www.raisecom.com

ISCOM2600G (A) Series Configuration Guide (CLI) (Rel_11)

Raisecom Technology Co., Ltd. provides customers with comprehensive technical support and services. For any assistance, please contact our local office or company headquarters.

Website: http://www.raisecom.com

Tel: 8610-82883305

Fax: 8610-82883056

Email: export@raisecom.com

Address: Raisecom Building, No. 11, East Area, No. 10 Block, East Xibeiwang Road, Haidian District, Beijing, P.R.China

Postal code: 100094

Notice

Copyright ©**2020**

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.**

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

All other trademarks and trade names mentioned in this document are the property of their respective holders.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Preface

Objectives

This document describes features supported by the ISCOM2600G series switch, and related configurations, including basic configurations, basic principles and configuration procedures of Ethernet, ring network protection, PoE, reliability, security, and QoS, and related configuration examples.

The appendix lists terms, acronyms, and abbreviations involved in this document.

By reading this document, you can master principles and configurations of the ISCOM2600G series switch, and how to network with the ISCOM2600G series switch.

Versions

The following table lists the product versions related to this document.

Product name	Software version	Hardware version
ISCOM2600G series switch	V3.60M	A

Conventions

Symbol conventions

The symbols that may be found in this document are defined as below.

Symbol	Description
Warning	Indicate a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
Caution	Indicate a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.

Copyright © Raisecom Technology Co., Ltd.

Symbol	Description
Note	Provide additional information to emphasize or supplement important points of the main text.
Tip	Indicate a tip that may help you solve a problem or save time.

General conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Arial	Paragraphs in Warning, Caution, Notes, and Tip are in Arial.
Boldface	Buttons and navigation path are in **Boldface**.
Italic	Book titles are in *italics*.
`Lucida Console`	Terminal display is in `Lucida Console`.
Book Antiqua	Heading 1, Heading 2, Heading 3, and Block are in Book Antiqua.

Command conventions

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	The parameter before the & sign can be repeated 1 to n times.

Copyright © Raisecom Technology Co., Ltd.

Change history

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Issue 11 (2019-12-30)

Eleventh commercial release

- Upgraded the system software to V3.60M.
- Updated commands of 802.1x, RADIUS, TACACS+, user management, ND Snooping, and L2CP.

Issue 10 (2019-08-30)

Tenth commercial release

- Fixed known bugs.

Issue 09 (2019-04-30)

Ninth commercial release

- Upgraded the system software to V3.60.
- Added commands of ISF, IP Source Guard, DHCP Snooping, and L2CP.
- Upgraded commands of interface management, static route, interface loopback, QoS, and ACL.
- Upgraded configuration steps and added examples to configuration steps.
- Fixed known bugs.

Issue 08 (2018-11-15)

Eighth commercial release

- Upgraded commands for device login, 802.1x, static route, and MAC address.
- Fixed known bugs.

Issue 07 (2018-05-14)

Seventh commercial release

- Upgraded the software version to V3.50.
- Added zero-configuration, DHCPv6 Relay, and BFD.
- Updated commands of BootROM, interface management, QoS, DHCP, multicast, storm control, TACACS+, RADIUS, and SNMP.
- Fixed known bugs.

Issue 06 (2017-06-30)

Sixth commercial release

- Added RIP.

Copyright © Raisecom Technology Co., Ltd.

- Updated commands of time management, interface management, QinQ, VLAN mapping, QoS, DHCP, multicast, storm control, TACACS+, and RADIUS.
- Fixed known bugs.

Issue 05 (2016-11-15)

Fifth commercial release

- Upgraded software to V3.11.
- Added MRSTP, PVLAN, Voice VLAN, Smart PoE, and ARP attack protection.
- Updated management files, DHCP Server, OAM, and hardware monitoring.
- Fixed known bugs.

Issue 04 (2016-05-12)

Fourth commercial release

- Added descriptions of PoE.

Issue 03 (2015-11-30)

Third commercial release

- Upgraded the software version to V3.10.
- Fixed known bugs.

Issue 02 (2015-11-05)

Second commercial release

- Optimized the document.
- Fixed known bugs.

Issue 01 (2015-08-15)

Initial commercial release

Copyright © Raisecom Technology Co., Ltd.

Contents

1 Basic configurations 1
1.1 CLI 1
1.1.1 Introduction 1
1.1.2 Privileges 2
1.1.3 Modes 2
1.1.4 Shortcut keys 5
1.1.5 Acquiring help 6
1.1.6 Display information 8
1.1.7 Command history 9
1.1.8 Restoring default value of command line 10
1.1.9 Logging commands 10
1.2 Accessing device 11
1.2.1 Introduction 11
1.2.2 Accessing through Console interface 11
1.2.3 Accessing through Telnet 13
1.2.4 Accessing through SSH 15
1.2.5 Managing users 18
1.2.6 Configuring local password management 21
1.2.7 Configuring login through serial cable 22
1.2.8 Checking configurations 22
1.2.9 Maintenance 23
1.2.10 Example for configuring user management 23
1.2.11 Example for configuring SSH login 25
1.3 File management 28
1.3.1 Managing BootROM files 28
1.3.2 Managing system files 29
1.3.3 Managing configuration files 30
1.3.4 Checking configurations 35
1.3.5 Maintenance 35
1.4 Loading and upgrade 36
1.4.1 Introduction 36
1.4.2 Upgrading system software through BootROM 37

Copyright © Raisecom Technology Co., Ltd.

