeout limit is computed according to system date, format is mm-dd-yy hh:mm:ss

15.3.4 Typical configuration example

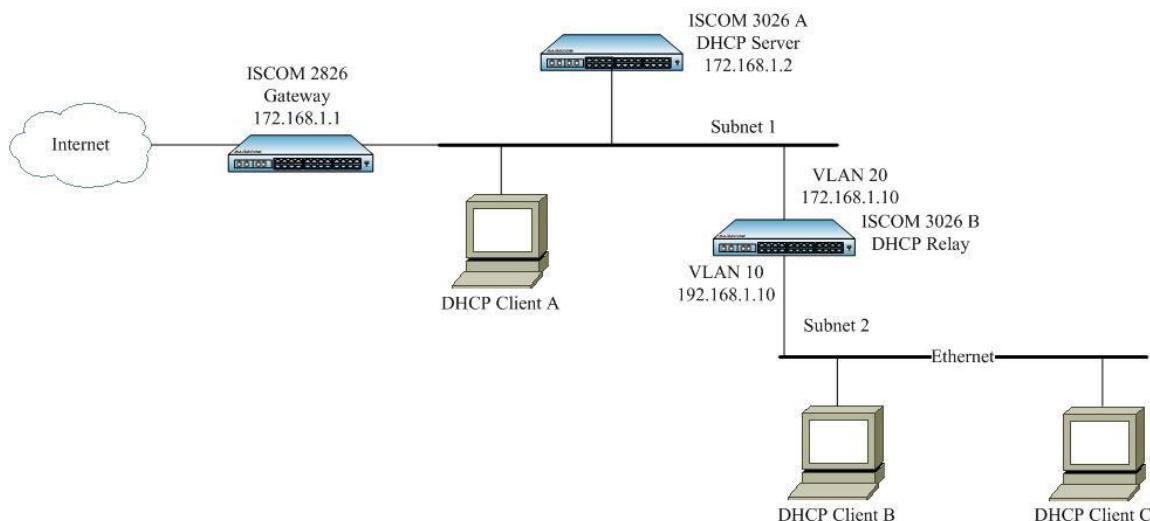
Note: ISCOM2128EA-MA products are not in support of routing.

The typical DHCP Relay and Server configuration case is as below:

- Direct connection to the client for IP address
- The client get IP address through proxy

The example is simple and typical in realizing DHCP protocol. Specific connection state is shown as below. In the figure ISCOM3026, as DHCP Relay, divides the two VLAN: VLAN 10 and VLAN 20, the two corresponding subnet IP address are 192.168.1.10 and 172.168.1.10 respectively. The DHCP server is ISCOM3026A, IP address is 172.168.1.2, suppose the subnet NDS be 172.168.1.3, subnet 1 and subnet 2 needs to get connection to public network through gateway 172.168.1.1. To realize the client accessing the resource of the public network, it is only needed to configure DHCP Server and DHCP Relay correctly.

2. Topology figure



Typical configuration example

3. Configuration steps

Configure DHCP Server:

➤ **Configure VLAN and interfaces:**

```
Raisecom(config)#create vlan 20 active
```

```
Raisecom(config)#interface port 1
```

```
Raisecom(config-port)#switchport access vlan 20
```

```
Raisecom(config-port)#exit
```

```
Raisecom(config)#interface ip 2
```

```
Raisecom (config-ip)#ip address 172.168.1.2 255.255.0.0 20
```

➤ **Configure address pool**

Configuring a address pool for both subnet 1 and subnet 2 respectively.

```
Raisecom (config)#ip dhcp server ip-pool pool1 172.168.1.100 172.168.1.200 255.255.0.0 ip 2
gateway 172.168.1.1 dns 172.168.1.3
```

```
Raisecom(config)#ip dhcp server ip-pool pool2 192.168.1.100 192.168.1.200 255.255.255.0 ip 2
gateway 172.168.1.1 dns 172.168.1.3
```

```
Raisecom (config)#exit
```

```
Raisecom #show ip dhcp server ip-pool
```

➤ **Start DHCP Server service**

Raisecom (config)#**ip dhcp server**

Raisecom(config)#**interface ip 2**

Raisecom(config-ip)#**ip dhcp server**

Raisecom #**show ip dhcp server**

➤ **Configure neighbour proxy IP address**

Raisecom (config)#**ip dhcp server relay-ip 192.168.1.10 255.255.255.0**

Raisecom (config)#**exit**

Raisecom #**show ip dhcp server relay-ip**

➤ **Configure the router**

Raisecom (config)#**ip route 192.168.1.0 255.255.255.0 172.168.1.10**

➤ **Configure DHCP Relay**

Create VLAN and the interface

Raisecom (config)#**create vlan 10 active**

Raisecom (config)#**interface port 1**

Raisecom(config-port)#**switchport access vlan 10**

Raisecom(config-port)#**exit**

Raisecom (config)#**interface ip 2**

Raisecom(config-ip)#**ip address 192.168.1.10 255.255.255.0 10**

Raisecom (config)#**create vlan 20 active**

Raisecom (config)#**interface port 2**

Raisecom(config-port)#**switchport access vlan 20**

Raisecom(config-port)#**exit**

Raisecom (config)#**interface ip 3**

Raisecom (config-ip)#**ip address 172.168.1.10 255.255.0.0 20**

➤ **Enable router function**

Raisecom(config-ip)#**exit**

Raisecom(config)#**ip routing**

➤ Configure DHCP server IP address

```
Raisecom(config)#ip dhcp relay ip-list 2 target-ip 172.168.1.2
```

```
Raisecom (config)#exit
```

```
Raisecom #show ip dhcp relay
```

➤ Start DHCP Relay

```
Raisecom (config)#ip dhcp relay
```

```
Raisecom(config)#exit
```

```
Raisecom #show ip dhcp relay
```

The client will be configured as auto acquiring IP address through DHCP.

4. Show the result

- Show DHCP configuration static information, address pool information and the configured IP address information.

On ISCOM3026A use the command **show ip dhcp server**、**show ip dhcp server ip-pool** and **show ip dhcp server lease**.

- Show DHCP Relay information

On switch device(OLT) use the command **show ip dhcp relay**.

➤ Show client A

```
c:\>ipconfig /all
```

Ethernet adapter: local connection:

Connection-specific DNS Suffix . :

Description : Realtek RTL8139/810x Family Fast Ethernet NIC

Physical Address. : 00-50-8D-4B-FD-27

DHCP Enabled. : Yes

Autoconfiguration Enable. : Yes

IP Address. : 172.168.1.100

Subnet Mask. : 255.255.0.0

Default Gateway. : 172.168.1.1

DHCP server. : 172.168.1.2

DNS Servers. : 172.168.1.3

Lease Obtained. : 13:03:24

Lease Expires. : 13:33:24

➤ Show client B

```
c:\>ipconfig /all
```

Ethernet adapter: local connection:

Connection-specific DNS Suffix . :

Description : Realtek RTL8139/810x Family Fast Ethernet NIC

Physical Address.....: 00-50-8D-4B-DE-46
DHCP Enabled.....: Yes
Autoconfiguration Enable...: Yes
IP Address.....: 192.168.1.100
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 172.168.1.1
DHCP server.....: 172.168.1.2
DNS Servers.....: 172.168.1.3
Lease Obtained.....: 13:03:24
Lease Expires.....: 13:33:24

- Show client C:

Client C is the same with client B in content, the IP address is 192.168.1.101

15.3.5 DHCP Server trouble shooting

- As per ISCOM3000 series switches, don't specify the IP address of the relay agent, the equipment can't accurately realize DHCP relay functions; ISCOM2800/2900 switches don't support the DHCP agent
- When setting neighbor agent, error is likely caused by: address is beyond the maximum limit(8); IP address is not correct;
- When setting IP-pool, error is likely caused by: ip-pool is above the maximum limit(4); IP address or other parameter is not correct;
- If delete ip-pool failed, the reason is probably that the input parameters are not correct; ip-pool does not exist.

If after above setting, the system still cannot work normally, check whether a DHCP server has the default gateway or routing, and check whether DHCP Relay opened the routing functions.

15.4 DHCP Relay Configuration

The part is about how to configure and maintain DHCP Relay on the switch, concluding the following contents:

- ❖ DHCP Relay principle overview
- ❖ DHCP Relay configuration
- ❖ Monitoring and maintenance
- ❖ Typical configuration example
- ❖ DHCP Relay trouble shooting

15.4.1 DHCP Relay principle overview

Early DHCP protocol is suitable for only the situation that the client and server are in the same subnet, which cannot go through network sections. Therefore, for dynamical host configuration, configuring a DHCP server on all the network sections is needed, which is obviously wasteful.

The introduction of DHCP Relay solves this problem: the local network client can communicate with the other subnet DHCP servers by DHCP Relay, and get the legal IP address finally. Thus, the DHCP client on several networks can use the same DHCP server, which decreases the cost and helps

centralized management

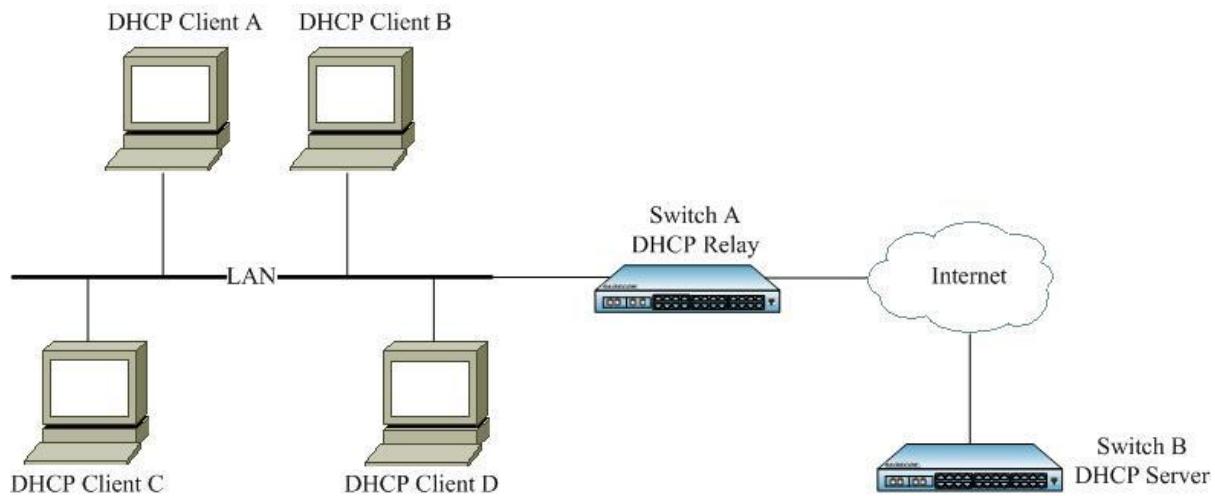
DHCP Relay provides DHCP broadcast message transparent transmission function, which is able to transmit the broadcast message of DHCP client (or server) transparently to the other network section DHCP server (or client).

In the process that DHCP Relay completes dynamic configuration, the processing way that DHCP client and server takes is basically the same with that of not through DHCP Relay. The following steps are only about DHCP Relay transmission:

- (1) DHCP client transmits DHCP-DISCOVER message in broadcasting.
- (2) When the network equipment with DHCP Relay function receives the broadcast message, by configuration it will transmit the message to the specific DHCP server in unicast.
- (3) DHCP server makes IP addresses distribution, and sends the configuration information to the client through DHCP Relay.

Usually, DHCP Relay can be host, two-layer switch, three-layer switch or router, if only DHCP Relay service program is enable.

The figure below is a typical DHCP Relay application:



DHCP Relay typical application

The mechanism of DHCP Relay support Option 82 is shown below:

- (1) DHCP client sends out request message in the form of broadcasting when initialized.
- (2) The DHCP Relay equipment that is connected with local network will receive the broadcast message, check out if there has been Option 82 in the message, and handles it in the corresponding way.
- (3) If there has been Option 82 in the message, the equipment will follow the configured strategy to handle the message (drop, replace the Option 82 in the message that has been there with the relay equipment's Option 82 or keep the Option 82 that has been there), and transmits the request message to DHCP server.
- (4) If there is no Option 82 in the request message, the Option 82 of DHCP equipment will be added into the message (located in the end of all the options) and be transmitted to DHCP server. At this time, the Option 82 of the request message contains the port number of the switch which is connected with DHCP client, the number of the VLAN that the port belongs to and the DHCP Relay equipment's own MAC address and so on.

(5) When DHCP server receives the DHCP request message that is transmitted by DHCP Relay equipment, it will record the information from Option in the message, then transmit the message that contains DHCP configuration information and Option 82 information.

(6) After DHCP Relay receives the response message of DHCP server it will peel off the message's Option 82 information, then transmit the message that contains DHCP configuration information to DHCP client.

Note: there are two sorts of request messages from DHCP client, DHCP-DISCOVER and DHCP-REQUEST message. Because of the different mechanisms that different manufacturers' DHCP server handle request messages, some equipments handle DHCP-DISCOVER message's Option 82 information, while some others handle DHCP-REQUEST message's Option 82 information, so DHCP Relay handles both the two messages in the strategy of Option 82.

Otherwise, if DHCP Relay receives the messages sent out from the two DHCP client DHCP-DECLINE and DHCP-INFORM, it will handle Option 82 uniformly according to the strategy, without affecting its basic function of supporting Option 82.

15.4.2 Configure DHCP Relay

15.4.2.1 Default DHCP Relay configuration

The following table is the default configuration steps of DHCP Relay:

Function	Default value
Global DHCP Relay state	Disabled
IP port DHCP Relay state	Enabled
IP port's destination IP address	N/A
DHCP Relay support Option 82	Disabled
The strategy of DHCP Relay handling option 82 request messages	Replace
Port DHCP Relay trust	Untrusted

15.4.2.2 DHCP Relay configuration guide

- Make sure the DHCP Snooping on the switch is not started; Global DHCP Relay must be started;
- If on a IP port DHCP Relay is not started, it cannot work on this IP port;
- When DHCP Relay is on, DHCP Snooping cannot be started either on the switch;
- Make sure the DHCP server that is connected with DHCP Relay has correct configuration and connection to the client. DHCP server must be ISCOM 3000 series switches. Except making sure the correct configuration of IP port addresses and address pool, correct configuration to the neighbor proxy address and Relay addresses;
- If the client acquires IP address automatically from DHCP server through multiplex Relay, you must make sure the connection of each equipment and correct configuration. The DHCP Relay number between the client and server, cannot exceed 16 in RFC1542 rules, it is usually suggested not to exceed 8.

15.4.2.3 Configure global DHCP Relay

By default, global DHCP Relay is off. Only when global DHCP Relay is on can the switch DHCP Relay takes effect. User can take the following steps to start global DHCP Relay.

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp relay	Start global DHCP Relay
3	exit	Return to privileged EXEC mode
4	show ip dhcp relay	Show DHCP Relay configuration

Note: If the switch starts DHCP Snooping, it cannot start global DHCP Relay. On the opposite, if the switch starts global DHCP Relay, it cannot start DHCP Snooping.

Use global command **no ip dhcp relay** to disable global DHCP Relay.

15.4.2.4 Configure IP port DHCP Relay

By default, IP port DHCP Relay function is on, user can use IP port command **no ip dhcp relay** to disable IP port DHCP Relay function. To start IP port DHCP Relay, use IP port command **ip dhcp relay**.

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 4	Enter IP port 4 configuration mode
3	ip dhcp relay	Start DHCP Relay
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp relay	Show DHCP Relay configuration

Note: When global DHCP Relay is off, on a certain IP port DHCP Relay can be started in advance. But only when global DHCP Relay starts can the DHCP Relay started on this port takes effect.

15.4.2.5 Configure IP port destination IP address

When the client equipment and DHCP server is not in the same broadcasting domain, the relay equipment in the middle must be able to transmit the kind of broadcasting packet. Configure the destination IP address of DHCP Relay points out the destination address of the DHCP broadcasting packet from DHCP client for the relay equipment.

When DHCP Relay is configuring destination IP address, use network port LIST for the convenience

of user's configuration. That is to say, according to the actual need, one command can be used to configure the same IP address for parts of the network ports or all the ports.

When DHCP Relay is configuring destination IP address, except the configuration commands in config mode, you can also configure the port's corresponding destination IP address in IP port, which is flexible.

Take the following steps to configure the port's destination IP address.

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp relay ip-list all target-ip 10.199.0.200	For all the IP ports configure the destination IP 10.199.0.200
3	ip dhcp relay ip-list 1-3 target-ip 10.200.0.200	For IP port 1-3 configure the destination IP 10.200.0.200
4	interface ip 3	Enter IP port 3 configuration mode
5	ip dhcp relay target-ip 10.201.0.200	Configure the destination IP 10.201.0.200
6	exit	Return to global configuration mode

Note:

- Here, the configured maximum destination IP address number for each port is 4. At the same time, make sure that the destination IP address is correct.
- When it comes to configuring destination IP address for several IP ports in one command, if configuring the destination IP address in a certain port fails, the rest IP port destination IP address configuration should be continued and return the cue which specific port configuring destination IP address fails, the format is: IP interface %s set target IP address unsuccessfully. Use IP table to replace %s in actual use. If only one port is configured successfully, the command line will return 'configuration successful' finally.

Use global configuration command **no ip dhcp relay ip-list target-ip** to delete the configured destination IP address of the IP port, or IP interface configuration command **no ip dhcp relay target-ip** in the corresponding port configuration mode.

Configuration example:

```
Raisecom#config
Raisecom(config)# ip dhcp relay ip-list all target-ip 10.199.0.200
Raisecom(config)# ip dhcp relay ip-list 1-3 target-ip 10.200.0.200
Raisecom(config)#interface ip 3
Raisecom(config-ip)#ip dhcp relay target-ip 10.201.0.200
Raisecom(config-ip)#exit
Raisecom(config)#exit
Raisecom#show ip dhcp relay
```

The result is shown below:

DHCP Relay: Enabled

<i>IP Interface</i>	<i>Enabled Status</i>	<i>Target IP Address</i>
0	<i>enabled</i>	10.199.0.200
1	<i>enabled</i>	10.199.0.200
		10.200.0.200
2	<i>enabled</i>	10.199.0.200
		10.200.0.200
3	<i>enabled</i>	10.199.0.200
		10.200.0.200
		10.201.0.200
4	<i>enabled</i>	10.199.0.200
...
...

15.4.2.6 Configure DHCP Relay support option 82

By default, DHCP Relay do not support option 82, in global configuration mode use **ip dhcp relay information option** to start DHCP Relay support option 82.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp relay information	Start DHCP Relay support option 82
3	exit	Return to privileged EXEC mode
4	show ip dhcp relay information	Show DHCP Relay support Option 82 configuration information and port trust list

Note: To active DHCP Relay support option 82, enable global DHCP Relay service first. To make option 82 function available, corresponding configuration on DHCP Server is needed.

Use global configuration command **no ip dhcp relay information option** to disable DHCP Relay support Option 82.

15.4.2.7 Configure DHCP Relay request message handling strategy

By default, DHCP Relay handling strategy to the client request messages is Replace, that is to fill Option 82 in the way of normal or verbose, replace the Option 82 contents that has been there and transmit it. In global configuration mode use the command **ip dhcp relay information policy {drop/keep/replace}** to configure the message handling strategy of DHCP Relay as drop, keep or replace.

The configuration steps are as follows:

Step	Command	Description
-------------	----------------	--------------------

1	config	Enter global configuration mode
2	ip dhcp relay information policy {drop / keep / replace} [schedule-list list-no]	Configure DHCP Relay request message handling strategy
3	exit	Return to privileged EXEC mode
4	show ip dhcp relay information	Show DHCP Relay handling strategy to client request message

Note: The command configured request message handling strategy can available only in DHCP Relay support Option 82.

Use global configuration command **no ip dhcp relay information policy {drop / keep / replace} [schedule-list list-no]** to recover default DHCP Relay handling strategy to Option 82.

The configuration example:

```
Raisecom#config
```

```
Raisecom(config)# ip dhcp relay information policy keep
Raisecom(config)#exit
Raisecom#show ip dhcp relay information
```

The result is shown below:

Option 82: Enabled

Policy: Keep

<i>Port</i>	<i>Trusted</i>

...	...

15.4.2.8 Port DHCP Relay trust configuration

By default, if one DHCP message gateway address part is 0 and relay agent information option part (option 82) exists, then DHCP Relay will drop messages of this kind. If DHCP Relay is required to transmit messages of this kind, use the command to configure DHCP Relay port trust. After the specific port has configured DHCP Relay port trust command, these port can transmit this kind of DHCP messages normally. You can also use the key word all to set all the system port Relay Agent Information Option port trust.

When configuring port trust, except the configuration commands in config mode, you can configure the port trust state under the port directly as well, which is flexible.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp relay information trusted port-list 1-7	Set port 1-7 to trusted port

3	interface ip 8	Enter port 8 configuration mode
4	ip dhcp relay information trusted	Configure the destination IP 10.201.0.200
5	exit	Return to global configuration mode
6	exit	Return to privileged EXEC mode
7	show ip dhcp relay information	Show DHCP Relay support Option 82 configuration information and port trust table

Note: Only when DHCP Relay support Option 82 can port trust take effect.

Use global configuration command **no ip dhcp relay information port-list** to set the port to distrust port, in the corresponding port configuration mode use port configuration command **no ip dhcp relay information option** to realize it.

Configuration example:

Raisecom#**config**

Raisecom(config)# **ip dhcp relay information trusted port-list 1-7**

Raisecom(config)#**interface ip 8**

Raisecom(config-port)# **ip dhcp relay information trusted**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show ip dhcp relay information**

Option 82: Disabled

Policy: Replace

<i>Port</i>	<i>Trusted</i>
1	<i>yes</i>
2	<i>yes</i>
3	<i>yes</i>
4	<i>yes</i>
5	<i>yes</i>
6	<i>yes</i>
7	<i>yes</i>
8	<i>yes</i>
...	...
...	...

15.4.3 Monitoring and maintenance

Use different show commands to show switch DHCP Relay running state and configuration state for monitoring and maintaining. All the show commands are listed below:

Note: ISCOM2128EA-MA products are not in support of ip-pool.

Command	Description
show ip dhcp relay	Show DHCP Relay configuration.
show ip dhcp relay statistics	Show DHCP Relay static.
show ip dhcp relay information	Show the configured neighbor DHCP proxy address information.

Use the command **show ip dhcp relay** to show DHCP Relay basic configuration information, including DHCP Relay state, IP port DHCP Relay state and the corresponding DHCP proxy destination IP address.

Raisecom#**show ip dhcp relay**

DHCP Relay: Enabled

IP Interface	Enabled Status	Target IP Address
0	<i>enabled</i>	10.199.0.200
1	<i>enabled</i>	10.199.0.200
		10.200.0.200
2	<i>enabled</i>	10.199.0.200
		10.200.0.200
3	<i>enabled</i>	10.199.0.200
		10.200.0.200
4	<i>enabled</i>	10.199.0.200
...
...

Use the command **show ip dhcp relay statistics** to show DHCP Relay static, including DHCP Relay running time and received/sending messages number.

Raisecom#**show ip dhcp relay ip-pool**

Runtime: 0 hours 23 minutes 34 seconds

Packet Type	Receive	Send
Bootp	0	0
Discover	1	1
Request	1	1
Decline	0	0
Offer	0	0
Ack	0	0
Nack	0	0
Decline	0	0
Inform	0	0
Unknowns	0	0

Total	2	2
-------	---	---

Use the command **show ip dhcp relay information** to show HDCP Relay support Option 82 configuration information and port trust table:

Raisecom#**show ip dhcp relay information**

Option 82: Enabled

Policy: Replace

<i>Port</i>	<i>Trusted</i>
1	<i>yes</i>
2	<i>no</i>
3	<i>yes</i>
4	<i>yes</i>
...	...

Note:

DHCP Relay supporting Option 82 includes:

- Enabled
- Disabled

The strategy includes:

- Drop
- Keep
- Replace

15.4.4 Typical configuration example

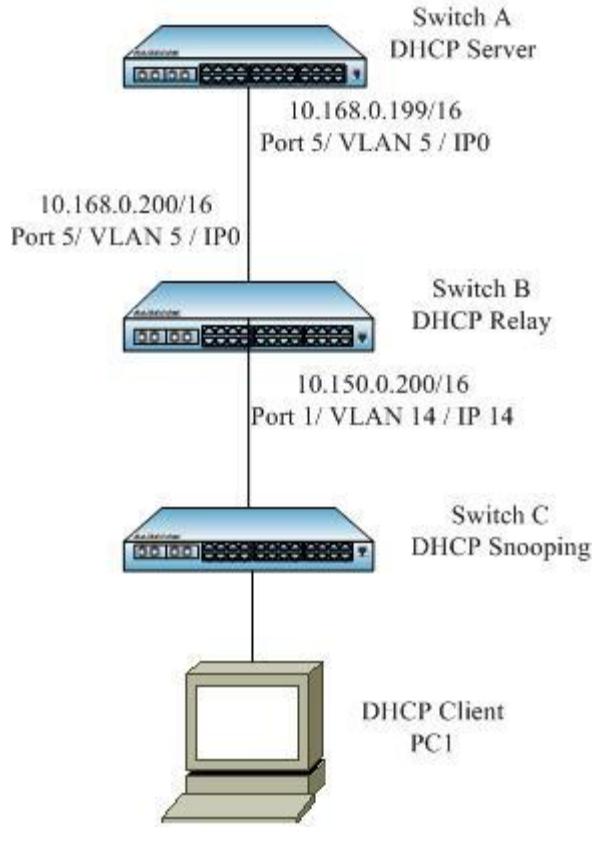
Note: ISCOM2128EA-MA products are not in support of routing.

DHCP Relay typical configuration example is like DHCP Server typical configuration example. The following is about a example that the client using DHCP Snooping connects to DHCP Relay and get IP address.

1.Configuration instruction

- 1: The connection of starting Snooping on DHCP Snooping equipment is as fig 3-2, start DHCP Snooping support option 82, and set port 2 to DHCP Snooping trust port.
- 2: DHCP Relay divides two subnets; the connection between it and the client and the server connection and configuration is as the figure below. Follow the figure to configure VLAN, IP port address and the VLAN that the port belongs to.
- 3: DHCP Server divides two subnets, establish correct address pool (10.150.0.2 – 10.150.0.100) on the subnet, start DHCP Server function at the same time and configure relay-ip shown in the figure (consult DHCP Server module configuration guide). Then follow the figure to configure VLAN, IP port address and VLAN the port belongs to, and configure it to the router belongs to 10.150 network segment.
- 4: Set PCI to auto acquiring IP address.

2.Topology figure



3.Configuration steps

Configure DHCP Relay:

- Start global DHCP Relay

```
Raisecom (config)#ip dhcp relay
```

- Prot 14 configure destination IP address

```
Raisecom (config)# ip dhcp relay ip-list 14 target-ip 10.168.0.199
```

- Start DHCP Relay support option 82

```
Raisecom (config) #ip dhcp relay information option
```

- Configure port 1 as DHCP Relay trust port

```
Raisecom (config) #ip dhcp relay information trusted port-list 1
```

- Open the router function

```
Raisecom (config)# ip dhcp relay ip routing
```

4.Show the result

- Show the client PC1

```
C:\>ipconfig /all
```

```
Ethernet adapter local connection
```

Connection-specific DNS Suffix . . . :
Description : Realtek RTL8139/810x Family Fast Ethernet NIC
Physical Address : 00-50-8D-4B-FD-27
DHCP Enabled : Yes
Autoconfiguration Enable : Yes
IP Address : 10.150.0.0
Subnet Mask : 255.255.0.0
Default Gateway :
DHCP server : 10.168.0.199
DNS Servers :
Lease Obtained : Apr-08-2007 13:03:24
Lease Expires : Apr-08-2007 13:33:24

15.4.5 DHCP Relay trouble shooting

- If the correct destination IP address is not designated, DHCP Relay cannot transmit the message correctly.
- If the gateway address field of a DHCP message is 0 and relay agent information option field exists, DHCP Relay distrusted port will drop messages of this kind.

If the configuration above still cannot help, please examine if DHCP Relay has started router function, and examine if DHCP server address is correctly configured, if the neighbor proxy default gateway or router is configured.

15.5 DHCP OPTION configuration

15.5.1 DHCP OPTION principle

The DHCP request message has a variety of options, including a special option exists in DHCP SNOOPING, DHCP RELAY, DHCP SERVER, to identify a client position. This option is OPTION82, which include circuit-id and remote-id. Through them, the SERVER can obtain client position for effectively management.

15.5.2 DHCP OPTION configuration

15.5.2.1 Default configuration

Function	Default value
global attach-string	None
global remote-id	switch-mac
port circuit-id	None

15.5.2.2 DHCP OPTION configuration guide

DHCP OPTION can be configured if DHCP SNOOPING and DHCP RELAY are available.

15.5.2.3 Global DHCP OPTION attach-string

By default, global DHCP OPTION attach-string is empty. OPTION82 format in DHCP OPTION is:
Port/VLAN/attach-string

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp information option attach-string raisecom	Configure DHCP OPTION attach-string as raisecom
3	exit	Return to privileged EXEC mode
4	show ip dhcp information option	Show DHCP OPTION configuration

15.5.2.4 Port DHCP OPTION circuit-id

By default, port circuit-id is empty. OPTION82 format in DHCP OPTION is: circuit-id.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port 10	Enter port 10 configuration
3	ip dhcp information option circuit-id raisecom	Configure circuit-id on port 10 as raisecom
4	exit	Return to global EXEC mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp information option	Show DHCP OPTION configuration

15.5.2.5 Global DHCP OPTION remote-id

By default, remote-id mode is switch-mac. After the configuration, DHCP OPTION82 will be sent by the configured mode.

- switch – mac: remote - id is sent by switch MAC address in binary form;
- client-mac : remote - id is sent by client MAC address in binary form
- switch-mac-string: remote - id is sent by switch MAC address string
- client-mac-string: remote - id is sent by client MAC address string
- hostname: remote- id is sent by user-defined host name
- string STRING: remote- id is sent by user-defined string

Step	Command	Description
1	config	Enter global configuration mode

2	ip dhcp information option remote-id switch-mac-string	Set remote-id mode transmitted by switch-mac-string
3	exit	Return to privileged EXEC mode
4	show ip dhcp information option	Show DHCP OPTION configuration

15.5.3 Monitoring and maintenance

Use **show** command to look over DHCP OPTION configuration information so as to make monitoring and maintenance.

Command	Description
show ip dhcp information option	Show DHCP OPTION configuration

Through above **show ip dhcp information option** command, users can look over the configuration information of DHCP OPTION, concluding global DHCP OPTION82 circuit-id state, port circuit-id configuration as well as remote-id configuration mode.

Raisecom#**show ip dhcp information option**

DHCP Option Config Information

Attach-string: raisecom

Remote-ID Mode: switch-mac

15.5.4 Typical configuration example

1. If the carrier do not configure OPTION module

If the carrier do not configure DHCP OPTION, the switch will mark the client device position in default way:

Vlan \Port number\ switch-mac

2. If the carrier wants to mark the client device position

➤ If the carrier wants to mark the client device position in the way of attach-string

Configure attach-string in global configuration mode

Raisecom(config)#**ip dhcp information option attach-string STRING**

The client position information is as follows:

Port number\VLAN\STRING MAC address (the carrier can choose MAC address mode)

➤ If the carrier wants to mark client device position completely in its own way

In port configuration mode, the carrier is able to mark the client position in its own way, for example, one carrier needs the client mark shown as follows:

Option 1

<Access-Node-Identifier>/PON/<rack> / <shelf> / <slot> / <PON> : <ONT> . <ONT-slot> . <UNI>

Circuit-id can be configuring to the needed format in port mode, the steps are as follows:

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode
2	interface port 10	Enter port 10 configuration mode
3	ip dhcp information option circuit-id CHINA/PON/1/1/08/01:28.1.10	Configure port 10 circuit-id to CHINA/PON/1/1/08/01:28.1.10
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp information option	Show DHCP OPTION module configuration

Chapter 16 RMON Function Configuration

16.1 RMON principle overview

The RMON refers to the IETF designated standards to monitor network data through different network agent and management station system; it can make the SNMP monitor remote device more effective and more actively, the network administrator can track the network, network segment or equipment fault more quickly. The method reduces the data flow between management station and agent, make it possible to manage the network simply and effectively, make up for the SNMP limitations in the growing distributed Internet.

We can monitor the network situation of all management switches through SNMP Agent. At present, the groups of RMON1, 2, 3, 9 have already completed the configuration. They are statistics group, history group, alarm group and event group.

- Statistics group gathers the statistic information on one port, including message count and size distribution statistics.
- History group is similar to statistics group, but it gathers statistics information just in a designated inspecting period.
- Alarm group is in a designated time period to monitor a designated MIB (Management Information Bank) target and set the ascending and descending threshold; it will trigger an event if the monitoring target reaches the threshold.
- When alarm group triggers an event, event and alarm groups will join together to record the related information, such as transmit TRAP, write in LOG and etc.

16.2 RMON configuration

16.2.1 Default configuration

Function	Default value
Statistics group	Open
History group	Close
Alarm group	N/A
Event group	N/A

16.2.2 RMOB statistics group configuration

Set statistics function parameter of the interface, if it is close, use this command to open again; if it is open, use this command to change the related parameter. By default, open the statistics function of all ports (including lay-3 interface and physical port).

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode
2	rmon statistics {ip 0- MAX_SW_STR port-list 1- MAX_PORT_STR } [owner STRING]	Set statistics function parameter of the interface; <i>l3_interface</i> : The scope of statistics function for l3_interface layer-3 is 0- MAX_SW_STR; <i>port_list</i> : The scope of statistics function for port_list physical port is 1- MAX_PORT_STR; <i>STRING</i> : the owner name of statistics group
3	exit	Exit global configuration mode and enter privileged EXEC mode
4	show rmon statistics	Show the information of statistics group

Use the command **no rmon statistics {ip 0- MAX_SW_STR | port 1- MAX_PORT_STR}** to close statistic group.

Note: Closing the statistic function of a port indicates users cannot continue to acquire the statistics data from this port, but it doesn't mean the device stops making data statistics.

16.2.3 RMON history statistics group configuration

Set history statistics function parameter of the interface, if it is close, use this command to open again; if it is open, use this command to change the related parameter. By default, close the history statistics function of all ports (including lay-3 interface and physical port), use **rmon history** command to open it again.

No longer to make data collection statistics when closed the history group function and simultaneously clear away all the previous history date.

Step	Command	Description
1	config	Enter global configuration mode
2	rmon history {ip 0-MAX_SW_STR port-list 1-MAX_PORT_STR } [shortinterval <1-600>] [longinterval <600-3600>] [buckets <10-1000>] [owner STRING]	Set history statistics group function parameter of the interface; <i>0-MAX_SW_STR</i> : The scope of statistics function for layer-3 interface is 0- MAX_SW_STR; <i>1-MAX_PORT_STR</i> : The scope of statistics function for physical port is 1- MAX_PORT_STR; <i><1-600></i> : The short interval for history collection is 1-600s; <i><600-3600></i> : The long interval for history collection is 600-3600s; <i><10-1000></i> : saves the circular queue size of history data, the scope is 10-1000; <i>STRING</i> : the owner name of history statistics group
3	exit	Exit global configuration mode and enter privileged EXEC mode

4	show rmon history { ip <0-"<i>MAX_SW_STR</i>" port <1-"<i>MAX_PORT_STR</i>" }	Show the information of history statistics group
---	--	--

16.2.4 RMON alarm group configuration

Use **rmon alarm** command to set RMON alarm group cases and monitor MIB variable. Use the command **no** to delete an alarm.

The monitoring MIB variables must be real, and belong to INTEGER of ASN.1, such as INTEGER, Counter, Gauge, TimeTicks etc. Return the error if the variable is absent or the type is incorrect. If the variable can't be collected in successfully setting alarm, then the alarm is closed; set the alarm again if you want to monitor the variables.

If you haven't set the trigger events index number, the default value is 0, says it will not trigger events, because 0 is not an effective events number. If the index number isn't 0, but you haven't set the event in corresponding event group, the event still cannot be triggered successfully when variable is over proof until the event is set.

Step	Command	Description
1	config	Enter global configuration mode
2	rmon alarm <1-65535> MIBVAR [interval <2-3600>] {delta absolute} rising-threshold <0-2147483647>₁ [<1-65535>₁] falling-threshold <0-2147483647>₂ [<1-65535>₂] owner STRING	Set alarm group function parameter of the interface; <i><1-65535></i> : alarm index number, the scope is <i><1-65535></i> ; MIBVAR designates the monitoring MIBtarget; <i><2-3600></i> : takes second as the unit to monitor the interval of MIB target; <i><0-2147483647>₁</i> : the rising threshold; <i><1-65535>₁</i> : the event number for reaching rising threshold; <i><0-2147483647>₂</i> : falling threshold; <i><1-65535>₂</i> : the event number for reaching falling threshold; <i>STRING</i> : the owner name of alarm group
3	exit	Exit global configuration mode and enter privileged EXEC mode
4	show rmon alarms <1-65535>	Show the configuration result

Use the command **no rmon alarm <1-65535>** to delete alarm.

16.2.5 RMON event group configuration

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode
2	rmon event <1-65535> [log] [trap community STRING₁] [description STRING₂] [owner STRING₃]	Set event group function parameter of the interface; <1-65535>: event index number STRING ₁ : SNMP community name STRING ₂ : description character string STRING ₃ : the owner name of event group
3	exit	Exit global configuration mode and enter privileged EXEC mode
4	show alarm <1-65535>	Show the configuration result and event index number

Use the command **no event <1-65535>** to delete event.

16.3 Monitoring and maintenance

Command	Description
show rmon	Show the information of all RMON groups
show rmon alarms	Show alarm information, including alarm number, name, threshold, sampling interval and value;
show rmon events	Show event information, including event number, name, description, log/trip, etc.
show rmon history	Show the interface information of all the open history group statistics function
show rmon statistics	Show the port information of all the open statistics function

Use the command **clear rmon** to set the function of all RMON groups for default state, which is starting state of the switch.

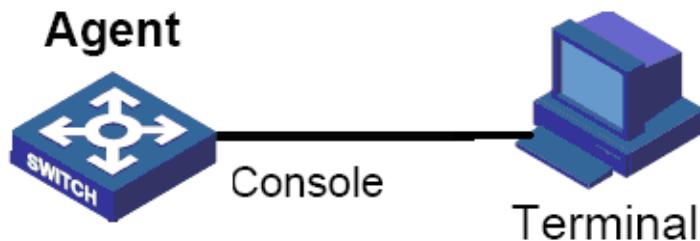
Step	Command	Description
1	config	Enter global configuration mode
2	clear rmon	Return to default state
3	exit	Exit global configuration mode and enter privileged EXEC mode

16.4 Typical configuration example

1.Network demand

Agent connects the configuration terminal by console port and connects remote NMS by Internet. Set a table entry in RMON Ethernet statistics table to make performance statistics for Ethernet port; when the number of bytes exceeds the threshold, record the log.

2.Network picture



3.Configuration Steps

Firstly, create an event with index number 1 to send log, the description character string is High-ifOutErrors, the owner is system. Secondly, set an alarm to monitor MIB variable 1.3.6.1.2.1.2.2.1.20.1, once every 20 seconds, check the rising and falling of variable, if it rises 15s, alarm will be triggered, the owner name is equal to event group.

```
Raisecom#config
Raisecom(config)#rmon event 1 log description High-ifOutErrors owner system
Raisecom(config)#rmon alarm 10 1.3.6.1.2.1.2.2.1.20.1 interval 20 delta rising-threshold 15 1
          falling-threshold 0 owner system
Raisecom(config)#exit
Raisecom#show rmon alarm
Alarm 10 is active, owned by system
Monitors 1.3.6.1.2.1.2.2.1.20.1 every 20 seconds
Taking delta samples, last value was 0
Rising threshold is 15, assigned to event 1
Falling threshold is 0, assigned to event 0
On startup enable rising and falling alarm
Raisecom#show rmon event
Event 1 is active, owned by system
Event generated at 0:0:0
Send TRAP when event is fired.
```

Chapter 17 ARP Management Configuration

This chapter focuses on introducing how to configure and maintain ARP on the switch, including the following contents:

- ❖ ARP overview
- ❖ ARP configuration
- ❖ Monitoring and maintenance
- ❖ Typical configuration example

17.1 ARP principle overview

In the process of IP packet forwarding, switch software system needs to find its physical address according to the target host's IP address so as to transmit the information to the target host. The mapping relationship of IP address and MAC address will be stored in the ARP address mapping table.

ARP mapping table contains 2 types of table entries:

- Dynamic table entry: MAC address learnt by ARP protocol. It will age without use.
- Static table entry: Table entry set by configuration staff manually. Never age.

ARP (Address Resolution Protocol) is mainly used to make the resolution from IP address to Ethernet MAC address.

ARP module is indispensable for the information forwarding of host network layer in LAN.

When the host A sends message to host B, host A can use the IP address of host B to search the corresponding physical address in its own mapping table. If found the physical address of host B, send IP message; If not found physical address, send ARP request to host B and add IP address and MAC address mapping of host B to mapping table.

In many cases, when host A sends data message to host B, host B will probably send data message to host A soon, so host B may also send ARP request packet to host A. In order to reduce the communication traffic on the network, when host A sends its ARP request packet, write its own IP addresses and physical address mapping in ARP request packet. When host B receives the ARP request packet from host A, host B will write the address mapping of host A to its own mapping table. Then it will be more convenient for host B to send data message to host A.

In special circumstances, the configuration staff can also operate ARP address mapping table through the static MAC address configuration command.

17.2 ARP configuration

The part is about how to configure and maintain ARP on the switch, including the following configuration information:

- ARP default configuration
- Add static ARP address table entry

- Delete ARP address mapping table entry
- Set the timeout of ARP dynamic address mapping table entry
- Set ARP dynamic learning mode
- Empty ARP address mapping table

17.2.1 ARP default configuration

Function	Default value
static ARP address table entry	N/A
Timeout of ARP dynamic address mapping table entry	1200s
ARP dynamic learning mode	learn-reply-only

17.2.2 Add static ARP address table entry

Generally, ARP mapping table is maintained by dynamic ARP protocol, ARP will search the resolution from IP address to Ethernet MAC address automatically according to the protocol without the operation of administrator. Use ARP manual configuration command to operate ARP mapping table just when it needs to add static ARP table entry.

Static ARP address table entry has the following characteristics:

- Static ARP address table entry must be added and deleted manually.
- Static ARP address never ages.

The configuration step is as below:

Step	Command	Description
1	config	Enter global configuration mode
2	arp ip-address mac-address	Add a static table entry to ARP address mapping table
3	exit	Exit global configuration mode and enter privileged EXEC mode
4	show arp	Show all table entries in ARP address mapping table

Note: The IP address of static ARP table entry must belong to the IP network segment of layer-3 switch interface.

Use global configuration command **no arp ip-address** to delete static ARP table entry.

17.2.3 Set the timeout of ARP dynamic address mapping table entry

User can set ARP dynamic table entry time. Passed the time, ARP dynamic table entry will be deleted.

The configuration step is as below:

Step	Command	Description
1	config	Enter global configuration mode
2	arp aging-time sec	Set ARP dynamic table entry time. Passed the time, ARP dynamic table entry will be deleted.
3	exit	Exit global configuration mode and enter privileged EXEC mode
4	show arp	Show all table entries in ARP address mapping table

Note: If the timeout is 0, ARP dynamic table entry will not age.

Use global configuration command **no arp aging-time** to restore the default configuration of ARP dynamic address mapping table entry timeout.

17.2.4 Set ARP dynamic learning mode

The above part said that in order to reduce the communication traffic on the network, when host A sends its ARP request packet, write its own IP addresses and physical address mapping in ARP request packet. When host B receives the ARP request packet from host A, host B will write the address mapping of host A to its own mapping table. Then it will be more convenient for host B to send data message to host A. This process can be realized by setting ARP dynamic learning mode to **learn-all**.

The purpose to set ARP dynamic learning mode is to prevent ARP attack in some cases. When set to **learn-all** mode, the ARP request message and response message both should be learnt; when set to **learn-reply-only** mode, only learn the ARP of response message after active request; for request message, only respond to ARP response message, but not make ARP learning.

Step	Command	Description
1	config	Enter global configuration mode
2	arp mode {learn-all / learn-reply-only}	Set ARP dynamic learning mode
3	exit	Exit global configuration mode and enter privileged EXEC mode
4	show arp	Show all table entries in ARP address mapping table

17.2.5 Empty ARP address mapping table

In some cases, the network administrator may need to use **clear arp** command to empty all the ARP table entries.

The configuration step is as below:

Step	Command	Description
1	config	Enter global configuration mode

2	clear arp	Empty all table entries in ARP address mapping table
3	exit	Exit global configuration mode and enter privileged EXEC mode
4	show arp	Show all table entries in ARP address mapping table

17.3 Monitoring and maintenance

Use the command to look over the commands of all the table entry in ARP address mapping table, including IP address, MAC address and the type of each table entry.

Command	Description
show arp	Show all table entries in ARP address mapping table
show arp ip ifNum	Show the ARP table entry of a certain IP interface
show arp A.B.C.D	Show the ARP table entry corresponding to IP address
show arp static	Show the static ARP table entry

17.4 Typical configuration example

1.Network demand

- Set the aging time of dynamic ARP table entry for 600s.
- For prevent the ARP attack in some cases, configure the dynamic ARP learning mode as **learn-reply-only**.
- Add a static ARP table entry after configuring IP interface address.

2.Configuration steps

```
Raisecom(config)# arp aging-time 600
Raisecom(config)# arp mode learn-reply-only
Raisecom(config)# arp 10.0.0.1 0050.8d4b.fd1e
```

Chapter 18 SNMP Function Configuration

18.1 SNMP principle overview

18.1.1 SNMP overview

Now, the network management protocol that is the most extensively used in computer network is SNMP (Simple Network Management Protocol), which is also one of the standard protocols for Internet management.

On structure, SNMP is made up of agent and Network Management Station (NMS), or agent/management station mode. Among them, NMS is the workstation that runs the client program, the management workstations that is usually used now are IBM NetView and Sun NetManager; Agent means the server software that is running on the network equipment like the switch, management information base (MIB) is maintained in Agent.

When SNMP Agent receives the request message Get-Request, Get-Next-Request, Get-Bulk-Request that about MIB variable from NMS, Agent will take read/write operation to the MIB variable that NMS requested according to the message type, then create Response message according to the result, and send it to NMS as response.

On the other side, when SNMP Agent receives the message about some equipment's state like cold/warm booting or anomalous event, it will create a Trap message and send it to NMS actively and report these important incidents.

Raisecom serious SNMP Agent supports SNMPv1, SNMPv2c and SNMPv3

18.1.2 SNMP V1/V2 overview

SNMPv1 is a simple request/response protocol. The network management system sends out a request, the manager returns a response. The action is realized by one of the four protocol operations. The four operations are GET, GETNEXT, SET and TRAP. Through GET operation, NMS get one or more object (instance) values. If the agent cannot offer all the request (instance) values from the request list, it will not offer any value. NMS use GETNEXT operation to get the next object instance value from the request list or the object list. NMS use SET operation to send commands to SNMP proxy and request re-configuration to the object value. SNMP proxy use TRAP operation to inform NMS the specific event irregularly.

Different from SNMPv1's simplex centralized management, SNMPv2 supports distributed/layered network management structure, in SNMPv2 management model some systems have both manager and proxy function; as proxy, it can receive the commands from senior management system, interview the local information stored, and offer the information summary of other proxy in the management domain that it charges, then send Trap information to senior manager.

18.1.3 SNMPv3 interview

SNMPv3 uses user-based security model. Whatever it is NMS sending query message to SNMP Agent, or SNMP Agent sending Trap message to NMS, the communication between NMS and SNMP Agent must be in the name of a certain user. Both SNMP NMS and proxy side maintains a local SNMP user table, user table record username, user related engine ID, if identification is needed and the identification key, encryption information, so that it could make correct resolution to the message content and suitable response. SNMP user's configuration is to create key through the password information in the command lines, and add a user in local SNMP user table of the switch.

18.2 SNMPv1/v2/v3 management configuration

18.2.1 Default SNMP configuration

Function	Default value																
trap switch	Enabled																
The mapping relationship between SNMP user and visiting group	<p>The existed ones by default: initialnone, initial group:</p> <table> <thead> <tr> <th>Index</th> <th>GroupName</th> <th>UserName</th> <th>SecModel</th> </tr> </thead> <tbody> <tr> <td>-0</td> <td>initialnone</td> <td>raisecommone</td> <td>usm</td> </tr> <tr> <td>1</td> <td>initial</td> <td>raisecomm5nopriv</td> <td>usm</td> </tr> <tr> <td>2</td> <td>initial</td> <td>raisecomshanopriv</td> <td>usm</td> </tr> </tbody> </table>	Index	GroupName	UserName	SecModel	-0	initialnone	raisecommone	usm	1	initial	raisecomm5nopriv	usm	2	initial	raisecomshanopriv	usm
Index	GroupName	UserName	SecModel														
-0	initialnone	raisecommone	usm														
1	initial	raisecomm5nopriv	usm														
2	initial	raisecomshanopriv	usm														
SNMP interview group	<p>The existed ones by default: initialnone, initial group:</p> <p><i>Index: 0</i></p> <p><i>Group: initial</i></p> <p><i>Security Model: usm</i></p> <p><i>Security Level: authnopriv</i></p> <p><i>Context Prefix: --</i></p> <p><i>Context Match: exact</i></p> <p><i>Read View: internet</i></p> <p><i>Write View: internet</i></p> <p><i>Notify View: internet</i></p> <p><i>Index: 1</i></p> <p><i>Group: initialnone</i></p> <p><i>Security Model: usm</i></p> <p><i>Security Level: noauthnopriv</i></p> <p><i>Context Prefix: --</i></p> <p><i>Context Match: exact</i></p> <p><i>Read View: system</i></p> <p><i>Write View: --</i></p> <p><i>Notify View: interne</i></p>																
SNMP user	The existed ones by default: raisecommone, raisecomm5nopriv, raisecomshanopriv user																

Index: 0
User Name: raisecommone
Security Name: raisecommone
EngineID: 800022b603000e5e00c8d9
Authentication: NoAuth
Privacy: NoPriv

Index: 1
User Name: raisecommnd5nopriv
Security Name: raisecommnd5nopriv
EngineID: 800022b603000e5e00c8d9
Authentication: MD5
Privacy: NoPriv

Index: 2
User Name: raisecomshanopriv
Security Name: raisecomshanopriv
EngineID: 800022b603000e5e00c8d9
Authentication: SHA
Privacy: NoPriv

SNMP group The existed ones by default: public, private group

Index Community Name View Name Permission
1 public internet ro
2 private internet rw

The network administrator's contact information and logo
Contact information: support@Raise.com.com
Device location : world china raise.com

SNMP object host address None

SNMP figure The existed ones by default: system, internet figure

Index: 0
View Name: system
OID Tree: 1.3.6.1.2.1.1
Mask: --
Type: included
Index: 1
View Name: internet
OID Tree: 1.3.6
Mask: --
Type: included

18.2.2 SNMPv1/v2 configuration

To protect itself and keep MIB from invalid visit, SNMP Agent brings in the idea of group. The management station in a group must use the group's name in all the Get/Set operations, or the request will not be taken.

The group name uses different character stream to sign different SNMP groups. Different groups may have read-only or read-write visit right. The group that has read-only right can only query the equipment information, while the group with read-write right can not only query the equipment information but also configure it.

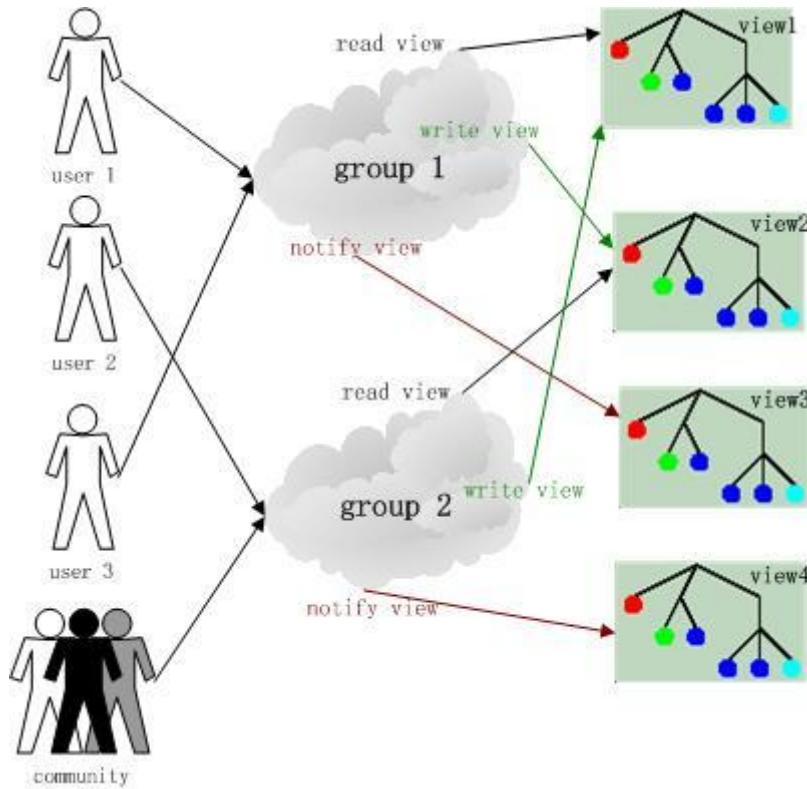
When SNMPv1 and SNMPv2 take group name authentication project, the SNMP message whose group name is not accorded will be dropped. The whole configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
(optional)	snmp-server view <i>view-name oid-tree [mask] {included excluded}</i>	Define the figure and the contained MIB tree range; <i>view-name</i> : figure name, the length cannot exceed 32 character; <i>oid-tree</i> : OID tree, OID number which the depth cannot exceed 128; <i>mask</i> : OID tree mask, the depth cannot exceed 128, format is OID, each option of OID can be only 0 or 1;
2	snmp-server community <i>community-name [view view-name] { ro rw }</i>	Configure the community name, corresponding view and the relevant attributes. <i>community-name</i> : the community name, the type is character string, the length must be less than 20; <i>view-name</i> : the view name, the length must be less than 32; <i>ro</i> : read-only <i>rw</i> : read-and-write
3	exit	Return to privileged EXEC mode
4	show snmp community	Show group information

Note: Both SNOMPV1 and SNOMPV2 takes group name authentication project, the SNMP message that is not accord with the group name that has been identified will be dropped.

18.2.3 SNMPv3 configuration

SNMPv3 takes USM (user-based security model) which is based on user's security safety model. USM brings the principle of interview group: one user or several users accord with an interview group, each interview group set the corresponding write, read, notify view; the user in interview group has the right in the figure. The interview group in which user send requests likeGet and Set must have the corresponding right, or the request will not be taken.



From the figure above, we can see that the normal interview to the switch for NMS, needs not only configuring the user but also making sure which group the user belongs to, the figure right that the interview group has and each figure. Complete configuration (including user's configuration) process is as follow:

Step	Command	Description
1	config	Enter global configuration mode
2	snmp-server view <i>view-name</i> <i>oid-tree</i> [<i>mask</i>] {included excluded}	Define the view and its privilege of the MIB <i>view-name</i> : view name, the length is less than 32 character string; <i>oid-tree</i> : OID tree, the depth is less than 128 OID number; <i>mask</i> : the mask of OID tree, the depth is less than 128, the form is OID, each OID entry only can be 0/1.
3	snmp-server user <i>username</i> [<i>remote engineid</i>] [authentication{md5 sha} <i>authpassword</i>]	Add a SNMP user by command; <i>username</i> : user name <i>engineid</i> : user SNMP engine ID, which must be named in even bytes; <i>authpassword</i> : authentication command.
4	snmp-server access <i>groupname</i> [<i>read readview</i>] [<i>write writeview</i>] [<i>notify notifyview</i>] [<i>context contextname</i> [{<i>exact</i> <i>prefix</i>}]] { v1sm v2csm usm } { noauthnopriv }	Add a SNMP access group <i>Groupname</i> : group name, the length is less than 32 character string; <i>readview</i> : read view name, the length is less than 32 character string; <i>writeview</i> : write view name, the length is less than 32 character string;

		<i>notifyview</i> : notify view name, the length is less than 32 character string;
		<i>contextname</i> : context or its prefix, the length is less than 32 character string;
		<i>noauthnopriv</i> : security level, no authentication and no encryption
		<i>authnopriv</i> : security level, authentication without encryption.
5	snmp-server group <i>groupname</i> user <i>username</i> { v1sm v2csm usm }	Define which group the user belongs to <i>groupname</i> : group name, the length is less than 32 character string; <i>username</i> : user name, the length is less than 32 character string;
6	exit	Exit to privileged configuration mode
7	show snmp group show snmp access show snmp view show snmp user	Show SNMP configuration information

18.2.4 SNMP v1/v2 TRAP configuration

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 0	Enter IP port mode
3	ip address <i>A.B.C.D</i> [<i>A.B.C.D</i>] <i>vlanID</i>	Configure the switch IP address <i>A. B. C. D</i> : IP address [<i>A. B. C. D</i>]: subnet mask <i>vlanID</i> : vlan number
4	exit	Quit global configuration mode and enter privileged EXEC mode
5	snmp-server host <i>A.B.C.D</i> version { 1 2c } NAME [udpport <1-65535>] [bridge] [config] [interface] [rmon] [snmp] [ospf]	Configure SNMPv1/v2 Trap object host <i>A.B.C.D</i> : NMS IP address <i>NAME</i> : SNMPv1/v2c group name <i><1-65535></i> : receiving port number that object host receives Trap, by default it is 162;
6	exit	Return to privileged EXEC mode.
7	show snmp host	Show configuration state.

18.2.5 SNMPv3 Trap configuration

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode.
2	interface ip 0	Enter IP port mode. Configure the switch IP address.
3	ip address A.B.C.D [A.B.C.D] vlanID	<i>A.B.C.D</i> : IP address. <i>[A.B.C.D]</i> : subnet mask. <i>vlanID</i> : vlan number.
4	exit	Quit global configuration mode and enter privileged EXEC mode.
5	snmp-server host A.B.C.D version 3 { noauthnopriv authnopriv } NAME [udpport <1-65535>]	Configure SNMPv3 Trap object host. <i>A.B.C.D</i> : HOST IP address. <i>NAME</i> : SNMPv3 username. <i><1-65535></i> : receiving port number that object host receives Trap, by default it is 162. <i>noauthnopriv</i> : security level, no authentication and no encryption <i>authnopriv</i> : security level, authentication without encryption.
6	exit	Return to privileged EXEC mode.
7	show snmp host	Show configuration state.

18.2.6 Other SNMP configuration

1. Configure the network administrator label and contact access

The network administrator label and contact access sysContact is a variable of system group, its effect is to configure the network administrator label and contact access for management switch.

Step	Command	Description
1	config	Enter global configuration.
2	snmp-server contact sysContact	Configure network administrator label and contact access.
3	exit	Return to privileged EXEC mode.
4	show snmp config	Show configuration situation.

2. Enable/disable system sending trap message

Trap is used mainly for providing some switch important events to NMS. For example, when receiving a request with a fault group name and being allowed to send SNMP Trap, the switch will send a Trap message of failed authentication.

Step	Command	Description
1	config	Enter global configuration mode

2	snmp-server enable traps	Allow the switch to send trap
3	exit	Return to privileged EXEC mode
4	show snmp config	Show the configuration

Use command **no snmp-server enable traps** to stop the switch from sending trap.

3. Configure the switch position

The switch position information sysLocation is a variable of MIB system group, which is used to describe the physical position of the switch.

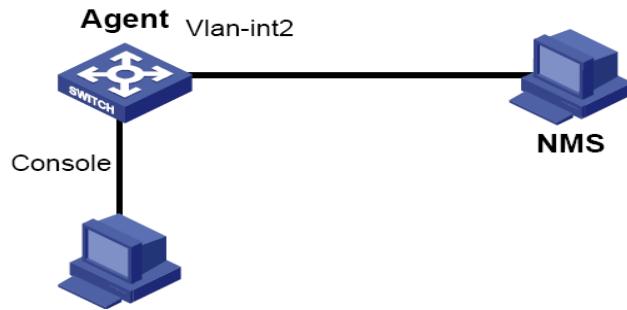
Step	Command	Description
1	config	Enter global configuration mode
2	snmp-server location <i>sysLocation</i>	Configure the switch position <i>sysLocation</i> specify the switch physical position, the type is character stream
3	exit	Return to privileged EXEC mode
4	show snmp config	Show the configuration

18.3 Monitoring and maintenance

Step	Command	Description
1	show snmp community	Show SNMP community information
2	show snmp host	Show IP address of trap target host computer.
3	show snmp config	Show the SNMP engine ID, network administrator contact method, the position of the switch and whether TRAP is enabled.
4	show snmp view	Show view information
5	show snmp access	Show all the names of access group and the attributes of access group.
6	show snmp group	Show all the mapping relationship from user to access group.
7	show snmp trap remote	Show SNMP trap remote state
8	show snmp statistics	Show SNMP statistics information

18.4 Typical configuration example

The interview control configuration example of V3:



First, set the local switch IP address to 20.0.0.10, user *guestuser1*, uses md5 identification algorithm, with the identification password *raisecom*, to interview the figure of MIB2, including all the MIB variable under 1.3.6.1.x.1, create guestgroup interview group, the safe mode safe model is usm, the safe grade is identified but not encrypted, the readable figure name is MIB2, thus the process of *guestuser1* mapping to interview group with the safe grade usm can be accomplished, and the result will be shown:

Raisecom#**config**

Raisecom(config)# **interface ip 0**

Raisecom(config-ip)#**ip address 20.0.0.10 1**

Raisecom(config-ip)#**exit**

Raisecom(config)#**snmp-server view mib2 1.3.6.1.2.1 1.1.1.1.0.1 included**

Set successfully

Raisecom(config)#**snmp-server user guestuser1 authentication md5 raisecom**

Set successfully

Raisecom(config)#**snmp-server access guestgroup read mib2 usm authnopriv**

Set successfully

Raisecom(config)#**snmp-server group guestgroup user guestuser1 usm**

Set successfully

Raisecom(config)#**exit**

Raisecom# **show snmp access**

Index: 0

Group: initial

Security Model: usm

Security Level: authnopriv

Context Prefix: --

Context Match: exact

Read View: internet

Write View: internet

Notify View: internet

Index: 1

Group: guestgroup

Security Model: usm

Security Level: authnopriv

Context Prefix: --
Context Match: exact
Read View: mib2
Write View: --
Notify View: internet

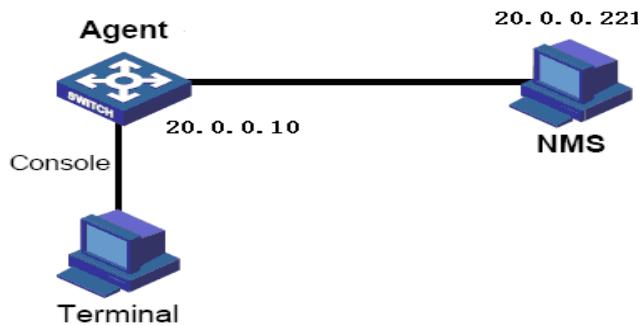
Index: 2
Group: initialnone
Security Model: usm
Security Level: noauthnopriv
Context Prefix: --
Context Match: exact
Read View: system
Write View: --
Notify View: internet

Raisecom# show snmp group

Index	GroupName	UserName	SecModel
0	guestgroup	guestuser1	usm
1	initialnone	raisecommone	usm
2	initial	raisecommd5nopriv	usm
3	initial	raisecomshanopriv	usm

V3 Trap configuration example:

Trap is the information Agent sending to NMS actively, used to report some urgent events. As is shown below, set the switch IP address to 20.0.0.10, NMS host IP address to 20.0.0.221, username to raisecom, SNMP version v3, identified but not encrypted, all Trap



Raisecom#config

```
Raisecom(config)# int ip 0
Raisecom(config-ip)#ip address 20.0.0.10 1
Raisecom(config-ip)#exit
Raisecom(config)#snmp-server host 20.0.0.221 version 3 authnopriv  raisecom
Raisecom#show snmp host
```

Index: 0
IP address: 20.0.0.221
Port: 162
User Name: raisecom
SNMP Version: v3
Security Level: authnopriv
TagList: bridge config interface rmon snmp ospf

Chapter 19 Time Management Function Configuration

19.1 Time management overview

Raisecom provides two kinds of system time setting methods: one is to use SNTP protocol to make switch system time to synchronize with SNTP host time, the SNTP protocol synchronization time is Greenwich mean time, transform to local time according to the system timezone settings; the other one is to set system time manually, which is called local time directly.

Raisecom series switches support three kinds of system clock modes, including the default system clock mode, timestamp mode and auxiliary clock mode. The quantity and type of device models depend on the specific hardware. At the same time, the precision and accuracy of system time provided by each mode are also restricted to device hardware. The administrator can choose the optimal system clock mode manually according to the practical application environment of device.

19.2 Time configuration function

19.2.1 Default time function configuration

Function	Default value
Default time	2000-01-01 08:00:00.000
Default clock mode	System clock
Default timezone offset	+08:00
Default summer time function	Disable

Note: If the equipment is to support the clock chip, then use the clock chip default time.

19.2.2 Time setting function configuration

Step	Command	Description
1 (optional)	clock mode {default timestamp auxiliary}	Set system clock mode, including default, timestamp and auxiliary clock modes.
2	clock set <0-23> <0-59> <0-59> <2000-2099> <1-12> <1-31>	Set system time for hour, minute, and seconds, year, month, day by turns.
3	show clock	Show system time and configuration

19.2.3 Timezone management function configuration

Step	Command	Description
1	clock timezone {+ -} <0-11> <0-59>	Set system timezone: +: the eastern hemisphere zone -: the western hemisphere zone <0-11>: timezone offset hours <0-59>: timezone offset minutes Default for Beijing time, which is 8 o'clock for the eastern hemisphere.
2	clock set <0-23> <0-59> <0-59> <2000-2099> <1-12> <1-31>>	Set system time for hour, minute, and seconds, year, month, day by turns.
3	show clock	Show system time and configuration

19.2.4 Summer time function configuration

When the summer time is enable, SNTP synchronization time will transform to local summer time.

The configuration steps are as below:

Step	Command	Description
1	clock summer-time enable	When summer time function s enable, use this command to close it if some countries don't use summer time.
2	clock summer-time recurring {<1-4>/last} { sun mon tue wed thu fri sat } {<1-12> MONTH } <0-23> <0-59> {<1-4> last} { sun mon tue wed thu fri sat } {<1-12> MONTH } <0-23> <0-59> <1-1440>	Set system time for hour, minute, and seconds, year, month, day by turns. <1-4> last : the start week, last : the last week sun : Sunday mon : Monday tue : Tuesday wed : Wednesday thu : Thursday fri : Friday sat : Saturday <1-12> MONTH : month, MONTH means the month input by himself <0-23>: hour <0-59>: minute <1-4> last : the end week, last : the last week sun : Sunday mon : Monday

tue: Tuesday

wed: Wednesday

thu: Thursday

fri: Friday

sat: Saturday

<1-12> | MONTH: month, MONTH means the month input by himself

<0-23>: hour

<0-59>: minute

3	show clock summer-time recurring	Show system time and configuration
----------	---	------------------------------------

Note:

- Set system time manually, if the system uses summer time, for example, the summer time is from 2:00 am on the second Sunday of April to 2:00 am on the second Sunday of September every year, in this time zone, the clock is set forward an hour, the time will offset 60 minutes, so the time from 2:00 to 3:00 on the second Sunday of April every year is nonexistent. Set time manually in this period will fail.
- The summer in southern hemisphere is opposite to northern hemisphere, which is often from September to the next April, if the start time of configuration is later than the end time, the system will assume that you are in the southern hemisphere, that is to say, the summer time is from the start time of this year to the end time of next year.

19.2.5 Monitoring and maintenance

The command to check time information:

Command	Description
show clock	Show time information

The command to check time information and summer time function state:

Command	Description
show clock summer-time-recurring	Show time information

Note: If the equipment is to support the clock chip, then get the current time from clock chip.

19.2.6 Typical configuration example

Time zone and summer time configuration:

Raisecom#clock timezone -10 30

set successfully!

Raisecom#clock set 11 14 20 2005 3 28

set successfully!

```
Raisecom#show clock summer-time-recurring
  Current system time: Mar-28-2005 11:15:22.68
  Timezone offset: -10:30:00
  Summer time recurring: Disable

Raisecom#clock summer-time enable
  set successfully!

Raisecom#clock summer-time recurring 2 sun 3 2 0 2 sun 9 2 0 60
  set successfully!

Raisecom#show clock summer-time-recurring
  Current system time: Mar-28-2005 12:15:53.556
  Timezone offset: -10:30:00
  Summer time recurring: Enable
  Summer time start: week 02 Sunday Mar 02:00
  Summer time end: week 02 Sunday Sep 02:00
  Summer time Offset: 60 min
```

19.3 SNTP function configuration

19.3.1 SNTP protocol default configuration

Function	Default value
SNMP server address	N/A

19.3.2 SNTP protocol function configuration

After configuring SNTP server address, the device will try to obtain clock information from SNTP server every 10 seconds, and the maximum timeout is 10 seconds, too.

Step	Command	Description
1	config	Enter global configuration mode
2	sntp server A.B.C.D	Configure SNTP server address
3	exit	Return to privileged EXEC mode
4	show sntp	Show configuration information

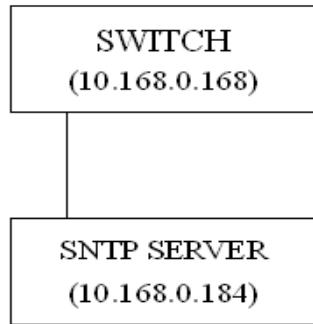
19.3.3 Monitoring and maintenance

The command to look over time management operation situation and configuration information of switch:

Command	Description
show clock	Show configuration information

19.3.4 Typical configuration example

For example: topology structure:



- Purpose:

The switch synchronizes system time from SNTP server.

- Configuration steps:

1. Show the current default system clock.

Raisecom(config)#**show clock**

```

Current system time: Jan-01-2000 08:00:37.672
Timezone offset: +08:00:00
  
```

2. Set SNTP server address

Raisecom(config)#**ntp server 10.168.0.184**

```

Set successfully!
JUN-15-2008 20:23:55 CONFIG-6-Get SNTP time , Date is Jun-15-2008 Time is 20:23:55
  
```

Raisecom(config)#**exit**

3. Show SNTP configuration state

Raisecom#**show ntp**

<i>SNTP Server</i>	<i>Stratum</i>	<i>Version</i>	<i>Synchronize Time</i>
10.168.0.184	15	1	2008-6-15 20:23:55

4. Show the current system clock

Raisecom#**show clock**

```

Current system time: Jun-15-2008 20:24:33.242
Timezone offset: +08:00:00
  
```

19.4 NTP configuration

19.4.1 NTP principle overview

As the development and extension of internet in all aspects of society, various of time application activities on the network, such as online real-time transaction, distributive network computing and

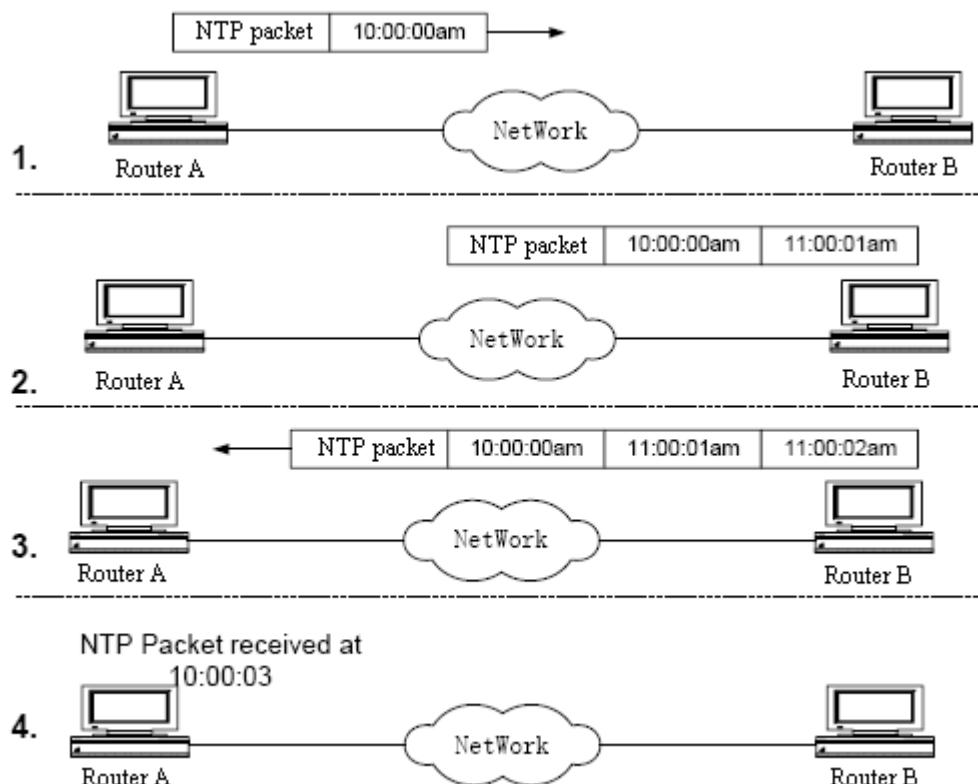
processing, transportation flight route management, database management, need precise and reliable time.

Network time protocol (NTP) refers to the standard internet protocol to synchronize time. The purpose of NTP is to synchronize the computer time to certain time standards. NTP takes a full consideration of the complexity of time synchronization in internet. It provides strict, practical and effective mechanism to adapt the internet environment with all kinds of scale, speed and connection route situation.

With the time information delivered by GPS time code as reference standard, UTC (Coordinated Universal Time) as time standard, Client/Server structure, UDP/IP base, and hierarchical time distribution model, the NTP has quite high flexibility so that it can adapt to all kinds of internet environment. Not only correcting the current time, NTP can track the change of time continuously and adjust automatically so as to maintain the stability of time even if the network is out of order. NTP has the advantage to guarantee network security with very little network fee.

The network time protocol (NTP) explains the detailed features of local clock and time server and the method to estimate the error between local clock and time server as well as introduces the clock filter and clock selection algorithm in the process of implementing the protocol. When there are many time servers in the network, it can improve the accuracy of local clock through synthesizing time offset of time server by the selection algorithm. Also, when a host receives many time samples delivered from time server, it can adjust local clock through the clock filtering algorithm to select sample with the minimum error and best performance.

The basic working principle of NTP is as below:



NTP basic working principle figure

The above shows the basic working principle of NTP. Router A and router B are connected by network; they have their own stand alone system clock, to realize the automatic synchronization, it needs to make the following assumption for clock synchronization process at first:

- Before the synchronization of router A and router B system clocks, set the clock of router A for 10:00:00am and router B for 11:00:00am.
- Take router B as NTP time server, router A will make its own clock synchronize router B.
- It takes 1 second for data packet to make unidirectional transmission between router A and router B.

The process of system clock synchronization is as below:

- Router A sends a NTP message packet to router B, it will seal the timestamp of 10:00:00am (t1).
- When the NTP message arrives at router B, router B will seal its own timestamp of 11:00:01 am (t2).
- When the message packet leaves router B, router B will seal its own timestamp again, the timestamp is 11:00:02 am (t3).
- When router A receives the response message packet, it will seal a new timestamp of 10:00:03 am (t4).

So far, router A has already had enough information to calculate the two important parameters:

The time delay for NTP message to cycle is: Delay = (t4 t1) - (t3-t2).

The time offset between routers A and router B is: offset= t2-t1+t3-t4/2.

In this way, router A can set its own clock according to the message in order to synchronize router B.

19.4.2 NTP configuration

19.4.2.1 Default NTP configuration

Function	Default value
Global NTP server	N/A
Global NTP peer	N/A
Reference clock source	0.0.0.0
NTP state	ntpSlave
Version number	v3

19.4.2.2 NTP configuration guide

When the device is configured for reference clock source, the device will transform to synchronization automatically; it is unable to configure NTP server or peer or synchronized by other devices.

When the device is configured for NTP server or peer but not for reference clock source, the device can be synchronized by other devices and synchronize other devices.

19.4.2.3 NTP server configuration

By default, the device isn't configured transceiver NTP server IP address. If execute NTP server configuration command without version number, then the default version number is 3.

The configuration step is as below:

Step	Command	Description
1	config	Enter global configuration mode
2	ntp server 20.0.0.110	Set NTP server
3	exit	Return to privileged EXEC mode
4	show ntp associations	Show NTP connection information

Note: If the device is configured reference clock source, it will fail to configure NTP server; on the contrary, if the device is configured NTP server or peer, it will fail to configure NTP reference clock source.

Use the command **no ntp server ip-address** to delete NTP server.

19.4.2.4 NTP peer configuration

By default, the device isn't configured peer IP address. If execute NTP server configuration command without version number, then the default version number is 3.

Step	Command	Description
1	config	Enter global configuration mode
2	ntp peer 20.0.0.110	Set NTP peer
3	exit	Return to privileged EXEC mode
4	show ntp associations	Show NTP connection information

19.4.2.5 Reference clock source configuration

Default device isn't NTP reference clock source, if configuring this command, then the default reference clock will be 127.127.1.0, the default level is 8.

Step	Command	Description
1	config	Enter global configuration mode
2	ntp reclock-master	Configure the device for NTP reference clock source
3	exit	Return to global configuration mode
4	show ntp status	Show NTP status information

Note: If the device is configured reference clock source, it will not synchronize by other devices; when the device is configured NTP server or peer, it will fail to configure NTP reference clock source.

Use the command **no ntp refclock** to cancel NTP reference clock source.

19.4.3 Monitoring and maintenance

Use the command **show ntp status** to look over NTP status information and use the command **show ntp associations** to look over NTP connection information.

Command	Description
show ntp status	Show NTP status information
show ntp associations	Show NTP connection information

Use the command **show ntp status** to show NTP status information, including clock status, the selected NTP peer, version number, device mode, leap instruction, polling time, clock precision, system level, reference clock source, the recently updated local time, the current time, root delay, root dispersion. It is shown as below:

Raisecom#**show ntp status**

```
Clock status : synchronized
NTP peer : 20.6.6.9
NTP version : 3
NTP mode : ntpSlave
Leap : 0
Poll : 8
Stratum : 5
Precision : 2**4
Reference clock : 20.6.6.9
Reference time : cd6c8915.0c0d3480(Thu Mar 19 09:04:21.047 UTC 2009)
Current clock : cd6d6ee4.0c0d3480(Fri Mar 20 01:24:52.047 UTC 2009)
Root delay : -1.000009
Root dispersion : 0.001380
```

Use the command **show ntp associations** to show NTP connection information, including peer type, synchronous status, peer level, peer polling time, delay, dispersion, mode, the time from last update to command execution, and the response packet. It is shown as below:

Raisecom#**show ntp associations detail**

Server(ip)	refid	stratum	poll	when	delay	offset	dispersion	mode	reach
(s)20.6.6.9	27.127.1.0	4	9	58927	-1.065525	0.005769	0.000000	1	255
Peer(ip)	refid	stratum	poll	when	delay	offset	dispersion	mode	reach
(u)20.6.6.8	0.0.0.0	16	10	58522	0.000000	0.000000	16.000000	0	0

Show the detailed connection information:

Server(ip)	refid	stratum	poll	when	delay	offset	dispersion	mode	reach			
(s)20.6.6.9	127.127.1.0	4	9	59216	-1.065525	0.005769	0.000000	1	255			
					filtoffset = 0.000741	0.001415	0.002088	0.002758	0.003422	0.003780	0.004427	0.005769

```

filtdelay =-1.065526 -1.065525 -1.065525 -1.065526 -1.065525 -1.065525 -1.065525 -1.065525
filtdispersion =16.000000 16.000000 16.000000 16.000000 16.000000 16.000000 16.000000 0.000000
Peer(ip) refid stratum poll when delay offset dispersion mode reach
(u)20.6.6.8 0.0.0.0 16 10 58811 0.000000 0.000000 16.000000 0 0
filtoffset =0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000
filtdelay =0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000
filtdispersion=16.000000 16.000000 16.000000 16.000000 16.000000 16.000000 16.000000 16.000000

```

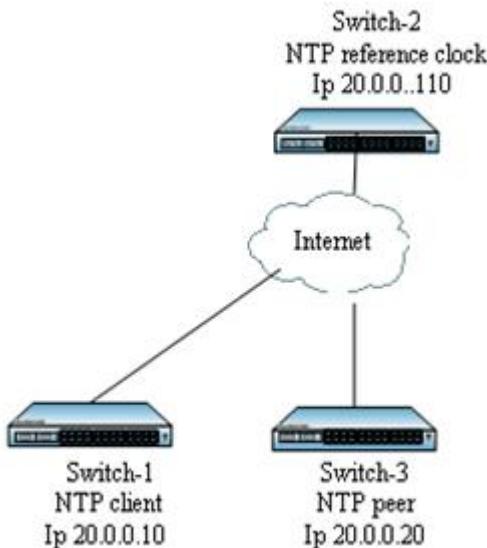
19.4.4 Typical configuration example

This part takes an example to introduce one NTP client connects a NTP server to obtain time, by which to show the NTP typical configuration.

1.Configuration instruction

Switch-2 is the reference clock source, switch-1 works in NTP client mode, switch-3 works in NTP active peer mode; switch-1 acquires time from switch-2; after switch-1 is synchronized, switch-3 acquires time from switch-1.