1.4.3 Upgrading system software through CLI 38
1.4.4 Checking configurations 39
1.5 Time management 39
1.5.1 Introduction 39
1.5.2 Preparing for configurations 42
1.5.3 Default configurations of time management 42
1.5.4 Configuring time and time zone 44
1.5.5 Configuring DST 44
1.5.6 Configuring NTP 45
1.5.7 Configuring SNTP 47
1.5.8 Checking configurations 48
1.5.9 Example for configuring NTP 48
1.6 Interface management 51
1.6.1 Introduction 51
1.6.2 Default configurations of interface management 52
1.6.3 Configuring basic attributes of interfaces 52
1.6.4 Configuring interface rate statistics 54
1.6.5 Configuring flow control on interfaces 55
1.6.6 Shutting down/Restarting interface 55
1.6.7 Configuring Combo interface 56
1.6.8 Configuring Console interface 56
1.6.9 Configuring VLAN interface 57
1.6.10 Configuring SNMP interface 57
1.6.11 Checking configurations 58
1.7 Configuring basic information 59
1.8 Task scheduling 60
1.8.1 Introduction 60
1.8.2 Configuring task scheduling 61
1.8.3 Checking configurations 62
1.9 Watchdog 62
1.9.1 Introduction 62
1.9.2 Preparing for configurations 62
1.9.3 Default configurations of Watchdog 62
1.9.4 Configuring Watchdog 62
1.9.5 Checking configurations 63
1.10 Configuring Banner 63
1.10.1 Preparing for configurations 63
1.10.2 Configuring Banner 63
1.10.3 Enabling Banner display 64
1.10.4 Checking configurations 64
2 Ethernet 65

Copyright © Raisecom Technology Co., Ltd.

2.1 MAC address table 65
2.1.1 Introduction 65
2.1.2 Preparing for configurations 67
2.1.3 Default configurations of MAC address table 68
2.1.4 Configuring static MAC address 68
2.1.5 Configuring blackhole MAC address 68
2.1.6 Filtering unknown multicast packets 69
2.1.7 Configuring MAC address learning 69
2.1.8 Configuring MAC address limit 70
2.1.9 Configuring aging time of MAC addresses 70
2.1.10 Enabling suppression of MAC address flapping 70
2.1.11 Checking configurations 71
2.1.12 Maintenance 71
2.1.13 Example for configuring MAC address table 72
2.2 VLAN 74
2.2.1 Introduction 74
2.2.2 Preparing for configurations 76
2.2.3 Default configurations of VLAN 77
2.2.4 Configuring VLAN attributes 77
2.2.5 Configuring interface mode 78
2.2.6 Configuring VLAN on Access interface 78
2.2.7 Configuring VLAN on Trunk interface 79
2.2.8 Configuring VLAN based on MAC address 81
2.2.9 Configuring VLAN based on IP subnet 82
2.2.10 Configuring VLAN based on protocol 83
2.2.11 Configuring VLAN filtering in egress direction 83
2.2.12 Checking configurations 84
2.2.13 Example for configuring VLAN 84
2.3 PVLAN 87
2.3.1 Introduction 87
2.3.2 Preparing for configuration 88
2.3.3 Default configurations of PVLAN 88
2.3.4 Configuring PVLAN type 88
2.3.5 Configuring PVLAN association 89
2.3.6 Configuring PVLAN mode on interface 89
2.3.7 Checking configuration 91
2.3.8 Example for configuring PVLAN 91
2.4 QinQ 94
2.4.1 Introduction 94
2.4.2 Preparing for configurations 95
2.4.3 Default configurations of QinQ 96
2.4.4 Configuring basic QinQ 96

Copyright © Raisecom Technology Co., Ltd.

2.4.5 Configuring selective QinQ 97
2.4.6 Configuring network-side interface to Trunk mode 99
2.4.7 Configuring TPID 99
2.4.8 Checking configurations 99
2.4.9 Example for configuring basic QinQ 100
2.4.10 Example for configuring selective QinQ 101
2.5 VLAN mapping 103
2.5.1 Introduction 103
2.5.2 Preparing for configurations 104
2.5.3 Default configurations of VLAN mapping 104
2.5.4 Configuring VLAN mapping 104
2.5.5 Checking configurations 105
2.5.6 Example for configuring VLAN mapping 106
2.6 STP/RSTP 108
2.6.1 Introduction 108
2.6.2 Preparation for configuration 111
2.6.3 Default configurations of STP 111
2.6.4 Enabling STP 112
2.6.5 Configuring STP parameters 112
2.6.6 Configuring edge interface 114
2.6.7 Configuring link type 115
2.6.8 Configuring BPDU filtering 116
2.6.9 Configuring BPDU Guard 116
2.6.10 Checking configurations 117
2.6.11 Example for configuring STP 117
2.7 MSTP 120
2.7.1 Introduction 120
2.7.2 Preparation for configuration 123
2.7.3 Default configurations of MSTP 123
2.7.4 Enabling MSTP 124
2.7.5 Configuring MST region and its maximum number of hops 125
2.7.6 Configuring root/backup bridge 126
2.7.7 Configuring interface priority and system priority 127
2.7.8 Configuring network diameter for switch network 128
2.7.9 Configuring internal path cost of interface 128
2.7.10 Configuring external path cost of interface 129
2.7.11 Configuring maximum transmission rate on interface 129
2.7.12 Configuring MSTP timer 130
2.7.13 Configuring edge interface 131
2.7.14 Configuring BPDU filtering 132
2.7.15 Configuring BPDU Guard 132
2.7.16 Configuring STP/RSTP/MSTP mode switching 133

Copyright © Raisecom Technology Co., Ltd.