2.Topology figure



NTP acquisition time topology figure

3.Configuration steps

[switch-2]

```
Raisecom(config)#ntp refclock 127.127.1.0 2
```

```
Raisecom(config)#interface ip 0
```

```
Raisecom(config-ip)#ip address 20.0.0.110 255.0.0.0 1
```

```
Raisecom(config-ip)#exit
```

```
Raisecom(config)#exit
```

Raisecom#**show ntp status**

[switch-1]

Raisecom(config)#**interface ip 0**

Raisecom(config-ip)#**ip address 20.0.0.10 255.0.0.0 1**

Raisecom(config-ip)#**exit**

Raisecom(config)#**ntp server 20.0.0.110 version v3**

Raisecom#**show ntp associations**

Raisecom#**show ntp status**

[switch-3]

Raisecom(config)#**interface ip 0**

Raisecom(config-ip)#**ip address 20.0.0.20 255.0.0.0 1**

Raisecom(config-ip)#**exit**

Raisecom(config)#**ntp peer 20.0.0.10 version v3**

Raisecom#**show ntp associations**

Raisecom#**show ntp status**

4. Show the result

[switch-1]

Raisecom#**show ntp associations**

<i>Server(ip)</i>	<i>refid</i>	<i>stratum</i>	<i>poll</i>	<i>when</i>	<i>delay</i>	<i>offset</i>	<i>dispersion</i>	<i>mode</i>	<i>reach</i>
(s)20.0.0.110	127.127.1.0	2	9	59216	-1.065525	0.005769	0.000000	1	255

Raisecom#**show ntp status**

Clock status : synchronized

NTP peer : 20.0.0.110

NTP version : 3

NTP mode : ntpSlave

Leap : 0

Poll : 8

Stratum : 5

Precision : 2***4

Reference clock : 20.0.0.110

Reference time : cd6c8915.0c0d3480(Thu Mar 19 09:04:21.047 UTC 2009)

Current clock : cd6d6ee4.0c0d3480(Fri Mar 20 01:24:52.047 UTC 2009)

Root delay : -1.000009

Root dispersion : 0.001380

[switch-3]

Raisecom#show ntp associations

<i>Server(ip)</i>	<i>refid</i>	<i>stratum</i>	<i>poll</i>	<i>when</i>	<i>delay</i>	<i>offset</i>	<i>dispersion</i>	<i>mode</i>	<i>reach</i>
(s)20.0.0.10	20.0.0.110	3	8	59216	-1.065525	0.005769	0.000000	1	255

Raisecom#show ntp status

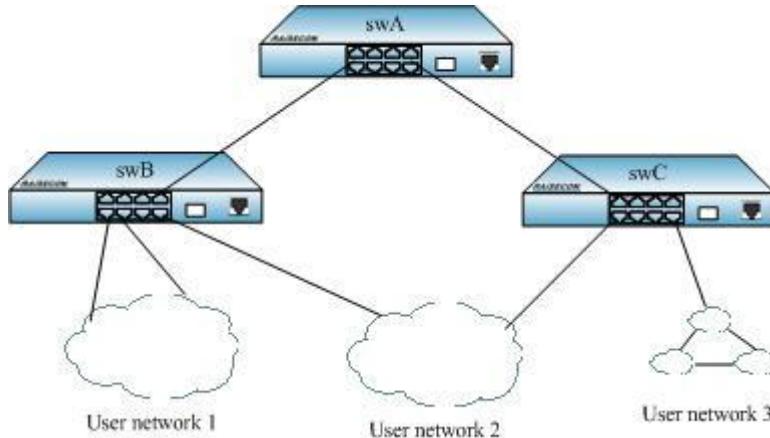
Clock status : synchronized
NTP peer : 20.0.0.10
NTP version : 3
NTP mode : ntpSlave
Leap : 0
Poll : 8
Stratum : 4
Precision : 2***4
Reference clock : 20.0.0.10
Reference time : cd6c8915.0c0d3480(Thu Mar 19 09:04:21.047 UTC 2009)
Current clock : cd6d6ee4.0c0d3480(Fri Mar 20 01:24:52.047 UTC 2009)
Root delay : -1.00089
Root dispersion : 0.011380

19.4.5 NTP trouble shooting

When NTP client cannot acquire time normally, the opposite port hasn't opened NTP server or the network is out of order.

Chapter 20 Loopback Detection Configuration Guide

20.1 Loopback detection introduction



Loopback detection is mainly used in edge port, as shown in Figure 1, swB and swC mouth. Open the loop detection function port and periodically send the loop detection message. As these ports are the edge port, so the switch under normal circumstances should not receive any message loop detection, if it receives, it means that there are Errors in configuration or loops. If a device receives its own message loop detection, it indicates that the ring appeared. In order to prevent the same time blocking several ports, the received message loop detection port will be blocked only in the case that the receiving package is not less than the sending port. If other devices received the message loop detection is considered an error configuration.

20.2 Loopback detection default configuration

Loopback detection function is disable.

20.3 Loopback detection function configuration

20.3.1 Open or close port loopback detection function

This configuration is used to open or close port loopback detection function.

Step	Command	Description
1	config	Enter global configuration mode
2	loopback-detection {enable disable} port-list portlist	Open/close port loopback detection function <i>portlist</i> : refers to port list
3	show loopback-detection port-list portlist	Show loopback detection status

20.3.2 Configure destination MAC address and VLAN Function

This configuration is used to configure loop detection of destination MAC address. It suggests that configuration within the topology is consistence, or may lead to fail to detect.

Step	Command	Description
1	config	Enter global configuration mode
2	[no] loopback-detection destination-address <i>HHHH.HHHH.HHHH</i>	Configure loopback detection message destinations MAC address. <i>HHHH.HHHH.HHHH</i> : configuration destination MAC address.
3	show loopback-detection port-list <i>portlist</i>	Show loopback detection status

This configuration is used to configure loop detection VLAN, as for specific topology and configuration, the different vlan will show different loop status. By configuring the value of this vlan, vlan can check whether there is a loop. It suggests that the configuration within topology is consistent, or may lead to fail to detect.

Step	Command	Description
1	config	Enter global configuration mode
2	[no] loopback-detection vlan <i>vlanid</i>	Configure loopback detection vlan. <i>vlanid</i> : requisite vlan
3	show loopback-detection port-list <i>portlist</i>	Show loopback detection status

20.3.3 Configure cycle loopback detection function

Circle detection is to detect the presence of loops by sending hello packets periodically; the cycle of sending periodic hello packets is loop detection cycle. It is not conducive to detect loop on time if cycle is too large, while it will make the hello packets increase in a certain period of time and increase the burden of network and equipment if cycle is too small. It suggests that the configuration in the topology is consistent, because the other parameters, such as blocking test time, need to refer to this cycle, if the cycle configuration is inconsistency that may lead to coordination errors between devices, the module does not work.

Step	Command	Description
1	config	Enter global configuration mode
2	loopback-detectionhello -time <i>hellotime</i>	Configure loopback detection cycle <i>hellotime</i> : the cycle value unit is second.
3	show loopback-detection port-list <i>portlist</i>	Show loopback detection status

20.3.4 Configure loop detection automatically release the blocked port time

The port after loop is blocked can be detected automatically after a certain period of time, if the loop has been eliminated then open the port, the time depends on the configuration and the actual situation.

This configuration is a real time base configuration, not the actual block time. When the port is blocked, after the configured time, the loop will be detected, if the loop is lifted, then release the port; if the loop is still there, then the next probe need to go through twice the time base, if there, Then three times the relationship was gradually increased, but the maximum of 65535s. It can also be configured to automatically restore said they did not infinite, and is configured to trap-only trap that only sent without closing the port.

Step	Command	Description
1	config	Enter global configuration mode
2	loopback-detection down-time { <i>infinite / trap-only / downtime</i> }	Configure loop detection automatically recover time Downtime is the base. The unit is second.
3	show loopback-detection port-listportlist	Show loopback detection status

20.3.5 Configure other receiving device loop detection the message approach

When an opened loop detection port received loop detection packet and MAC address the packet carrying is inconsistent with this device, the default approach is to send a trap. If the MAC address is smaller than the MAC address of the device, the port will make a suspension to send the loop detection packet 10 hellotime times. In addition, in the case of the presence of the loop, a packet may be flooded, leading repeatedly to receive the same packet, in order to prevent excessive trap against increasing the burden of network and network management, if within 20 hellotime Receive the same message will not send trap. When receiving other devices loop detection packet, it can also choose the method that deals with blocking. In order to avoid blocking multiple devices at the same time, only the receiving packets carried the MAC address is smaller than the device itself will be blocked.

Step	Command	Description
1	config	Enter global configuration mode
2	loopback-detection error-device { <i>discarding / trap-only</i> } port-list portlist	Configure loopback detection receiving other device approach <i>discarding</i> : sending trap and blocking <i>trap-only</i> : only sending <i>portlist</i> : the port list
3	show loopback-detection port-listportlist	Show loopback detection status

20.3.6 Manually open the port blocked

After the port is blocked by loop detection, it can be allowed to automatically recover; besides, you can also manually open ports. Before opening the port will conduct loop detection, if the loop is there, it will continue to obstruct.

Step	Command	Description
1	config	Enter global configuration mode

2	interface port port_num	Enter port configuration mode <i>port_num</i> : port number It can use interface range portlist Into the batch configuration mode to configure multiple ports <i>portlist</i> : port list
3	no loopback-detection discarding	Release loop detection blocked port
4	show loopback-detection port-list portlist	Show loopback detection status

20.3.7 Clear loop detection statistics

Statistical information is recorded in units of the port, including the number of sent packets loop detection, the number of received packets loop detection, the number of blocked, error device records information. Clear statistics will make counting become zero.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port port_num	Enter port configuration mode <i>port_num</i> : port list It can use interface range portlist Into the batch configuration mode to configure multiple ports <i>portlist</i> : port list
3	clear loopback-detection statistic	Clear loopback detection statistics information Portlist port list
4	show loopback-detection statistic port-list portlist	Show loopback detection statistics information

20.4 Monitoring and maintenance

Command	Description
show loopback-detection port-list portlist	Show loopback detection statistics information <i>portlist</i> : port list
show loopback-detection statistic port-list portlist	Show loopback detection statistics information <i>portlist</i> : port list

20.5 Typical configuration examples

Example 1: enable port 1-5 loopback detection.

Raisecom#**config**

Raisecom(config)#**loopback-detection enable port-list 1-5**

Raisecom(config)#**show loopback-detection port-list 1-9**

Destination address: FFFF.FFFF.FFFF

VLAN:1

Period of loopback-detection:4s

Restore time:infinite

<i>Port</i>	<i>State</i>	<i>Status</i>	<i>exloop-act</i>	<i>Last</i>	<i>Last-Occur</i>	<i>Open-Time</i>	<i>vlan</i>
					<i>Loop-with</i>	<i>(ago)</i>	<i>(ago)</i>

1	Ena	no	trap-only	--	--	--	--
2	Ena	no	trap-only	--	--	--	--
3	Ena	no	trap-only	--	--	--	--
4	Ena	no	trap-only	--	--	--	--
5	Ena	no	trap-only	--	--	--	--
6	Dis	no	trap-only	--	--	--	--
7	Dis	no	trap-only	--	--	--	--
8	Dis	no	trap-only	--	--	--	--
9	Dis	no	trap-only	--	--	--	--

Example 2: Configure destination MAC address as 0012.3456.7890, VLAN as 3, Cycle as 10s, automatically open port time is 60s, port 6-9 receive the other device approach is discarding.

Raisecom(config)#**loopback-detection destination-address 0012.3456.7890**

Raisecom(config)#**loopback-detection vlan 3**

Raisecom(config)#**loopback-detection hello-time 10**

Raisecom(config)#**loopback-detection down-time 60**

Raisecom(config)#**loopback-detection error-device discarding port-list 6-9**

Raisecom(config)#**show loopback-detection port-list 1-9**

Destination address: 0012.3456.7890

VLAN:3

Period of loopback-detection:10s

Restore time:60s

<i>Port</i>	<i>State</i>	<i>Status</i>	<i>exloop-act</i>	<i>Last</i>	<i>Last-Occur</i>	<i>Open-Time</i>	<i>vlan</i>	<i>Loop-with</i>	<i>(ago)</i>	<i>(ago)</i>
-------------	--------------	---------------	-------------------	-------------	-------------------	------------------	-------------	------------------	--------------	--------------

1	Ena	no	trap-only	--	--	--	--	--	--
2	Ena	no	trap-only	--	--	--	--	--	--
3	Ena	no	trap-only	--	--	--	--	--	--
4	Ena	no	trap-only	--	--	--	--	--	--
5	Ena	no	trap-only	--	--	--	--	--	--
6	Dis	no	discarding	--	--	--	--	--	--
7	Dis	no	discarding	--	--	--	--	--	--

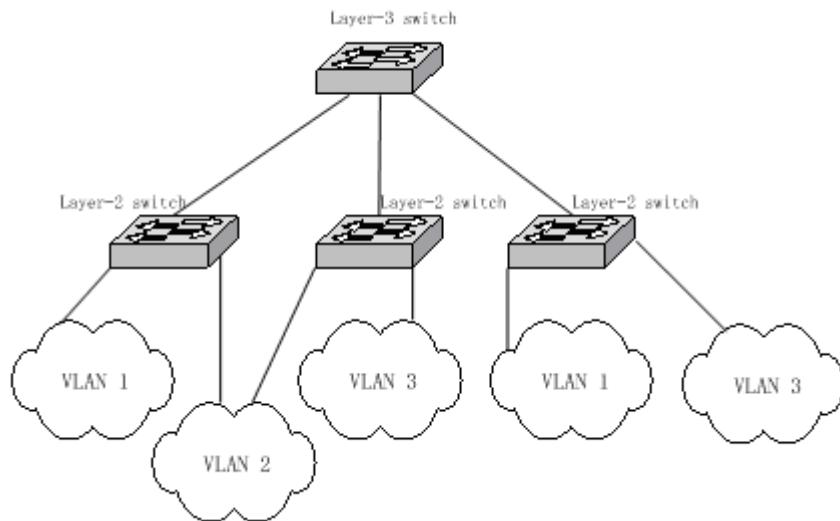
8	<i>Dis</i>	<i>no</i>	<i>discarding</i>	--	--	--	--
9	<i>Dis</i>	<i>no</i>	<i>discarding</i>	--	--	--	--

Chapter 21 VLAN Configuration

21.1 VLAN Principle overview

IEEE802.1Q VLAN

VLAN stands for virtual LAN (virtual Local Area Networks). In terms of functions, VLAN has the same characteristics with LAN. However, VLAN members are not restricted by physical locations. For instance, the users connected to the same switch can belong to different VLANs. The broadcast domain and multicast domain are both in reference to VLAN member, multicast, broadcast and unicast will not flood to other VLANs. Different VLANs can communicate with each other only via Layer-3 switch or router. The features above offer much convenience for network management; user can allocate VLANs based on functions in the network so as to promote the network bandwidth utility and security. A typical VLAN network topology is shown below:



VLAN, a protocol to handle the Ethernet problems from broadcasting and safety, is added VLAN port based on Ethernet frame, divides users into smaller working group using VLAN ID and limits the two-layer visit between users within different working groups. Each working group is a virtual LAN.

In 1999 IEEE issues the 802.1Q protocol standard draft for VLAN realization project. As the criterion of VLAN, it encapsulates VLAN ID in the frame header, so that the VLAN information can be kept when a frame is crossing different equipments. The switches of different producers can be under unified management and cross switches if only they support 802.1Q VLAN.

21.2 Switch VLAN Function Configuration

Note: ISCOM2128EA-MA isn't in support of priority.

21.2.1 VLAN based on port

VLAN division based on port is the most simple and effective way for VLAN division. It defines VLAN member according to the equipment port, and when the given port enters the given VLAN, it can transmit messages from the given VLAN.

21.2.1.1 VLAN port mode interview

Port mode	VLAN member attributes
Access	Under this mode, the port can be allocated to a single VLAN, packet sent from Access port does not have no 802.1Q tag, Access ports within different VLANs cannot communicate with each other.
Trunk	Trunk port can be allocated with different VLANs by default, packet forwarded from it carries 802.1Q tag expect for Native VLAN. However, you can limit the packets through which VLAN they are forwarded by using <i>allowed vlans</i>

21.2.1.2 Default VLAN configuration

Function	Default value
Create stable VLAN	There are default VLAN and cluster VLAN in the system, that is VLAN 1 and VLAN 2, all the ports exists in VLAN 1 in access mode
VLAN name	The default system VLAN (VLAN 1) is ‘Default’, cluster VLAN name is ‘Cluster-Vlan’, other stable VLAN name is ‘VLAN’ adding VLAN ID(four figures number)
Configure the activity state of stable VLAN	The new created stable VLAN activity state is suspended.
Configure the port mode	Access
Configure the VLAN number that is allowed to pass in TRUNK mode	VLAN1
Configure Native VLAN for Trunk port	VLAN1
VLAN filtration attribute	Enable
Port protection	The port is not protected port
Transmission port list	All the other ports except its own port
VLAN priority	No priority

21.2.1.3 Configure VLAN Attribute

VLAN attribute configuration includes the VLAN configuration of creation, deletion, name, and activity state. The configuration steps are as follows:

Step	Command	Command parameter explain
1	config	Enter global configuration mode
2	create vlan {2-4094} (active suspend)	Create VLAN and make sure the state: active/suspend

		0-7: VLAN priority {2-4094}: VLAN ID
3	vlan <1-4094>	Create VLAN and enter the configuration mode <1-4094>: VLAN ID
4	name WORD	Dominate VLAN WORD: VLAN name, no longer than 15 characters
5	state {active suspend}	Configure VLAN state: active/suspend
6	exit	Return to global configuration mode
7	exit	Return to privileged EXEC mode
8	show vlan	Show VLAN configuration

Use **no vlan <2-4094>** to delete VLAN.

Use **no name** to delete VLAN name and recover to default name.

Note:

- The new created VLAN using VLAN <1-4094> is in suspend state, if user wishes to activate it in the system, the command state that would be introduced later is needed to activate VLAN.
- By default there are VLAN existed in the system, that is default VLAN (VLAN 1) and cluster VLAN (VLAN 2), all the ports are Access mode belongs to the default VLAN. VLAN priority range is 0-7.
- The new created VLAN, has no priority by default, is shown as N/A. VLAN priority range is 0-7.
- By default, default VLAN (VLAN 1) name is ‘Default’, cluster VLAN (VLAN 2) name is ‘Cluster-VLAN’, other VLAN name is character stream ‘VLAN’ added four figures VLAN ID. For example, the default VLAN 1 name is ‘VLAN0001’, the default VLAN 4094 name is ‘VLAN4094’.
- All the VLAN configuration cannot take effect until the VLAN is activated. When VLAN activity state is suspend, user can still configure the VLAN, like delete/add port, configure VLAN name and so on, the system will keep the configuration, once the VLAN is activated, the configuration will take effect in the system.

21.2.1.4 Configure port VLAN mode

Each mode and the configuration are shown below:

1. Configure port VLAN mode

Port VLAN mode configuration must be done in physical interface configuration mode, the steps are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port portid	Enter the corresponding physical port configuration mode <i>portid</i> : port number
3	switchport mode {access / trunk }	Configure port VLAN mode access : ACCESS mode, that is port exists in the unique VLAN in the form of UNTAG;

trunk: TRUNK mode, port exists in several VLAN in TAG mode, and exists in Native Vlan in UNTAG mode.

4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface port [port-list] switchport	Show port VLAN attribute configuration

Use **no switchport mode** to restore port VLAN mode to default value, which is port VLAN mode is Access mode.

2. Configure Access VLAN for port, the steps are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter physical port configuration mode
3	switchport access vlan <1-4094>	Configure VLAN that is allowed to pass Access port
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface port [port-list] switchport	Show port VLAN attribute configuration

Use **no switchport access vlan** command to restore Access VLAN to default value, or port Access VLAN is VLAN 1.

3. Configure VLAN that is allowed to pass Trunk port, the steps are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter corresponding physical port configuration mode
3	switchport trunk allowed vlan { all <i>vlan-list</i> add <i>add-vlan-list</i> remove <i>remove-vlan-list</i> }	Configure the allowed VLAN for the Trunk port All: allow all vlan <i>vlan-list</i> : allow all VLAN, rewrite the primary configuration Add: <i>add-vlan-list</i> : add vlan base on the existent vlan <i>remove</i> : remove-vlan-list, remote vlan base on the existent vlan
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface port [port-list] switchport	Show port VLAN attribute configuration

Use **no switchport trunk allowed vlan** to restore Trunk port allowed VLAN list to default value, that is, all the VLAN.

When the user is configured the HYBRID mode or UNTAG VLAN that is allowed to pass, user will be noticed ‘please input ‘y’ to confirm the allowed VLAN’, input ‘y/Y’ or press ENTER directly for confirmation, then the configured value will take effect, or the configuration will not take effect when user input other value.

4. Configure Native VLAN of Trunk port, the steps are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter corresponding physical port configuration mode
3	switchport trunk native vlan <i><1-4094></i>	Configure Native VLAN of Trunk port
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface port [<i>port-list</i>] switchport	Show port VLAN attribute configuration

Use **no switchport native vlan** to restore Native VLAN of Trunk port to default value, or VLAN1.

21.2.1.5 Configure port protection (isolation)

The configuration steps are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter corresponding physical port configuration mode
3	switchport protect	Configure the physical port to protected port Protect the protected port
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show switchport protect	Show physical port protection attribute

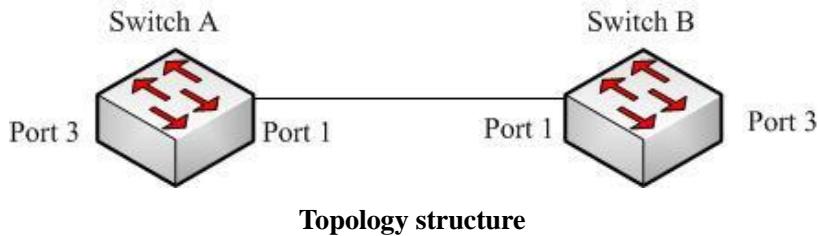
Use **no switchport protect** to cancel port protection configuration.

21.2.1.6 Monitoring and maintenance

Command	Description
show interface port [<i>port-list</i>] switchport	Show port VLAN attribute configuration
show interface port protected	Show physical port protection attribute
show vlan	Show port VLAN attribute configuration

21.2.1.7 Typical configuration example

The topology structure is shown below:



As is shown in figure 1, the Switch A and SwtichB use Port1 (SwtichA) and Port1 (SwitchB) to connect each other, configure Port1 of the two equipments to Trunk port, allowVLAN1-VLAN100 to pass, Port3 (SwtichA) and Port3 (SwtichB) are Access port, Access VLAN is VLAN6. The configuration of SwitchA and SwitchB are totally the same, now SwitchA configuration will be shown.

SwitchA configuration is as follows:

```
Raisecom#config
Raisecom(config)#vlan 6
Raisecom(config-vlan)#state active
Raisecom(config-vlan)#exit
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 1-100
Raisecom(config-port)# exit
Raisecom(config)#interface port 3
Raisecom(config-port)#switchport mode access
Raisecom(config-port)# switchport access vlan 6
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show vlan
```

Outer TPID: 0x9100					
VLAN	Name	Status	VLAN-Priority	Ports	
1	Default	active	N/A	1,2,4-26	
6	VLAN0006	active	0	3	

Raisecom#show interface port 1 switchport

Port 1:
Administrative Mode: trunk

Operational Mode: trunk
Access Mode VLAN: 1(default)
Tunnel Mode VLAN: 1(default)
Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a
Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a
Administrative Trunk Allowed VLANs: 1-100
Operational Trunk Allowed VLANs: 1,3-100
Administrative Hybrid Allowed VLANs: 1-4094
Operational Hybrid Allowed VLANs: n/a
Administrative Hybrid Untagged VLANs: 1
Operational Hybrid Untagged VLANs: n/a
Native Mode VLAN: 1(default)
VLAN Ingress Filtering: Enabled
switchport forwarding allowed portlist: n/a

Raisecom#show interface port 3 switchport

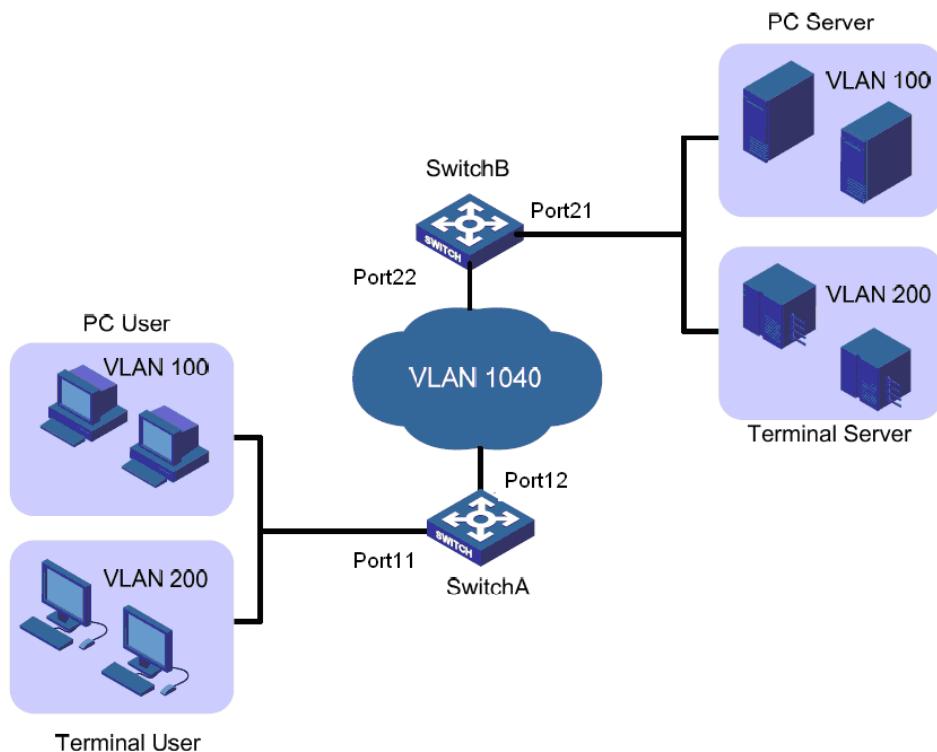
Port 3:
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 6
Tunnel Mode VLAN: 6
Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a
Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: n/a
Administrative Hybrid Allowed VLANs: 1-4094
Operational Hybrid Allowed VLANs: n/a
Administrative Hybrid Untagged VLANs: 1
Operational Hybrid Untagged VLANs: n/a
Native Mode VLAN: 1(default)
VLAN Ingress Filtering: Enabled
switchport forwarding allowed portlist: n/a

Chapter 22 QinQ Configuration

22.1 QinQ principle overview

22.1.1 Basic QinQ

Basic QinQ is a kind of simple layer-two VPN channel technology, which makes message being able to go through the carriers' backbone network (public network) by encapsulating outer-layer VLAN Tag on the carrier access end for the private network messages. In public network, messages transmit according only to outer-layer VLAN Tag, while user private VLAN Tag can be transmitted as the data in the message. The technology helps relieving the public network VLAN ID resource that is becoming rare, while user can now his own private VLAN ID which wouldn't conflict with public network VLAN ID. The typical topology structure of basic QinQ is shown below:



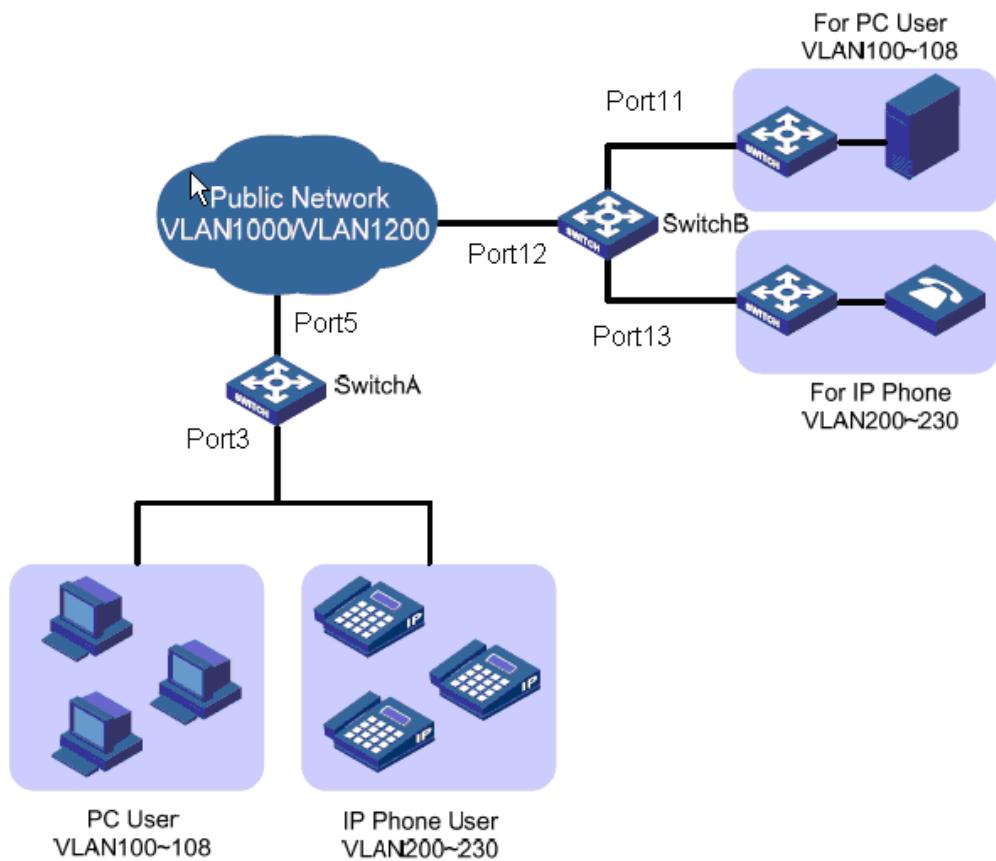
The typical topology of basic QinQ

With QinQ, the limitation of 4096 VLAN on metropolitan area Ethernet can be broken through. The technology extends the ability of establishing layer-two network with VLAN, and it realizes MAN layer-two VPN, which fits MAN and WAN services.

22.1.2 Flexible QinQ

Flexible QinQ is an enhanced application of basic QinQ, which is based on the combination of port and VLAN. Except all the function of basic QinQ, flexible QinQ can take different action according to different VLAN Tags for the messages received from the same port, and adds different outer-layer VLAN ID for different inner-layer VLAN ID. With flexible QinQ, user can configure inner and outer

layer Tag mapping rule, and encapsulate different outer-layer Tags for the messages with different inner-layer Tags according to the mapping rules. Flexible QinQ makes carriers network structure more elastic, and different terminal users can be sorted on the port that is connected with access devices according to VLAN Tag, while QoS strategy can be configured on public network according to outer-layer Tag, and configure the transmission priority flexibly, so that each user can acquire corresponding service. The typical topology structure of flexible QinQ is shown below:



A typical topology structure of flexible QinQ

22.1.3 VLAN conversion

VLAN conversion is mainly used to replace the private VLAN Tag of user message with the VLAN Tag of public network, so that the message can be transmitted as the network planning of the public network. When the messages are transmitted to user's private network, the VLAN Tag will be restored the previous user private network VLAN Tag, so that the messages can be sent to destination correctly.

When the switch receives a message with user private network VLAN Tag, user private network message will be matched following the configured VLAN conversion rules. If they match each other successfully, the private network VLAN Tag will be replaced following the VLAN conversion rules.

Different from QinQ, VLAN conversion function needs not multi-layer VLAN Tag encapsulation, and let the messages transmit in the network planning of public network. The typical topology of VLAN conversion is similar with typical flexible QinQ topology.

22.2 Basic QinQ configuration

22.2.1 Default configuration

Function	Default value
Outer-layer Tag TPID value	0x8100
Port basic QinQ	disable
Port double Tag function	disable

22.2.2 Basic QinQ function configuration

Step	Command	Description
1	config	Enter global configuration
2	mls double-tagging tpid <i>HHHH</i>	Configure outer-layer Tag TPID (optional) <i>HHHH</i> : TPID value, range is 0x0000-0xFFFF
3	interface port <i>portid</i>	Enter port configuration mode
4	switchport qinq dot1q-tunnel	Enable port basic QinQ function qinq VLAN nesting dot1q-tunnel enable port TUNNEL function
5	exit	Return to global configuration mode
6	exit	Return to global configuration mode

Use **no mls double-tagging tpid** to restore outer-layer Tag TPID to default value, which is 0x8100.

Use **no switchport qinq** to disable port basic qinq function.

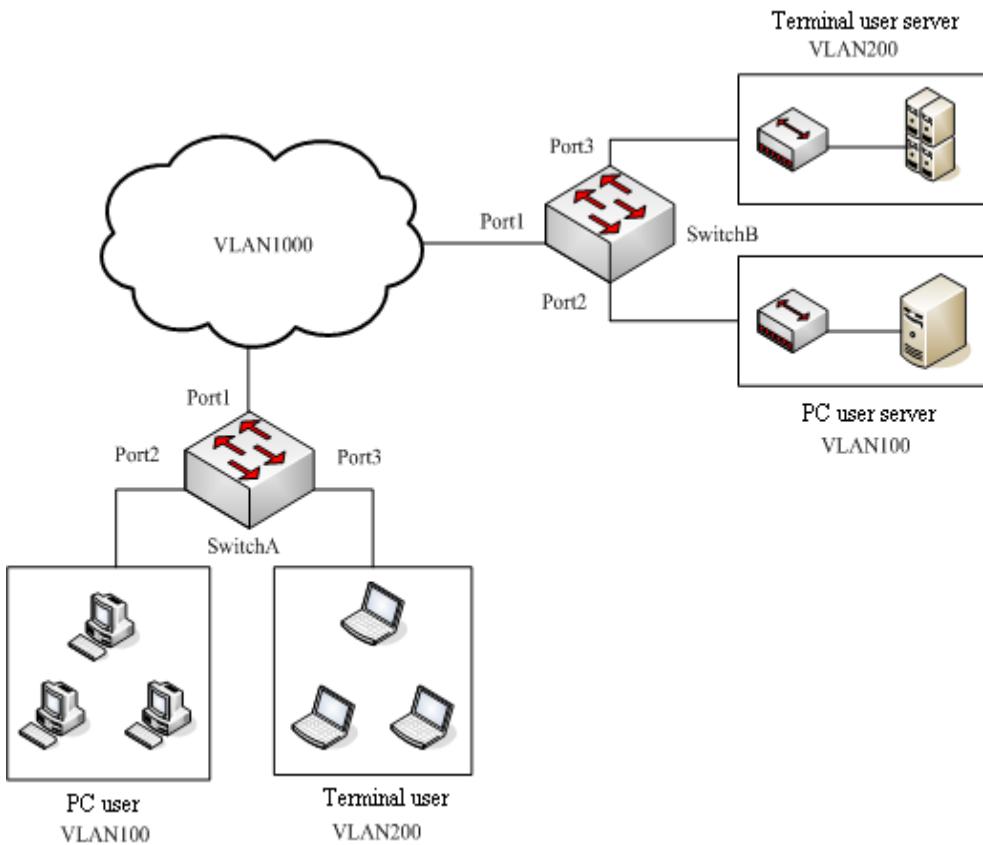
Use **no switchport qinq** to disable port double Tag function.

22.2.3 Monitoring and maintenance

Command	Description
show switchport qinq	Show port basic QinQ related configuration

22.2.4 Typical configuration example

The topology is shown below:



Basic QinQ topology structure

As above, Switch A Port2 and Port3 connect PC user in VLAN 100 and terminal user in VLAN 200 respectively, SwitchB port2 and Port3 connect PC user server in VLAN 100 and terminal user server in VLAN 200, VLAN 1000 is used in carrier network for transmission, and the carrier network TPID is 9100. Configure SwitchA and SwitchB to realize basic QinQ function.

The steps to configure SwitchA are shown below:

Raisecom#**config**

```
Raisecom(config)#mls double-tagging tpid 9100
```

```
Raisecom(config)#create vlan 100,200,1000 active
```

```
Raisecom(config)#interface port 1
```

```
Raisecom(config-port)#switchport mode trunk
```

```
Raisecom(config-port)#switchport trunk allowed vlan 1000
```

```
Raisecom(config-port)#exit
```

```
Raisecom(config)#interface port 2
```

```
Raisecom(config-port)#switchport mode access
```

```
Raisecom(config-port)#switchport access vlan 1000
```

```
Raisecom(config-port)#switchport qinq dot1q-tunnel
```

```
Raisecom(config-port)#exit
```

```
Raisecom(config)#interface port 3
```

```
Raisecom(config-port)#switchport mode trunk
```

```
Raisecom(config-port)#switchprot trunk native vlan 1000
Raisecom(config-port)#switchport qinq dot1q-tunnel
Raisecom(config-port)#exit
Raisecom(config)#show switchport qinq

Outer TPID: 0x9100
Port      QinQ Status
-----
1        Double-tagging
2        Dot1q-tunnel
3        Dot1q-tunnel
4        --
5        --
6        --
7        --
8        --
```

SwtichB are shown below:

```
Raisecom#config
Raisecom(config)#mls double-tagging tpid 9100
Raisecom(config)#create vlan 100,200,1000 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 1000
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode access
Raisecom(config-port)#switchport access vlan 1000
Raisecom(config-port)#switchport qinq dot1q-tunnel
Raisecom(config-port)#exit
Raisecom(config)#interface port 3
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchprot trunk native vlan 1000
Raisecom(config-port)#switchport qinq dot1q-tunnel
Raisecom(config-port)#exit
Raisecom(config)#show switchport qinq

Outer TPID: 0x9100
Port      QinQ Status
```

1	<i>Double-tagging</i>
2	<i>Dot1q-tunnel</i>
3	<i>Dot1q-tunnel</i>
4	--
5	--
6	--
7	--
8	--

22.3 Configure flexible QinQ

Note: RC551 series devices are not in support of this configuration.

22.3.1 Configure flexible QinQ function

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter port configuration mode
3	switchport vlan-mapping <i>vlanlist</i> add-outer <i>vlanid</i>	Add Tag VLAN mapping vlan-mapping: VLAN nesting <i>vlanlist</i> : user network inner layer VLAN IDs add-outer: add outer-layer Tag <i>vlanid</i> : outer-layer VLAN ID
4	exit	Return to global configuration mode

Use **no switchport vlan-mapping add-outer *vlanid*** to delete flexible QinQ adding TAG VLAN mapping rules.

Note:

- In the same port, if the VLAN list of the VLAN mapping rule conflicts with the existed VLAN mapping rules, then the system will return mapping rules confliction, and the configuration fails;
- In the same port, if the VLAN matched mapping rule that is designated by VLAN mapping rule has existed, delete the existed VLAN mapping rule, then the later configured VLAN mapping rule will cover the existed mapping rule.

22.3.2 Monitoring and maintenance

Command	Description
show interface port [<i>portid</i>] vlan-mapping add-outer	Show port flexible QinQ adding Tag VLAN mapping rule
show interface line [<i>lineid</i>]	Show line port flexible QinQ adding

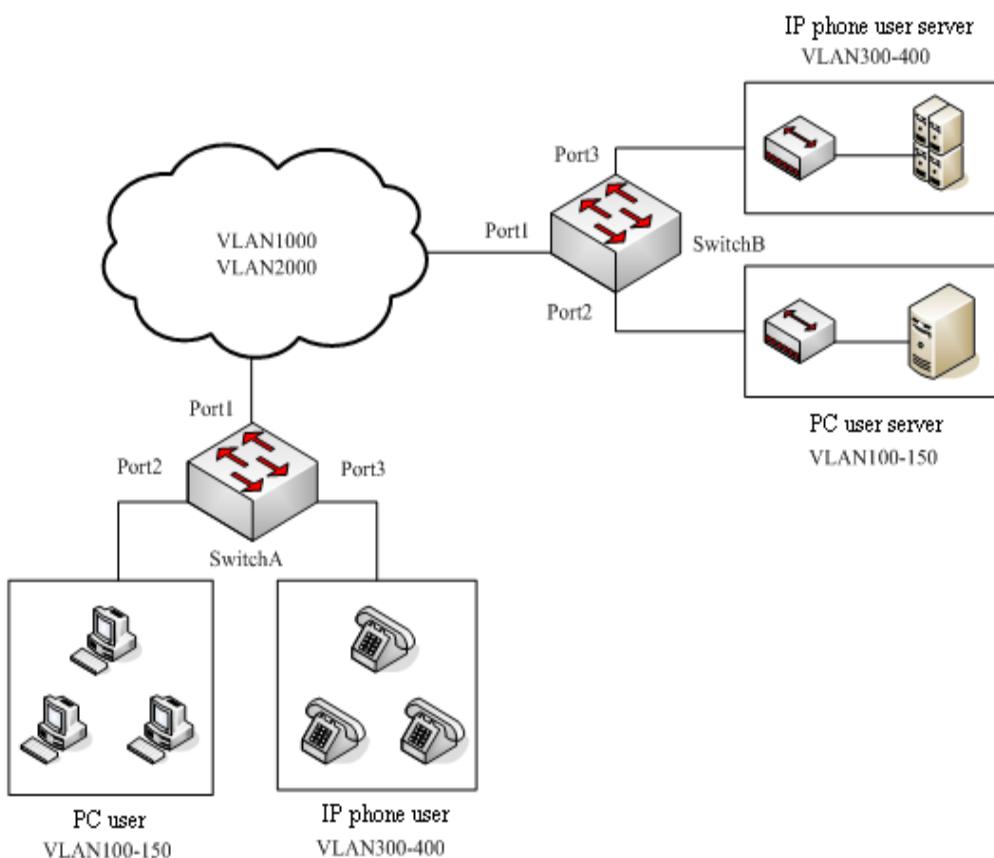
vlan-mapping add-outer	Tag VLAN mapping rule
show interface client [clientid]	Show user port flexible QinQ adding

vlan-mapping add-outer Tag VLAN mapping rule

22.3.3 Typical configuration example

The topology structure is as below:

SwitchA Port2 and Port3 connect PC user in VLAN 100 and terminal user in VLAN 200 respectively, SwitchB port2 and Port3 connect PC user server in VLAN 100-150 and IP phone user server using VLAN 300-400, VLAN 1000 is used in carrier network for transmission, and the carrier network TPID is 9100. Configure SwitchA and SwitchB flexible QinQ function to realize the normal communication between the server and PC/IP phone user.



Flexible QinQ topology structure

The steps to configure Switch A are shown below:

Raisecom#config

Raisecom(config)#mls double-tagging tpid 9100

Raisecom(config)#create vlan 100-150,300-400,1000,2000 active

Raisecom(config)#interface port 1

Raisecom(config-port)#switchport mode trunk

Raisecom(config-port)#switchport trunk allowed vlan 1000,2000

```

RaiseCom(config-port)#exit
RaiseCom(config)#interface port 2
RaiseCom(config-port)#switchport mode trunk
RaiseCom(config-port)# switchport qinq dot1q-tunnel
RaiseCom(config-port)#switchport vlan-mapping 100-150 add-outer 1000
RaiseCom(config-port)#switchport trunk untag vlan 1000,2000
RaiseCom(config-port)#exit
RaiseCom(config)#interface port 3
RaiseCom(config-port)#switchport mode trunk
RaiseCom(config-port)# switchport qinq dot1q-tunnel
RaiseCom(config-port)#switchprot vlan-mapping 300-400 add-outer 2000
RaiseCom(config-port)#switchport trunk untag vlan 1000,2000
RaiseCom(config-port)#exit
RaiseCom(config)#show interface port 2 vlan-mapping add-outer

```

<i>Port</i>	<i>Original Inner VLAN List</i>	<i>Add-outer VLAN</i>	<i>Hw Status</i>	<i>Hw-ID</i>
2	100-150	1000	Enable	1

```
RaiseCom(config)#show interface port 3 vlan-mapping add-outer

```

<i>Port</i>	<i>Original Inner VLAN List</i>	<i>Add-outer VLAN</i>	<i>Hw Status</i>	<i>Hw-ID</i>
3	300-400	2000	Enable	2

SwitchB is configured as below:

```

RaiseCom#config
RaiseCom(config)#mls double-tagging tpid 9100
RaiseCom(config)#create vlan 100-150,300-400,1000,2000 active
RaiseCom(config)#interface port 1
RaiseCom(config-port)#switchport mode trunk
RaiseCom(config-port)#switchport trunk allowed vlan 1000,2000
RaiseCom(config-port)#exit
RaiseCom(config)#interface port 2
RaiseCom(config-port)#switchport mode trunk
RaiseCom(config-port)#switchport vlan-mapping 100-150 add-outer 1000
RaiseCom(config-port)#switchport trunk untag vlan 1000,2000
RaiseCom(config-port)# switchport qinq dot1q-tunnel

```

```

Raisecom(config-port)#exit
Raisecom(config)#interface port 3
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport vlan-mapping 300-400 add-outer 2000
Raisecom(config-port)#switchport trunk untag vlan 1000,2000
Raisecom(config-port)# switchport qinq dot1q-tunnel
Raisecom(config-port)#exit
Raisecom(config)#show interface port 2 vlan-mapping add-outer

      Port   Original Inner VLAN List   Add-outer VLAN      Hw Status   Hw-ID
-----
      2       100-150                      1000            Enable      1
Raisecom(config)#show interface port 3 vlan-mapping add-outer

      Port   Original Inner VLAN List   Add-outer VLAN      Hw Status   Hw-ID
-----
      3       300-400                      2000            Enable      2

```

22.4 Configure VLAN conversion

22.4.1 Configure VLAN conversion function

22.4.1.1 Configure VLAN conversion based on single Tag

Note: ISCOM2128EA-MA products are not in support of the vlan-mapping and egress outer commands in step 2 and step 4.

The configuration steps are shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter port configuration mode
3	switchport vlan-mapping ingress <i>vlanlist translate <i>vlanid</i></i>	Configure ingress VLAN conversion rule (RC551 series devices are not in support of this configuration.)
		vlan-mapping: VLAN-mapping ingress: ingress vlanlist: user VLAN IDs translate: translate vlanid: VLAN-mapping rule ID
4	switchport vlan-mapping egress <i>vlanlist translate <i>vlanid</i></i>	Configure egress VLAN conversion rule
		vlan-mapping: VLAN-mapping egress: egress vlanlist: user VLAN IDs

5**exit**

Return to global configuration mode

Use **no switchport vlan-mapping ingress translate *vlanid*** to delete ingress VLAN transmission rule configured under port.

Use **no switchport vlan-mapping egress translate *vlanid*** to delete egress VLAN transmission rule under port.

Note:

- To configure 1:1 VLAN transmission, it is needed to configure both ingress VLAN conversion and egress VLAN conversion.
- For some equipment, in port egress VLAN conversion outer VLAN can't be the same with TRUKE NATIVE VLAN on the port. Under ACCESS mode, configure TRUNK NATIVE alike outer vlan of VLAN conversion rule, then it will failure when configured to TRUNK. Modify or delete it, TRUNK mode can be successful again.

22.4.1.2 Configure VLAN conversion based on two Tags

Note: ISCOM2128EA-MA products are not in support of VLAN conversion based on two tags.

The configuration steps are shown below:

Step	Command	Description
1	config	Enter global configuration
2	interface port <i>portid</i>	Enter port configuration mode
3	switchport vlan-mapping ingress outer (all <i>vlanlist</i>) inner (all <i>vlanlist</i>) translate outer <i>vlanid</i>	Configure flexible QinQ adding Tag VLAN mapping rule vlan-mapping: VLAN-mapping ingress: ingress outer: outer-layer tag all: all VLAN IDs vlanlist: user network outer-layer VLAN ID inner: inner-layer tag all: all VLAN IDs vlanlist: user network inner-layer VLAN IDs translate: translate outer: outer-layer Tag vlanid: outer-layer VLAN ID
4	exit	Return to global configuration mode

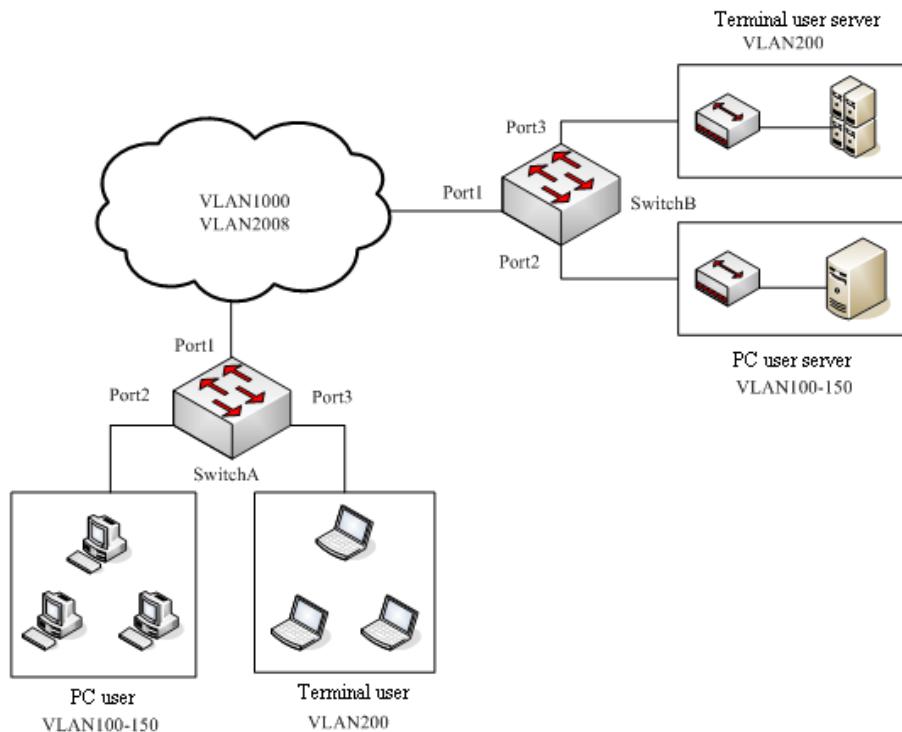
Use **no switchport vlan-mapping ingress translate <1-4094>** to delete VLAN conversion rule configured under port.

Note:

- In the same port, if the VLAN list of VLAN transmission rule conflicts with the existed VLAN conversion rule, then the system will return conversion rule confliction and configuration failure.
- In the same port, if the conversion rule that matches the VLAN designated with the VLAN conversion rules exists, then the existed VLAN conversion rule will be deleted, and the later configured VLAN conversion rule will cover the existed conversion rule.

22.4.2 Monitoring and maintenance

Command	Description
show interface port [portid] vlan-mapping (ingress / egress) translate	Show port VLAN conversion rule (RC551 series devices are not in support of ingress configuration)
show interface line [lineid] vlan-mapping (ingress / egress / both) translate	Show line port VLAN conversion rule (RC551 series devices are not in support of ingress configuration)
show interface client [clientid] vlan-mapping (ingress / egress / both) translate	Show user port VLAN conversion rule (RC551 series devices are not in support of ingress configuration)

22.4.3 Typical configuration example**22.4.3.1 The typical configuration example based on single Tag VLAN****VLAN conversion topology structure based on single TAG**

As above, SwitchA Port2 and Port3 connects PC user in VLAN100-150, SwitchB Port2 and Port3 connects PC user server using VLAN100-150 and terminal user server using VLAN200. In the carrier network VLAN1000 will be designated to PC user for transmission, while VLAN2008 will be

designated to terminal user for transmission. By configuring 1:1 and N:1 VLAN conversion on SwitchA and SwtichB to realize the communication between the servers and PC/terminal user.

The configuration:

SwitchA configuration:

Raisecom#**config**

Raisecom(config)#**create vlan 100-150,200,1000,2008 active**

Raisecom(config)#**interface port 1**

Raisecom(config-port)#**switchport mode trunk**

Raisecom(config-port)#**switchport trunk allowed vlan 1000,2008**

Raisecom(config-port)#**exit**

Raisecom(config)#**interface port 2**

Raisecom(config-port)#**switchport mode trunk**

Raisecom(config-port)#**switchport vlan-mapping cvlan 100-150 translate 1000**

Raisecom(config-port)#**switchport trunk allowed vlan 100-150**

Raisecom(config-port)#**exit**

Raisecom(config)#**interface port 3**

Raisecom(config-port)#**switchport mode trunk**

Raisecom(config-port)#**switchport vlan-mapping ingress 200 translate 2008**

Raisecom(config-port)#**switchport vlan-mapping egress 2008 translate 200**

Raisecom(config-port)#**switchport trunk allowed vlan 200**

Raisecom(config-port)#**exit**

Raisecom(config)#**show interface port 2 vlan-mapping both translate**

Direction: Both

<i>Port</i>	<i>Outer VLAN</i>	<i>Customer VLAN List</i>	<i>Provider VLAN List</i>
-------------	-------------------	---------------------------	---------------------------

2	1000	n/a	100-150
---	------	-----	---------

Raisecom(config)#**show interface port 3 vlan-mapping ingress translate**

Direction: Ingress

<i>Original</i>	<i>Original</i>	<i>Outer-tag</i>	<i>New</i>	<i>Inner-tag</i>	<i>New</i>
<i>Port Inner VLANs</i>	<i>Outer VLANs</i>	<i>Mode</i>		<i>Outer-VID Mode</i>	<i>Inner-VID Hw-ID</i>

3	n/a	200	Translate	2008	--	--	1
---	-----	-----	-----------	------	----	----	---

Raisecom(config)#**show interface port 3 vlan-mapping egress translate**

Direction: Egress

<i>Original</i>	<i>Original</i>	<i>Outer-tag</i>	<i>New</i>	<i>Inner-tag</i>	<i>New</i>
<i>Port Inner VLANs</i>	<i>Outer VLANs</i>	<i>Mode</i>		<i>Outer-VID Mode</i>	<i>Inner-VID Hw-ID</i>

3	n/a	2008	Translate	200	--	--	2
---	-----	------	-----------	-----	----	----	---

SwitchB is configured as below:

```
Raisecom#config
```

```
Raisecom(config)#create vlan 100-150,200,1000,2008 active
```

```
Raisecom(config)#interface port 1
```

```
Raisecom(config-port)#switchport mode trunk
```

```
Raisecom(config-port)#switchport trunk allowed vlan 1000,2008
```

```
Raisecom(config-port)#exit
```

```
Raisecom(config)#interface port 2
```

```
Raisecom(config-port)#switchport mode trunk
```

```
Raisecom(config-port)#switchport vlan-mapping both 100-150 translate 1000
```

```
Raisecom(config-port)#switchport trunk allowed vlan 100-150
```

```
Raisecom(config-port)#exit
```

```
Raisecom(config)#interface port 3
```

```
Raisecom(config-port)#switchport mode trunk
```

```
Raisecom(config-port)#switchport vlan-mapping ingress 200 translate 2008
```

```
Raisecom(config-port)#switchport vlan-mapping egress 2008 translate 200
```

```
Raisecom(config-port)#switchport trunk allowed vlan 200
```

```
Raisecom(config-port)#exit
```

```
Raisecom(config)#show interface port 2 vlan-mapping both translate
```

Direction: Both

Port	Outer VLAN	Customer VLAN List	Provider VLAN List
------	------------	--------------------	--------------------

2	1000	n/a	100-150
---	------	-----	---------

```
Raisecom(config)#show interface port 3 vlan-mapping ingress translate
```

Direction: Ingress

Port	Inner VLANs	Outer VLANs	Mode	Outer-VID	Mode	Inner-VID	Hw-ID
------	-------------	-------------	------	-----------	------	-----------	-------

3	n/a	200	Translate	2008	--	--	1
---	-----	-----	-----------	------	----	----	---

```
Raisecom(config)#show interface port 3 vlan-mapping egress translate
```

Direction: Egress

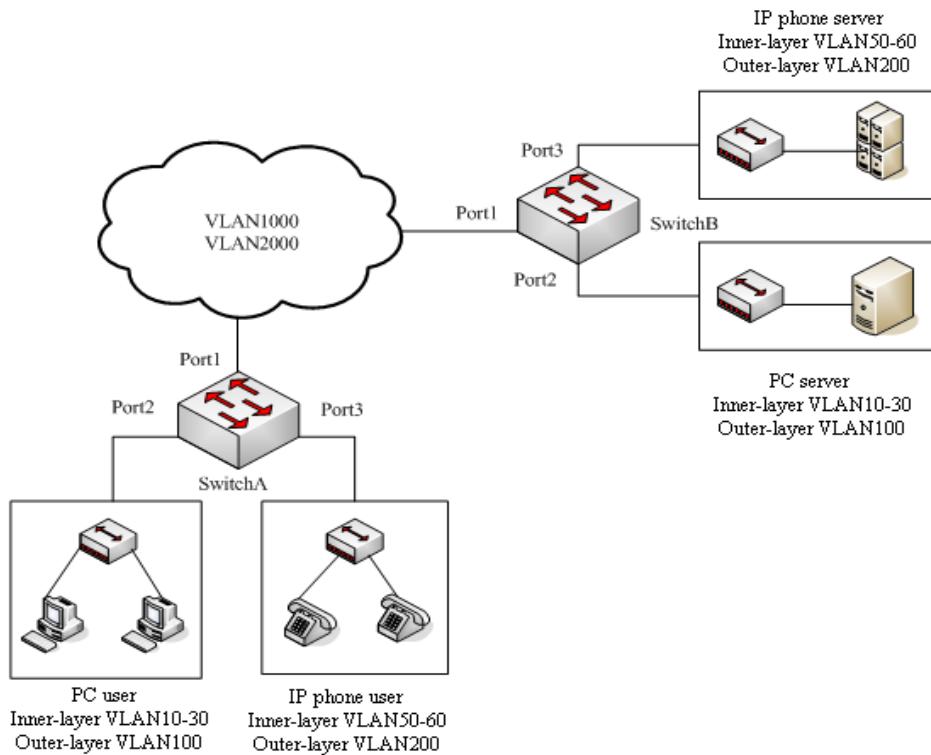
Port	Inner VLANs	Outer VLANs	Mode	Outer-VID	Mode	Inner-VID	Hw-ID
------	-------------	-------------	------	-----------	------	-----------	-------

3	n/a	2008	Translate	200	--	--	2
---	-----	------	-----------	-----	----	----	---

22. 4. 3. 2 The typical configuration example of VLAN conversion based on two Tags

Note: ISCOM2128EA-MA products are not in support of VLAN conversion based on two tags.

The topology is shown below:



The topology of VLAN conversion based on two Tags

SwitchA Port2 and Port3 connect PC user that uses outer-layer VLAN100 and inner-layer10-30 and IP phone user that uses outer-layer VLAN200 and inner-layer VLAN50-60 respectively, SwtichB Port2 and Port3 uses PC server that uses outer-layer VLAN100 and inner-layer10-30 and IP phone server that uses outer-layer VLAN200 and inner-layer VLAN50-60. In carrier network VLAN1000 is used for PC user service, while VLAN2000 is used for IP phone service. By configuring VLAN conversion function based on two Tag on SwitchA and SwtichB, the communication between the server and PC/IP user can be realized, the configuration is as follows:

Switch configuration:

Raisecom#config

```
Raisecom(config)#create vlan 10-30,50-60,100,200,1000,2000 active
```

```
Raisecom(config)#interface port 1
```

```
Raisecom(config-port)#switchport mode trunk
```

```
Raisecom(config-port)#switchport trunk allowed vlan 100,200,1000,2000
```

```
Raisecom(config-port)#switchport vlan-mapping ingress outer 1000 inner 10-30 translate outer 100
```

```
Raisecom(config-port)#switchport vlan-mapping ingress outer 2000 inner 50-60 translate outer 200
```

```
Raisecom(config-port)#mac-address-table vlan-copy from 1000 to 100
```

```
Raisecom(config-port)#mac-address-table vlan-copy from 2000 to 200
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport vlan-mapping ingress outer 100 inner 10-30 translate outer 1000
Raisecom(config-port)#switchport trunk allowed vlan 100
Raisecom(config-port)#mac-address-table vlan-copy from 100 to 1000
Raisecom(config-port)#exit
Raisecom(config)#interface port 3
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport vlan-mapping ingress outer 200 inner 50-60 translate outer 2000
Raisecom(config-port)#mac-address-table vlan-copy from 200 to 2000
Raisecom(config-port)#switchport trunk allowed vlan 200
Raisecom(config-port)#exit
Raisecom(config)#show interface port 1 vlan-mapping ingress translate
```

Direction: Ingress

<i>Port</i>	<i>Original Inner VLANs</i>	<i>Original Outer VLANs</i>	<i>Outer-tag Mode</i>	<i>New Outer-VID Mode</i>	<i>Inner-tag Mode</i>	<i>New Inner-VID Hw-ID</i>
<hr/>						
1	10-30	1000	Translate	100	--	--
1	50-60	2000	Translate	200	--	--

```
Raisecom(config)#show interface port 2 vlan-mapping ingress translate
```

Direction: Ingress

<i>Port</i>	<i>Original Inner VLANs</i>	<i>Original Outer VLANs</i>	<i>Outer-tag Mode</i>	<i>New Outer-VID Mode</i>	<i>Inner-tag Mode</i>	<i>New Inner-VID Hw-ID</i>
<hr/>						
2	10-30	100	Translate	1000	--	--

```
Raisecom(config)#show interface port 3 vlan-mapping ingress translate
```

Direction: Ingress

<i>Port</i>	<i>Original Inner VLANs</i>	<i>Original Outer VLANs</i>	<i>Outer-tag Mode</i>	<i>New Outer-VID Mode</i>	<i>Inner-tag Mode</i>	<i>New Inner-VID Hw-ID</i>
<hr/>						
3	50-60	200	Translate	2000	--	--

SwitchB is configured as below:

```
Raisecom#config
```

```

Raisecom(config)#create vlan 10-30,50-60,100,200,1000,2000 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100,200,1000,2000
Raisecom(config-port)#switchport vlan-mapping ingress outer 1000 inner 10-30 translate outer 100
Raisecom(config-port)#switchport vlan-mapping ingress outer 2000 inner 50-60 translate outer 200
Raisecom(config-port)#mac-address-table vlan-copy from 1000 to 100
Raisecom(config-port)#mac-address-table vlan-copy from 2000 to 200
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport vlan-mapping ingress outer 100 inner 10-30 translate outer 1000
Raisecom(config-port)#switchport trunk allowed vlan 100
Raisecom(config-port)#mac-address-table vlan-copy from 100 to 1000
Raisecom(config-port)#exit
Raisecom(config)#interface port 3
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport vlan-mapping ingress outer 200 inner 50-60 translate outer 2000
Raisecom(config-port)#mac-address-table vlan-copy from 200 to 2000
Raisecom(config-port)#switchport trunk allowed vlan 200
Raisecom(config-port)#exit
Raisecom(config)#show interface port 1 vlan-mapping ingress translate

```

Direction: Ingress

<i>Port</i>	<i>Original Inner VLANs</i>	<i>Outer VLANs</i>	<i>Mode</i>	<i>Outer-tag</i>	<i>New</i>	<i>Inner-tag</i>	<i>New</i>
<hr/>							
1	10-30	1000		Translate	100	--	--
1	50-60	2000		Transalte	200	--	--

```
Raisecom(config)#show interface port 2 vlan-mapping ingress translate
```

Direction: Ingress

<i>Port</i>	<i>Original Inner VLANs</i>	<i>Outer VLANs</i>	<i>Mode</i>	<i>Outer-tag</i>	<i>New</i>	<i>Inner-tag</i>	<i>New</i>
<hr/>							
2	10-30	100		Translate	1000	--	--

Raisecom(config)#**show interface port 3 vlan-mapping ingress translate**

Direction: Ingress

<i>Port</i>	<i>Inner VLANs</i>	<i>Outer VLANs</i>	<i>Mode</i>	<i>Outer-VID Mode</i>	<i>Inner-VID Hw-ID</i>	
3	50-60	200	<i>Translate</i>	2000	--	--

Chapter 23 Multicast

23.1 Multicast Overview

23.1.1 The confusion of unicast/broadcast

As Internet develops, on one side the interactive data, voice and video information in the network are becoming more and more, on the other side the rising services like electronic commerce, network meeting, network auction, video on demand and remote education are in gradual rise. These services have new request on information security and payment, which traditional unicast and broadcast can not meet well.

23.1.2 Information transmission in unicast

With unicast, the system will establish a single data transmission channel for the user who needs the information, and send a single copy to the user, as is shown below:

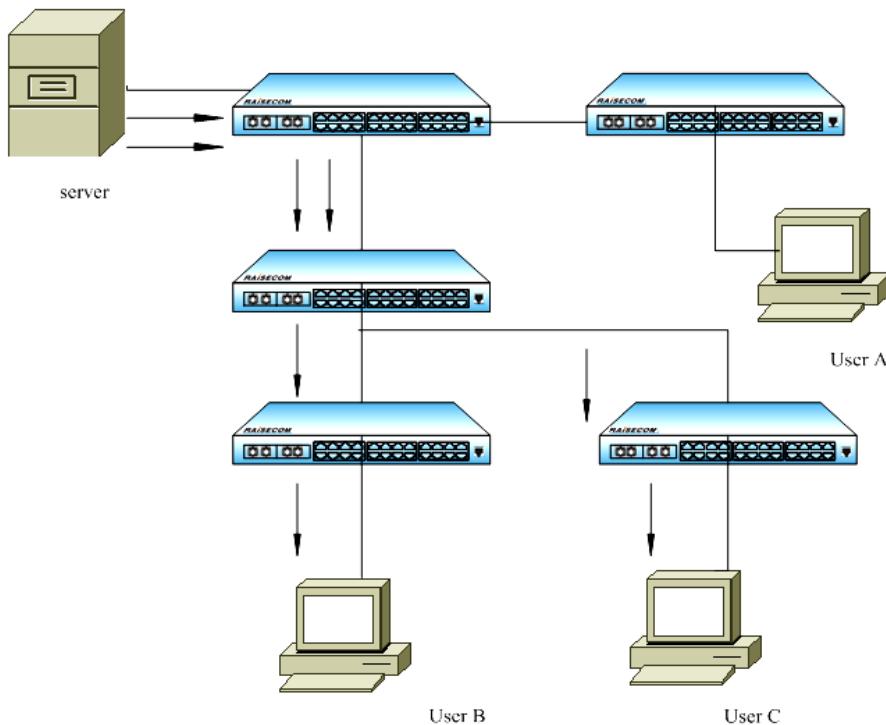


Fig 23-1 unicast transmission

Suppose user B and C need the information, the information source Server will establish transmission channel for user B and C respectively. Because the information capacity transmitted in the network is in proportion to the capacity of users who need the information, when the number of users who need the information is large, there will be several same information stream in the network. Then bandwidth will be a important bottleneck and unicast goes against sending information in large scale.

23.1.3

Transmitting information in broadcasting

Using broadcast, the system will send the information to all the network users, caring not if it is needed, any user can receive the information from broadcasting, as is shown below:

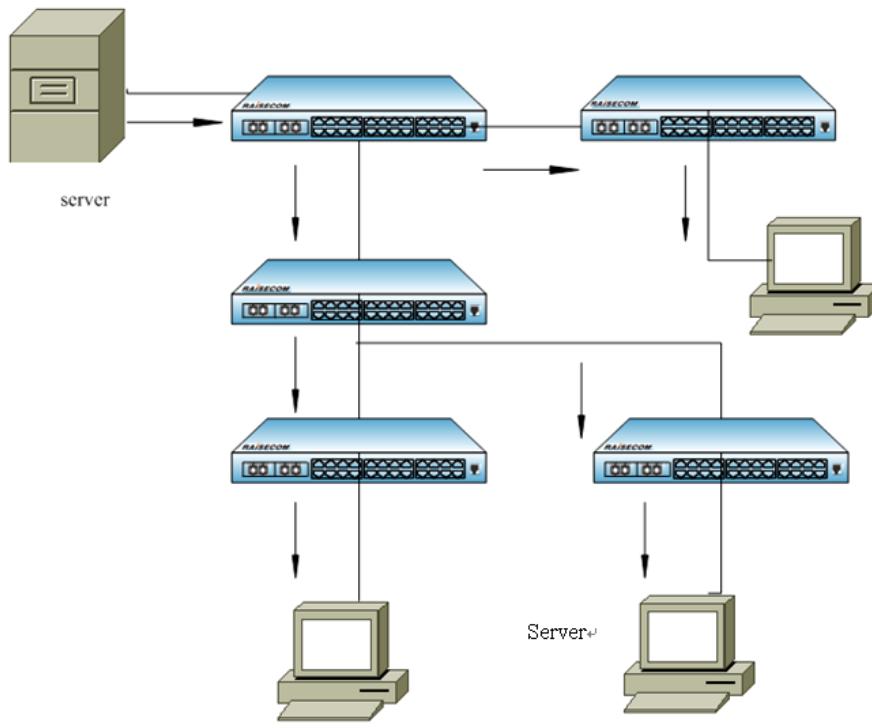


Fig 23-2 Information transmission in broadcast

Suppose user B and C need the information, then information source Server will broadcast the information by router, another network user A can also receive the information, which means information security and payment services can not be ensured. On the other side, when there is not so many users who need the information, network resource use ratio will be quite low, which is a great waste of the bandwidth. In summary, unicast suits the network with rare users, while broadcast suit the network with a lot of people. When the number of users who need the information is not so sure, unicast and broadcast are both low in efficiency.

23.1.4

Information transmission in multicast

The appearance of multicast handles the problem in time. When some users in the network need specific information, multicast source send out information only once, and the information sent out will be copied and sent out in the crossing as far as possible, as is shown below:

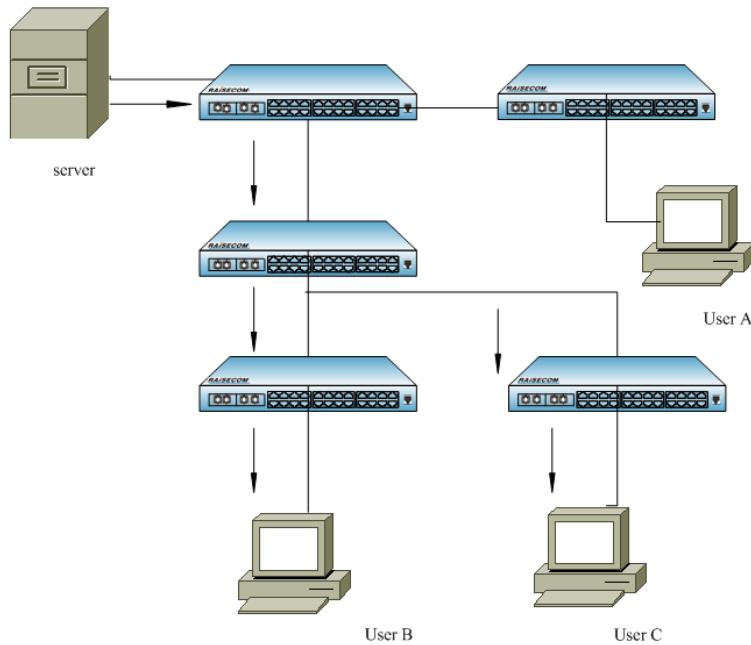


Fig 23-3 Information transmission in multicast

Suppose user B and C need the information, to send the information successfully to the user who really needs it, it is needed to form B, C into a receiver combination, then each switch in the network form its own multicast transmission table according to IGMP message, at last the information will be transmitted accurately to receiver B, C who need it really. In multicast information sender is called ‘multicast source’, but some information receiver call it the ‘multicast group’ of the information. The receiver member who joins the same multicast group can be located in any place in the network, that is to say, there is no domain limit with ‘multicast group’. It should be noted that multicast source does not have to belong to multicast group, it send data to multicast group and don’t have to be receiver itself. There can be several sources sending out messages to one multicast group.

23.1.5

The advantage of multicast is:

- Increase the efficiency and decrease the network traffic, ease the load of the server and CPU;
- Optimize the performance and decrease the redundant traffic;
- Distributed application makes multi-point use possible.

23.2

IGMP Snooping Configuration

This chapter is mainly about how to configure and maintain IGMP Snooping, including:

- About IGMP Snooping
- Configuration task list
- Monitoring and maintenance
- Typical application
- Trouble shooting

23.2.1

About IGMP Snooping protocol

IGMP Snooping, unlike ISO module, has no clear concept module, which takes the upper-layer protocol data information as the bottom-layer working consideration factor. In the transmission of multicast, IGMP Snooping confines data flooding to all the ports, but transmits information only to the multicast member ports, which helps saving the bandwidth.

IGMP snooping allows LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure MAC multicast groups by using the **ip igmp snooping static** command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings. Raisecom series switches supports 1024 two-layer multicast transmission table item, and support IGMPv1 and IGMPv2 version.

23.2.2

IGMP snooping configuration

This part is about how to configure and maintain IGMP Snooping on switch, including:

- Enable and disable IGMP Snooping
- IGMP Snooping aging time
- Multicast Router port configuration
- Configuring immediate-leave function
- Manually configure multicast MAC address table.

Default IGMP snooping configuration

Function	Default value
IGMP SNOOPING starting	On
IGMP SNOOPING out-time	300 seconds
Configure the router time	Do not configure
MVR mode	Compatible
Quit immediately	Disabled
Multicast stable transmission table	Not configured

IGMP Snooping enable and disable

IGMP snooping is disabled on the switch by default. If IGMP snooping is globally enabled/disabled, all the VLAN will enable or disable IGMP snooping function. The following commands are used to enable IP IGMP Snooping:

Step	Command	Description
1	config	Enter global configuration mode
2	ip igmp snooping	Enable IGMP Snooping
3	exit	Exit to privilege mode
4	show ip igmp snooping	Show configuration situation

Use **no ip igmp-snooping** command to disable IP IGMP Snooping.

This command is used to globally disable IGMP snooping function. In order to disable IP IGMP

snooping function on particular VLAN, use the following commands under VLAN configuration mode.

Step	Command	Description
1	config	Enter global configuration mode
2	vlan vlan-id	Enter VLAN configuration mode
3	no ip igmp snooping	Disable the IGMP snooping function for this VLAN.
4	exit	Exit to global configuration mode
5	exit	Exit to privileged EXEC mode
6	show ip igmp snooping vlan vlan-id	Show VLAN configuration information

In order to enable IGMP snooping function on the VLAN, use **ip igmp snooping** in VLAN configuration mode.

If IGMP snooping is disabled globally, IGMP snooping function can not be enabled on particular VLAN.

If user needs to enable or disable IGMP Snooping function on several VLANs, use **ip igmp-snooping vlan** command in global configuration mode according to the following table:

Step	Command	Description
1	config	Enter global configuration mode
2	ip igmp snooping vlan 1-100	Enable IGMP snooping function on VLAN1-100
3	exit	Exit to privileged user mode
4	show ip igmp snooping	Show IGMP Snooping configuration information

Use **no ip igmp snooping vlan** command to disable IGMP snooping function on several VLAN at a time.

In order to check whether the configuration is correct or not, use show command:

Raisecom#**show ip igmp snooping**

IGMP snooping: Enable

IGMP snooping aging time: 300s

IGMP snooping active VLAN: 1,2

IGMP snooping immediate-leave active VLAN: --

Raisecom#**show ip igmp snooping vlan 2**

IGMP snooping: Enable

IGMP snooping aging time: 300s

IGMP snooping on VLAN 2: Enable.

IGMP snooping immediate-leave on VLAN 2: Disable.

Multicast flow filtration mode configuration

The relevant commands are as follows:

Step	Command	Description
1	config	Enter global configuration

		mode
2	mac-address-table multicast filter-mode{ filter-all /forward-all }	Configure multicast flow filtration mode
3	exit	Exit to privilege mode
4	show ip igmp snooping	Show configuration situation

By default, multicast flow filtration mode is forward-all. When you configure it as forward-all, for those unknown multicast flow, switch will forward according to broadcast. For those known multicast flow, switch will forward according to the learnt multicast. When you configure it as filter-all, for those unknown multicast flow, switch will discard. For those known multicast flow, switch will forward according to the learnt multicast.

IGMP snooping aging time configuration

If switch does detect IGMP Snooping Join or Query message within a period, the subscriber may have left already without sending any leaving message, so the switch needs to be deleted the multicast MAC address from the address table. The default aging time is 300 seconds. Configuration steps are showed as follows:

Step	Command	Description
1	config	Enter global configuration mode.
2	ip igmp snooping timeout <i>timeout</i>	Set IGMP overtime.
3	exit	Exit to privilege EXEC mode
4	show ip igmp snooping	Show IGMP Snooping configuration information

The range of aging time is 30 seconds to 3600 seconds, in order to recover default value, use following command: **no ip igmp snooping timeout**

Example:

Raisecom#**config**

SCOM2826(config)# **ip igmp snooping timeout 1200**

ISCOM2128EA-MA(config)#**exit**

Raisecom#**show ip igmp snooping**

IGMP snooping: Enable

IGMP snooping aging time: 3000s

IGMP snooping active VLAN: 1, 2

IGMP snooping immediate-leave active VLAN: 1

Router port configuration

The Multicast Router port can be assigned by dynamically address learning (through IGMP request message), or manually configured (that is to say, multicast report and leave message of downlink hosts can be forwarded to multicast router port). The manual configuration steps of multicast router port are as follows:

Step	Command	Description															
1	config	Enter global configuration mode															
2	ip igmp snooping mrouter vlan <1-4094> port <1-26>	Configure router port															
3	exit	Exit to privileged EXEC mode															
4	show ip igmp snooping mrouter	Show Multicast Router port configuration information															
		Use following command to delete configured Multicast Router port: no ip igmp snooping mrouter vlan 1 port 2.															
		Configuration example:															
	ISCOM2128EA-MA# config																
	ISCOM2128EA-MA(config)# ip igmp snooping mrouter vlan 1 port 2																
	ISCOM2128EA-MA(config)# exit																
	ISCOM2128EA-MA# show ip igmp snooping mrouter																
		<table> <thead> <tr> <th><i>Ip Address</i></th> <th><i>Port</i></th> <th><i>Vlan</i></th> <th><i>Age</i></th> <th><i>Type</i></th> </tr> </thead> <tbody> <tr> <td>-----</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>224.0.0.0/8</td> <td>2</td> <td>1</td> <td>--</td> <td>USER</td> </tr> </tbody> </table>	<i>Ip Address</i>	<i>Port</i>	<i>Vlan</i>	<i>Age</i>	<i>Type</i>	-----					224.0.0.0/8	2	1	--	USER
<i>Ip Address</i>	<i>Port</i>	<i>Vlan</i>	<i>Age</i>	<i>Type</i>													

224.0.0.0/8	2	1	--	USER													

Immediate-leave function configuration:

When you enable IGMP Immediate-Leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port.

The settings are as following:

Step	Command	Description
1	config	Enter global configuration mode
2	vlan 1	Enter VLAN configuration mode
3	ip igmp snooping immediate-leave	Set immediate-leave function on the VLAN.
4	exit	Exit to global configuration mode.
5	exit	Exit to privilege EXEC mode.
6	show ip igmp snooping	Show IGMP Snooping configuration information

In VLAN configuration mode, use **no ip igmp snooping immediate-leave** command to restore default setting:

Configuration example:

```
ISCOM2128EA-MA#config
ISCOM2128EA-MA (config)#vlan 1
ISCOM2128EA-MA (config-vlan)# ip igmp snooping immediate-leave
ISCOM2128EA-MA (config-vlan)#exit
ISCOM2128EA-MA (config)#exit
ISCOM2128EA-MA#show ip igmp snooping vlan 1
```

IGMP snooping: Enable
IGMP snooping aging time: 300s
IGMP snooping on VLAN 1: Enable.
IGMP snooping immediate-leave on VLAN 1: Enable.

In order to configure the immediate-leave function in multiple VLAN, use following commands:

Step	Command	Description
1	config	Enter global configuration mode.
2	ip igmp snooping vlan <i>vlanlist</i> immediate-leave	Set immediate-leave function on the VLAN.
3	exit	Exit to privileged EXEC mode.
4	show ip igmp snooping	Show IGMP Snooping configuration information

In order to restore default settings, use following command: **no ip igmp snooping vlan *vlanlist* immediate-leave**

Example:

```
iscom2016#config
iscom2016(config)# ip igmp snooping vlan 1-10 immediate-leave
iscom2016(config)#exit
iscom2016#show ip igmp snooping
    igmp snooping is globally Enabled
    igmp snooping aging time is 1200(s)
    IGMP snooping active vlan: 1
    IGMP snooping immediate-leave active vlan:1-10
```

Stable multicast transmission table configuration

Usually a port joins multicast router through the IGMP report message from the host. For maintenance, you can add a port to the multicast group manually.

Step	Command	Description
1	config	Enter global configuration mode
2	mac-address-table static multicast mac-addr <i>vlan</i> <i>vlanid</i> <i>port-list</i> <i>portlist</i>	Add the port to the multicast group
3	exit	Exit to privilege user mode
4	show mac-address-table multicast	Show multicast MAC address information

The MAC address is the multicast MAC address, and the format is HHHH.HHHH.HHHH. For example, multicast IP address 224.8.8.8 is mapped to multicast MAC address 0100.5e08.0808; the range of the port is from 1 to 26. In order to delete the port from multicast group manually, use command **no mac-address-table static multicast mac-addr *vlan* *vlanid* *port-list* *portlist***.

Configuration example:

```
Raisecom#config
```

```

ISCOM2128EA-MA(config)# mac-address-table static multicast 0100.5e08.0808 vlan 2 port-list
1-6

ISCOM2128EA-MA(config)#exit

ISCOM2128EA-MA# show mac-address-table multicast

Multicast filter mode: Forward-all

Vlan  Group Address      Ports[Static](Hardware)

-----
2      0100.5E08.0808    1-6[1-6](1-6)

```

23.2.3 Monitoring and maintenance

Use show command to check switch IGMP snooping running and configuration status:

Step	Command	Description
1	show ip igmp snooping [vlan <i>vlan-id</i>]	Show IGMP snooping configuration information in all the VLAN or designated VLAN of the switch.
2	show ip igmp snooping multicast [vlan <i>vlan-id</i>]	Show multicast router port information (dynamically learned or manually configured) of all the VLAN or a designated VLAN.
3	show mac-address-table multicast [vlan <i>vlan-id</i>] [<i>count</i>]	Show all the multicast MAC address; <i>Count</i> : indicates the total number of multicast MAC address

Use **show ip igmp snooping** command to check configuration information, for example the timer, VLAN configuration information.

Show IGMP Snooping configuration information:

Raisecom# **show ip igmp snooping**

IGMP snooping: Enable

IGMP snooping aging time: 300s

IGMP snooping active VLAN: 1, 2

IGMP snooping immediate-leave active VLAN: 1

Use **show ip igmp snooping vlan *vlanid*** command to show the IGMP snooping information in a particular VLAN. If you do not specify VLAN, all the VLAN information will be displayed, that is all the existent and active VLAN.

Show igmp-snooping multicast router information:

Raisecom# **show ip igmp snooping mrouter**

<i>Ip Address</i>	<i>Port</i>	<i>Vlan</i>	<i>Age</i>	<i>Type</i>
224.0.0.8	4	3	--	USER

Raisecom#**show mac-address-table multicast**

Multicast filter mode: Forward-all

Vlan	Group Address	Ports[Static](Hardware)
------	---------------	-------------------------

2	0100.5E08.0808	1-61-6
---	----------------	---------------

23.2.4 Typical configuration example

1) Configuration instruction:

To realize the switch IGMP Snooping function, it is needed to start IGMP Snooping on the switch (by default it's on). The router port (physical port 1) on the switch connects to the router, while other not-router ports connect to users' PC.

2) Typical network structure figure

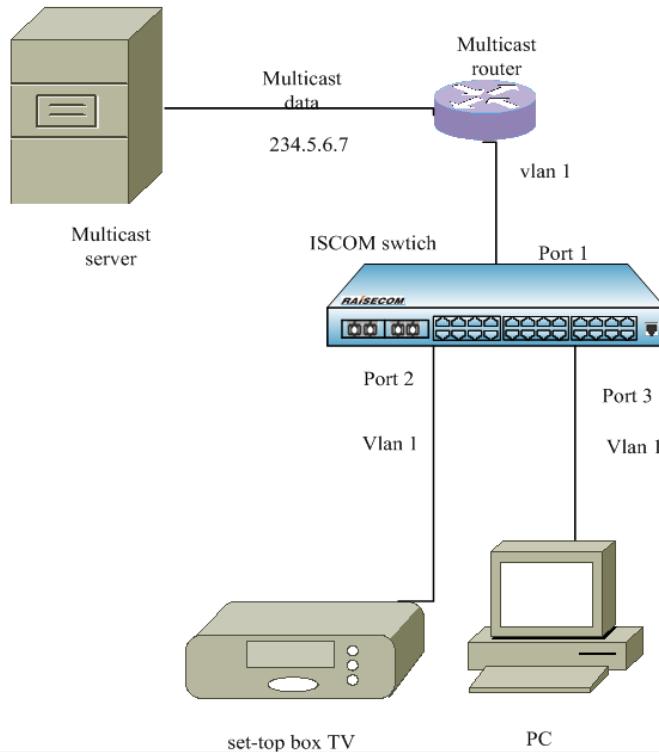


Fig 23-4 Typical IGMP Snooping network structure

3) Configuration command

```
Raisecom(config)#ip igmp snooping
```

Enable IGMP snooping successfully.

```
Raisecom(config)#mac-address-table multicast filter-mode filter-all
```

Set multicast filter mode successfully.

23.2.5

IGMP snooping trouble shooting

1. If multicast router port has not been specified, all the IGMP reports will be transmitted to the port directly connected to the router;

2. If it is failed to add port to a multicast group manually, the reason may be incorrect multicast MAC address format or the maximum layer 2 multicast router table (255) has been achieved;
3. If it is failed to delete the port from multicast group manually, the possible reason may be incorrect multicast MAC address format or MAC address/VLAN/port are not existent in multicast router.

23.3 MVR Configuration

This chapter is mainly about how to configure and maintain MVR and IGMP filtration on the switch, including:

- MVR overview
- MVR proxy principle introduction
- IGMP filtration overview
- MVR configuration
- MVR monitoring and maintenance
- MVR proxy configuration
- MVR proxy monitoring and maintenance
- IGMP filtration configuration
- IGMP filtration monitoring and maintenance
- Typical configuration example
- MVR and IGMP filtration trouble shooting

23.3.1 MVR principle

Multicast VLAN registration is applied as traffic multicast in the network of service provider, such as TV programme ordering. MVR allows subscriber on the port to order or cancel the multicast traffic in VLAN, allows data traffic sharing for different VLANs. There are two MVR aims:

1. By using simple configurations, user can transmit multicast among different VLANs safely and effectively;
2. Support multicast group joining and leaving dynamically;

The operation manner of MVR is similar to that of IGMP snooping. These two functions can be enabled simultaneously. MVR only processes the joining and leaving of configured multicast groups, the other multicast groups are managed by IGMP snooping. The difference between these two is that: with IGMP snooping, the multicast traffic can be transmitted within only one VLAN, while with MVR the multicast traffic can be transmitted within different VLANs.

There are two operation modes:

1. Compatible mode: all multicast data received at the source port (port connected with multicast router) will be forwarded to the other ports, no matter whether these source ports have members to join in or not. Simultaneously, multicast data are only forwarded to those receiving ports (ports connected with subscribers) which are specified to have already joined in the MVR group, the joining can be in the form of IGMP report or MVR static configuration. IGMP report will not be forwarded to the source port of switch. Therefore, the switch does not support source port joining dynamically. Under this mode, multicast router should be configured as forwarding all multicast data to the source port, since switch will not send IGMP joining information to the router.
2. Dynamic mode: Received multicast data are only forwarded to those ports which have member

to join (source port or receiving port), the joining can be in the form of IGMP report information or MVR static configurations. All received IGMP information is forwarded to the source port of the switch. This method could save much bandwidth.

MVR are operative only on Layer-2. It dose not work on Layer-3. One switch can configure only one multicast VLAN, support 256 multicast groups at most.

23.3.2 IGMP filtration introduction

Administrator needs to limit the multicast users under some circumstances, such as to allow which ports to receive multicast on a switch, which ports to reject multicast data. Use can realize this kind of control on the port by configuring IGMP profile. One IGMP profile includes one or multiple multicast groups, and permit/deny items to access these groups. If one “deny” type IGMP profile is applied to the port, when the port receives IGMP joining information of this group, it will drop and do not allow receiving multicast data from this group. IGMP profile can be applied to dynamic multicast group, not suitable for static group.

In addition, the maximum multicast group can be configured on port.

23.3.3 MVR configuration

This part is about how to configure MVR on the switch, including:

- ❖ Default MVR configuration
- ❖ Global MVR configuration
- ❖ Configure MVR port information

Default MVR configuration

Attributes	Default configuration
MVR enable/disable	disabled
Multicast address	Not configured
MVR timeout	600 seconds
Multicast VLAN	1
MVR mode	compatible
Port MVR enable/disable	disabled
Port default configuration	Non MVR (neither source port, nor receiving port)
Intermediate leave	disabled

The steps below should be followed:

- Receiving port can be only ACCESS port, but cannot be TRUNK port. Receiving port can belong to different VLANs, but cannot belong to multicast VLAN;
- The maximum MVR multicast address is 256;
- Since ISCOM28 series switches support Layer-2 multicast, which means multiple IP multicast addresses correspond to one MAC multicast address, MVR multicast address is not allowed using repetitive names during configuration.
- MVR and IGMP snooping can coexist;
- Source port should be in the multicast VLAN;

Global MVR configuration

Under the default situation, MVR is disabled. User can carry out the commands below to enable MVR under global configuration mode. Multicast VLAN, multicast address, operation modes can be configured as well. If MVR has not been enabled yet, it is allowed to configure MVR. Once MVR is enabled, these configurations will take effect at once.

Step	Command	Description
1	config	Enter global configuration mode
2	mvr enable	Enable MVR
3	mvr vlan <i>vlanid</i> group <i>ip-address</i> [count]	Configure IP multicast address, if the parameter count is specified, you can configure a consecutive MVR group addresses (the range for count is from 1 to 256, 1 by default)
4	mvr timeout <i>timeout</i>	optional,MVR multicast entity timeout, unit is second, range is from 60 to 36000, 600 seconds by default.
5	mvr vlan <i>vlanid</i>	Optional, to specify the VLANs for receiving multicast, all source ports should belong to this VLAN. Range is from 1 to 5094. 1 by default.
6	mac-address-table multicast filter-mode{ filter-all /forward-all }	Configure multicast flow filtration mode
7	exit	Back to privileged EXEC mode
8	show mvr	Show MVR configuration
9	show mvr members	Show MVR group address

To disable MVR, carry out command **mvr disable** under global configuration mode. To set the other configurations back to default status, you can use the command **no mvr {mode | group *ip-address* | timeout | vlan}**.

Command **mvr group *ip-address*** indicates which multicast traffic can be received. If this parameter is not specified, all traffics will be received.

The example below shows how to enable MVR, how to configure multicast address, timeout and multicast vlan:

```
raisecom(config)# mvr enable
raisecom (config)# mvr group 234.5.6.7
raisecom (config)# mvr timeout 180
raisecom (config)# mvr vlan 22
raisecom (config)# mvr mode dynamic
```

To check if the configurations are correct, use command **show**:

```
Raisecom#show mvr
```

```
MVR Running: Enable
MVR Multicast VLAN: 22
MVR Max Multicast Groups: 256
```

MVR Current Multicast Groups: 1

MVR Timeout: 180 (second)

MVR Mode: dynamic

To view MVR group address configurations:

Raisecom#**show mvr members**

<i>MVR Group IP</i>	<i>Status</i>	<i>Members</i>
<hr/>		
234.5.6.7	<i>Inactive</i>	<i>none</i>

MVR port information configuration

Under default situation, ports on switch are neither receiving port, nor source ports. User can configure them under interface configuration mode:

Step	Command	Description
1	config	Enter global configuration mode
2	mvr	enable MVR
3	interface port 3	Enter interface configuration mode
4	mvr	Enable interface MVR
		Mvr type configuration: <i>source</i> : uplink port can be configured as souce port for receiving multicast data, this port cannot be connect directly to subscribers, all source ports should belong to multicast VLAN.
5	mvr type {source/receiver}	 <i>receiver</i> : configured as to connect subscribers straightforward, cannot belong to multicast VLAN.
7	mvr immediate	Enable automatic leaving function onthis port, this command can be only applied on receiving port
8	exit	Back to global configuration mode
9	exit	Back to privileged EXEC mode
10	show mvr	Show MVR configuration status
11	show mvr port [portid]	Show port mvr configuration information
12	show mvr port [portid] members	Show port member information

To set port MVR configuration back to default status, you can use command **no mvr [type | immediate | vlan vlan-id group]**. Use command **no mvr vlan vlan-id group** to delete all static multicast group, you can specify a multicast address if you want to delete only one group. The example below shows how to configure port 3 as MVR receiving port, and how to enable intermediate leaving function and how to join into the static multicast group:

Raisecom#**config**

Raisecom(config)#**inter port 3**

Raisecom(config-port)#**mvr**

Raisecom(config-port)#**mvr type receiver**

Raisecom(config-port)#**mvr immediate**

```
Raisecom(config-port)#mvr vlan 1 group 234.5.6.7
Raisecom(config-port)#exit
Raisecom(config)#exit
```

To check if the configurations are correct, use command **show**:

```
Raisecom#show mvr port 3
```

Running: Enable
Type: Receiver
Status: Inactive/down
Immediate Leave: Enable

```
Raisecom#show mvr port 3 members
```

MVR Group IP	Type	Status
234.5.6.7	static	Inactive

23.3.4 MVR monitoring and maintaining

You can use some “show” commands to view the MVR running status and configurations for the switch in which way you can achieve a better monitor and maintenance:

Command mode	Commands below need to run under ENABLE mode
show mvr	Show MVR global configuration information
show mvr members	show MVR group information
show mvr port [portid]	show MVR port configuration information
show mvr port portid members	Show MVR static or dynamic group information

Show MVR global configuration information

```
Raisecom#show mvr
```

MVR Running: Enable
MVR Multicast VLAN: 1
MVR Max Multicast Groups: 256
MVR Current Multicast Groups: 0
MVR Timeout: 600 (second)
MVR Mode: Compatible

Show MVR group information

```
Raisecom#show mvr members
```

MVR Group IP	Status	Members
234.5.6.7	Active	1

```

234.5.6.8      Active      1
234.5.6.9      Inactive    None
234.5.6.10     Inactive    None

```

Show MVR port configuration information

Raisecom#**show mvr port**

<i>Port</i>	<i>Running</i>	<i>Type</i>	<i>Status</i>	<i>Immediate Leave</i>
<hr/>				
1	Enable	Receiver	Inactive/down	Enable
2	Disable	Non-MVR	Inactive/down	Disable
3	Disable	Non-MVR	Inactive/down	Disable
4	Disable	Non-MVR	Inactive/down	Disable
5	Disable	Non-MVR	Inactive/down	Disable
6	Disable	Non-MVR	Inactive/down	Disable
7	Disable	Non-MVR	Inactive/Up	Disable
<hr/>				
.....				
25	Disable	Non-MVR	Inactive/down	Disable
26	Disable	Non-MVR	Inactive/down	Disable

To show designated port information:

Raisecom#**show mvr port 1**

```

Running: Enable
Type: Receiver
Status: Inactive/down
Immediate Leave: Enable

```

Show MVR port group information

Raisecom#**show mvr port 1 members**

<i>MVR Group IP</i>	<i>Type</i>	<i>Status</i>
<hr/>		
234.5.6.7	static	Inactive
234.5.6.8	static	Inactive

23.3.5 IGMP filter configuration

This part is about how to configure IGMP filter on the switch, including:

- Default IGMP filter configuration
- IGMP profile configuration
- Use IGMP profile

Default IGMP filter configuration

Feature	state
IGMP filter enable/disable	Enabled
Port application	No application
Maximum group	No limit
Maximum group action	Reject
IGMP profile	Not defined
IGMP profile action	reject

IGMP profile configuration

Use command **ip igmp profile** under global configuration mode, you can create IGMP profile and enter profile configuration mode. Parameters such as range, actions and etc. can be configured under this mode.

Step	Command	Description
1	config	Enter global configuration mode
2	ip igmp profile <i>profile-number</i>	Create profile and enter profile configuration mode, series number of profile is from 1 to 65535.
3	permit deny	Optional, actions configuration including permit or deny multicast group access, the default status is deny.
4	range <i>start-ip</i> [<i>end-ip</i>]	IP multicast address or address range configurations. If inputting address range, the starting address, blanks and ending address should be within the group address.
5	exit	Back to global configuration mode
6	exit	Back to privileged EXEC mode
8	show ip igmp profile [<i>profile-number</i>]	Show IGMP profile configuration information

To delete profile, carry out **no ip igmp profile** under global configuration mode. To delete a multicast address of profile, use command **no range *start-ip***.

The example below shows how to create profile 1 and configure single multicast address:

```
raisecom(config)# ip igmp profile 1
raisecom (config-profile)# range 234.5.6.7 234.5.6.9
raisecom (config-profile)# permit
raisecom (config-profile)#exit
raisecom (config)#exit
```

To check if the configurations are correct, use command show:

```
Raisecom#show ip igmp profile 1
IGMP profile 1
  permit
    range 234.5.6.7
    range 234.5.6.9
```

Applying IGMP filter under interface

Use command **ip igmp filter** under interface configuration mode to apply the created IGMP profile on a specified port. One IGMP profile can be applied to multiple ports, but one port can have only one IGMP profile.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port 1	Enter interface mode
3	ip igmp filter profile-number	Apply IGMP profile on the port
4	ip igmp max-groups group-number	Set the maximum number of the groups that is allowed for entry
5	ip igmp max-groups action {deny / replace}	The action taken when the group number on the port exceeds the maximum group number
6	exit	Return to global configuration mode
7	exit	Return to privileged EXEC mode
8	show ip igmp filter port [portid]	Show the IGMP profile applied on the port

To cancel applying IGMP profile, use command **no ip igmp filter** under interface configuration mode. If no IGMP profile is applied to port, no result will be shown.

The example below shows how to apply IGMP profile 1:

```
raisecom(config)# interface port 1
raisecom (config-port)# ip igmp filter 1
raisecom (config-port)#exit
raisecom (config)#exit
```

To check if the configurations are correct, use command **show**:

```
Raisecom#show ip igmp filter port
```

Port	Filter	Max Groups	Current Groups	Action
1	1	20	0	Deny
2	0	20	0	Deny
3	0	0	0	Deny
.....				
25	0	0	0	Deny
26	0	0	0	Deny

To view port 1 information:

Raisecom#**show ip igmp filter port 1**

IGMP Filter: 1

Max Groups: 20

Current groups: 0

Action: Deny

Appling IGMP filter under VLAN

By default, there is no IGMP filter applying rules under VLAN, no maximum group limit, the maximum group action is deny. Follow the steps below in global configuration mode to configure the applied filter rules under VLAN, maximum group limit and maximum action.

Step	Command	Description
1	config	Enter global configuration mode
2	ip igmp filter <i>profile-id</i> vlan <i>vlanlist</i>	Specify the defined filter rules on VLAN. The applied filter rule number should have been created, or the configuration fails. Vlanlist range is 1-4094.
3	ip igmp max-group <i>max-group</i> <i>vlan</i> <i>vlanlist</i>	Set the maximum group number on specified VLAN. The configured maximum group number must be no larger than the maximum group number that the equipment supports
4	ip igmp max-group action {deny/replace} <i>vlan</i> <i>vlanlist</i>	Configure the maximum group action the specified VLAN, default value is ‘deny’.
5	exit	Return to privileged EXEC mode
6	show ip igmp filter vlan [vlandid]	Show the configured filter information under VLAN.
7	config	Enter global configuration mode

Use **no ip igmp filter *vlan* *vlanlist*** to delete the configured filter rules under VLAN, use **no ip igmp max-group *vlan* *vlanlist*** to delete the configured maximum group limit under VLAN.

The following example shows how to apply filter rules under VLAN and configure the maximum group limit and maximum group action:

Raisecom (config)# **ip igmp filter 1 vlan 1**

Raisecom (config)# **ip igmp max-group 10 vlan 1**

Raisecom (config)# **ip igmp max-group action replace vlan 1**

Use the command **show** to examine if the configuration is correct

Raisecom # **show ip igmp filter vlan 1**

VLAN	Filter	Max Groups	Current Groups	Action
1	1	10	0	Replace

23.3.6 IGMP filter monitoring and maintenance

Use some **show** commands to show the switch IGMP filter running state and configuration state for

monitoring and maintenance. Use the following **show** commands to do IGMP filter monitoring and maintenance:

Command	Description
show ip igmp filter	Show IGMP filter global configuration information
show ip igmp profile [profile-number]	Show IGMP profile information
show ip igmp filter port [portid]	Show IGMP filter port configuration information
show ip igmp filter vlan [vlanid]	Show the IGMP filter rules configuration under specified VLAN. When vlanid is not specified, show the configuration state of VLAN that have been configured filter rules.

23.3.7 Typical configuration example

MVR typical configuration example

PC or TV set-top box can receive multicast traffics, one or multiple PC or televisions can connect to a receiving port called subscriber. When selecting scheduled programs, set-top or PC sends IGMP report information to join a group. If IGMP report matches to the configured multicast addresses on the switch, the CPU on the switch will modify the multicast switch table in the hardware, and add this port to the multicast VLAN group. When the source port receives the multicast traffic, it will send the traffic to the receiving ports according to the multicast forwarding table in the hardware.

When switching channels or shutting down the TV, the set-top box or PC will send IGMP leaving information, then the switch will forward this information to the multicast router, the router will send IGMP query information, if there is no other member in this group, the switch will delete this port from the group.

If enabling immediate leaving function on the receiving port, port will leave the group faster. If the immediate leaving function is not enabled yet, when the receiving port receives IGMP leaving information, the switch will forward router's IGMP query information and wait IGMP member report. If no report is received within the maximum query time, the member will be deleted from the group. If enabling the immediate leaving function, port member will be deleted as soon as it receives IGMP leaving information. This feature is normally used in the situation that one port is connected to only one user.

Multicast traffic will not be transmitted in all VLANs, but only need to be transmitted in multicast VLAN. Use can save much bandwidth in this way.

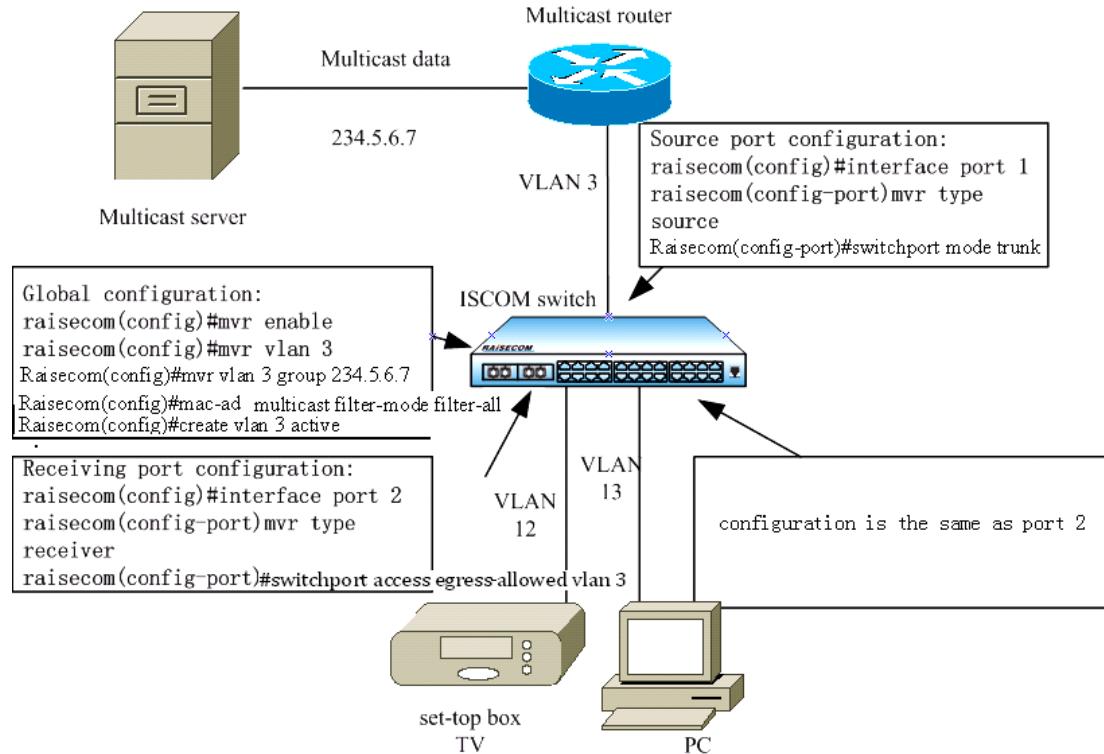


Fig 23-5 MVR application topology

IGMP filter under VLAN typical configuration example

The user under VLAN 12 can be able to receive IPTV program whose multicast address is from 234.5.6.7 to 234.5.6.46. However, the users under VLAN 13 do not pay, so the operator prohibited them to use these kinds of services. The configuration commands are as follows:

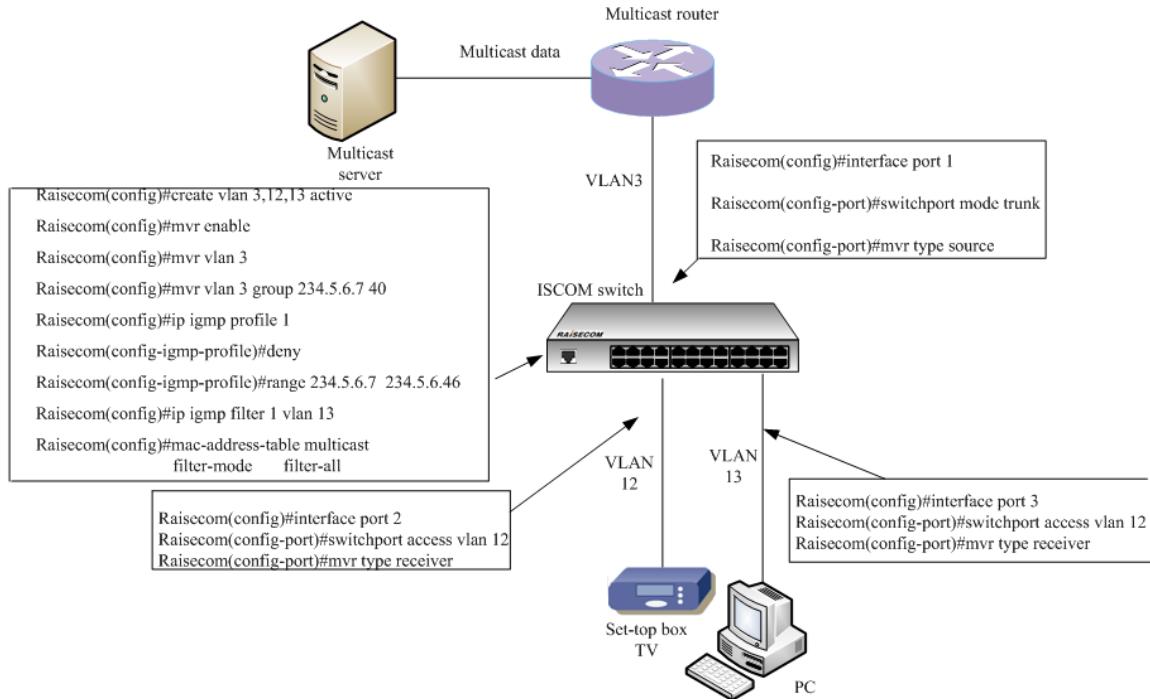


Fig 23-6 the IGMP filter application topology under VLAN

The IGMP filter under port typical configuration example

Enable IGMP filter on the switch, establish filter rule profile 1, and set address range from 234.5.6.7 to 234.5.6.10, the action is set to allow. According to the IGMP filter rule under port 2, PC and set-top box can both enter the multicast group 234.5.6.7, PC can join the multicast group 234.5.6.11 while set-top box can not. According to the maximum group limit of port 2, after set-top box enter 234.5.6.7, if it enter 234.5.6.8, it will quit from the multicast group 234.5.6.7 before.

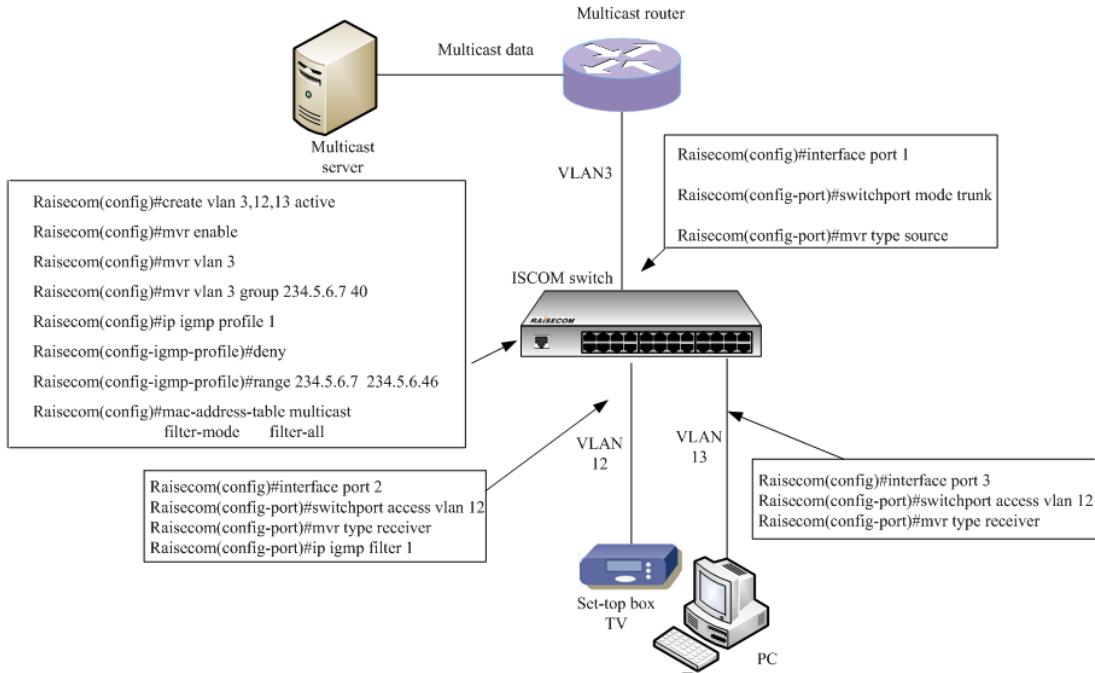


Fig 23-7 the IGMP filter application topology under port

23.3.8 MVR and IGMP filter trouble shooting

1. When configuring source port, it is not within multicast VLAN;
2. When configuring receives port, it is in multicast VLAN;
3. When configuring MVR group, the group addresses conflict because several IP multicast addresses suit one MAC multicast address;
4. When configuring stable group on the port, the address is not within MVR range;
5. In MVR compatible mode, configure stable multicast on source port.

Chapter 24 ACL Function Configuration

24.1 Configuration Description

This chapter is suit to configuration ACL function on the following devices: ISCOM2812f/2826/2826e/2828f/2852, ISCOM2128EA-MA/2924gf, ISCOM3012f/3026/3026e/3028f/3052, ISCOM2250.

24.2 ACL Introduction

In order to filter packets, network equipment needs to set a series of matching rules to identify the filtered objects. Only after this, user can allow or prohibit relative packets to pass through according to the designated strategy in advance. ACL (Access Control list) is used to realize these operations. ACL can be applied to VLAN, Layer-2 physical port and Layer-3 management interface. ACL makes classification to packets according to a series of matching conditions; these conditions can be packet source address, destination address and port number etc. It is combined with a series of judgment sentences. After activating a ACL, switch will check each received packet according to the judgment conditions, packets will be forwarded or dropped then according to these conditions. User can specify *permit* or *deny* while configuring ACLs. When it is set as *deny*, packets that are in accord with the rules will be dropped, the others will be forwarded; when it is set as *permit*, packets that are in accord with the rules will be forwarded, the others will be dropped.

24.3 IP ACL Configuration

Switch supports 400 IP access control lists at most with corresponding series number 0~399. It specifies classification rules according to the source IP address, destination IP address in the IP packet header, used TCP or UDP protocol port number and etc. packet attributes information, and then processes related operations to the packets according these rules. The construction of IP packet header can be referred to RFC791 and other related documents.

24.3.1 IP ACL Default Configuration

N/A

24.3.2 IP ACL Configuration

Steps	Command	Description
1	config	Entry into global configuration mode
2	ip-access-list <i>list-number</i> { <i>deny</i> / <i>permit</i> } <i>protocol</i> { <i>source-address mask</i> any }	ip-access-list configuration IP address access control list

	[source-protocol-port] {destination-address mask any} [destination-protocol-port]	<i>list-number</i> IP address access control list serial number, range from 0-399 deny permit represents reject/accept access. protocol binding protocol type.
		<i>source-address mask any</i> is source IP address with its mask, format is dotted decimal in the form of A.B.C.D, any indicates arbitrary address.
		<i>source-protocol-port</i> is source port for TCP/UDP protocol
		<i>destination -address mask any</i> is the destination address and its mask, the format is dotted decimal as A.B.C.D; any indicates arbitrary address.
		<i>destination -protocol-port</i> is the destination port of TCP/UPD.
3	exit	Exit global configuration mode and enter privileged EXEC mode
4	show ip-access-list <i>list-number</i>	Show IP access control list relevant information <i>list-number</i> is the series number for the IP access control list to be shown, rang is 0-399.
5	No ip-access-list <i>list-number</i>	Delete IP access control list <i>list-number</i> : the list series number to be deleted

24.3.3 Monitoring and Maintenance

Check and display indicated IP ACL command:

Command	Description
show ip-access-list [<i>{0-399}</i>] Show IP Access Control List	

24.3.4 Specific Configuration Example

➤ Destination

Configure source IP address as 192.168.1.0 segment, destination IP address as random address , protocol type as IP and access type as deny IP access rule;

Configure source IP address is 10.168.1.19; mask is 255.255.255.255; source protocol port is 80; destination address is random port; protocol type is TCP; visit type is deny IP access rule.

Configure source IP address is 10.168.1.19; mask is 255.255.255.255; destination address is 10.168.0.0 segment; protocol type is TCP; access type is permit's IP access rule.

➤ Set up Steps

Raisecom#config

Raisecom(config)#ip-access-list 0 deny ip 192.168.1.0 255.255.255.0 any

```
Raisecom(config)#ip-access-list 1 deny tcp 10.168.1.19 255.255.255.255 80 any
Raisecom(config)#ip-access-list 2 permit tcp 10.168.1.19 255.255.255.255 80 10.168.0.0
255.255.0.0 80
Raisecom(config)#exit
Raisecom#show ip-access-list
      Src Ip: Source Ip Address
      Dest Ip: Destination Ip Address
      List  Access   Protocol Ref. Src Ip:Port          Dest Ip:Port
      0    deny      IP      0    192.168.1.0:0          0.0.0.0:0
      1    deny      TCP     0    10.168.1.19:80        0.0.0.0:0
      2    permit     TCP     0    10.168.1.19:80        10.168.0.0:80
```

24.4 MAC ACL Function

Switch supports 400 digital-identified Layer-2 (MAC) access control lists at most with corresponding series number 0~399. Layer-2 access control list in conjunction with filter can process relevant operations to packets according to the source MAC address carried in Layer-2 frame, destination MAC address, source VLAN ID, Layer-2 protocol types and other Layer-2 information rules.

24.4.1 MAC ACL Default Configuration

Steps	Command	Description
1	config	Entry into global configuration mode
2	mac-access-list <i>list-number</i> {deny permit} [protocol / any] {source-MAC-address any} {destination-MAC-address / any}	MAC access control list configuration <i>list-number</i> access control list series number, range 0-399. <i>deny/permit</i> indicates deny/permit access [protocol any] indicates bonded protocol type, any indicates unrestricted protocol type. <i>source-MAC-address</i> indicates the source MAC address to be configured, format is hexadecimal string as “HHHH.HHHH.HHHH”, dotted every 4 characters; <i>any</i> indicates arbitrary source MAC address. <i>destination-MAC-address</i> is the destination MAC address to be configured, format is hexadecimal string as “HHHH.HHHH.HHHH”, dotted every 4 characters; <i>any</i> indicates arbitrary destination MAC address.
3	exit	Exit global configuration mode and enter privileged EXEC mode
4	show mac-access-list <i>list-number</i>	Show MAC access control list <i>list-number</i> is the series number for the MAC access

	control list to be shown, rang is 0-399.
5 no mac-access-list <i>list-number</i>	Delete configured MAC access control list <i>list-number</i> is the list series number to be deleted

24.4.2 Monitoring and Maintenance

Check and display indicated MAC ACL command:

Command	Description
show mac-access-list [{0-399}]	Display MAC access control list

24.4.3 Specific Configuration Examples

➤ Destination

Configure source MAC address as 1234.1234.1234; destination MAC address as 5678.5678.5678; protocol as IP; access type as deny's MAC access rule;

Configuration source MAC address as 1111.2222.3333; destination MAC address as 4444.5555.6666; protocol as ARP; access type as permit's MAC access rule.

➤ Set up Steps

Raisecom#config

Raisecom#config

Raisecom(config)# **mac-access-list** 0 **deny ip** 1234.1234.1234 5678.5678.5678

Raisecom(config)# **mac-access-list** 1 **permit arp** 1111.2222.3333 4444.5555.6666

Raisecom(config)#exit

Raisecom#**show mac-access-list**

Src Mac: Source MAC Address

Dest Mac: Destination MAC Address

List	Access	Protocol	Ref.	Src Mac	Dest Mac
0	deny	ip	0	1234.1234.1234	5678.5678.5678
1	permit	arp	0	1111.2222.3333	4444.5555.6666

24.5 MAP ACL Function

Switch supports 400 digital-identified access list maps at most with corresponding series number 0~399. Access list map can define more protocols and more detailed protocol character fields than IP access list and MAC access list, also can implement matching to any bytes in the first 64 bytes of Layer-2 frame according to user's definition before corresponding processing to the data packets from matched results. User needs to be familiar with Layer-2 data frame before using user-defined access list map.

Access list map uses command *match* to set the expected matching character field, no conflicts can exist in the same access list map when setting matching character field. Character fields that can be matched are shown below:

- Mac destination address
- Mac source address
- Ethernet protocol type
- CoS
- ARP protocol type
- Hardware address of ARP protocol sender
- Hardware address of ARP protocol receiver
- IP address of ARP protocol sender
- IP address of ARP protocol receiver
- IP protocol destination address
- IP protocol source address
- IP protocol priority
- IP protocol ToS
- IP protocol dscp
- IP protocol segmentation bit
- IP protocol type
- TCP protocol destination port
- TCP protocol source port
- TCP protocol bit
- UDP protocol destination port
- UDP protocol source port
- ICMP protocol information type
- ICMP protocol information code
- IGMP protocol information type

User can also use regular mask and offset to define any byte in the first 64 bytes in data frame, and then compare them with the user-defined rules to obtain the matched data frame, after this user can implement relevant operations. User-defined rules can be certain data fixed attributes, such as that in order to obtain all the TCP packets, user can define the rules as “06”, mask as “FF”, offset as “27”, by using such a method, regular rules and offsets can work together to pick up the segment of TCP protocol number in data frame, then compare it with defined rules to obtain all matched TCP packets.

Attention: Rules should be even hexadecimal, offset includes segment of 802.1Q VLAN TAG even if what the switch receives is untagged packet.

24.5.1 MAP ACL Default Configuration

24.5.2 MAP ACL Configuration

Steps	Command	Description
1	config	Entry into global configuration mode
2	access-list-map <i>list-number</i> { deny permit }	<i>list-number</i> : list serial number, from 0-399 <i>deny / permit</i> deny or permit data packets to go through when matching.
3	match mac { destination source } <i>HHHH.HHHH.HHHH</i>	<i>destination / source</i> match source mac or destination mac <i>HHHH.HHHH.HHHH</i> mac address
4	match cos <0-7>	<0-7> match cos value
5	match ethertype <i>HHHH [HHHH]</i>	<i>HHHH[HHHH]</i> match Ethernet type [mask]
6	match { <i>arp / eapol / flowcontrol / ip / ipv6 / loopback / mpls / mpls-mcast / pppoe / pppoedisc / x25 / x75</i> }	<i>arp</i> : match ARP protocol <i>eapol</i> : match eapol protocol

		<i>flowcontrol</i> : match flow control protocol
		<i>ip</i> : match ip protocol
		<i>ipv6</i> : match ipv6 protocol
		<i>loopback</i> : match loopback protocol
		<i>mpls</i> : matchmpls single cast protocol
		<i>mpls-mcast</i> : matchmpls group cast protocol
		<i>pppoe</i> : match pppoe protocol
		<i>pppoedisc</i> : match pppoe discover protocol
		<i>x25</i> : match x25 protocol
		<i>x75</i> : match x75 protocol
7	no match mac { <i>destination/source</i> }	Do not match MAC address <i>destination / source</i> : match source mac or destination mac
8	no match cos	Do not match CoS value
9	no match ethertype	Do not match Ethernet type
10	match arp opcode { <i>request /reply</i> }	Match arp protocol type <i>request / reply</i> arpprotocol reply /request packet
11	match arp { <i>sender-mac / target-mac</i> <i>HHHH.HHHH.HHHH</i> }	Match arp protocol hardware address <i>sender-mac/ target-mac</i> : match arp sender/target mac address <i>HHHH.HHHH.HHHH</i> : MAC address
12	match arp { <i>sender-ip / target-ip</i> <i>A.B.C.D [A.B.C.D]</i> }	Match arp protocol IP address <i>sender-ip / target-ip</i> sender/target: IPaddress <i>A.B.C.D [A.B.C.D]</i> : Ip address [mask]
13	no match arp opcode	do not matcharp protocol type
14	no match arp { <i>sender-mac / target-mac</i> }	do not match arp protocol hardware address
15	no match arp { <i>sender-ip / target-ip</i> }	do not matcharp protocol IPaddress <i>sender-ip/ target-ip</i> sender/target IP address
16	match ip { <i>destination-address / source-address</i> } <i>A.B.C.D [A.B.C.D]</i>	Match IP protocol address <i>destination-address / source-address</i> Ip protocol destination/source address <i>A.B.C.D [A.B.C.D]</i> IP address [mask]
17	match ip precedence {<0-7>/ <i>routine/priority/immediate/flash/</i> <i>flash-override/critical/internet/network</i> }	Match IP priority <0-7>: IP priority value <i>routine</i> : IP priority value 0 <i>priority</i> : IP priority value 1 <i>immediate</i> : IP priority value 2 <i>flash</i> : IP priority value 3 <i>flash-override</i> : IP priority value 4 <i>critical</i> : IP priority value 5

- 18 `match ip ToS {<0-15> / normal / min-monetary-cost / min-delay / max-reliability / max-throughput}`**
- internet:* IP priority value 6
network: IP priority value 7
ToS value: Match IP priority ToS value
<0-15>: ToS value
normal: normal ToS value (0)
min-monetary-cost: Min monetary cost ToS value(1)
min-delay: Min delay ToS value(8)
max-reliability: Max reliability ToS value(2)
max-throughput: Max throughput ToS value(4)
- 19 `match ip dscp {<0-63> / af11 / af12 / af13 / af21 / af22 / af23 / af31 / af32 / af33 / af41 / af42 / af43 / cs1 / cs2 / cs3 / cs4 / cs5 / cs6 / cs7 / ef / default}`**
- Match IP DSCP value
<0-63>: IP DSCP value
af11: AF11 DSCP value(001010)
af12: AF12 DSCP value(001100)
af13: AF13 DSCP value(001110)
af21: AF21 DSCP value(010010)
af22: AF22 DSCP value(010100)
af23: AF23 DSCP value(010110)
af31: AF31 DSCP value(011010)
af32: AF32 DSCP value(011100)
af33: AF33 DSCP value(011110)
af41: AF41 DSCP value(100010)
af42: AF42 DSCP value(100100)
af43: AF43 DSCP value(100110)
cs1: CS1(priority 1) DSCP value(001000)
cs2: CS2(priority 2) DSCP value(010000)
cs3: CS3(priority 3) DSCP value(011000)
cs4: CS4(priority 4) DSCP value(100000)
cs5: CS5(priority 5) DSCP value(101000)
cs6: CS6(priority 6) DSCP value(110000)
cs7: CS7(priority 7) DSCP value(111000)
default: Default DSCP value(000000)
ef: EF DSCP value(101110)
- 20 `match ip no-fragments`**
- Match no-fragment IP packet
- 21 `match ip protocol <0-255>`**
- Match IP protocol value
<0-255>: IP protocol type value
- 22 `match ip { ahp /esp/gre/icmp/igmp/igrp /ipinip/ospf/pcp/pim/tcp/udp}`**
- Match IP protocol value
ahp: autherize header protocol
esp: encapsulation security payload protocol
gre: General routing encapsulation protocol

		<i>icmp</i> : Internet control message protocol <i>igmp</i> : Internet group message protocol <i>igrp</i> : Interior gateway routing protocol <i>ipinip</i> : IP-in-IP tunnel <i>ospf</i> : Open shortest path first <i>pcp</i> : Payload compression protocol <i>pim</i> : protocol independent multicast protocol <i>tcp</i> : Transmission control protocol <i>udp</i> : user datagram protocol
23	no match ip {destination-address / source-address}	Do not match IP protocol address <i>destination-address</i> / <i>source-address</i> : IP protocol destination/source address
24	no match ip precedence	do not match IP priority
25	no match ip ToS	do not match IP ToS value
26	no match ip dscp	do not match IP DSCP value
27	no match ip no-fragments	do not match IP no-fragment
28	no match ip protocol	do not match IP protocol value
29	match ip tcp { destination-port / source-port} {<0-65535> / bgp / domain / echo / exec / finger / ftp / ftp-data / gopher / hostname / ident / irc / klogin / kshell / login / lpd / nntp / pim-auto-rp / pop2 / pop3 / smtp / sunrpc / syslog / tacacs / talk / telnet / time / uucp / whois / www}	Match Tcp protocol port number <i>destination-port</i> / <i>source-port</i> : TCP protocol destination/source port <0-65535>: tcp port number <i>bgp</i> : border gateway protocol (179) <i>domain</i> : domain name service protocol (53) <i>echo</i> : echo protocol (7) <i>exec</i> : Exec (rsh, 512) <i>finger</i> : Finger (79) <i>ftp</i> : File transfer protocol (21) <i>ftp-data</i> : FTP data connections (20) <i>gopher</i> : Gopher (70) <i>hostname</i> : NIC hostname server (101) <i>ident</i> : identify protocol (113) <i>irc</i> : Internet Relay Chat protocol (194) <i>klogin</i> : Kerberos login (543) <i>kshell</i> : Kerberos shell (544) <i>login</i> : Login (rlogin, 513) <i>lpd</i> : Printer Service protocol(515) <i>nntp</i> : network news transport protocol <i>pim-auto-rp</i> : PIM Auto-RP (496) <i>pop2</i> : post office protocol v2 (109) <i>pop3</i> : post office protocol v3 (110)

		<i>smtp</i> : simple mail transport protocol (25)
		<i>sunrpc</i> : Sun Remote Procedure Call (111)
		<i>syslog</i> : System log (514)
		<i>tacacs</i> : TAC access control system (49)
		<i>talk</i> : Talk (517)
		<i>telnet</i> : Telnet (23)
		<i>time</i> : Time (37)
		<i>uucp</i> : Unix-to-Unix Copy program (540)
		<i>whois</i> : Nicname(43)
		<i>www</i> : World Wide Web (HTTP, 80)
30	match ip tcp {<i>ack</i> / <i>fin</i> / <i>psh</i> / <i>rst</i> / <i>syn</i> / <i>urg</i> }	Match TCP protocol bit <i>ack</i> : match ACK bit <i>fin</i> : matchFIN bit <i>psh</i> : matchPSH bit <i>rst</i> : matchRST bit <i>syn</i> : matchSYN bit <i>urg</i> : matchURG bit
31	no match ip tcp { <i>destination-port</i> / <i>source-port</i> }	do not match Tcp protocol port number <i>destination-port</i> / <i>source-port</i> : TCP protocol destination/source port
32	no match ip tcp {<i>ack</i> / <i>fin</i> / <i>psh</i> / <i>rst</i> / <i>syn</i> / <i>urg</i> }	do not match TCP protocol bit <i>ack</i> : match ACK bit <i>fin</i> : match FIN bit <i>psh</i> : match PSH bit <i>rst</i> : match RST bit <i>syn</i> : match SYN bit <i>urg</i> : match URG bit
33	match ip udp { <i>destination-port</i> / <i>source-port</i> } {<0-65535>} / <i>biff</i> / <i>bootpc</i> / <i>bootps</i> / <i>domain</i> / <i>echo</i> / <i>mobile-ip</i> / <i>netbios-dgm</i> / <i>netbios-ns</i> / <i>netbios-ss</i> / <i>ntp</i> / <i>pim-auto-rp</i> / <i>rip</i> / <i>snmp</i> / <i>snmptrap</i> / <i>sunrpc</i> / <i>syslog</i> / <i>tacacs</i> / <i>talk</i> / <i>tftp</i> / <i>time</i> / <i>who</i> }	Match udp protocol port number <i>destination-port</i> / <i>source-port</i> : TCP protocol destination/source port <0-65535>: udp port number <i>biff</i> : Biff (mail notification, comsat, 512) <i>bootpc</i> : bootstrap protocol (BOOTP) client (68) <i>bootps</i> : bootstrap protocol(BOOTP) server (67) <i>domain</i> : domain name service protocol (53) <i>echo</i> : echo protocol (7) <i>mobile-ip</i> : mobile IP registration (434) <i>netbios-dgm</i> : NetBios datagram eservic (138) <i>netbios-ns</i> : NetBios name service (137)

		<i>netbios-ss</i> : NetBios session service (139)
		<i>ntp</i> : network time protocol(123)
		<i>pim-auto-rp</i> : PIM Auto-RP (496)
		<i>rip</i> : routing information protocol(520)
		<i>snmp</i> : simple network magagement protocol(161)
		<i>snmptrap</i> : SNMP Traps (162)
		<i>sunrpc</i> : Sun remote procedure call (111)
		<i>syslog</i> : system log (514)
		<i>tacacs</i> : TAC access control system (49)
		<i>talk</i> : talk (517)
		<i>tftp</i> : trivial file transfer protocol(69)
		<i>time</i> : Time (37)
		<i>who</i> : Who service (rwho, 513)
34	no match ip udp { <i>destination-port / source-port</i> }	do not match udp protocol port number <i>destination-port / source-port</i> : TCP protocol destination/sourceport
35	match ip icmp <0-255> [<0-255>]	Match icmp protocol information type <0-255> [<0-255>]: information type[information code]
36	match ip igmp {<0-255> <i>dvmrp / query / leave-v2 / report-v1 / report-v2 /report-v3 / pim-v1</i> }	Match igmp protocol information type <0-255>: IGMP information type <i>dvmrp</i> : Distance Vector Multicast Routing Protocol <i>leave-v2</i> : IGMPv2 leave group <i>pim-v1</i> : protocol Independent Multicast version 1 <i>query</i> : IGMP member query <i>report-v1</i> : IGMPv1 member report <i>report-v2</i> : IGMPv2 member report <i>report-v3</i> : IGMPv3 member report
37	match user-define <i>rule-string rule-mask <0-64></i>	Match user-defined segment <i>rule-string</i> : user-defined regular string, must be combined of hexadecimal, no more than 64 bytes. <i>rule-mask</i> : mask rule, used to implement “or” operation with data packet <0-64>: offset, based on dataframe header, and implement “or” operation from the beginning of specified bytes
38	no match user-define	do not match user-defined segment
39	exit	Exit global configuration mode and enter privileged EXEC mode

40	show access-list-map [list-number]	Show port <i>access-list-map</i> <i>list-number</i> is the port access-list-map series number to show, range is 0-399
41	no access-list-map list-number	Delete user-defined access-list-map <i>list-number</i> is the list number to delete

24.5.3 Monitoring and Maintenance

Check and display indicated access control list command:

Command	Description
show access-list-map [/0-399]	Display access control list map list

24.5.4 Specific Configuration Example

➤ Destination

To filter bytes 123456 from the 40th bytes in the data frame, access type is “deny”. ARP protocol request packet is filtered.

➤ Set up Steps

Raisecom#**config**

```
Raisecom(config)#access-list-map 0 deny
Raisecom(config-aclmap)#match user-define 123456 ffffff 40
Raisecom(config-aclmap)#exit
Raisecom(config)#access-list-map 1 permit
Raisecom(config-aclmap)# match arp opcode request
Raisecom(config-aclmap)#exit
Raisecom(config)#exit
Raisecom#show access-list-map
access-list-map 0 deny
Match user-define 123456 ffffff 40
access-list-map 1 permit
Match arp Opcode request
```

24.6 Application Configuration Based on Hardware ACL

3 steps for using ACL on Layer-2 physical port or VLAN are as follows:

1. Define ACL

Described in section 1.4.

2. Configuration Filter

After setting up ACL, you need to set the filter. Whether the filter is configured successfully depends on if the global status is enabled or not. You can use specific commands to make ACLs effective or to delete the filters that are already take effects. You can user command **no filter** to disable the related rules, if rules have been written in hardware, they will be deleted from the hardware and configurations.

In a physical port or VLAN filter rule can be composed by multi “permit/deny” statements and every statement indicated different size range of data packet. There is a problem of match order while a data packet and access control rule are matching. The match order of access control rule depends on configuration filter rule’s order. The later the order, the higher the priority. If there is conflicts in the rules, high priority will be followed.

There are four kinds of configurations: one is based on switch, one is based on port, on is based from ingress port to egress port, one is based on VLAN. For the filtering rules based on port, you have two options, one of which is based on flow ingress with the other one based on flow egress.

3. Simulate Filter

Use filter command to make the access control rule effect or no effect. Default status is no effect. Once command is configured as effect, not only the earlier configuration filter rules will be effect, but also the later configuration filter rule will effect as well.

24.6.1 Application Default Configuration Based on Hardware ACL

1. Application based on switch

Steps	Command	Description
1	config	Entry into global configuration mode
2	[no] filter (ip-access-list / mac-access-list / access-list-map) {acclist / all}	ip-access-list indicates that the filter uses IP access list mac-access-list indicates that the filter uses MAC access list access-list-map indicates that the filter uses user-defined access list map acclist / all access control list series number, all means all the configured access control lists
3	filter (enable / disable)	enable: filter function effect enable disable: filter function effect disable
4	exit	Exit global configuration mode and enter privileged EXEC mode
5	show filter	Show all filter status

2. Application based on port

Steps	Command	Description
1	config	Entry into global configuration mode
2	[no] filter (ip-access-list 	Set filter based on port

	mac-access-list access-list-map) {aclist / all} {ingress / egress }	ip-access-list indicates that the filter uses IP access list mac-access-list indicates that the filter uses MAC access list access-list-map indicates that the filter uses user-defined access list map
	port-list {portlist }	acllist all access control list series number, all means all the configured access control lists ingress egress means to carry out the filtering on ingress egress
3	filter (enable / disable)	port-list the filter is applied to port portlist Phisical port list range enable filter function effect enable disable filter function effect disable
4	exit	Exit global configuration mode and enter privileged EXEC mode
5	show filter	Show all filter status

3. Based from ingress port to egress port

Steps	Command	Description
1	config	Entry into global configuration mode
2	[no] filter (ip-access-list mac-access-list access-list-map) {all/ aclist} from ingress-port to egress-port	ip-access-list indicates that the filter uses IP access list mac-access-list indicates that the filter uses MAC access list access-list-map indicates that the filter uses user-defined access list map acllist all access control list series number, all means all the configured access control lists from to directions ingress-port : ingress port egress-port : egress port
3	filter (enable disable)	enable : filter function effect enable disable : filter function effect disable
4	exit	Exit global configuration mode and enter privileged EXEC mode
5	show filter	Show all filter status

4. Application based on VLAN

Steps	Command	Description
-------	---------	-------------

1	config	Entry into global configuration mode
2	[no] filter (ip-access-list mac-access-list access-list-map) {all/ aclist} vlan vlanid	Set the filter based on VLAN ip-access-list indicates that the filter uses IP access list mac-access-list indicates that the filter uses MAC access list access-list-map indicates that the filter uses user-defined access list map aclist all access control list series number, all means all the configured access control lists Vlan the filter is applied to VLAN vlanid VLAN ID
3	filter (enable disable)	enable filter function effect enable disable filter function effect disable
4	exit	Exit global configuration mode and enter privileged EXEC mode
5	show filter	Show all filter status

24.6.2 Monitoring and Maintenance

Check and display all configuration filter status command:

Command	Description
show filter	Display all configuration filter status

24.6.3 Specific Configuration Examples

Example 1:

- Destination

The switch does not allow TCP packet to pass through with destination port 80

- Set up steps

Raisecom#**config**

```
Raisecom(config)# ip-access-list 0 deny tcp any any 80
Raisecom(config)# filter ip-access-list 0
```

```
Raisecom(config)#filter enable
```

```
Raisecom(config)#exit
```

Example 2:

- Destination

The switch does not allow ARP packets with the MAC address 000e.3842.34ea to pass through on port 2 to 8.

- Set up Steps

Raisecom#**config**

```
Raisecom(config)# mac-access-list 2 deny arp any 000e.3842.34ea
Raisecom(config)# filter mac-access-list 2 ingress portlist 2-8
Raisecom(config)#filter enable
Raisecom(config)#exit
```

Example 3:

➤ Destination

The switch allows IP packets with the source address in network segment 10.0.0.0/8 to pass through in VLAN 3

➤ Set up Steps

Raisecom#**config**

```
Raisecom(config)# ip-access-list 2 deny ip any any
Raisecom(config)# ip-access-list 3 permit ip 10.0.0.0 255.0.0.0 any
Raisecom(config)# filter ip-access-list 2,3 vlan 3
Raisecom(config)#filter enable
Raisecom(config)#exit
```

24.7 Configuration Function Based on Software IP ACL

The steps below show how to use software IP ACL on Layer-3 interface:

1) Define access control list

Show in section 1.2

2) ACL Configuration

Filtering rules on a Layer-3 interface can be combined of one or multiple “permit | deny” sentences, every sentence has different specified packet ranges, so matching order problem may happen when matching one packet and ACL rule. The matching order depends on the orders of configured filtering rules, as the order closer to the back, the higher the priority will be. When conflict happens, high priority will be the benchmark.

24.7.1 Layer-3 Interface Protect Configuration Based on IP ACL

Steps	Command	Description
1	config	Entry into global configuration mode
2	interface ip <0-14>	Enter Layer-3 interface configuration mode
3	[no] ip ip-access-list {all/ acclist}	Set Layer-3 interface filter ip-access-list indicates that the filter uses IP access list

		acllist all access control list series number, all means all the configured access control lists
4	exit	Exit Ethernet Layer-3 interface configuration mode and enter global configuration mode
5	exit	Exit global configuration mode and enter privileged EXEC mode
6	show interface ip ip-access-list	Show filters status for all interfaces

24.7.2 Monitoring and Maintenance

Check and display configuration filter status command:

Command	Description
show interface ip ip-access-list	Show all filters status for Layer-3 interface

24.7.3 Specific Configuration Example

Example 1:

➤ Destination

Switch only allow IP packet with 10.0.0.0/8 access

➤ Set up steps

Raisecom#**config**

Raisecom(config)# **ip-access-list 2 deny ip any any**

Raisecom(config)# **ip-access-list 3 permit ip 10.0.0.0 255.0.0.0 any**

Raisecom(config)#**interface ip 0**

Raisecom(config-ip)# **ip ip-access-list 2,3**

Raisecom(config-ip)#**exit**

Raisecom(config)#**exit**

Chapter 25 QoS Configuration

This chapter describes the function of ISCOM series of switches and how to configure QoS. By using the QoS features, it can achieve on a particular type of flow control, it provides service guarantee quality for the business and user.

25.1 Configuration Description

To guide the user to configuration QoS function except for Policy and class function; to guide the user to configuration most QoS function on the most Switch device. User can look up the QoS function command one to the QoS function command nine to see the details.

25.2 QoS Introduction

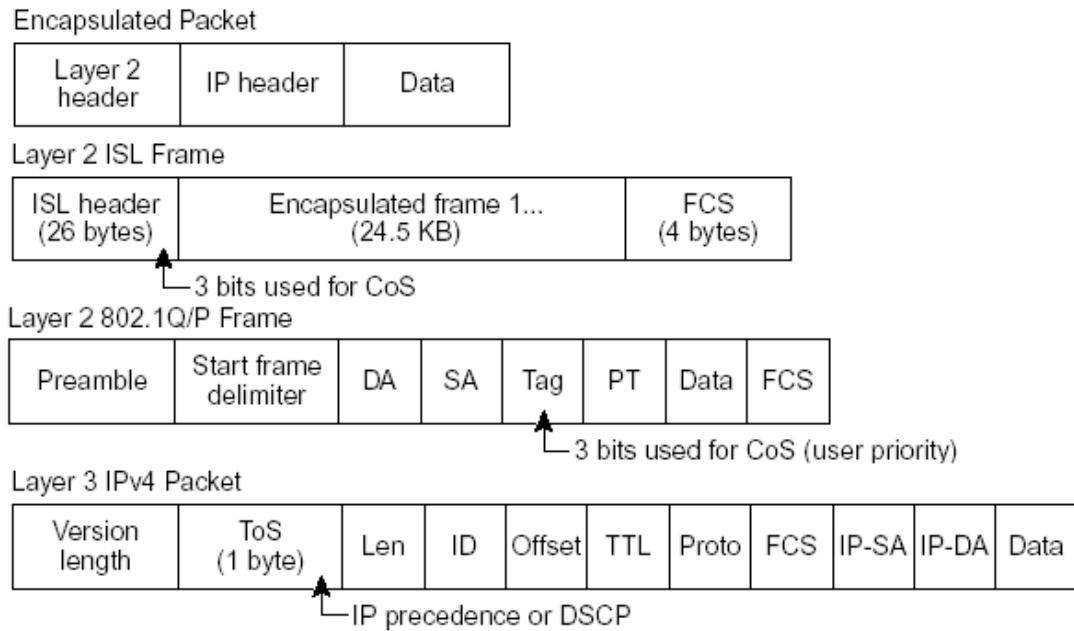
25.2.1 Introduction

Generally speaking, Internet (Ipv4 standard) provides users only “best effort” service, cannot guarantee a real-time and complete packets transmission, and the quality of services either. Since user always has different requirements for the transmission quality of separate multi-media applications, network resources should be redistributed and scheduled according to user’s demands. By using network quality of service, user is able to process specific data traffic with higher priority, or applies particular management schedule strategy to make the network more predictable and the bandwidth management more effective.

1. QoS Basis

ISCOM2800 mechanism realizes layer-2 packets classification based on 802.1P and 802.1Q standards. 802.1Q defines VLAN, though QoS is not defined in this standard, the given mechanism which mention than the frame precedence can be modified configures a strong groundwork to realize QoS. 802.1P standard defines priority mechanism. If packets with high priority have not been transmitted, packets with low priority will not be transmitted.

In Layer-2 802.1Q frame header, there are 2 bytes of TAG control information string, the first 3 bits carry CoS (Class of Service) value, the values is from 0 to 7, shown in the figure below:



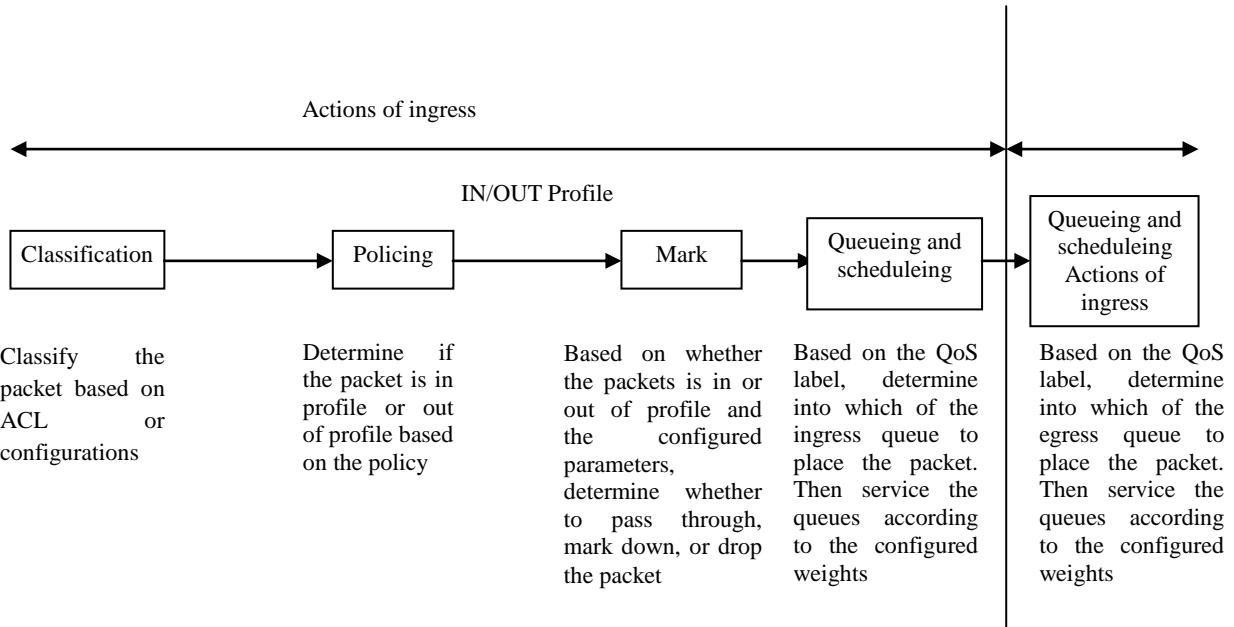
The 8 priority defined by CoS can be considered as the following 8 kinds of packets: Priority		Message type	Application
000	Routine	Level 0 corresponds to the default of the best efforts of the information delivery	
001	Priority		
010	Intermediate		
011	Flash	Level 1 - 4 are corresponds for the definition of multi-media data or important enterprise data.	
100	Flash Override		
101	Critical		
110	Internet Control	Level 5 or 6 is used in the sensitive-delay inter-act video/audio data	
111	Network Control	Level 7 is applied for the important high-level network data stream, such as routing information	

2. QoS basic mode

- Actions at ingress ports include traffic classification, policing and marking:
 - Classifying: to classify the traffic. This process generates an inner DSCP to identify the data's QoS characteristics.
 - Policing: Comparing inner DSCP and configured policies to determine whether the packet goes into the policy profile or out. Policy limits the occupied bandwidth. The results will be sent to marker.
 - Marking: Evaluates the policy and configuration information for the action to be taken when a packet is out of profile and determines what to do with the packet (pass through a packet without modification, mark down the QoS label in the packet, or drop the packet).
- Actions at the egress port include queueing and scheduling:
 - Queueing: evaluates the QoS packet label and the corresponding DSCP before selecting which queues to use. The DSCP value is mapped to an inner CoS value for the selection of an output queue.
 - Scheduling: based on configured WRR (Weighted round robin) and threshold to provide

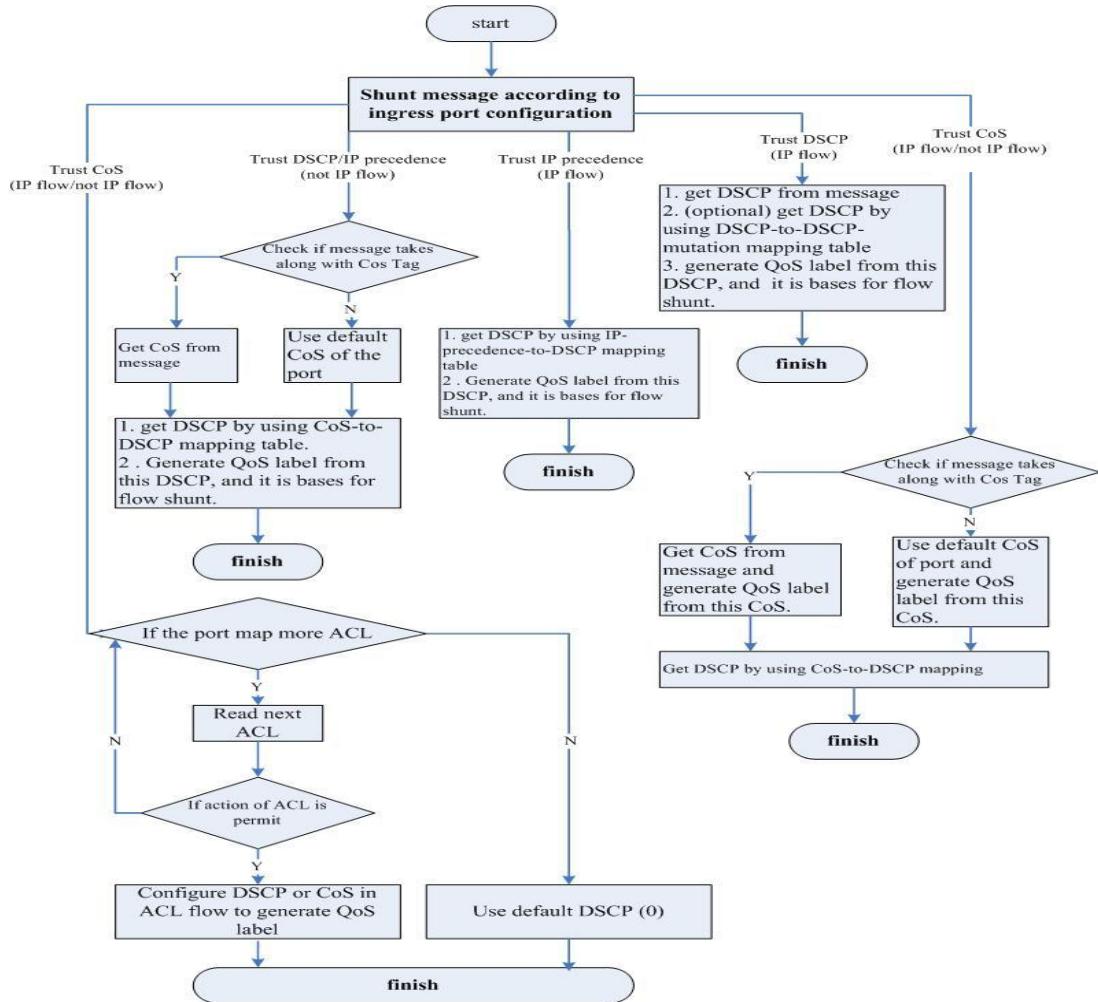
service for output queue.

- The figure below shows the QoS basic model:



25.2.2 Classification

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet. Classification works only when the global QoS function is enabled. QoS is disabled by default. You specify which fields in the frame or packet that you want to use to classify incoming traffic.



Description: For none-IP traffic, the classification procedure is as follows:

- Use port default value: if the data frame does not have CoS value, assign the incoming frame with the port default Cos value, and then use CoS-to-DSCP map to generate inner DSCP value.
- TRUST the CoS value of input frame (configure the port as TRUST COS): use configurable CoS-to-DSCP mapping table to generate inner DSCP value. For none-IP traffic, whether to configure it as DSCP TRUST and IP precedence TRUST is meaningless, system will use port default CoS value.
- Based on configured Layer-2 MAC ACL classification, check the source MAC, destination MAC and Ethernet field. If there is no configured ACL, assign the default DSCP value as 0. Otherwise, assign DSCP value to the incoming frame based on policy mapping table.
- ✓ For IP traffic:
 - TRUST IP DSCP value of incoming packets (configure the port as TRUST DSCP): use DSCP of IP packets as the inner DSCP value. You can use DSCP-to-DSCP mapping table to modify the DSCP value if the port is edge port of two QoS domains.
 - TRUST IP precedence of incoming packet (configure the port as TRUST IP precedence): use IP-precedence-to-DSCP mapping table to generate DSCP value.
 - TRUST CoS value of incoming packets: use CoS-to-DSCP mapping table to generate DSCP value.
 - Based on configured IP ACL for classification, check every field in IP packet header. If no ACL is configured, assign the default DSCP value as 0 to the packet. Otherwise, to assign DSCP value to the packet according to policy map.

As described in the diagram, not only we can classify the traffic by different traffic configuration port “TRUST”, and the message CoS, DSCP, IP-precedence; but also we can classify the traffic more flexible by the ACL function, class-map.

Attention: The use of two classification ways are mutually exclusive and later configuration will take effects.

Class-map mechanism describe data flow classification on ACL:

1. Classification based on QoS ACL:

- 1) If a matched permit ACL (the first one) is found, related QoS actions will be activated.
- 2) If a matched deny ACL is found, ignore this one, and go on to the next one.
- 3) If all ACLs are checked but no matched permit ACL, packet will not be processed.
- 4) When matching multiple ACLs, implement QoS processing as the first permit ACL is found.
- 5) After defining an ACL classification, user can bond it to a policy. Policies include class classification (such as aggregation) or rate limiting, bond the policy to a port before taking effects.

2. Classification based on class-map:

A class map is a mechanism that you use to isolate and name a specific traffic flow (or class) from all other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it:

- 1) by ACL match
- 2) by DCSP, IP priority match.

25.2.3 Policy and Marking

1. Policy map

Each policy may have a lot of class-maps, to identify those flow movements.

2. Policy action

In each policy, different actions identify different flow movements. So far, there are 6 actions:

- TRUST: the TRUST status of flow as TRUST CoS, DSCP and ToS;
- Set: modify the data packets of flow into new value include CoS, DSCP, ToS;
- Policy: limit the speed of streams and modify them, also notice what actions are going to use if the flow is over speed limit.
- Set VLAN: VLAN coverage.
- Re-direct to port: redirect message.
- Copy-to-mirror: flow image.

3. Policy Application

A policy mapping is needed to binding on the IN/OUT port to be effective.

25.2.4 Bit-Rate Limitation and Reshaping

QoS uses policy for speed limiting and reshaping, also modify the DSCP data packet or byte losing.

1. Three types of policy:

single-policy: each rule of class-map is using this policy individually.

class-policy: all rules of each class-map are sharing this policy.

aggregate-policy: all class-map of one policy-map are sharing this policy.

If the flow bit rate is out profile, each policy will have two actions: either drop or marked down DSCP value.

2. Policy uses token bucket algorithm

When the switch receives a frame, a token will be added on the bucket. According to the indicated average bit rate, each token is added on the bucket after the switch checked the available space on the bucket. If not, the packet will be marked as nonconforming, then follow the policy actions (drop or modify). Moreover, burst will cause the actions as well.

25.2.5 Mapping Table

During QoS processing, switch describes the inner DSCP precedence for all traffics:

- During the classification procedure, QoS use configured map table (CoS-to-DSCP、IP-precedence-to-DSCP), based on the CoS or IP precedence value in the incoming packet to obtain an inner DSCP value; To configure DSCP TRUST status on port, if the DSCP values are different in the two QoS domains, use can use DSCP-to-DSCP-mutation map to modify DSCP value.
- During the policing procedure, QoS can assign new DSCP values to IP or non-ip packets (if the packet is out of profile and the policy has indicated mark down action), this map is called policed-DSCP mapping.
- Before traffics go into the scheduling, QoS use DSCP-to-CoS map to obtain CoS value according to inner DSCP value, and then use CoS-to-egress-queue map to select the egress queuing.

Attention: If the map table of DSCP-to-DSCP-mutation and policed-DSCP is empty, the default will be the DSCP value of incoming packet;

DSCP-to-DSCP-mutation mapping table is applied for the port, other mapping tables are applied for the switch.

25.2.6 Queueing and Scheduling

Queueing and scheduling will be carried out for packets processing after policing and marking. ISCOM switch realizes two kinds of processing according to different classified packets:

- Regenerate packet COS value according to the defined rules while maintaining the packet's native COS value
- The policy is effective only when the rules are configured as relying on TOS value, that is to say: modify the packet's native COS value according to TOS value.

ISCOM series switches support 4 kinds of priority output queues, the priority values are 0-3. The highest priority is level 3; the switch also supports 3 kinds of queue scheduling policies: strict priority scheduling, control forward weight scheduling and control forward delay scheduling.

ISCOM series switches also support the processing of untagged Layer-2 frame. Every port has default priority which is COS value. When the port receives an untagged packet, the switch will consider the port default priority as the packet's COS value for queue dispatching and scheduling. After the packet goes out of the switch, it will Renew to the original format.

25.2.7 QoS Default Configuration

Step	Attribute	Default configuration
1	QoS enable	Disable
2	Global QoS Trust Status	UNTRUST
3	Port QoS Trust Status	UNTRUST
4	Port Default CoS	0
5	Port Default DSCP	0
6	Port Default CoS override	Disable
7	Port Default DSCP override	Disable
8	class-map match type	match-all
9	Policy Trust Status	DSCP
10	Queue scheduling policy	Strict priority secheduling SP

CoS-DSCP default map:

CoS	0	1	2	3	4	5	6	7
DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

IP-Precedence-DSCP default map:

ToS	0	1	2	3	4	5	6	7
DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

DSCP-CoS default map:

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS	0	1	2	3	4	5	6	7

DSCP-to-DSCP-Mutation default map(default-dscp):

DSCP	0	1	2	3	4	5	6	7
0	8	9	10	11	12	13	14	15
1	16	17	18	19	20	21	22	23
2	24	25	26	27	28	29	30	31
3	32	33	34	35	36	37	38	39
5	40	41	42	43	44	45	46	47
6	48	49	50	51	52	53	54	55
7	56	57	58	59	60	61	62	63

Inner CoS to queue map:

Inner CoS value	0	1	2	3	4	5	6	7
-----------------	---	---	---	---	---	---	---	---

Queue ID	1	1	2	2	3	3	4	4
----------	---	---	---	---	---	---	---	---

25.3 QoS Enable and Disable

25.3.1 QoS Start and Stop Default Configuration

No.	Attributes	Default configuration
1	QoS start	Disable

25.3.2 QoS Start and Close Default Configuration

Under the default situation, QoS is disabled. Use the command below to enable QoS function under global configuration mode.

Step	Command	Description
1	config	Enter global configuration mode
2	mls qos	Enable QoS
3	exit	Back to privileged EXEC mode
4	show mls qos	Show QoS configuration status

In order to disable QoS, implement command **no mls qos**.

Before enabling QoS, some functions are still effective, such as port default CoS, port default DSCP, queue scheduling mode, CoS to queue map and so on. Users are suggested to disable the flow control function before enabling QoS.

25.3.3 Monitoring and Maintenance

Command	Description
show mls qos	Show QoS switch status

25.3.4 Configuration Examples

Open QoS function:

```
Raisecom#config
```

```
Raisecom(config)#mls qos
```

```
Raisecom#show mls qos
```

Show as below:

QoS is enabled.

25.4 Classification Function Configuration

25.4.1 Classification Default Configuration

Function	Default Value
Global QoS TRUST status	UNTRUST
Port QoS TRUST status	UNTRUST
Port default CoS	0
Port default DSCP	0
Port default CoS override	Disable
Port default DSCP override	Disable
Class-mapbmatch type	match-all

25.4.2 Flow Classification Configuration Based on Port TRUST Status

Attention:

- Port TRUST status and ACL/Class-map flow classification are mutually exclusive, and later configuration will take effects.
- Global and port QoS TRUST status configurations are used for different devices. So far, it is not capable for those two configurations in one equipment.
- QoS TRUST status configuration and TRUST policy status configuration are mutually exclusive, and later configuration will take effects.

Configuring Global QoS TRUST status

Configure QoS TRUST status for all ports. Reverse command: **no mls qos TRUST**.

Steps	Command	Description
1	Config	Entry to global configuration mode
2	mls qos TRUST [cos / dscp / port-priority]	All QoS TRUST status ports configuration cos: configuration the switch as TRUST CoS status dscp: configuration the switch as TRUST DSCP status port-priority: configuration the switch as TRUST IP priority status.
3	Exit	Return to privileges mode
4	show mls qos port	Show QoS port configuration

Configuration example:

```
Raisecom#config
Raisecom(config)#mls qos TRUST cos //configure port TRUST status
Raisecom(config)#exit
Raisecom# show mls qos port
```

Show results as:

<i>TRUST state: TRUST CoS</i>	
<i>Port Id</i>	<i>Default CoS</i>
1	0
2	0
.....	

Configuring QoS port TRUST status

Configure QoS port TRUST status. In default situation, the switch TRUST status is UNTRUST. Reverse Command is: **no mls qos TRUST**.

Steps	Command	Description
1	config	Entry to global configuration mode
2	interface port <i>portid</i>	Entry to port configuration mode
3	mls qos TRUST [cos / dscp]	Set QoS TRUST mode cos: set port as TRUST CoS status dscp: set port as TRUST DSCP status
4	Exit	Return to global configuration mode
5	Exit	Return privileges mode
6	Show mls qos port <i>portid</i>	Show QoS port configuration

Configuring CoS port default

Only if the port TRUST status is CoS, configuring default CoS takes effects. When the message is untag, CoS default port as CoS value. In default situation, that value will be 0. Reverse command: **no mls qos default-cos**. It can be set under port mode.

Steps	Command	Description
1	config	Entry to global configuration mode
2	interface port <i>portid</i>	Entry to port configuration mode
3	mls qos default-cos override	Set default CoS value CoS-value: set default port CoS value 0-7
4	Exit	Return to global configuration mode
5	Exit	Return to privileges mode
6	Show mls qos port <i>portid</i>	Show QoS port configuration

Configuration example: in Port 1, configure TRUST status as CoS, and when the incoming message is as untag, the CoS value will be 2.

Raisecom#**config**

Raisecom(config)#**inter port 1**

Raisecom(config-port)#**mls qos TRUST cos** //configure port TRUST status

Raisecom(config-port)# **mls qos default-cos 2** //configure CoS port default

```
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom# show mls qos port 1
```

Show results as:

```
Raisecom#sh mls qos port 1
Port 1:
TRUST state: TRUST CoS
Default CoS: 2
Default DSCP: 0
DSCP override: Disable
DSCP mutation map: default-dscp
```

Configuring default port DSCP

Only if the port TRUST status is DSCP, the default configuration DSCP takes effect. When the incoming message of DSCP is 0, default port DSCP is used as DSCP value. In default situation, that value is 0. Reverse command is: no mls qos default-dscp. It can be set up in port mode:

Steps	Command	description
1	Config	Entry into global configuration mode
2	Interface port portid	Entry into port configuration mode
3	mls qos default-dscp dscp-value	Set default DSCP value dscp-value: est default port DSCP value as 0-63
4	Exit	Return to global configuration mode
5	Exit	Return to privilege mode
6	show mls qos port portid	Show QoS port configuration mode

The configuration is similar to CoS port default configuration.

Configuring port CoS override (Support equipment is not available)

Only if the port TRUST status is CoS, port CoS override configuration takes effect. Whether incoming message is untag or tag, CoS override value is used as CoS value. In Default situation, there will be no override. Reverse command: **no mls qos default-cos override**. It can be set up in port mode:

Steps	Command	Description
1	config	Entry into global configuration mode
2	interface port portid	Entry into port configuration mode
3	mls qos default-cos override	Set CoS override value
4	Exit	Return to global configuration mode
5	Exit	Return to privilege mode

6	show mls qos port <i>portid</i>	Show QoS port configuration
----------	--	-----------------------------

Configuring port DSCP override

Only if port TRUST status is DSCP, that configuration takes effect. Whatever the incoming message DSCP is, DSCP override value is used as DSCP value. In default situation, there will be no override. Reverse command: **no mls qos default-dscp override**. It can be set in port mode:

Steps	Command	Description
1	config	Entry into global configuration mode
2	interface port <i>portid</i>	Entry into port configuration mode
3	mls qos default-dscp override	Set default DSCP value
4	Exit	Entry into global configuration mode
5	exit	Return to privilege mode
6	show mls qos port <i>portid</i>	Show QoS port configuration

Configuration example: set TRUST status as DSCP in port 1 and port DSCP override value as 2.

Raisecom#**config**

Raisecom(config)#**inter port 1**

Raisecom(config-port)#**mls qos TRUST dscp** //set port TRUST status

Raisecom(config-port)# **mls qos default-dscp 2**

Raisecom(config-port)# **mls qos default-dscp override** //set port DSCP override value as 2

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom# **show mls qos port 1**

Show results:

Raisecom#**sh mls qos port 1**

Port 1:

TRUST state: TRUST DSCP

Default CoS: 0

Default DSCP: 2

DSCP override: Enable

DSCP mutation map: default-dscp

25.4.3 Configuring Flow Classification on ACL/class-map

Create delete class-map

Class-map is used to isolate the specific data stream, matching conditions include ACL, IP priority and DSCP, VLAN and class.

Creating **class-map** follows the steps below:

Steps	Command	Description
1	config	Entry into global configuration mode
2	Class-map <i>class-map-name</i> [match-all/match-any]	Create name as aaa, class-map and entry into config-cmap mode. <i>class-map-name</i> : class-map name, Max 16 characters match-all: satisfy all rules in class match-any: satisfy only one rule in class
3	description WORD	Description of information <i>WORD</i> : description of information in class map, max 255 characters.
4	exit	Return to global configuration mode
5	exit	Return to privilege mode
6	show class-map [WORD]	Show CLASS MAP <i>WORD</i> : class-map name, max 16 characters

class-map has two matching types: match-all runs AND operation, as multi match statements and operation. If there is conflict, then the match states fail; match-any is run or operation and default is match-all.

Configuration examples:

```
Raisecom#config
```

```
Raisecom(config)# class-map aaa match-all
```

```
Raisecom(config-cmap)# description this-is-test-class
Raisecom(config-cmap)#exit
```

```
Raisecom(config)#exit
```

```
Raisecom#show class-map
```

Show results as:

```
Class Map match-all aaa (id 0)
```

```
Description:this-is-test-class
```

```
Match none
```

If **class-map** is needed to delete, run **no**, as **no class-map *class-map-name***.