2.7.17 Configuring link type 134
2.7.18 Configuring root interface protection 134
2.7.19 Configuring interface loopguard 135
2.7.20 Configuring TC packet suppression 136
2.7.21 Checking configurations 136
2.7.22 Maintenance 137
2.7.23 Example for configuring MSTP 137
2.8 Loop detection 142
2.8.1 Introduction 142
2.8.2 Preparing for configurations 143
2.8.3 Default configurations of loop detection 144
2.8.4 Configuring loop detection 144
2.8.5 Checking configurations 145
2.8.6 Maintenance 146
2.8.7 Example for configuring inner loop detection 146
2.9 Interface protection 148
2.9.1 Introduction 148
2.9.2 Preparing for configurations 148
2.9.3 Default configurations of interface protection 148
2.9.4 Configuring interface protection 148
2.9.5 Configuring interface isolation 149
2.9.6 Checking configurations 149
2.9.7 Example for configuring interface protection 149
2.10 Port mirroring 151
2.10.1 Introduction 151
2.10.2 Preparing for configurations 152
2.10.3 Default configurations of port mirroring 152
2.10.4 Configuring port mirroring on local port 152
2.10.5 Checking configurations 153
2.10.6 Example for configuring port mirroring 154
2.11 L2CP 155
2.11.1 Introduction 155
2.11.2 Preparing for configurations 155
2.11.3 Defaul configurations of L2CP 155
2.11.4 Configuring global L2CP 156
2.11.5 Configuring L2CP profile 156
2.11.6 Configuring L2CP profile on interface 158
2.11.7 Checking configurations 158
2.11.8 Maintenance 159
2.11.9 Example for configuring L2CP 159
2.12 Voice VLAN 162
2.12.1 Introduction 162

Copyright © Raisecom Technology Co., Ltd.

2.12.2 Preparing for configurations 163
2.12.3 Default configurations of voice VLAN 163
2.12.4 Configuring QoS of voice VLAN 164
2.12.5 Enabling voice VLAN 165
2.12.6 Configuring OUI address 166
2.12.7 Checking configurations 166
2.12.8 Example for adding interface to voice VLAN and configuring it to work in manual mode 166
2.12.9 Example for configuring IP phone to access voice VLAN packets through LLDP 168
2.13 GARP/GVRP 170
2.13.1 Introduction 170
2.13.2 Preparing for configurations 172
2.13.3 Default configurations of GARP 172
2.13.4 Configuring basic functions of GARP 173
2.13.5 Configuring GVRP 174
2.13.6 Checking configurations 174
2.13.7 Maintenance 175
2.13.8 Example for configuring GVRP 175
3 IP services 179
3.1 IP basis 179
3.1.1 Introduction 179
3.1.2 Preparing for configurations 179
3.1.3 Default configurations of Layer 3 interface 179
3.1.4 Configuring IPv4 adress of VLAN interface 180
3.1.5 Configuring IPv6 address of VLAN interface 180
3.1.6 Configuring basic attributes 181
3.1.7 Checking configurations 182
3.1.8 Example for configuring VLAN interface to interconnect with host 182
3.2 Loopback interface 184
3.2.1 Introduction 184
3.2.2 Preparing for configurations 184
3.2.3 Default configurations of loopback interface 184
3.2.4 Configuring IP address of loopback interface 184
3.2.5 Checking configurations 185
3.3 Interface loopback 185
3.3.1 Introduction 185
3.3.2 Preparing for configurations 186
3.3.3 Default configurations of interface loopback 186
3.3.4 Configuring interface loopback 186
3.3.5 Checking configurations 187
3.3.6 Maintenance 187
3.4 ARP 188

Copyright © Raisecom Technology Co., Ltd.

3.4.1 Introduction 188
3.4.2 Preparing for configurations 188
3.4.3 Default configurations of ARP 189
3.4.4 Configuring static ARP entries 189
3.4.5 Configuring dynamic ARP entries 189
3.4.6 Configuring proxy ARP 190
3.4.7 Checking configurations 191
3.4.8 Maintenance 191
3.4.9 Example for configuring ARP 191
3.5 NDP 193
3.5.1 Introduction 193
3.5.2 Preparing for configurations 193
3.5.3 Default configurations of NDP 194
3.5.4 Configuring static neighbor entries 194
3.5.5 Configuring aging time of dynamic NDPs 194
3.5.6 Configuring times of sending NS messages for detecting duplicated addresses 195
3.5.7 Configuring maximum number of NDPs allowed to be learnt 195
3.5.8 Checking configurations 196
3.5.9 Maintenance 196
3.6 Static route 196
3.6.1 Introduction 196
3.6.2 Preparing for configurations 197
3.6.3 Configuring static route 197
3.6.4 Configuring route mangement 199
3.6.5 Checking configurations 199
3.6.6 Example for configuring static route 200
3.7 Routing policy 202
3.7.1 Configuring IP prefix list 202
3.7.2 Configuring routing table 204
3.7.3 Checking configurations 207
3.7.4 Maintenance 207

4 PoE 209

4.1 Introduction 209
4.1.1 Principles of PoE 209
4.1.2 PoE modules 210
4.1.3 PoE advantages 210
4.1.4 PoE concepts 210
4.1.5 Smart PoE 211
4.2 Configuring PoE 211
4.2.1 Preparing for configurations 211
4.2.2 Default configurations of PoE 212

Copyright © Raisecom Technology Co., Ltd.

4.2.3 Enabling interface PoE 212
4.2.4 Configuring maximum output power of PoE 212
4.2.5 Configuring maximum output power of device 213
4.2.6 Configuring priority of PoE 213
4.2.7 Configuring PSE power utilization rate threshold 214
4.2.8 Configuring identification of non-standard PDs 214
4.2.9 Enabling forcible power supply on interface 214
4.2.10 Enabling overtemperature protection 215
4.2.11 Enabling global Trap 215
4.2.12 Checking configurations 215
4.3 Configuring Smart PoE 216
4.3.1 Preparing for configurations 216
4.3.2 Default configurations of PoE 216
4.3.3 Configuring PoE scheduling profile for interface 217
4.3.4 Configuring linktrace 217
4.3.5 Configuring PD active check 218
4.3.6 Checking configurations 219
4.4 Example for configuring PoE power supply 220
5 DHCP 223
5.1 DHCP Client 223
5.1.1 Introduction 223
5.1.2 Preparing for configurations 226
5.1.3 Default configurations of DHCP Client 226
5.1.4 Configuring DHCP Client 227
5.1.5 Configuring DHCPv6 Client 228
5.1.6 Checking configurations 228
5.1.7 Example for configuring DHCP Client 229
5.2 Zero-configuration 230
5.2.1 Introduction 230
5.2.2 Default configurations of zero-configuration 231
5.2.3 Preparing for configuration 231
5.2.4 Configuring DHCP Client 232
5.2.5 (Optional) configuring zero-configuration polling 232
5.2.6 Checking configurations 232
5.3 DHCP Snooping 233
5.3.1 Introduction 233
5.3.2 Preparing for configurations 234
5.3.3 Default configurations of DHCP Snooping 234
5.3.4 Configuring DHCP Snooping 234
5.3.5 Configure DHCP Snooping to support Option 82 236
5.3.6 Configuring DHCPv6 Snooping 236

Copyright © Raisecom Technology Co., Ltd.

5.3.7 Checking configurations 237
5.3.8 Maintenance 238
5.3.9 Example for configuring DHCP Snooping 238
5.4 DHCP Options 240
5.4.1 Introduction 240
5.4.2 Preparing for configurations 241
5.4.3 Default configurations of DHCP Option 242
5.4.4 Configuring DHCP Option field 242
5.4.5 Configuring DHCP Option 18 over IPv6 246
5.4.6 Configuring DHCP Option 37 over IPv6 247
5.4.7 Configuring user-defined DHCP Option over IPv6 248
5.4.8 Checking configurations 249
5.5 DHCP Server 250
5.5.1 Introduction 250
5.5.2 Preparing for configurations 252
5.5.3 Creating and configuring IPv4 address pool 253
5.5.4 Enabling DHCP Server on VLAN interface 254
5.5.5 (Optional) recycling IP address or adress pool 255
5.5.6 Configuring DHCP Server to support Option 82 255
5.5.7 Checking configurations 255
5.5.8 Maintenance 256
5.5.9 Example for configuring DHCPv4 Server 256
5.6 DHCP Relay 258
5.6.1 Introduction 258
5.6.2 Preparing for configurations 258
5.6.3 Default configurations of DHCP Relay 259
5.6.4 Configuring global DHCP Relay 259
5.6.5 Configuring DHCP Relay on VLAN interface 259
5.6.6 Configuring global DHCPv6 Relay 259
5.6.7 Configuring DHCPv6 Relay on VLAN interface 260
5.6.8 (Optional) configuring DHCP Relay to support Option 82 260
5.6.9 Checking configurations 261
5.6.10 Maintenance 261
5.6.11 Example for configuring DHCPv4 Relay 261

6 QoS 264

6.1 Introduction 264
6.1.1 Service model 264
6.1.2 Priority trust 265
6.1.3 Traffic classification 265
6.1.4 Traffic policy 267
6.1.5 Priority mapping 268

Copyright © Raisecom Technology Co., Ltd.

6.1.6 Queue scheduling 268
6.1.7 Congestion avoidance 270
6.1.8 Traffic shaping 271
6.1.9 Rate limiting based on interface and VLAN 271
6.1.10 QoS enhancement 271
6.2 Configuring priority 272
6.2.1 Preparing for configurations 272
6.2.2 Default configurations of basic QoS 272
6.2.3 Configuring types of priorities trusted by interface 273
6.2.4 Configuring mapping from CoS to local priority 274
6.2.5 Configuring mapping from DSCP to local priority and color 275
6.2.6 Configuring DSCP mutation 276
6.2.7 Configuring CoS remarking 276
6.2.8 Checking configurations 277
6.3 Configuring congestion management 278
6.3.1 Preparing for configurations 278
6.3.2 Default configurations of congestion management 278
6.3.3 Configuring SP queue scheduling 279
6.3.4 Configuring WRR or SP+WRR queue scheduling 279
6.3.5 Configuring DRR or SP+DRR queue scheduling 279
6.3.6 Configuring queue bandwidth guarantee 280
6.3.7 Checking configurations 280
6.4 Configuring congestion avoidance 281
6.4.1 Preparing for configurations 281
6.4.2 Default configurations of congestion avoidance 281
6.4.3 Configuring SRED 281
6.4.4 Checking configurations 282
6.5 Configuring traffic classification and traffic policy 282
6.5.1 Preparing for configurations 282
6.5.2 Default configurations of traffic classification and traffic policy 283
6.5.3 Creating traffic class 283
6.5.4 Configuring traffic classification rules 283
6.5.5 Creating rate limiting rule and shapping rule 285
6.5.6 Creating traffic policy 288
6.5.7 Defining traffic policy mapping 289
6.5.8 Defining traffic policy operation 289
6.5.9 Applying traffic policy to interfaces 291
6.5.10 Checking configurations 291
6.5.11 Maintenance 292
6.6 Configuring traffic shaping and rate limiting 292
6.6.1 Preparing for configurations 292
6.6.2 Configuring rate limiting based on interface 293

Copyright © Raisecom Technology Co., Ltd.