Attention:

- If class-map is quoted by policy in the port, then it is not able to be deleted.
- When matching configuration of class-map is match-all, the configuration may fail because the matching message may have conflicts.
- When a ACL is matched, ACL must be identified and its type must be permit.
- When a class-map is matched, sub class-map must be match-all type.

Configuring match statements

Steps	Command	Description
1	config	Entry into global configuration mode

2	class-map <i>class-map-name</i>	Entry into config-cmap mode <i>class-map-name</i> : class-map name, max 16 characters
3	match {ip-access-list / mac-access-list / access-list-map} acl-index	Match ACL <i>ip-access-list</i> : match IP access list <i>mac-access-list</i> : match MAC access list <i>access-list-map</i> : match access control list map table <i>acl-index</i> : access control list index
4	match ip dscp {0-63}	Match DSCP value
5	match ip precedence {0-7}	Match ToS value
6	match vlan {1-4094}	Match VLAN
7	match class-map WORD	Match class map WORD: match class-map name, max16 characters
8	exit	Return to global configuration mode
9	exit	Return to privilege mode
10	show class-map [WORD]	Show CLASS MAP WORD: class-map name, max 16 characters

Attention:

- When access control list is matched, ACL must be created first.
- When class map is matched, class-map must be created first.
- If the match type of class-map is match-all, the configuration may fail because there be conflicts in matched messages.
- If the same class-map has been applied for some port, then it is not allowed to modify the match statement.

To delete some match statement:

Steps	Command	Description
1	config	Entry into global configuration mode
2	class-map <i>class-map-name</i>	Entry into config-cmap mode <i>class-map-name</i> : class-map name, max 16 characters
3	no match {ip-access-list / mac-access-list / access-list-map} acl-index	Match ACL <i>ip-access-list</i> : match IP access list <i>mac-access-list</i> : match MAC access list <i>access-list-map</i> : match access control list map table <i>acl-index</i> : access control list index
4	no match ip dscp {0-63}	Match DSCP value
5	no match ip precedence {0-7}	Match ToS value
6	no match vlan {1-4094}	Match VLAN

7	no match class-map WORD	Match class map WORD: Match class-map name, max 16 characters
8	exit	Return to global configuration mode
9	exit	Return to privilege mode
10	show class-map [WORD]	Show CLASS MAP message WORD: class-map name, max 16 characters

Attention: If the class-map has already been applied for some other port, it is not allowed to delete the match statement.

25.4.4 Monitering and Maintenance

Command	Description
show mls qos port [portlist]	Show QoS port information Portlist: port number list
show class-map [WORD]	Show CLASS MAP information WORD: class-map name, max 16 characters

Show QoS port information

Attention: Show different information according to the supports of different equipments. There are the examples for supports of all configurations as show below.

Raisecom#show mls qos port 1

```
port 1:  
Attached policy-map: aaa  
TRUST state: not TRUSTed  
default COS: 2  
default DSCP: 3  
DSCP override: disable  
DSCP Mutation Map: aaa
```

If all port information is needed to check:

Raisecom#show mls qos port

```
port 1:  
Attached policy-map: aaa  
TRUST state: not TRUSTed  
default COS: 2  
default DSCP: 3  
DSCP override: disable  
DSCP Mutation Map: aaa
```

port 2:
Attached policy-map: aaa
TRUST state: not TRUSTed
default COS: 2
default DSCP: 3
DSCP override: disable
DSCP Mutation Map: aaa

.....

port 26:
TRUST state: not TRUSTed
default COS: 0
default DSCP: 0
DSCP override: disable
DSCP Mutation Map: default-dscp

Show QoS class-map information:
Raisecom#show class-map

Class Map match-all aaa (id 0)
Match ip-access-list 1
Match ip dscp 2
Match class-map bbb
Match vlan 1

Class Map match-all bbb (id 1)
Match ip-access-list 2

If it is needed to show the specific name of class-map, use commands as below:

Raisecom#show class-map aaa
Class Map match-all aaa (id 0)
Match ip-access-list 1
Match ip dscp 2
Match class-map bbb
Match vlan 1

25.4.5 Typical Configuration Examples

Configuration examples: classify the flow and satisfy the flow in aaa condition: in VLAN1, DSCP is 2 and the messages are from 10.0.0.2 and 10.0.0.3.

Raisecom#config

Raisecom(config)# ip-access-list 1 permit ip 10.0.0.2 255.255.255.0 any

Raisecom(config)# ip-access-list 2 permit ip any 10.0.0.3 255.255.255.0

```
Raisecom(config)# class-map bbb match-all
Raisecom(config-cmap)#match ip-access-list 2
```

```
Raisecom(config)# class-map aaa match-all
Raisecom(config-cmap)#match ip-access-list 1
Raisecom(config-cmap)#match ip dscp 2
Raisecom(config-cmap)#match vlan 1
Raisecom(config-cmap)#match class-map bbb
Raisecom(config-cmap)#exit
Raisecom(config)#exit
Raisecom#show class aaa
```

Show results as:

```
Raisecom#show class aaa
```

```
Class Map match-all aaa (id 0)
Match ip-access-list 1
Match ip dscp 2
Match class-map bbb
Match vlan 1
```

25.5 Policy and Marking Function Configuration

25.5.1 Policy and Marking Default Configuration

Function	Default value
Policy TRUST status	DSCP

25.5.2 Policy and Marking Configuration

Create delete policy-map

Use **policy-map** command to encapsulate and classify the data flow of class-map. Create **policy-map** as the steps below:

Steps	Command	Description
1	Config	Entry into global configuration mode
2	policy-map policy-map-name	Create name as bbb, policy-map and entry into config-pmap mode. policy-map-name: policy map name, max 16 characters

3	description WORD	Description information WORD: policy map description information, max 255 characters
4	Exit	Return to global configuration mode
5	Exit	Return to privilege mode
6	show policy-map [WORD]	Show POLICY MAP information <i>WORD: policy map name, max 16 characters</i>

Configuration examples:

Raisecom#**config**

Raisecom(config)# **policy-map bbb**

Raisecom(config-pmap)#**description this-is-test-policy**

Raisecom(config-pmap)#**exit**

Raisecom(config)# **exit**

To check whether the configuration is right, use show command:

Raisecom#**show policy-map**

Policy Map bbb

Description:this-is-test-policy

If it is needed to delete a **policy-map**, use **command no, no policy-map policy-map-name**.

Attention: If a policy-map is applied for other ports, then it is not able to be deleted.

Define policy map

To define one or more defined class-map as a policy, following steps below are used:

Steps	Command	Descriptions
1	config	Entry into global configuration mode
2	policy-map policy-map-name	Entry into config-pmap mode policy-map-name: policy map name, max 16 characters
3	class-map class-map-name	Encapsulate class-map aaa into policy aaa, and entry into config-pmap-c mode class-map-name: class-map name, max 16 characters
4	exit	Return to config-pmap mode
5	exit	Return to global configuration mode
6	exit	Return to privilege mode
7	show policy-map [WORD]	Display POLICY MAP information WORD: policy map name, max 16 characters
8	show policy-map class {WORD}	Display POLICY MAP some classification information WORD: class-map name, max 16 characters

One class can be applied for many policies.

Configuration examples:

Raisecom#**config**

Raisecom(config)# **policy-map aaa**

Raisecom(config-pmap)# **class-map aaa**

Raisecom(config-pmap-c)#**exit**

Raisecom(config-pmap)#**exit**

Raisecom(config)# **exit**

To check whether the configuration is right, use show command:

Raisecom#**show policy-map**

Policy Map aaa

Class aaa

To delete class-map from a policy:

Steps	Command	Description
1	config	Entry into global configuration mode
2	policy-map policy-map-name	Entry into config-pmap mode policy-map-name: policy map name, max 16 characters
3	no class-map class-map-name	Delete class-map from policy <i>class-map-name</i> : class-map name, max 16 characters
4	exit	Return privilege mode
5	show policy-map [WORD]	Display POLICY MAP information <i>WORD</i> : policy map name, max 16 characters

Attention: It is not allowed to delete class-map if the policy-map has been applied for some other port.

Define policy action

Different actions are used for different data flow in policy, show as below:

Steps	Command	Description
1	config	Entry into global configuration mode
2	policy-map policy-name	Entry into config-pmap mode policy-name: policy map name, max 16 characters
3	Class-map class-name	Encapsulate class-map into policy, and entry into config-pmap-c mode <i>class-name</i> : class-map name, max 16 characters

4	police <i>policer-name</i>	Use policer for the policy data flow for bit-rate limiting and reshaping, check the link for more infomaiton: bit-Rate Limitation and reshaping function configuration <i>policer-name</i> : policer name, max 16 characters
5	TRUST [<i>cos / dscp / ip-precedence</i>]	Policy TRUST status, default use DSCP <i>cos</i> : set switch TRUST CoS status <i>dscp</i> : set switch TRUST DSCP status <i>ip-precedence</i> : set switch TRUST IP priority
6	statistics enable	Open flow statistic switch
7	set {ip dscp new-dscp ip precedence new-precedence cos new-cos }	Set new value for data flow <i>new-dscp</i> : DSCP value, 0-63; <i>new-precedence</i> : IP priority value, 0-7 <i>new-cos</i> : set CoS value, 0-7
8	set vlan <1-4094>	Set VLAN override
9	redirect-to port <i>to-port</i>	Redirect the ports <i>to-port</i> : redirect the ports numbers
10	copy-to-mirror	Data flow mirror image
11	exit	Return to config-pmap mode
12	exit	Return to global configuration mode
13	exit	Return to privilege mode
14	show policy-map [<i>WORD</i>]	Display POLICY MAP information <i>WORD</i> : policy map name, max 16 characters

Attention:

- So far, policy TRUST (TRUST command) functions are not supported
- Set command and policy TRUST command are mutually exclusive.
- In one class-map, set command can only be configured in one. Later configuration will take effect

Configuration examples:

Raisecom#**config**

Raisecom(config)#**policy-map** *aaa*

Raisecom(config-pmap)#**class-map** *aaa*

Raisecom(config-pmap-c)#**police** *aaa*

Raisecom(config-pmap-c)#**set cos** 6

Raisecom(config-pmap-c)#**set ip dscp** 5

Raisecom(config-pmap-c)#**set ip precedence** 4

Raisecom(config-pmap-c)#**set vlan** 10

Raisecom(config-pmap-c)#**redirect-to port** 3

Raisecom(config-pmap-c)#**exit**

```
Raisecom(config-pmap)#exit
Raisecom(config)#exit
Raisecom# show policy-map aaa
```

Show as:

```
Policy Map aaa
Class aaa
police aaa
set ip precedence 4
set vlan 10
redirect-to port 3
```

To delete or modify data flow actions:

Steps	Command	Description
1	Config	Entry into global configuration mode
2	policy-map <i>policy-name</i>	Entry into config-pmap mode <i>policy-name</i> : policy map name,max 16 characters
3	class-map <i>class-name</i>	Encapsulate class-map aaa into policy aaa, and entry into config-pmap-c mode <i>class-name</i> : class-map name, max 16 characters
4	no police <i>policer-name</i>	Apply policer in this policy data flow <i>policer-name</i> : policer name, max 16 characters
		Data flow TRUST status, default use DSCP
5	no TRUST [<i>cos / dscp / ip-precedence</i>]	<i>cos</i> : set switch as TRUST CoS status <i>dscp</i> : set switch as TRUST DSCP status <i>ip-precedence</i> : set switch as TRUST IP priority status
6	statistics enable	Open flow statistic switch Set new value for data flow
7	no set {<i>ip dscp/ip precedence/cos</i>}	<i>new-dscp</i> : DSCP value, 0-63; <i>new-precedence</i> : IP priority value, 0-7 <i>new-cos</i> : set CoS value, 0-7
8	no set vlan	Set VLAN override
9	no redirect-to port	Redirect to port
10	no copy-to-mirror	Data flow mirror image
11	exit	Return to config-pmap mode
12	exit	Return to global configuration mode
13	exit	Return to privilege mode
14	show policy-map [WORD]	Display POLICY MAP WORD: policy map name, max 16 characters

Attention: It is not allowed to modify the action if its policy-map has been applied for other ports

Apply policy service-policy in ports

It actually does not take effect after all data flow and policy defined. They need to be applied for the ports. The steps for the apply policy are as below:

Steps	Command	Description
1	config	Entry into global configuration mode
2	service-policy <i>policy-name</i> ingress <i>portid</i> [egress <i>portlist</i>]	Apply policy on in/out port. <i>policy-name</i> : policy map name, max 16 characters <i>portid</i> : in port number <i>portlist</i> : out port list
3	exit	Return to privilege mode
4	show policy-map port [<i>portlist</i>]	Display port policy application information <i>portlist</i> : port number

Attention:

- QoS must start before applying policy;
- When configuring data flow becomes big, it may fail because it may get the biggest rule of capacity based on those 256 rules for 8 ports.
- The TRUST status are mutually exclusive if the TRUST status of the applied front port is not UNTRUST status. After applied, the status will become UNTRUST status.

Application examples:

```
Raisecom#config
Raisecom(config)#service-policy aaa ingress 2 egress 1-5
Raisecom(config)#service-policy bbb egress 1
Raisecom(config)#exit
Raisecom#show policy-map port
```

Display as:

```
port 2 on ingress:
Policy Map aaa:
Egress:1-5
Class Map :aaa (match-all)
```

```
port 1 on egress:
Policy Map bbb:
```

25.5.3 Monitoring and Maintenance

Command	Description
show policy-map [WORD]	Display POLICY MAP information

show policy-map class {WORD}	<i>WORD</i> : policy map name, max 16 characters Display some classified information of POLICY MAP
show policy-map port [portlist]	<i>WORD</i> : class-map name, max 16 characters Display port policy application information <i>portlist</i> : port numbers

1. Display QoS policy-map information

Raisecom#**show policy-map**

Policy Map aaa

Class aaa

police aaa

set ip precedence 4

Class bbb

police aaa

To display the specific name of policy-map information:

Raisecom#**show policy-map aaa**

Policy Map aaa

Class aaa

police aaa

set ip precedence 4

Class bbb

police aaa

2. Display some classified information of POLICY MAP

If wanted to show specific policy-map name、indicated class-map name information:

Raisecom#**show policy-map aaa class-map aaa**

Policy Map aaa

Class aaa

police aaa

set ip precedence 4

3. Display QoS policy-map application information

If wanted to check which policy-map information applied on which ports:

Raisecom#**show policy-map port 1**

port 1:

Policy Map aaa:

Egerss:1-5

Class Map :aaa (match-all)

Class Map :bbb (match-all)

If wanted which policy-map information applied on all ports:

```
Raisecom#show policy-map port
```

port 1:

Policy Map aaa:

Egress:1-5

Class Map :aaa (match-all)

Class Map :bbb (match-all)

25.5.4 Specific Configuration Examples:

```
Raisecom#config
```

//Define ACL

```
Raisecom(config)# ip-access-list 1 permit ip 10.0.0.2 255.255.255.0 10.0.0.3 255.255.255.0
```

```
Raisecom(config)# ip-access-list 2 permit ip 10.0.0.3 255.255.255.0 10.0.0.2 255.255.255.0
```

//classify data flow

```
Raisecom(config)# class-map aaa match-all
```

```
Raisecom(config-cmap)#match ip-access-list 1
```

```
Raisecom(config-cmap)# exit
```

```
Raisecom(config)# class-map bbb match-all
```

```
Raisecom(config-cmap)#match ip-access-list 2
```

```
Raisecom(config-cmap)# exit
```

//bit-rate limitation and reshapeing definition, details see: bit-Rate Limitation and reshaping function configuration

```
Raisecom(config)#mls qos class-policer p-aaa 4000 100 exceed-action drop
```

```
Raisecom(config)# mls qos class-policer p-bbb 8000 200 exceed-action drop
```

//define policy

```
Raisecom(config)#policy-map wmj
```

```
Raisecom(config-pmap)#class-map aaa //define data flow classification aaa in policy
```

```
Raisecom(config-pmap-c)# set ip dscp 5 //define policy action---set IP DSCP
```

```
Raisecom(config-pmap-c)#police p-aaa //define policy action——bit-rate limited reshaping
```

```
Raisecom(config-pmap-c)#exit
```

```

Raisecom(config-pmap)#class-map bbb //define data flow bbb in policy
Raisecom(config-pmap-c)# set ip dscp 6 //define policy action——set IP DSCP
Raisecom(config-pmap-c)#police p-bbb //define policy action——bit-rate limited reshaping
Raisecom(config-pmap-c)#exit

Raisecom(config-pmap)#exit
Raisecom(config)#mls qos
Raisecom(config)#service-policy wnj ingress 1 egress 2 //apply policy in ports

```

25.6 Bit-Rate Limitation and Reshaping Function Configuration

25.6.1 Configuration Based on Bit-Rate and Reshaping of Data Flow

Create policer as following steps:

Note: ISCOM2128EA-MA products do not support marked-dscp.

Steps	Command	Description
1	config	Entry into global configuration mode
		Create policer in type of single <i>policer-name</i> : set policer name
		<i>rate</i> : bit-rate value (Kbps), 8—2000000
2	mls qos single-policer <i>policer-name</i> <i>rate burst exceed-action {drop policed-dscp-transmit marked-dscp }</i>	<i>burst</i> : Burst value (KBps), 8—512000 <i>drop</i> : droped packets once it is over bit-rate value <i>policed-dscp-transmit</i> : modified DSCP value once it is over bit-rate value <i>marked-dscp</i> : modified DSCP value once it is over bit-rate value
		Create policer as type of class <i>policer-name</i> : set policer name
		<i>rate</i> : bit-rate value(Kbps), 8—2000000kbps
3	mls qos class-policer <i>policer-name</i> <i>rate burst exceed-action {drop policed-dscp-transmit marked-dscp }</i>	<i>burst</i> : burst value (KBps), 8—512000 <i>drop</i> : droped packets once it is over bit-rate value <i>policed-dscp-transmit</i> : modify DSCP once it is over bit-rate value <i>marked-dscp</i> : modified DSCP value once over bit-rate value
		Create policer as type of aggregate <i>policer-name</i> : set policer name
4	mls qos aggregate-policer <i>policer-name rate burst exceed-action {drop policed-dscp-transmit marked-dscp }</i>	<i>rate</i> : bit-rate value(Kbps), 8—2000000kbps <i>burst</i> : burst value (KBps), 8—512000 <i>drop</i> : droped packets once it is over bit-rate value

		<i>policed-dscp-transmit:</i> modify DSCP once it is over bit-rate value
		<i>marked-dscp:</i> modified DSCP value once over bit-rate value
5	exit	Return to global configuration mode
		Display policer information
6	show mls qos policer [single-policer class-policer aggregate-policer]	<i>single-policer:</i> display single policer <i>class-policer:</i> display class policer <i>aggregate-policer:</i> display aggregate policer

To delete a policer, use command of no, **no {single-policer/class-policer/aggregate-policer} placer-name.**

Attention: When delete a policer, it is not allowed to delete it if its policy is applied for other ports.

25.6.2 Monitering and Maintenance

Command	Description
	Display policer information
show mls qos policer [single-policer / class-policer / aggregate-policer]	<i>single-policer:</i> Display single policer <i>class-policer:</i> Display class policer <i>aggregate-policer:</i> display aggregate policer

Raisecom#**show mls qos policer**

single-policer aaa 44 44 exceed-action policed-dscp-transmit 4

Used by policy map aaa

To show which port is using policer, use the commands below:

Raisecom#**show mls qos port policers**

Port id 1

policymap name: aaa

policer type: Single, name: aaa

rate: 44 kbps, burst: 44 kbyte, exceed action: policed-dscp-transmit, dscp:4

25.6.3 Specific Configuration Examples

Configuration examples:

Raisecom#**config**

Raisecom(config)# mls qos single-policer aaa 44 44 exceed-action policed-dscp-transmit 4
 Raisecom(config)# exit

Raisecom#**show mls qos policer**

Display results as:

single-policer aaa 44 44 exceed-action policed-dscp-transmit 4

Not used by any policy map

If aaa is applied for a port:

Raisecom#show mls qos port policers

```
Port id 1
policymap name: aaa
policer type: Single, name: aaa
rate: 44 kbps, burst: 44 kbyte, exceed action: policed-dscp-transmit, dscp: 4
```

25.7 Map Function Configuration

25.7.1 Map Default Configuration

COS-localpriority default configuration relationship as:

CoS value	0	1	2	3	4	5	6	7
Localpriority value	0	1	2	3	4	5	6	7

DSCP - localpriority default map relation as:

DSCP value	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
Localpriority value	0	1	2	3	4	5	6	7

TOS- localpriority default map relation as:

ToS value	0	1	2	3	4	5	6	7
localpriority	0	1	2	3	4	5	6	7

25.7.2 CoS-localpriority map List Configuration

CoS-localpriority map list maps incoming packet COS value as a localpriority value. QoS is used to describe data flow priority. It default map relation as:

CoS value	0	1	2	3	4	5	6	7
Localpriority value	0	1	2	3	4	5	6	7

To modify the map relations, the following steps are set:

Steps	Command	Description
1	config	Entry into global configuration mode
2	mls qos mapping cos <cosVal> to localpriority <localPrioVal>	Set new map relation <i>cosVal</i> : COSvslur, range 0-7 <i>localPrioVal</i> : local priority, range 0-7
3	exit	Return to privilege mode
4	show mls qos mapping cos	Show cos-localpritoiry map inforamtion

Configuration examples:

```
Configuration cos as 5localpritoiry
Raisecom#config
Raisecom(config)# mls qos mapping cos 5 to localpriority 3
Raisecom(config)#exit
Raisecom# show mls qos mapping cos
```

Show results as:

```
CoS-LocalPriority Mapping:
CoS:   0   1   2   3   4   5   6   7
-----
LocalPriority:  0   1   2   3   4   5   6   7
```

To backup COS-DSCP map list to default map relation, use command **no**.

Steps	Command	description
1	config	Entry into global configuration mode
2	no mls qos map cos-dscp	Backup to default map relation
3	exit	Return to privilege mode
4	show mls qos maps cos-dscp	Display QoS localPriority map list

Raisecom#**show mls qos maps cos-dscp**

```
Cos-dscp map:
cos:   0   1   2   3   4   5   6   7
-----
LocalPriority:  0   1   2   3   4   5   6   7
```

25.7.3 DHCP-localpriorityMap List Configuration

DHCP-localpriority map-list configuration maps incoming packet into a localpriority value. QoS is used to describe the data flow priority. Its default map relation as show below:

dscp value	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
Localpriority value	0	1	2	3	4	5	6	7

To modify that map relation, set as the following steps:

Steps	Command	Description
1	config	Entry global configuration mode
2	mls qos mapping dscp <dscpVal> to localpriority <localPrioVal >	Set new map relationship <i>dscpVal</i> :dscp value,range 0-63 <i>localPrioVal</i> : local priority value, range 0-7
3	exit	Return to privilege mode
4	show mls qos mapping dscp	Display dscp-localpritoiry map information

Configuration example:

Configure dscp map as **5 localpriority**:

Raisecom#**config**

Raisecom(config)# **mls qos mapping dscp 5 to localpriority 3**

Raisecom(config)#**exit**

Raisecom# **show mls qos mapping dscp**

Show results as:

DSCP-LocalPriority Mapping:

d1 : d2 0 1 2 3 4 5 6 7 8 9

<i>0 :</i>	0	0	0	0	0	0	0	0	1	1
<i>1 :</i>	2	1	1	1	1	1	2	2	2	2
<i>2 :</i>	2	2	2	2	3	3	3	3	3	3
<i>3 :</i>	3	3	4	4	4	4	4	4	4	4
<i>4 :</i>	5	5	5	5	5	5	5	5	6	6
<i>5 :</i>	6	6	6	6	6	6	7	7	7	7
<i>6 :</i>	7	7	7	7						

Backing up dscp-localpriority map list to default map relation, use command **no**.

Steps	Command	Description
1	config	Entry into global configuration mode
2	no mls qos mapping dscp	Backup to default map relation
3	exit	Return to privilege mode
4	show mls qos mapping dscp	Show dscp-localpriority map list

DSCP-LocalPriority Mapping:

d1 : d2 0 1 2 3 4 5 6 7 8 9

<i>0 :</i>	0	0	0	0	0	0	0	0	1	1
<i>1 :</i>	2	1	1	1	1	1	2	2	2	2
<i>2 :</i>	2	2	2	2	3	3	3	3	3	3
<i>3 :</i>	3	3	4	4	4	4	4	4	4	4
<i>4 :</i>	5	5	5	5	5	5	5	5	6	6
<i>5 :</i>	6	6	6	6	6	6	7	7	7	7
<i>6 :</i>	7	7	7	7						

25.7.4 tos-localpriority List Configuration

Note: ISCOM2128EA-MA products do not support tos.

Tos-localpriority list maps the incoming packet DSCP value into a localpriority value. QoS use its description data flow priority.

To modify that map relation, follows the steps below:

Steps	Command	Description
1	Config	Entry into global configuration mode
2	mls qos mapping tos <tosVal> to localpriority <localPrioVal>	set new map relation <i>tosVal</i> :TOS value, range 0-7 <i>localPrioVal</i> : local priority value, range 0-7
3	Exit	Return to privilege mode
4	show mls qos maps dscp-cos	Show tos map information

Configuration examples:

Configure **cos** map as **5 localpriority**

Raisecom#**config**

Raisecom(config)# **mls qos mapping tos 5 to localpriority 3**

Raisecom(config)#**exit**

Raisecom# **show mls qos mapping tos**

show results as:

ToS-LocalPriority Mapping:

ToS: 0 1 2 3 4 5 6 7

LocalPriority: 0 1 2 3 4 5 6 7

To delete tos-localpriority map list to default mapping relation, use command **no**:

steps	command	description
1	config	Entry into global configuration mode
2	no mls qos mapping tos	Back to the default mapping relation
3	exit	Return to privilege mode
4	show mls qos mapping tos	Show tos-localpriority map list

Raisecom#**show mls qos maps dscp-cos**

ToS-LocalPriority Mapping:

ToS:	0	1	2	3	4	5	6	7
<hr/>								
LocalPriority:	0	1	2	3	4	5	6	7

25.7.5 Set Ports Based on smac, dmac, vlan's Frame Priority and Priority Override Function

Ports can be based on smac、dmac、vlan entering switch's message frame priority and queue priority override.

Configuration steps as below:

Steps	Command	Description
1	config	Entry into global configuration mode
2	interface { port-list } <1-MAX_PORT_NUM >	Entry into Ethernet physic interface mode <i>1-MAX_PORT_NUM</i> equipement port numbers
3	mls qos {smac / dmac} {priority-set/cos-override}	set up ports based on smac, dmac's frame priority or queue priority override function Smac: source MAC Dmac: destination MAC <i>cos-override</i> : frame priority <i>priority-set</i> : queue priority
4	mls qos {smac/dmac} priority-set cos-override	set up ports based on smac,dmac's frame priority and queue priority override function Smac: source MAC Dmac: destination MAC <i>cos-override</i> : frame priority <i>priority-set</i> : queue priority
5	mls qos vlan {priority-set/cos-override}	set up ports based on vlan's frame priority or queue priority override function <i>cos-override</i> : frame priority <i>priority-set</i> : queue priority
6	mls qos vlan priority-set cos-override	set up ports based on vlan's frame priority and queue priority override function <i>cos-override</i> : frame priority <i>priority-set</i> : queue priority
7	exit	Exit
8	show mls qos port-list {1-MAX_PORT_NUM }	Display QoS configuration information <i>1-MAX_PORT_NUM</i> equipement port numbers

To use command no Renew all priority override based on smac, dmac, vlanto default configuration (even both of them are not override).

25.7.6 Monitering and Maintenance

Command	Description
show mls qos mapping [cos dscp tos localpriority]	Display all map list's configuration content. <i>cos</i> : show cos map configuration information <i>dscp</i> : show cos map configuration information <i>tos</i> : show cos map configuration information <i>localpriority</i> : show local priority queue map configuration information
show mls qos queue	Display QoS queue map list
show mls qos port [portid]	Display QoS configuration information <i>Portid</i> : portID

Map list information maps

Raisecom#**show mls qos mapping cos**

CoS-LocalPriority Mapping:

<i>CoS:</i>	0	1	2	3	4	5	6	7
<i>LocalPriority:</i>	0	1	2	3	4	5	6	7

Raisecom# **show mls qos mapping dscp**

DSCP-LocalPriority Mapping:

<i>d1 : d2</i>	0	1	2	3	4	5	6	7	8	9
<i>0 :</i>	0	0	0	0	0	0	0	1	1	
<i>1 :</i>	2	1	1	1	1	2	2	2	2	
<i>2 :</i>	2	2	2	2	3	3	3	3	3	
<i>3 :</i>	3	3	4	4	4	4	4	4	4	
<i>4 :</i>	5	5	5	5	5	5	5	6	6	
<i>5 :</i>	6	6	6	6	6	7	7	7	7	
<i>6 :</i>	7	7	7	7						

Raisecom#**show mls qos mapping cos**

ToS-LocalPriority Mapping:

<i>ToS:</i>	0	1	2	3	4	5	6	7
<i>LocalPriority:</i>	0	1	2	3	4	5	6	7

Raisecom#**show mls qos mapping localpriority**

LocalPriority-Queue Mapping:

<i>LocalPriority:</i>	0	1	2	3	4	5	6	7
<hr/>								
<i>Queue:</i>	1	2	3	4	5	6	7	8

Queue map list information queueing

Raisecom(config)#**show mls qos queue port 1**

Port:1

<i>Queue</i>	<i>Weight(WRR)</i>
<hr/>	
1	1
2	1
3	1
4	1
5	1
6	1
7	1

Display QoS configuration information

Raisecom#**show mls qos port 1**

<i>Port</i>	<i>Priority</i>	<i>Scheduler</i>
<hr/>		
1	0	SP

25.8 Queue and Adjust Function Mode

So far, the equipments support four queue adjust modes: strict priority (SP), weighted priority (WRR), BOUND-DELAY mode and SP+WRR's mixed mode. Default set is priority mode.

25.8.1 Queue and Adjust Default Configuration

Function	Default value
Queue adjust policy	Strict priority adjust SP

25.8.2 SP Configuration

Configuration steps as:

Steps	Command	Description

1	config	Entry into global configuration mode
2	mls qos queue scheduler sp	Configuration is strict priority
3	exit	Return to privilege mode
4	show mls qos que	display QoS queuing information

25.8.3 WRR Configuration

Configuration steps as:

Steps	Command	Description
1	config	Entry into global configuration mode
2	mls qos queue scheduler wrr <i><weightVal1> <weightVal2></i> <i><weightVal3> <weightVal4></i> [<i><weightVal5> <weightVal6></i> <i><weightVal7> <weightVal8></i>]	Set ports' adjust mode as WRRmode Weight 1-8: set queue 1-8 weight value
3	exit	Return to privilege mode
4	show mls qos que	display QoS queuing information

25.8.4 DRR Configuration

Note: ISCOM2128EA-MA products do not support drr.

Configuration steps as:

Steps	Command	Description
1	config	Entry into global configuration mode
2	mls qos queue scheduler drr <i><weightVal1></i> <i><weightVal2> <weightVal3> <weightVal4></i> [<i><weightVal5> <weightVal6> <weightVal7></i> <i><weightVal8></i>]	Set ports' adjust mode as DRR mode Weight 1-8: set queue 1-8 weight value
3	exit	Return to privilege mode
4	show mls qos queue	display QoS queuing information

25.8.5 WFQ Configuration

Configuration steps as:

Steps	Command	Description
1	config	entry into global configuration mode
2	mls qos queue scheduler wfq <i><weightVal1></i> <i><weightVal2> <weightVal3> <weightVal4></i> [<i><weightVal5> <weightVal6> <weightVal7></i>	Set ports' adjust mode as WFQ mode Weight 1-8: set queue 1-8 weight value

	<weightVal8>]	
3	exit	Return to privilege mode
4	show mls qos queue	display QoS queuing information

25.8.6 Monitoring and Maintenance

Command	Description
show mls qos queue	Display QoS's queuemap list

Queue map list information queueing

Raisecom(config)#**show mls qos queue port 1**

Port:1

<i>Queue</i>	<i>Weight(WRR)</i>
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1

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

25.8.7 Specific Configuration Examples

Configuration examples: set queue as WRR mode, weight as 1:2:4:8:

Raisecom#**config**

Raisecom(config)# **queue wrr-weight 1 2 4 8**

Raisecom(config)#**exit**

Raisecom#**show mls qos queuing**

Display results:

<i>Queue</i>	<i>Weight(WRR)</i>
--------------	--------------------

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

25.9 QoS Trouble Shoot

- Port TRUST status and policy configuration are mutually exclusive.
- Data flow TRUST status and SET actions are mutually exclusive.
- To delete class-map、policy-map、policer, it will be failed if they have been applied for the ports.
- If class-map、policy-map have been applied for the ports, then modification for match statements and data flow actions (as set action) will fail.
- Before apply data flow policy, QoS must be started first; data flow policy will be failed if QoS is stopped.
- If class-map match type is match-all, the configuration may fail because there might be conflicts between matching information.
- To match a ACL, ACL must be defined first and its type must be permit.
- To match a class-map, sub class-map must be type of match-all.
- As configuration data flow become more, it may be failed in applying because it is getting the capacity biggest rule. (8 ports have 256 rules).
- To start QoS policy, it is suggested to turn off data flow control function.

25.10 QoS Command Reference

Command	Description
class-map <i>class-map-name</i> [match-any match-all]	Create class-map
no class-map <i>class-map-name</i>	Delete class-map
[no] policy-map <i>policy-map-name</i>	Create delete policy map
description <i>WORD</i>	Set policy map and class-map description information
[no] class <i>class-map-name</i>	apply class map on policy
match { ip-access-list <i>acl-index</i> mac-access-list <i>acl-index</i> access-list-map <i>acl-index</i> ip dscp <i>dscp-list</i> ip precedence <i>ip-precedence-list</i> class calss-name vlan <i>vlanlist</i> }	Set match statements
no match { ip-access-list <i>acl-index</i> mac-access-list <i>acl-index</i> access-list-map <i>acl-index</i> ip dscp ip precedence class calss-name vlan <i>vlanlist</i> }	Delete match statements
[no] trust [cos dscp]	Set data flow TRUST status
set { ip dscp <i>new-dscp</i> ip precedence <i>new-precedence</i> cos <i>new-cos</i> }	Set actions
no set { ip dscp ip precedence cos }	Delete set value
mls qos { aggregate-policer class-policer single-policer } <i>policer-name</i> <i>rate burst</i> [exceed-action { drop policed-dscp-transmit <i>dscp</i> }]	Create policer
no mls qos { aggregate-policer class-policer single-policer } <i>policer-name</i>	Delete policer

[no] police <i>policer-name</i>	Apply policer
service-policy <i>policy-map-name</i> ingress <i>portid</i> [egress <i>portlist</i>]	Apply policy
no service-policy <i>policy-map-name</i> ingress <i>portid</i>	Decline apply policy
mls qos map cos-dscp <i>dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8</i>	configurationCoS to DSCP map
no mls qos map cos-dscp	Renew CoS to DSCP map
mls qos map ip-prec-dscp <i>dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8</i>	Configuration ToS to DSCP map
no mls qos map ip-prec-dscp	Renew ToS to DSCP map
mls qos map dscp-cos <i>dscp-list to cos</i>	Configuration DSCP to switch internal priority map
no mls qos map dscp-cos	Renew DSCP to switch internal priority map
queue cos-map <i>queue-id cos-list</i>	Configuration switch internal priority to queue map
no queue cos-map	Renew switch internal priority to queue map
queue wrr-weight <i>weight0 weight1 weight2 weight3</i>	Configuration switch queue adjust mode as WRR
queue bounded-delay <i>weight0 weight1 weight2 weight3 delaytime</i>	Set port adjust mode as BOUNDDELAY mode
queue preemp-wrr <i>weight1 weight2 weight3</i>	Set port adjust mode as PREEMP-WRR mode
queue strict-priority	Set port adjust mode as strict priority mode
show mls qos	Display QoS on/off status
show mls qos policer [<i>policename aggregate-policer /class-policer / single-policer</i>]	Display policer information
show mls qos maps [cos-dscp / dscp-cos / dscp-mutation / ip-prec-dscp]	Display every map list configuration content
show mls qos queueing	Display in/out queue configuration information
show mls qos port <i>portid</i> [policers]	Display port strategy configuration, policer,etc information
show class-map [<i>class-map-name</i>]	Display class-map information
show policy-map [<i>policy-map-name</i> [port <i>portId</i>] [class <i>class-name</i>]	Display policy information

Chapter 26 Dynamic ARP Inspection Configuration

This chapter is mainly about how to configure and maintain Dynamic ARP Inspection, including:

- ❖ Dynamic ARP Inspection principle overview
- ❖ Dynamic ARP Inspection configuration
- ❖ Monitoring and maintenance
- ❖ Typical configuration example

26.1 Dynamic ARP inspection principle overview

As ARP protocol's design, to decrease too much ARP data communication on the network, a host, even if the received ARP response is not for its own request, it will also insert the response to its own ARP cache table, which may cause 'ARP cheat'. If a hacker wants to monitor the communication between the two hosts in the same network (even if they connect each other with switches), he will send ARP response packets to each of the hosts, and let the hosts mistake the MAC address of the opposite side to the hacker's host, the two sides' communication that seems to be straight through, is in fact going through the hacker's host. The hacker gets the content he wants at one side, and needs to change some information in the packets and make transmission on the other side. In this way of sniffer, the hacker needs not to change his host's network card to hybrid mode, because the packets between the two hosts are all sent to the hacker's transferring host.

These attacks can all be prevented by DAI (Dynamic ARP Inspection), which ensures that the switch sends only 'valid' ARP request and response information.

DAI binding table is made up of DHCP Snooping monitoring binding table and static configuration ARP inspection rules, including IP address MAC address and VLAN binding information and relate it to specific switch port. Dynamic ARP inspection can use the content of the binding table to detect all the not-trusted port ARP request and response (active ARP and no-active ARP) to make sure that the response is from the real ARP owner. By checking the recorded port binding information and ARP responding IP address, the switch determines if it is the real ARP owner. The invalid ARP packets will be dropped.

At the same time, Dynamic ARP inspection provides ARP packet rate limit function which is used to prevent attacking by sending a large number of ARP packets. If the attackers maliciously construct a large number of ARP packets and send to switch port, CPU of switch will overload, resulting in abnormal operation or paralyzed status. By enabling port ARP packet rate limit function; switch will do a statistic for port ARP packet numbers by seconds. If ARP packets which is received per second exceed the set threshold, the port will be under the ARP attack, then switch will discard all ARP packets of this port in order to avoid attacking. In addition, device also provides port auto-recovery function and supports auto-configuration recovery time. For those overspeed ports, when auto-recovery outtimes, it will automatically recover to normal status. At the same time, ARP packets can continue to go through.

26.2 Configure Dynamic ARP Inspection

This part is about how to configure and maintain DAI, including:

- Default Dynamic ARP Inspection configuration
- Global Dynamic ARP Inspection configuration
- Static ARP binding table configuration
- DAI protection VLAN configuration
- Port ARP trust configuration
- ARP packets limit default configuration
- ARP packets rate-limit port configuration
- ARP packet rate-limit global configuration

26.2.1 Default Dynamic ARP Inspection configuration

Function	Default value
DAI binding table static configuration function	Disable
Dynamic DHCP Snooping binding table learning function	Disable
Protection VLAN status	Protect all VLAN
Static DAI binding table rules	None
Port ARP trust	Distrust

26.2.2 Global Dynamic ARP Inspection configuration

By default, the equipment DAI binding table static configuration function and dynamic DHCP Snooping binding table learning function is disabled. In global mode run the commands below, and start the two functions above.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	ip arp-inspection static-config	Enable configuring static ARP binding table rule function
3	ip arp-inspection dhcp-snooping	Dynamic DHCP Snooping binding table learning function
4	exit	Quit from global configuration mode and enter privileged EXEC mode
5	show ip arp-inspection	Show DAI running state

Notice: When configuring static ARP binding table rule function or dynamic DHCP Snooping binding table learning function is enabled, ARP detection will start to distrust ports.

The example below shows how to start configuring static ARP binding table rule function and dynamic DHCP Snooping binding table learning function:

```
Raisecom (config)# ip arp-inspection static-config
```

```
Raisecom (config)# ip arp-inspection dhcp-snooping
```

Use **show** to examine if the configuration is correct:

Raisecom#**show ip arp-inspection**

```
Static Config ARP Inspection:      Enable
DHCP Snooping ARP Inspection:    Enable
Port      Trust
-----
1        no
2        no
....
```

26.2.3 DAI Protection VLAN Configuration

By default, DAI will protect all VLAN of non-trusted port. If the table does not match with the bind, it will be not allowed to go through. By carrying out the following command in global mode, you can configure the VLAN which is needed to protect.

The configuration step is as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	ip arp-inspection static-config	Enable configuration static ARP binding table rules function
3	ip arp-inspection vlan 1-3	Set VLAN 1-3 inside ARP packets protection, the packet which accords with binding rule can be allowed to go through.
4	exit	Exit global configuration mode and enter privilege user mode
5	show ip arp-inspection	Show DAI running condition

Note: Open either configuration static ARP binding table rules function or dynamic DHCP snooping binding table learning function, it will carry out ARP detection in the non-trusted port.

The following example show how to enable configuration static ARP binding table rules function and dynamic DHCP snooping bingding table learning function, configuring protected VLAN:

```
Raisecom (config)# ip arp-inspection static-config
Raisecom (config)# ip arp-inspection dhcp-snooping
Raisecom (config)# ip arp-inspection vlan 1-3
```

Use command **show** to view the configuration:

Raisecom#**show ip arp-inspection**

```
Static Config ARP Inspection:      Enable
DHCP Snooping ARP Inspection:    Enable
ARP Inspection Protect Vlan:     1-3
Bind Rule Num                   : 0
Vlan Acl Num                    : 72
Remained Acl Num                : 240
```

<i>Port</i>	<i>Trust</i>
<hr/>	
1	<i>no</i>
2	<i>no</i>
<hr/>	

26.2.4 Configure port ARP trust

By default, the port does not trust any ARP message. In port mode, use the commands below to configure port trusted ARP message. When configured trusted ARP messages, the port will not longer make ARP inspection.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port 1	Enter port configuration mode
3	ip arp-inspection trust	Configure port trusted ARP message
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip arp-inspection	Show DAI port trust configuration

The example below shows how to configure port ARP trust:

```
Raisecom (config)# interface port 1
Raisecom (config-port)# ip arp-inspection trust
```

Use **show** to examine if the configuration is correct:

```
Raisecom#show ip arp-inspection
Static Config ARP Inspection:      Enable
DHCP Snooping ARP Inspection:     Enable
Port      Trust
-----
1        yes
2        no
....
```

26.2.5 Configure static Dynamic ARP Inspection

By default there is not static ARP binding table rule configured on the equipment. Use the commands below to add static ARP binding table rule. If static ARP binding table configuration function is not enabled, the configured static binding table will not take effect immediately until the function is enabled.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	ip arp-inspection binding A.B.C.D [HHHH.HHHH.HHHH] [vlan vlanid] port port-id	Configure static ARP binding table rule
3	exit	Quit from global configuration mode and enter privileged EXEC mode
4	show ip arp-inspection binding	Show all the DAI binding rules in binding table

The example below shows how to configure static ARP binding table rule:

```
Raisecom (config)# interface port 1
```

```
Raisecom (config-port)# ip arp-inspection binding 192.168.0.1 001A.A00F.9A81 vlan 1 port 1
```

Use **show** to configure if the configuration is correct:

```
Raisecom# show ip arp-inspection binding
```

Ip Address	Mac Address	VLAN	Port	Type	Inhw
192.168.0.1	001A.A00F.9A81	1	1	static	yes

Current Rules Num: 1
History Max Rules Num: 1

26.2.6 ARP Packets Rate-limit Default Configuration

Function	Default
Port ARP packet rate-limit function	Disable
Port ARP Packets rate-limit	100
ARP Packets rate-limit auto-recovery function	Disable
Recovery time of Auto-recovery function	30

26.2.7 ARP Packets Rate-limit Port Configuration

By default, port does not enable ARP packets rate-limit function. By configuring the following command under port mode, you can open port ARP packets rate-limit function.

Configuration steps are as follows:

Step	Command	Description
1	Config	Enter global configuration mode
2	interface port 1	Enter port configuration mode
3	ip arp-rate-limit rate rate-value	Configure ARP packets rate-limit which is allowed by port.
4	ip arp-rate-limit enable	Open port ARP packets rate-limit.
5	exit	Back to global configuration mode

6	exit	Back to privilege mode
7	show ip arp-rate-limit	Show ARP packets rate-limit configuration information and port overspeed status.

The following example shows how to configure port ARP packets rate-limit function:

```
Raisecom (config)# interface port 1
Raisecom (config-port)# ip arp-rate-limit rate 20
Raisecom (config-port)# ip arp-rate-limit enable
```

Use command **show** to view configuration:

```
Raisecom#show ip arp-rate-limit
arp rate limit auto recover: disable
arp rate limit auto recover time: 30 second
Port      Enable-Status     Rate(Num/Sec)      Overload
-----
1        Enabled            20                  Yes
2        Disabled           100                 No
3        Disabled           100                 No
4        Disabled           100                 No
.....
26       Disabled           100                 No
```

26.2.8 ARP Packets rate-limit global configuration

By default, the rate-limit auto-recovery functions of ARP packets disable. By carrying out the following command under global mode, you can enable auto-recovery function.

The configuration steps are as follows:

Step	Command	Description
1	Config	Enter global configuration mode
2	ip arp-rate-limit recover time time-value	Set the recovery time of auto-recovery function
3	ip arp-rate-limit recover enable	Enable auto-recovery function
4	exit	Exit global configuration mode and enter privilege user mode.
5	show ip arp-rate-limit	Show ARP packets rate-limit configuration information.

The following example shows how to enable ARP packets rate-limit auto-recovery function:

```
Raisecom (config)# ip arp-rate-limit recover time 60
Raisecom (config)# ip arp-rate-limit recover enable
```

Use command **show** to view configuration:

```
Raisecom#show ip arp-rate-limit
arp rate limit auto recover: enable
```

<i>arp rate limit auto recover time: 60 second</i>			
<i>Port</i>	<i>Enable-Status</i>	<i>Rate(Num/Sec)</i>	<i>Overload</i>
1	<i>Enabled</i>	20	<i>Yes</i>
2	<i>Disabled</i>	100	<i>No</i>
3	<i>Disabled</i>	100	<i>No</i>
4	<i>Disabled</i>	100	<i>No</i>
.....			
26	<i>Disabled</i>	100	<i>No</i>

26.3 Monitoring and maintenance

Use **show** to show DAI running and configuration state.

Command	Description
show ip arp-inspection	Show ARP inspection global configuration and port ARP trust configuration
show ip arp-inspection binding [port port-id]	Show DAI binding table

Show ARP inspection global configuration and port ARP trust configuration

```
Raisecom#show ip arp-inspection
Static Config ARP Inspection: Enable
DHCP Snooping ARP Inspection: Enable
ARP Inspection Protect Vlan: All
Bind Rule Num : 0
Vlan Acl Num : 0
Remained Acl Num : 512
Port      Trust
-----
1        no
2        no
```

Show Dynamic ARP Inspection binding table:

```
Raisecom# show ip arp-inspection binding
Ip Address      Mac Address      VLAN      Port      Type      Inhw
-----
192.168.0.1    001A.A00F.9A81    1         1         static     yes
Current Rules Num: 1
History Max Rules Num: 1
```

You can view ARP packets rate-limit function configuration and running status information by command **show**

Command	Description
----------------	--------------------

show ip arp-rate-limit

Show ARP packets rate-limit function configuration and status information

Show ARP packets rate-limit function global configuration information, port configuration information overspeed status.

Raisecom#**show ip arp-rate-limit**

arp rate limit auto recover: enable

arp rate limit auto recover time: 60 second

Port	Enable-Status	Rate(Num/Sec)	Overload
1	Enabled	20	Yes
2	Disabled	100	No
3	Disabled	100	No
4	Disabled	100	No
.....			
26	Disabled	100	No

When the number of ARP packets is more than specific rate, the parameter of overload will show **Yes**, or **No**.

26.4 Typical configuration example

Enable DHCP Snooping binding table learning function on the switch, and the switch will inspect the received ARP messages on port, and compare it with the content of DHCP Snooping module binding table, the ARP messages that satisfy the binding condition will be allowed to pass, while the ones that do not will be dropped.

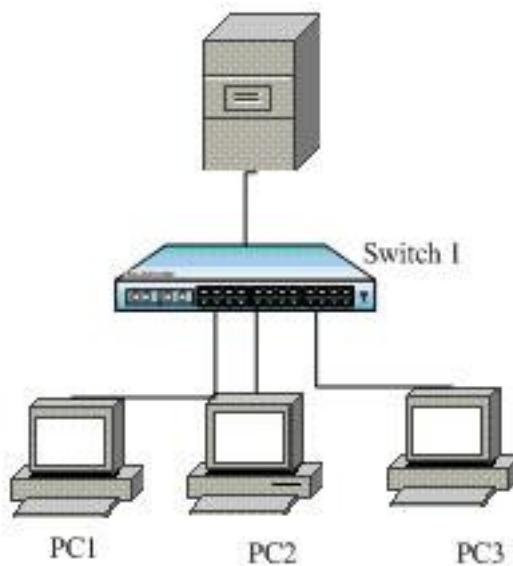


Fig 26-1 Dynamic ARP Inspection typical usage topology

Configuration steps:

! Enable DHCP Snooping on the access switch:

Raisecom (config)# **ip dhcp snooping**

! Configure the access switch uplink port to DHCP Snooping trust port

Raisecom(config-port)#**ip dhcp snooping trust**

! Configure the access switch uplink port to ARP trust:

Raisecom(config-port)#**ip arp-inspection trust**

! Configure the access switch dynamic ARP inspection

Raisecom(config)#**ip arp-inspection dhcp-snooping**

In order to prevent attacking from sending a large number of ARP packets, you can enable ARP rate-limit function in switch port, then switch will detect ARP packets number which is received per second, if the received ARP packets number per second on the corresponding port is overthreshold, the port will be attacked and switch will discard all ARP packets of this port. At the same time, you can set auto-recovery function, then switch will recover port after auto-recovery time timeouts so that ARP packets can continue to go through.

Configuration steps:

! set ARP packets rate which ARP packets rate-limit allowed on the input switch relevant port

Raisecom (config-port)# **ip arp-rate-limit rate 20**

! enable ARP rate-limit function on the input switch relevant port

Raisecom (config-port)# **ip arp-rate-limit enable**

! set ARP packets rate-limit recovery time of auto-recovery function

Raisecom(config)#**ip arp-rate-limit recover time 60**

!enable ARP packets rate-limit auto-recovery function

Raisecom(config)#**ip arp-rate-limit recover enable**

Chapter 27 IP Source Guard Configuration

27.1 IP Source Guard principle overview

Without authentication, a way to handle IP address embezzlement is IP source guard. IP source guard can cooperate with DHCP snooping and build up dynamic binding relationship, manually configuring stable binding relationship is also available. DHCP snooping provides a kind of safety feature by creating and maintaining a DHCP binding database to filtrate the unauthentic DHCP messages. It makes sure the validness by starting DHCP snooping. That is to say, all the DHCP OFFER are sent out from DHCP Server, not faked. With this guarantee IP source guard can be used to prevent IP embezzlement.

IP source guard's realization is based on IP source binding table to implement the IP traffic constraint on the port, only the source IP in the binding table is allowed to pass, while others can not.. IP source binding table can be learned dynamically (through DHCP Snooping), or by stable configuration.

The message feature items that IP Source Guard supports include: source IP address, source MAC address, VLAN. The combination of a port and the following feature item is supported:

- IP
- IP+MAC
- IP+VLAN
- IP+MAC+VLAN

27.2 Configure IP Source Guard

27.2.1 Default IP Source Guard configuration

By default IP Source Guard configuration is as follows:

Feature	State
Stable binding function	disable
Dynamic binding function	disable
Port credit state	no

27.2.2 Enable/disable global stable binding function

By default, IP Source Guard global stable binding function is disabled. When it is disabled, the stable binding relationship don not affect the hardware, and the binding relationship is not available. Only when global stable binding function is enabled can the stable binding relationship take effect.

Step	Command	Description
1	config	Enter global configuration mode
2	ip verify source	Enable static binding function
3	exit	Return to privileged EXEC mode

4	show ip verify source	Show static/dynamic banding function and port credit state
----------	------------------------------	--

For example: Raisecom (config) # **ip verify source**

Use **no ip verify source** can close global static banding function.

27.2.3 Enable/disable global dynamic binding function

By default, IP Source Guard global dynamic binding function is disabled. When it is disabled, the dynamic binding relationship learned from DHCP SNOOPING module does not affect the hardware, and the binding relationship is not available. Only when global dynamic binding function is enabled can dynamic binding relationship take effect.

Step	Command	Description
1	config	Enter global configuration mode
2	ip verify source dhcp-snooping	Enable dynamic binding function
3	exit	Return to privileged EXEC mode
4	show ip verify source	Show static/dynamic banding function and port credit state

For example: Raisecom (config) # **ip verify source dhcp-snooping**

Use **no ip verify source dhcp-snooping** can close global dynamic banding function.

27.2.4 Configure port credit state

By default, port is in unauthentic state, when all the IP messages except DHCP message or these according to binding relationship can not be transmitted. When a port is in credible state, all the messages can be transmitted normally. The commands to configure port credit state are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>port_id</i>	Enter the figure of one port
3	ip verify source trust	Set the port to credible state
4	no ip verify source trust	Set the port to incredible state
5	exit	Return to global configuration mode
6	exit	Return to privileged EXEC mode
7	show ip verify source	Show static/dynamic banding function and port credit state

For example:

Raisecom(config)# **interface port 10**

Raisecom(config-port)# **ip verify source trust**

```
Raisecom(config-port)# no ip verify source trust
```

27.2.5 Configure stable binding relationship

Stable binding relationship can be configured manually, and the static binding relationship can cover the dynamic binding relationship that has the same IP. When the stable binding relationship is deleted manually, the system will recover to the stable binding relationship that has the same IP (if it exists). If the binding relationship that does not exist is deleted, the system will take it as successful operation.

Step	Command	Description
1	config	Enter global configuration mode
2	ip source binding ip-address [mac-address] [vlan vlanid] port port-id	Set stable binding relationship
3	no ip source binding ip-address	Delete stable binding relationship
4	exit	Return to privileged EXEC mode
5	show ip source binding [port port-id]	Show the banding list in the switch

For example:

```
Raisecom(config)# ip source binding 1.2.3.4 port 10
Raisecom(config)# ip source binding 10.10.1.5 1234.1234.1234 port 10
Raisecom(config)# ip source binding 100.1.101.50 5678.5678.5678 vlan 100 port 10
Raisecom(config)# no ip source binding 1.2.3.4
Raisecom(config)# no ip source binding 100.1.101.50
```

27.2.6 Transfer dynamic binding relationship to static binding

To transfer dynamic binding relationship to static binding, when deleting static binding relationship by manual, system automatically recover to dynamic binding relationship with identical IP (if there is one).

Step	Command	Description
1	config	Enter global configuration mode
2	ip source binding dhcp-snooping static	Transfer dynamic binding to static binding relationship.
3	no ip source binding ip-address	Delete static binding IP.
4	exit	Return to Privileged EXEC mode.
5	show ip source binding [port port-id]	Show the banding list in the switch

Example: Raisecom(config)# ip source binding dhcp-snooping static

27.2.7 Enable/disable auto-update to static binding

After enabling this switch, the dynamic binding IP learned by dhcp-snooping will auto-update to static binding.

Step	Command	Description
1	config	Enter global configuration mode
2	[no] ip source binding auto-update	Enable/disable auto-update function.
3	exit	Return to Privileged EXEC vmode.
4	show ip source binding [port port-id]	Show the banding list in the switch

Example: Raisecom(config)# **ip source binding auto-update**

27.3 Monitoring and maintenance

Use the **show** commands to look over the running state and configuration state of IP Source Guard for monitoring and maintaining. The **show** commands are shown as follows:

Command	Description
show ip source binding [port port-id]	Show the binding relationship table of the switch
show ip verify source	Show stable/dynamic binding and port credit state

Raisecom#**show ip verify source**

Static Bind: Enable
Dhcp-Snooping Bind: Enable
Port Trust

1	yes
2	no
3	no
4	no
5	no
6	no
7	no
8	no
9	no
10	yes
11	no
12	no
13	no
14	no
15	no

```

16    no
17    no
18    no
19    no
20    no
21    no
22    no
23    no
24    no
25    no
26    no
27    no
28    no

```

Raisecom#

Raisecom#show ip source binding

History Max Entry Num: 6

Current Entry Num: 6

<i>Ip Address</i>	<i>Mac Address</i>	<i>VLAN</i>	<i>Port</i>	<i>Type</i>	<i>Inhw</i>
2.2.2.3	--	--	10	static	no
1.2.3.4	--	--	10	static	no
10.10.1.5	1234.1234.1234	--	10	static	no
100.1.101.50	5678.5678.5678	100	10	static	no
2.3.5.8	--	--	13	static	yes
1.3.5.8	--	10	22	static	yes

Raisecom#show ip source binding port 10

<i>Ip Address</i>	<i>Mac Address</i>	<i>VLAN</i>	<i>Port</i>	<i>Type</i>	<i>Inhw</i>
2.2.2.3	--	--	10	static	no
1.2.3.4	--	--	10	static	no
10.10.1.5	1234.1234.1234	--	10	static	no
100.1.101.50	5678.5678.5678	100	10	dhcp-snooping	no

Raisecom#

27.4 Typical configuration example

➤ Destination

The switch allows all IP packets in port 10 to pass. The port 3 allows IP packets which is specified as 10.10.10.1 and accords with dynamic banding relationship that dhcp snooping module learnt to pass. The other port allows IP packet which dhcp snooping accords with dynamic banding relationship that dhcp snooping module learnt to pass.

- Configuration steps

```
Raisecom(config)# ip verify source
Raisecom(config)# ip verify source dhcp-snooping
Raisecom(config)# interface port 10
Raisecom(config-port)# ip verify source trust
Raisecom(config-port)# exit
Raisecom(config)# exit
Raisecom# show ip verify source
Raisecom# config
Raisecom(config)# ip source binding 10.10.10.1 port 3
Raisecom(config)# exit
Raisecom# show ip source binding
```

27.5 IP Source Guard command list

Command	Description
[no] ip source binding <i>ip-address</i> [mac-address] [vlan <i>vlanid</i>] port <i>port-id</i>	[cancel] the binding based on port
show ip source binding [port <i>port-id</i>]	Show the configured port binding
[no] ip verify source dhcp-snooping	The switch of global dynamic binding function
[no] ip verify source	The switch of stable binding function
[no] ip verify source trust	Bind enable switch in the port
show ip verify source	Show stable/dynamic and port credit state

Chapter 28 Unicast Router Configuration Guide

28.1 Routing Overview

28.1.1 Overview

If there is no L3 device between VLANs, the devices which are in different VLAN can not communicate with each other. There are three kinds of routing.

- Default routing;
- Static routing;
- Dynamic routing.

A default routing is a special routing. You can configure a default routing using a static routing.

A static routing is a special routing configured manually by an administrator.

The advantage of static routing that it's safe and saves bandwidth, but can not adapt the dynamic change of network topology structure, like link invalidation and so on, so it may cause the destination unreachable. As network topology spreads, static routing will cost much time and energy.

Routing use dynamic routing protocol, which is able to compute the best routing for data stream. There are two types of dynamic routing protocol:

1. Use distance vector protocol to maintain routing table, it takes the distance of network resource as the computing evidence, and it can send routing table to neighbours periodically. Distance vector protocol uses one or one serious metric to compute the best routing, which makes it more convenient for configuration and usage.
2. Use link state protocol to maintain the data-base of network topology, that is to exchange link state announces (LSAs) among routings for maintenance. Sending LSAs is touched off by incidents, like constringency timer overtime or receiving request timer overtime. Link state protocol is able to answer the topology changes rapidly, but it needs more bandwidth and resources compared with distance vector protocol.

The distance vector protocol that ISCOM three-layer switch supports is RIP, which uses metric to choose the best routing. At the same time, the switch also supports open frame shortest path first link state protocol.

In some network environment, VLAN connects to different network or subnet. In IP network, each subnet is mapped to a signal VLAN. VLAN configuration is about to control the size of broadcasting domain. However, when one VLAN end needs to communicate with the end in another terminal, the communication between VLAN- routing among VLAN is needed. You can configure one or more routing to transmit data stream to each destination VLAN.

Figure 1-1 shows basic routing topology structure, switch A is in VLAN 1, switch B is in VLAN 2, routing has a port in each VLAN. When host A in VLAN 1 needs to communicate with host B in VLAN 1, it sends out a data packet, the destination address is host B, the switch will transmit the data packet directly to host B, without sending to routing. When host A sends data packet to host C in VLAN 2, switch A will transmit the data packet to routing. The routing will receive the packet on the port in VLAN 1, check out routing table, choose the correct outgress port, and send the data packet

to the port of switch B on VLAN 2. Switch B will receive the data packet and transmit it to host C.

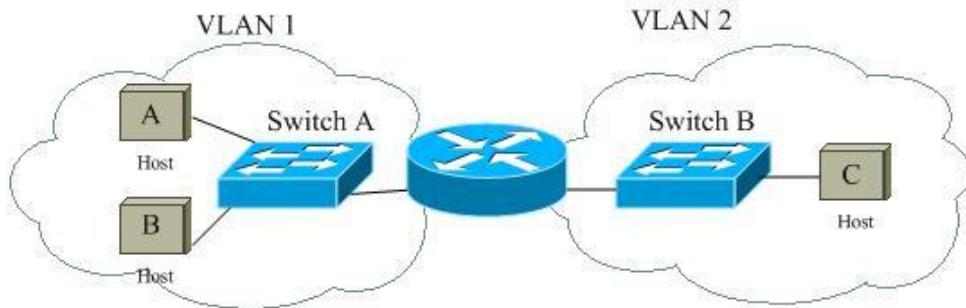


Fig 28-1 basic routing topology structure

28.2 Static Routing Configuration

28.2.1 Static routing overview

Static routing

Static routing is a special routing, it is manually configured by the administrator. By configuring static routing a communicating network can be established.

The advantage of static routing is safety and bandwidth saving. In the network with simple structure, it is only needed to configure static routing to make routing work, proper configuration and usage of static routing can improve the performance of network and offer enough bandwidth for important application. However, static routing can not adapt the dynamic change of network topology structure automatically, like unavailable link, so it may the destination is unreachable. As the growth of network topology, static routing will waste more and more time and energy.

Default routing

Default routing is a special routing. In brief, default routing is the routing that will be used only when there is no corresponding table item. That is, only when there is no proper routing, can default routing be used. In the routing table, default routing can appear with the address 0.0.0.0 (mask 0.0.0.0). Use **show ip routing** to check out if it is configured. If the destination address can not match up with any table item in the routing table, the message will be selected as default routing. If there is no default routing while the message destination is not in the routing table, then when the message is dropped, a ICMP message will be returned to the source end to report that the destination or network is unreachable.

28.2.2 Configure static routing

Default static routing configuration

Function	Default value
Static routing	Empty
Default routing	empty

Configure static routing

Sometimes, for simple network, the administrator can configure static routing manually. The process is as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	ip routing 10.0.0.0 255.0.0.0 192.168.1.1	Set the IP address of the next hop to destination network 10.0.0.0 is 192.168.1.1
3	exit	Return to privileged EXEC mode
4	show ip routing	Show routing table
5	config	Enter global configuration mode
6	no ip routing 10.0.0.0	Delete the routing in 10.0.0.0 network
7	exit	Return to privileged EXEC mode
8	show ip routing	Show routing table

When using **no ip routing**, network mask can be designated, and it can be undesignated to default mask. The next hop of routing must be the routing in the straight-through network.

Default gateway configuration

When a message that is needed for transmission do no find the destination network routing, use **ip default-gateway** to let the system transmit all the messages to default gateway. The steps are shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	ip default-gateway 192.168.1.1	Configure default gateway
3	exit	Return to privileged EXEC mode
4	show ip routing	Show routing table
5	config	Enter global configuration mode
6	no ip default-gateway	Cancel default gateway configuration
7	exit	Return to privileged EXEC mode
8	show ip routing	Show routing table

Notice: For successful configuration, configure IP address is needed first, or configuring default gateway will be failed.

28.3 Monitoring and maintenance

Show routing table commands:

Command	Description
show ip routing	Show routing table

Chapter 29 802.3ah OAM Function Configuration

29.1 802.3ah OAM Principle Introduction

IEEE802.3ah OAM (Operation Administration Maintenance) is used to provide more efficient Ethernet link operation, management and maintenance. As the efficient complimentarily of the high managing tool, OAM enhances the Ethernet management and monitoring.

29.1.1 OAM mode and discovery

The process of Ethernet OAM connecting is also called Discovery, which is the process of one OAM entity discovers another one in the remote device for creating a stable conversation.

In the process, the connected Ethernet OAM (OAM Function port) entity sends the Ethernet configuration information and local node support Ethernet OAM ability information by switching the information OAM PDU to the opposite in two way. Once OAM receives the configuration data from the opposite, it will decide whether build the OAM connection up. If both ends are agreed to build up the OAM connections, Ethernet OAM protocol will start to run on the LAN Layer.

There are two modes for building up Ethernet OAM connection: active mode and passive mode. The connection can only be active by OAM entity and passive OAM entity has to wait for the connecting request from the opposite OAM entity.

After the Ethernet OAM is connected, OAM entities from both ends send information OAMPDU to keep the connection. If the Information OAMPDU is not received by the OAM entity from opposite in 5 seconds, it will be considered as connection time-out. Thus OAMs are needed to reconnect.

Information OAMPDU packet is sent by internal counter control with maximum rate of 10 packets/second.

29.1.2 OAM loop-back

OAM loop-back can only be achieved after Ethernet OAM connection is built up. In connected situation, active mode OAM will send OAM loop-back command and opposite will response for that command. As remote is in loop-back mode, all packets but OAMPDU packet will be sent back in the original route.

Periodical loop-back detection can detect network failure on time and find out the failure happened location by subsection loop-back detection. It can help users to remove failure.

29.1.3 OAM events

It is difficult to detect the Ethernet failure, especially when the physical network communication is in no-breakdown but low network. OAMPDU states a Flag Domain which allows Ethernet OAM entity sends the failure information to the opposite. That Flag also states the threshold events as

shown below:

- Link Fault: Signal lost in the opposite link.
- Dying Gasp: Unpredict states happen, as power cut-down.
- Critical Event: Uncertain critical events happen.

Ethernet OAM connecting process is continually sending the Information OAMPDU. Local OAM entity can send the local threshold event information to opposite OAM entity through Information OAMPDU. The Administrators can always notice the link status and solve the related problems on time.

Ethernet OAM monitors the link by Event Notification OAMPDU switchs. Once the link fails, the local link will monitor the failure. And it will send monitors the Event Notification OAMPDU to opposite Ethernet OAM entity to inform the threshold events. Administrator can notice the network status by monitoring the link.

- Error frame event: error frame number in unit time is over stated threshold number.
- Error frame period event: states frame number N as a period; it means in the period of received N error frames, the error fame number is over stated threshold one.
- Error frame second event: indicated in M seconds, the error frame's time in seconds are over the stated threshold number.(error frame second states: an error frame happens in a specific second and this second is called error frame second.)

29.1.4 OAM mib

Devices can gain opposite device link configuration/ statistics value through OAM and then get link status/ data.

29.2 802.3ah OAM Mode Configuration

OAM supports two modes: active mode and passive mode. Active mode starts OAM opposite discover process, supports functions but non-response remote loop-back command and variable gained requests; passive mode does not start OAM opposite discover process, does not send remote loop- back command and veriable gained request. Different devices use different mode supports and default configurations. If the device supports passive mode, then its default mode will be passive mode or it will be active mode. If the device only supports one mode, then it does not support mode configuration.OAM mode is all OAM port link share, and users can set mode configuration on the devices which support both two mode as shown below:

Steps	Command	Description
1	config	Entry global configuration mode
2	oam {active/passive}	Set OAM as active/passive mode
3	Exit	Return to privilege use mode
4	show oam	Show OAM loop-back information

Set device OAM as active mode:

Raisecom#**config**

Raisecom(config)#**oam active**

Raisecom(config)#**exit**

Raisecom#**show oam**

29.3 802.3ah OAM Active Mode Function

29.3.1 OAM default configuration

Function	Default Value
OAM Enable\Disable	Enable
Opposite OAM event alarm	Disable

29.3.2 OAM enable/disable configuration function

➤ OAM Enable\Disable

OAM is Ethernet point to point link protocol. Enable/Disable is used for all the link ports. In default situation, all ports OAM are Enable, user can Enable/ Disable OAM by the following steps:

Steps	Command	Description
1	Config	Entry global configuration mode
2	interface port <i>port_number</i>	Entry Ethernet physical interface mode <i>port_number</i> : physical interface number
3	oam { disable / enable }	Enable or Disable OAM
4	Exit	Return Global Configuration mode
5	Exit	Return privileged EXEC mode
6	show oam	Show OAM Configuration state

Disable port 2 OAM:

Raisecom#**config**

Raisecom(config)#**interface port 2**

Raisecom(config-port)#**oam disable**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

➤ Show OAM local link status

Privilege mode command: show oam can display OAM link local configuration and status include mode configuration, management status, working status, maximum packet length, configuration version and function support, etc. Through this command, users can understand OAM link configuration, running status, etc.

Raisecom#**show oam**

Port: 1
Mode: Passive
Administristrate state: Enable
Operation state: Disabled
Max OAMPDU size: 1518
Config revision: 0
Supported functions: Loopback, Event, Variable

Port: 2
Mode: Passive
Administristrate state: Disable
Operation state: Disable
Max OAMPDU size: 1518
Config revision: 0
Supported functions: Loopback, Event, Variable

➤ Show OAM opposite link status

Privilege mode command: show oam peer can display the opposite device information on OAM link, include: opposite MAC address, manufactory OUI, manufactory information, mode configuration, maximum packet length, configuration version and function support information. If OAM link is not connected, then there no information will be displayed.

Raisecom#**show oam peer**

Port: 1
Peer MAC address: 000E.5E00.91DF
Peer vendor OUI: 000E5E
Peer vendor info: 1
Peer mode: Active
Peer max OAMPDU size: 1518
Peer config revision: 0
Peer supported functions: Loopback, Event

29.3.3 Run OAM loop-back function

OAM provide link layer remote loop-back system, which can be used for located link error position, performance and quality test. Under link loop-back status, devices will loop-back all link received packets to the opposite devices except OAM packet. Local device uses OAM remote command to enable or disable remote loop-back. Opposite device will use loop-back configuration command to control whether response loop-back command.

In central office end , users can build up remote loop-back through remote loop-back command.

Steps	Command	Description
1	config	Entry global configuration mode

2	interface port <i>port_number</i>	Entry Ethernet physical interface mode, <i>port_number</i> is physical interface number
3	oam remote-loopback	Build up remote loop-back
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show oam loopback	Show OAM loop-back situation

Build remote loop-back on port link 2:

```
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)#oam remote-loopback
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam loopback
```

Users can remove remote loop-back as below:

Steps	Command	Description
1	Config	Entry global configuration mode
2	interface port <i>port_number</i>	Entry Ethernet physical interface mode <i>port_number</i> is physical interface number
3	no oam remote-loopback	Remove remote loop-back
4	Exit	Return global configuration mode
5	Exit	Return privileged EXEC mode
6	show oam loopback	Show OAM loop-back state

Remote loop-back on remove end link 2:

```
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)#no oam remote-loopback
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam loopback
```

Note:

- Remote loop-back only can be achieved after Ethernet OAM is connected.
- Except for OAM packets, all other packets are loopbacked.
- In loopback port, it only allows OAM packets to hand CPU
- Loopback port is prohibited forwarding packets to other ports

- The other ports are prohibited forwarding packets to loopback port

29.3.4 Opposite OAM event alarm function

By default, when opposite link monitor event is received, device will not inform network managing center through SNMP TRAP. Users can use Enable/Disable opposite monitor events is informed to the network managing center.

Steps	Command	Description
1	config	Entry global configuration mode
2	interface port <i>port_number</i>	Entry Ethernet physical interface mode <i>port_number</i> is physical interface number
3	oam peer event trap {disable / enable}	Enable or Disable opposite OAM monitor event is informed network managing center
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show oam trap	show OAM TRAP information

Enable port 2 opposite link monitoring event informed to network managing center:

```
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)# oam peer event trap enable
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam trap
```

29.3.5 View opposite IEEE 802.3 Clause 30 mib

OAM variable gain is a link monitoring measure. It allows local device to get opposite device current variable value thus get current link status. IEEE802.3 Clause30 particularly states the variables which support OAM gain and their representing way. Variable can be divided into its biggest unit -- object which include package and attribute. Package also is combined by several attribute. Attribute is variable's smallest unit. OAM variable gain uses Clause 30 to state object/package/attribute's branch described requesting objects. And branches plus the variable value are used to represent object response variable request. Now, all devices have supported both OAM information and port statistics as object variable gain. EPON OLT device also supports MPCP and OMPEmulation object information gain.

When device OAM work as active mode, users can gain opposite devices OAM information or port statistics variable values as the steps below:

Steps	Command	Description
-------	---------	-------------

1	show oam peer {link-statistics oam-info} {port-list client line} port_number	Gain opposite device OAM information or port statistics variable value <i>port_number</i> : physical interface number
---	---	--

Gain port 2 opposite device OAM information value is shown as below:

Raisecom(debug)#**show oam peer oam-info port-list 2**

Note: OAM variable gain is only achieved if and only if Ethernet OAM connection is built up.

29.3.6 OAM statistics clear function

OAM calculates the number of all different types of OAM packets which are sent/received on each OAM port link. The types of packets are: information, link event information, loop-back control, variable gain request, variable gain response, organise using, uncertain type and repeated event information. Users can clear port link OAM statistics information as follow steps:

Steps	Command	Description
1	config	Entry global configuration mode
2	interface port <i>port_number</i>	Entry Ethernet physical interface mode <i>port_number</i> : physical interface number
3	clear oam statistics	Clear OAM port link statistics information
4	exit	Entry global configuration mode
5	exit	Return to privileged EXEC mode
6	show oam statistics	show OAM link statistics information

Clear port 2 OAM link statistics information as below:

Raisecom#**config**

Raisecom(config)#**interface port 2**

Raisecom(config-port)#**oam clear statistics**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#**show oam statistics**

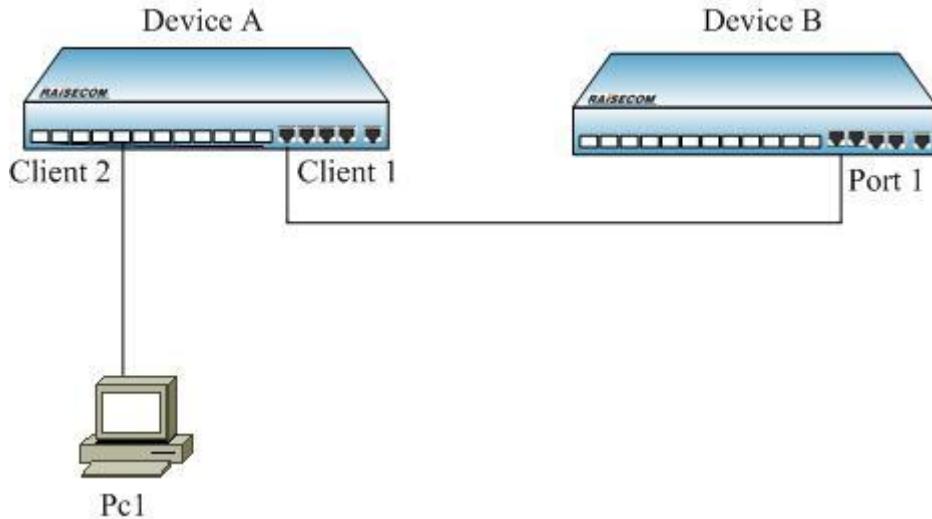
29.3.7 Monitoring and maintenance

Command	Description
show oam	show OAM link's local configuration and status
show oam peer	show OAM link's opposite device information
show oam loopback	Show remote loop-back information

show oam peer event	show opposite device informed event
show oam trap	Show OAM related SNMP TRAP information and its configuration situation.
show oam statistics	show all OAM port link statistics information

The command which is showed above supports based-on port, the format is same as [port-list *port-list*]

29.3.8 Configuration example



As figure above, to set remote loop-back as following configuration:

```

Raisecom#config
Raisecom (config)#interface port 1
Raisecom(config-port)#oam enable
Raisecom(config-port)#exit
Raisecom#show oam port-list 1
  
```

Port: 1
Mode: Active
Administrative state: Enable
Operational state: Operational
Max OAMPDU size: 1518
Config revision: 0
Supported functions: Loopback, Event

```

Raisecom#config
Raisecom (config)#interface port 1
Raisecom(config-port)#oam remote-loopback
Raisecom(config-port)#exit
  
```

```
Raisecom(config)#exit
Raisecom#show oam loopback
```

Port: 1
Loopback status: Remote
Loopback react: Ignore

29.4 802.3ah OAM Passive Function

29.4.1 OAM default configuration

Function	Default Value
Oam Enable\Disable	Enable
Oam mode	Passive
Response\Ignore opposite oam loop-back Configuration	Response
Local oam event alarm	Disable
Oam failure indication	Enable
Error frame periodical event window and threshold.	window 1 (s) Threshold 1 (unit)
Error frame event window and threshold	Window 1 (s) Threshold 1 (unit)
Error frame second statistics event window and threshold	Window 60 (s) Threshold 1 (unit)
Symbol error event window and the threshold	Window 1 (s) Threshold 1 (unit)

29.4.2 OAM enable/disable configuration

❖ OAM Enable\Disable

OAM is Ethernet point to point link protocol, Enable/Disable is for different link port. In default situation, all ports OAM are Enable. Users can enable/disable OAM by following steps:

Steps	Command	Description
1	config	Entry global configuration mode
2	interface {line client} port_number	Entry Ethernet physical interface mode <i>port_number</i> : physical interface number
3	oam {disable / enable}	Enable or Disable OAM
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show oam	show OAM configuration situation

Disable port 2 OAM as follow:

Raisecom#**config**

```
Raisecom(config)#interface port 2
Raisecom(config-port)#oam disable
Raisecom(config-port)#exit
Raisecom(config)#exit
```

➤ Show OAM local link status

Privileged EXEC mode command: show oam can show OAM link local configuration and status, displayed information is include mode configuration, managing status, running status, maximum packet length, configuration version and function support information. By this command, users can understand OAM link configuration, running status such information.

Raisecom#**show oam**

```
Port: 1
Mode: Passive
Administrative state: Enable
Operation state: Disabled
Max OAMPDU size: 1518
Config revision: 0
Supported functions: Loopback, Event, Variable
```

```
Port: 2
Mode: Passive
Administrative state: Disable
Operation state: Disable
Max OAMPDU size: 1518
Config revision: 0
Supported functions: Loopback, Event, Variable
```

➤ Show OAM opposite link status

Privileged EXEC mode command: show oam peer can show OAM link's opposite device information, include opposite MAC address, manufactory OUI, manufactory information, mode configuration, maximum packet length, configuration version and function support information. If OAM link is not built up, then it will not show any information.

Raisecom#**show oam peer**

```
Port: 1
Peer MAC address: 000E.5E00.91DF
Peer vendor OUI: 000E5E
Peer vendor info: 1
Peer mode: Active
Peer max OAMPDU size: 1518
Peer config revision: 0
```

Peer supported functions: Loopback, Event

29.4.3 Response/ignore opposite OAM loop-back configuration function

OAM provide link layer remote loop-back system, can be used for locating link error position, function and quality testing. In link loop-back status, all packets received from the link but OAM packet loop-back to opposite device. Local device use OAM remote loop-back command enable or disable remote loop-back, opposite device uses loop-back configuration command control to response loop-back command.

In default situation, device loop-back responses as Enable, users set loop-back response configuration as below:

Steps	Command	Description
1	config	Entry global configuration mode
2	interface {line client} port_number	Entry Ethernet physical interface mode <i>port_number</i> : physical interface number
3	oam loopback {ignore process}	Enable or Disable OAM loop-back response
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show oam loopback	show OAM loop-back situation

Disable response port link 2 OAM remote loop-back:

```
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)#oam loopback ignore
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam loopback
```

29.4.4 OAM link monitor configuration function

OAM link monitor is used to detect and report different link errors. When link errors are detected, device informs opposite error cause time, window and threshold configuration by OAM event information packets. Opposite reports events to network managing center by SNMP TRAP. Local device reports events directly to network managing center by SNMP TRAP. OAM link monitoring supports events below:

Error frame events: indicates periodical error frames over threshold. When indicated time periodically error frames over threshold, device will have that event.

Error frame periodical event: lately N frames' error is over threshold, N is indicated value; once laterly N frames' error over threshold is detected, and device will release that event.

Error frame second statistics event: lately M seconds, the error frames' second number over threshold. M is the indicated value. When error frame second number is over indicated threshold in M seconds, device releases that event.

OAM named the previous monitoring period, frame calculate number and second statistics number as monitoring window.

Users can set the link monitoring configuration as steps below:

Steps	Command	Description
1	config	Entry global configuration mode
2	interface {line client} port_number	Enter Ethernet physical interface mode <i>port_number</i> : physical interface number
3	oam errored-frame window <1-60> threshold <0-65535>	Config error frame monitoring window and threshold <1-60>: monitoring window, unit is second. <0-65535>: threshold.
4	oam errored-frame-period window <100-60000> threshold <0-65535>	Config error frame periodical event monitoring window and threshold <100-60000>: monitoring window, unit is second. <0-65535>: threshold.
5	oam errored-frame-seconds window <10-900> threshold <0-65536>	Config error frame statistics monitoring window and threshold <10-900>: monitoring window, unit is second. <0-65536>: threshold.
6	oam errored-symbol-period window <1-60> threshold <0-65535>	Set the error code statistics event monitoring window and threshold <1-60>: monitoring window, unit is second <0-65535>: threshold, unit is one
7	exit	Return to global configuration mode
8	exit	Return to privileged EXEC mode
9	show oam notify	show OAM events configuration situation

Configuration port 2 error frame event monitoring window is 2 seconds, threshold is 8 error frame; error frame period event monitoring window is 100 ms, threshold is 128 error frames; error frame second statistics event monitoring window is 100 seconds, threshold is 8 seconds.