6.6.3 Configuring rate limiting based on VLAN 293
6.6.4 Configuring traffic shaping 294
6.6.5 Checking configurations 294
6.7 Bandwidth rate limiting 295
6.7.1 Introduction 295
6.7.2 Preparing for configurations 296
6.7.3 Default configurations of bandwidth rate limiting 296
6.7.4 Configuring bandwidth guarantee 296
6.7.5 Configuring hierarchical bandwidth guarantee 300
6.7.6 Checking configurations 303
6.8 Configuration examples 303
6.8.1 Example for configuring congestion management 303
6.8.2 Example for configuring rate limiting based on traffic policy 306
6.8.3 Example for configuring rate limiting based on interface 308

7 Multicast 311

7.1 Multicast 311
7.2 Basic functions of Layer 2 multicast 316
7.2.1 Introduction 316
7.2.2 Preparing for configurations 318
7.2.3 Default configurations of Layer 2 multicast basic functions 318
7.2.4 Configuring basic functions of Layer 2 multicast 318
7.2.5 Checking configurations 319
7.2.6 Maintenance 320
7.3 IGMP Snooping 320
7.3.1 Introduction 320
7.3.2 Preparing for configurations 321
7.3.3 Default configurations of IGMP Snooping 321
7.3.4 Configuring IGMP Snooping 322
7.3.5 Checking configurations 323
7.3.6 Example for applying multicast on ring network 323
7.4 IGMP Querier 326
7.4.1 Introduction 326
7.4.2 Preparing for configurations 327
7.4.3 Default configurations of IGMP Querier 327
7.4.4 Configuring IGMP Querier 328
7.4.5 Checking configurations 329
7.4.6 Example for configuring IGMP Snooping and IGMP Querier 329
7.5 IGMP MVR 331
7.5.1 Introduction 331
7.5.2 Preparing for configurations 332
7.5.3 Default configurations of IGMP MVR 333

Copyright © Raisecom Technology Co., Ltd.

7.5.4 Configuring IGMP MVR 333
7.5.5 Checking configurations 334
7.5.6 Example for configuring IGMP MVR 335
7.6 IGMP filtering 337
7.6.1 Introduction 337
7.6.2 Preparing for configurations 337
7.6.3 Default configurations of IGMP filtering 338
7.6.4 Enabling global IGMP filtering 338
7.6.5 Configuring IGMP filtering profile 338
7.6.6 Configuring maximum number of multicast groups 340
7.6.7 Checking configurations 342
7.6.8 Example for applying IGMP filtering on interface 343
7.7 Multicast VLAN copy 345
7.7.1 Introduction 345
7.7.2 Preparing for configurations 347
7.7.3 Default configurations of multicast VLAN copy 347
7.7.4 Configuring multicast VLAN copy 348
7.7.5 Configuring static multicast members of VLAN copy 349
7.7.6 Configuring customer VLAN of VLAN copy 349
7.7.7 Configuring host joining function of VLAN copy 350
7.7.8 Checking configurations 350

8 OAM 352

8.1 Introduction 352
8.2 EFM 354
8.2.1 Introduction 354
8.2.2 Preparing for configurations 354
8.2.3 Default configurations of EFM 354
8.2.4 Configuring basic functions of EFM 355
8.2.5 Configuring active functions of EFM 356
8.2.6 Configuring EFM passive function 358
8.2.7 Checking configurations 361
8.2.8 Maintenance 362

9 Security 363

9.1 ACL 363
9.1.1 Introduction 363
9.1.2 Preparing for configurations 364
9.1.3 Configuring MAC ACL 364
9.1.4 Configuring ACL period 372
9.1.5 Configuring filter 372
9.1.6 Checking configurations 374
9.1.7 Maintenance 375

Copyright © Raisecom Technology Co., Ltd.

9.2 Port security MAC 375
9.2.1 Introduction 375
9.2.2 Preparing for configurations 376
9.2.3 Default configurations of port security MAC 377
9.2.4 Configuring basic functions of port security MAC 377
9.2.5 Configuring static secure MAC address 378
9.2.6 Configuring dynamic secure MAC address 379
9.2.7 Configuring sticky secure MAC address 380
9.2.8 Checking configurations 381
9.2.9 Maintenance 381
9.2.10 Example for configuring port security MAC 382
9.3 Dynamic ARP inspection 384
9.3.1 Introduction 384
9.3.2 Preparing for configurations 385
9.3.3 Default configurations of dynamic ARP inspection 385
9.3.4 Configuring trusted interfaces of dynamic ARP inspection 386
9.3.5 Configuring static binding of dynamic ARP inspection 386
9.3.6 Configuring dynamic binding of dynamic ARP inspection 387
9.3.7 Configuring protection VLAN of dynamic ARP inspection 387
9.3.8 Configuring rate limiting on ARP packets on interface 388
9.3.9 Configuring number of binding tables on interface 388
9.3.10 Checking configurations 389
9.3.11 Example for configuring dynamic ARP inspection 389
9.4 RADIUS 392
9.4.1 Introduction 392
9.4.2 Preparing for configurations 392
9.4.3 Default configurations of RADIUS 393
9.4.4 Configuring basic functions of AAA 393
9.4.5 Configuring RADIUS authentication 394
9.4.6 Configuring RADIUS accounting 396
9.4.7 Checking configurations 397
9.4.8 Example for configuring RADIUS 397
9.5 TACACS+ 399
9.5.1 Introduction 399
9.5.2 Preparing for configurations 399
9.5.3 Default configurations of TACACS+ 400
9.5.4 Configuring basic functions of AAA 400
9.5.5 Configuring TACACS+ authentication 401
9.5.6 Configuring TACACS+ accounting 402
9.5.7 Checking configurations 403
9.5.8 Maintenance 403
9.5.9 Example for configuring TACACS+ 404

Copyright © Raisecom Technology Co., Ltd.

9.6 Storm control 405
9.6.1 Introduction 405
9.6.2 Preparing for configurations 406
9.6.3 Default configurations of storm control 406
9.6.4 Configuring storm control over interface 406
9.6.5 Configuring DLF packet forwarding 408
9.6.6 Checking configurations 408
9.6.7 Example for configuring storm control 409
9.7 802.1x 410
9.7.1 Introduction 410
9.7.2 Preparing for configruations 412
9.7.3 Default configurations of 802.1x 413
9.7.4 Configuring basic functions of 802.1x 413
9.7.5 Configuring 802.1x re-authentication 416
9.7.6 Configuring 802.1x timers 416
9.7.7 Checking configurations 418
9.7.8 Maintenance 418
9.7.9 Example for configuring 802.1x 418
9.8 IP Source Guard 420
9.8.1 Introduction 420
9.8.2 Preparing for configurations 421
9.8.3 Default configurations of IP Source Guard 422
9.8.4 Configuring interface trust status of IP Source Guard 422
9.8.5 Configuring IP Source Guard binding 423
9.8.6 Configuring priority and rate limit of IP source guard 424
9.8.7 Checking configurations 425
9.8.8 Example for configuring IP Source Guard 425
9.9 PPPoE+ 427
9.9.1 Introduction 427
9.9.2 Preparing for configurations 428
9.9.3 Default configurations of PPPoE+ 429
9.9.4 Configuring basic functions of PPPoE+ 429
9.9.5 Configuring PPPoE+ packet information 431
9.9.6 Checking configurations 433
9.9.7 Maintenance 433
9.9.8 Example for configuring PPPoE+ 434
9.10 Configuring CPU protection 436
9.10.1 Preparing for configurations 436
9.10.2 Configuring global CPU CAR 436
9.10.3 Checking configurations 437
9.10.4 Maintenance 437
9.11 Configuring ARP attack protection 438

Copyright © Raisecom Technology Co., Ltd.

9.11.1 Preparing for configurations 438
9.11.2 Configuring ARP 438
9.11.3 Checking configurations 439
9.12 ND Snooping 440
9.12.1 Introduction 440
9.12.2 Preparing for configurations 440
9.12.3 Default configurations of ND Snooping 440
9.12.4 Configuring ND Snooping 441
9.12.5 RA Snooping 441
9.12.6 Checking configurations 442
9.12.7 Maintenance 442
9.12.8 Example for configuring ND Snooping 443
10 Reliability 446
10.1 Link aggregation 446
10.1.1 Introduction 446
10.1.2 Preparing for configurations 447
10.1.3 Configuring manual link aggregation 447
10.1.4 Configuring static LACP link aggregation 449
10.1.5 Configuring manual master/slave link aggregation 452
10.1.6 Checking configurations 453
10.1.7 Example for configuring static LACP link aggregation 454
10.2 Interface backup 456
10.2.1 Introduction 456
10.2.2 Preparing for configurations 458
10.2.3 Default configurations of interface backup 458
10.2.4 Configuring basic functions of interface backup 459
10.2.5 (Optional) configuring FS on interfaces 460
10.2.6 Checking configurations 461
10.2.7 Example for configuring interface backup 461
10.3 Link-state tracking 464
10.3.1 Introduction 464
10.3.2 Preparing for configurations 464
10.3.3 Default configurations of link-state tracking 464
10.3.4 Configuring link-state tracking 464
10.3.5 Checking configurations 467
10.3.6 Example for configuring link-state tracking 467
10.4 Key-chain 469
10.4.1 Introduction 469
10.5 UDLD 472
10.5.1 Introduction 472
10.5.2 Preparing for configurations 472

Copyright © Raisecom Technology Co., Ltd.

10.5.3 Default configurations of UDLD 472
10.5.4 Configuring UDLD 472
10.5.5 Checking configurations 473

11 System management 474

11.1 SNMP 474
11.1.1 Introduction 474
11.1.2 Preparing for configurations 476
11.1.3 Default configurations of SNMP 476
11.1.4 Configuring basic functions of SNMPv1/SNMPv2c 477
11.1.5 Configuring basic functions of SNMPv3 478
11.1.6 Configuring IP address authentication by SNMP server 482
11.1.7 Configuring other information about SNMP 482
11.1.8 Configuring Trap 483
11.1.9 Checking configurations 485
11.1.10 Example for configuring SNMPv1/SNMPv2c and Trap 486
11.1.11 Example for configuring SNMPv3 and Trap 488
11.2 RMON 491
11.2.1 Introduction 491
11.2.2 Preparing for configurations 492
11.2.3 Default configurations of RMON 492
11.2.4 Configuring RMON statistics 493
11.2.5 Configuring RMON historical statistics 493
11.2.6 Configuring RMON alarm group 494
11.2.7 Configuring RMON event group 495
11.2.8 Checking configurations 496
11.2.9 Maintenance 496
11.2.10 Example for configuring RMON alarm group 497
11.3 LLDP 498
11.3.1 Introduction 498
11.3.2 Preparing for configurations 501
11.3.3 Default configurations of LLDP 501
11.3.4 Enabling global LLDP 501
11.3.5 Enabling interface LLDP 502
11.3.6 Configuring basic functions of LLDP 502
11.3.7 Configuring LLDP alarm 503
11.3.8 Configuring TLV 503
11.3.9 Checking configurations 505
11.3.10 Maintenance 505
11.3.11 Example for configuring LLDP 506
11.4 Optical module DDM 509
11.4.1 Introduction 509

Copyright © Raisecom Technology Co., Ltd.