Raisecom#**config**

Raisecom(config)#**interface port 2**

Raisecom(config-port)# **oam errored-frame window 2 threshold 8**

Raisecom(config-port)# **oam errored-frame-period window 100 threshold 128**

Raisecom(config-port)# **oam errored-frame-second window 100 threshold 8**

Raisecom(config-port)#**exit**

```
Raisecom(config)#exit
Raisecom#show oam notify
```

Using physical layer interface configuration command **no oam errored-frame** can resume error frame event monitoring window and threshold as Default Value.

Using physical layer interface configuration command **no oam errored-frame-period** can resume error frame event monitoring window and threshold as Default Value.

Using physical layer interface configuration command **no oam errored-frame-second** can resume error frame event monitoring window and threshold as Default Value.

29.4.5 OAM fault indication function

OAM fault indication function is used to inform opposite device local device with abnormal event as link-fault, power break, abnormal temperature, etc. Those will cause the faults as link disable, device restart, ect. Now stated faults are link-fault, dying-gasp and critical-event caused by abnormal temperature. In default, device fault indicated as Enable status, thus when fault happened, device informs opposite by OAM. Users can Enable or Disable faults (except link-fault fault indicated must inform opposite) by following steps:

Steps	Command	Description
1	config	Entry global configuration mode
2	interface { line client } port_number	Entry Ethernet physical interface mode <i>port_number</i> is physical interface number
3	oam notify {dying-gasp / critical-event} {disable/enabl}	Enable or Disable OAM error indicated opposite
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show oam notify	show OAM event configuration situation

Disable port 3 critical-event fault indication:

```
Raisecom#config
Raisecom(config)#interface port 3
Raisecom(config-port)# oam notify critical-event disable
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam notify
```

29.4.6 Local OAM event alarm function

In Default, when link monitoring event is detected, device will not inform network managing center

by SNMP TRAP. Users can use Enable or Disable to inform network managing center the monitor events by following steps:

Steps	Command	Description
1	config	Entry global configuration mode
2	interface {line client} <i>port_number</i>	Entry Ethernet physical interface mode <i>port_number</i> :physical interface number
3	oam event trap {disable/enable}	Enable or Disable OAM monitoring event to inform network managing center
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show oam trap	show OAM TRAP information

Enable port 2 link monitoring event inform to network managing center:

```
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)# oam event trap enable
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam trap
```

29.4.7 IEEE 802.3 Clause 30 mib support

OAM variable gain is a link monitoring measure. It allows local device to gain opposite device lately variable value. Thus it can gain lately link status. IEEE802.3 Clause30 detailly states support OAM gain variable and its representation. Object is the biggest division of variable. Each object has package and attribute. Package is include many attribute. Thus attributes are the smallest variable unit. OAM variable gain states object/package/attribute branches description as request objects, and branches plus variable value are used to represent as object response variable request. Now, all devices can support OAM information and port statistics variable gain. EPON OLT device also supports MPCP and OMPEmulation object information gain.

When device OAM is in active mode, users can gain opposite device OAM information or port statistics variable value by following steps:

Steps	Command	Description
1	show oam peer {link-statistics oam-info} {client line} <i>port_number</i>	Gain opposite device OAM information or port statistics variable value <i>port_number</i> : physical interface number <i>link-statistic</i> link statistic <i>oam-info</i> oam information

Gain port 2 opposite device OAM information value:

Raisecom(debug)#show oam peer oam-info port-list 2

29.4.8 OAM statistics clear function

OAM statistics sending/receiveing all OAM packets number on each OAM port link. Packets types:information, link events information, loop-back control, variable gain request, variable gain response, organise using, uncertain type and repeat event inforamtion. Users can clear port link OAM statistics information as following steps:

Steps	Command	Description
1	config	Entry global configuration mode
2	interface {line client} port_number	Entry Ethernet physical interface mode <i>port_number</i> : physical interface number
3	clear oam statistics	Clear OAM port link statistics information
4	exit	Return to global Configuration mode
5	exit	Return to privileged EXEC mode
6	show oam statistics	show OAM link statistics information

Clear port 2 OAM link statistics information

```
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)#oam clear statistics
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam statistics
```

OAM record recent happening local and opposite link monitoring and fault (key) events. Users can clear port link OAM local and opposite events record as following steps:

Steps	Command	Description
1	config	Entry global configuration mode
2	interface { line client} port_number	Entry Ethernet physical interface mode <i>port_number</i> : physical interface number
3	clear oam event	Clear OAM port link event record
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show oam event	Show OAM link local event record

7	Show oam peer event	Show OAM link opposite event record
----------	----------------------------	-------------------------------------

Clear port 2 OAM link events record:

```
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)# clear oam event
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam event
Raisecom#show oam peer event
```

29.4.9 Monitoring and maintenance

Command	Description
show oam	Show OAM link local configuration and status
show oam peer	Show OAM link information on opposite device
show oam loopback	Show remote loop-back information
show oam event	Show local device happening events
show oam peer event	Show opposite device informing events
show oam notify	Show all OAM link local events informing configuration
show oam statistics	Show all OAM port link statistics information

29.4.10 Configuration example

Note: ISCOM2128EA-MA series products do not support client.

If response remote loop-back, device A can be configured as below:

```
Raisecom#config
Raisecom(config)#oam passive
Raisecom (config)#interface client 1
Raisecom(config-port)#oam enable
Raisecom (config-port)# oam loopback process
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam loopback
```

Port: client1

Loopback status: No

Loopback react: Process

Chapter 30 Extended OAM Configuration

30.1 Extended OAM principle overview

Extended OAM, using IEEE802.3ah OAM to manage and monitor the remote device. It is composed by 3 parts:

1. Get the attribute of remote device;
2. Upload and down file of remote device;
3. Manage extended OAM link state and statistic.

Extended OAM includes the followings:

- Get remote attribute: the extended OAM attribute can be used to get the remote attribute form the center site.
- Set remote device: config the remote device, including host name, enable and disable port, duplex, bandwidth, fault transfer etc.
- Set remote device network management parameter: can config remote device network management parameter, such as ip address, gateway, community parameter and management VLAN etc, then implement full management with SNMP protocol.
- Remote TRAP: when the port of remote device show LINK UP/DOWN, the remote device will send extended OAM notification fram to inform the center site, then the center device will send TRAP.
- Extended remote loopback: the remote optical port can be set loopback function, the function of whether to count repeatedly can be set.
- Reset remote device: send command to reset remote device.
- Other remote device function management: with the increasing of remote device, center device can manage more remote device with extended OAM function such as: SFP、Q-in-Q、Virtual Circuit diagnosis etc.
- Download remote file: the remote can get remote file from FTP/TFTP server. The file also can be send from the server to center device, then the remote device can get from the center device.
- Upload remote file: put the file to FTP/TFTP server, or from the remote device to center one, then put to server from the center device.
- Link statistic and management of extended OAM function.

Note: extended OAM link can only be established between center and remote site. The devices of two end must be set to master and passive, or the link can't be up.

30.2 Extended OAM management

30.2.1 Default extended OAM configuration

Function	Default configuration
Powered configuration request	Enable
Extended OAM notice	Enable
Remote end trap switch	open

30.2.2 Extended OAM configuration mode

To configure remote equipments on a local end equipment, you need to enter remote configuration mode. The steps to enter remote configuration mode are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} <i>portid</i>	Enter ethernet physical port mode <i>portid</i> : physical port ID
3	remote-device	Enter remote configuration mode

To configure remote equipment ports on local equipment, you need to enter remote interface configuration mode. The steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} <i>portid</i>	Enter ethernet physical port mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode
4	interface client <i>client-id</i>	Enter remote physical port configuration mode <i>Clinet-id</i> port ID

30.2.3 Remote equipment system configuration

Configure remote equipment system configuration, including configuring remote equipments' hostname, the maximum frame length, save and delete the configuration files.

The steps to configure remote equipment hostname and remote equipment maximum frame length are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} <i>portid</i>	Enter ethernet physical port mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode
4	hostname <i>HOSTNAME</i>	Configure remote equipment hostname <i>HOSTNAME</i> remote system network name
5	system mtu <1500-8000>	Configure remote equipment maximum frame length

6	show remote-device information	Show current remote equipment hostname and actual effective maximum frame length
----------	---------------------------------------	--

Note: configure the maximum frame length of remote equipment; the actual effective value may be different because of different remote equipment. For example, RC552-GE can configure remote maximum frame length to 1916 bytes or 1536 bytes. If the remote end is RC552-GE, and the configuration value is less than 1916, the effective value is 1536, or it is 1916.

The steps to save remote equipment configuration file is as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>portid</i> : physical port number
3	remote-device	Enter remote configuration mode
4	write	Save remote equipment configuration file

The steps to delete remote equipment configuration file is as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>portid</i> : physical port number
3	remote-device	Enter remote configuration mode
4	erase	Delete remote equipment configuration file

When executing the command to delete remote equipment configuration file, you need to confirm your operation.

Note:

- The operation to the configuration file is to save and delete the file on remote equipment, not to operate the local equipments file system.
- It takes a long time save and delete remote files, so when executing the command, there may be some unusual situations like OAM link breaking down.

30.2.4 Configure extended OAM protocol

The steps to enable/disable powered configuration request configuration are as follows:

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration
2	extended-oam config-request enable extended-oam config-request disable	Enable/disable powered configuration request <i>enable</i> : enable powered configuration request <i>disable</i> : disable powered configuration request
3	exit	Return to privileged EXEC mode
4	show extended-oam status	Show extended OAM link state

The steps to disable/enable sending extended OAM notices configuration are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	extended-oam notification enable extended-oam notification disable	Enable/disable sending extended OAM notice <i>enable</i> : enable sending extended OAM notice <i>disable</i> : disable sending extended OAM notice
3	exit	Return to privileged EXEC mode
4	show extended-oam notification	Show OAM informing frame enable configuration state

30.2.5 Configure remote equipment port

- Configure remote equipment port enable/disable

The steps to disable remote equipment ports are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>portid</i> : port physical ID
3	remote-device	Enter remote configuration mode
4	interface client client-id	Enter remote physical port configuration mode <i>client-id</i> : port ID
5	shutdown	Shutdown remote equipment port

In remote port configuration mode, use **no shutdown** to enable remote equipment port.

- Configure remote equipment port rate/duplex

The steps to configure remote equipment ports rate/duplex are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode
3	remote-device	Enter remote configuration mode
4	interface client client-id	Enter remote physical port configuration mode
5	speed {auto / 10/ 100 /1000 } duplex {full / half}	Configure port rate and duplex mode

When the equipment has 1000M optical port, we can configure optical port auto-negotiation function, the steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode
4	line-speed auto	Configure remote equipment optical port auto-negotiation

In remote configuration mode, use **no line-speed auto** to shutdown optical port auto-negotiation function.

Note: when remote equipment is configured port rate/duplex, there may be some unusual situations like OAM link breaking down.

- Configure remote equipment port stream control/speed control

The steps to enable/disable remote equipment stream control are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode
4	interface client client-id	Enter remote physical port configuration mode
5	flowcontrol {on/off}	Enable/disable remote equipment port stream control function

The steps to configure remote equipment port in/out direction bandwidth are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode
4	rate-limit line line-id ingress rate rate-limit client client-id ingress rate	Configure remote equipment port in direction bandwidth <i>Line-id</i> line port ID <i>Client-id</i> client port ID <i>Rate</i> bandwidth
5	rate-limit line line-id egress rate rate-limit client client-id egress rate	Configure remote equipment port out direction bandwidth

Run **no rate-limit line line-id ingress** or **no rate-limit client client-id ingress** to restore in remote configuration mode.

Run **no rate-limit line line-id egress** or **no rate-limit client client-id egress** to restore in remote configuration mode.

- Configure remote equipment port description

The steps to configure remote port information are as follows:

Step	Command	Description
1	config	Enter global configuration
2	interface {port line client} portid	Enter ethernet physical port mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode
4	description line line-id WORD description client client-id WORD	Configure remote equipment port description information <i>Line-id WORD</i> remote port description information <i>Client-id WORD</i> remote port description information

In remote configuration mode, use **no description line line-id** or **description client client-id WORD** to delete the description information.

In remote configuration mode, use **show interface port** and **show interface port detail** to show remote port configuration information.

- Start/shutdown extended remote loopback

Starting loopback function may affect data transmission.

Enable remote equipment optical port inside-loopback, you can select the parameter so that the response end could recalculate CRC. The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode
4	inside-loopback [crc-recalculate]	Start remote equipment optical port inside-loopback

In remote configuration mode, use **no inside-loopback** to stop remote equipment inside-loopback, use **show inside-loopback** to show remote optical port inside-loopback state and parameter.

- Run remote equipment line diagnoses function

Executing remote equipment line diagnoses function may affect the link and data transmission. The steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode
4	test cable-diagnostics	Run remote equipment line diagnoses

In remote configuration mode, use **show cable-diagnostics** to show remote equipment line diagnoses result.

30.2.6 Upload/download files from remote equipment

- Download the file from server to remote equipment

The system bootrom file, startup file, startup configuration file and FPGA file of remote device can be downloaded from server to remote device (center device as the relay). This function can be started by center device or remote device, and multiple remote devices can be upgraded at the same time.

Center device starts, download from FTP/TFTP server:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>Portid</i> physical port ID

3	remote-device	Enter remote configuration mode
		Download the file from FTP server to remote equipment
4	download {bootstrap system-boot startup-config fpga} ftp A.B.C.D USRNAME PASSWORD FILENAME	<i>A.B.C.D:</i> Server IP address <i>USRNAME:</i> FTP server username <i>PASSWORD:</i> FTP server password
	download {bootstrap system-boot startup-config fpga} tftp A.B.C.D FILENAME	<i>FILENAME:</i> The filename on the server Download the files from TFTP server to remote equipment <i>A.B.C.D:</i> server IP address <i>FILENAME:</i> the filename on the server

Acting from the remote equipment, the steps to download files from FTP/TFTP server to remote end are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>Portid</i> phisical port ID
3		Download the file from FTP server to remote equipment <i>A.B.C.D:</i> Server IP address
	download {bootstrap system-boot startup-config fpga} ftp A.B.C.D USRNAME PASSWORD FILENAME	<i>USRNAME:</i> FTP server username <i>PASSWORD:</i> FTP server password
	download {bootstrap system-boot startup-config fpga} tftp A.B.C.D FILENAME	<i>FILENAME:</i> The filename on the server Download the files from TFTP server to remote equipment <i>A.B.C.D:</i> server IP address <i>FILENAME:</i> the filename on the server

When the file downloading is over, the remote equipment can be shown with **dir** in privileged EXEC mode, and use **erase** to delete.

➤ Upload files to the server from remote equipment

The system bootrom file and startup configuration file on the remote equipment can be transmitted through local end to do uploading from remote equipment to the server. The function can be started by local equipment or remote equipment. When it is started from local equipment, we can no upgrade several remote equipments at the same time.

Started from local equipment, the steps to upload file from remote equipment to FTP/TFTP server are as follows:

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode
4	upload {startup-config system-boot } ftp A.B.C.D <i>USRNAME</i> <i>PASSWORD</i> <i>FILENAME</i>	Upload file from remote equipment to FTP server <i>A.B.C.D</i> : Server IP address <i>USRNAME</i> : FTP server username <i>PASSWORD</i> : FTP server password
	upload {startup-config system-boot} tftp A.B.C.D <i>FILENAME</i>	<i>FILENAME</i> : The filename on the server Upload file from remote equipment to TFTP server <i>A.B.C.D</i> : server IP address <i>FILENAME</i> : the filename on the server

Started from remote equipment, the steps to upload file from remote equipment to FTP/TFTP server are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical interface mode <i>Portid</i> physical port ID
3		Upload file from remote equipment to FTP server
4	upload {startup-config system-boot } ftp A.B.C.D <i>USRNAME</i> <i>PASSWORD</i> <i>FILENAME</i>	<i>A.B.C.D</i> : Server IP address <i>USRNAME</i> : FTP server username <i>PASSWORD</i> : FTP server password
	upload {startup-config system-boot} tftp A.B.C.D <i>FILENAME</i>	<i>FILENAME</i> : The filename on the server Upload file from remote equipment to TFTP server <i>A.B.C.D</i> : server IP address <i>FILENAME</i> : the filename on the server

➤ Download remote equipment file from the server to local end

The remote equipment system bootrom file, startup file, startup configuration file and FPGA file can all be downloaded from server to local end using FTP/TFTP protocol, then be saved in local FLASH file system with a designated filename, making preparation for further upgrading.

When local end saves remote file, it will add postfix automatically according to the file type, so the local filename designated by user does not need postfix. What's else, the filename designated by remote file can not be the same with the filename of local end its own in flash. That is, the remote equipment's bootrom file can not be named as system-boot; the remote equipment's startup

configure file can not be named as startup-config; the remote equipment's FPGA file can not be named as FPGA. However, the system bootroom file is not saved in FLASH, so the bootroom file of remote equipment can be named as bootstrap.

In privileged EXEC mode, the steps to download remote equipment file from the server to local end are as follows:

Step	Command	Description
	download {remote-bootstrap remote-system-boot remote-startup-config remote-fpga} ftp A.B.C.D USRNAME PASSWORD FILENAME LOCAL-FILENAME	<i>A.B.C.D</i> : server IP address <i>USRNAME</i> : FTP server username <i>PASSWORD</i> : FTP server password <i>FILENAME</i> : the filename on FTP server <i>LOCAL-FILENAME</i> : the filename saved in local end
1	download { remote-bootstrap remote-system-boot remote-startup-config remote-fpga} tftp A.B.C.D FILENAME LOCAL-FILENAME	<i>A.B.C.D</i> : server IP address <i>FILENAME</i> : the filename on the server <i>LOCAL-FILENAME</i> : the filename saved on local end

When the downloading is over, you can use **dir** to show the state in privileged EXEC mode on local equipments, and use **erase** to delete.

- Upload remote equipment file from local end to the server

The remote file saved in local equipment's FLASH can be uploaded using FTP/TFTP to the server. The steps are as follows:

Step	Command	Description
	upload {remote-bootstrap remote-system-boot remote-startup-config remote-fpga} ftp A.B.C.D USRNAME PASSWORD FILENAME LOCAL-FILENAME	<i>A.B.C.D</i> : server IP address <i>USRNAME</i> : FTP server username <i>PASSWORD</i> : FTP server password <i>FILENAME</i> : the filename on FTP server <i>LOCAL-FILENAME</i> : the filename saved in local end
1	upload {remote-bootstrap remote-system-boot remote-startup-config remote-fpga} tftp A.B.C.D FILENAME LOCAL-FILENAME	<i>A.B.C.D</i> : server IP address <i>FILENAME</i> : the filename on the server <i>LOCAL-FILENAME</i> : the filename saved on local end

- Download file from local end to remote equipment

The remote file saved in local equipment FLASH, can be downloaded to remote equipment using extended OAM protocol. The function can be started from local equipment or remote equipment. When started from local equipment, several remote equipments can be upgraded at the same time.

Started from local equipment, the steps to download file from local end to remote equipments are as

follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter Ethernet physical interface mode
3	remote-device	Enter remote configuration mode
4	download { bootstrap system-boot fpga } FILENAME	Download bootroom file, startup file and FPGA file from local end to remote equipment <i>FILENAME</i> : the filename on local end
	download startup-config [FILENAME]	Download configuration file from local end to remote equipment <i>FILENAME</i> : the filename on local end

Started from remote end, the steps to download file from local end to remote end are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical interface mode <i>Portid</i> physical port ID
3	download {bootstrap system-boot fpga} FILENAME	Download bootroom file, startup file and FPGA file from local end to remote equipment <i>FILENAME</i> : the filename on local end
	download startup-config [FILENAME]	Download configuration file from local end to remote equipment <i>FILENAME</i> : the filename on local end

When file download is over, you can use **dir** to show the state in privileged EXEC mode on remote equipment and use **erase** to delete.

30.2.7 Configure remote equipment to network management enabled equipment

- Configure remote equipment SNMP community and IP address

The steps to configure remote equipment community name and IP address are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter Ethernet physical interface mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode

		Configure remote equipment community name and priority.
4	snmp-server community <i>community-name {ro/rw}</i>	<i>community-name</i> community name <i>ro</i> read only <i>rw</i> read & write
		Configure remote equipment IP address
5	ip address <i>ip-address [ip-mask] vlan-list</i>	<i>ip-address</i> <i>ip-mask</i> <i>vlan-list:</i> the managed VLAN list

In remote configuration mode, use **no snmp-server community** *community-name* to delete remote equipment community name.

When configuring IP address we need to designate and manage VLAN as well, if the VLAN does not exist, create VLAN (by default all the ports are member port); if related VLAN exists, the member port configuration will not be modified. In remote configuration mode, use **no ip address ip-address** to delete remote port IP address.

In remote configuration mode, use **show remote-device information** to show remote community name and IP address information.

➤ Configure remote equipment Q-in-Q

Configure remote equipment flexible Q-in-Q function, the attributions that need to be configured include: switch mode, TPID, local VLAN and access interface.

When configuring remote equipment to complete transparent mode, the other configurations, like TPID, local VLAN and access interface, are all not available. The steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode
4	switch-mode transparent	Configure remote equipment to complete transparent mode

When configuring remote equipment to Dot1q VLAN transparent mode, or single TAG mode, local VLAN and access port is valid, while TPID is not. When the equipment is configured to single TAG mode, the data packet coming from the access port will be marked local VLAN ID TAG if it has no TAG; if it has, it will not be handled.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode

2	interface {port line client} portid	Enter ethernet physical port mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode
4	switch-mode dot1q-vlan native-vlan <1-4094> [line]	Configure remote equipment to Dot1q VLAN transmission mode native-vlan: local VLAN <1-4094>: VLAN ID; line: Line port is the access port, when the keyword line is not selected, it means that client port is the access port

Configure remote equipment to Double tagged VLAN transmission mode, that is in double TAG mode, TPID, local VLAN and access port are all valid. When the equipment is configured double TAG mode, the data packet coming from the access port will be marked specific TPID and local VLAN ID outer layer TAG, whatever it has TAG or not.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode
4	switch-mode double-tagged-vlan [tpid HHHH] native-vlan <1-4094> [line]	Configure remote equipment to Double tagged VLAN transmission mode native-vlan: local VLAN; <1-4094>: VLAN ID; Line: Line port is the access port tpid: outer-layer tagged TPID <i>HHHH:</i> outer-layer tagged TPID, hexadecimal number, 0000 to FFFF When tpid is not configured, it means the TPID that takes 0x9100 as the outer-layer TAG

In remote configuration mode, run **show remote-device information** to show remote equipment flexible Q-in-Q function related configuration.

30.2.8 Save remote equipment configuration information to local end

When remote equipment belongs to RC552 series, the equipment itself will not save configuration file, but it is able to save remote configuration content to local end using **writ local**. When the local equipment is rebooted, it will load the saved 552 configuration file, and if there is configuration request from remote 552, the saved configuration will be sent to remote end. The saving steps are as

follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical interface mode <i>Portid</i> physical port mode
3	remote-device	Enter remote configuration mode
4	write local	Save remote configuration to local FLASH

If there is no 552 configuration file when local end is started, and local end has not sent configuration to remote 552 yet after booting, execute the command and you will be failed.

Saving FLASH file takes a long time, so when executing the command, unusual situations like OAM link breaking down may happen.

30.2.9 Reset remote equipment

The steps to reset remote equipment are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port line client} portid	Enter ethernet physical port mode <i>Portid</i> physical port ID
3	remote-device	Enter remote configuration mode
4	reboot	Reset remote equipment

You need to confirm your operation after reset command is executed.

When remote equipment is resetting or rebooting, OAM link may break down, and local equipment may lose the connection to remote equipment.

30.2.10 Extended OAM statistic clear function

Extended OAM counts the sending and receiving extended OAM messages number on each OAM link, the extended OAM message types include: variable acquirement and response, variable setting and response, file request and file data, notice and so on. User can follow the steps below to clear statistic information:

Step	Command	Description
1	config	Enter global configuration mode
2	clear extended-oam statistics [port-list <i>port-list</i>]	Clear extended OAM link static information
	clear extended-oam statistics	

[line-list *line-list*]

clear extended-oam statistics
[client-list *client-list*]

30.2.11 Monitoring and maintenance

Command	Description
show interface port	Show remote equipment port information
show interface port detail	Show remote equipment port detailed information
show interface port statistics	Show remote equipment port static information
show oam capability	Show remote equipment ability of supporting OAM management
show remote-device information	Show remote equipment basic information
show sfp	Show remote equipment SFP information
show cable-diagnostics	Show link diagnoses result
show inside-loopback	Show remote loopback state and parameter
show extended-oam statistics	Show extended OAM frame static information
show extended-oam status	Show extended OAM link state
show snmp trap remote	Show remote trap enable configuration

30.2.12 Typical configuration example

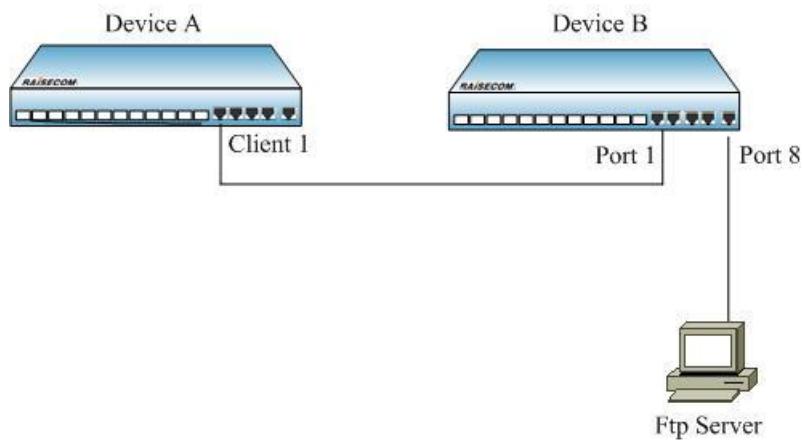


Figure 30-1 Remote file upload/download function typical configuration

If you want to back-up and upgrade device A's startup configuration file on device B, configure B as the steps below:

- 1) upload startup configuration file to the server from remote device
- Raisecom#config

```
Raisecom(config)# interface port 1
```

```
Raisecom (config-port)# remote-device
```

```
Raisecom(config-remote)# upload startup-config ftp 12.0.0.1 raisecom raisecom  
configfile_version_1
```

2) download startup configuration file to remote device from the server:

```
Raisecom(config-remote)# download startup-config ftp 12.0.0.1 raisecom raisecom  
configfile_version_2
```

Chapter 31 Optical Module Digital Diagnoses

31.1 Optical Module Digital diagnoses principle

SFP (Small Form Pluggable) is a kind of optical module in media converter. The fault diagnoses function provides the system a way of performance monitoring. Using the data monitoring function provided by this module, network administrator can forecast the lasting time of the module, insulate the system fault and validate the module compatibility when fixing equipments.

Each SFP module provides five performance parameters: the media converter temperature, inner power supply voltage, sending electronic current, sending optical power and receiving optical power.

The digital diagnoses module polls all the SFP ports every 5 seconds, and gives three datasheet according to the performance parameter getting from the poll: the real-time monitoring table of the optical module, the period performance monitoring table of the optical module, the current period performance monitoring table. When the parameter exceeds the threshold, it will send trap and offer its global switch control.

The index of optical module real-time monitoring table is SFP port number and parameter type. Inside the software the table has stable number of rows, but when you look over it in the command lines only the information of the ports that are active (the row mark is valid) can be shown. Seen from the network management software, the table has stable number of rows, when SFP is not active it means the row mark of the table is invalid. The table restores the parameter value, threshold value, the time and value that the last time the threshold value is exceeded of each parameter for each SFP module. The initialized value of last threshold exceeding is -1000000, the left values are all 0. When the digital diagnose module polls SFP port every 5 seconds, if SFP is active, read SFP's 5 parameter value, adjusting measure, adjusting parameter and threshold value, refresh the parameter value and threshold value of the optical module real-time monitoring table, if it exceeds the threshold value, update the time and value of the exceeding Digital diagnoses configuration. Configure real-time monitoring table that the row mark is invalid. Each row of the table contains 2 variables, which stands for how many 15 minutes' cycle records and 24 hours' cycle records are restored in the parameters of SFP ports. Now digital diagnoses module supports 96 15 minutes' cycle record and 1 24 hours' cycle record at the most.

The index of optical module current period performance monitoring table is SFP port number, period type and parameter type. The table records the maximum value, least value and the average value of the parameters that are within a recording cycle. The table has stable row number, and all the initialized parameter values are 0. When the equipment is started, the digital diagnoses module polls all the SFP ports every 5 seconds, and the value that read first will be evaluated to the maximum, least and average value. Then, if the polling value is larger than the maximum value, refresh it to the larger value; if it is smaller than the least value, refresh the recorded least value, and compute the summation, add 1 on the digit. If SFP is not active when polling, no data record will be refreshed. After 180 polling (15 minutes later), add a row in the period performance monitoring table, and configure the maximum, least and average value of the row's parameter according to current period monitoring table record, cycle type is 15 minutes, then reset all the data in the current period row, and start recording the next cycle. It is the same to record the data of 24 hour cycle. When it reaches

24 hours, add a row in period monitoring table, then reset all the data in the current period row, and start recording the next cycle.

The index of period performance monitoring table of the optical module is port number, cycle type, cycle recording number and parameter type. The monitoring table restores data of two cycles, that is 15 minutes data and 24 hours data. The table is empty originally. Every 15 minutes, a 15 minutes cycle record will be added to the table. The record number of the newest one is 1, larger recording number means older recording. The table keeps at most 96 fifteen minutes record. When it reaches 96 records, the oldest one will be deleted when a new one is added. Every time it reaches 24 hours, a 24 hour cycle record will be added to the table. The newest recording number is 1, at most 1 twenty-four hour cycle record will be restored in the table, and the old record will be covered every 24 hours.

31.2 Optical module digital diagnostic configuration

31.2.1 Optical module digital diagnostic default configuration

Function	Default
Enable/disable digital diagnostic function	Disable digital diagnostic function
Trap Enable / disable send optical module parameters abnormal trap	Allow to send optical module parameters abnormal trap

31.2.2 Optical module digital diagnostic anable/disable configuration

Step	Command	Description
1	config	Enter global configuration mode
2	transceiver digitaldiagnostic {enable/disable}	Enable/disable digital diagnostic function. <i>enable</i> : enable <i>disable</i> : disable
3	exit	Back to privilege mode
4	show interface port [port-list] transceiver detail	Show digital diagnostic information

Note:

When the digital diagnostic functions are configured to disable, the optical module real-time monitoring watch signs is invalid, the table more than the previous threshold parameter value is -1000000, and the rest of parameter values are all 0; the current cycle of performance monitoring for all parameter values in the table is 0; periodic performance monitoring records in the table is cleared, the table is empty.

If the digital diagnostic function is disabled, optical module parameter status is not unusual to send trap.

31.2.3 Optical module parameter abnormal alarm configuration

Step	Command	Description
1	config	Enter global configuration mode
2	snmp trap transceiver {enable/disable}	Enable/disable to send optical module parameter status abnormal trap. <i>enable</i> : enable. <i>disable</i> : disable
3	exit	Back to privilege mode
4	show interface {client/line} transceiver	Show digital diagnostic information

Note:

Configure allowed sending optical module parameters state exception trap, and properly configure the device IP address and SNMP Server circumstances, when the transceiver temperature, the internal supply voltage, bias current, transmit, transmit optical power, received optical power beyond the threshold parameter values To send trap. If digital diagnostic function is disabled, it will not sent trap.

31.2.4 Optical module digital diagnostic parameters monitoring and maintenance

Command	Description
show interface port [port-list] transceiver [threshold-violations] [detail]	Show digital diagnostic information

Chapter 32 802.1x Configuration

32.1 802.1x principle overview

802.1x module is based on IEEE802.1x protocol, or port based network access control technology, it makes authorization and control to access equipments on the equipments' physical access layer, and defines the point-to-point connection mode between the access equipment and access port.

The system structure of IEEE 802.1x includes three parts:

- Suplicant
- Authenticator
- Authorization Server

LAN access control equipment (like access switch) needs the Authenticator of 802.1x; user side equipment, like computer, needs to install 802.1x client (Suplicant) software (or the 802.1x client pre-positioned in Windows XP); while 802.1x Authorization Server System usually stays in operator's AAA centre.

Authenticator and Authorization Server exchange information using Extensible Authorization Protocol; while Suplicant and Authenticator use EAPOL (EAP over LANs, defined in IEEE802.1x) for communication, the authorization data is encapsulated in EAP frame. The authorization data is encapsulated in the message of other AAA upper layer protocol (like RADIUS) so that it is able to go through complicated network and reach Authorization Server, this process is called EAP Realy.

The figure below is 802.1x system structure:

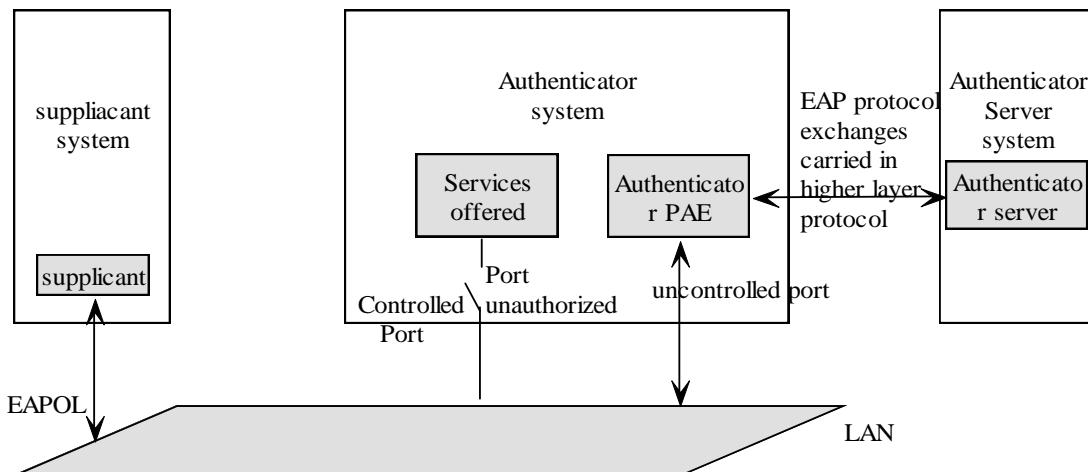


Fig 32-1 802.1x system structure

'port based network access control' means to do authorization and control to the access equipments in LAN access control equipment port layer. If the user equipment connected to the port can go through the authorization, then it is able to visit the resources in LAN; if it can not pass the authorization, then it can not visit the network resources through switch – same as physical link down.

32.2 Configure 802.1x

802.1x configuration includes:

1. Default 802.1x configuration situation;
2. Enable/disable 802.1x global feature and port feature;
3. Configure RADIUS server IP address and RADIUS public key;
4. Show RADIUS server configuration;
5. Configure port access control mode;
6. Enable/disable 802.1 x reauthorization function;
7. Configure 802.1x reauthorization period;
8. Configure 802.1x silence time;
9. Configure Request/Identity resending period;
10. Configure Request/Identity resending period;
11. Configure RADIUS server overtime.

32.2.1 Default 802.1x configuration

Function	Default value
Global 802.1x feature	disable
Port 802.1x feature	disable
Port access control mode	auto
RADIUS server overtime	100s
802.1x reauthorization function	disable
802.1x reauthorization period	3600s
802.1 silence time	60s
Request/Identity resending period	30s
Request/Challenge resending period	30s

32.2.2 Basic 802.1x configuration

The basic 802.1x configuration is shown below:

- Enable/disable 802.1x global feature and port feature;
- Configure RADIUS server IP address and RADIUS public key;
- Configure port access control mode.

1. Enable/disable 802.1x global feature and port feature;

802.1x feature includes global 802.1x feature and port 802.1x feature, if one of them is not enabled, it will lead to 802.1x feature shown as constraint authorization passing through. 802.1x protocol and spanning tree protocol (STP) can not be opened at the same time in the same port.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	dot1x { disable enable }	Enable/disable global 802.1x feature
3	interface { port line client } <1- MAX_PORT_NUM >	Enter ethernet physical port mode <i>1- MAX_PORT_NUM</i> the equipment port
4	dot1x { disable enable }	Enable/disable port 802.1x feature
5	exit	Return to global configuration mode
6	exit	Return to privileged EXEC mode
7	show dot1x { port-list line client } portlist	Show physical port 802.1x configuration information <i>portlist</i> : use ‘_’ and ‘,’ to input more ports number

Notice:

- If a port has enabled STP and 802.1x protocol port can not be opened successfully, we need to disable port STP first.
- 802.1x protocol is physical port based access control protocol, it is not suggested that user enable 802.1x feature on aggregation port and not-Access port. When several users connects to the same switch port using shared network, if one user passes the authorization, then other users do not need authorization before they visit the network, but in this situation several user doing authorization at the same time may cause unsuccessful authorization because of interaction.

2. Configure RADIUS server IP address and RADIUS public key:

Configuring RADIUS server IP address and RADIUS public key is a necessary precondition of 802.1x port authorization.

The configuration steps are as follows:

Step	Command	Description
1	[no] radius ipaddress	Configure RADIUS server IP address
2	[no] radius-key string	Configure RADIUS server public key
3	show radius-server	Show RADIUS server configuration information

3. Configure port access control mode:

Port access control mode can be divided into three states: auto, authorized-force, unauthorized-force. By default it is auto. When global 802.1x feature and port 802.1x feature is on, the configuration determines directly if the authorization process will use authorized-force, unauthorized-force or protocol control mode.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface { port line client} <1-MAX_PORT_NUM >	Enter ethernet physical port mode <i>1-MAX_PORT_NUM</i> equipment port
3	dot1x auth-control {auto/authorized-force/ unauthorized-force}	Configure port control mode
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show dot1x {port-list / line / client} portlist	Show physical port 802.1x configuration information <i>portlist</i> : use ‘_’ and ‘,’ to input more port numbers.

32.2.3 802.1x reauthorization configuration

Reauthorization function is for authorized users, so you should make sure that global and port 802.1x feature are enabled. By default reauthorization function is disabled. The authorized port keeps the state of authorized in the process of authorization; if reauthorization failed, then the port will enter unauthorized state.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port / line / client} <1-MAX_PORT_NUM >	Enter ethernet physical port mode <i>1-MAX_PORT_NUM</i> equipment port
3	dot1x reauthentication {enable/disable}	Enable/disable reauthorization function
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show dot1x {port-list/line/client} portlist	Show physical port 802.1x configuration information <i>Portlist</i> , use ‘_’ and ‘,’ to input more port numbers

32.2.4 Configure 802.1x timer

In 802.1x authorization process, there are 5 timers related:

1. reauth-period: reauthorization overtime timer. In the time configured by the timer, 802.1x reauthorization will be raised. Reauth-period-value: the time length configured by reauthorization overtime timer, range is 1-65535, unit is second. By default it is 3600 seconds.
2. quit-period: quiet timer. When user authorization failed, the switch needs to keep quiet for a period of time, which is configured by quiet timer. When quiet timer exceeds the time it will make

reauthorization. In quiet time, the switch will not process authorization messages. Quiet-period-value: the quiet time value configured by quiet timer, range is 10-120, unit is second. By default, quiet-period-value is 60 seconds;

3. tx-period: transmission overtime timer. When the switch sends Request/Identity messages to user request end, the switch will start the timer, if in the configured time length user end software can not send request answering messages, the switch will re-send authorization request message, which will be sent three times. Tx-period-value: the time length configured by sending overtime timer, range is 10-120, unit is second. By default tx-period-value is 30 seconds.

4. supp-timeout: Supplicant authorized timeout timer. When the switch sends Request/Challenge message to user request end, the switch will start supp-timeout timer. If the user request end can not react in the time length configured in the timer, the switch will re-send the message twice. Supp-timeout-value: the time length configured by Supplicant authorization overtime timer, range is 10-120, unit is second. By default supp-timeout-value is 30 seconds.

5. server-timeout: Authentication Server. The timer defines the authenticator and the total overtime-length of RADIUS server dialog, when the timer exceeds the time the authenticator will end the dialog with RADIUS server, and start a new authorization process. The resending times and interval of RADIUS is determined by the switch RADIUS client. The switch RADIUS client message resend 3 times, while the waiting time is 5s. server-timeout-value: the overtime length configured by RADIUS server timer, range is 100-300, unit is second. By default server-timeout-value is 100s.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface { port line client } <1- MAX_PORT_NUM >	Enter ethernet physical port mode
3	[no] dot1x timer reauth-period <i>reauth-period-value</i>	Configure reauthorization timer value Range is 1-65535, unit is second. By default the value is 3600s
4	[no] dot1x timer quiet-period <i>quiet-period-value</i>	Configure quiet-time timer value Range is 10-120, unit is second. By default quiet-period-value is 60s
5	[no] dot1x timer tx-period <i>tx-period-value</i>	Configure Request/Identity resending timer value Range is 10-120, unit is second. By default tx-period-value is 30s
6	[no] dot1x timer supp-timeout <i>supp-timeout-value</i>	Configure Request/Challenge resending timer value Range is 10-120, unit is second. By default supp-timeout-value is 30s
7	[no] dot1x timer server-timeout <i>server-timeout-value</i>	Configure RADIUS server overtime timer value Range is 100-300, unit is second. By default server-timeout-value is 100s
8	exit	Return to global configuration mode

9	exit	Return to privileged EXEC mode
10	show dot1x { port-list line client} portlist	Show physical port 802.1x configuration information Portlist, use ‘_’ and ‘,’ to input more port numbers.

32.2.5 802.1x statistics cleanup

Monitoring and port statistics information is used to count the EAPOL messages number for the switches and user end exchanging data. Cleaning port stat. will clean all the statistics information of the selected ports. The steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	clear dot1x{ port-list line client } portlist statistics	Clear physical port 802.1x statistics information
3	exit	Return to privileged EXEC mode
4	show dot1x { port-list line client} portlist statistics	Show physical port 802.1x statistics information Portlist, use ‘_’ and ‘,’ to input more port numbers.

32.2.6 Maintenance

Use **show** to show the configuration and running state of switch 802.1x function for the convenience of monitoring and maintenance.

The related **show** commands are shown below:

Commands	Description
show radius-server	Show RADIUS server configuration
show dot1x {port-list/line/client} portlist	Show physical port 802.1x configuration information
show dot1x {port-list/line/client} portlist statistics	Show physical port 802.1x statistics information

32.2.7 Configuration example

1. Configuration request:
 - PC user can visit outer network after passing ARDIUS server authorization
 - In authorization-force mode, PC needs not authorization before visiting outer network;
 - In unauthorization-force mode, PC can not visit outer network;
 - After passing authorization, PC will do reauthorization 600s later automatically.
2. Network structure:

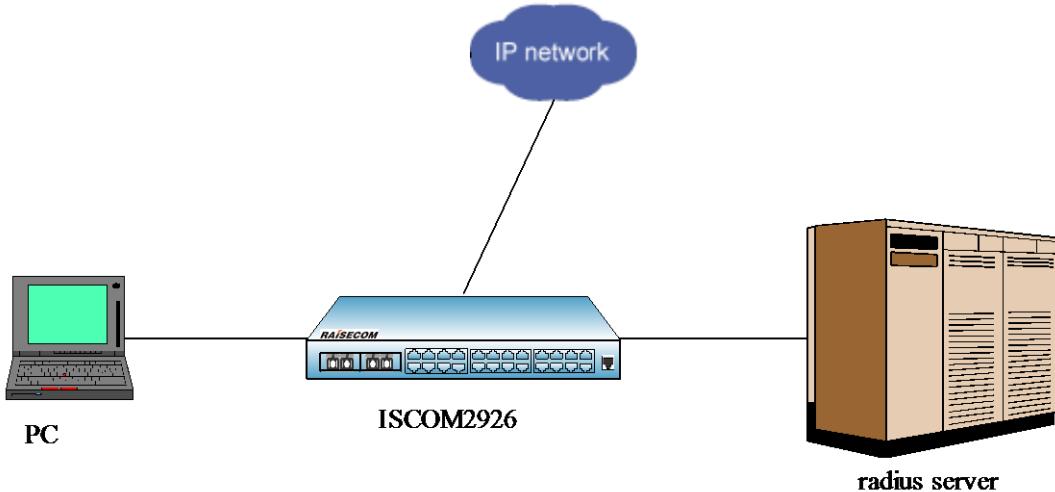


Fig 32-2 network structure

3. Configuration steps:

- Configure RADIUS server:

Follow ISCOM switch 802.1x user guide, add user raisecom in the server, the password is 123;

- Configure switch IP address and RADIUS server address:

```
Raisecom(config)#interface ip 0
```

```
Raisecom(config-ip)#ip address 10.10.0.1 255.255.0.0 1
```

```
Raisecom(config-ip)#exit
```

```
Raisecom(config)#ip default-gateway 10.10.0.2
```

```
Raisecom(config)#exit
```

```
Raisecom# radius 192.168.0.1
```

```
Raisecom# radius-key raisecom
```

- Configure enabling global and port 802.1x authorization function:

```
Raisecom(config)#dot1x enable
```

```
Raisecom(config)#interface port 1
```

```
Raisecom(config-port)#spanning-tree disable(STP and 802.1x are mutex)
```

```
Raisecom(config-port)# dot1x enable
```

- PC end uses the client software for authorization request, username: raisecom, password: 123;

The PC client software will inform passing authorization, then we can visit outer network;

- Change the authorization mode to authorization-force mode:

```
Raisecom(config)#interface port 1
```

```
Raisecom(config-port)#dot1x auth-control authorized-force
```

- PC end uses the client software for authorization request, username: raisecom, password: 123;

The PC client software will inform passing authorization, then we can visit outer network;

- Chang authorization-force mode to unauthorization-force mode

```
Raisecom(config)#interface port 1
```

```
Raisecom(config-port)#dot1x auth-control unauthorized-force
```

- PC end uses the client software for authorization request, username: raisecom, password: 123;

The PC client software will inform passing authorization, then we can visit outer network;

- Enable reauthorization, and configure the time to 600s:

```
Raisecom(config)#interface port 1
```

```
Raisecom(config-port)#dot1x reauthentication enable
```

- Show the statistics information:

```
Raisecom#show dot1x port-list 1 statistics
```

Notice: The switch's IP address, RADIUS server IP and key must well-configured first of all.

Chapter 33 Auto-update Configuration

33.1 Principle of auto-update function

Auto-update module mainly uses DHCP protocol renew requisition to get file update information and then download latest system boot, system bootstrap and configuration file from service via TFTP. Applying rules, analysis and downloading rules of auto-update information of raisecom:

- DHCP Server file update information applying rules:

System boot and system bootstrap file applying rules:

Option17: path\device type#ROS version#BOOTROM version;

Example: Option17 is raisecom\2109A##0906031 if want to apply system-boot software 0906031 update of ISCOM2109A under content raisecom.

Note: All fields must exist. The version can not be followed after # if the field is blank. Relevant # can be emitted if Bootstrap of the last device is not existing, like raisecom\2109A#0906031.

Configuration files applying rules:

Option67: path\explain rule#date of update

Example: Option67 is raisecom\81000#0906030 if the date of device configuration file update is 200906030, explain rule is 81000 and under content raisecom.

- System file explain rules

1. System boot, bootstrap file explain rule:

If DHCP Option17 is raisecom\image\2109A#0906031#; 2924GF##0906051, the device is ISCOM2109A, and then, it is considered there is a system boot file named ROS-ISCOM2109A-0906031 under content raisecom\image to download.

2. System startup configuration explain rules:

If DHCP Option67 is \raisecom\config\80000#0906050, configuration filename is RCJF-2109A, the device will explain to generate a configuration file name RCJF-2109A -0906050 for downloading.

Please refer to 1.3.3 for description of configuration filename rules.

- Download rule

Compare the stored version and applied version information, if the applied version is newer, the auto-update module will try to download the file:

If the system boot or system bootstrap file are existing and download successfully, update the file version information;

File downloading order is configuration file→ system bootstrap file→ system boot file.

If the device doesn't have configuration file or has not gotten configuration file by auto-update (the configuration file version is 0000000 now), and there is no option67, then, downloading startup_config.conf; if there is Option67, downloading “rule character string”. The version is

0000001 after downloading successfully.

Trying to download “configuration filename-version” or “rule character string-version” when the next updating process starts. Update configuration file version as version in file name after downloading. If there is rule number, the rule takes precedence. Update configuration file version if configuration file downloading successfully.

Both TFTP server and rule number take manual configuration precedence to decide server or generated filename take efficient.

Generally, the configuration file should not include version information of file, or else, the next auto-update process may be affected.

- Version initial definition

If the initial status doesn't have configuration file or there is no system software version in configuration file, take “date+0” to combine current version.

- Default to start auto-update if system doesn't have configuration file started; if there is configuration file, the file will decide the status of auto-update module.

33.2 Default Auto-update configuration

Function	Default value
Auto-update module status	enable
TFTP server address	0.0.0.0 (not available)
The configuration files name on the server	None
The naming rules of configuration files on the server	No rule number
Cover local configuration file switch state	Disable
System software version	Default to be software coding date+0
System configuration file version	0000000 by default, no configuration file
Send completing Trap switch state	Disable
Auto configuration and load running state	DONE
Auto configuration and load running result	NONE

33.3 Auto configuration and load function configuration

33.3.1 Enable auto-update

By default, auto-update module is enabled, and use the command **show service config** can view it displayed as enable.

Step	Command	Description
1	config	Enter global configuration mode
2	service config	Enable auto-update function
3	exit	Quit global configuration mode and enter

4	show service config	privileged EXEC mode Show Auto-update information, Config server IP address shows the configuration information of TFTP server address
---	----------------------------	--

Use the command **no service config** can disable auto-update.

33.3.2 Configure TFTP server address

By default, TFTP server address is 0.0.0.0, 0.0.0.0 can not be configured by the command. Run the opposite command **no service config tftp-server** and TFTP server address will be 0.0.0.0, but 0.0.0.0 can not be taken as a available address to download configuration files and load it, use the command **show service config** to view and it shows as “--”.

Step	Command	Description
1	config	Enter global configuration mode
2	service config tftp-server A.B.C.D	Configure TFTP server address, A.B.C.D must satisfy RFC1166.
3	exit	Quit global configuration mode and enter privileged EXEC mode
4	show service config	Show Auto-update and load information, Config server IP address shows the configuration information of TFTP server address

To restore default address, use **no service config tftp-server**.

Notice:

- The configure IP address must accord with RFC1166, otherwise it may cause configuration failure.
- After using the command to configure TFTP server address, when you run Auto-update, the address that is configured by the command will be used, not the address acquired from DHCP Client. So, if you don't want to use local configured address, you don't have to configure it; if it has been configured, use **no service config tftp-server** to restore and run Auto-update function.

33.3.3 Configure file name rule

By default, there is no filename naming rule, use **show service config** and it will show: --. When naming rule and filename are not configured, while no configuration filename is acquired successfully from DHCP Client function, the system will use default filename: **startup_config.conf**.

The configured file naming rule has the highest priority. When configured naming rule, you should use the naming rule to make sure the filename according to the equipment attribute.

Step	Command	Description
1	config	Enter global configuration mode
2	service config filename rule [<80001-89999>]	Configure file naming rules [<80001-89999>]: rules number of configuration file name
3	exit	Quit from global configuration mode and enter privileged EXEC mode

4	show service config	Show Auto-update and load information, among them, Config filename rule shows the filename configuration information
----------	----------------------------	--

Use command **no service config filename rule** to delete the configured filename naming rules.

If there is no input rule number, then the system will create rule number in the way of question according to the answer user offers.

Raisecom(config)#**service config filename rule**

Enter the first question:

Please check device type rule, configuration filename

0 - includes no device type information

1 - includes device type information

Please select:

0 means that the configuration files do not contain equipment type;

1 means that the configuration files do not contain switch type.

Input 0 or 1, press Enter, and enter the second question:

Notice:

- If the input number is neither 0 nor 1, it will be returned fault and failure in rule creation.

Please check MAC address rule, configuration filename

0 - includes no MAC address information

1 - includes the first 2 characters in MAC address

2 - includes the first 4 characters in MAC address

3 - includes the first 6 characters in MAC address

4 - includes the first 8 characters in MAC address

5 - includes the first 10 characters in MAC address

6 - includes all characters in MAC address

Please select:

0 means that ROS software version information is not contained in the configuration filename;

1 means that complete ROS software version information is contained in the configuration filename;

2 means that the software version information except the equipment type is contained in the configuration filename;

3 means that the software version information except the equipment type and date is contained in the configuration filename;

4 means that the software version high 3 figures are contained in the configuration filename;

5 means that the software version high 2 figures are contained in the configuration filename;

6 means that the software version the highest figure is contained in the configuration filename.

Input a random number among 0 and 6, press Enter, and end up rule number configuration.

Notice:

- If you input any number that is not in range from 0 to 6, it will return fault and failure in rule creation.

Please check MAC address rule, configuration filename

0 - includes no MAC address information

1 - includes the first 2 characters in MAC address

2 - includes the first 4 characters in MAC address

3 - includes the first 6 characters in MAC address

4 - includes the first 8 characters in MAC address

5 - includes the first 10 characters in MAC address

6 - includes all characters in MAC address

Please select:

Notice:

- If the input number belongs not to 0-6, it will be returned fault and failure in rule creation.

Please check ROS version rule, configuration filename

0 - includes no ROS version information

1 - includes entire ROS version information

2 - includes all except device type

3 - includes all except device type and date

4 - includes the highest 3 version number

5 - includes the highest 2 version number

6 - includes the highest version number

Please select:

Notice:

- If the input number belongs not to 0-6, it will be returned fault and failure in rule creation.

The configuration file naming rules are as follows:

The rule number is made up of 5 numbers, myriabit is 8, which has no actual meaning.

1) Kilobit shows the equipment type rules:

0 – equipment type is not included in the configuration file name;

1 – equipment type is included in the configuration file name;

2 – 9, reserved number, for rules extension.

2) Hundred shows MAC address rules: (take 000E08.5118 for example)

0 – the equipment MAC address information is not included in the configuration file name

1 – the first 2 characters of the equipment MAC address is included in the configuration file name (that is 00)

2 - the first 4 characters of the equipment MAC address is included in the configuration file name

(000E)

3 - the first 6 characters of the equipment MAC address is included in the configuration file name (000E.5E)

4 - the first 8 characters of the equipment MAC address is included in the configuration file name (000E.5E08)

5 - the first 10 characters of the equipment MAC address is included in the configuration file name (000E.5E08.51)

6 - the first 6 characters of the equipment MAC address is included in the configuration file name (000E.5E.5E08.5118)

7 – 9 reserved number, for extension.

3) Tens show the software version number rule: (take ROS_4.3.2 ISCOM 2926.1.20080602)

0 – no software version information is contained;

1 – complete version information is contained (ROS_4.3.2 ISCOM 2926.1.20080602)

2 – the software version information without equipment type is contained (ROS_4.3.2.1.20080602)

3 – the software version information without equipment type and data is contained in the software version information (ROS_4.3.2.1)

4 – the software version information contains the higher three-figure (ROS_4.3.2)

5 – the software version information contains the higher two-figure (ROS_4.3)

6 – the software version information contains the higher one-figure (ROS_4)

7 – 9 restored, for extension.

4) Units digit shows the extension rules:

0 – extension rule is not supported;

1 – 9 restored, for extension.

The configuration file name is of the following style:

(equipment type)_M(MAC address)_ (software version number)

For example: rule number 81650 stands for the configuration file rule string:

ISCOM2128EA-MA_M000E.5E08.5118_ROS_4

Notice: After using the command to configure the naming rules, when Auto-update is loaded, the naming rule will be used to configure the filename, while manual configuration filename and the one acquired from DHCP Client will no be used. So, if you do not want to use the naming rules, you don't have to configure the naming rules, and if it had been configured, use **no service config filename rule** to restore to default cases.

33.3.4 Configure the filename

By default, the filename is empty, use **show service config** and you will see: --. Follow the steps below to configure the filename, the length can not be longer than 80 bytes.

Step	Command	Description
1	config	Enter global configuration mode
2	service config filename <i>FILENAME</i>	Configure the filename <i>FILENAME</i> : the filename, shorter than 80 bytes
3	exit	Quit from global configuration mode and enter privileged EXEC mode
4	show service config	Show Auto-update loading information; config file name shows the configuration information of the filename.

Use **no service config filename** to delete the configured configuration filename.

Notice:

- If the configuration filename rule had been configured, then the configuration filename using this command will not be used.
- Under the promise that no naming rule is configured, if the command is used to configure the filename, then when Auto-update is loaded, the filename configured by this command will be used, while the filename acquired from DHCP Client will not be used.
- If you want to use the filename acquired from DHCP Client or default filename, there is no need to configure the filename. And if it had been configured, use **no service config filename** to resume and run Auto-update loading function.

33.3.5 Configure the switch of covering local configuration

Enable/disable covering local configuration file switch function. If it is enabled, use the file on the server to cover local configuration file in the process of Auto-update loading.

Step	Command	Description
1	config	Enter global configuration mode
2	service config overwrite {enable disable}	Configure the switch of overwriting local configuration file
3	exit	Return to global configuration mode and enter privileged EXEC mode
4	show service config	Show Auto-update loading information, config file name show the configuration information of the filename

33.3.6 Set auto-update TRAP switch

Enable/disable auto-update TRAP switch function. If in enable status, device sends a file finish status TRAP after updating a file:

Step	Command	Description
1	config	Enter global configuration mode
2	service config trap	Configure the switch of auto-update TRAP

		{enable disable}
3	exit	Return to global configuration mode and enter privileged EXEC mode
4	show service config	Show Auto-update information, Send Completion trap: show enable/disable

33.3.7 Set Auto-update file version

Set system boot, system bootstrap, system startup configuration file version. In format: year-month-date, like 0906032. auto-update module will only download file newer than itself.

Step	Command	Description
1	config	Enter global configuration mode
2	service config version (<i>system-boot/bootstrap/ startup-config</i>) <i>VERSION</i>	Set auto-update file version. <i>VERSION</i> : file version, format: year-month-date-times.
3	exit	Return to global configuration mode and enter privileged EXEC mode
4	show service config	Show Auto-update information, display system boot, system bootstrap, system startup configuration file version.

Note: The file version is generally automatically saved during updating. If user configure or download configuration file with version, the version will be too lower or higher and cause miss updating. The version is dynamic updating during updating process. It must be 7 bit and in format of year-month-date-times, like: 0906032.

33.4 Monitoring and maintenance

Use **show service config** to show Auto-update information and the running situation and result information.

The information shown is as follows:

<i>Auto upgrade :</i>	<i>enable</i>
<i>Config server IP address:</i>	--
<i>Config filename rule:</i>	80600
<i>Config file name:</i>	--
<i>System boot file version:</i>	0906182
<i>Bootstrap file version :</i>	0906121
<i>Startup-config file version:</i>	0000000
<i>Overwrite local configuration file:</i>	<i>disable</i>
<i>Send Completion trap:</i>	<i>disable</i>
<i>Current File Type:</i>	<i>bootstrap</i>
<i>Operation states:</i>	<i>writing</i>

Result: *none*

Use the command below to show the meaning of the configuration filename rule:

Command	Description
show service config filename rule [ruleNum]	Describe the meaning of filename rule, and provide the optical Auto-update loading command rule number.

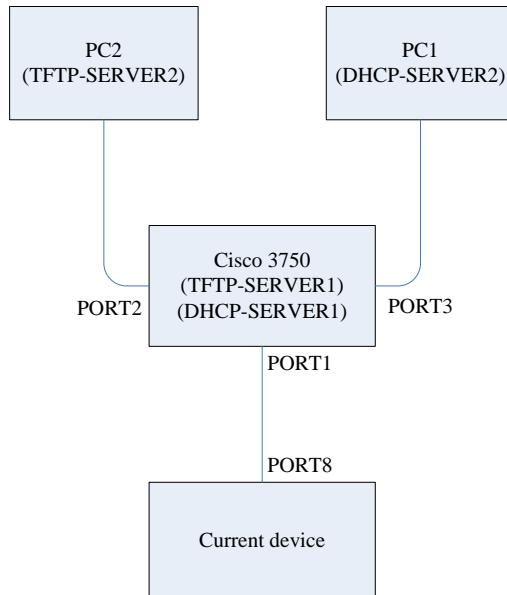
33.5 Typical configuration example

1.Destination

When the switch is started, by running Auto-update loading twice, the switch can go through VLAN and get the specific configuration file.

2.The topology structure

The topology structure is shown below:



3.The configuration steps on Cisco 3750:

Start DHCP SERVER and TFTP service on Cisco 3750:

Step 1: configure IP address on VLAN port 100:

Switch#**config**

Switch(config)#**interface vlan 100**

Switch(config-if)#**ip address 20.100.0.100 255.255.255.0**

Switch(config-if)#**no shutdown**

Switch(config-vlan)#**exit**

Step 2: configure TFTP-SERVER1

```

Switch(config)#tftp-server flash:startup_config.conf

Step 3: configure DHCP-SERVER1 on VLAN 100:
Switch(config)#ip dhcp pool newpool

Switch(dhcp-config)#network 20.100.0.100 255.255.255.0
Switch(dhcp-config)#option 150 ip 20.100.0.100
Switch(dhcp-config)#exit

Step 4: configure port 2 to access mode and enter VLAN 200
Switch(config)#interface G 1/0/2
Switch(config-if)#switch mode access
Switch(config-if)#switch access vlan 200
Switch(config-if)#exit

Step 5: configure port 3 to access mode and enter VLAN 200
Switch(config)#interface G 1/0/3
Switch(config-if)#switch mode access
Switch(config-if)#switch access vlan 200
Switch(config-if)#exit

Step 6: configure port 1 to Trunk mode and native VLAN to 100
Switch(config)#interface G 1/0/1
Switch(config-if)#switch trunk encapsulation dot1q
Switch(config-if)#switch mode trunk
Switch(config-if)#switch trunk native vlan 100

```

The content of the configuration file **startup_config.conf** that is added to TFTP-SERVER1:

```

!ROS Version 3.7.1043.ISCOM2009.84.20080602
!command in view_mode
!
!command in config_mode first-step
Schedule-list 0 startup-time 0 0:30:0 every 0 0:50:0
create vlan 200 active
!
!command in enable_mode
!
!command in ip igmp profile mode
!
!command in port_mode
Interface port 8
Switch mode trunk

```

```

!
!command in vlan configuration mode
!
!command in ip interface mode
interface ip 0
ip address dhcp 200
ip dhcp client renew schedule-list 0
!
!command in cluster_mode
!
!command in config_mode
service config filename filename rule 81260
service config overwrite enable
service config

```

Note: If you want to gain renewed file information periodically, you need to renew a contract regularly. You need to configure command schedule-list 0 start up-time 0 0:30:0 every 0 0:50:0 and ip dhcp client renew schedule-list 0. The deviece can also renew a contract according to DHCP protocol prescriptive time and obtain renewed file information. If the device does not configuration file (the version nummer of configuration file is 0000000), and there is no option67, then you need to download startup_config.conf, if there is a Option67, then you need to download “rule string”. The vesion number is 0000001 after downloading successfully. In the next renewed procedure, you can download “configuration file name-version” or “rule string-version” file, after downloading, renewed configuration file version number is file version number. When there is a rule NO., then it will be priority.

4.Configure PC1

Start DHCP service on PC1:

IP address: 20.100.10.101

DHCP related configuration: DHCP server (DHCP-SERVER2), Option150: 20.100.10.102; Option17: raisecom\image\2109A##0906035;2924GF#0906053, Option67: raisecom\config\81260#0906032.

IP pool start address: 20.100.10.1

IP pool ending address: 20.10.10.220

5.Configure PC2

Start TFTP service on PC2:

IP address: 20.100.10.102

TFTP configuration: server (TFTP-SERVER2), the configuration file ISCOM2009A_M000E_ROS_3-0906032 will be saved in raisecom\config, while system-boot file BOOTSTRAP-ISCOM2109A-0906035 will be saved in raisecom\image.

6.Devices Auto-update Finish

After auto-update, if there is only configuration file up-date, then you can load configuration file directly. If there is a system software up-date, then device will save the configuration and auto-restart.

7.Auto-update erratum

At present, the automatic update interval of our company's device is 10 minutes. If the auto-update is not carried out, please use monitoring command **show service config** and view whether auto-update is running. If it is running but not up-date, please use **show ip dhcp client** command view whether auto-update option is correct. If the above conditions are no problem, please view whether TFTP server relevant file catalog is correct and whether relevant renewed file name accords with Specification (please refer to view download rule and resolution rule). At the same time, you can open auto-update debugging information **debug service config** under Enable mode and **logging console debugging** under Config mode. To view auto-update procedure debugging information, you can find the unsuccessful factors.

Note: Some path separators of operation systems are not the same, some only supports “/” or “\”, the auto-update inforamtion under DHCP Server, the path information can only be recongnized by TFTP. At present, our company file system supports two path separators.

Chapter 34 Function Configuration of Ethernet Ring

34.1 Overview

Most Ethernet network uses star or dual-homed structure (as shown in figure 34-1). Usually star network is used in access layer without protective redundancy, and a single fault of a critical point may lead to network unavailable. Dual-homed network is usually used on or above in the aggregation layer of the network, which supports protective redundancy, but needs dual equipment and lines and lead to network resource waste. Both the two typical link mode has the inborn limitation on network response time, protection mechanism and multicast.

As Ethernet develops to metropolitan area network, voice and video multicast have more need on Ethernet protective redundancy and fault recovery time. The former STP mechanism needs seconds for fault recovery convergence, which is far from metropolitan area network's need on fault recovery.

Ethernet ring technology is a solution to the problem mentioned above. As a metropolitan Ethernet technology, Ethernet ring helps traditional data network from the problems like poor protection ability and long fault recovery time, and it provides 50ms rapid protection in theory. At the same time, it is compatible to typical Ethernet protocols. It's an important technology and solution to MAN access network optimization and improvement.

Raisecom Ethernet ring technology uses self-developed protocol and simple configuration, realize the function like removing loop, fault protection switching and automatic fault recovery, and the fault switching time is less than 50ms.

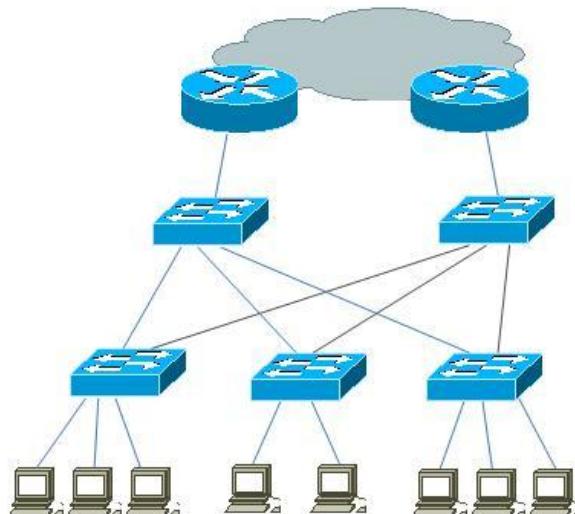


Figure 34-1 Dual-homed network topology

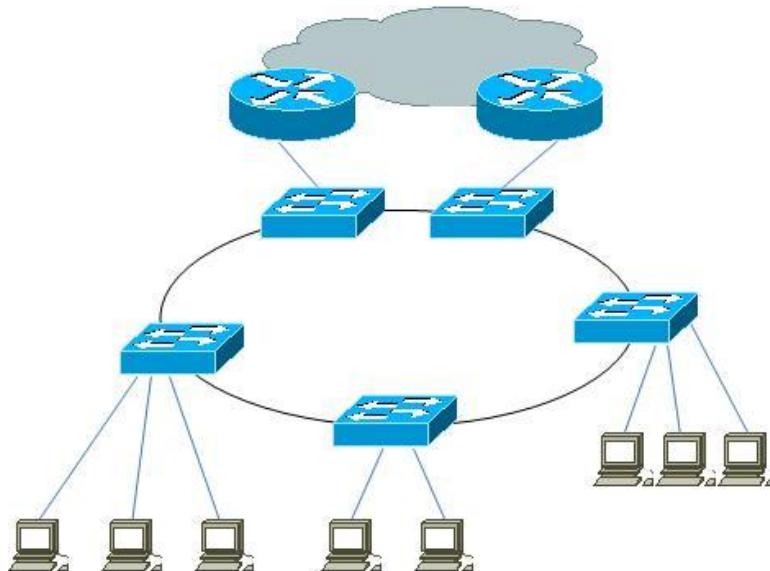


Figure 34-2 Ring network topology

34.2 Default configuration list of Ethernet ring

Function	Default value
Hello message sending interval	1s
Delay time of fault recovery	5s
Bridge priority	1
Description of ring	Ethernet ring X
Aging time of ring port	15s
Ring protocol message	2

Note: To all the equipments on a ring, it is suggested to configure the values of the parameters that delay time of fault recovery, holle message sending interval, ring protocol message, aging time of ring port to the same.

34.3 Function configuration of Ethernet ring

34.3.1 Create and delete ring

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port primary port	Enter primary port mode.
3	ethernet ring <1-8> secondaryport	Create ring and configure the corresponding ring port.
4	exit	Return to global configuration mode.
5	exit	Return to privileged EXEC mode.

6	show ethernet ring	Show ring configuration.
7	config	Enter global configuration mode.
8	interface port secondary port	Enter secondary port mode.
9	no ethernet ring <1-8>	Delete ring.

Note: You can delete Ethernet ring in both primary port mode and secondary mode.

34.3.2 Configure ring switch

By default, ring switch is disabled.

Step	Command	Description
1	config	Enter global configuration mode.
2	ethernet ring X enable	Enable ring switch.
3	show ethernet ring	Show ring configuration information.

34.3.3 Configure sending interval of Hello message

Step	Command	Description
1	config	Enter global configuration mode.
2	ethernet ring X hello-time 5	Configure Ethernet ring hello time.
3	exit	Quit from global configuration mode and enter privileged EXEC mode.
4	show ethernet ring	Show Ethernet ring information.

34.3.4 Configure fault-delay

Step	Command	Description
1	config	Enter global configuration mode.
2	ethernet ring X restore-delay 10	Configure Ethernet ring restore delay.
3	exit	Quit from global configuration and enter privileged EXEC mode.
4	show ethernet ring	Show Ethernet ring information.

34.3.5 Configure bridge priority information

Step	Command	Description
1	config	Enter global configuration mode.
2	ethernet ring X priority 3	Configure Ethernet ring bridge priority.

3	exit	Quit from global configuration mode and enter privileged EXEC mode.
4	show ethernet ring	Show Ethernet ring information.

34.3.6 Configuration ring description information

Step	Command	Description
1	config	Enter global configuration mode.
2	ethernet ring <i>X</i> description <word>	Configure Ethernet ring description information.
3	exit	Quit from global configuration mode and enter privileged EXEC mode.
4	show ethernet ring	Show Ethernet ring information.

34.3.7 Configure ring port aging time

Step	Command	Description
1	config	Enter global configuration mode.
2	ethernet ring <i>X</i> hold-time <3-360>	Configure Ethernet ring port aging time.
3	exit	Quit from global configuration mode and enter privileged EXEC mode.
4	show ethernet ring	Show Ethernet ring information.

34.3.8 Configure ring protocol vlan

Step	Command	Description
1	config	Enter global configuration mode.
2	ethernet ring <i>X</i> protocol-vlan <2-4094>	Configure Ethernet ring protocol vlan.
3	exit	Quit from global configuration mode and enter privileged EXEC mode.
4	show ethernet ring	Show Ethernet ring information.

34.3.9 Clear ring port static.

Step	Command	Description
1	config	Enter global configuration mode.
2	clear Ethernet ring <i>X</i> statistics	Clear ring port static.

3	exit	Quit global configuration mode and enter privileged EXEC mode.
4	show ethernet ring port statistic	Show Ethernet ring port message static.

34.3.10 Configure upstream-group

Step	Command	Description
1	config	Enter global configuration mode.
2	ethernet ring upstream-group {1-10}	Configure upstream-group.
3	exit	Quit global configuration mode and enter privileged EXEC mode.
4	show ethernet ring	Show Ethernet ring information.

Note:

- The upstream-group must combine the failover, to support the application of dual attribution topological.
- The upstream-group number corresponds to failover number.

34.4 Monitoring and maintenance

Use **show** commands to view the switches on the Ethernet ring configuration and running situations, in order to carry out the monitoring and maintenance. The **show** command used in monitoring and maintenance are as follows:

Command	Description
show ethernet ring [ringID]	Show all/designated Ethernet ring infomration
show ethernet ring [ringID] port	Show all/designated Ethernet ring port information
show ethernet ring port statistic	Show ring port message static.

34.4.1 Ethernet ring information monitoring

Use **show ethernet ring** to show the priority of Ethernet ring, hello time and fault recovery delay time, you can also check out local node state and nodes state, main node information (red means the option can be configured). Specified configuration is shown below:

Raisecom# **show ethernet ring RingId**

Ethernet Ring Upstream-Group: 1

Ethernet Ring 1:

Ring Admin: Enable

Ring State: Unenclosed

Bridge State: Down
Ring state duration: 0 days, 3 hours, 30 minutes, 15 seconds
Bridge Priority: 1
Bridge MAC: 000E.5E03.5B81
Ring DB State: Down
Ring DB Priority: 1
Ring DB: 000E.5E03.5B81
Hello Time: 1
Restore delay: 5
Hold Time: 15
Protocol Vlan: 2

34.4.2 Ethernet ring port information monitoring

User can use **show Ethernet ring port** to show Ethernet ring port information, including ring port, the actual effected ring port number and ring equipment list.

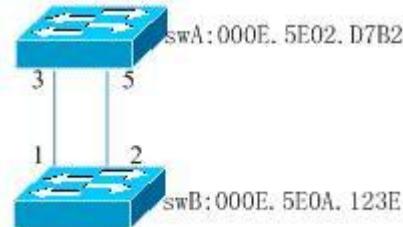


Figure 34-3 Single ring topology

In the figure above, two equipments forms a ring network, on swA ring network port it is shown:

swA#show Ethernet ring port

< Ethernet ring description, by default it is Ethernet ring X>

Ethernet Ring 1:

Primary Port: 3
State: Block
Port Active State: Active
State: Block
Peer State: None
Switch counts: 5

Current state duration: 0 days, 3 hours, 32 minutes, 33 seconds

Peer Ring Node:

--1:000E.5E0A.123E:2--

Secondary Port: 5
State: Block

Port Active State: Active
State: Forward
Peer State: None
Switch counts: 6

Current state duration: 0 days, 3 hours, 32 minutes, 37 seconds

Peer Ring Node:

--2:000E.5E0A.123E:1--

swA#show ethernet ring port statistics

< Ethernet ring description, by default it is Ethernet ring X>

Primary Port: 3
Receive hello packets: XX
Receive change packets: XX
Receive change relay packets: XX
Receive flush packets: XX
Send hello packets: XX
Send change packets: XX
Send change relay packets: XX
Send flush packets: XX

Secondary Port: 5
Receive hello packets: XX
Receive change packets: XX
Receive change relay packets: XX
Receive flush packets: XX
Send hello packets: XX
Send change packets: XX
Send change relay packets: XX
Send flush packets: XX

34.5 Typical configuration illustration

34.5.1 Ethernet ring typical application

Raisecom Ethernet ring itself can be used in single ring or tangent dual ring networking topology;
 We will introduce them respectively.

34.5.2 Configuration illustration of single ring

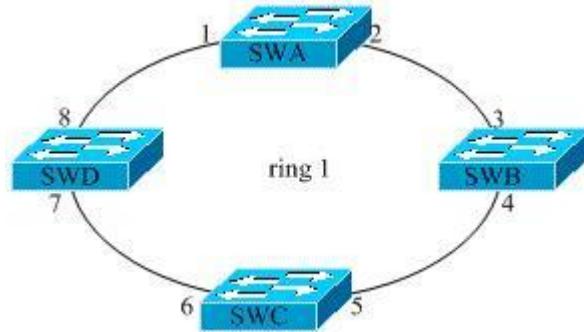


Figure 34-4 Single ring

As shown in above figure, the ring1 consists of four equipments SWA, SWB, SWC and SWD. Map marked the four devices to join ring port of the ring 1. Mac addresses are: SWA (000E.5E00.000A), SWB (000E.5E00.000B), SWC (000E.5E00.000C), and SWD (000E.5E00.000D).

34.5.2.1 Configuration Steps

SWA

SWA#config

SWA (config) #**interface port 1**

SWA (config-port) #**ethernet ring 1 2**

SWA (config) #**ethernet ring 1 enable**

SWB

SWB#config

SWB (config) #**interface port 3**

SWB (config-port) #**ethernet ring 1 4**

SWB (config) #**ethernet ring 1 enable**

SWC

SWC#config

SWC (config) #**interface port 5**

SWC (config-port) #**ethernet ring 1 6**

SWC (config) #**ethernet ring 1 enable**

SWD

SWD#config

SWD (config) #**interface port 7**

SWD (config-port) #**ethernet ring 1 8**

SWD (config) #**ethernet ring 1 enable**

34.5.2.2 Normal ring status

If the ring is normal, first ring port of master node SWD: port 7 is blocked, to dismiss data ring loop.

Here we can see that ring status and port status of masker node SWD and a normal node SWB:

SWD

SWD# show ethernet ring

Ethernet Ring Upstream-Group: 1

Ethernet Ring 1:

Ring Admin: Enable

Ring State: Enclosed

Bridge State: Block

Ring state duration: 0 days, 3 hours, 30 minutes, 15 seconds

Bridge Priority: 1

Bridge MAC: 000E.5E00.000D

Ring DB State: Block

Ring DB Priority: 1

Ring DB: 000E.5E00.000D

Hello Time: 1

Restore delay: 5

Hold Time: 15

Protocol Vlan: 2

SWD#show ethernet ring port

Ethernet Ring 1:

Primary Port: 7

State: Block

Port Active State: Active

Peer State: Full

Switch counts: 5

Current state duration: 0 days, 3 hours, 32 minutes, 33 seconds

Peer Ring Node:

--6:000E.5E00.000C:5--

--4:000E.5E00.000B:3--

--2:000E.5E00.000A:1--

Secondary Port: 8

State: Block

Port Active State: Active

Peer State: Full

Switch counts: 6

Current state duration: 0 days, 3 hours, 32 minutes, 37 seconds

Peer Ring Node:

--1:000E.5E00.000A:2--
--3:000E.5E00.000B:4--
--5:000E.5E00.000C:6--

SWD#show ethernet ring port statistic

Primary Port: 7

Receive hello packets: xx
Receive change packets: xx
Receive change relay packets: xx
Receive flush packets: xx
Send hello packets: xx
Send change packets: xx
Send change relay packets: xx
Send flush packets: xx

Secondary Port: 8

Receive hello packets: xx
Receive change packets: xx
Receive change relay packets: xx
Receive flush packets: xx
Send hello packets: xx
Send change packets: xx
Send change relay packets: xx
Send flush packets: xx

SWB

SWB# show ethernet ring

Ethernet Ring Upstream-Group:1

Ethernet Ring 1:

Ring Admin: Enable
Ring State: Enclosed
Bridge State: Two-Forward
Ring state duration: 0 days, 3 hours, 30 minutes, 15 seconds
Bridge Priority: 1
Bridge MAC: 000E.5E00.000B
Ring DB State: Block
Ring DB Priority: 1

Ring DB: 000E.5E00.000D
Hello Time: 1
Restore delay: 5
Hold Time: 15
Protocol Vlan: 2

SWB#show ethernet ring port

Ethernet Ring 1:
Primary Port: 3
State: Forward
Port Active State: Active
Peer State: Full
Switch counts: 5
Current state duration: 0 days, 3 hours, 32 minutes, 33 seconds
Peer Ring Node:
--2:000E.5E00.000A:1--
--8:000E.5E00.000D:7--
--6:000E.5E00.000C:5--

Secondary Port: 4
State: Forward
Port Active State: Active
Peer State: Full
Switch counts: 6
Current state duration: 0 days, 3 hours, 32 minutes, 37 seconds
Peer Ring Node:
--5:000E.5E00.000C:6--
--7:000E.5E00.000D:8--
--1:000E.5E00.000A:2--

SWB#show ethernet ring port statistic

Primary Port: 3
Receive hello packets: xx
Receive change packets: xx
Receive change relay packets: xx
Receive flush packets: xx
Send hello packets: xx
Send change packets: xx

Send change relay packets: xx
Send flush packets: xx

Secondary Port: 4
Receive hello packets: xx
Receive change packets: xx
Receive change relay packets: xx
Receive flush packets: xx
Send hello packets: xx
Send change packets: xx
Send change relay packets: xx
Send flush packets: xx

34.5.2.3 Ring status after fault protect switch

If there is a link fault between SWA and SWB, SWD port 7 will change its **block** status into **forwarding** status, SWB port 3 is going to change **forwarding** status into **block** status. The redbody is different place prepared to ring normally.