11.4.2 Preparing for configurations 509
11.4.3 Default configurations of optical module DDM 510
11.4.4 Enabling optical module DDM 510
11.4.5 Enabling optical module DDM Trap 510
11.4.6 Checking configurations 511
11.5 System log 512
11.5.1 Introduction 512
11.5.2 Preparing for configurations 513
11.5.3 Default configurations of system log 513
11.5.4 Configuring basic information of system log 513
11.5.5 Configuring system log output 515
11.5.6 Checking configurations 520
11.5.7 Maintenance 521
11.5.8 Example for configuring outputting system logs to log host 521
11.6 Alarm management 522
11.6.1 Introduction 522
11.6.2 Preparing for configurations 526
11.6.3 Configuring basic functions of alarm management 527
11.6.4 Checking configurations 530
11.7 Hardware environment monitoring 531
11.7.1 Introduction 531
11.7.2 Preparing for configurations 533
11.7.3 Default configurations of hardware environment monitoring 534
11.7.4 Enabling global hardware environment monitoring 534
11.7.5 Configuring temperature monitoring alarm 534
11.7.6 Configuring power supply alarm 535
11.7.7 Clearing all hardware environment monitoring alarms manually 535
11.7.8 Checking configurations 536
11.8 CPU monitoring 536
11.8.1 Introduction 536
11.8.2 Preparing for configurations 537
11.8.3 Default configurations of CPU monitoring 537
11.8.4 Configuring CPU monitoring alarm 537
11.8.5 Checking configurations 538
11.9 Fan monitoring 538
11.9.1 Introduction 538
11.9.2 Preparing for configurations 538
11.9.3 Configuring fan monitoring 539
11.9.4 Checking configurations 539
11.10 Cable diagnosis 539
11.10.1 Introduction 539
11.10.2 Preparing for configurations 540

Copyright © Raisecom Technology Co., Ltd.

11.10.3 Configuring cable diagnosis 540
11.10.4 Checking configurations 540
11.11 Memory monitoring 541
11.11.1 Preparing for configurations 541
11.11.2 Configuring memory monitoring 541
11.11.3 Checking configurations 542
11.12 PING 542
11.12.1 Introduction 542
11.12.2 Configuring PING 542
11.13 Traceroute 544
11.13.1 Introduction 544
11.13.2 Configuring Traceroute 544
11.14 Performance statistics 546
11.14.1 Introduction 546
11.14.2 Preparing for configurations 546
11.14.3 Default configurations of performance statistics 547
11.14.4 Configuring performance statistics 547
11.14.5 Checking configurations 548
11.14.6 Maintenance 548
12 Appendix 549
12.1 Terms 549
12.2 Acronyms and abbreviations 554

Copyright © Raisecom Technology Co., Ltd.

Figures

Figure 1-1 Accessing device through PC connected with RJ45 Console interface 12
Figure 1-2 Configuring communication parameters in Hyper Terminal 12
Figure 1-3 Networking with device as Telnet server 13
Figure 1-4 Networking with device as Telnet client 15
Figure 1-5 User management networking 24
Figure 1-6 Configuring SSH login 25
Figure 1-7 Basic principles of NTP 41
Figure 1-8 NTP networking 49
Figure 2-1 Forwarding packets according to the MAC address table 66
Figure 2-2 MAC networking 73
Figure 2-3 VLAN partitions 74
Figure 2-4 VLAN and interface protection networking 85
Figure 2-5 Networking with PVLAN 92
Figure 2-6 Principles of basic QinQ 94
Figure 2-7 Basic QinQ networking 100
Figure 2-8 Selective QinQ networking 102
Figure 2-9 Principles of VLAN mapping 103
Figure 2-10 VLAN mapping networking 106
Figure 2-11 Network storm due to loopback 109
Figure 2-12 Loop networking with STP 110
Figure 2-13 Failure in forwarding VLAN packets due to RSTP 111
Figure 2-14 STP networking 118
Figure 2-15 Basic concepts of the MSTI network 121
Figure 2-16 MSTI concepts 122
Figure 2-17 Networking with multiple spanning trees instances in MST region 123
Figure 2-18 MSTP networking 138

Copyright © Raisecom Technology Co., Ltd.

Figure 2-19 Loop detection networking 142
Figure 2-20 Loop detection networking 146
Figure 2-21 Interface protection networking 150
Figure 2-22 Principles of port mirroring 151
Figure 2-23 Port mirroring networking 154
Figure 2-24 L2CP networking 159
Figure 2-25 Networking for IP phone to connect to switch 163
Figure 2-26 Networking for IP phone to connect PC to the switch 163
Figure 2-27 Networking with adding interface to voice VLAN and configuring it to work in manual mode ... 167
Figure 2-28 Configuring IP phone to access voice VLAN packets through LLDP 169
Figure 2-29 Principles of GVRP 172
Figure 2-30 GVRP networking 176
Figure 3-1 VLAN interface networking 182
Figure 3-2 Interface loopback 186
Figure 3-3 Configuring ARP networking 192
Figure 3-4 Principles of NDP address resolution 193
Figure 3-5 Configuring static route 201
Figure 4-1 Principles of PoE 210
Figure 4-2 PD Active check 216
Figure 4-3 PoE switch power supply networking 220
Figure 5-1 DHCP typical networking 224
Figure 5-2 Structure of DHCP packet 224
Figure 5-3 DHCP Client networking 226
Figure 5-4 DHCP Client networking 229
Figure 5-5 Zero-configuration server networking 231
Figure 5-6 DHCP Snooping 233
Figure 5-7 DHCP Snooping networking 239
Figure 5-8 DHCP Server and Client networking 251
Figure 5-9 Structure of a DHCP packet 251
Figure 5-10 DHCP Server networking 256
Figure 5-11 Typical application of DHCP Relay 258
Figure 5-12 DHCP Relay networking 262
Figure 6-1 Traffic classification 266

Copyright © Raisecom Technology Co., Ltd.