SWD

SWD# show ethernet ring

Ethernet Ring Upstream-Group: 1

Ethernet Ring 1:

Ring Admin: Enable
Ring State: Unenclosed
Bridge State: Two-Forward
Ring state duration: 0 days, 3 hours, 30 minutes, 15 seconds
Bridge Priority: 1
Bridge MAC: 000E.5E00.000D
Ring DB State: Block
Ring DB Priority: 1
Ring DB: 000E.5E00.000B
Hello Time: 1
Restore delay: 15
Hold Time: 15
Protocol Vlan: 2

SWD#show ethernet ring port

Ethernet Ring 1:

Primary Port: 7

State: **Forward**

Port Active State: **Active**

Peer State: **Full**

Switch counts: **5**

Current state duration: 0 days, 3 hours, 32 minutes, 33 seconds

Peer Ring Node:

--6:000E.5E00.000C:5--

--4:000E.5E00.000B:3--

Secondary Port: **8**

State: **Block**

Port Active State: **Active**

Peer State: **Full**

Switch counts: **6**

Current state duration: 0 days, 3 hours, 32 minutes, 37 seconds

Peer Ring Node:

--1:000E.5E00.000A:2--

SWB**SWB# show ethernet ring***Ethernet Ring Upstream-Group:* **1***Ethernet Ring 1:**Ring Admin:* **Enable***Ring State:* **Unenclosed***Bridge State:* **Block***Ring state duration:* 0 days, 3 hours, 30 minutes, 15 seconds*Bridge Priority:* **1***Bridge MAC:* **000E.5E00.000B***Ring DB State:* **Block***Ring DB Priority:* **1***Ring DB:* **000E.5E00.000B***Hello Time:* **1***Restore delay:* **15***Hold Time:* **15***Protocol Vlan:* **2****SWB#show ethernet ring port***Ethernet Ring 1:**Primary Port:* **3**

State: Block
 Port Active State: Active
 Peer State: Full
 Switch counts: 5
 Current state duration: 0 days, 3 hours, 32 minutes, 33 seconds

Peer Ring Node:

Secondary Port: 4
 State: Forward
 Port Active State: Active
 Peer State: Full
 Switch counts: 6
 Current state duration: 0 days, 3 hours, 32 minutes, 37 seconds

Peer Ring Node:

```
--5:000E.5E00.000C:6--
--7:000E.5E00.000D:8--
--1:000E.5E00.000A:2--
```

34.5.3 Tangent dual ring networking application

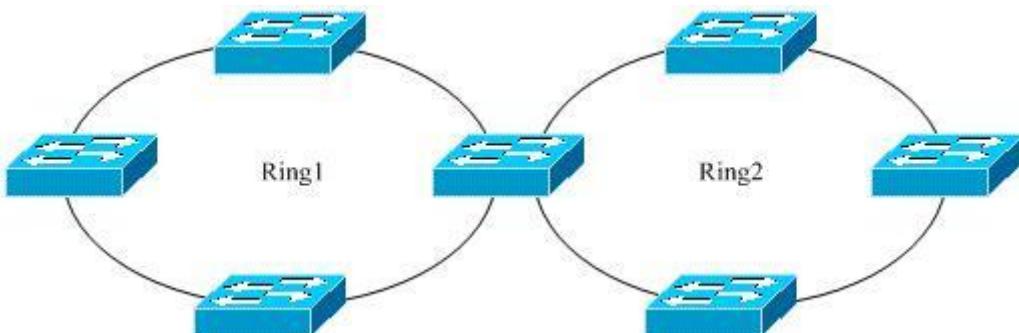


Figure 34-5 tangent dual/multi ring topology

Tangent dual ring networking shows in above figure. Dual ring is formed by two absolute rings. Thus the configuration in each ring is same as single ring. Not detailed information stated here.

34.5.4 Non-Raisecom Upstream Device

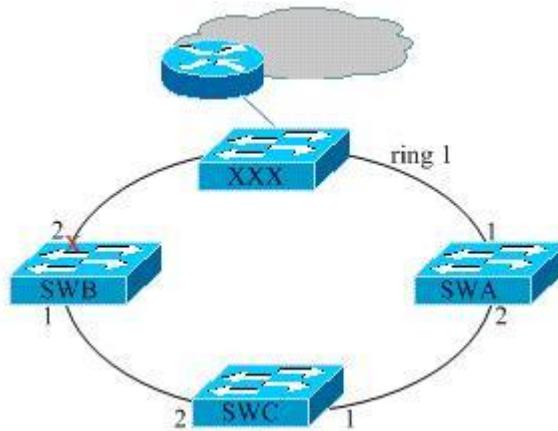


Figure 34-6

As above, ring 1 is formed by SWA, SWB, SWC, and XXX, where XXX does not support device of Raisecom Ethernet technology. Map marked ring port of the three devices to join the ring 1. Mac addresses: SWA (000E.5E00.000A), SWB (000E.5E00.000B), and SWC (000E.5E00.000C).

Normally, ring 1 is blocked at SWB port 2, because port 2 could not discover its neighbor and mac address of SWB is bigger than mac address of SWA. There is no loop of data, and each device is communicated in the ring.

Possible abnormal situations may happen are shown as below figures, X represents port block, || represents link fault.

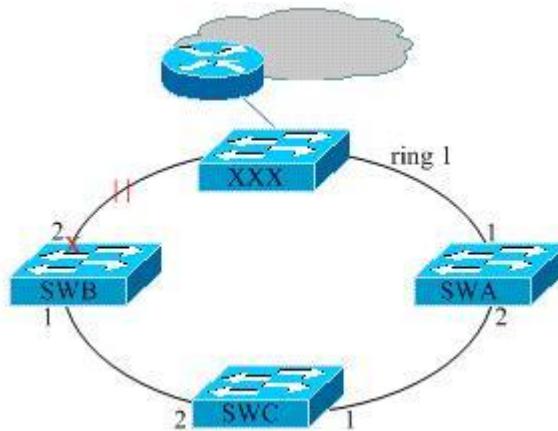


Figure 34-7

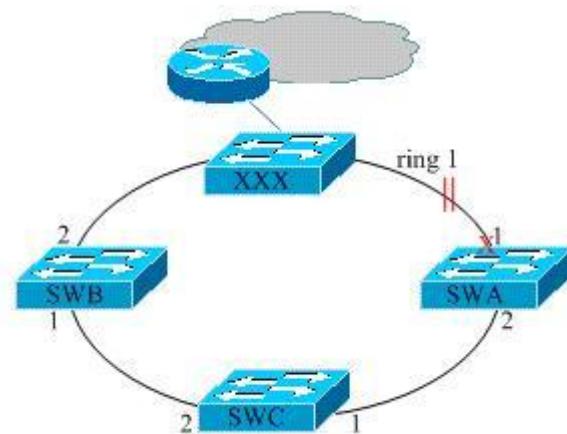


Figure 34-8

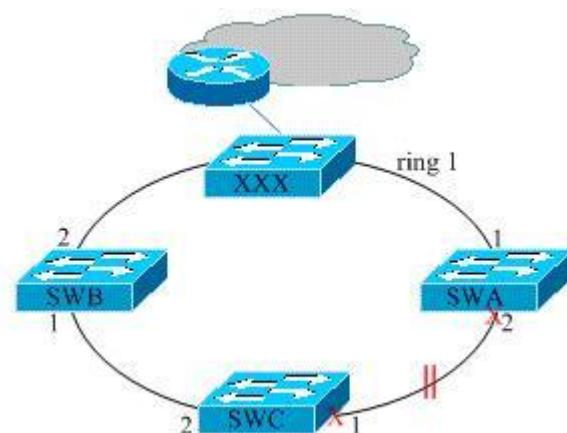


Figure 34-9

34.5.5 Typical application of looped network dual-link protection

Typical topology of dual-link protection shows as below:

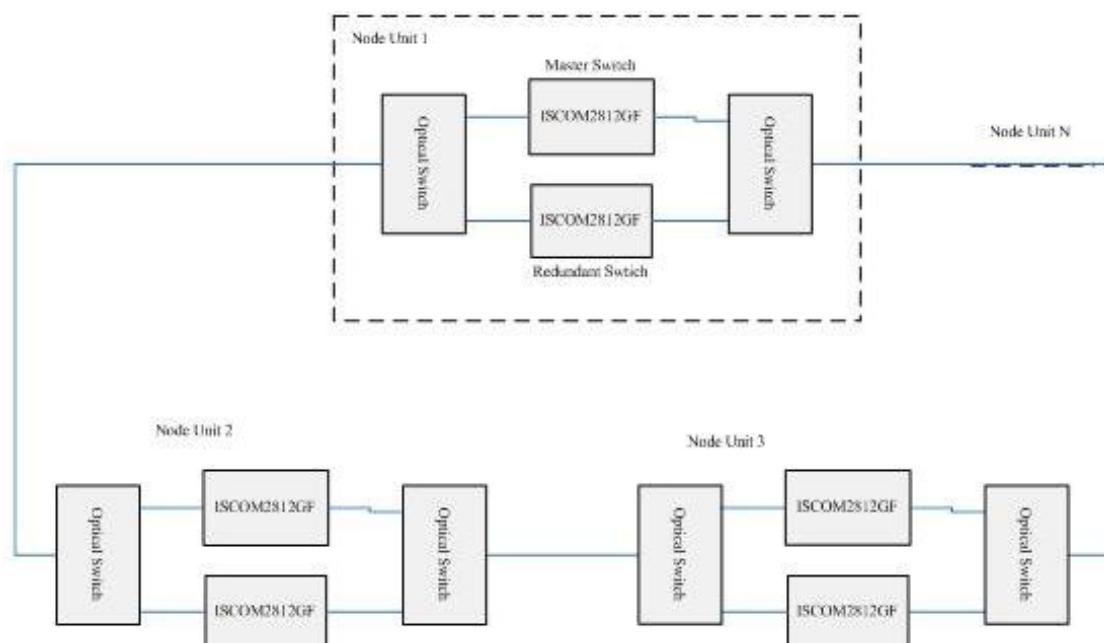


Figure 34-10 typical application diagram of dual-link protection

As shown in above figure, we give a introduction using an illustration of basic node unit 1. The basic node unit in the figure can be considered as a switch of single ring or tangent ring. When there is power fault in Node Unit 1 master switch, optical switch will detect the optical signal changing and informs Node Unit 2. The redundant switch is switched on.

In typical application of dual-link protection, we use optical switch and ISCOM series switches to achieve dual assurance: fault fast switch and link redundancy. This case is mainly used in more safety areas as power factory, banks, etc.

Note: If link is normal, optical switches should be connected to master switch for normal communication.

Figures below shows different fault situations, || represents link fault.

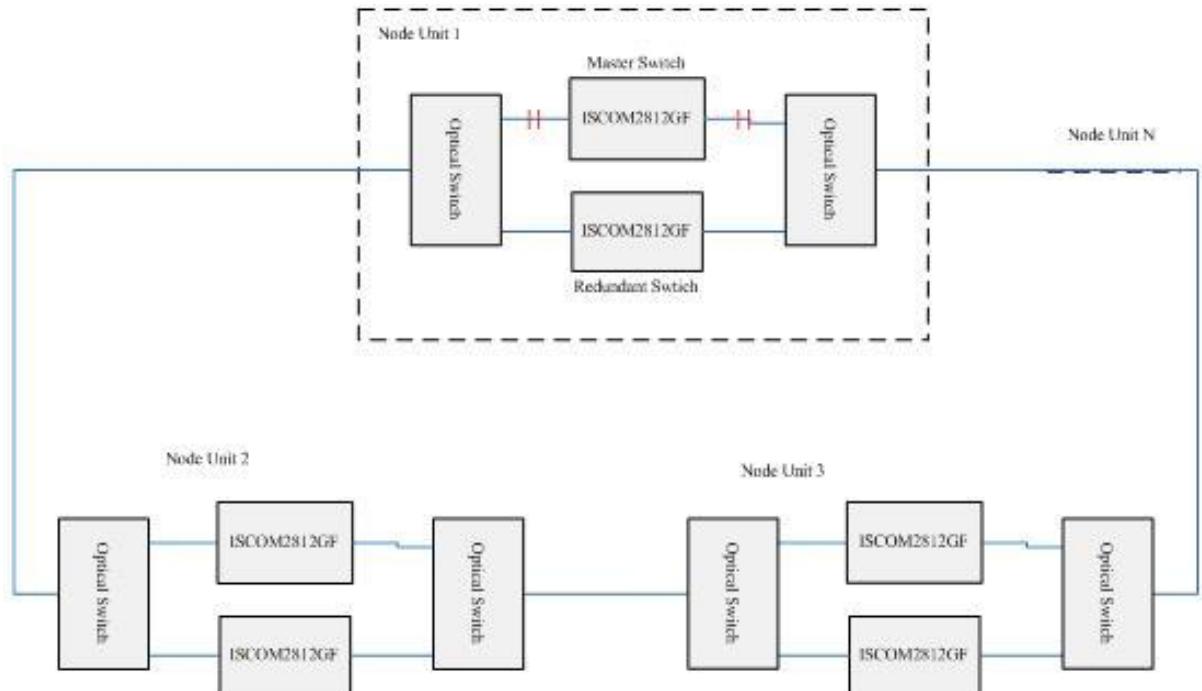


Figure 34-11 abnormal 1 of dual link protection

If there is link fault at master device, we can see it in the figure 34-11. Optical switch can detect optical signal in DOWN event quickly and switch link to redundant switch for normal communication.

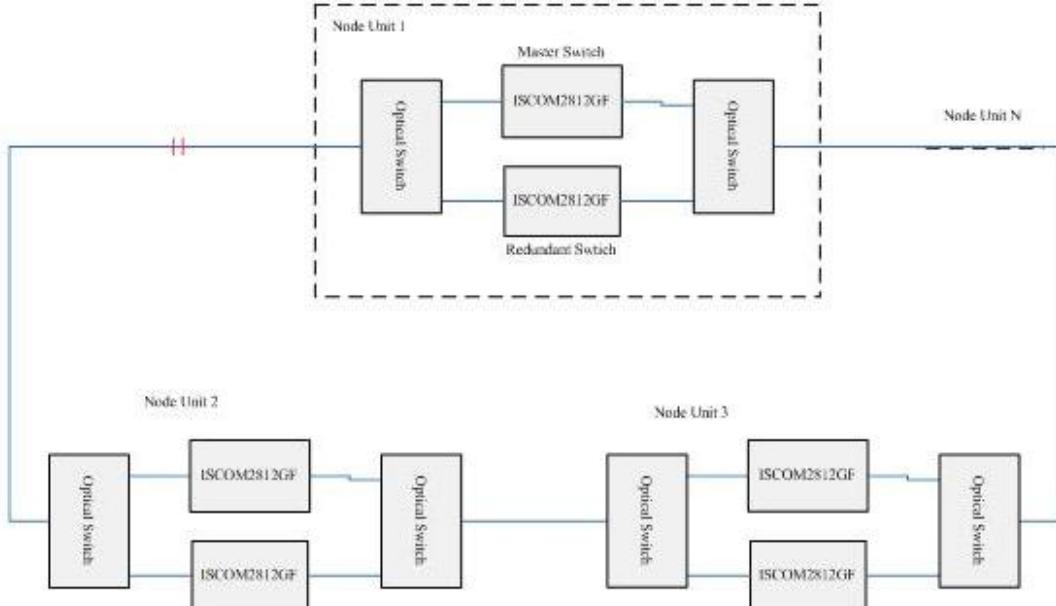


Figure34-12 abnormal 2 of dual link production

If there is link fault between Node Units, as figure 34-12, Fault ends of node unit rapidly detect fault and notifies the master node, the master node unit unlocks alternate blocking port to achieve rapid fault switching purposes.

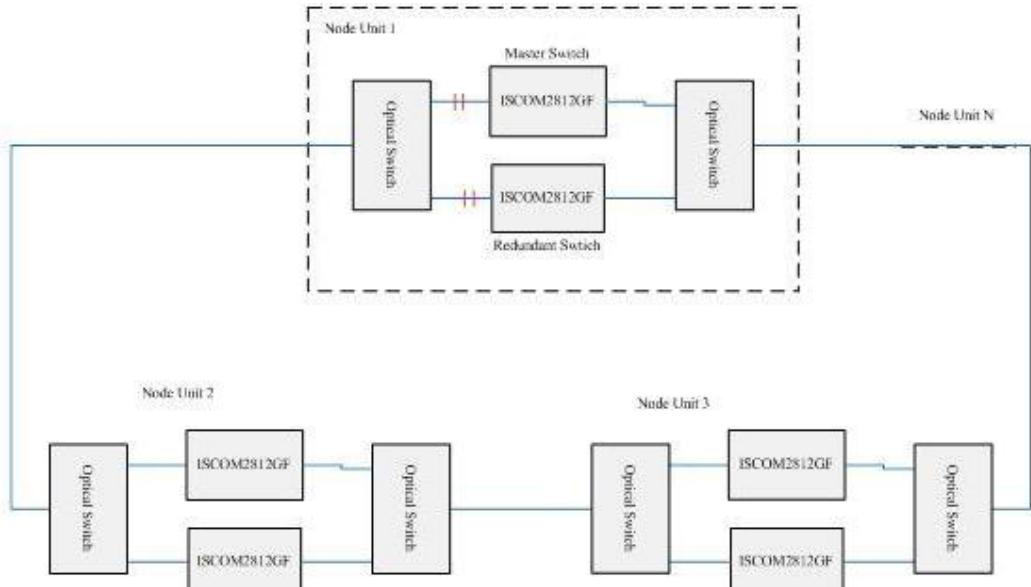


Figure34-13 abnormal 3 of dual link production

If there is unilateral link fault in both master and redundant switches, the ring network is in uncompleted status. The master equipment will prompt notice link failure event to the master node unit, the master node unit open blocked port to ensure normal communication.

34.5.6 Typical application of dual homing topology

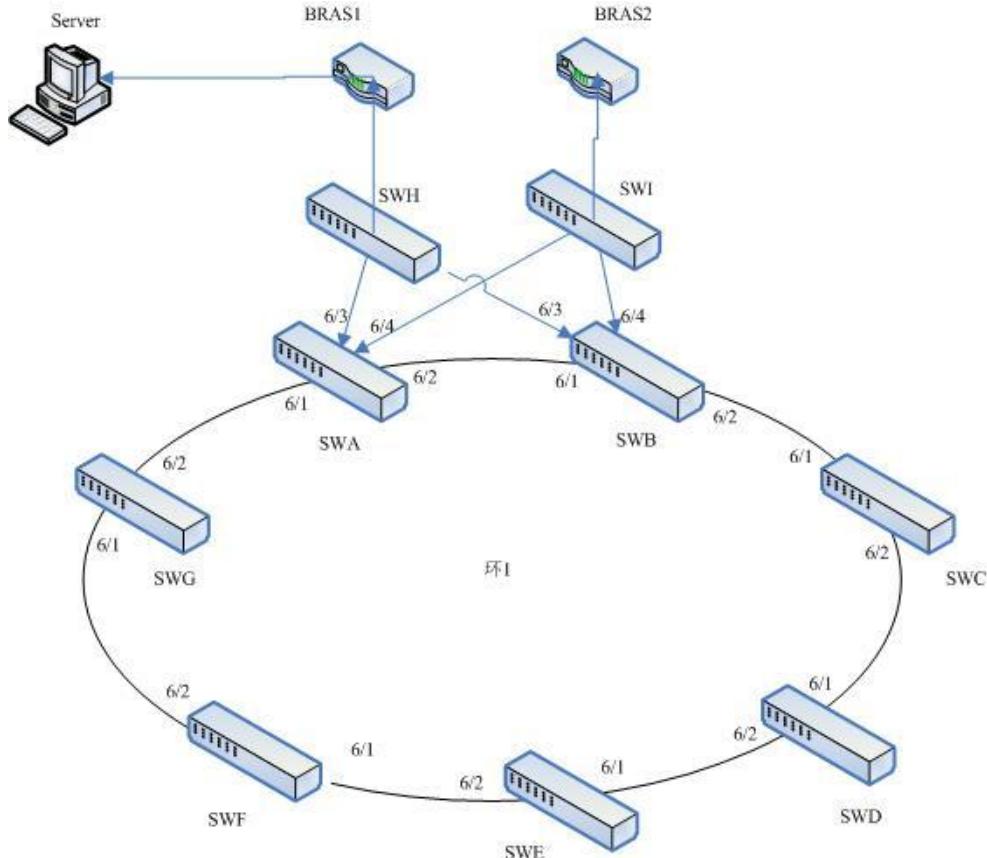


Figure 34-14 Dual homing topology networking

As shown in above figure, SWA ~ SWG (OLT) composes ring 1 by seven devices, upstreamed two switches SWI and SWH. Enable port backup on SWI and SWH, set restore-delay for 0; compared with SWC ~ SWG, SWA and SWB not only open Ethernet ring, but also configure failover group and Ethernet ring upstream-group;

34.5.6.1 Configuration Steps:

```

SWA
SWA#config
    SWA(config)#interface port 1
    SWA(config-port)#ethernet ring 1 2
    SWA(config)#ethernet ring 1 enable
    SWA(config)#link-state-track group 1
    SWA(config)#link-state-track group 2
    SWA(config)#interface port 3
    SWA(config-port)#link-state-group 1 upstream
    SWA(config-port)#switchport trunk allowed vlan 1-100
    SWA(config-port)#exit
    SWA(config)#interface port 4
    SWA(config-port)#link-state-group 2 upstream

```

```
SWA(config-port)#switchport trunk allowed vlan 101-200  
SWA(config-port)#exit  
SWA(config)#ethernet ring upstream 1,2
```

```
SWB  
SWB#config  
SWB(config)#interface port 1  
SWB(config-port)#switchport backup port 2 vlanlist 1-100  
SWB(config-port)#exit  
SWB(config)#switchport backup restore-delay 0
```

```
SWC  
SWC#config  
SWC(config)#interface port 1  
SWC(config-port)#ethernet ring 1 2  
SWC (config) #ethernet ring 1 enable
```

Configuration steps of other equipments are similar, so not do in detail.

The network can not only realize the load sharing, which vlan1-100 and vlan101-200 respectively take different upstream equipment SWH and SWI; but also has a mutual backup. Then when SWI or SWH is at fault, related service can smooth switch to another one.

Chapter 35 Failover Configuration

35.1 Overview of failover

Failover function is used to provide port linkage scheme for specific application and it can extend range of link backup. Doing synchronization setting of downstream by monitoring the upstream, the fault from upstream can be rapidly passed to downstream devices if upstream faults, so as to trigger the switchover of backup link and prevent flow loss for long time upstream fault.

Failover group consists of upstream port and downstream port. A failover group can have multiple upstream ports and a plurality of downstream port. Upstream port will be real-time monitored when failover group is configured. All downstream ports of the group will be forced to DOWN once all upstream ports of the failover group failure. When one or more ports of the upstream ports are recover to normal, the downstream port restores UP state. Failure of downstream port neither affects the status of upstream port, nor other downstream port.

Failover is generally applied to the network topology of dual upstream or multi-upstream. When the master link failure, ensure fast switching from the master link to the backup link by transferring the upstream port fault to the downstream port. In the dual upstream network, when one upstream is redundant block, the other link will be used to forward. When link failure, intermediate switches pass the fault to downstream switch rapidly and notify downstream switch to perform link switch to reduce flow loss.

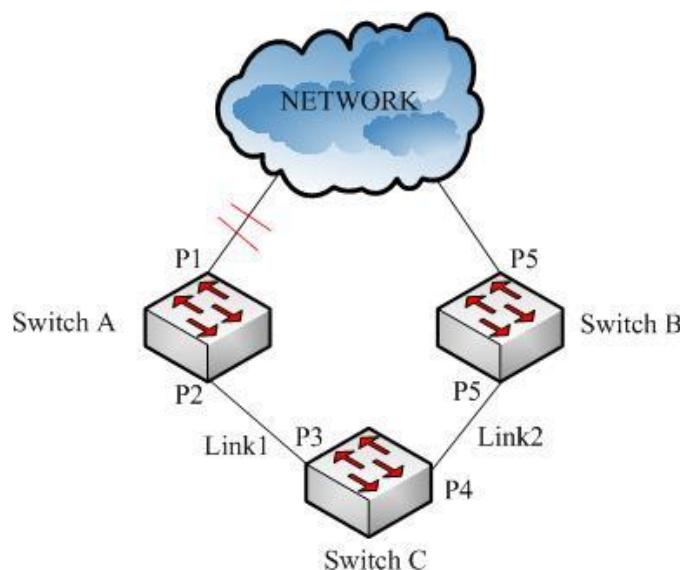


Figure 35-1 failover

As shown in Figure above, Switch C is connected to NETWORK via the main link Link1 and the backup link Link2. When the link between Switch A and NETWORK fails, Switch A passes the fault to downstream port rapidly, then the Link1 becomes disconnected. Switch C detects Link1 disconnection and switches to Link2 quickly, thereby realizing fast switching of failover.

35.2 Failover configuration

Failover configuration includes configuration of failover group and failover port and a switch supports 1- 10 failover groups. We create failover group firstly, and then add the port into the failover group and a port can only belong to a failover group. The specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode.
2	link-state-tracking group <i>groupNumber [upstream cfm-mepid mepid]</i>	Create and enable failover group. If this fault transfer group did not create, first create the metastasis group and then enable it. <i>groupNumber</i> : failover group number, range 1-10. <i>mepid</i> : failover group upstream MEP ID.
3	interface port <i><1-MAX_PORT_NUM></i>	Enter physical port mode.
4	link-state-tracking group <i>groupNumber {upstream downstream}</i>	Configure failover group which port belongs to and port type <i>groupNumber</i> : failover group number, range 1-10; upstream : upstream ports. downstream : downstream ports.
5	exit	Return to global configuration mode.
6	exit	Return to privilege mode.
7	show link-state-tracking group [<i>groupNumber</i>]	Show configuration and state information of failover group.

Use the **no link-state-tracking group** *groupNumber* command to delete the failover group.

Use the **no link-state-tracking group** command will remove port from failover group.

Note:

- Create a failover group specified on the upstream MEP, failover group is failover group based on MEP fault type , and we cannot add port into upstream port of failover group based on MEP fault type;
- A failover group can have many upstream ports, and as long as there is an upstream port is UP state, there is not failover; only when all the upstream port is DOWN state, there is failover.

35.3 Monitoring and maintenance

Command	Description
show link-state-tracking group [<i>groupNumber</i>]	Show configuration and state of failover group.
show link-admin-status port <i>portlist</i>	Show UP/DOWN management state of port.

Note:

- Use the **show link-state-tracking group [groupNumber]** command does not display failover group information which was created but not enabled, and there isn't failover information of port.

35.4 Typical configuration illustration

35.4.1 Failover group application based on port

Failover typical topology structure based on ports as shown in Figure 35-2:

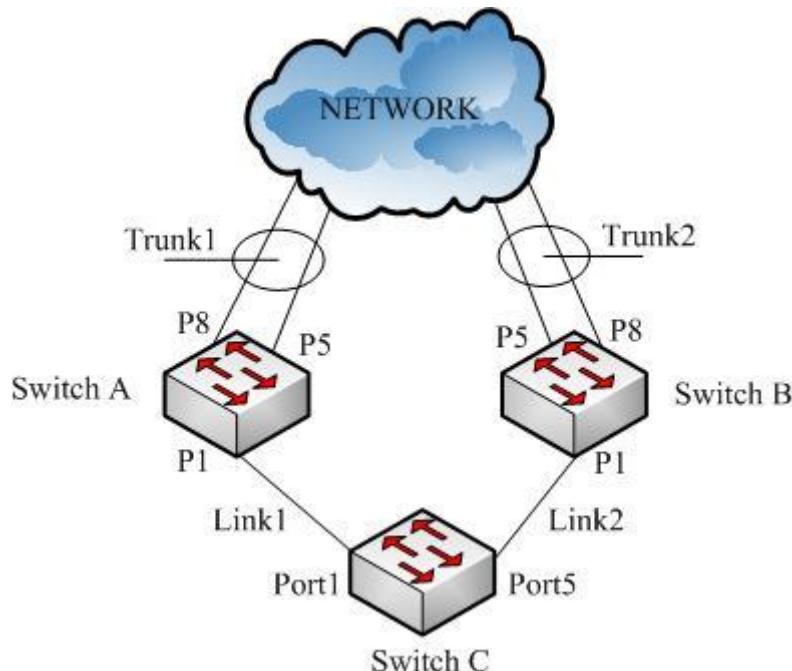


Figure 35-2 Failover typical topology structure based on ports

Topology structure shows as Figure 35-2, Switch C upstreams via two links Link1 and Link2 in order to ensure the reliability of the network. Switch A and Switch B connected to the network via Trunk1 and Trunk2. Switch C enables and generates spanning tree protocol, and Link2 is in the discarding state. When the Link1 breaks, spanning tree will immediately switch the connection to the Link2. But if upstream Trunk1 circuit of Switch A breaks, the Switch C may not be able to quickly detect the connected channels which have been blocked, thus causing packet loss. If the Trunk1 circuit breaks, Switch A will also disconnect downstream port, then the Switch C immediately switch upstream channel to Link2 in order to ensure the unlocked upstream channel. Therefore, we configure failover group in the Switch A and Switch B, failover group configuration of Switch A and Switch B are the same. Here we only explain configuration method of Switch A.

Configuration of Switch A as follows:

```
Raisecom#config
```

```
Raisecom(config)#link-state-tracking group 1
```

```
Raisecom(config)#intface port 1
```

```
Raisecom(config-port)#link-state-tracking group 1 downstream
```

```
Raisecom(config-port)#exit
```

```
Raisecom(config)#intface range 5,8
Raisecom(config-range)#link-state-tracking group 1 upstream
Raisecom(config-range)#exit
Raisecom(config)#exit
Raisecom#show link-state-tracking group 1
Raisecom#show link-admin-status port 1, 5, 8
```

Link State Tracking Group: 1 (Enable)

Status: Normal

Upstream Interfaces:

Port5(Down) Port8(Up)

Downstream Interfaces:

Port1(Down)

<i>Port</i>	<i>module</i>	<i>admin</i>
<hr/>		
<i>1</i>	<i>shutdown</i>	<i>Up</i>
	<i>LoopbackDetect</i>	<i>Up</i>
	<i>linkStateTrack</i>	<i>Up</i>
<i>5</i>	<i>shutdown</i>	<i>Up</i>
	<i>LoopbackDetect</i>	<i>Up</i>
	<i>linkStateTrack</i>	<i>Up</i>
<i>8</i>	<i>shutdown</i>	<i>Up</i>
	<i>LoopbackDetect</i>	<i>Up</i>
	<i>linkStateTrack</i>	<i>Up</i>

If the upstream Trunk1 circuit of SwitchA breaks, the configuration results shows as follows:

Link State Tracking Group: 1 (Enable)

Status: Failover

Upstream Interfaces:

Port5(Down) Port8(Down)

Downstream Interfaces:

Port1(Disable)

<i>Port</i>	<i>module</i>	<i>admin</i>
<hr/>		
<i>1</i>	<i>shutdown</i>	<i>Up</i>

	<i>LoopbackDetect</i>	<i>Up</i>
	<i>linkStateTrack</i>	<i>Down</i>
5	<i>shutdown</i>	<i>Up</i>
	<i>LoopbackDetect</i>	<i>Up</i>
	<i>linkStateTrack</i>	<i>Up</i>
8	<i>shutdown</i>	<i>Up</i>
	<i>LoopbackDetect</i>	<i>Up</i>
	<i>linkStateTrack</i>	<i>Up</i>

35.4.2 Failover group application based on MEP fault

Typical topology structure of failover group based on MEP fault as shown in Figure 35-3:

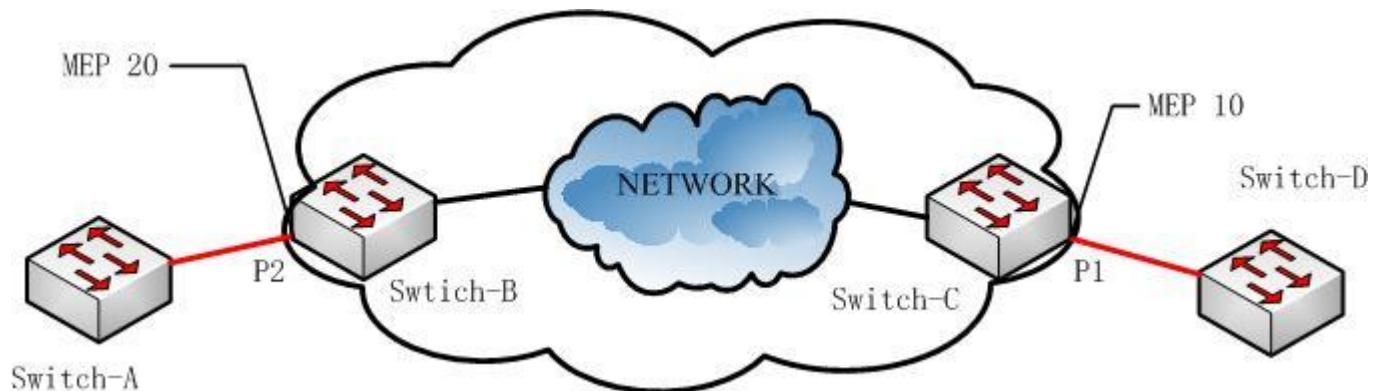


Figure 35-3 typical topology structure of transfer group based on MEP fault

Topology structure is shown in figure 35-3. Switch-A and Switch-D belong to the user domain device, the intermediate region is the operator domain. When the equipment of Switch-D or Switch-A and link of operation domain fail, we need to transfer the fault to the other user domain equipment Switch-A or Switch-D. In this case, it requires configure failover group based on MEP fault in Switch-B and Switch-C equipment, and we need configure MEP of the port which is used in the link between Switch-C and Switch-B device and user domain device. When the link between Switch-C or Switch-B and Switch-D or Switch-B fails, MEP will pass fault information to the Switch-B or Switch-C of the other end, Switch-B and Switch-C pass fault to equipment of user domain through failover function. Assuming that the CFM configuration in the operator domain is complete, P1 port of Switch-C configure MEP 10, P2 port of Switch-B configure MEP 20. Failover function of Switch-B equipment shown as follows, failover configuration of Switch-C equipment similar to Switch-B, here is no longer a detailed description.

Failover configuration of Switch-B:

Raisecom#config

Raisecom(config)#link-state-tracking group 1 upstream cfm-mepid 10

Raisecom(config)#intface port 2

Raisecom(config-port)#link-state-tracking group 1 downstream

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#**show link-state-tracking group 1**

Link State Tracking Group: 1 (Enable)

Status: Normal

Upstream Mep: 10

Upstream Interfaces:

Downstream Interfaces:

Port2(Up)

If the link between Switch-C and Switch-D fails, configuration result shown as follows:

Link State Tracking Group: 1 (Enable)

Status: Failover

Upstream Mep: 10

Upstream Interfaces:

Downstream Interfaces:

Port2(Disable)

Chapter 36 TACACS+ Configuration

This chapter introduces how to configure TACACS+ on switches and the contents are:

- ❖ TACACS+ Overview
- ❖ TACACS+ Function Configuration
- ❖ TACACS+ Monitoring and Maintenance

36.1 TACACS+ Theory

TACACS is a simple control protocol based on UDP initially which was developed by BBN for MEILNET; Cisco has improved several times on it, so called XTACACS; TACACS+ is the newest version of TACACS. Now, there are three versions of TACACS, and the third version TACACS+ is not compatible with the old two versions.

TACACS+ is the newest version of TACACS and it has certain improvements compared with old versions:

- It separates authentication, authorization and fee service;
- It encrypts all data except message head between NAS and server instead of only encrypting password.
- It is based on TCP, rather than UDP like the old version. Tacacs+'s port number is 49.

TACACS+ provide access control service for router, network access server and other network process devices through one or more central servers. TACACS+ can provide separately authentication, authorization and charging service.

Figure 36-1 shows the relationship among clients, NAS and TACACS+ server. We can say AAA application which runs on NAS is the server end to client; however, we also can say that AAA application is client end to TACACS+ server; TACACS+ protocol describes the telecommunication mechanism between NAS and TACACS+ server.

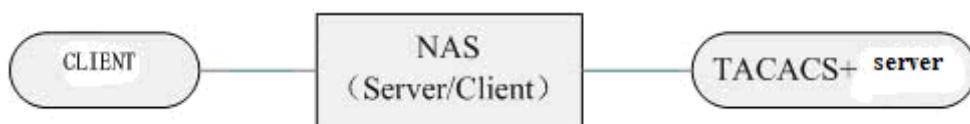


Figure 36-1 relationship among client, NAS and TACACS+ server

36.2 TACACS+ Function Configuration

36.2.1 TACACS+ Function Default Configuration

In default, switch does not configure tacacs+ authorization server address and shared key. Client login mode and enable login mode are both set as local-user.

36.2.2 TACACS+ function configuration

- Configure tacacs+ server address and shared key:

Steps	Commands	Description
1	tacacs-server <i>A.B.C.D</i>	Configure tacacs+ server address.
2	tacacs-server key <i>WORD</i>	Configure tacacs+ shared key.
3	show tacacs-server	Display tacacs+ server address, shared key and authentication message statistics.

Correspondingly, we also can use **no** commands to cancel tacacs+ server and shared key configuration:

Steps	Commands	Description
1	no tacacs-server	Delete tacacs+ authentication server address.
2	no tacacs-server key	Delete tacacs+ shared key.

- Configure client login mode

Commands	Description
user login { local-radius / local-user / radius-local[server-no-response] / radius-user / tacacs-user / tacacs-local [server-no-response] / local-tacacs }	Configure client login mode.
enable login {local-radius / local-user / radius-local[server-no-response] / radius-user / tacacs-user / tacacs-local[server-no-response] / local-tacacs }	Configure enable login mode.

36.2.3 Monitoring and Maintenance

We can check switch tacacs+ server address, shared key and authentication message statistics by using **show** Commands. That makes it easy to monitor and maintenance. The **show** command is:

Commands	Description
show tacacs-server	Display tacacs+ server address, shared key and authentication message statistics.

36.2.4 Typical Configuration Illustration

Tacacs+ server address is 192.168.0.100, shared key is 123, and tacacs+ client name and password are individually *test* and *test*. Configuring steps are:

Raisecom#**tacacs-server 192.168.0.100**

Raisecom#**tacacs-server key 123**

Raisecom#**user login tacacs-local**

Chapter 37 GVRP Configuration Guide

This chapter introduces how to configure GVRP function, the function is used to propagation VLAN dynamically.

The chapter includes following contents:

- ❖ GVRP Overview
- ❖ GVRP Configuration
- ❖ Monitoring and Maintenance
- ❖ Typical configuration illustration

37.1 GVRP overview

GVRP (GARP VLAN Registration Protocol) is an application of GARP (Generic Attribute Registration Protocol). We will introduce related content of the GARP firstly.

37.1.1 Brief introduction of GARP

GARP provides a mechanism for assistance with the exchange, transmission and registered some information (such as VLAN, multicast information etc.) among members of distribution in the same local area network.

The GARP itself is not as an entity presented in the equipment, it follows the GARP protocol application entity, so it called GARP application. GVRP is an application of GARP. When the GARP application entities exist on a port of the equipment, the port corresponds to a GARP application entity.

1. GARP message and timer

(1) GARP message

Interactive information between GARP members completed based on message passing. There are mainly three types of messages, respectively, Join message, Leave message and LeaveAll message.

- When a GARP application entity hope that other equipment register their attribute information, it will send out Join message; when receiving Join messages of the other entity or the equipment static configure with certain attributes and require other GARP application entity to register, it will send out the Join message.
- When a GARP application entity hope that other switches cancel some attribute information of it, it will send out Leave message; when receiving Leave message of the other entity to cancel certain attributes or static cancellation of certain attributes, it will send out the Leave message.
- After each GARP application entity enable, it also enable LeaveAll timer at the same time. When the timer timeout, GARP application entity will send out LeaveAll message to the others, LeaveAll messages are used to cancel all attributes, so that the other GARP application entities

re-register all the entity attribute information.

The Leave message, LeaveAll message and Join message are used to ensure the cancellation of attribute or re-register. All attribute information which to be registered can be transmitted to all devices which enable GARP function in the same LAN through the information interaction.

(2) GARP timer

Transmission time interval of GARP message is achieved by the timer. GARP defines four timers used to control period of the GARP message transmission:

- Join timer: GARP application entity can achieve reliable message transmission by transmission out each Join message two times. GARP application entity will send the second Join message if the entity did not get the reply after transmission the first Join message. The time interval between two Join messages sending is controlled by the Join timers.
- Leave timer: when GARP application entities that wish to cancel attribute information, it will send Leave message, GARP application entities receiving the message enable the Leave timer, cancelling the attribute information if the application entity didn't receive the Join message before the timer timeout.
- LeaveAll timer: after each GARP application entity enable, it will enable LeaveAll timer at the same time. If the timer overtime, GARP application entity will send LeaveAll messages, so that other GARP application entities re-register all the entity attribute information if the timer timeout. Then enable the LeaveAll timer to begin a new round of cycle.

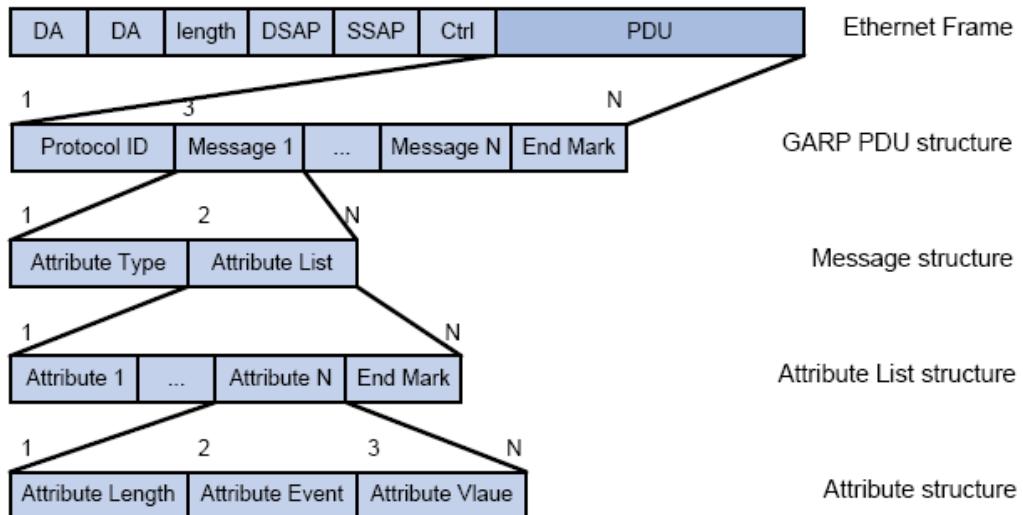
2. Operation process of GARP

Configuration information of a GARP member will quickly spread to the whole LAN through the GARP mechanism. GARP member can be terminal workstation or Network Bridge. GARP members notify other GARP member registration or cancellation of its attribute information through statement or recovery statement, and the member register or cancel attribute information of other GARP members according to statement or recovery statement of the other members. When the port receives an attribute declaration, the port will register the property. If the port receives the recovery property declarations, the port will cancel the attribute.

Protocol data message of GARP application entity use a specific multicast MAC address as the destination MAC. The device will distinguish the message according to the destination MAC address and different GARP applications (such as GVRP) will deal with them after receiving the message of GARP application entity.

3. Message format of GARP

Message format of GARP shown in figure 37-2:

**Figure 37-2 Message format of GARP**

Description of each fields shows in table 37-1.

Table 37-1 description of each field

Field	Meaning	Value
Protocol ID	Protocol ID.	Value is 1.
Message	Message, each message consists of Attribute Type and Attribute List.	-
Attribute Type	Attribute type is defined by specific application of GARP.	To GVRP, attribute type is 0x01, means attribute value is VLAN ID.
Attribute List	Attribute list consists of many attributes.	-
Attribute	Each attribute consists of Attribute Length, Attribute Event, Attribute Value. LeaveAll Attribute consists of Attribute Length and LeaveAll Event.	-
Attribute Length	Length of attribute	2~255, unit is byte.
Attribute Event	Event descripted by attrivute	0: LeaveAll Event 1: JoinEmpty Event 2: JoinIn Event 3: LeaveEmpty Event 4: LeaveIn Event 5: Empty Event
Attribute Value	Attribute value	Attribute value of GVRP is VLAN ID, but Attribute Value of LeaveAll contribute doesn't effect.

End Mark	End mark of CPU (protocol data unit) of GARP	Defined by 0x00.
-----------------	--	------------------

37.1.2 Brief introduction of GVRP

GVRP (GARP VLAN Registration Protocol) is an application of GARP. It is based on working mechanism of GARP, VLAN dynamic registration information in the switch, and transmits the information to the other switches. All the switches which support GVRP characteristics can receive VLAN registration information from other switches and dynamic update the local VLAN registration information including current member of VLAN, the port which is used to arrive the destination. And all the switches which support characteristics of the GVRP can transfer the local VLAN registration information to the other switches, so VLAN information of all devices which support GVRP characteristics in the same switching network get agreement. VLAN registration information spreaded by GVRP includes both the static registration information of local manual configuration and dynamic registration information from the other switch.

GVRP has three registered modes: normal mode (Normal), fixed mode (Fixed) and forbidden mode (Forbidden).

Normal mode (Normal): allowing dynamic registration, cancellation of VLAN, propagation of dynamic and static VLAN information;

Fixed mode (Fixed): prohibiting dynamic registration, cancellation of VLAN, propagation of static VLAN information, propagation of no dynamic VLAN information, allowing only the static VLAN pass through, that is only transmission static VLAN information to the other GVRP members;

Forbidden mode (Forbidden): forbidden dynamic registration, cancellation of VLAN, forbidden static VLAN is created in the TRUNK port; delete all VLAN without VLAN 1 on port at the same time, allowing only the default VLAN (VLAN1) pass through that is only transmission VLAN1 information to other GARP members.

37.1.3 Protocol specification

There is a detailed description of The GVRP protocol in IEEE 802.1Q documentation.

37.2 Configuration of GVRP

The section includes following contents:

- ❖ Default configuration
- ❖ Configuration guide
- ❖ Configure GVRP

37.2.1 Default configuration

Function	Default value
----------	---------------

Global GVRP function switch	Disable
Port GVRP function switch	Disable
GARPJoin timer value	20 units(10ms)
GARP Leave timer value	60 units(10ms)
GARP Leaveall timer value	1000 units(10ms)
GVRP registration mode	Normal mode

37.2.2 Configuration guide

- Port must set TRUANK mode firstly to enable port GVRP function;
- Not recommended that users enable GVRP function in the TRUANK member port;
- If three timers are restored as the default values, it is proposed recovery in accordance with the Join timer, Leave timer, and Leaveall timer sequentially.

37.2.3 Configure GVRP

37.2.3.1 Enable global GVRP function

Step	Command	Description
1	config	Enter global configuration mode.
2	gvrp enable	Enable global GVRP function.
3	show gvrp [port-list {1-maxport}] statistics	Show gvrp relative configuration and statistics. <i>1-maxport</i> is port list.

Illustration:

```
Raisecom#config
Raisecom(config)# gvrp enable
```

Reverse configuration command: **gvrp disable**

37.2.3.2 Enable port GVRP function

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <i>port_num</i>	Enter port configuration mode. <i>port_num</i> is port number.
3	switchport mode trunk	Set port as TTRUNK mode.

4	gvrp enable	Enable GVRP function of port.
5	show gvrp [port-list {1-maxport}] statistics	Show gvrp relative configuration and statistics. <i>1-maxport</i> is port list.

Illustration:

Raisecom#**config terminal**

Configuration mode, one command input per times. End with CTRL-Z.

CONFIG-I: Configured from console...

Raisecom (config) # **interface port 5**

Raisecom (config-port) # **switchport mode trunk**

Raisecom (config-port) # **gvrp enable**

Raisecom (config-port) # **show gvrp port-list 5 statistics**

37.2.3.3 Configure GVRP registration mode

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <i>port_num</i>	Enter port configuration mode. <i>port_num</i> is port number.
3	gvrp registration {normal fixed forbidden}	Configure GVRP register mode.
4	show gvrp [port-list {1-maxport}]	Show relative configuration and statistic of gvrp. <i>1-maxport</i> is port list.

Illustration:

Raisecom#**config terminal**

Raisecom (config) # **interface port 5**

Raisecom (config-port) # **gvrp registration fixed**

Raisecom (config-port) # **show gvrp port-list 5**

37.2.3.4 Clear garp statistics of port

Step	Command	Description
1	config	Enter global configuration mode.
2	clear garp [portl-ist {1-maxport}] statistics	Clear garp statistic of port. <i>1-maxport</i> is port list.

Illustration:

Raisecom#**config terminal**

```
Raisecom (config) # clear garp statistics portl-list 5
```

37.3 Monitoring and Maintenance

Check port garp statistics, port garp timer value and the gvrp configuration information by the **show** command.

Command	Description
show garp [portl-list {1-maxport}] statistics	Check garp statistics of port. <i>1-maxport</i> is port list.
show gvrp [port-list {1-maxport}] statistics	Check gvrp relative configuration.

```
Raisecom#show garp timer port-list 5
```

GARP timers unit: (10ms)

Port	GarpJoinTimer	GarpLeaveTimer	GarpLeaveAllTimer
5	25	60	1000

```
Raisecom#show gvrp port-list 21 statistics
```

GVRP Global Admin State: Enable

Port	PortStatus	RegMode	LastPduOrigin	Running
21	Enable	Normal	0000.0000.0000	YES

```
Raisecom#show garp statistics port-list 21 statistics
```

Port	GvrpRxTotal	GvrpTxTotal	GvrpFailRegs	DiscardTotal
21	0	24	0	0

37.4 Typical configuration illustration

37.4.1 Networking demand

As shown in figure 37-2, we configure static VLAN5-10 in Switch A and Switch C. we configure static VLAN15-20 in Switch D and configure static VLAN25-30 in Switch E. All port which connected with other switch is set to be TRUNK mode, and then enable GVRP function of all port which connected to other switches.

After enables GVRP, VLAN learned by ports of switch shows as below:

Switch A-Port 1: VLAN 1, VALN5-10, VLAN 25-30;

Switch A-Port 2: VLAN 1, VALN5-10;

Switch A-Port 3: VLAN 1, VALN5-10, VLAN 15-20;
 Switch B-Port 1: VLAN 1, VALN5-10, VLAN 15-20;
 Switch B-Port 2: VLAN 1, VALN25-30;
 Switch C-Port 1: VLAN 1, VALN5-10, VLAN 15-20, VLAN 25-30;
 Switch D-Port 1: VLAN 1, VALN5-10, VLAN 15-20, VLAN 25-30;
 Switch E-Port 1: VLAN 1, VALN5-10, VLAN 15-20, VLAN 25-30.

37.4.2 Figure of networking

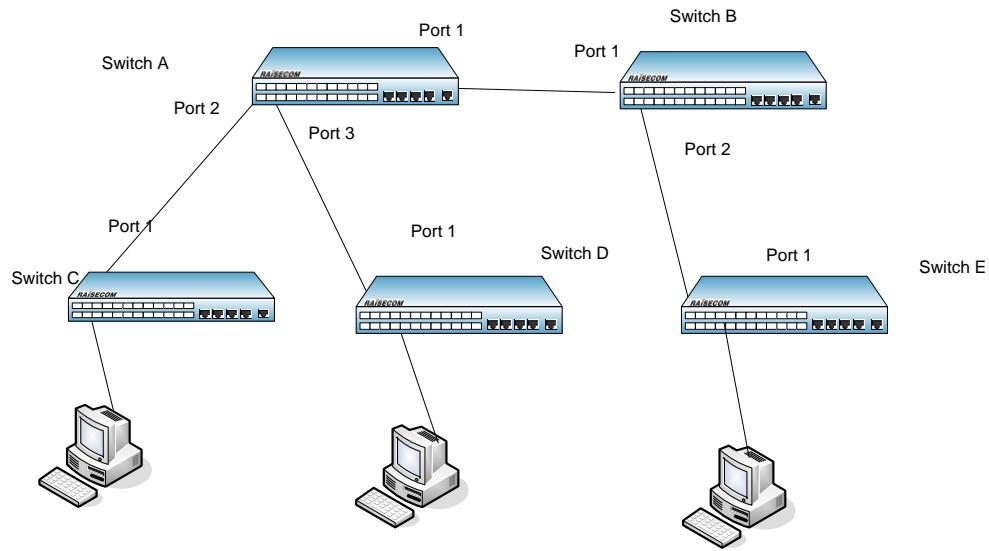


Figure 37-3

37.4.3 Configuration steps

Switch A:

```

SwitchA#config terminal
SwitchA (config)#create vlan 5-10 active
SwitchA (config)#gvrp enable
SwitchA (config)#interface port 1
SwitchA (config-port)#switchport mode trunk
SwitchA (config-port)#gvrp enable
SwitchA (config-port)#exit
SwitchA (config)#interface port 2
SwitchA (config-port)#switchport mode trunk
SwitchA (config-port)#garp timer join 3000
SwitchA (config-port)#gvrp enable
  
```

```
SwitchA (config-port)#exit  
SwitchA (config)#interface port 3  
SwitchA (config-port)#switchport mode trunk  
SwitchA (config-port)#gvrp enable
```

Switch B:

```
SwitchB#config terminal  
SwitchB (config)#gvrp enable  
SwitchB (config)#interface port 1  
SwitchB (config-port)#switchport mode trunk  
SwitchB (config-port)#gvrp enable  
SwitchB (config-port)#exit  
SwitchB (config)#interface port 2  
SwitchB (config-port)#switchport mode trunk  
SwitchB (config-port)#gvrp enable
```

Switch C:

```
SwitchC#config terminal  
SwitchC (config)#create vlan 5-10 active  
SwitchC (config)#gvrp enable  
SwitchC (config)#interface port 1  
SwitchC (config-port)#switchport mode trunk  
SwitchC (config-port)#gvrp enable
```

Switch D:

```
SwitchD#config terminal  
SwitchD (config)#create vlan 15-20 active  
SwitchD (config)#gvrp enable  
SwitchD (config)#interface port 1  
SwitchD (config-port)#switchport mode trunk  
SwitchD (config-port)#gvrp enable
```

Switch E:

```
SwitchE#config terminal
```

```
SwitchE (config)#create vlan 25-30 active
SwitchE (config)#gvrp enable
SwitchE (config)#interface port 1
SwitchE (config-port)#switchport mode trunk
SwitchE (config-port)#gvrp enable
```

Chapter 38 PPPoE Configuration Guide

38.1 Function principle of PPPoE+

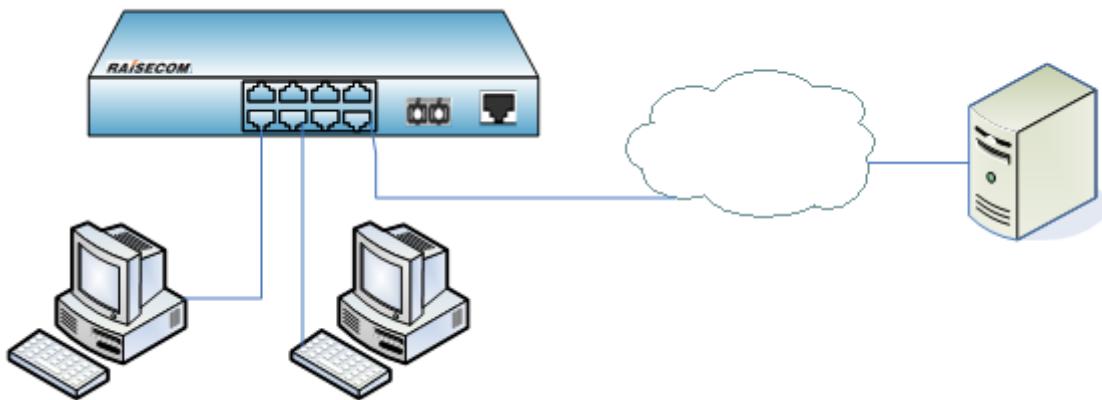


Figure 38-1 network topological graph

As shown in Figure 38-1, the PC connects with network through the PPPoE certification. If the certification information just contains the username and password information, the server will be very difficult to distinguish for the user, because there may be account sharing or account theft case in the user side. Therefore, if the server needs to locate the user, authentication message needs more information. PPPoE + protocol are used for PPPoE authentication message processing, so that the server can obtain sufficient information to identify users.

When authentication message of PPPoE user side pass through the switch, if the switch have PPPoE + function and the corresponding port is already enable the function, then switch will deal with the authentication message of PPPoE, treatment method depends on the configuration of PPPoE + function by users. The server can identify and locate the user according to processing of PPPoE + message by the switch.

38.2 Function default configuration of PPPoE+

PPPoE + function are based on the port, no global switch. By default, the PPPoE + function of switch ports disabled.

38.3 Function configuration of PPPoE+

38.3.1 Enable or disable PPPoE+ function

This configuration is used to enable or disable the port PPPoE + function.

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <i>port_num</i>	Enter port configuration mode. <i>port_num</i> is port number. interface range <i>portlist</i> can be used to enter batch configuration mode and configure multiports. <i>portlist</i> is port list.
3	pppoeagent {enable / disable}	Enable/disable PPPoE+ function of port.
4	show pppoeagent	Show state of PPPoE.

38.3.2 Configure function of trusted port

The configuration is used to configuring/canceling a port as a trust port, it generally configures the port connected to server as trust port, and PPPoE client message will be forwarded to trust port.

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <i>port_num</i>	Enter port configuration mode. <i>port_num</i> is port number. interface range <i>portlist</i> can be used to enter batch configuration mode and configure multiports. <i>portlist</i> is port list.
3	[no] pppoeagent trust	Configure/cancel port as trusted port.
4	show pppoeagent	Show PPPoE+ state.

38.3.3 Configure add/modify message information of PPPoE+

PPPoE + is used to processing a specific TAG in PPPoE messages. The TAG contains two fields of Circuit ID and Remote ID.

Configure Circuit ID.

Circuit ID has two kinds of filling pattern: switch mode and onu mode, when the port is used as onu mode, otherwise switch mode. In switch mode, Circuit ID has two kinds of filling format: 1, fill format is not configured for a custom Circuit ID, filled in for: vlan number\port number\ attached string. 2, configured custom Circuit ID, filling for the configured Circuit ID string. In onu mode, the Fill Format: 00 / 0 / 0: 0 / 0 / 0 / 0 / 0 / MAC 0 / 0 / Port: eth / 4096. CVLAN LN, where MAC is the MAC address of the device, Port is the port number, CVLAN message carrying the VLAN or native VLAN port. Filling content are ASCII code format.

The user can configure global filling mode.

Step	Command	Description
1	config	Enter global configuration mode.
2	pppoeagent circuit-id mode {switch / onu}	Configure filling mode of Circuit ID, default is switch mode.
3	show pppoeagent	Show PPPoE+state.

In the switch mode, default format of Circuit ID is: VLAN number\port number\attached string.
Users can use the Circuit ID configuration for a custom string.

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <i>port_num</i>	Enter port configuration mode. <i>port_num</i> is port number.
3	pppoeagent circuit-id <i>INFO</i>	Configure Circuit ID as a character string. <i>INFO</i> is character string which length is less than 63. In port mode, we can use no pppoeagent circuit-id command to restore Circuit ID to default value.
4	show pppoeagent	Show PPPoE+ state.

Configure attached string of Circuit ID.

Circuit ID contains a attached string in the default format, attached string is hostname of switch by default, and the user can configure it to a customized character string.

Step	Command	Description
1	config	Enter global configuration mode.
2	pppoeagent circuit-id attach-string <i>STRING</i>	Configure attatched string of Circuit ID as a customized string. <i>STRING</i> is a string which length is less than 55. In global mode, we can use no pppoeagent circuit-id attach-string command to return Circuit ID to default value.
3	show pppoeagent	Show PPPoE+ state.

Configure Remote ID

Filled Remote ID is an MAC address, and we can choose MAC address.of the switch or MAC address of PPPoE client.

Step	Command	Description
1	config	Enter global configuration mode.

2	interface port <i>port_num</i>	Enter port configuration mode. <i>port_num</i> is port number.
		interface range <i>portList</i> is used to enter the batch configuration mode and configure multiple port; <i>portlist</i> is port list.
3	pppoeagent remote-id {switch-mac client-mac}	Configure Remote ID of port PPPoE + as switch or the MAC address of the client.
4	show pppoeagent	Show state of PPPoE+.

Configure format mode of Remote ID

Remote ID can use binary or ASCII code format to fill, and user can choose the format mode.

Step	Command	Description
p		
1	config	Enter global configuration mode.
2	interface port <i>port_num</i>	Enter port configuration mode. <i>port_num</i> is port number.
		interface range <i>portList</i> can be used to enter the batch configuration mode and configure multiple port. <i>portlist</i> is port list.
3	pppoeagent remote-id format {binary/ascii}	Configure Remote ID format of port PPPoE + for binary or ASCII code format.
4	show pppoeagent	Show state of PPPoE+.

Configure TAG overlay function:

For some reasons, we need to cover original TAG of message (for example, TAG may be forged by client). After enable the TAG overlay function, if the PPPoE message has been carrying the TAG, it will be covered, if not then add.

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <i>port_num</i>	Enter port configuration mode. <i>port_num</i> is port number;
		interface range <i>portList</i> is used to enter the batch configuration mode and configure multiple port. <i>portlist</i> is port list.
3	pppoeagent vendor-specific-tag overwrite {enable / disable}	Enable or disable TAG overlay function.
4	show pppoeagent	Show state of PPPoE+.

38.3.4 Clear statistics

If PPPoE + function enable, it will statistics received/sent PADI and PADR packets, clear statistics functions can clear statistical information.

Command	Description
clear pppoeagent statistic [port-list <i>portlist</i>]	Clear statistics of PPPoE+. <i>portlist</i> is port list.

38.4 Monitoring and maintenance

Command	Description
show pppoeagent [port-list <i>portlist</i>]	Show configuration of PPPoE+. <i>portlist</i> is port list.
show pppoeagent statistic [port-list <i>portlist</i>]	Show statistics of PPPoE+. <i>portlist</i> is port list.

38.5 Typical configuration illustration

Illustration 1: enable PPPoE + function of port 1-5.

Raisecom#config

Raisecom(config)#interface range 1-5

Raisecom(config-range)#pppoeagent enable

Raisecom(config-range)#show pppoeagent

Attach-string: %default%

Circuit ID padding mode: switch

Port	Enable	Overwrite	Remote-ID	Format-rules	Circuit-ID
------	--------	-----------	-----------	--------------	------------

1	enable	disable	switch-mac	binary	%default%
2	enable	disable	switch-mac	binary	%default%
3	enable	disable	switch-mac	binary	%default%
4	enable	disable	switch-mac	binary	%default%
5	enable	disable	switch-mac	binary	%default%
6	disable	disable	switch-mac	binary	%default%
7	disable	disable	switch-mac	binary	%default%
8	disable	disable	switch-mac	binary	%default%
9	disable	disable	switch-mac	binary	%default%

**In switch mode, Circuit-ID's default string is: Port\Vlan\Attach-string.

***In onu mode, Circuit-ID's default string is: 0 0/0/0:0.0 0/0/0/0/0/MAC 0/0/Port:eth/4096.CVLAN LN.*

***Attach-string's default string is the hostname.*

Illustration 2: configure Circuit ID of port 1 as “hello”, Remote ID of port 2 is client MAC address, format of Remote ID of port 3 is ASCII format, enable overlay enable of port 4.

Raisecom#**config**

Raisecom(config)#**interface port 1**

Raisecom(config-port)#**pppoeagent circuit-id hello**

Raisecom(config-port)#**interface port 2**

Raisecom(config-port)#**pppoeagent remote-id client-mac**

Raisecom(config-port)#**interface port 3**

Raisecom(config-port)#**pppoeagent remote-id format ascii**

Raisecom(config-port)#**interface port 4**

Raisecom(config-port)#**pppoeagent vendor-specific-tag overwrite enable**

Raisecom(config-port)#**show pppoeagent**

Attach-string: %default%

Port	Enable	Overwrite	Remote-ID	Format-rules	Circuit-ID
1	disable	disable	switch-mac	binary	hello
2	disable	disable	client-mac	binary	%default%
3	disable	disable	switch-mac	ASCII	%default%
4	disable	enable	switch-mac	binary	%default%
5	disable	disable	switch-mac	binary	%default%
6	disable	disable	switch-mac	binary	%default%
7	disable	disable	switch-mac	binary	%default%
8	disable	disable	switch-mac	binary	%default%
9	disable	disable	switch-mac	binary	%default%

***In switch mode, Circuit-ID's default string is: Port\Vlan\Attach-string.*

***In onu mode, Circuit-ID's default string is: 0 0/0/0:0.0 0/0/0/0/0/MAC 0/0/Port:eth/4096.CVLAN LN.*

***Attach-string's default string is the hostname.*

Chapter 39 CFM Configuration

This chapter describes how to configure CFM in switch and the contents are shown as below:

- ❖ CFM introduction
- ❖ CFM default configuration list
- ❖ CFM configuration guide and limitation
- ❖ CFM configuration list and specifications
- ❖ CFM monitoring and maintenance
- ❖ CFM basic configuration illustration

39.1 CFM Introduction

Since it grows rapidly, Ethernet technology has been used widely in MAN (metropolitan area network) and WAN (wide area network). Because of the complex network structure of MAN and WAN and a huge number of various users in WAN and MAN, many operators co-operate their network together to provide end-to-end service. Thus, there will be more strict requirements for the Ethernet's management, maintenance and its reliability. Traditional Ethernet don't have telecommunication administrative capacity, so they can't detect bi-level network fault. Every research groups and standards organization are working on the technology development and standard modification actively in order to realize the same level of service compared with traditional telecommunication transmission network.

CFM protocol (802.1ag) established by IEEE and ITU-T provide end-to-end service OAM ability. CFM is able to detect the end-to-end linkage fault quickly. It also can provide the on-demand fault confirmation and fault isolation function. All those can provide a more complete OAM function for the Ethernet network.

CFM (Connectivity Fault Management) protocol is a bi-layer Ethernet OAM protocol. CFM works as the active fault diagnoses for point-to-point or multi-points to multi-points EVC (Ethernet Virtual Connection). It is OAM protocol based on end-to-end service level. We can use CFM protocol to cut down the network maintenance cost effectively. It is suitable for end to end Ethernet network. It is used in Ethernet access network, convergence network and core network and it can be used in all Ethernet devices.

39.1.1 CFM Modules

1. MD

MD (Maintenance Domain) is a network which is used to manage CFM. It states range of network used to checking CFM. MD has level attribute which has 8 levels in total (0-7). The bigger level number, the higher MD level and the bigger the MD range. In one VLAN, different MDs can be nearby or nesting but not cross.

2. MA

One MA is corresponding one service instance and S-VLAN. One MA can configure many MEPs. MEPs of the same MA have same VLAN TAG in their sending messages. Also, a MEP can receive sending CFM messages from other MEPs in the same MA.

3. MIP

MIP is a managing activity entity which is formed by two MHF (MIP Half Function). MIP can not send CFM messages actively, but can process and reply CFM messages.

4. MEP

MEP is configured at MD edge and a managing activity entity related to service instance. One MEP is related to one service instance. MEP can send and process CFM messages, MD and MA (MEP belonged) confirm MEP sending messages level and VLAN. MEPs stop and process the receiving messages which are same or lower level than their MEP level; MEPs relay directly those levels higher than them. MEP and MIP are called MP.

39.1.2 CFM Basic Function

CFM function is based on right configurations of MD, MA, MEP and MIP. Its function is realized among configured MP. CFM mainly has three functions:

Fault detection function (Continuity Check, CC)

Fault confirmation function (Loopback, LB)

Fault isolation function (Linktrace, LT)

39.1.2.1 Fault Detection

Fault detection function is that using CC (Continuity Check) protocol to check connectivity of an Ethernet Virtual Connection (EVC) and also confirm connections between MPs. The Function is achieved by MEP periodically sending CCM (Continuity Check Message) multi-cast message. Other MEPs from same MA receive that message thus to check the remote MEP status. If device fault or link configured error, then MEP can not send CCM messages to remote MEP and can not receive remote CCM message as well. If MEP does not receive remote CCM message in 3.5 times of CCM interval period, then it will state the link fault occurring and send fault alarm information to the administrator according to the alarm and priority configuration. When multiple MEPs of multiple MAs from the same MD send CCM messages that can be multi-points to multi-points link check.

39.1.2.2 Fault Confirm

Faults confirm function is used to check the connectivity between local devices and remote devices. The function can send LBM (Loop back Message) through MEP to the MPs which needs fault confirm. When that MP receives LBM message, it sends a LBR reply message to source MEP, shows route is connected. If source MEP does not receive LBR message, then the link has fault. Faults confirm function is similar to layer 2 ping functions. Both sending LBM and receiving LTR are uni-cast message. LBM and LTR receiving are used to confirm the link status between to MPs.

39.1.2.3 Fault Isolation

Fault isolation function is used to confirm the route between source MEP and destination MP. The function is achieved by source MEP sending LTM (Linktrace Message) to MP which can confirm route; bridge device from each configured MP on that route sends LTR reply message to source MEP. Information can be reformed by recording effective LTR and LTM. Lastly the route between MP is confirmed. LTM is multi-cast message and LTR is uni-cast message.

By the three functions above, CFM protocol can achieve end to end OAM technology, reduces service providers' operation and maintenance cost. So in a certain way, it increases the service providers' competitive advantage.

39.2 CFM Default Configuration List

No.	Attribute	Default Value
1	CFM protocol global enable and disable	CFM protocol disable
2	Port CFM protocol status	All ports CFM enable
3	CCM messages sending status	Not sending CCM messages
4	Time intervals of sending CCM messages	10 seconds
5	The time which CC database save error CCM	100 minutes
6	Linktrace Database switch	Disable
7	Linktrace Database saving data time	100 minutes
8	Configure Linktrace Database saved data Enter number	When Linktrace Database is enable, data entries can be saved as 100; as it is disable, data entries can be saved as 0.
9	Configure network bug alarm	When it is set as macRemErrXcon is set, it supports four bug alarms: Macstatus, RemoteCCM, ErrorCCM and XconCCM.

39.3 CFM Configuration Constraint and Limitation

- MEP is based on MD and MA. MD has 8 levels. MA service instance can corresponding to 4094 VLANs. Each switch can configure 128 MD, 128 MA and 128 MEP at most in order to ensure performance of switch. The range of MEPID is 1-8191. Each port can configure 1 MIP at most.
- Configure sending interval of CCM messages, protocol can be configured as 3.33 ms, 10ms, 100ms, 1s, 10s, 1m and 10m. For stable performance of the switch, our support range is among 1s, 10s, 1m and 10m. Configuration of millisecond don't support for the moment. In addition, once each MEP receives CCM messages, it will record the efficient CCM in MEP CCM Database. Each MEP maintaining CCM Database can save 100*128 bars.
- To state maintenance domain (MD), the length of domain name's character string is 1-16 byte, maintaining level are level 0-7.

- When we configure customer service instance MA, the length of service instance ID's character string is 1-16 bytes. The range of Vlan list is 1-4094.
- The range of saved time of error CCM message in MEP CCM Database is 1-65535.
- Configure saved data time (minute) of Linktrace Database is in the range of 1-65535, saved data entries could be in the range of 1-4095.

39.4 CFM Configuration List and Specification

A. Configure CFM domain

- a) Configure CFM maintain MD
- b) Configure CFM service illustration MA
- c) Configure MIP
- d) Configure MEP

B. Fault Check

- a) Configure CC protocol switch
- b) Configure sending interval of CCM messages
- c) Configure saving time of error CCM messages

C. Launch Loopback protocol

D. Route trace

- a) Launch Linktrace protocol
- b) Configure Linktrace data switch status
- c) Configure saving time of Linktrace data
- d) Configure Linktrace Database saved data entries' number

E. Fault indication

F. Protocol enable/disable

39.4.1 Configure CFM Maintenance Domain MD

Before configure MD name, MD name must be the only name in the whole CFM managing network range. Different name of MD can be configured in the same level, but two MDs with same name could not be related to different levels.

Delete MD: **no ethernet cfm domain *domain-name* level *level-id***

Steps	Command	Description
1	config	Enter global configuration mode.
2	ethernet cfm domain <i>domain-name</i> level <i>level-id</i>	Configure CFM maintain domain, state MD name and level. <i>domain-name</i> : domain name character

		string with 1-16 bytes.
		<i>level-id</i> : level of maintain domain is 0-7.
3	exit	Return to Privileged EXEC mode.
4	show ethernet cfm domain	Display indicated maintain domain configure information.

Illustration: Configure MD, name is md3-1, level is 3

Raisecom#config

```
raiecom(config)#ethernet cfm domain md3-1 level 3
```

```
raiecom(config-ether-cfm)#exit
```

```
raiecom(config)#exit
```

39.4.2 Configure Service Instance MA

When configure service illustration, we need to configure MD first and make sure the name of service illustration is the only one inside that MD; but in two different MD, we can configure the same name service illustration; in one MD, a VLAN can only be related to one service illustration. If configured MA name is same as the existed MA name, but the related VLAN is different, then that MA should be given a new related VLAN.

Delete service illustration: **no service csi-id vlan vlan-id**. Before delete service illustration, we need to delete its all MEP first.

Steps	Commands	Description
1	config	Enter global configuration mode.
2	ethernet cfm domain [md-name <i>domain-name</i>] level <i>level</i>	Configure CFM MD, states MD name and MD level. <i>domain-name</i> : domain name character string length 1-16 bytes; <i>level</i> : MD level 0-7.
3	service vlan-list <i>vlan-id</i>	Configure service instance related VLAN. <i>vlan-id</i> : service instance ID string, length is 1-16 byte.
4	exit	Return to global configuration mode.
5	exit	Return to Privileged EXEC mode.
6	show ethernet cfm domain	Show specific maintenance field configuration information

Illustration: In MD named md3-1, configure service illustration as ma3-1-4 and its related VLAN as 4.

Raisecom#config

```
Raisecom (config) #ethernet cfm domain md-name md3-1 level 3
Raisecom (config) #service ma3-1-4 level 3
```

```
Raisecom (config-service) #service vlan-list 4
Raisecom (config-service) #exit
```

39.4.3 Configure MIP

Note: the ISCOM2128EA-MA doesn't support MIP.

Before configure MIP, we must make sure that configure the switch with the same level MD, and there should not be any same or higher level MEP on the port. The same port can only be configured one MIP. If we configure two MIP, the new one will replace the old one. Before delete MIP, we should make sure there is no lower level MEP in the port.

Delete MIP: **no ethernet cfm mip level *level-id***

Steps	Commands	Description
1	config	Enter global configuration mode.
2	interface port <i>portid</i>	Enter <i>portid</i> port mode. <i>port-num</i> : port number.
3	ethernet cfm mip level <i>level-id</i>	In indicated MD, configure MIP, same level as MD. <i>level-id</i> : MD level: 0-7.
4	exit	Return to global configuration mode.
5	exit	Return to privileged EXEC mode.
6	show ethernet cfm mp local	Display local MP configuration information includes MEP and MIP.

Illustration: in port 5, configure MIP as level 5(we have configured MD as level 5)

```
Raisecom#config
Raisecom(config)#interface port 5
Raisecom(config-port)#ethernet cfm mip level 5
```

39.4.4 Configure MEP

Before configuring MEP, we configure a MD which MEP located in, and corresponding service illustration in MD and a high level MIP. If level of MEP is 7, we don't need to configure high level of MIP. If there is an MIP configured in the port, then we can configure any same or higher level MEP on that port. So far, all supported configured MEP directions are UP, so if commands are not indicated, the default is UP.

Delete indicated MEP: **no ethernet cfm mep level *level-id* [up] mpid *mep-id* vlan {all|*vlanlist*}**

Steps	Commands	Description
1	config	Enter global configuration mode.
2	service <i>CSIID</i> level <i>level</i>	Enter service instance mode. <i>CSIID</i> : service instance name, length is 1-13 byte.

		<i>level</i> : maintenance domain level, range is 0-7.
		Configure MEP in service instance.
3	service mep [up/down] mpid <i>mepid {port port-id}</i>	<i>up</i> : up direction MEP. <i>mpid</i> : MEPID.
		<i>port-id</i> : port number, range from 1 to max port number.
4	exit	Return to global mode.
5	exit	Return to Privileged EXEC mode.
6	show ethernet cfm domain <i>[domain-name]</i>	Display specified MD configuration information

Illustration:

- Steps of configuring the MEP whose level is not 7: First configure high level (level is 5) MD; we configure the corresponding level MIP under that MD. We configure a level 3 MD and corresponding service illustration; finally, we configure its corresponding MEP.

Raisecom#**config**

Configure high level MD: Raisecom (config) #**ethernet cfm domain md5 level 5**

Raisecom (config-ether-cfm) #**exit**

Configure indicated level MD: Raisecom (config) #**ethernet cfm domain md3 level 3**

Configure related service illustration: Raisecom (config-ether-cfm) #**service vlan-list 4**

Raisecom (config-ether-cfm) #**exit**

Enter port mode: Raisecom (config) #**interface port 1**

Under high level, configure MIP: Raisecom (config-port) #**ethernet cfm mip level 5**

Configure MEP: Raisecom (config-port) #**service mep up mpid 1 port 1**

Raisecom (config-port) #**exit**

Raisecom (config) #**exit**

- Configure MEP which is level7: Firstly, configure a level 7 MD and its related service instance; then configure MEP.

Raisecom#**config**

Configure level 7 MD:

Raisecom (config) #**ethernet cfm domain md-name md7 level 7**

Configure related service instance:

Raisecom (config) #**service ma7-1-4 level 7**

Raisecom (config-service) # **service mep up mpid 1**

Raisecom (config-service) #**exit**

Enter service instance mode:

Raisecom (config) # **service ma7-1-4 level 7**

```
Configure MEP: Raisecom (config-port) #service mep up mpid 1 port 1
Raisecom (config-port) #exit
Raisecom (config) #exit
```

39.4.5 Configure CC Protocol Switch

Launch CC protocol on the indicate service instance, thus all MEP from the service instances can send CCM messages. When CC protocol disables, MEP stops sending CCM messages. As configure that command, we should make sure that the switch is configured same level MD and each VLAN from VLAN list is found a related MA from the same level MD. In default, prohibiting send CCM message.

Steps	Commands	Description
1	config	Enter global configuration mode.
		Enter service instance mode.
2	service <i>CSIID</i> level <i>level</i>	<i>CSIID</i> : service instance name, length is 1-13 byte; <i>level</i> : maintenance domain level, range is 0-7.
		Enable/disable MEP to send CCM.
3	service cc {enable/disable} mep {{1-8191} all}	<i>enable</i> : enable <i>disable</i> : disable {1-8191}: MEP ID list, range is 1-8191; all : all configured MEP;
4	exit	Return to global mode.
5	exit	Return to Privileged EXEC mode.
6	show ethernet cfm domain [domain-name]	Display specified maintenance domain configuration information

Illustration: Configure the named as md3-1, level-3 MD; inside the MD configure the named ma3-1-4 MA and its related VLAN 4, enable cc protocol.

```
Raisecom#config
Raisecom (config) #ethernet cfm domain md-name md3-1 level 3
Raisecom (config-ether-cfm) #service ma3-1-4 level 3
Raisecom (config-service) #service mep up mpid ma3-1-4 port 1
Raisecom (config-ether-cfm) #exit
Raisecom (config) #service cc enable mep ma3-1-4
Raisecom (config) #exit
```

39.4.6 Configure Sending Interval of CCM Message

Before configure this command, we should make sure the switch is configured same MD level and each VLAN in the VLAN list has a related MA within the same MD level. In default situation, MEP

CCM messages sending interval is 10 seconds.

In recover indicated service illustration, we configure the CCM messages sending interval as default value: **no service cc interval**

Steps	Commands	Description
1	config	Enter global configuration mode. Enter instance service mode.
2	service <i>CSIID</i> level <i>level</i>	<i>CSIID</i> : service instance name, length is 1-13 byte; <i>level</i> : maintenance domain level, range is 0-7. Set the CCM message transmission time interval, can be in control of the situation, a specified level for all service instances, a specified service instance or a specified level designated service on an instance of
3	service cc interval {1/10/60/600}	CCM packet transmission time interval. Configuration service instance CCM transmission interval. Unit: Second.
4	exit	Return to global mode.
5	exit	Return to Privileged EXEC mode.
6	show ethernet cfm domain [level <0-7>]	Display related information of local configuration MD.

Illustration: Set sending interval as 60 seconds, configure corresponding MD and service instance.

Raisecom#**config**

Raisecom (config) #**ethernet cfm domain md3-1 level 3**

Raisecom (config) #**service ma3-1-4 vlan 4**

Raisecom (config-service) #**service cc interval 60**

Raisecom (config- service) #**exit**

Raisecom (config) #**exit**

39.4.7 Configure Archive Time of Error CCM Message in MEP CCM Database

Each error CCM records created time of error data and we use the commands won't change the created time of error information. Unless error data archive time is reset, the error list archive time does not change. Only if it is reset, then the new error list will use the new archive time. Before configure the CCM messages archive time, we should configure the related MEP. In default situation, CC database can archives CCM error for 100 minutes.

Recover archive time of error data in MEP CCM Database: **no ethernet cfm mep archive-hold-time**

Steps	Commands	Description
1	config	Enter global configuration mode.
2	ethernet cfm error archive-hold-time minutes	Configure saving time of error CCM messages. <i>minutes</i> : archive time (minutes), range is 1-65535.
3	exit	Return to privileged EXEC mode.
4	show ethernet cfm	Display related information of cfm.

Illustration: set archive time of error CCM messages as 50, firstly configure related MEP.
RaiseCom#**config**

```
RaiseCom (config) #ethernet cfm error archive-hold-time 50
RaiseCom (config) #exit
```

39.4.8 Launch Loopback Protocol

Before uses the commands, the switch must be configured same level, same VLAN MEP and CFM master switch enable, otherwise it fails. When there is only one related MEP, we don't need to add the key word *source mpid* in commands; if switch has more than one same level same VLAN MEPs, we must indicate the MEPIP of the source MEP – as add the key word *source mpid* in the commands.

Steps	Commands	Description
1	config	Enter global configuration mode.
2	service CSIID level level	Enter service instance mode. <i>CSIID</i> : service instance name, length is 1-13 byte. <i>level</i> : Maintenance domain level.
3	ping {HHHH.HHHH.HHHH mep rme pid } [count count] [size size] [source mep id]	Launch Loopback protocol, achieve fault confirm function. <i>HHHH.HHHH.HHHH</i> : MAC address of remote MP, format is HHHH.HHHH.HHH. <i>rme pid</i> : ID number of remote MEP (1-8191). <i>count</i> : number of sending LBM, range is 1-1024. <i>vlan id</i> : VLAN ID1-4094. <i>size</i> : data TLV length, range is 1-1484. <i>mpid</i> : source MEPID, range is 1-8191.
4	exit	Return global configuration mode.
5	exit	Return to privileged user mode.

Illustration: ping of service instance:

```
RaiseCom#config
```

```
Raisecom (config) #ethernet cfm enable
Raisecom (config) #ethernet cfm domain md-name md3-1 level 3
Raisecom (config) #service ma3-1-4 level 3
Raisecom (config-service) #ping 000E.5E03.5318 size 512
```

Sending 5 ethernet cfm loopback messages to 000E.5E03.5318, timeout is 2.5 seconds:

!!!!

Success rate is 100 percent (5/5).

Ping statistics from 000E.5E03.5318:

Received loopback replies: < 5/0/0 > (Total/Out of order/Error)

Ping successfully.

```
Raisecom (config-service) #exit
```

Ping based on port:

```
Raisecom#config
```

```
Raisecom (config) #interface port 1
```

```
Raisecom (config-port) #ethernet cfm ping 000E.5E03.5318 size 512
```

Sending 5 ethernet cfm loopback messages to 000E.5E03.5318, timeout is 2.5 seconds:

!!!!

Success rate is 100 percent (5/5).

Ping statistics from 000E.5E03.5318:

Received loopback replies: < 5/0/0 > (Total/Out of order/Error)

Ping successfully.

```
Raisecom (config-port) #exit
```

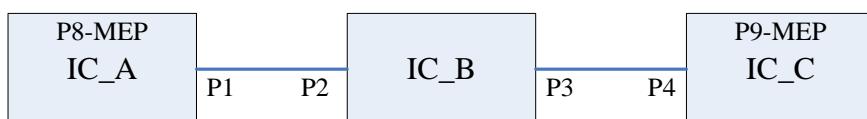


Figure 39-1

39.4.9 Launch Linktrace Protocol

Before uses the commands, the switch must be configured same level, same vlan MEP and CFM master switch enable, otherwise it fails. When there is only one related MEP, we don't need to add the key word *source mpid* in commands; if switch has more than one same level same vlan MEPs, we must indicate the MEPIP of the source MEP – as add the key word *source mpid* in the commands.

Steps	Commands	Description
1	config	Enter global configuration mode.
2	service CSID level level	Enter service instance mode.

		<i>CSID</i> : service instance name, length is 1-13 byte; <i>level</i> : Maintenance domain level, range is 0-7.
3	traceroute { <i>HHHH.HHHH.HHHH</i> <i>mep rmepid</i> } [ttl <i>ttl</i>] [<i>source mepid</i>]	Executing layer-2 TRACEROUTE function, used to fault isolation. <i>HHHH.HHHH.HHHH</i> : MAC address of remote MP. <i>rmepid</i> : remote MEPID, range is 1-8191. <i>ttl</i> : start TTL, range is 1-255. <i>mpid</i> : source MEPID, range is 1-8191.
4	exit	Return global configuration mode.
5	exit	Return to privileged user mode.

Illustration: Topology structure and configurations are same as last section; launch Traceroute Commands in two MEPs which have same MD and MA.

Raisecom#config

```
Raisecom(config)#ethernet cfm enable
Raisecom(config)#ethernet cfm domain md-name md3-1 level 3
Raisecom (config)#service ma3-1-4 level 3
Raisecom (config-service)#traceroute 000E.5E03.5318 ttl 128
```

Shown result:

```
TTL: <128>
Tracing the route to 000E.5E03.5318 on domain <md3-1>, level <3>, VLAN <4>.
Traceroute send via port <port-id>.
```

Hops	HostMAC	Ingress/EgressPort	IsForwarded	RelayAction	NextHop
<1>	<AAAA>	<8/1>	<yes>	<RlyFDB>	<AAAA>
<2>	<AAAA>	<2/3>	<yes>	<RlyFDB>	<BBBB>
!<3>	<BBBB>	<-/9>	<no>	<RlyHit>	<CCCC>

Hops	HostMAC	Ingress/EgressPort	IsForwarded	RelayAction	NextHop
<1>	<AAAA>	<8/1>	<yes>	<RlyFDB>	<AAAA>
<2>	<AAAA>	<2/3>	<yes>	<RlyFDB>	<BBBB>
!<3>	<BBBB>	<-/9>	<no>	<RlyHit>	<CCCC>

39.4.10 Configure Linktrace Database Switch Status

When switch of LinkTrace database is enable status, LinkTrace data protocol link trace information is saved in LinkTrace database and can use command: **show ethernet cfm traceroute-cache** to view them; when LinkTrace database is disable status, then we can not use that command: **show ethernet cfm traceroute-cache** to check the route trace information. The default configuration is disable status.

Steps	Commands	Description
1	config	Enter global configuration mode.
2	ethernet cfm traceroute	Configure database switch status.

	cache {enable / disable}	<i>traceroute</i> : trace router discovery of LTM messages;
3	exit	Return to privileged user mode.
4	show ethernet cfm traceroute-cache	Checks trace route information.

Illustration: Enable database and check the data information

Raisecom#**config**

Raisecom (config) #**ethernet cfm traceroute cache enable**

Raisecom (config) #**exit**

Raisecom#**show ethernet cfm traceroute-cache**

39.4.11 Configure Linktrace Database Archive Time

Only if LinkTrace database enable, we can configure archive time of the data. Default archive time is 100 minutes. Default data archive time of recovers database, we use command: **no ethernet cfm traceroute cache hold-time**

Steps	Commands	Description
1	config	Enter global configuration mode.
2	ethernet cfm traceroute cache enable	Enable Linktrace database
3	ethernet cfm traceroute cache hold-time minutes	Configure Linktrace database data archive time <i>minutes</i> : database archive time, unit is minute, range in 1-65535
4	exit	Return to privileged user mode.
5	show ethernet cfm traceroute-cache	Check data information

Illustration: Enable database and set configure archive time 1000.

Raisecom#**config**

Raisecom (config) #**ethernet cfm traceroute cache enable**

Raisecom (config) #**ethernet cfm traceroute cache hold-time 1000**

Raisecom (config) #**exit**

Raisecom (config) #**show ethernet cfm traceroute-cache**

39.4.12 Configure Linktrace Database to Store Data Entries

Only if LinkTrace database enable, we can configure the size of data entries. When LinkTrace database is enable, default entries number is 100; when LinkTrace database is disable, default data entries number is 0. To recover Linktrace database entries number default value, we use command: **no ethernet cfm traceroute cache size**

Steps	Commands	Description
1	config	Enter global configuration mode.
2	ethernet cfm traceroute cache enable	Enable LinkTrace database
3	ethernet cfm traceroute cache size entries	Configure the number of data entries. <i>entries</i> : Database data entry number, range is 1-512.
4	exit	Enter global configuration mode.
5	show ethernet cfm traceroute-cache	Check data information

Illustration: Enable database; configure data entries number as 150.

Raisecom#**config**

Raisecom (config) #**ethernet cfm traceroute cache enable**

Raisecom (config) #**ethernet cfm traceroute cache size 150**

Raisecom (config) #**exit**

39.4.13 Fault Indication

When we configure the five network trouble alarms, we need to configure them by their priorities. After configure some priority alarm, the network trouble alarms which are equal or higher than this alarm are enabling. Different alarm switches are configured to send all types of alarms (5 alarms): macRemErrXcon sends Macstatus, RemoteCCM, ErrorCCM and XconCCM alarms, which are also called sending alarm type 1-4; remErrXcon sends RemoteCCM, ErrorCCM and XconCCM alarms, which can be called alarm type 1-3; errXcon sends ErrorCCM and XconCCM alarms, which also can be called alarm type 1-2; Xcon sends XconCCM alarm – alarm type 1; None, do not send any alarm. Default status is macRemErrXcon, which are sent Macstatus, RemoteCCM, ErrorCCM and XconCCM four alarms. To recover sending alarm types, we use command: **no snmp-server cfm-trap**.

Steps	Commands	Description
1	config	Enter global configuration mode.
2	service CSIID level level	Enter service instance mode. <i>CSIID</i> : name of service instance, length is 1-13 byte. <i>level</i> : level of maintenance domain. <i>all</i> : allow all warming; <i>macremerr</i> : allow level 2-5 warming; <i>remerr</i> : allow level 3-5 warming; <i>xcon</i> : allow level 5 warming; <i>none</i> : don't allow warming;
3	snmp-server trap cfm {all/ macremerr / remerr / ccmerr / xcon / none} mep {mepid-list all}	

		<i>mepid-list</i> : mep list, range is 1-8191.
4	exit	Enter global configuration mode.
5	exit	Return to privileged mode;
6	show ethernet cfm	Display CFM basic information;

Illustration: Set alarm as remerrxcon:

```
Raisecom (config) #snmp-server trap cfm all mep all
```

```
Raisecom (config) #exit
```

Sent none as alarm:

```
Raisecom (config) #snmp-server cfm-trap none
```

39.4.14 Configure Enable/Disable CFM Protocol in Global Mode

It is used to command CFM protocol in global mode. In default situation, CFM protocol disables.

Steps	Commands	Description
1	config	Enter global configuration mode.
2	ethernet cfm {enable /disable}	Enable/disable CFM protocol. <i>enable</i> : enable CFM protocol in GLOBAL mode; <i>disable</i> : Disable CFM protocol in GLOBAL mode.
3	exit	Return to Privileged EXEC mode.
4	show ethernet cfm	Check all configuration information of CFM protocol on switches.

Illustration: In global mode, enable CFM protocol

```
raiecom #config
```

```
raiecom(config)#ethernet cfm enable
```

```
raiecom(config)#exit
```

39.4.15 Configure Enable/Disable CFM Protocol in Port Mode

We use the command to allow switch port runs CFM protocol and enable\disable CFM protocol of some port. When switch of port CFM protocol disable, MP configurated on port is not effective. By default CFM protocols of all ports enable.

Steps	Commands	Description
1	config	Enter global configuration mode.
2	interface port <i>portid</i>	Enter indicated <i>portid</i> port.
3	ethernet cfm {enable / disable}	Enable/disable CFM protocol.

		<i>enable</i> : in global mode, enable CFM <i>disable</i> : in global mode, disable CFM
4	exit	Return to global configuration mode.
5	exit	Return to privileged EXEC mode.
6	show ethernet cfm	Check the switch about the CFM protocol's whole configuring information.

Illustration: In port 3, enable CFM protocol

```
raiecom#config
```

```
Raisecom (config) #interface port 3
```

```
Raisecom (config-port) #ethernet cfm enable
```

39.5 Monitoring and Maintenance

Commands	Description
show ethernet cfm traceroute-cache	Show LinkTrace database studied route trace information.
show ethernet cfm mp local	Show local MP configuration information, include MEP and MIP.
show ethernet cfm errors	Show error CCM database information.
show ethernet cfm domain	Show indicated maintenance domain configuration information.
show ethernet cfm mp remote	Show remote MEP information.
show ethernet cfm mp remote detail	Show remote MEP detail information.
show ethernet cfm	Show CFM protocol configuration information.
clear ethernet cfm errors	Clear error CCM database indicated information.
clear ethernet cfm mp remote	Clear indicated remote MEP information.
clear ethernet cfm traceroute-cache	Clear Linktrace database archived route trace information.

39.5.1 Display Route Trace Information Studied in LinkTrace Database

Commands format: `show ethernet cfm traceroute-cache`

Function: shows LinkTrace database archived entry number and time, related MD names, levels and service instance related VLANs. Also, it also can display each Linktrace hop number; reply LTR messages MP's MAC address, LTM messages receiving and sending port, LTM messages transmitting status, LTM messages transmitting type and next-hop devices' mac address. When LinkTrace database is in disable status, there is no any route trace information is displayed.

Display results: Default archive data entry number is 100, archive time is 100 (database is enable). Trace one MEP route with MD of md1, level of 3, VLAN of 4 and MAC address is CCCC.

IC_A#show ethernet cfm traceroute-cache

The size of the linktrace database: 100 hold-time: 100

Tracing the route toCCCC on domain md1, level 3, VLAN 4.

Hops	HostMAC	Ingress/EgressPort	IsForwarded	RelayAction	NextHop
1	AAAA	8/1	Yes	RlyFdb	BBBB
2	BBBB	2/3	Yes	RlyFdb	CCCC
3	CCCC	-/9	No	RlyHit	CCCC

39.5.2 Display local MP Configuration Information, include MEP and MIP

Command Format: **show ethernet cfm mp local [mep / mip] [interface port portid / domain domain-name / level level-id]**

Function: It is used to check the local MP configuration information and also can check the MIP related MD levels, related port number and MAC address information. Also, it can check MEP name, related MD level, port number, MEP send direction, MAC address information, CCM messages enable/disable status, sent entries number, etc. We can choose whether display MEP, MIP or both; we also can choose display indicated port MP or all port MP, or choose to display MP of indicated MD.

Display results: Show the level 5 MIP which is configured in port 2 and related MAC address as BBBB; when a MEP is configured as level 3, sending direction is up, CCM messages is disable, sent messages entries number is 0.

Raisecom(config)#**show ethernet cfm mp local-mp**

Local mep configuration information:

Mpid	Level	PrimaryVlan	Direction Port	Cc-Status	SendCCMs	Trap-status
301	3	100	UP	1	Enable	2950 macRemErr

39.5.3 Display Error CCM Database Information

Command Format: **show ethernet cfm errors [domain domain-name / level level-id]**

Function: it is used to check levels of MD which has fault occurred, fault occurred MA's VLAN, fault occurred local MEP's MEPID, fault related remote MEP's MAC address, the fault types which can be checked at the same time, we can choose to show the CCM fault information in indicated MD, also can choose to show indicated MD level's CCM fault information.

Display results: Display level 1 fault CCM information, fault MA's VLAN is 4, fault found local MEP's MPID as 2, fault found remote MAC address as CCCC, fault type as ErrorCCM.

Raisecom(config)#**show ethernet cfm errors**

Level	VLAN	MPID	RemoteMep Mac	ErrorType	Age(s)	AffectedService

39.5.4 Display Indicated Maintenance Domain Configuration Information

Commands format: show ethernet cfm domain [domain-name]

Function: It is used to check the created MD level and MA related VLAN. Also CCM messages' sending interval can be displayed.

Display results: Displays MD which is configured as name of md3-1, level 3, service instance named ma3-1-4 and related VLAN 4. Also it shows MD named md5-1, level 5.

Raisecom#show ethernet cfm domain

Maintenance Domain(MD)

Level:3 MD Name Format:none MD Name: (NULL)

Total services: 1

Service	Format	PrimaryVlan	VlanNumber	C-vlan	Priority	CcmInterval	CC-Check
ma3-1-4	ITU-IC	100	6	10	4	1	

39.5.5 Display Remote MEP Information

Commands format: show ethernet cfm mp remote [domain domain-name / level level-id]

Function: it is used to check the remote MEP's MEP ID, the remote MEP located MD name, and that MD's level, the remote MEP located MD level, the remote MEP located MA's related VLAN, the remote MEP name located port status, the remote MEP MAC address, the local switch port which receive CCM messages sent by the remote MEP, and the CCM messages receiving interval from the same remote MEP last time.

Display results: Display MPID of the remote MEP as 1, its MD is md3; Level is 3; remote MEP located MA VLAN 4; port status is up; remote MEP MAC address is CCCC; local switch port number which receives messages is 1; the interval is 9 seconds.

Raisecom(config)#show ethernet cfm remote-mep

Maintenance Domain (MD) level: 3

Maintenance Domain (MD) name:

Mpid	Service	Primary Vlan	IfState	PortState	Mac Address	Source Age
------	---------	--------------	---------	-----------	-------------	------------

39.5.6 Display Particular Information of Remote MEP

Note: ISCOM2128EA-MA products doesn't support the application.

Commands format: show ethernet cfm mp remote detail {mpid mep-id/mac mac-address}[domain domain-name / level level-id [vlan vlan-id]]

Function: it can display remote MEP MAC address, remote MEP located MD name, remote MEP located MD level, remote MEP located MA VLAN, remote MEP's MEP ID, the local switch port which receives CCM messages sent by that remote MEP, CCM messages receiving time interval since last time from that remote MEP port, CCM receiving amount statistics sent by that remote MEP and error CCM receiving amount statistics.

By commands parameter, filter remote MEP and display:

- [Compulsory] choose to indicate remote MEP's MEP ID or MAC address.
- [Optional] do not indicate MD, MD name or MD level; If choose to indicated MD level, we also can choose to indicate VLAN ID or not.

We can form the filter remote MEP by those two parameters above.

Display Results: We can find the remote MEP MAC address is CCCC, located MD's name is Md1, level is 3, located MA VLAN is 4, remote MEP's MEPID us 1, local switch port number which receives messages is 8, time interval is 9 seconds, CCM messages received are 120 and error packet is 0.

```
IC_A#show ethernet cfm remote detail mpid 1 domain md1
```

MAC address: CCCC
MD/Level: Md1/3
VLAN: 4
MPID: 1
Ingress Port: 8
Age: 9
CCM statistics: 122/0 (Received/Error)

39.5.7 Display CFM Protocol Configuration

Commands format: **show ethernet cfm**

Function: It is used to display CFM configuration information such as CFM protocol status in GLOBAL mode, CFM status in the port, error CCM messages archived time and error indication level.

Display results: enable global CFM protocol, default port CFM protocol is enable, error archive time is 100, error sending level macRemErrXcon.

```
Raisecom#show ethernet cfm
```

Global cfm status: enable
Port cfm enabled portlist: 1-28
Archive hold time of error CCMs: 100(Min)
Remote mep aging time: 100(Min)

39.5.8 Clear Error CCM Database Indicated Information

Commands format: **Clear Ethernet cfm errors [level level-id]**

Function: By enter MD name, we can clear indicated MD error information; by enter MD level parameters, we can clear the indicated level error information; if do not enter any parameter, it will delete all the error information.

Illustration: Clear all level 3 error information in CCM error database

```
Raisecom (config) #clear ethernet cfm errors level 3
```

39.5.9 Clear Archive Route Trace Information in Linktrace Database

Commands format: `Clear Ethernet cfm traceroute-cache`

Function: Clear data information in LinkTrace database

Illustration: Raisecom (config) #clear ethernet cfm traceroute-cache

39.5.10 Clear Indicated Remote MEP Information

Command Format: `clear ethernet cfm remote-mp [level level [service service-instance [mpid mepid]]]`

Function: It is used to clear CC database indicated remote MEP information and it also can indicate the MD which needs to be cleared.

Illustration: Clear remote MEP information in MD named md3-1

Raisecom (config)#`clear ethernet cfm mp remote domain md3-1`

39.6 Typical Configuration Illustration

Topology structure as shown below:

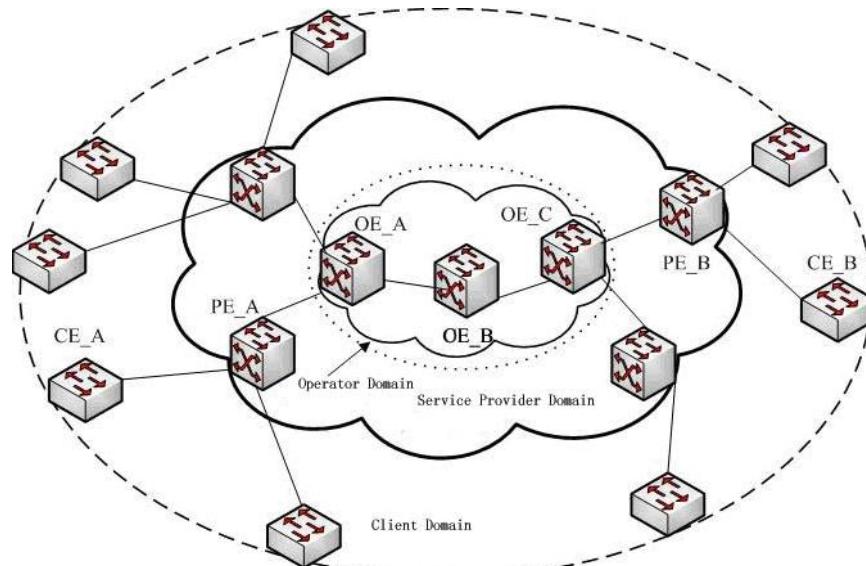


Figure 39-2

We divide metropolitan access network (MAN) into three maintenance domains: client domain with level 5, service provider domain with level 3 and operator domain with level 1. As the figure above, CE_A is connected to PE_A, PE_A is connected to OE_A, OE_A is linked to device OE_C through device OE_B, CE_B is connected to PE_B, PE_B is connected to OE_C. We configure CE_A and CE_B with level 5 MEP; PE_A and PE_B are configured as level 5 MIP, level 3 MEP and level 3 MIP; OE_A and OE_C are configured level 3 MIP, level 1 MEP and level 1 MIP; OE_B is configured with two level 1 MIPs. Details are:

Configuration steps of CE_A:

```
Raisecom(config)#ethernet cfm domain md7-1 level 7
Raisecom(config-ether-cfm)#exit
Raisecom(config)#ethernet cfm domain md5-1 level 5
```

```
Raisecom(config-ether-cfm)#service ma5-1-100 vlan 100
Raisecom(config-ether-cfm)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#ethernet cfm mip level 7
Raisecom(config-port)#ethernet cfm mep level 5 up mpid 501 vlan 100
Raisecom(config-port)#exit
Raisecom(config)#ethernet cfm enable
Raisecom(config)#ethernet cfm cc enable level 5 vlan 100
```

PE_A configuration steps:

```
Raisecom(config)#ethernet cfm domain md5-1 level 5
Raisecom(config-ether-cfm)#exit
Raisecom(config)#ethernet cfm domain md3-1 level 3
Raisecom(config-ether-cfm)#service ma3-1-100 vlan 100
Raisecom(config-ether-cfm)#exit
Raisecom(config)#interface port 1
Raisecom(config-port)#ethernet cfm mip level 5
Raisecom(config-port)#ethernet cfm mep level 3 up mpid 301 vlan 100
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#ethernet cfm mip level 3
Raisecom(config-port)#exit
Raisecom(config)#ethernet cfm enable
Raisecom(config)#ethernet cfm cc enable level 3 vlan 100
```

OE_A configuration steps:

```
Raisecom(config)#ethernet cfm domain md3-1 level 3
Raisecom(config-ether-cfm)#exit
Raisecom(config)#ethernet cfm domain md1-1 level 1
Raisecom(config-ether-cfm)#service ma1-1-100 vlan 100
Raisecom(config-ether-cfm)#exit
Raisecom(config)#interface port 1
Raisecom(config-port)#ethernet cfm mip level 3
Raisecom(config-port)#ethernet cfm mep level 1 up mpid 101 vlan 100
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#ethernet cfm mip level 1
Raisecom(config-port)#exit
```

```
Raisecom(config)#ethernet cfm enable
Raisecom(config)#ethernet cfm cc enable level 1 vlan 100
```

OE_B configuration steps:

```
Raisecom(config)#ethernet cfm domain md1-1 level 1
Raisecom(config-ether-cfm)#exit
Raisecom(config)#interface port 1
Raisecom(config-port)#ethernet cfm mip level 1
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#ethernet cfm mip level 1
Raisecom(config-port)#exit
Raisecom(config)#ethernet cfm enable
```

OE_C configuration steps:

```
Raisecom(config)#ethernet cfm domain md3-1 level 3
Raisecom(config-ether-cfm)#exit
Raisecom(config)#ethernet cfm domain md1-1 level 1
Raisecom(config-ether-cfm)#service ma1-1-100 vlan 100
Raisecom(config-ether-cfm)#exit
Raisecom(config)#interface port 1
Raisecom(config-port)#ethernet cfm mip level 3
Raisecom(config-port)#ethernet cfm mep level 1 up mpid 102 vlan 100
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#ethernet cfm mip level 1
Raisecom(config-port)#exit
Raisecom(config)#ethernet cfm enable
Raisecom(config)#ethernet cfm cc enable level 1 vlan 100
```

PE_B configuration steps:

```
Raisecom(config)#ethernet cfm domain md5-1 level 5
Raisecom(config-ether-cfm)#exit
Raisecom(config)#ethernet cfm domain md3-1 level 3
Raisecom(config-ether-cfm)#service ma3-1-100 vlan 100
```

```

RaiseCom(config-ether-cfm)#exit
RaiseCom(config)#interface port 1
RaiseCom(config-port)#ethernet cfm mip level 5
RaiseCom(config-port)#ethernet cfm mep level 3 up mpid 302 vlan 100
RaiseCom(config-port)#exit
RaiseCom(config)#interface port 2
RaiseCom(config-port)#ethernet cfm mip level 3
RaiseCom(config-port)#exit
RaiseCom(config)#ethernet cfm enable
RaiseCom(config)#ethernet cfm cc enable level 3 vlan 100

```

CE_B configuration steps:

```

RaiseCom(config)#ethernet cfm domain md7-1 level 7
RaiseCom(config-ether-cfm)#exit
RaiseCom(config)#ethernet cfm domain md5-1 level 5
RaiseCom(config-ether-cfm)#service ma5-1-100 vlan 100
RaiseCom(config-ether-cfm)#exit
RaiseCom(config)#interface port 2
RaiseCom(config-port)#ethernet cfm mip level 7
RaiseCom(config-port)#ethernet cfm mep level 5 up mpid 502 vlan 100
RaiseCom(config-port)#exit
RaiseCom(config)#ethernet cfm enable
RaiseCom(config)#ethernet cfm cc enable level 5 vlan 100

```

After configuring CE_A, PE_A, OE_A, OE_B, OE_C, PE_B and CE_B, the MEP configured device should be able to ping MAC address and trace route success with other devices which are configured MEP with same level MP.

On CE_A, ping and trace route CE_B as below, use “CE_B” represents CE_B device’s MAC address:

```

RaiseCom#ping ethernet CE_B level 5 vlan 100
RaiseCom#traceroute ethernet CE_B level 5 vlan 100

```

On PE_A, ping and trace route PE_B are described as below, use “PE_B” represents PE_B device’s MAC address:

```

RaiseCom#ping ethernet PE_B level 3 vlan 100
RaiseCom#traceroute ethernet PE_B level 3 vlan 100

```

On OE_A, ping and trace route OE_B are OE_C as described as below, use “OE_B”and “OE_C” represent OE_B and OE_C device MAC address:

Raisecom#**ping ethernet OE_B level 1 vlan 100**

Raisecom#**traceroute ethernet OE_B level 1 vlan 100**

Raisecom#**ping ethernet OE_C level 1 vlan 100**

Raisecom#**traceroute ethernet OE_C level 1 vlan 100**

Chapter 40 Y.1731 Configuration

This chapter describes how to configure Y.1731 function, including the following:

- ❖ Functional overview of Y.1731
- ❖ Default configuration list of Y.1731
- ❖ Configuration guidance and restrictions of Y.1731
- ❖ Configuration list and itemized explanation of Y.1731
- ❖ Monitoring and maintenance of Y.1731
- ❖ Typical configuration illustration of Y.1731

40.1 Functional overview of Y.1731

With the rapid development of Ethernet technology, Ethernet technology has been widely used in MAN and WAN. As the complexity of MAN and WAN network infrastructure, and the existence of abundant various users, usually require a number of different network operators to work together to provide end-to-end business customers, thus a higher demand brings forward for the Ethernet management maintenance and reliability. Traditional Ethernet has not carrier-managed capabilities, cannot detect the second floor of a network failure. In order to achieve the same level of traditional carrier-class transport network service standards, for various research groups and organizations are actively engaged in technology research and standard-setting.

IEEE and ITU-T work together to end-to-end business-class OAM technology research, providing a comprehensive OAM tool for carrier-class Ethernet OAM. ITU-Y.1731 proposal published by ITU-T divide Ethernet OAM into fault management and performance monitoring while IEEE802.1ag detailed technically, such as state machine of the fault management and MIB. RAISECOM provides fault management capabilities of compatible ITU-Y.1731 and IEEE802.1ag standard, as well as performance monitoring function defined in Y.1731, which collectively referred to as functional Y.1731.

Fault Management CFM (Connectivity Fault Management), is an end-to-end business-class OAM protocol for active fault diagnosis of EVC (Ethernet Virtual Connection) for. Through fault management functions effectively reduce network maintenance costs and improve Ethernet maintainability. Fault management functions include end-to-end connectivity fault detection tools (CC: Continuity Check) the provision of, end-to-end connectivity fault recognition tools (LB: LoopBack) and fault isolation tools (LT: LinkTrace).

40.1.1 Components of Y.1731

➤ Maintenance Domain

Maintenance Domain is a network running 1731 function, which defines network scope of the OAM management. Level attributes in maintenance domain are divided into 8 (0 ~ 7), the bigger the higher, corresponding to the larger scope of maintenance domain. In the same VLAN scope, the different maintenance domains can be adjacent, nested, but not cross.

➤ Service instance

Service Instance, also known as Maintenance Associations, corresponds to a business, can be mapped to a set of S-VLAN. A Maintenance Domain can be configured to several service instances, each service instance has dependency association to several S-VLAN, and VLAN in different dependency association cannot be cross-linked. Although the service instances can be mapped to several VLAN, but only a VLAN in a service instance, used to transceiver OAM message, this VLAN is called main VLAN in VLAN instance, in short, service instances VLAN.

A service instance can be configured with several MEP, message sent by MEP in same service instance has same S-VLAN TAG, the same priorities and the same C-VLAN TAG, and MEP can receive OAM message send by other MEP e in same MA.

➤ MEP

MEP (Maintenance associations End Point) is a management activity configured on edge of the service instance related to service instance, the most important activity entity in Y.1731. MEP can send and processed CFM message, whereabouts of MEP service instances and maintenance domain determine VLAN sent by MEP and level. MEP cut-off messages in the same main VLAN at the same level self-closing or lower, and transmit message over its own high-level.

➤ MIP

MIP is a management activity entity configured within service instance. A MIP is component of 2 MHF (MIP Half Function). MIP cannot take the initiative to send CFM message, but can handle and respond to LTM and LBM messages. MIP is created by automation according to auto-configuration rule, cannot be created by manual. Auto-configuration rules for MIP showing in appendix 1.7.

➤ MP

MEP and MIP are called by a joint name MP.

40.1.2 Basic function of Y.1731

The realization of Y.1731 function based on the correct configuration of the maintenance domain, service instances, MEP and MIP, including the following 3 sub-functions:

Fault detection function (Continuity Check, CC)

Failure confirm functional (loop back, LB)

Fault isolation function (Link Trace, LT)

➤ Fault detection function

Fault detection function is the use of CC (Continuity Check) protocol to detect the connectivity of Ethernet virtual connection (EVC), to determine the connection status between MP. This function through MEP periodically sent CCM (Continuity Check Message) to achieve, other MEP in the same service instance receive the message, which determine the status of the remote MEP. If equipment failure or the middle link configuration error, lead that MEP can not receive and process CCM sent by remote MEP. If the MEP did not receive remote CCM messages in 3.5 CCM interval cycle, the existence of that link failure, will in accordance with the alarm priority configuration to send fault alarm.

➤ Failure confirm function

Failure confirm function used to identify connected status of local facilities and remote equipment,

this function via source MEP sent LBM (LoopBack Message) and the destination MP to respond to LBR (LoopBack Reply) to determine the connectivity between two MP. MEP send the MP with failure confirms to LBM, after the MP received a LBM message the, it sent 1 LBR to source MEP. If the source MEP received LBR, then confirm the path is connected. Otherwise, confirm the existence of connectivity failure. Failure confirm function function is similar to layer-3 ping, and therefore failure confirm function form as layer-2 ping in application

➤ Fault isolation function

Fault isolation is used to determine trace from source MEP to the target MP. This function sent LTM through source MEP (Link Trace Message) to destination MP, each bridge device configured with LTM transmission path will respond to LTR (Link Trace Reply) to source MEP, reorganize through effective LTR and LTM by record, ultimately confirmed that the path between the MP. Fault isolation is similar to layer-3 traceroute functions, so in application it forms as Layer-2 traceroute.

Altogether, Y.1731 realizes OAM technology on end-to-end layer, which helps reduce service providers' operation cost and enhance their competition advantages.

40.2 Default configuration list of Y.1731

No.	Property	Default
1	Default MD configuration status	No MD
2	Default service instance configuration status	No service instance
3	Default global functional switch status	Disable
4	Default port functional switch status	Enable
5	Default error CCM database saving time	100 minutes
6	Default fault alarm level	macRemErrXcon, in support of 4 bug alarms: port fault, loss of remote end, CCM error, cross-connection.
7	Default service instance VLAN mapping	No VLAN mapping
8	Default MEP configuration status in service instance	No MEP
9	Default static remote MEP in service instance	No static remote MEP
10	Default MEP configuration status in port	No MEP
11	Default static remote MEP configuration in port	No static remote MEP
12	Default service instance CCM sending time interval	10 seconds
13	Default MEP CCM transmitting switch status	disable
14	Default MEP CCM transmitting mode	Passive mode
15	Default remote MEP dynamic import function	Doesn't import dynamically
16	Default cc check function learned by remote MEP	disable

17	Default aging time of dynamic remote MEP	100 minutes
18	Default service instance OAM packets priority	6
19	Default LBM number transmitted by layer-2 ping	5
20	Default TLV length of layer-2 ping data	64
21	Default source MEP of layer-2 ping	Auto searching
22	Default initial TTL of layer-2 traceroute	64
23	Default source MEP of layer-2 traceroute	Auto searching
24	Default LT database switch	disable
25	Default LT database max. save data amount	Save at most 100 data item by default when LT database enable. Save 0 data item by default when LT database disable.
26	Default LT database save data time	100 minutes
27	Default service instance OAM packets C-VLAN configuration	No C-VLAN

40.3 CFM configuration constraints and limitations

- Each device can be configured for 8-level (0-7) maintenance domain (MD); If you specify the maintenance domain names, the allowable string length of domain name is between 1-16 bytes;
- The maximum number in service instance (MA) configured in each device exist differences in equipment, the details may refer to the list of equipment characteristics and other related document;
- Before delete the maintenance domain, user should delete all MEP of maintenance domain, otherwise deletion of the maintenance domain will lead to failure;
- When configuring service instance, the allowed string length of MA Name is between 1-13 bytes;
- Each service instance is mapped to 32 VLAN at most, use the smallest VLAN as main VLAN, MEP in service instance utilize main VLAN for OAM transmitting messages, other VLAN is not used for send and receive messages. In overall scope, VLAN mapping associations can not cross, otherwise will lead to the failure in service instance VLAN mapping
- If the service instance has not yet been mapped to any VLAN, then configure the local MEP in service instance is not allowed
- If the service instance has been configured MEP, it mustn't delete and modify VLAN mapping of services instance
- In accordance with standard protocols, CCM transmitting interval in service instance can configure seven kinds of cycle: 3.33 ms, 10ms, 100ms, 1s, 10s, 60s and 600s; later four kinds of time cycle for fault management and configuration, therefore the allowing cycle scope of equipment is 1s, 10s, 60s and 600s.

- Before modifying CCM transmitting interval, user need to close all CCM transmitting switch of MEP in services instance
- Before delete the service instance user should delete all MEP in service instance, otherwise will lead to the failure of delete services instances;
- Maximum MEP of each device exist differences in equipment, the details may refer to the list of equipment characteristics and other related document

40.4 CFM configuration list and instruction

- The overall functional switches and ports functional switch

➤ Related entities configuration of Y.1731

Configure maintain domain MD

Configure service instance MA

Configure MEP

Configure a static remote MEP

- Fault detection

Configure CCM transmitting switch

Configure CCM transmitting interval

Configure CCM transmitting mode

Configure dynamic import function learned by remote MEP

Configure aging time of remote MEP

Configure client VLAN of OAM message

Configure OAM message priority

Configure hold time of error CCM message

Configure fault alarm level

- Failure confirm--the implementation of layer-2 ping operation

- Fault isolation

The implementation of layer-2 traceroute operation

Configure switch status of database LT

Configure hold time of database LT

Configure preservable data entries of database LT

40.4.1 Configure overall functional switch of Y.1731

Disable Y.1731 global function by default (Disable).

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode
2	ethernet cfm {enable/disable}	Enable/disable global functional switch. <i>enable</i> : global function enable. <i>disable</i> : global function disable.
3	exit	Return to privileged user mode
4	show ethernet cfm	Show Y.1731 global configuration information

Illustration: Enable global functional switch in global configuration mode.

Raisecom#**config**

Raisecom(config)#**ethernet cfm enable**

Raisecom(config)#**exit**

Note: Although the command contains the keyword "cfm", the functional switch impact that whether CC, LB, LT, PM, RFC2544 take into force within the overall scope.

40.4.2 Configure ports functional switch of Y.1731

When Y.1731 port switch function switch disable, MP configured on the port will not take into effect, OAM message of Y.1731 cannot be transmitted or received on port. Enable functional switch of all ports by default.

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <i>port-id</i>	Enter specified <i>port-id</i> port mode.
3	ethernet cfm {enable/disable}	Enable/disable port Y.1731 function. <i>enable</i> : port function enable. <i>disable</i> : port function disable.
4	exit	Return to global configuration mode.
5	exit	Return to privilege mode.
6	show ethernet cfm	Show Y.1731 overall configuration information.

Illustration: Enable Y.1731 function on ports 3.

Raisecom#**config**

Raisecom(config)#**interface port 3**

Raisecom(config-port)#**ethernet cfm enable**

Note: Although the command contains the keyword “cfm”, the functional switch impact that whether CC, LB, LT, PM, RFC2544 take into force within the overall scope.

40.4.3 Configure maintenance domain

When configuring maintenance domain, you must specify the level of domain maintenance. RAISECOM Y.1731 supports to configure maintenance domain of IEEE802.1ag style, and maintenance domain of ITU-T Y.1731 style. Name of maintenance domain parameter is optional parameters, if specify domain name , the maintenance domain is IEEE802.1ag style, all MA of maintenance domain is IEEE802.1ag style, MAID field sending CCM Message by all MEP of the maintenance use the format IEEE802.1ag; If you do not specify the maintenance domain names, maintenance domain is the ITU-T Y.1731 style, all service instance of the maintenance domain is the ITU-T Y.1731 styles, MEGID field sending the CCM message by all MEP of the maintenance domain to use format ITU-T Y.1731.

Delete MD: **no ethernet cfm level level**

Step	Command	Description
1	config	Enter global configuration mode.
2	ethernet cfm domain [md-name domain-name] level level	Configure maintenance domain. <i>domain-name</i> : name of the maintenance domain, the string length: 1-16 bytes; <i>level</i> : the level of maintenance domain, range in: 0-7.
3	exit	Return to privileged user mode.
4	show ethernet cfm domain [level <0-7>]	Show configuration information of maintenance domain.

Illustration 1: Configure maintenance domain of style IEEE802.1ag, name is md3-1, level is 3.

Raisecom#**config**

Raisecom (config) #**ethernet cfm domain md-name md3-1 level 3**

Raisecom (config) #**exit**

Illustration 2: Configure maintenance domain of ITU-T Y.1731-style, level-3.

Raisecom#**config**

Raisecom (config) #**ethernet cfm domain level 3**

Raisecom (config) #**exit**

Note:

- Level of specified the maintenance domain can not be repeated, otherwise, it will result in failure to configure maintenance domain;

- If user specify maintenance domain name, the maintenance domain name must be unique, otherwise it will result in failure to configure maintenance domain.

40.4.4 Configure service instance

When configuring service instance, user need to specify the level of maintenance domain. Service instance name must meet the following requirements: (maintenance domain name, service instance name) composed string is unique in the global scope. If service instance configuration succeeds or already exists, user will enter service instance mode, which is the most important mode of Y.1731 function configuration.

Delete service instance: **no service *service-instance* level *level-id***.

Step	Command	Description
1	config	Enter global configuration mode
2	service <i>CSIID</i> level <i>level</i>	Create service instance and enter the service instance mode. <i>CSIID</i> : name in service instance, the length is 1-13 bytes; <i>level</i> : the range of maintenance domain level: 0-7.
3	exit	Return to global configuration mode
4	exit	Return to privileged user mode
5	show ethernet cfm domain [level <0-7>]	Shows maintenance domain and configuration information in service instance

Illustration: Configure the service instance of name ma3-1-4 in a level-3 maintenance domain.

Raisecom#**config**

Raisecom (config) #**ethernet cfm domain level 3**

Raisecom (config) #**service ma3-1-4 level 3**

Raisecom (config-service) #**exit**

Raisecom (config) #**exit**

Note:

- If there is no same maintenance domain in specified level, the configuration of the service instance will lead to failure;
- If name of the maintenance domain + name in service instance composed string is not unique, it will lead to the failure of MA configuration;
- If configurations in service instance reach the maximum, it will lead to failure of configuration in service instance.

40.4.5 Configure VLAN mapping in service instance

When configuration in service instance is mapped to a VLAN list, VLAN list allows a maximum of

32 VLAN, in VLAN list smallest VLAN is main VLAN in service instance. All MEP in service instance send and receive packets through the main VLAN, other VLAN is not used to transmit or receive packets.

Service instance is mapped to a group of VLAN, namely the VLAN in VLAN list is fully equivalent, as use main VLAN for transmitting and receiving packets, which all of other VLAN in the list are mapped to the main VLAN in logic. This logical VLAN mapping is global and VLAN mapping association of different service instance can be the same, but you can not cross.

The following is illegal:

Counter-Illustration 1: When service instance ma3-1-1 related to VLAN 10-20 and service instance ma3-1-2 mapping VLAN 15-30. VLAN 16-20 have been mapped repeatedly to the main VLAN 10 and the main VLAN 15.

Counter-illustration 2: When service instance ma3-1-3 mapped to the VLAN 100-120 and service instance ma3-1-4 mapped to the VLAN 90-100, main VLAN 100-120 is mapped to main VLAN 100, and VLAN 100 is mapped to VLAN 90.

Counter-illustration 3: Service instance ma3-1-5 in maintenance domain of Level 3 map to the VLAN 10-20, level 3 of the other service instance in maintenance domain of Level 3 also map to VLAN10-20 used in the same main VLAN.

The following is legal:

Positive Illustration 1: service instance ma3-1-5 in maintenance domain of Level 3 map to VLAN 10-20, service instance ma5-1-1 in maintenance domain of Level 5 is mapped to the VLAN 10-20.

Delete service instance: **no service vlan-list**

Step	Command	Description
1	config	Enter global configuration mode
2	service service-instance level level	Enter service instance mode <i>service-instance</i> : name in service instance, the length of 1-13 bytes; <i>level</i> : the range of maintenance domain level: 0-7;
3	service vlan-list vlan-list	<i>vlan-list</i> : vlan list, range in 1-4094;
4	exit	Return to global configuration mode
5	exit	Return to privileged user mode
6	show ethernet cfm domain level [<0-7>]	Shows maintenance domain and configuration information in service instance.

Illustration: Configure VLAN mapping relation in the service instance ma3-1-4.

Raisecom#**config**

Raisecom (config) #**ethernet cfm domain level 3**

Raisecom (config) #**service ma3-1-4 level 3**

Raisecom (config-service) #**service vlan-list 10-25**

Raisecom (config) #**exit**

Note:

- If the number of VLAN in VLAN list is more than 32, it will lead to the failure of VLAN mapping;
- If VLAN mapping is cross to VLAN mapping of other service instance, VLAN mapping fail;
- If same VLAN mapping exists in the same services instance, VLAN mapping will lead to the failure;
- If a service instance has been mapping the VLAN, user must delete the VLAN mapping relations before in order to configure a new VLAN mapping;
- If the service instance has been configured MEP, user should first delete the MEP, and then delete the VLAN mapping relationship.

40.4.6 Configure MEP

There are two kinds of MEP configuration: one is MEP configuration over service instance, and the other one is over port. Before configuring MEP over service instance, user should configure maintenance domain first, and then configure service instances in the maintenance domain, and map VLAN in service instance. The direction of MEP currently configured only support the UP, if the command is not specified, the default direction is UP. For MEP configuration over port, one port can only configure one MEP and the direction is down.

Delete designated MEP over service instance: **no service mep mepid**

Delete designated MEP over port: **no ethernet cfm down-mep**

Step	Command	Description
1	config	Enter global configuration mode
2	service CSIID level level	Enter service instance mode <i>CSIID</i> : name in service instance, the length of 1-13 bytes; <i>level</i> : the range of maintenance domain level: 0-7.
3	service mep [up/down] mpid mepid {port port-id line line-id client client-id }	Configure MEP in service instance <i>up</i> : up-bound MEP <i>mepid</i> : MEPID; <i>port-id</i> : Port ID, value 1 to the largest port ID; <i>line-id</i> : Line port ID, value 1 to the largest line port ID; <i>client-id</i> : Client port ID, value 1 to the largest Client port ID.
4	exit	Return to global configuration mode.
4	exit	Return to privileged user mode.

5 show ethernet cfm local-mp [interface port <1-MAX_PORT_STR> | level <0-7>] Show information of local MEP.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter port mode <i>portid</i> : port ID
3	ethernet cfm down-mep mpid <1-8191>	Configure down mep over port <1-8191>: MEPID range in 1-8191.
4	show ethernet cfm local-mp [interface port <1-MAX_PORT_STR> level <0-7>]	Show information of local MEP

Illustration: Configure MEP in the service instance, port 1

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level 3**

Raisecom(config)#**service ma3-1-4 level 3**

Raisecom(config-service)#**service vlan-list 10-45**

Raisecom(config-service)#**service mep up mpid 100 port 1**

Raisecom(config)#**exit**

Configure MEP under port:

Raisecom#**config**

Raisecom(config)#**interface port 1**

Raisecom(config-port)#**ethernet cfm down-mep mpid 1**

Raisecom(config- port)# **exit**

Raisecom(config)#**exit**

Note:

- If the service instance is not mapped VLAN, it will lead to the failure of MEP configuration;
- If specified port already exists MEP in the current service instance, it will lead to the failure of MEP configuration;
- If the maximum number of MEP configured in the device has already reached the ceiling, it will lead to the failure of MEP configuration;
- If the local MEP static or remote MEP of MEPID already exists in the service instance, it will lead to the failure of MEP configuration;
- Configure failed if there is MEP existing in configuration over port;
- Configure failed if the MEP over port has been configured as static remote over port.

40.4.7 Configure a static remote MEP

There is a MEP list in each service instance, which saves all the MEP information in the service instance, including: local MEP, static remote MEP, and dynamic remote MEP. User can use **show ethernet cfm remote-mep static** to show all the static MEP information under service instance.

Before configuring static remote MEP, you should configure maintaining domain first, and configure service instance in the maintaining domain. When MEP receives CCM, if service instance enables cc check function and no remote MEP with identical MEP ID as CCM carried from MEP list, MEP is considered to receive unexpected CCM. User can direct configure static remote over port under the port and one port can only configured one static remote.

Delete the specified static remote MEP: **no service remote mep {1-8191}**

Delete static remote MEP under port: **no ethernet cfm down-mep**.

Step	Command	Description
1	config	Enter global configuration mode
2	service service-instance level level	Enter service instance mode <i>service-instance</i> : name in service instance, the length of 1-13 bytes; <i>level</i> : the range of maintenance domain level: 0-7.
3	service remote-mep {1-8191}	Configure static remote MEP.
4	exit	Return to global configuration mode
5	exit	Return to privileged user mode
6	show ethernet cfm remote-mep static	Show information of static remote mep.

Illustration: Configure static remote MEP in service instance.

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level 3**

Raisecom(config)#**service ma3-1-4 level 3**

Raisecom(config-service)#**service remote-mep 100-1000**

Raisecom(config)#**exit**

Configure static remote MEP under port.

Raisecom#**config**

Raisecom(config)#**interface port 1**

Raisecom(config-port)#**ethernet cfm remote-mep 2**

Raisecom(config)#**exit**

Note: If the assigned MEPID is used by local MEP in service instance or static remote MEP, the configuration is unsuccessful.

40.4.8 Configure CCM transmitting switch

Configure CCM sending switch for MEP. When CCM switch of MEP is disabled, disable MEP transmitting CCM. MEP default status is disabling transmitting CCM packets.

Step	Command	Description
1	config	Enter global configuration mode.
2	service CSIID level level	Enter service instance mode. CSIID: name of service instance, 1-13 bytes. level: level of maintenance domain, value in 0-7.
2	service cc {enable / disable} mep {{1-8191} all}	Enable/disable MEP transmitting CCM. enable: enable disable: disable {1-8191}: MEPID list, value in 1-8191. all: all of the configured MEP
3	exit	Return to Privileged EXEC mode.
4	show ethernet cfm local-mp [interface port <1-MAX_PORT_STR> level <0-7>]	Show MP configuration information of local maintenance domain.

Illustration: Enable MEP1 CCM transmitting switch in service instance ma3-1-4.

```
Raisecom#config
Raisecom(config)#ethernet cfm domain md3-1 level 3
Raisecom(config)#service ma3-1-4 vlan 4
Raisecom(config-service)#service cc enable mep 1
Raisecom(config-service)#exit
Raisecom(config)#exit
```

40.4.9 Configure CCM transmitting interval

By default, CCM transmitting interval in service instance is 10 seconds. If the service instance of the existence of CCM switch send by MEP enable, then configure and modify CC transmitting interval do not allowed.

Restoration the default values of CCM message transmitting interval in specified service instance: **no service cc interval**.

Step	Command	Description
1	config	Enter global configuration mode

2	service <i>CSIID</i> level <i>level</i>	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain, value in 0-7.
3	service cc interval {1 / 10 /60 /600}	Configure CCM transmitting interval for service instance. Unit: second
4	exit	Return to global configuration mode.
5	exit	Return to Privileged EXEC mode.
6	show ethernet cfm domain [level <0-7>]	Show configuration information of maintenance domain and service instance

Illustration: Set transmitting interval in service instance as 60 seconds

Raisecom#config

```
Raisecom(config)#ethernet cfm domain md3-1 level 3
Raisecom(config)#service ma3-1-4 vlan 4
Raisecom(config-service)#service cc interval 60
Raisecom(config- service)#exit
Raisecom(config)#exit
```

Note:

In order to prevent a large number of MEP inner service instance report CCM error fault at the same time as a result of modifications of CCM transmitting interval. Before configuring CCM transmitting interval in service instance, user needs to close CCM transmitting switch of MEP in the service instance, otherwise will lead to the failure of CCM transmitting interval configuration, we strongly recommended that before the revision of the CCM transmitting interval, shutdown CCM transmitting switch of all MEP in all the current network equipment, and then amend the CCM transmitting interval.

40.4.10 Configure CCM transmitting mode

CCM transmitting mode includes master mode and slave mode. By default, it is slave mode. This command is a global configuration command. For the device, all service instance transmits CCM packets according to configured mode. When it is configured in master mode, transmitting multicast CCM packet, the packet will take its own private TLV to denote the CCM packet is in master mode; when configured in slave mode, the device transmit multicast CCM packet in normal, but in below conditions it is special: when device receives CCM packets from remote is master mode, the device will transmit unicast CCM packet.

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet cfm mode (<i>slave/master</i>)	Configure mode for all service instance on device transmits CCM packets.

3	exit	Return to Privileged EXEC mode.
4	show ethernet cfm	Show local MD information.

Illustration: Set device as master transmitting mode.

Raisecom#**config**

Raisecom(config)#**ethernet cfm mode master**

Raisecom(config)#**exit**

Note: Since the master device mode is written mac address through acl, the configuration of master mode request for the device supporting acl.

40.4.11 Configure dynamic import function for remote learning

By default, service instance remote MEP learning dynamic import function is not effective.

This command is to transfer dynamic learned remote MEP to static remote MEP, namely, every time receiving CCM packets, automatic transfer the dynamic remote MEP to static remote.

Step	Command	Description
1	config	Enter global configuration mode
2	service CSIID level level	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain.
3	service remote mep learning active	Configure dynamic import function learned by remote MEP.
4	exit	Return to global configuration mode.

Illustration: Execute operation of importing remote mep dynamically.

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain md3-1 level 3**

Raisecom(config)#**service ma3-1-4 vlan 4**

Raisecom(config-service)#**service remote mep learning active**

Raisecom(config-service)#**exit**

Raisecom(config)#**exit**

40.4.12 Configure cc check function of remote MEP

By default, this function is disabled. When enabling this function, system check dynamic learnedremote MEP ID consistent with static remote MEP id once it receives CCM message, if inconsistent, the CCM message is considered incorrect.

Step	Command	Description
1	config	Enter global configuration mode
2	service CSIID level level	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain.
3	service remote-mep cc-check (enable / disable)	Configure cc check function learned by remote MEP.
4	exit	Return to global configuration mode.
5	show ethernet cfm domain [level <0-7>]	Show configuration of local maintenance domain and service instance.

Illustration: Execute cc check function of remote mep.

```
Raisecom#config
Raisecom(config)#ethernet cfm domain md3-1 level 3
Raisecom(config)#service ma3-1-4 vlan 4
Raisecom(config-service)#service remote-mep cc-check enable
Raisecom(config- service)#exit
Raisecom(config)#exit
```

40.4.13 Configure aging time for remote MEP

By default, the remote MEP aging time is 100 minutes.

Restore aging time to the default aging time by command of **no ethernet cfm remote mep age-time**.

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet cfm remote mep age-time minutes	Configure MEP aging time <i>minutes</i> : range in1-65535, unit: minute
3	exit	Return to Privileged EXEC mode.
4	show ethernet cfm	Show the global configuration information.

Illustration: Configure remote MEP aging time for 101 minutes.

```
Raisecom#config
Raisecom(config)# ethernet cfm remote mep age-time 101
Raisecom(config)#exit
```

40.4.14 Configure client VLAN for Y.1731 OAM message

Defaulted Y.1731 OAM message does not carry C-TAG, after configuring CVLAN for the service

instance, all CCM, LTM, LBM and DMM sent by MEP under service instance will use dual-TAG, C-TAG uses CVLAN.

Delete Client VLAN of Y.1731 OAM message: **no service cvlan**.

Step	Command	Description
1	config	Enter global configuration mode
2	service <i>CSIID</i> level <i>level</i>	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain
3	service cvlan <i>vlan</i>	Configure client vlan of OAM message <i>vlan</i> : client VLAN, range in 1-4094
3	exit	Return to global configuration mode.
4	exit	Return to Privileged EXEC mode.
5	show ethernet cfm domain	Show configuration information of maintenance domain and service instance.

Illustration: Set client VLAN for Y.1731 OAM message as 1001

```
Raisecom#config
```

```
Raisecom(config)#ethernet cfm domain md3-1 level 3
```

```
Raisecom(config)#service ma3-1-4 vlan 4
```

```
Raisecom(config-service)#service cvlan 1001
```

```
Raisecom(config-service)#exit
```

```
Raisecom(config)#exit
```

Note: When service instance has configured client VLAN, OAM packets of Y.1731 CCM, LTM, LBM, DMM use dual TAG, VLAN configured client VLAN in C-TAG; but for OAM packets in type of LBR, LTR, DMR, whether use dual TAG is consistent to LBM, LTM and DMM packets received by VLAN in C-TAG.

40.4.15 Configure priority for Y.1731 OAM message

Defaulted priority of Y.1731 OAM message is 6, after configuring OAM message priority, CCM, LBM, LTM, DMM sent by all MEP message in service instance use the specified priority.

Delete Client VLAN of Y.1731 OAM message: **no service priority**.

Step	Command	Description
1	config	Enter global configuration mode
2	service <i>CSIID</i> level <i>level</i>	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes.

		<i>level</i> : level of maintenance domain
3	service priority <i>priority</i>	Configure priority of OAM message <i>priority</i> : priority ,value 0-7
4	exit	Return to global configuration mode.
5	exit	Return to Privileged EXEC mode.
6	show ethernet cfm domain	Show configuration information of maintenance domain and service instance.

Illustration: Set the Priority of Y.1731 OAM Message as 2

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain md3-1 level 3**

Raisecom(config)#**service ma3-1-4 vlan 4**

Raisecom(config-service)#**service priority 2**

Raisecom(config-service)#**exit**

Raisecom(config)#**exit**

Note:

- Message types of OAM message in type CCM, LTM, LBM, DMM of Y.1731 use service instance to configure priority; but for OAM message in type LBR, LTR, and DMR the message priority is consistent with LBM, LTM, DMM message received.
- Please pay attention to trust configuration of port COS, this configuration impact on priority of the OAM message, and may modify the priority of OAM message.

40.4.16 Configure hold time for error CCM batabase

Error CCM database is used to save fault information reported by all MEP in the equipment each record of CCM error information record created time of the error message, use this command won't change the created time of error CCM messages. When the system configures new retention time will immediately check data in the database, if there is data beyond time will be immediately removed. By default, retention time of error CCM time in CC database is 100 minutes.

To restore the hold time of error CCM data: **no ethernet cfm error archive-hold-time**.

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet cfm error archive-hold-time <i>minutes</i>	Configure hold time of error CCM message <i>minutes</i> : retention time(min), range in 1-65535
3	exit	Return to Privileged EXEC mode.
4	show ethernet cfm	Show relative information of cfm

Illustration: Set the hold time of error CCM database as 50.

Raisecom#**config**

Raisecom(config)#**ethernet cfm error archive-hold-time 50**

Raisecom(config)#**exit**

40.4.17 Configure CFM fault alarm level

CC function of Y.1731 can detect fault in five levels, in accordance with the order of descending order: 5-cross-connect faults, 4-CCM error fault, 3-Remote MEP lost fault, 2-port state fault and 1-RDI fault.

Configure all to allow five types of alarm transmitting;

Configure macRemErrXcon allows transmitting four kinds of fault: cross-connect fault, CCM error fault, remote MEP lost fault, port state fault, namely transmitting alarms types 2-5;

Configure remErrXcon allows transmitting three kinds of fault: cross-connect fault, CCM error fault, remote MEP lost fault, namely transmitting alarms types 3-5;

Configure errXcon allows transmitting two kinds of fault: cross-connect fault, CCM error fault, namely transmitting alarms types 4-5;

Configure xcon allows transmitting one kind of fault: cross-connect fault, namely transmitting alarms type 5;

Configure none doesn't transmit any alarm.

Default state is macRemErrXcon.

Restoration types of the transmitting alarm: **no snmp-server cfm-trap**.

Step	Command	Description
1	config	Enter global configuration mode
2	service <i>CSIID</i> level <i>level</i>	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain.
3	snmp-server trap cfm {all/ <i>macRemErr</i> / <i>remErr</i> / <i>ccmErr</i> / <i>xcon</i> / <i>none</i>} <i>mep</i> {<i>mepid-list all</i>}	Configuration C-level fault alarm <i>all</i> : enable alarm all <i>macRemErr</i> : enable alarm of 2-5. <i>remErr</i> : enable alarm of 3-5. <i>ccmErr</i> : enable alarm of 4-5. <i>xcon</i> : enable alarm of level 5. <i>none</i> : alarm disable. <i>mepid-list</i> : meplist, range in 1-8191
4	exit	Return to Privileged EXEC mode.
5	show ethernet cfm local-mp	Show configuration information of local MP

Illustration: Set fault alarm level as all.

```
Raisecom(config-service)#snmp-server trap cfm all mep all
```

```
Raisecom(config-service)#exit
```

Note:

- When the MEP detect fault, before troubleshooting, fault detection of MEP at the same level or low-level will not be re-generated;
- When MEP detects a fault, after a post-10s of troubleshooting, fault can be removed.

40.4.18 Execute layer-2 ping operation (fault reset)

Before executing the command, you must make sure that Y.1731 global function switch is enabled, or the operation will fail.

Layer-2 ping function contains ping over service instance and over port two kinds, the two are of identical functional after configuration. If it is to do layer-2 PING to designated MEPID, Y.1731 needs to find destination MEP MAC address using MEPID, there are two ways provided:

One way: use MEP list, find remote MEP MAC address according to MEP ID, if static remote MEP is found while user has not configured remote MEP MAC address, then the search fails;

The other way: use remote MEP database, when source MEP finds remote MEP and is stable, it will save remote MEP data to remote MEP database in MEP, and find remote MEP MAC from remote MEP database according to MEPID;

By default LBM sending number is 5, default message TLV length is 64, one available source MEP will found automatically.

Step	Command	Description
1	config	Enter global configuration mode
2	service <i>CSIID</i> level <i>level</i>	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain.
3	ping {<i>HHHH.HHHH.HHHH</i> mep <i>rme pid</i> } [<i>count count</i>] [<i>size size</i>] [<i>source mepid</i>]	Execute layer-2 PING, used for fault reset <i>HHHH.HHHH.HHHH</i> : remote MP MAC address, unicast valid address. <i>rme pid</i> : remote MEP ID, range in 1-8191 <i>count</i> : transmitted LBM amount, range in 1-1024. <i>size</i> : data TLV length, range in 1-1484. <i>mepid</i> : source MEPID, range in 1-8191.
3	exit	Return to global configuration mode.
4	exit	Return to Privileged EXEC mode.

Illustration: ping service instance.

Raisecom#**config**

Raisecom(config)#**ethernet cfm enable**

Raisecom(config)#**ethernet cfm domain md-name md3-1 level 3**

Raisecom (config)#**service ma3-1-4 level 3**

Raisecom (config-service)#**ping 000E.5E03.5318 size 512**

Sending 5 ethernet cfm loopback messages to 000E.5E03.5318, timeout is 2.5 seconds:

!!!!!

Success rate is 100 percent (5/5).

Ping statistics from 000E.5E03.5318:

Received loopback replys: < 5/0/0 > (Total/Out of order/Error)

Ping successfully.

Raisecom (config-service)#**exit**

Ping over port:

Raisecom#**config**

Raisecom(config)#**interface port 1**

Raisecom (config-port)#**ethernet cfm ping 000E.5E03.5318 size 512**

Sending 5 ethernet cfm loopback messages to 000E.5E03.5318, timeout is 2.5 seconds:

!!!!!

Success rate is 100 percent (5/5).

Ping statistics from 000E.5E03.5318:

Received loopback replys: < 5/0/0 > (Total/Out of order/Error)

Ping successfully.

Raisecom (config-port)#**exit**

Note:

- If MEP is not configured in service instance, it will lead to PING failure because there is no source MEP;
- If the designated source MEP fails it will lead to PING failure, for illustration the designated source MEP does not exist or the designated MEP located Y.1731 function is disabled;
- If designated destination MEPID operates PING, it will fail because of the MAC address that can not find destination MEP according to MEPID;
- If other user is using designated source MEP to execute PING it may cause operation failure.

40.4.19 Execute layer-2 traceroute operation (fault isolation)

Before executing the command, you must make sure that Y.1731 global function is enabled, or it may cause execution failure.

When designating destination MEPID for layer-2 traceroute operation, Y.1731 needs to find

destination MEP MAC through MEPID, Y.1731 provides two ways:

Method 1: use MEP list to find remote MEP MAC address according to MEPID, if static remote MEP is found while static remote MEP MAC address is not configured by user, or the search fails;

Method 2: use remote MEP database to do the searching, when source find remote MEP and keeps steady, it will save remote MEP data to remote MEP database, and find remote MEP MAC according to MEPID from remote MEP database;

By default the original TTL of sending LTM is 64 and one available source MEP will be found.

Step	Command	Description
1	config	Enter global configuration mode
2	service CSIID level level	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : maintaining domain level
3	traceroute {HHHH.HHHH.HHHH mep rmepid} [ttl ttl] [source mepid]	Execute layer-2 TRACEROUTE function, used for fault isolation. <i>HHHH.HHHH.HHHH</i> : remote MP MAC address; <i>rmepid</i> : remote MEPID, range in 1-8191; <i>ttl</i> : original TTL, range is 1-255; <i>mepid</i> : source MEPID, range in 1-8191
3	exit	Return to global configuration mode.
4	exit	Return to Privileged EXEC mode.

Illustration:

```
Raisecom#config
```

```
Raisecom(config)#ethernet cfm enable
```

```
Raisecom(config)#ethernet cfm domain md-name md3-1 level 3
```

```
Raisecom (config)#service ma3-1-4 level 3
```

```
Raisecom (config-service)#traceroute 000E.5E03.5318 ttl 128
```

Show result:

```
TTL: <128>
```

```
Tracing the route to 000E.5E03.5318 on domain <md3-1>, level <3>, VLAN <4>.
```

```
Traceroute send via port <port-id>.
```

Hops	HostMAC	Ingress/EgressPort	IsForwarded	RelayAction	Nexthop
------	---------	--------------------	-------------	-------------	---------

<1>	<AAAA>	<8/1>	<yes>	<RlyFDB>	<AAAA>
<2>	<AAAA>	<2/3>	<yes>	<RlyFDB>	<BBBB>
!<3>	<BBBB>	<-/9>	<no>	<RlyHit>	<CCCC>

Note:

- If there is no configured MEP in service instance, it may lead to traceroute operation failure because source MEP is not found;
- If the designated source MEP is invalid it may lead to traceroute operation failure, for illustration, the designated source MEP does not exist or the port that the designated source MEP lays in is shut down;
- If the designated destination MEPID execute traceroute, if you can not find destination MEP MAC address according to MEPID, it may lead to operation failure;
- If CC function fails, by configuring static remote MEP and designate MAC address, layer-2 traceroute can be made sure available;
- If any other user traceroute the designated source MEP it may lead to operation failure.

40.4.20 Configure switch status for LT database

When the database LT switch is in the enabled state, traceroute information found by the agreement of database LT cache, you can keep track to command **show ethernet cfm traceroute cache**.

When the database LT switch is disabled, user can not see information of traceroute by command **show ethernet cfm traceroute-cache**

The switch is disabled by default.

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet cfm traceroute cache {enable/disable}	Configure switch status of database LT <i>enable</i> : enable <i>disable</i> : disable
3	exit	Return to privileged EXEC mode.
4	show ethernet cfm traceroute-cache	Show traceroute information.

Illustration: After enable database LT, user can view data information.

Raisecom#**config**

Raisecom(config)#**ethernet cfm traceroute cache enable**

Raisecom(config)#**exit**

Raisecom#**show ethernet cfm traceroute-cache**

Note: When database LT is closed, operation of 2-layer traceroute can still be carried out, but the traceroute results will be deleted automatically after the implementation of the traceroute.

40.4.21 Configure data holding time in LT database

When database LT switch is enabled, user can configure retention time of the database. When the LT database switch is enable, the default save time for 100 minutes; when the LT database switch is

disable, default to save time for 100 minutes.

Restore data retention time of database by default: **no ethernet cfm traceroute cache hold-time**.

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet cfm traceroute cache enable	Enable database LT switch
3	ethernet cfm traceroute cache hold-time <i>minutes</i>	Configure data hold time in LT database. <i>minutes</i> : hold time, unit is minutes, range in 1-65535.
4	exit	Return to Privileged EXEC mode
5	show ethernet cfm traceroute-cache	Show data information

Illustration: After the database enable, set holding time for data as 1000 minutes

Raisecom#**config**

Raisecom(config)#**ethernet cfm traceroute cache enable**

Raisecom(config)#**ethernet cfm traceroute cache hold-time 1000**

Raisecom(config)#**exit**

Raisecom(config)#**show ethernet cfm traceroute-cache**

40.4.22 Configure data entries can be stored in database LT

When the database LT switch enable, user can configure data entries can be stored in database LT. When the database LT switch is turned on, defaulted stored number is 100; when the database LT switch is closed, defaulted entries can be stored is 0.

Restore default values of entries can be stored in database: **no ethernet cfm traceroute cache size**.

Step	Command	Description
1	config	Enter global configuration mode.
2	ethernet cfm traceroute cache enable	Enable database LT.
3	ethernet cfm traceroute cache size <i>entries</i>	Configure entries can be stored <i>entries</i> : entries can be stored in database, range in 1-512.
4	exit	Return to global configuration mode.
5	show ethernet cfm traceroute-cache	Show data information.

Illustration: Set stored entries as 150 after enabling database LT.

Raisecom#**config**

Raisecom(config)#**ethernet cfm traceroute cache enable**

Raisecom(config)#**ethernet cfm traceroute cache size 150**

Raisecom(config)#exit

40.5 Monitoring and maintenance

Command	Description
show ethernet cfm traceroute-cache	Show traceroute discovery information of database LT
show ethernet cfm local-mp [interface port port-id level level]	Show configuration information of local MP, contains MEP and MIP
show ethernet cfm remote-mep [level level [service service-instance [mep mepid]]]	Show discovery information of remote MEP
show ethernet cfm errors [level level]	Show information of error CCM database
show ethernet cfm domain [level level]	Show configuration information of maintenance domain and service instance
show ethernet cfm mep level level service service-instance	Show MEP information in service instance
show ethernet cfm remote-mep static	Show static remote MEP information.
show ethernet cfm	Show global configuration information of Y.1731.
Show ethernet cfm performance-monitor throughput level level service service-instance	Show measurement result of last RFC2544
clear ethernet cfm traceroute-cache	Delete information of database LT
clear ethernet cfm remote-mep [level level [service service-instance [mpid mepid]]]	Delete specified information of remote MEP database
clear ethernet cfm errors [level level]	Delete specified information of remote MEP database

40.5.1 Show LT database traceroute information

Command format: show ethernet cfm traceroute-cache

Function: Display entries have been stored in the database LT and retention time, the name of the corresponding MD, rank and vlan associated service instances. It also can display initiation TTL of traceroute discovery, the transceived port of each hop LTM message, status of LTM message transmitting, method of LTM message transmitting as well as MAC address of the next hop the device. When the switch of the LT database is turned off, do not show discovery information of any traceroute.

Show results:

IC_A#show ethernet cfm traceroute-cache

The size of the linktrace database: 100 hold-time: 100

Tracing the route toCCCC on domain md1, level 3, VLAN 4.

Hops	HostMAC	Ingress/EgressPort	IsForwarded	RelayAction	NextHop
------	---------	--------------------	-------------	-------------	---------

1	AAAA	8/1	Yes	RlyFdb	BBBB
2	BBBB	2/3	Yes	RlyFdb	CCCC

!3	CCCC	-/9	No	RlyHit	CCCC
----	------	-----	----	--------	------

40.5.2 Show local MEP configuration information

Command format: show ethernet cfm local-mp [interface port *port-id* | level *level*]

Function: View configuration information of local MP, you can view the level of MIP corresponds to MD, the corresponding port ID and MAC address information, you can also view name of the MEP, the corresponding level of MD, port ID, direction of MEP sending, MAC address information, switching status of CCM message, entries have been transmitting and so on. User can choose to display MP on the specified port or MP of designated level.

Show results: The configuration of 3-level MEP, UP direction, shutdown of CCM transmitting, a number of messages have been transmitting as 0.

IC_B#show ethernet cfm mp local

Level	Type	Port	Mac Address
<hr/>			
5	MIP	2	BBBB
<hr/>			
<i>Mpid</i>	<i>MdName</i>	<i>Level</i>	<i>Vlan</i> <i>Type</i> <i>Port</i> <i>Mac Address</i> <i>CC-Status</i> <i>SendCCMs</i>
<hr/>			
1	md3-1	3	4 UP 2 BBBB Disable 0

40.5.3 Show discovery information of remote MEP

Command format: show ethernet cfm remote-mep [level *level* [service *service-instance* [mep *mepid*]]]

Function: View a remote MEP found by the local MP, show the level of MEP corresponds to MD, MAID, and MAC address information, MEPID, port status, MAC address information, switching state of CCM message, entries have been transmitting and so on. User can choose to display the remote MEP found in specified maintenance domain, the remote MEP found in the designated service instance or the remote MEP found by specified MEP

Showing results: Show MPID of remote MEP for 1, whereabouts of MD for md3, levels of 3, VLAN associated MA where remote MEP exist for 4, the port status is up, the MAC address of the remote MEP for CCCC, a local switch port ID receiving message for 1, a period of 9 seconds.

Maintenance Domain(MD) level:3

Maintenance Domain(MD) name: md3-1

<i>MPID</i>	<i>MD name</i>	<i>Level</i>	<i>VLAN</i>	<i>PortState</i>	<i>MAC</i>	<i>IngressPort</i>	<i>Age</i>
<hr/>							

Note: According to state machine defined of the agreement IEEE802.1ag, after MEP receiving remote MEP and the first CCM, it shows remote MEP discovery information, remote ME MAC address will be shown all FF. It will not get back to normal till MEP receives the second CCM message of remote MEP.

40.5.4 Show error CCM database information

Command Format: show ethernet cfm errors [level level]

Function: it used to view fault MD level, fault MA associated VLAN, MEPID of fault local MEP, MAC address of remote MEP related to fault, and meanwhile to view error type. User can choose to display error CCM information in assigned MD, error CCM information in assigned MD level.

Show result: Show error CCM information of level 1, fault associated vlan is 4, MPID of fault discover local MEP is 2, remote MAC address is CCCC, error type is ErrorCCM.

Raisecom#show ethernet cfm errors level 1

Level	VLAN	MPID	RemoteMEP MAC	ErrorType	AffectedService
1	4	2	CCCC	ErrorCCM	md1-ma4

40.5.5 Show configuration information of maintenance domain and service instance

Command format: show ethernet cfm domain [level level]

Function: it used to view the level of generated MD, VLAN associated corresponding MA, user can view transmitting interval of CCM message at the same time, as well as the remote MEP learning switch.

Showing results: it shows MD configured level of 3 named md3-1, as well as service instance named ma3-1-4 is associated with vlan 4, while equipped with 5-level MD called md5-1.

Raisecom#show ethernet cfm domain

Maintenance Domain(MD)							
Level:3	MD Name Format:Char	MD Name: md3-1					
Total services: 1							
Service	Format	PrimaryVlan	VlanNumber	C-vlan	Priority	CcmInterval	CC-Check
ma3-1-4	Char	4	1	1001	7	1	Enable

40.5.6 Show information of static remote MEP

Command format: show ethernet cfm remote-mep static

Function: To view static remote MEP information.

Show result: Show MD level 3, with empty name, MA named ma2 and static remote MEP list under MA is 5-9.

Raisecom#show ethernet cfm remote-mep static

Maintenance Domain(MD) level: 3
Maintenance Domain(MD) name:
Service Instance: ma3
Static remote MEP list: 5-9

40.5.7 Show global configuration information of Y.1731

Command format: show ethernet cfm

Function: Display the related configuration information of CFM, such as CFM protocol status in the global mode, the CFM status under the port, retention time of error CCM message and aging time of the remote MEP.

Show result: The global CFM protocol has been opened, the default CFM protocols on port, error retention time for 100, the default aging time of the remote MEP.

Raisecom#**show ethernet cfm**

Global cfm status: disable

Port cfm enabled portlist: 1-28

Archive hold time of error CCMs: 100(Min)

Remote mep aging time: 100(Min)

Device mode: Slave

40.5.8 Show the measurement results of previous RFC2544 throughput

Note: ISCOM2128EA-MA products don't support performance-monitor.

Command Format: show ethernet cfm performance-monitor throughput level <0-7> service CSIID

Function: Display measurement results information of previous RFC2544 throughput.

Show result:

RFC2544 throughput test information:

Throughput testing between MEP 100 in port 1 and remote mep 200:

Expected object: 3 Mbps

Packet length: 256

Rfc2544 throughput test result: succeeded

Far End throughput result:

<i>Local Send(bps)</i>	<i>Remote Recv(bps)</i>	<i>Local Send(pps)</i>	<i>Remote Recv(pps)</i>
------------------------	-------------------------	------------------------	-------------------------

<i>3,000,000</i>	<i>2,890,000</i>	<i>1700</i>	<i>1701</i>
------------------	------------------	-------------	-------------

Near End throughput result:

<i>Remote Send(bps)</i>	<i>Local Recv(bps)</i>	<i>Remote Send(pps)</i>	<i>Local Recv(pps)</i>
-------------------------	------------------------	-------------------------	------------------------

<i>3,000,000</i>	<i>2,960,000</i>	<i>1710</i>	<i>1708</i>
------------------	------------------	-------------	-------------

40.5.9 Clear information of database LT

Clear all the layer-2 traceroute information in database LT.

Step	Command	Description
1	config	Enter global configuration mode
2	clear ethernet cfm traceroute-cache	Clear information of LT database
4	exit	Return to Privileged EXEC mode.
5	show ethernet cfm traceroute-cache	Show data information

Illustration: Clear all information in LT database.

Raisecom#**config**

Raisecom(config)#**clear ethernet cfm traceroute-cache**

Raisecom(config)#**exit**

40.5.10 Clear information of remote MEP database

Clear specified information of remote MEP database.

Step	Command	Description
1	config	Enter global configuration mode
2	clear ethernet cfm remote-mep [level level [service service-instance [mpid mepid]]]	Clear information of remote MEP database <i>level</i> : level of maintenance domain, value in 0-7. <i>service-instance</i> : name in service instance length:1-13 bytes. <i>mepid</i> : local MEPID.
4	exit	Return to Privileged EXEC mode.
5	show ethernet cfm remote-mep	Show data information.

Illustration: Clear remote MEP information of 3-level maintenance domain.

Raisecom#**config**

Raisecom(config)#**clear ethernet cfm remote-mep level 3**

Raisecom(config)#**exit**

40.6 Typical configuration

Note: ISCOM2128EA-MAproducts don't support PM.

Topology structure:

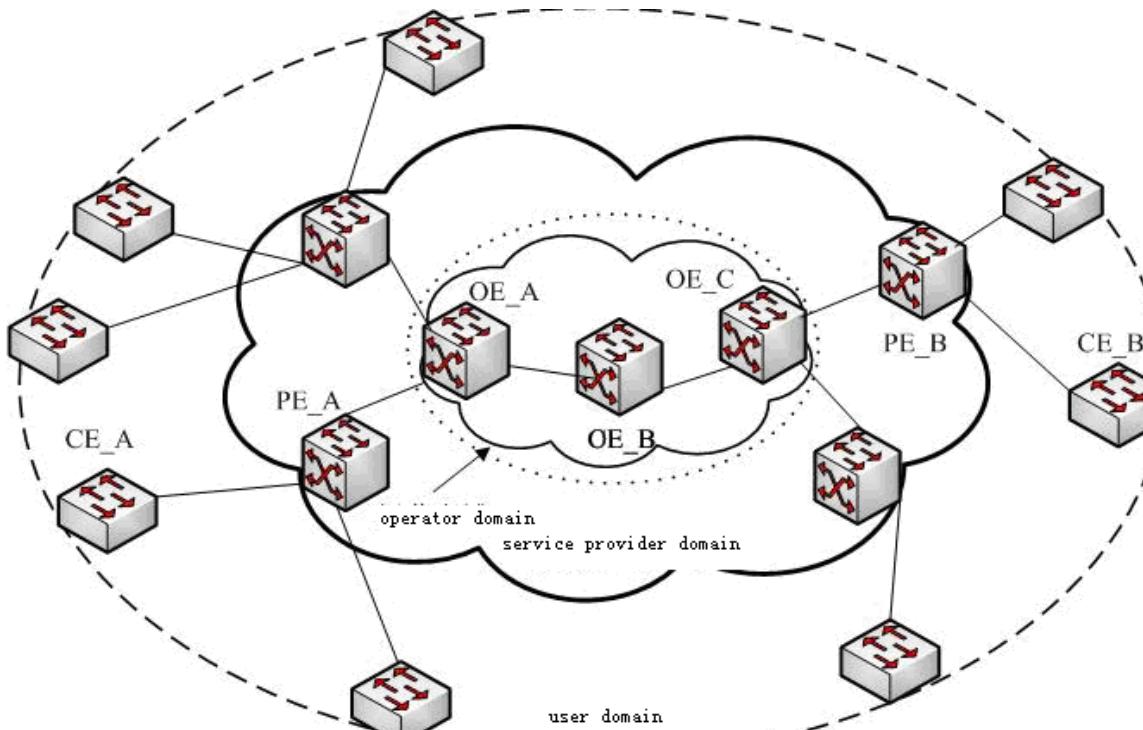


Figure 40-1

Metropolitan Area Network will be defined as user domain, service provider domain and operator domain. This three maintenance domain can be divided into three levels: respectively, level 5, level3 and level 1. As shown, CE_A connect to PE_A, PE_A connect to OE_A, OE_A connect to OE_C through OE_B, CE_B connect to PE_B, PE_B connect to OE_C. Configure 3-level MEP and 3-level MIP between PE_A and PE_B, configure 1-level MEP and 1-level MIP between OE_C and OE_A, and configure two 1-level MIP on OE_B. Specific configuration is as follows:

Configuration steps of PE_A:

```
Raisecom(config)#ethernet cfm domain level 3
Raisecom(config)#service ma3-1-4 level 3
Raisecom(config-service)#service vlan-list 100-105
Raisecom(config-service)#service cvlan 10
Raisecom(config-service)#service priority 4
Raisecom(config-service)#service mep up mpid 301 port 1
Raisecom(config-service)#service cc enable mep all
Raisecom(config-service)#service remote mep 302
Raisecom(config-service)#service performance-monitor delay object 20
Raisecom(config-service)#service performance-monitor delay-variation object 5
Raisecom(config-service)#service performance-monitor frame-loss-ratio rising-threshold 2
Raisecom(config-service)#service performance-monitor delay rising-threshold 2
Raisecom(config-service)#service performance-monitor delay-variation rising-threshold 2
```

```
Raisecom(config-service)#snmp-server trap performance-monitor enable  
Raisecom(config-service)#exit  
Raisecom(config)#interface port 1  
Raisecom(config-port)#switch access vlan 100  
Raisecom(config-port)#exit  
Raisecom(config)#interface port 2  
Raisecom(config-port)#switch mode trunk  
Raisecom(config-port)#exit  
Raisecom(config)#snmp-server cfm-trap all  
Raisecom(config)#ethernet cfm enable
```

Configuration steps of OE_A:

```
Raisecom(config)#ethernet cfm domain level 3  
Raisecom(config)#ethernet cfm domain md-name ma1-1 level 1  
Raisecom(config)#service ma1-1-100 level 1  
Raisecom(config-service)#service vlan-list 100-105  
Raisecom(config-service)#service mep up mpid 101 port 1  
Raisecom(config-service)#service cc enable mep all  
Raisecom(config-service)#service remote mep learning enable  
Raisecom(config-service)#exit  
Raisecom(config)#interface port 1  
Raisecom(config-port)#switch mode trunk  
Raisecom(config-port)#exit  
Raisecom(config)#interface port 2  
Raisecom(config-port)#switch mode trunk  
Raisecom(config-port)#exit  
Raisecom(config)#ethernet cfm enable
```

Configuration steps of OE_B:

```
Raisecom(config)#ethernet cfm domain md-name ma1-1 level 1  
Raisecom(config)#service ma1-1-100 level 1  
Raisecom(config-service)#service vlan-list 100-105  
Raisecom(config)#interface port 1  
Raisecom(config-port)#switch mode trunk
```

```
Raisecom(config-port)#exit  
Raisecom(config)#interface port 2  
Raisecom(config-port)#switch mode trunk  
Raisecom(config-port)#exit  
Raisecom(config)#ethernet cfm enable
```

Configuration steps of OE_C:

```
Raisecom(config)#ethernet cfm domain level 3  
Raisecom(config)#ethernet cfm domain md-name ma1-1 level 1  
Raisecom(config)#service ma1-1-100 level 1  
Raisecom(config-service)#service vlan-list 100-105  
Raisecom(config-service)#service mep up mpid 102 port 1  
Raisecom(config-service)#service cc enable mep all  
Raisecom(config-service)#service remote mep learning enable  
Raisecom(config-service)#exit  
Raisecom(config)#interface port 1  
Raisecom(config-port)#switch mode trunk  
Raisecom(config-port)#exit  
Raisecom(config)#interface port 2  
Raisecom(config-port)#switch mode trunk  
Raisecom(config-port)#exit  
Raisecom(config)#ethernet cfm enable
```

Configuration steps of PE_B:

```
Raisecom(config)#ethernet cfm domain md-name md5-1 level 5  
Raisecom(config)#ethernet cfm domain level 3  
Raisecom(config)#interface port 1  
Raisecom(config-port)#exit  
Raisecom(config)#service ma3-1-4 level 3  
Raisecom(config-service)#service vlan-list 100-105  
Raisecom(config-service)#service cvlan 10  
Raisecom(config-service)#service priority 4  
Raisecom(config-service)#service mep up mpid 302 port 1  
Raisecom(config-service)#service cc enable mep all
```

```

Raisecom(config-service)#service remote mep 301
Raisecom(config-service)#service performance-monitor delay object 20
Raisecom(config-service)#service performance-monitor delay-variation object 5
Raisecom(config-service)#service performance-monitor frame-loss-ratio rising-threshold 2
Raisecom(config-service)#service performance-monitor delay rising-threshold 2
Raisecom(config-service)#service performance-monitor delay-variation rising-threshold 2
Raisecom(config-service)#snmp-server trap performance-monitor enable
Raisecom(config-service)#exit
Raisecom(config)#interface port 1
Raisecom(config-port)#switch access vlan 100
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switch mode trunk
Raisecom(config-port)#exit
Raisecom(config)#snmp-server cfm-trap all
Raisecom(config)#ethernet cfm enable

```

Expression of CC function:

In PE_A, PE_B on, OE_A or OE_C:

By showing a command of remote MEP can display found remote MEP command;

By showing error CCM database can display an error message;

Reflection of LB function:

Suppose MAC address of PE_A is AAAA; MAC address of PE_B is BBBB; MAC address of OE_A is CCCC; MAC address of OE_B is DDDD; the MAC address of OE_C is EEEE.

After configuration of PE_A, OE_A, OE_B, OE_C, PE_B is completed, ping and traceroute MP equipment at the same level of MEP through MAC address on the device configured MEP

Ping its peer MEPID of MEP on PE_A

```
Raisecom(config)#service ma3-1-4 level 3
```

```
Raisecom(config-service)#ping mep 302 source 301
```

Sending 5 ethernet cfm loopback messages to BBBB, timeout is 2.5 seconds:

!!!!

Success rate is 100 percent (5/5).

Ping statistics from BBBB:

Received loopback replies: < 5/0/0 > (Total/Out of order/Error)

Ping successfully.

Ping the MAC of the peer MEP on PE_A:

Raisecom(config)#**service ma3-1-4 level 3**

Raisecom(config-service)#**ping BBBB source 301**

Sending 5 ethernet cfm loopback messages to BBBB, timeout is 2.5 seconds:

!!!!

Success rate is 100 percent (5/5).

Ping statistics from BBBB:

Received loopback replys: < 5/0/0 > (Total/Out of order/Error)

Ping successfully.

Reflection of LT function:

Traceroute its peer MEPID of MEP on PE_A:

Raisecom(config)#**service ma3-1-4 level 3**

Raisecom(config-service)#**traceroute mep 302 source 301**

TTL: <64>

Tracing the route to BBBB on domain -, level 3, VLAN 100.

Traceroute send via port <1>.

Hops HostMAC Ingress/EgressPort IsForwarded RelayAction NextHop

<i><1></i>	<i><AAAA></i>	<i><2/I></i>	<i><yes></i>	<i><RlyFDB></i>	<i><AAAA></i>
<i><2></i>	<i><AAAA></i>	<i><-/I></i>	<i><yes></i>	<i><RlyFDB></i>	<i><CCCC></i>
<i><3></i>	<i><CCCC></i>	<i><-/-></i>	<i><yes></i>	<i><RlyFDB></i>	<i><DDDD></i>
<i><4></i>	<i><DDDD></i>	<i><I/-></i>	<i><yes></i>	<i><RlyFDB></i>	<i><EEEE></i>
<i>!<5></i>	<i><EEEE></i>	<i><2/-></i>	<i><no></i>	<i><RlyHit></i>	<i><BBBB></i>

Traceroute its peer MAC of MEP on PE_A:

Raisecom(config)#**service ma3-1-4 level 3**

Raisecom(config-service)#**traceroute mep BBBB source 301**

TTL: <64>

Tracing the route to BBBB on domain -, level 3, VLAN 100.

Traceroute send via port <1>.

Hops HostMAC Ingress/EgressPort IsForwarded RelayAction NextHop

<i><1></i>	<i><AAAA></i>	<i><2/I></i>	<i><yes></i>	<i><RlyFDB></i>	<i><AAAA></i>
------------------	---------------------	--------------------	--------------------	-----------------------	---------------------

<2>	<AAAA>	<-/I>	<yes>	< RlyFDB >	<CCCC>
<3>	<CCCC>	<-/->	<yes>	< RlyFDB >	<DDDD>
<4>	<DDDD>	<I/->	<yes>	< RlyFDB >	<EEEE>
<5>	<EEEE>	<2/->	<no>	< RlyHit >	<BBBB>

Reflection of PM function:

In PE_A, PE_B:

By showing statistics command display statistical information of the current performance within 15 minutes, performance statistics in current 24-hour period, historical performance statistics within 15 minutes, statistical information, historical performance statistics 24 hours.

40.7 Appendix

Automatic configuration rules of MIP as follows, for each port, each vlan:

- Finding out matched MD
 - If the port is configured with MEP, suppose the highest level of all configured MEP is N, then the minimum level is the matching MD if there is MD level higher than N; or else, there is no matched MD.

Illustration: In case of a MA port is configured with two MEP, and associated four MD for this MA.

MEP1 level = 2, MEP2 level = 3;

MD1 level = 2, MD2 level = 3, MD3 level = 5, MD4 level = 6

Then, MD3 is the matched MD.

- If there is no MEP configured on port, configure MD of minimum level as matched MD.
- Processing according to MIP configuration rules
 - Create MIP under MD if only there is matched MD.

Chapter 41 SLA Configuration

This chapter is about how to configure SLA on switch, including:

- ❖ Overview of SLA
- ❖ Default configuration list of SLA
- ❖ configuration guide and limit of SLA
- ❖ configuration list and instruction of SLA
- ❖ Monitoring and maintenance of SLA
- ❖ Typical configuration illustration of SLA

41.1 SLA overview

SLA (Service Level Agreements) is a protocol between service provider and user, a contract between service provider and user on service quality, privilege and duty, it is also a telecom service evaluation standard.

Technologically, SLA is a real-time network performance detection and statistic technology, which is able to make statistics for response time, network jitter, delay, packet lose rate and so on. SLA is able to choose different work and monitor the related value according to different application.

41.1.1 SLA modules

➤ Task

Static concept, it is an end-to-end SLA network performance test task, including layer-2 network delay/jitter test (y1731-echo/y1731-jitter) and layer-3 network delay/jitter test (icmp-echo/icmp-jitter).

➤ Exploration

Dynamic concept, it is used to describe the process of an exploration message being sent and received in task test.

➤ Test

Dynamic concept, it is used to describe execution of a task. According to the definition of the task, one task test may contain several exploration (for Echo task, one test contains only one exploration).

➤ Schedule

Dynamic concept, it is used to describe a schedule of one task. A schedule may contain several seasonal test execution.

41.1.2 Basic function of SLA

SLA module is mainly used to measure network performance and take the result as the basic for user performance guarantee. Therefore, choosing two checking points (source and destination switch),

configure SLA on one and schedule to run it, then user can detect network performance between the two points.

The basic topology shows as below. If IC_A and IC_B is the same user located at different position, and user want to know the network performance between these two points. Then user configures SLA on IC_A with destination IC_B, to operate SLA performance test by scheduling and get statistic result.

The upper layer application software (NMS) can statistic data through SLA module, test out packets dropping ratio between IC_A and IC_B, bi-directional or uni-directional (SD/DS) delay, jitter, jitter variance, jitter distribution, etc. and then perform network performance analysis to get data user want to see.

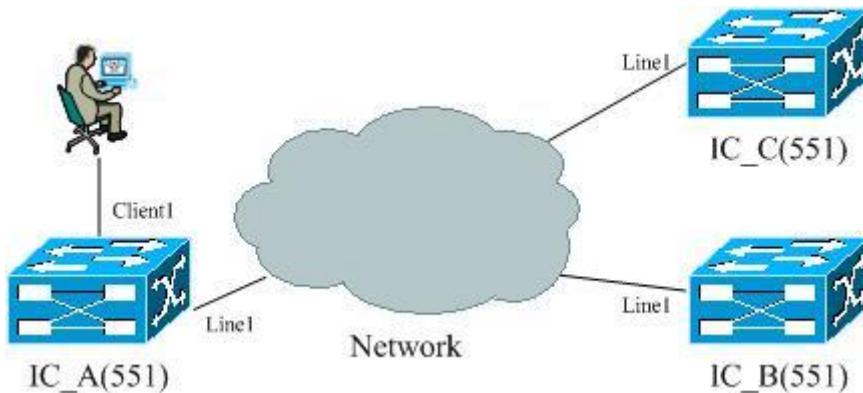


Figure 41-1 Application Topology of SLA

41.2 SLA default configuration list

No.	Attribute	Default value
1	SLA lay-2 service level	Service level is level 0 (the highest).
2	SLA jitter detecting time interval	Detecting interval is 1000ms.
3	SLA jitter detecting packets number	Detecting packets number is 5.
4	SLA schedule subsistence period.	Schedule period is forever (always in schedule status).
5	SLA schedule test period.	Test period is 20s.

41.3 SLA configuration guide and limit

- Layer-2 SLA operation schedule requires CFM environment (refer to CFM Configuration Guide for related description of CFM).
- It is suggested to set CFM packets transmitting interval in 1S to improve layer-2 operation executing accuracy. If transmitting interval is set long, it cannot reflect remote change in time and affect network performance detection.
- Max. Configuration items of sla operation is 100, after configuring the basic information of one operation (identified by operation ID), users cannot modify or configure it again. Delete the

operation before modifying basic information of it.

- Max. Concurrent schedule for sla operation is 10 pieces. One operation cannot be modified or schedule again before stopping it. User must wait the schedule to stop (reach schedule exist period or schedule halt) for the next time schedule.
- Statistic information of one operation is at most 5 groups. If it over 5 groups, the oldest statistic information (take the starting time of schedule as benchmark) will be got aging.

41.4 SLA configuration list and instruction

- Configure basic information for SLA operation
 - Configure SLA y1731-echo
 - Configure SLA y1731-jitter
 - Configure SLA icmp-echo
 - Configure SLA icmp-jitter
- Configure SLA schedule information and enable schedule

41.4.1 Configure SLA y1731-echo

Delete sla: **no sla oper-num.**

Steps	Commands	Description
1	config	Enter global configuration mode
2	sla oper-num y1731-echo remote-mep mep-id level level-id svlan vlan-id [cvlan vlan-id][cos cos-id]	Configure basic information for y1731-echo. <i>oper-num</i> : ID of sla operation, range in 1-65535. <i>mep-id</i> : remote mep, range in 1-8191. <i>level-id</i> : MD level, range in 0-7. <i>vlan-id</i> : vlan ID, range in 1- 4094. <i>cos-id</i> : service level, range in 0-7.
3	exit	Return to Privileged EXEC mode.
4	show sla {all oper-num } configuration	Show configuration information related to sla operation.

Illustration: Configure y1731-echo, operation ID is 2, remote mep is 2, MD level is 3, vlan id is 4, and service level is 1.

Raisecom#**config**

Raisecom (config) # **sla 2 y1731-echo remote-mep 2 level 3 svlan 4 cvlan 2 cos 1**

Raisecom (config) #**exit**

41.4.2 Configure SLA y1731-jitter

Delete sla: **no sla oper-num.**

Steps	Commands	Description
1	config	Enter global configuration mode
2	sla oper-num y1731-jitter remote-mep mep-id level level-id svlan vlan-id [cvlan vlan-id][interval interval-time] [packets packets-num] [cos cos-id]	Configure basic information for SLA y1731-jitter. <i>oper-num</i> : ID of sla operation, range in 1-65535. <i>mep-id</i> : remote mep, range in 1-8191. <i>vlan-id</i> : vlan ID, range in 1-4094. <i>interval-time</i> : detecting time interval, range in 1- 6000 ms. <i>packets-num</i> : detecting packets number, range in 1-20. <i>cos-id</i> : service level, range in 0-7.
3	exit	Return to Privileged EXEC mode.
4	show sla {all oper-num } configuration	Show configuration information related to sla operation.

Illustration: Configure y1731-jitter, operation ID is 2, remote mep is 2, MD level is 3, vlan id is 4, probe detecting interval is 10ms, detecting packets number is 10, and service level is 1.

Raisecom#**config**

```
Raisecom (config)# sla 2 y1731-jitter remote-mep 2 level 3 svlan 4 cvlan 2 interval 10 packets 10  
cos 1
```

Raisecom (config)#**exit**

41.4.3 Configure SLA icmp-echo

Delete sla: **no sla oper-num**.

Steps	Commands	Description
1	config	Enter global configuration mode
2	sla oper-num icmp-echo ip-address	Configure basic information for SLA icmp-echo. <i>oper-num</i> : operation ID of sla, range in 1-65535. <i>ip-address</i> : destination IP address, format in XXX.XXX.XXX.XXX.
3	exit	Return to Privileged EXEC mode.
4	show sla {all oper-num } configuration	Show configuration information related to sla operation.

Illustration: Configure icmp-echo, operation ID is 2, destination IP address is 20.0.0.20.

Raisecom#**config**

```
Raisecom (config)#sla 2 icmp-echo dest-ipaddr 20.0.0.20
```

Raisecom (config)#**exit**

41.4.4 Configure SLA icmp-jitter

Delete sla: **no sla oper-num.**

Steps	Commands	Description
1	config	Enter global configuration mode
2	sla oper-num icmp-jitter ip-address [interval interval-time] [packets packets-nums]	Configure basic information for SLA icmp-jitter. <i>oper-num</i> : operation ID of sla, range in 1-65535. <i>ip-address</i> : destination IP address, format in XXX.XXX.XXX.XXX. <i>interval-time</i> : detecting time interval, range in 1-60000 ms. <i>packets-nums</i> : detecting packets number, range in 1-20.
3	exit	Return to Privileged EXEC mode.
4	show sla {all oper-num } configuration	Show configuration information related to sla operation.

Illustration: Configure icmp-jitter, operation ID is 2, destination IP address is 20.0.0.20, detecting time interval is 10s, packets number is 5.

Raisecom#**config**

Raisecom (config) #**sla 2 icmp-jitter dest-ipaddr 20.0.0.20 interval 10 packets 5**

Raisecom (config) #**exit**

41.4.5 Configure SLA schedule information and enable schedule

Make sure the basic information has been configured when user performs sla operation schedule.

Use this command to stop sla operation schedule: **no sla schedule oper-num**.

There is no keyword begin in schedule command, which means immediate performing schedule operation and the command is not saved in auto-configuration loading.

Steps	Commands	Description
1	config	Enter global configuration mode
2	sla schedule oper-num [life {forever} life-time] [period period-time]	Configure information for SLA schedule and enable sla operation schedule. <i>oper-num</i> : operation ID of sla, range in 1-65535. forever : always in schedule state; <i>life-time</i> : schedule period, range in 1- 604800s. <i>period-time</i> : test period, range in 1-604800s.
3	exit	Return to Privileged EXEC mode.
4	show sla {all oper-num } result	Show test information of the latest operation.
5	show sla {all oper-num } statistic	Show statistic information of operation schedule.

Illustration: Schedule information of sla operation 2, life time is 20s, period time is 10s, enable schedule.

Raisecom#**config**

Raisecom (config) #**sla schedule 2 life 20 period 10**

Raisecom (config) #**exit**

NOTE:

- It is suggested to set CFM packet transmitting in interval of 1s to improve accuracy of layer-2 operation execution. The longer transmitting interval cannot reflect remote change in time and may affect network performance detection.

41.5 Monitoring and maintenance

Command	Description
show sla {all oper-num } configuration	Show configuration information related to operation.
show sla {all oper-num } result	Show the latest test information of operation.
show sla {all oper-num } statistic	Show statistic information of operation schedule.

41.5.1 Show configuration information related to operation

Command Format: **show sla {all | oper-num } configuration**

Function: to show basic configuration information of sla operation and schedule information.

Show result:

- 1). Configure icmp-jitter, operation ID is 2, destination IP address is 11.0.0.20, detecting time interval is 10s, packets number is 5. At present operation 2 doesn't enable schedule.

IC_A# **show sla 2 configuration**

Operation <2>:

Type: icmp jitter

StartTime:<0>

Destination Ip Address: 11.0.0.20

Jitter Interval(msec): 10

Frame Numbers: 5

Timeout(sec): 5

Schedule Life(sec): 0

Schedule Period(sec): 0

Schedule Status: Initial!

- 2). Configure y1731-echo, operation ID is 1, remote mep is 2, MD level is 3, vlan id is 4, service level is 0, at present operation has finished schedule.

IC_A# **show sla 1 configuration**

Operation <1>:

Type: cfm echo

StartTime: <146400>

<i>Cos:</i>	<i>0</i>
<i>Vlan ID:</i>	<i>4</i>
<i>MD Level:</i>	<i>3</i>
<i>Remote MEP ID:</i>	<i>2</i>
<i>Timeout(sec):</i>	<i>5</i>
<i>Schedule Life(sec):</i>	<i>20</i>
<i>Schedule Period(sec):</i>	<i>10</i>
<i>Schedule Status:</i>	<i>Completed!</i>

41.5.2 Show the latest test information of operation

Command Format: show sla {all | *oper-num*} result

Function:

- Showing as below for sla-echo (delay) operation:
 - Test successful or not;
 - Delay of this test.
- Showing as below for sla-jitter (jitter) operation:
 - Sending detection number;
 - Successful detection number in this test;
 - Packets dropping ratio in this test;
 - Max. delay of successful detection in this test (bi-directional/uni-directional SD/DS);
 - Min. delay of successful detection in this test (bi-directional/uni-directional SD/DS);
 - Sum of all successful detection delay in this test (bi-directional/uni-directional SD/DS);
 - Sum of all successful detection delay square in this test (bi-directional/uni-directional SD/DS);
 - Current dealy of successful detection in this test (bi-directional/uni-directional SD/DS);
 - Max. jitter of successful detection in this test (bi-directional/uni-directional SD/DS);
 - Min. jitter of successful detection in this test (bi-directional/uni-directional SD/DS);
 - Sum of all successful detection jitter in this test (bi-directional/uni-directional SD/DS);
 - Current jitter of successful detection in this test (bi-directional/uni-directional SD/DS).

Show result:

- 1). Configure icmp-jitter, operation ID is 2, destination IP address is 11.0.0.20, detection time interval is 10s, packets number is 5, operation 2 enable schedule, life time is 20s, test period is 10s.

IC_A# **show sla 2 result**

Operation <2>:

Schedule Status: *Active*

Number of Send Test: *19*

Number of Successful Test: *19*

Percent of Drop Pkts: *0.00000%*

Info of Latest Test : TWO-WAY ONE-WAY(SD) ONE-WAY(DS)

<i>Delay Min(usec)</i>	<i>:</i>	<i>463</i>	<i>232</i>	<i>232</i>
------------------------	----------	------------	------------	------------

<i>Delay Max(usec)</i>	:	489	245	245
<i>Delay Current(usec)</i>	:	477	239	239
<i>Delay Sum(usec)</i>	:	2386	1195	1195
<i>Jitter Min(usec)</i>	:	1	1	1
<i>Jitter Max(usec)</i>	:	18	9	9
<i>Jitter Current(usec)</i>	:	10	5	5
<i>Jitter Sum(usec)</i>	:	40	21	21

2). Configure y1731-echo, operation ID is 1, remote mep is 2, MD level is 3, vlan id is 4, service level is 0, operation 1 enable schedule, life time is 20s, test period is 10s.

IC_A# show sla 1 result

Operation <1>: Success!

Info of Latest Test : TWO-WAY ONE-WAY(SD) ONE-WAY(DS)

Current Delay(usec) : --- --- ---

41.5.3 Show statistic information of operation schedule

Command Format: **show sla {all | oper-num} statistic**

Function:

➤ Showing information as below for one schedule:

- Starting time
- Life time and schedule period
- Total amount of transmitted detection
- Total amount of successful detection
- Packets dropping percent
- Max. delay of successful detection (bi-directional/uni-directional SD/DS)
- Min. delay of successful detection (bi-directional/uni-directional SD/DS)
- Average delay of successful detection (bi-directional/ uni-directional SD/DS)

➤ Showing the below information also for SLA jitter operation:

- Sum of all successful detection delay (bi-directional/ uni-directional SD/DS)
- Sum of all successful detection delay square (bi-directional/ uni-directional SD/DS)
- Current delay of successful detection (bi-directional/ uni-directional SD/DS)
- Max. jitter of successful detection (bi-directional/ uni-directional SD/DS)
- Min. jitter of successful detection (bi-directional/ uni-directional SD/DS)
- Sum of all successful detection jitter (bi-directional/ uni-directional SD/DS)
- Average jitter of successful detection (bi-directional/ uni-directional SD/DS)

Show result:

1). Configure icmp-jitter, operation ID is 2, destination IP address is 11.0.0.20, detection time interval is 10s, packets amount is 5, operation 2 enable schedule, life time is 20s, test period is 10s, operation 2 has finished two schedules.

IC_A# show sla 2 statistic*Operation <2>:**StartTime <519330304>:*

Schedule Life(sec): 20

Schedule Period(sec): 10

Number of Send Test: 1700

Number of Successful Test: 1631

Percent of Drop Pkts: 4.06%

Statistic of Schedule: TWO-WAY ONE-WAY(SD) ONE-WAY(DS)

	:	457	228	228
Delay Min(usec)	:	1624	812	812
Delay Average(usec)	:	487	243	243
Delay Sum(usec)	:	85261	42667	42667
Jitter Min(usec)	:	1	< 1	< 1
Jitter Max(usec)	:	1147	573	573
Jitter Average(usec)	:	29	14	14
Jitter Sum(usec)	:	5173	2581	2581

*Operation <2>:**StartTime <519307376>:*

Schedule Life(sec): 20

Schedule Period(sec): 10

Number of Send Test: 10

Number of Successful Test: 10

Percent of Drop Pkts: 0.00%

Statistic of Schedule: TWO-WAY ONE-WAY(SD) ONE-WAY(DS)

Number of Successful Test :	10	10	10
Delay Min(usec) :	0	0	0
Delay Max(usec) :	1	0	1
Delay Average(usec) :	56	28	28
Delay Sum(usec) :	7	0	7
Jitter Min(usec) :	1	1	1
Jitter Max(usec) :	6	3	3
Jitter Average(usec) :	5	2	2
Jitter Sum(usec) :	8	4	4

2). Configure y1731-echo, operation ID is 1, remote mep is 2, MD level is 3, vlan id is 4, service level is 0, operation 1 enable schedule, life time is 20s, test period is 10s, operation 1 has finished 3 schedule.

IC_A# show sla 1 statistic

Operation <1>:

StartTime <519650608>:

Schedule Life(sec): 20

Schedule Period(sec): 10

Number of Send Test: 10

Number of Successful Test: 10

Percent of Drop Pkts: 0.00%

Statistic of Schedule: TWO-WAY ONE-WAY(SD) ONE-WAY(DS)

Delay Min(usec) : 0 0 0

Delay Max(usec) : 0 0 0

Delay Avreage(usec): 0 0 0

Operation <1>:

StartTime <519522992>:

Schedule Life(sec): 20

Schedule Period(sec): 10

Number of Send Test: 10

Number of Successful Test: 10

Percent of Drop Pkts: 0.00%

Statistic of Schedule: TWO-WAY ONE-WAY(SD) ONE-WAY(DS)

Delay Min(usec) : 0 0 0

Delay Max(usec) : 1 0 1

Delay Avreage(usec): 0 0 0

Operation <1>:

StartTime <146400>:

Schedule Life(sec): 20

Schedule Period(sec): 20

Number of Send Test: 10

Number of Successful Test: 10

Percent of Drop Pkts: 0.00%

Statistic of Schedule: TWO-WAY ONE-WAY(SD) ONE-WAY(DS)

<i>Number of Successful Test :</i>	1	1	1
<i>Delay Min(usec) :</i>	0	0	0
<i>Delay Max(usec) :</i>	0	0	0
<i>Delay Average(usec):</i>	0	0	0

41.6 Typical configuration applications

As figure shows below, MAC address of RC_A is 000e.5e03.451e, IP address is 11.0.0.10; IP address of RC_C is 11.0.0.20; MAC address of IC_B is 000E.5EE8.ED56.

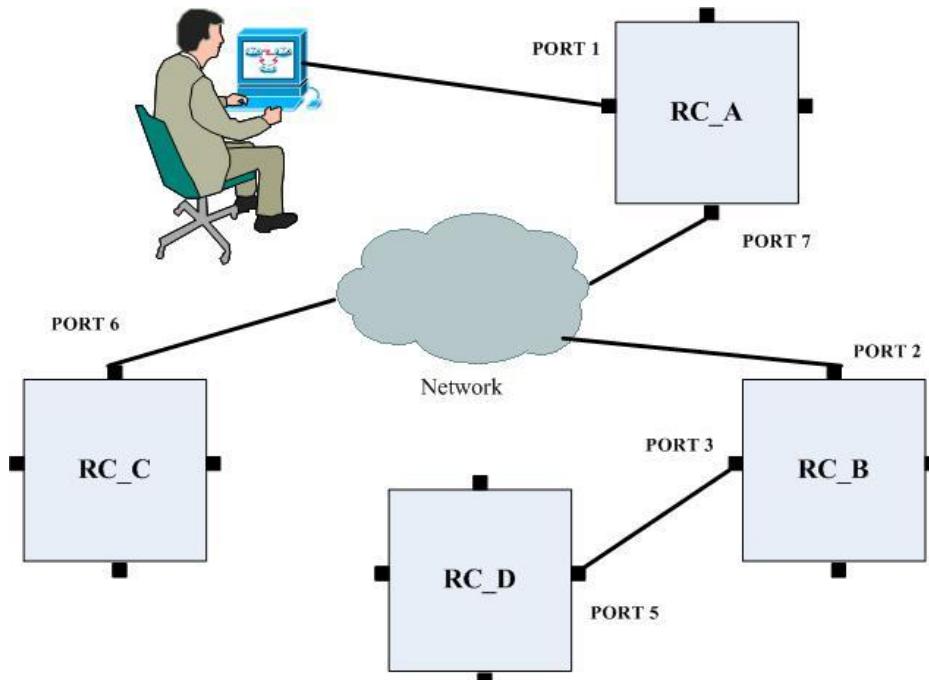


Figure 41-2

cfm configuration for RC_A as below:

Configure VLAN:

```
RC_A(config)# create vlan 4 active
```

Configure MD:

```
RC_A(config)# ethernet cfm domain md-name md5 level 5
RC_A(config)# ethernet cfm domain md-name md3 level 3
```

Configure service instance:

```
RC_A(config)# service ma4 level 3
```

Associating VLAN:

```
RC_A (config-service)# service vlan-list 4
```

Enable CC:

```
RC_A (config-service)# service cc enable
```

Set port mode:

```
RC_A(config)# interface port 7
RC_A (config-port)# switchport mode trunk
RC_A (config-port)# exit
```

Enable cfm:

```
RC_A(config)# ethernet cfm enable
```

cfm Configuration for RC_B as below:

Configure VLAN:

```
RC_B (config)# create vlan 4 active
```

Configure MD:

```
RC_B (config)# ethernet cfm domain md-name md5 level 5
RC_B (config)# ethernet cfm domain md-name md3 level 3
```

Configure service instance:

```
RC_B(config)# service ma4 level 3
```

Associating VLAN:

```
RC_B (config-service)# service vlan-list 4
```

Enable CC:

```
RC_B (config-service)# service cc enable
```

Configure MEP:

```
RC_B (config-service)# service mep up mpid 2 port 3
```

Set port mode:

```
RC_B(config)# interface port 2
RC_B (config-port)# switchport mode trunk
RC_B (config-port)# exit
RC_B(config)# interface port 3
RC_B (config-port)# switchport mode trunk
RC_B (config-port)# exit
```

Enable cfm:

```
RC_B(config)# ethernet cfm enable
```

- 1). RC_A switch performs layer-3 jitter test to RC_C switch, make sure network connection between RC_A and RC_C is OK (the two device can ping successfully). RC_A configures with icmp-jitter, operation ID is 2, destination IP address is 11.0.0.20 (RC_C IP address), detection time interval is 10s, packets number is 5, life time is 20s, and test period is 10s.

Configure IC_A as below:

RC_A#config

```
RC_A (config)# sla 2 icmp-jitter dest-ipaddr 11.0.0.20 interval 10 packets 5
```

```
RC_A (config)# sla schedule 2 life 20 period 10
```

```
RC_A (config)# exit
```

RC_A# show sla 2 configuration

Operation <2>:

Type: icmp jitter

StartTime:<519330304>

Destination Ip Address: 11.0.0.20

Jitter Interval(msec): 10

Frame Numbers: 5

Timeout(sec): 5

Schedule Life(sec): 20

Schedule Period(sec): 10

Schedule Status: Completed!

RC_A# show sla 2 result

Operation <2>:

Schedule Status: Active

Number of Send Test: 19

Number of Successful Test: 19

Percent of Drop Pkts: 0.00000%

Info of Latest Test : TWO-WAY ONE-WAY(SD) ONE-WAY(DS)

<i>Delay Min(usec) :</i>	<i>460</i>	<i>230</i>	<i>230</i>
--------------------------	------------	------------	------------

<i>Delay Max(usec) :</i>	<i>491</i>	<i>246</i>	<i>246</i>
--------------------------	------------	------------	------------

<i>Delay Current(usec) :</i>	<i>472</i>	<i>236</i>	<i>236</i>
------------------------------	------------	------------	------------

<i>Delay Sum(usec) :</i>	<i>2363</i>	<i>1183</i>	<i>1183</i>
--------------------------	-------------	-------------	-------------

<i>Jitter Min(usec) :</i>	<i>13</i>	<i>7</i>	<i>7</i>
---------------------------	-----------	----------	----------

<i>Jitter Max(usec) :</i>	<i>27</i>	<i>14</i>	<i>14</i>
---------------------------	-----------	-----------	-----------

<i>Jitter Current(usec) :</i>	<i>19</i>	<i>10</i>	<i>10</i>
-------------------------------	-----------	-----------	-----------

<i>Jitter Sum(usec) :</i>	<i>77</i>	<i>40</i>	<i>40</i>
---------------------------	-----------	-----------	-----------

RC_A# show sla 2 statistic

Operation <2>:

StartTime <519330304>:

Schedule Life(sec): 20

Schedule Period(sec): 10

Number of Send Test: 1700

Number of Successful Test: 1631

Percent of Drop Pkts: 4.05882%

<i>Statistic of Schedule: TWO-WAY</i>		<i>ONE-WAY(SD)</i>	<i>ONE-WAY(DS)</i>
<i>Delay Min(usec)</i>	:	453	227
<i>Delay Max(usec)</i>	:	4913	2457
<i>Delay Average(usec)</i>	:	508	254
<i>Delay Sum(usec)</i>	:	374054	187186
<i>Jitter Min(usec)</i>	:	2	1
<i>Jitter Max(usec)</i>	:	4429	2215
<i>Jitter Average(usec)</i>	:	62	31
<i>Jitter Sum(usec)</i>	:	45967	22986

2). RC_A switch performs layer-2 delay test to RC_B switch, make sure network connection between RC_A and RC_B is OK (the two device can ping successfully). RC_A configures with y1731-echo, operation ID is 1, remote mep is2, MD level is 3, vlan id is 4, service level is 0, life time is 20s, and test period is 10s.

Configure RC_A as below:

RC_A#config

RC_A (config)# **sla 2 y1731-echo remote-mep 2 level 3 vlan 4 cos 0**

RC_A (config)# **sla schedule 2 life 20 period 10**

RC_A (config)# **exit**

RC_A# show sla 1 configuration

Operation <1>:

Type: cfm echo

StartTime: <519522992>

<i>Cos:</i>	0
<i>Vlan ID:</i>	4
<i>MD Level:</i>	3
<i>Remote MEP ID:</i>	2
<i>Timeout(sec):</i>	5
<i>Schedule Life(sec):</i>	20
<i>Schedule Period(sec):</i>	10
<i>Schedule Status:</i>	<i>Completed!</i>

RC_A# show sla 1 result

Operation <1>: Success!

Info of Latest Test : TWO-WAY ONE-WAY(SD) ONE-WAY(DS)

<i>Current Delay(usec):</i>	466	233	233
-----------------------------	-----	-----	-----

RC_A# show sla 1 statistic

Operation <1>:

StartTime <519522992>:

Schedule Life(sec): 20

Schedule Period(sec): 10

Number of Send Test: 50

Number of Successful Test: 50

Percent of Drop Pkts: 0.00%

Statistic of Schedule: TWO-WAY ONE-WAY(SD) ONE-WAY(DS)

Delay Min(usec) : 452 226 226

Delay Max(usec) : 3426 1713 1713

Delay Average(usec) : 486 243 243

Chapter 42 LLDP Configuration

This chapter describes how to configure LLDP, include the following:

- ❖ Overview of LLDP
- ❖ default configuration list of LLDP
- ❖ configuration guide and limit of LLDP
- ❖ configuration list and item-by-item description of LLDP
- ❖ monitoring and maintenance of LLDP
- ❖ typical configuration illustration of LLDP

42.1 Overview of LLDP

LLDP is composed of IEEE 802.1AB definition of a link layer discovery protocol, network management system via the protocol rapid mastery of two layer network topology and its changes. LLDP local device sends information to directly connected neighbors; the neighbors to the information in the standard MIB preserve the form, for the NMS query and judgment of link status.

LLDP network topology diagram as shown in figure 42-1. In Figure 42-1, two adjacent switches S-switch-A and S-switch-B port is connected to the LLDP LLDPDU message, send each other; S-switch-A and S-switch-B received LLDPDU message, analytically obtained neighbor Tlv information, at the same time the record has been administrator query.

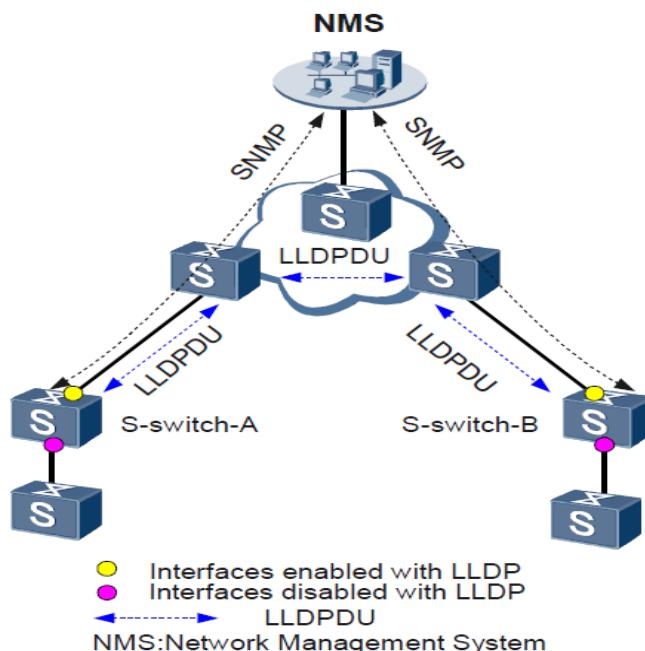


Figure 42-1 LLDP application environment network

42.2 LLDP default configuration list

No.	Attribute	Default value
1	LLDP global enable	Disable
2	LLDP port enable	Enable
3	Delay transmission timer	2s
4	Cycle transmission timer	30s
5	Aging coefficient	4s
6	Reset timer	2s
7	Alarm enable	Enable
8	Alarm notice timer	5s

42.3 Configuration constraints and limitations of LLDP

1. LLDP global enable then closed, it cannot enable immediately, and it must wait to restart the timer overtime to enable. Because the closure or enable that can send and receive packets register and unregister operation, when closed LLDP function, it will send protocol ShutDown message, the sending of all ports must be completed, and then cancel LLDP, namely there will be a delay after LLDP cancellation. If enabled LLDP again in the delay before the write-off, and cancellation in time delay cancellation, it will cause situation that the configuration does not match with the actual.
2. Configuration delay timer and timer, value of timer should be less than 0.25 times of the cycle timer value.

42.4 Configuration list and item-by-item description of LLDP

- Configure the LLDP function
 - Configure the LLDP global enable
 - Configure the LLDP port enable
 - Configure the LLDP delay timer
 - Configure the LLDP cycle of transmission timer
 - Configure LLDP aging coefficient
 - Configure the LLDP restart timer
- Configure the LLDP alarm correlation
 - Configure the LLDP alarm enable
 - Configure the LLDP alarm timer

42.4.1 Configure the LLDP global enable

Disable LLDP in global field: **lldp disable**

Step	Command	Description
1	config	Enter global configuration mode.
2	lldp enable	Enable global LLDP function.
3	exit	Return to privileged user mode.
4	show lldp local config	Show relatively configuration of LLDP.

Raisecom#**show lldp local config**

System configuration:

<i>LLDP enable status:</i>	<i>disable</i> (<i>default is disabled</i>)
<i>LLDP enable ports:</i>	<i>1-26</i>
<i>LldpMsgTxInterval:</i>	<i>30</i> (<i>default is 30s</i>)
<i>LldpMsgTxHoldMultiplier:</i>	<i>4</i> (<i>default is 4</i>)
<i>LldpReinitDelay:</i>	<i>2</i> (<i>default is 2s</i>)
<i>LldpTxDelay:</i>	<i>2</i> (<i>default is 2s</i>)
<i>LldpNotificationInterval:</i>	<i>5</i> (<i>default is 5s</i>)
<i>LldpNotificationEnable:</i>	<i>enable</i> (<i>default is enabled</i>)

Raisecom#**config**

Raisecom(config)#**lldp enable**

Raisecom(config)#**exit**

Raisecom#**show lldp local config**

System configuration:

<i>LLDP enable status:</i>	<i>enable</i> (<i>default is disabled</i>)
<i>LLDP enable ports:</i>	<i>1-26</i>
<i>LldpMsgTxInterval:</i>	<i>30</i> (<i>default is 30s</i>)
<i>LldpMsgTxHoldMultiplier:</i>	<i>4</i> (<i>default is 4</i>)
<i>LldpReinitDelay:</i>	<i>2</i> (<i>default is 2s</i>)
<i>LldpTxDelay:</i>	<i>2</i> (<i>default is 2s</i>)
<i>LldpNotificationInterval:</i>	<i>5</i> (<i>default is 5s</i>)
<i>LldpNotificationEnable:</i>	<i>enable</i> (<i>default is enabled</i>)

42.4.2 Configure LLDP port enable

Disable LLDP of port: **lldp disable**

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode.
2	interface port <portlist>	Enter interface mode.
3	lldp disable	Disable LLDP function of port.
4	exit	Return to global configuration mode.
5	exit	Return to privileged user mode.
6	show lldp local config	Show relatively configuration of LLDP.

Raisecom#**show lldp local config**

System configuration:

<i>LLDP enable status:</i>	<i>disable (default is disabled)</i>
<i>LLDP enable ports:</i>	<i>1-26</i>
<i>LldpMsgTxInterval:</i>	<i>30 (default is 30s)</i>
<i>LldpMsgTxHoldMultiplier:</i>	<i>4 (default is 4)</i>
<i>LldpReinitDelay:</i>	<i>2 (default is 2s)</i>
<i>LldpTxDelay:</i>	<i>2 (default is 2s)</i>
<i>LldpNotificationInterval:</i>	<i>5 (default is 5s)</i>
<i>LldpNotificationEnable:</i>	<i>enable (default is enabled)</i>

Raisecom#**config**

Raisecom#**interface port 4**

Raisecom(config-port)#**lldp disable**

Raisecom(config)#**exit**

Raisecom(config)#**exit**

Raisecom#**show lldp local config**

System configuration:

<i>LLDP enable status:</i>	<i>disable (default is disabled)</i>
<i>LLDP enable ports:</i>	<i>1-3, 5-26</i>
<i>LldpMsgTxInterval:</i>	<i>30 (default is 30s)</i>
<i>LldpMsgTxHoldMultiplier:</i>	<i>4 (default is 4)</i>
<i>LldpReinitDelay:</i>	<i>2 (default is 2s)</i>
<i>LldpTxDelay:</i>	<i>2 (default is 2s)</i>
<i>LldpNotificationInterval:</i>	<i>5 (default is 5s)</i>
<i>LldpNotificationEnable:</i>	<i>enable (default is enabled)</i>

42.4.3 Configure LLDP sending delay timer

Delete configuration of LLDP delay timer: **no lldp message-transmission delay**

Step	Command	Description
1	config	Enter global configuration mode.
2	lldp message-transmission delay <delay>	Configure value of message delay timer.
3	exit	Return to privileged user mode.
4	show lldp local config	Show relatively configuration of LLDP.

Raisecom#**show lldp local config**

System configuration:

<i>LLDP enable status:</i>	<i>disable (default is disabled)</i>
<i>LLDP enable ports:</i>	<i>1-26</i>
<i>LldpMsgTxInterval:</i>	<i>30 (default is 30s)</i>
<i>LldpMsgTxHoldMultiplier:</i>	<i>4 (default is 4)</i>
<i>LldpReinitDelay:</i>	<i>2 (default is 2s)</i>
<i>LldpTxDelay:</i>	<i>2 (default is 2s)</i>
<i>LldpNotificationInterval:</i>	<i>5 (default is 5s)</i>
<i>LldpNotificationEnable:</i>	<i>enable (default is enabled)</i>

Raisecom#**config**

Raisecom(config)#**lldp message-transmission delay 10**

*Message transmission delay(10 s) > 0.25 * Message transmission interval(30 s).*

Set unsuccessfully

Raisecom(config)#**lldp message-transmission delay 5**

Raisecom(config)#**exit**

Raisecom#**show lldp local config**

System configuration:

<i>LLDP enable status:</i>	<i>disable (default is disabled)</i>
<i>LLDP enable ports:</i>	<i>1-26</i>
<i>LldpMsgTxInterval:</i>	<i>30 (default is 30s)</i>
<i>LldpMsgTxHoldMultiplier:</i>	<i>4 (default is 4)</i>
<i>LldpReinitDelay:</i>	<i>2 (default is 2s)</i>
<i>LldpTxDelay:</i>	<i>5 (default is 2s)</i>
<i>LldpNotificationInterval:</i>	<i>5 (default is 5s)</i>
<i>LldpNotificationEnable:</i>	<i>enable (default is enabled)</i>

42.4.4 Configure LLDP aging coefficient

Delete configuration of LLDP aging coefficient: **no lldp message-transmission hold-multiplier**

Step	Command	Description
1	config	Enter global configuration mode.
2	lldp message-transmission hold-multiplier <hold-multiplier>	Configure value of message aging coefficient.
3	exit	Return to privileged user mode.
4	show lldp local config	Show relatively configuration of LLDP.

Raisecom#**show lldp local config**

System configuration:

```
-----
LLDP enable status: disable (default is disabled)
LLDP enable ports: 1-26
LldpMsgTxInterval: 30 (default is 30s)
LldpMsgTxHoldMultiplier: 4 (default is 4)
LldpReinitDelay: 2 (default is 2s)
LldpTxDelay: 2 (default is 2s)
LldpNotificationInterval: 5 (default is 5s)
LldpNotificationEnable: enable (default is enabled)
```

Raisecom#**config**

Raisecom(config)#**lldp message-transmission hold-multiplier 10**

Raisecom(config)#**exit**

Raisecom#**show lldp local config**

System configuration:

```
-----
LLDP enable status: disable (default is disabled)
LLDP enable ports: 1-26
LldpMsgTxInterval: 30 (default is 30s)
LldpMsgTxHoldMultiplier: 10 (default is 4)
LldpReinitDelay: 2 (default is 2s)
LldpTxDelay: 2 (default is 2s)
LldpNotificationInterval: 5 (default is 5s)
LldpNotificationEnable: enable (default is enabled)
```

42.4.5 Configure cycle transmission timer of LLDP

Delete configuration of LLDP cycle transmission timer: **no lldp message-transmission interval**

Step	Command	Description
1	config	Enter global configuration mode.
2	lldp message-transmission interval <interval>	Configure value of cycle sending timer.
3	exit	Return to privileged user mode.
4	show lldp local config	Show relatively configuration of LLDP.

Raisecom#**show lldp local config**

System configuration:

```
-----
LLDP enable status: disable (default is disabled)
LLDP enable ports: 1-26
LldpMsgTxInterval: 30 (default is 30s)
LldpMsgTxHoldMultiplier: 4 (default is 4)
LldpReinitDelay: 2 (default is 2s)
LldpTxDelay: 2 (default is 2s)
LldpNotificationInterval: 5 (default is 5s)
LldpNotificationEnable: enable (default is enabled)
```

Raisecom#**config**

Raisecom(config)#**lldp message-transmission interval 50**

Raisecom(config)#**exit**

Raisecom#**show lldp local config**

System configuration:

```
-----
LLDP enable status: disable (default is disabled)
LLDP enable ports: 1-26
LldpMsgTxInterval: 50 (default is 30s)
LldpMsgTxHoldMultiplier: 4 (default is 4)
LldpReinitDelay: 2 (default is 2s)
LldpTxDelay: 2 (default is 2s)
LldpNotificationInterval: 5 (default is 5s)
LldpNotificationEnable: enable (default is enabled)
```

42.4.6 Configure the LLDP alarm notification delay timer

Delete Configuration of the LLDP alarm notification delay timer: **no lldp trap-interval**

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode.
2	lldp trap-interval <interval>	Configure value of cycle sending timer.
3	exit	Return to privileged user mode.
4	show lldp local config	Show relatively configuration of LLDP.

Raisecom#**show lldp local config**

System configuration:

```
-----  
LLDP enable status: disable (default is disabled)  
LLDP enable ports: 1-26  
LldpMsgTxInterval: 30 (default is 30s)  
LldpMsgTxHoldMultiplier: 4 (default is 4)  
LldpReinitDelay: 2 (default is 2s)  
LldpTxDelay: 2 (default is 2s)  
LldpNotificationInterval: 5 (default is 5s)  
LldpNotificationEnable: enable (default is enabled)
```

Raisecom#**config**

Raisecom(config)#**lldp trap-interval 100**

Raisecom(config)#**exit**

Raisecom#**show lldp local config**

System configuration:

```
-----  
LLDP enable status: disable (default is disabled)  
LLDP enable ports: 1-26  
LldpMsgTxInterval: 30 (default is 30s)  
LldpMsgTxHoldMultiplier: 4 (default is 4)  
LldpReinitDelay: 2 (default is 2s)  
LldpTxDelay: 2 (default is 2s)  
LldpNotificationInterval: 100 (default is 5s)  
LldpNotificationEnable: enable (default is enabled)
```

42.4.7 Configure LLDP alarm enable

Disable LLDP alarm reporting function: **snmp-server lldp-trap disable**.

Step	Command	Description
1	config	Enter global configuration mode.

2	snmp-server lldp-trap enable	Enable alarm function of LLDP.
3	exit	Return to privileged user mode.
4	show lldp local config	Show relatively configuration of LLDP.

Raisecom#**show lldp local config**

System configuration:

<i>LLDP enable status:</i>	<i>disable (default is disabled)</i>
<i>LLDP enable ports:</i>	<i>1-26</i>
<i>LldpMsgTxInterval:</i>	<i>30 (default is 30s)</i>
<i>LldpMsgTxHoldMultiplier:</i>	<i>4 (default is 4)</i>
<i>LldpReinitDelay:</i>	<i>2 (default is 2s)</i>
<i>LldpTxDelay:</i>	<i>2 (default is 2s)</i>
<i>LldpNotificationInterval:</i>	<i>5 (default is 5s)</i>
<i>LldpNotificationEnable:</i>	<i>enable (default is enabled)</i>

Raisecom#**config**

Raisecom(config)# **snmp-server lldp-trap disable**

Raisecom(config)#**exit**

Raisecom#**show lldp local config**

System configuration:

<i>LLDP enable status:</i>	<i>disable (default is disabled)</i>
<i>LLDP enable ports:</i>	<i>1-26</i>
<i>LldpMsgTxInterval:</i>	<i>30 (default is 30s)</i>
<i>LldpMsgTxHoldMultiplier:</i>	<i>4 (default is 4)</i>
<i>LldpReinitDelay:</i>	<i>2 (default is 2s)</i>
<i>LldpTxDelay:</i>	<i>2 (default is 2s)</i>
<i>LldpNotificationInterval:</i>	<i>5 (default is 5s)</i>
<i>LldpNotificationEnable:</i>	<i>disable (default is enabled)</i>

42.5 Monitoring and maintenance

Command	Description
clear lldp statistic [port-list portlist]	Clear statistics of LLDP.
clear lldp remote-table [port-list portlist]	Clear neighbor information of LLDP.
show lldp local config	Show local configuration of LLDP.

show lldp local system-data [port-list portlist]	Show local LLDP system and port information.
show lldp remote [port-list portlist] [detail]	Show LLDP neighbor information of LLDP.
show lldp statistic [port-list portlist]	Show statistics of LLDP.

42.5.1 Clear statistics of LLDP

Command format: `clear lldp statistic [port-list portlist]`

Function: clear statistics of all ports or specific port.

Illustration:

- a) clear global statistical information, use the show to display statistical information of each port of the current system, and then clear the statistical information of the system and all the ports, and through the show query

Raisecom(config)#**show lldp statistic**

System remote table statistics:

Last change time: Mon Jan 25 13:13:31 2010

Inserts: 1 Deletes: 1

AgesOut: 0 Drops: 0

<i>Port</i>	<i>TxFrames</i>	<i>RxFrames</i>	<i>ErrFrames</i>	<i>DropFrames</i>	<i>UnknownTlvs</i>	<i>AgeoutFrames</i>
-------------	-----------------	-----------------	------------------	-------------------	--------------------	---------------------

<i>port1</i>	<i>6</i>	<i>7</i>	<i>4</i>	<i>4</i>	<i>2</i>	<i>1</i>
<i>port2</i>	<i>5</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port3</i>	<i>5</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port4</i>	<i>5</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port5</i>	<i>5</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>

...

Raisecom(config)#**clear lldp statistic**

Raisecom(config)#**show lldp statistic**

System remote table statistics:

Last change time: Thu Jan 01 08:00:00 1970

Inserts: 0 Deletes: 0

AgesOut: 0 Drops: 0

<i>Port</i>	<i>TxFrames</i>	<i>RxFrames</i>	<i>ErrFrames</i>	<i>DropFrames</i>	<i>UnknownTlvs</i>	<i>AgeoutFrames</i>
-------------	-----------------	-----------------	------------------	-------------------	--------------------	---------------------

<i>port1</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
--------------	----------	----------	----------	----------	----------	----------

<i>port2</i>	0	0	0	0	0	0
<i>port3</i>	0	0	0	0	0	0
<i>port4</i>	0	0	0	0	0	0
<i>port5</i>	0	0	0	0	0	0
...						

- b) Clear statistical information of specific port, use the show to display statistical information of specific port, and then clear the port specified statistical information, and through the show query.

Raisecom(config)#**show lldp statistic port-list 1**

System remote table statistics:

Last change time: Mon Jan 25 13:13:31 2010

Inserts: 1 *Deletes:* 1

AgesOut: 0 *Drops:* 0

<i>Port</i>	<i>TxFrames</i>	<i>RxFrames</i>	<i>ErrFrames</i>	<i>DropFrames</i>	<i>UnknownTlvs</i>	<i>AgeoutFrames</i>
-------------	-----------------	-----------------	------------------	-------------------	--------------------	---------------------

<i>port1</i>	33	7	4	4	2	1
--------------	----	---	---	---	---	---

Raisecom(config)#**clear lldp statistic port-list 1**

Raisecom(config)#**show lldp statistic port-list 1**

System remote table statistics:

Last change time: Mon Jan 25 13:13:31 2010

Inserts: 1 *Deletes:* 1

AgesOut: 0 *Drops:* 0

<i>Port</i>	<i>TxFrames</i>	<i>RxFrames</i>	<i>ErrFrames</i>	<i>DropFrames</i>	<i>UnknownTlvs</i>	<i>AgeoutFrames</i>
-------------	-----------------	-----------------	------------------	-------------------	--------------------	---------------------

<i>port1</i>	0	0	0	0	0	0
--------------	---	---	---	---	---	---

42.5.2 clear neighbor information of LLDP

Command format: **clear lldp remote [port-list *portlist*]**

clear lldp remote [line *portlist*]

clear lldp remote [client *portlist*]

Function: Clear neighbor information of all ports or specified ports.

Illustration:

- Clear neighbor information of all ports.

Raisecom(config)#**show lldp remote**

<i>Port</i>	<i>ChassisId</i>	<i>PortId</i>	<i>SysName</i>	<i>MgtAddress</i>	<i>ExpiredTime</i>
<i>port1</i>	<i>1b-d5-d0-8b-00-00</i>	<i>Fa0/1</i>	<i>sw1</i>	<i>192.168.217.14</i>	<i>105</i>
<i>port2</i>	<i>1b-d5-d0-8b-00-00</i>	<i>Fa0/1</i>	<i>sw1</i>	<i>192.168.217.14</i>	<i>114</i>

Raisecom(config)#**clear lldp remote**

Raisecom(config)#**show lldp remote**

<i>Port</i>	<i>ChassisId</i>	<i>PortId</i>	<i>SysName</i>	<i>MgtAddress</i>	<i>ExpiredTime</i>

- Clear neighbor information of specific port.

Raisecom(config)#**show lldp remote**

<i>Port</i>	<i>ChassisId</i>	<i>PortId</i>	<i>SysName</i>	<i>MgtAddress</i>	<i>ExpiredTime</i>
<i>port1</i>	<i>1b-d5-d0-8b-00-00</i>	<i>Fa0/1</i>	<i>sw1</i>	<i>192.168.217.14</i>	<i>104</i>
<i>port2</i>	<i>1b-d5-d0-8b-00-00</i>	<i>Fa0/1</i>	<i>sw1</i>	<i>192.168.217.14</i>	<i>110</i>
<i>port3</i>	<i>1b-d5-d0-8b-00-00</i>	<i>Fa0/1</i>	<i>sw1</i>	<i>192.168.217.14</i>	<i>116</i>

Raisecom(config)#**clear lldp remote port-list 1**

Raisecom(config)#**show lldp remote**

<i>Port</i>	<i>ChassisId</i>	<i>PortId</i>	<i>SysName</i>	<i>MgtAddress</i>	<i>ExpiredTime</i>
<i>port2</i>	<i>1b-d5-d0-8b-00-00</i>	<i>Fa0/1</i>	<i>sw1</i>	<i>192.168.217.14</i>	<i>110</i>

42.5.3 Show local configuration information

Command format: `show lldp local config`

Function:

- Content:
 - LLDP global enable state;
 - LLDP function enable port list;
 - LLDP transmission cycle timer value;
 - LLDP aging coefficient;
 - LLDP restart timer value;
 - LLDP send delay timer value;
 - LLDP notification alarm delay timer value;
 - LLDP notification alarms enable state.

Display results:

We have give illustration in the above configuration commands, so here we don't take more introductions.

42.5.4 Show local system and port information

Command format: **show lldp local system-data [port-list *portlist*]**

show lldp local system-data [line *portlist*]

show lldp local system-data [client *portlist*]

Function:

- Display content:
 - LLDP ID type frame;
 - LLDP ID box;
 - The LLDP system name;
 - LLDP system description;
 - LLDP system support ability;
 - LLDP system enables ability;
 - Each LLDP port ID subtype;
 - Each LLDP port ID;
 - Each LLDP port description.

Display results:

- 1) Show information of all ports.

Raisecom(config)#**show lldp local system-data**

System information:

<i>ChassisIdSubtype:</i>	<i>macAddress</i>
<i>ChassisId:</i>	<i>XXXX.XXXX.XXXX</i>
<i>SysName:</i>	<i>Raisecom</i>
<i>SysDesc:</i>	<i>ROS</i>
<i>SysCapSupported:</i>	<i>Repeater/Hub,Bridge/Switch</i>
<i>SysCapEnabled:</i>	<i>Repeater/Hub,Bridge/Switch</i>

<i>Port</i>	<i>SubType</i>	<i>PortID</i>	<i>Description</i>
<i>port1</i>	<i>ifName</i>	<i>port 1</i>	<i>Port1-FastEthernet</i>
<i>port2</i>	<i>ifName</i>	<i>port 2</i>	<i>Port2-FastEthernet</i>
<i>port3</i>	<i>ifName</i>	<i>port 3</i>	<i>Port3-FastEthernet</i>
<i>...</i>			

- 2) Show information of specific port.

Raisecom(config)#**show lldp local system-data port-list 1**

System information:

<i>ChassisIdSubtype:</i>	<i>macAddress</i>
<i>ChassisId:</i>	<i>XXXX.XXXX.XXXX</i>
<i>SysName:</i>	<i>Raisecom</i>
<i>SysDesc:</i>	<i>ROS</i>
<i>SysCapSupported:</i>	<i>Repeater/Hub,Bridge/Switch</i>

SysCapEnabled: Repeater/Hub,Bridge/Switch

<i>Port</i>	<i>SubType</i>	<i>PortID</i>	<i>Description</i>
<hr/>			
<i>port1</i>	<i>ifName</i>	<i>port 1</i>	<i>Port1 -FastEthernet</i>

42.5.5 show neighbor information

Command format: **show lldp remote [port-list portlist] [detail]**

show lldp remote [line portlist] [detail]

show lldp remote [client portlist] [detail]

Function:

- Abstract information display content:
 - LLDP neighbor frame ID;
 - LLDP neighbor port ID;
 - LLDP neighbor system name;
 - LLDP neighbor management address;
 - LLDP neighbor aged time.
 - Detailed information display content:
 - LLDP neighbors ID type frame;
 - LLDP ID neighbor frame;
 - LLDP neighbor port ID subtype;
 - LLDP neighbor port ID;
 - LLDP neighbor port description;
 - LLDP neighbor system name;
 - LLDP neighbor system description;
 - LLDP neighbor system support ability;
 - LLDP neighbor system enables the ability;
 - LLDP neighbor management address;
 - LLDP neighbor aged time.

Display results:

We have give illustration in the above configuration commands, so here we take simple introductions.

- 1) Show detailed information of neighbor of all ports

Raisecom(config)#**show lldp remote detail**

Port port1 has 1 remotes:

Remote1

<i>ChassisIdSubtype:</i>	<i>macAddress</i>
<i>ChassisId:</i>	<i>XXXX.XXXX.XXXX</i>
<i>PortIdSubtype:</i>	<i>ifName</i>
<i>PortId:</i>	<i>Fa0/1</i>
<i>PortDesc:</i>	<i>FastEthernet0/1</i>
<i>SysName:</i>	<i>sw1</i>

SysDesc: Cisco IOS Software, ME340x Software (ME340x-METROACC
ESSK9-M), Version 12.2(52)SE, RELEASE SOFTWARE (fc3)
Copyright (c) 1986-2009 by Cisco Systems, Inc. Compiled Fri 25-Sep-09 10:29 by sasyamal

SysCapSupported: Bridge/Switch,Router

SysCapEnabled: Bridge/Switch

Mgt address: 192.168.217.14

Expired time: 115(s)

Port port2 has 0 remotes:

Port port3 has 0 remotes:

...

- 2) Show detailed information of neighbor of specific port.

Raisecom(config)#**show lldp remote port-list 1 detail**

Port port1 has 1 remotes:

Remote1

ChassisIdSubtype: macAddress

ChassisId: XXXX.XXXX.XXXX

PortIdSubtype: ifName

PortId: Fa0/1

PortDesc: FastEthernet0/1

SysName: sw1

SysDesc: Cisco IOS Software, ME340x Software (ME340x-METROACC
ESSK9-M), Version 12.2(52)SE, RELEASE SOFTWARE (fc3)
Copyright (c) 1986-2009 by Cisco Systems, Inc. Compiled Fri 25-Sep-09 10:29 by sasyamal

SysCapSupported: Bridge/Switch,Router

SysCapEnabled: Bridge/Switch

Mgt address: 192.168.217.14

Expired time: 117(s)

42.5.6

Show statistics of system and ports

Command format: show lldp remote [port-list *portlist*] [detail]

show lldp remote [line *portlist*] [detail]

show lldp remote [client *portlist*] [detail]

Function:

- System statistics display content:
 - A recent neighbor change time;

- Insert the total number of neighbors;
 - The total statistics number of neighbor delete;
 - Total number of neighbors aging;
 - Total number of neighbors discarded.
- Port statistics:
- Send message number statistics;
 - Receiving the message number statistics;
 - Error statistics;
 - Discarded packets statistic;
 - Not recognizing message number statistics;
 - Statistics of aging message.

Display results:

We have give illustration in the above configuration commands, so here we take some simple introductions.

- 1) Show statistics of system and all ports.

Raisecom(config)#**show lldp statistic**

System remote table statistics:

Last change time: Mon Jan 25 14:49:43 2010

Inserts: 8 Deletes: 5

AgesOut: 5 Drops: 0

<i>Port</i>	<i>TxFrames</i>	<i>RxFrames</i>	<i>ErrFrames</i>	<i>DropFrames</i>	<i>UnknownTlvs</i>	<i>AgeoutFrames</i>
<i>port1</i>	<i>171</i>	<i>5</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port2</i>	<i>171</i>	<i>3</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port3</i>	<i>172</i>	<i>1</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port4</i>	<i>172</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port5</i>	<i>172</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port6</i>	<i>172</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port7</i>	<i>172</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
...						

<i>port1</i>	<i>171</i>	<i>5</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port2</i>	<i>171</i>	<i>3</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port3</i>	<i>172</i>	<i>1</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port4</i>	<i>172</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port5</i>	<i>172</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port6</i>	<i>172</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>
<i>port7</i>	<i>172</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>	<i>0</i>

...

- 2) Show statistics of system and specific ports.

Raisecom(config)# **show lldp statistic port-list 1**

System remote table statistics:

Last change time: Mon Jan 25 14:49:43 2010

Inserts: 8 Deletes: 5

AgesOut: 5 Drops: 0

<i>Port</i>	<i>TxFrames</i>	<i>RxFrames</i>	<i>ErrFrames</i>	<i>DropFrames</i>	<i>UnknownTlvs</i>	<i>AgeoutFrames</i>
<i>port1</i>	171	5	0	0	0	0

42.6

typical configuration illustration

Configure the LLDP function network as shown in Figure 42-2, at the same time setting data is prepared as follows:

- a) Management of the IP address of S-switch-A and S-switch-B are the 10.10.10.1 and 10.10.10.2, two IP addresses are set in the IP interface 1, binding in Vlan1024.
- b) Enable LLDP interface of S-switch-A and S-switch-B is port 1; port 1 are permitted access to Vlan 1024.
- c) Cycle of sending LLDP message is 60 seconds, the delay time is 9 seconds, changes in the LLDP alarm delay time of sending neighbor information is 10 seconds.

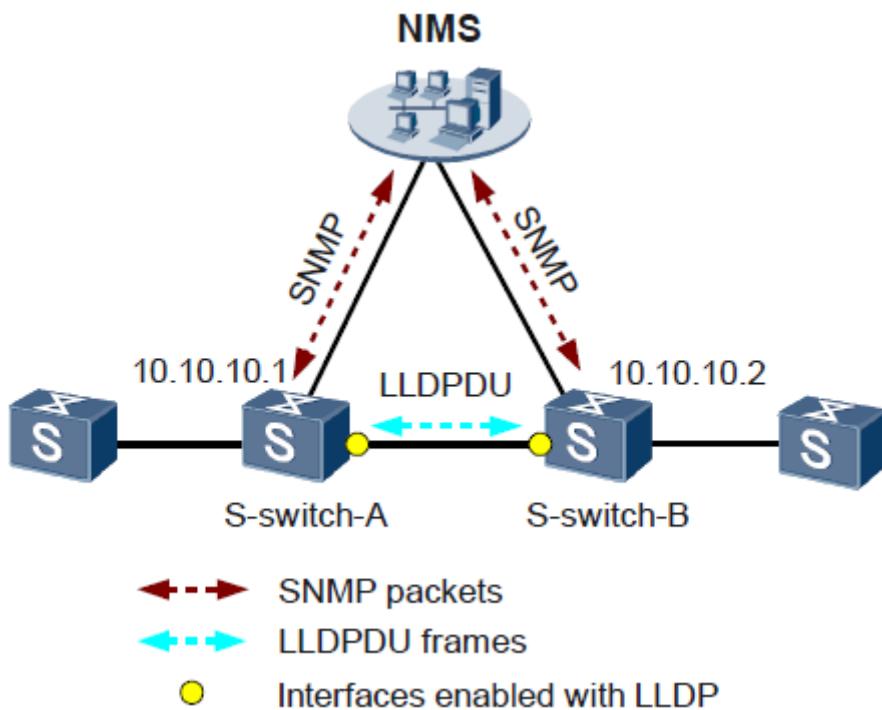


Figure 42-2 configure LLDP function network

Configuration method:

Use the following ideas to configure LLDP function:

1. Enable LLDP alarm of S-switch-A and S-switch-B.
2. Enable global LLDP function of S-switch-A and S-switch-B.
3. Configure S-switch-A and S-switch-B management of IP address for network management system.
4. Configure LLDP attribute of S-switch-A and S-switch-B.

Configure S-switch-A as follow:

1. Configure name of system:

```
Raisecom#hostname S-switch-A
```

2. Configure LLDP alarm:

```
S-switch-A (config)#snmp-server lldp-trap enable
```

3. Configure LLDP:

```
S-switch-A (config)# lldp enable
```

4. Configure management address IP:

```
S-switch-A (config)# create vlan 1024 active
```

```
S-switch-A(config)#interface port 1
```

```
S-switch-A(config-port)#switchport access vlan 1024
```

```
S-switch-A(config)#interface ip 1
```

```
S-switch-A(config-port)#ip address 10.10.10.1 1024
```

5. Configure LLDP attribute:

```
S-switch-A (config)# lldp message-transmission interval 60
```

```
S-switch-A (config)# lldp message-transmission delay 9
```

```
S-switch-A (config)# lldp trap-interval 10
```

6. Show local configuration:

```
S-switch-A (config)# show lldp local config
```

System configuration:

<i>LLDP enable status:</i>	<i>enable</i>	<i>(default is disabled)</i>
----------------------------	---------------	------------------------------

<i>LLDP enable ports:</i>	<i>1</i>
---------------------------	----------

<i>LldpMsgTxInterval:</i>	<i>60</i>	<i>(default is 30s)</i>
---------------------------	-----------	-------------------------

<i>LldpMsgTxHoldMultiplier:</i>	<i>4</i>	<i>(default is 4)</i>
---------------------------------	----------	-----------------------

<i>LldpReinitDelay:</i>	<i>2</i>	<i>(default is 2s)</i>
-------------------------	----------	------------------------

<i>LldpTxDelay:</i>	<i>9</i>	<i>(default is 2s)</i>
---------------------	----------	------------------------

<i>LldpNotificationInterval:</i>	<i>10</i>	<i>(default is 5s)</i>
----------------------------------	-----------	------------------------

<i>LldpNotificationEnable:</i>	<i>enable</i>	<i>(default is enabled)</i>
--------------------------------	---------------	-----------------------------

7. Show neighbor information:

```
S-switch-B (config)# show lldp remote
```

<i>Port</i>	<i>ChassisId</i>	<i>PortId</i>	<i>SysName</i>	<i>MgtAddress</i>	<i>ExpiredTime</i>
-------------	------------------	---------------	----------------	-------------------	--------------------

<i>port1</i>	<i>XXXX.XXXX.XXXX</i>	<i>Fa0/1</i>	<i>S-switch-B</i>	<i>10.10.10.2</i>	<i>106</i>
--------------	-----------------------	--------------	-------------------	-------------------	------------

...

Configuration of S-switch-B shown as follow:

1. Configure name of system:

```
Raisecom#hostname S-switch-B
```

2. Configure LLDP alarm

```
S-switch- B (config)#snmp-server lldp-trap enable
```

3. Configure LLDP:

```
S-switch- B (config)# lldp enable
```

4. Configure management address IP:

```
S-switch- B (config)# create vlan 1024 active
```

```
S-switch- B (config)#interface port 1
```

```
S-switch- B (config-port)#switchport access vlan 1024
```

```
S-switch- B (config)#interface ip 1
```

```
S-switch- B (config-port)#ip address 10.10.10.2 1024
```

5. Configure attribute of LLDP:

```
S-switch- B (config)# lldp message-transmission interval 60
```

```
S-switch- B (config)# lldp message-transmission delay 9
```

```
S-switch- B (config)# lldp trap-interval 10
```

6. Show local configuration:

```
S-switch- B (config)# show lldp local config
```

System configuration:

<i>LLDP enable status:</i>	<i>enable</i>	<i>(default is disabled)</i>
----------------------------	---------------	------------------------------

<i>LLDP enable ports:</i>	<i>1</i>
---------------------------	----------

<i>LldpMsgTxInterval:</i>	<i>60</i>	<i>(default is 30s)</i>
---------------------------	-----------	-------------------------

<i>LldpMsgTxHoldMultiplier:</i>	<i>4</i>	<i>(default is 4)</i>
---------------------------------	----------	-----------------------

<i>LldpReinitDelay:</i>	<i>2</i>	<i>(default is 2s)</i>
-------------------------	----------	------------------------

<i>LldpTxDelay:</i>	<i>9</i>	<i>(default is 2s)</i>
---------------------	----------	------------------------

<i>LldpNotificationInterval:</i>	<i>10</i>	<i>(default is 5s)</i>
----------------------------------	-----------	------------------------

<i>LldpNotificationEnable:</i>	<i>enable</i>	<i>(default is enabled)</i>
--------------------------------	---------------	-----------------------------

7. Show neighbor information:

```
S-switch- B (config)# show lldp remote
```

<i>Port</i>	<i>ChassisId</i>	<i>PortId</i>	<i>SysName</i>	<i>MgtAddress</i>	<i>ExpiredTime</i>
-------------	------------------	---------------	----------------	-------------------	--------------------

<i>port1</i>	<i>XXXX.XXXX.XXXX</i>	<i>Fa0/1</i>	<i>S-switch-A</i>	<i>10.10.10.1</i>	<i>104</i>
--------------	-----------------------	--------------	-------------------	-------------------	------------

...

Chapter 43 Port Backup Configuration Guide

This chapter describes how to configure backup, this function is used to switch on the port mutual backup.

This chapter includes the following contents:

- ❖ Port backup overview
- ❖ Port backup configuration
- ❖ Monitoring and maintenance
- ❖ Typical configuration illustration

43.1 Overview

This section includes the following contents:

- Port backup
- Based on the VLAN port backup

43.1.1 Switch port backup

Switch port backup is another solution to STP (Spanning Tree Protocol). User can keep basic link redundancy when STP is disabled. If the switch has enabled STP, there is no need to enable port backup, because STP has offered similar function.

Switch port backup group includes a pair of port, one is the main port, and the other one is backup port. If one is in Up state, the other one is in Standby state. Only one port can be in Up state at any time, and when there is link fault on the port, the one in Standby state will change to Up.

As is shown in the figure below, switch A and B connects with switch B and C respectively. If switch A port 1 and port 2 are the members of switch port backup group, then only one port is UP, the other one will be Standby. If port 1 is the main port, then port 1 will transmit messages with switch B, port 2(backup port) and switch C cannot transmit messages. If there is link fault between port 1 and switch B, then messages will be transmitted between port 2(backup port) and switch C. Then, after a short time (restore delay) when the link connected with port restores, port 1 will be Up, and port 2 will turn to Standby.

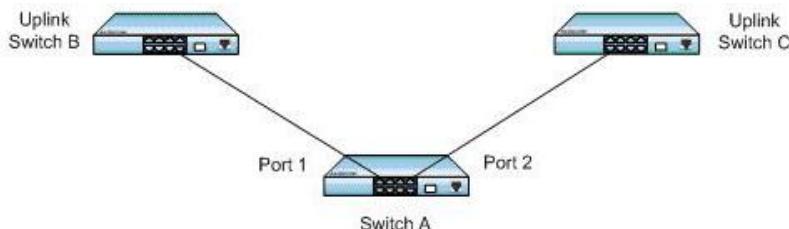


Figure 43-1 port backup configuration

If switching between the main port and backup port, switch will send a TRAP.

Members of port backup group support the physical port and link aggregation group and do not support the 3 layer interface.

43.1.2 port backup based on VLAN

Switch port backup based on VLAN realizes the communication between two ports in different VLAN.

As is shown in the figure above, if switch A is configured the main port on VLAN 1-100, switch B to backup port; on VLAN 101-200 port 2 is the main port, port 1 is the backup port. Then port 1 transmits flows on VLAN 1-100, while port 2 transmits flows on VLAN 101-200. In this way, switch port backup based on VLAN can be used on load balancing. At the same time, this application lays not on the configuration of upstream switches.

43.2 Configure port backup

This section includes the following contents

- Default configuration
- Configuration guide
- Configure backup

43.2.1 Default configuration

Function	Default value
Port backup group	None
Restore time	15s
Restore mode	Port link mode (port-up)

43.2.2 Configuration guide

- On the same VLAN, one port /link aggregation group cannot be the member of two switch port backup groups;
- In one switch port backup group, one port cannot be either main port and backup port;
- The main port and backup port of backup group can be physical port or link aggregation group. The members of switch port backup group can be two physical ports or two link aggregation groups, or one physical port added with one link aggregation group;
- If one link aggregation group is configured to the member of switch port backup group, then it is needed to configure the least member port of the link aggregation group to the member of switch port backup group.
- The port that has enabled STP cannot be configured port backup, while when configured switch port backup STP cannot be enabled.

43.2.3 Configure port backup

43.2.3.1 Configure port backup group

Step	Command	Description
1	config	Enter global configuration mode;
2	interface port <i>port_num</i>	Enter port configuration mode;
3	switchport backup port <i>portNum [vlanlist <i>vlanlist</i>]</i>	Configure <i>portNum</i> to backup port on <i>vlanlist</i> , <i>port_num</i> : main port;
4	show switch port backup	Show switch port backup configuration;

For illustration:

Raisecom#**config terminal**

Configuration mode, one command input per times. End with CTRL-Z.

CONFIG-I:Configured from console ...

Raisecom(config)# **interface port 3**

Raisecom(config-port)# **switch port backup port 5 vlanlist 1-100**

Raisecom(config-port)# **show switch port backup**

Restore delay: 15s

Restore mode: port-up

Active Port(State) Backup Port(State) Vlanlist

3 (Up) 5(Standby) 1-100

43.2.3.2 Configure restore delay

Step	Command	Description
1	config	Enter global configuration group.
2	switch port backup restore-delay <i>delay-time</i>	Configure restore delay time. <i>delay-time</i> : restore delay, range is 0-300s;
3	show switch port backup	Show port backup information.

For illustration:

Raisecom#**config terminal**

Configuration mode, one command input per times. End with CTRL-Z.

CONFIG-I:Configured from console ...

Raisecom(config)# **switch port backup restore-delay 35**

Raisecom(config)# **show switch port backup**

Restore delay: 35s

Restore mode: port-up

Active Port(State) Backup Port(State) Vlanlist

Note: To the backup group that is in restore state, it is useless to configure restore relay.

Illustration:

- When main port and backup port are in LINK_UP state, configure restore delay to 35s, when the main port turns to LINK_DOWN state and then LI NK_UP and keeps still for 35s, then the main port turn to Up state
- When main port and backup port are in LINK_UP state, and when the main port turn to LINK_DOWN state and turn to LINK_UP again, then configure the restore delay time to 35s in the latest configured restore delay time, then the configured value is invalid in this restore process to the port backup group (effective value is a recent configuration value).

43.2.3.3 Configure restore mode

Step	Command	Description
1	config	Enter global configuration mode
2	switchport backup restore-mode {port-up/neighbor-discover/disable }	Configure restore mode. <i>port-up</i> : port link mode, when port is Up the link is thought to be normal. <i>neighbor-discover</i> : neighbor discovery mode, port through RNDP(Raisecom Neighbor Discover Protocol). <i>disable</i> : disable backup recovery function.
3	show switch port backup	Show switch port backup information

For illustration:

Raisecom#**config terminal**

Configuration mode, one command input per times. End with CTRL-Z.

CONFIG-I:Configured from console ...

Raisecom(config)# **switchport backup restore-mode neighbor-discover**

Raisecom(config)# **show switchport backup**

Restore delay: 15s

Restore mode: neighbor-discover

Active Port(State) Backup Port(State) Vlanlist

Note: It is invalid to configure restore mode to the switch port backup group that is in restore state.

Illustration:

- When the main port and backup port are both in LINK_UP state, the configuration mode will be neighbor-discover, and when the main port turns to LINK_DOWN state, and uses RNDP (Raisecom Neighbor Discover Protocol) to discover neighbor and keeps restore delay, the main port will turn to Up.

- When both the main port and the backup port are in LINK_UP state, and when the main port turns to LINK_DOWN and LINK_UP, then configure restore mode to neighbor-discover in the restore delay time, the configured value is invalid to the restore process of the switch port backup group (effective value is a recent configuration value).

43.2.3.4 Configure force-switch

Step	Command	Description
1	config	Enter global configuration mode
2	switchport backup force-switch	Configure force-switch. Available on master port and specify the backup port in the command.
3	show switchport backup	Show switch port backup information

For illustration:

Raisecom#**config terminal**

Configuration mode, one command input per times. End with CTRL-Z.

CONFIG-I:Configured from console ...

Raisecom(config)# interface port X

Raisecom(config-port)# **switchport backup port Y force-switch**

Raisecom(config)# show switchport backup

Restore delay: 15s

Restore mode: neighbor-discover

Active Port(State) Backup Port(State) Vlanlist

Note: This command can force switch the data from main link to backup link, regardless of current link state.

Illustration:

- When the main port and backup port are both in LINK_UP state, the data is transmitting on main port. Then use force-switch command.
- After carry on the command **no switchport backup [port portnum] force-switch**, data transmission link will re-choose according to link state, selecting principle is: the up port first; main port is the priority if two up ports;

43.3 Monitoring and maintenance

We can use command **show switchport backup** to check backup of port.

Command	Description
show switchport backup	Show switch port backup information

Use **show switchport backup** to show the related state information of switch port backup, including restore delay, restore mode, switch port backup group information. Switch port backup information includes main port, backup port, main port state (Up/Down/Standy), backup port state

(Up/Down/Standy), VLAN list, as is shown below:

```
Raisecom#show switchport backup
```

Restore delay: 15s

Restore mode: port-up

Active Port(State)	Backup Port(State)	Vlanlist
3 (Up)	5(Standby)	1-100
6 (Down)	7(Up)	1-100

43.4 Typical configuration illustration

This section includes the following contents:

- Networking requirement
- Networking structure
- Configuration steps

43.4.1 Networking requirement

As is shown in the figure below, Switch A needs to support switch port back function, while Switch B, C and D need not.

To realize the stable connection between remote PC and the server, you need to configure:

Configure switch port backup group, and designate VLAN list.

43.4.2 Networking structure

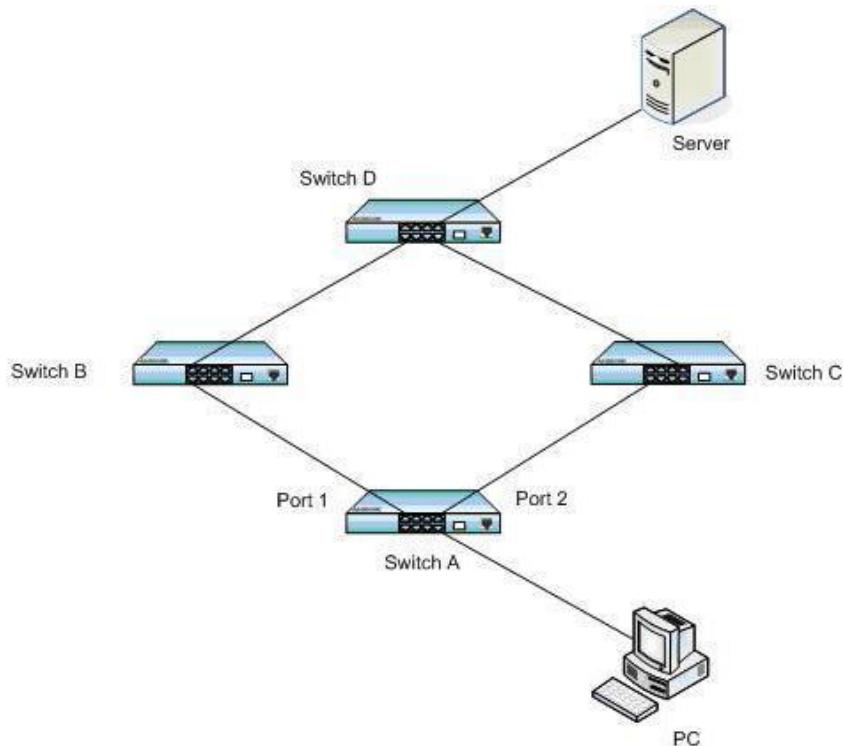


Figure 43-2

43.4.3 configuration steps

Enter port 1 configuration mode, and configure the main port to port 1, backup port to port 2 on VLAN 1-100:

Raisecom#**config terminal**

Configuration mode, one command input per times. End with CTRL-Z.

CONFIG-I:Configured from console ...

Raisecom(config)# **interface port 1**

Raisecom(config-port)# **switchport backup port 2 vlanlist 1-100**

Raisecom(config-port)# **exit**

Raisecom(config)#

Enter port 2 configuration mode, on VLAN 101-200, configure the main port to port 2, backup port to port 1:

Raisecom(config)# **interface port 2**

Raisecom(config-port)# **switchport backup port 1 vlanlist 101-200**

When both Port 1 and Port 2 is LINK_UP, port 1 will transmit flows on VLAN 1-100, while port 2 on will transmit flows on VLAN 101-200:

Raisecom(config-port)# **show switchport backup**

Restore delay: 15s

Restore mode: port-up

Active Port(State) Backup Port(State) Vlanlist

<i>Active Port(State)</i>	<i>Backup Port(State)</i>	<i>Vlanlist</i>
<i>1 (Up)</i>	<i>2(Standby)</i>	<i>1-100</i>
<i>2 (Standby)</i>	<i>1(Up)</i>	<i>101-200</i>

When port 1 turns to LINK_DOWN, port 2 will engage in transmitting the flows on VLAN 1-200:

Raisecom(config-port)# **show switchport backup**

Restore delay: 15s

Restore mode: port-up

Active Port(State) Backup Port(State) Vlanlist

<i>Active Port(State)</i>	<i>Backup Port(State)</i>	<i>Vlanlist</i>
<i>1 (Down)</i>	<i>2(Up)</i>	<i>1-100</i>
<i>2 (Up)</i>	<i>1(Down)</i>	<i>101-200</i>

When port 1 restore to normal LINK_UP and stays 15s restore delay), then port 1 will transmit flows

on VLAN 1-100, port 2 will transmit flows on VLAN 101-200.

Raisecom(config-port)# **show switchport backup**

Restore delay: 15s

Restore mode: port-up

Active Port(State) Backup Port(State) Vlanlist

<i>1 (Up)</i>	<i>2(Standby)</i>	<i>1-100</i>
<i>2 (Standby)</i>	<i>1(Up)</i>	<i>101-200</i>



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>