Figure 6-2 Structure of an IP packet header 266
Figure 6-3 Structures of the ToS priority and DSCP 266
Figure 6-4 Structure of a VLAN packet 266
Figure 6-5 Structure of CoS 267
Figure 6-6 SP scheduling 269
Figure 6-7 WRR scheduling 269
Figure 6-8 DRR scheduling 270
Figure 6-9 Queue scheduling networking 304
Figure 6-10 Rate limiting based on traffic policy 306
Figure 6-11 Rate limiting based on interface 309
Figure 7-1 Multicast transmission networking 312
Figure 7-2 Basic concepts in multicast 314
Figure 7-3 Mapping between IPv4 multicast address and multicast MAC address 315
Figure 7-4 Operating of IGMP and Layer 2 multicast features 315
Figure 7-5 IGMP Snooping networking 321
Figure 7-6 Ring network multicast networking 324
Figure 7-7 IGMP Snooping networking 330
Figure 7-8 IGMP MVR networking 332
Figure 7-9 MVR networking 335
Figure 7-10 Applying IGMP filtering on interface 343
Figure 7-11 Data transmission of IGMP MVR 346
Figure 7-12 Data transmission of multicast VLAN copy 346
Figure 7-13 Multicast VLAN copy networking 347
Figure 8-1 OAM loopback 354
Figure 9-1 Port security MAC networking 382
Figure 9-2 Principles of dynamic ARP inspection 385
Figure 9-3 Configuring dynamic ARP inspection 390
Figure 9-4 RADIUS networking 398
Figure 9-5 TACACS+ networking 404
Figure 9-6 Storm control networking 409
Figure 9-7 802.1x structure 410
Figure 9-8 Dot1x networking 419
Figure 9-9 Principles of IP Source Guard 421

Copyright © Raisecom Technology Co., Ltd.

Figure 9-10 Configuring IP Source Guard 426
Figure 9-11 Accessing the network through PPPoE authentication 428
Figure 9-12 PPPoE+ networking 434
Figure 9-13 ND Snooping networking 443
Figure 10-1 Static LACP mode Link aggregation networking 454
Figure 10-2 Principles of interface backup 457
Figure 10-3 Networking with interface backup in different VLANs 458
Figure 10-4 Interface backup networking 462
Figure 10-5 Link-state tracking networking 467
Figure 11-1 Principles of SNMP 475
Figure 11-2 SNMPv3 authentication mechanism 479
Figure 11-3 SNMPv1/SNMPv2c networking 486
Figure 11-4 SNMPv3 and Trap networking 489
Figure 11-5 RMON networking 492
Figure 11-6 RMON networking 497
Figure 11-7 Structure of a LLDPDU 499
Figure 11-8 Structure of a TLV packet 499
Figure 11-9 LLDP networking 506
Figure 11-10 Networking of outputting system log to log host 521
Figure 11-11 Principles of PING 542
Figure 11-12 Principles of Traceroute 544

Copyright © Raisecom Technology Co., Ltd.

Tables

Table 1-1 Shortcut keys for display features 8
Table 2-1 Interface mode and packet processing 75
Table 5-1 Fields of a DHCP packet 224
Table 5-2 Common DHCP options 240
Table 5-3 Fields of a DHCP packet 251
Table 6-1 Mapping from DSCP or CoS to local priority 268
Table 6-2 Mapping between local priority and queue 268
Table 6-3 Default mapping from CoS to local priority 273
Table 6-4 Default mapping from DSCP to local priority 273
Table 6-5 Default mapping from local priority to CoS 273
Table 11-1 TLV types 499
Table 11-2 IEEE 802.1 organization-defined TLVs 499
Table 11-3 IEEE 802.3 organization-defined TLVs 500
Table 11-4 Log levels 512
Table 11-5 Alarm fields 523
Table 11-6 Alarm levels 524
Table 11-7 Trap information 532
Table 11-8 Syslog information 533

Copyright © Raisecom Technology Co., Ltd.

1 Basic configurations

This chapter describes basic configurations and configuration procedures of the ISCOM2600G series switch, and provides related configuration examples, including the following sections:

- CLI
- Accessing device
- File management
- Loading and upgrade
- Time management
- Interface management
- Configuring basic information
- Task scheduling
- Watchdog
- Configuring Banner

1.1 CLI

1.1.1 Introduction

The Command-line Interface (CLI) is a medium for you to communicate with the ISCOM2600G series switch. You can configure, monitor, and manage the ISCOM2600G series switch through the CLI.

You can log in to the ISCOM2600G series switch through the terminal equipment or through a computer that runs the terminal emulation program. Enter commands at the system prompt.

The CLI supports the following features:

- You can configure the ISCOM2600G series switch locally through the Console interface.
- You can configure the ISCOM2600G series switch locally or remotely through Telnet/Secure Shell v2 (SSHv2).
- Commands are protected by levels. Users with different privileges can execute commands corresponding to their level only.

Copyright © Raisecom Technology Co., Ltd.

- Commands of different types belong to different commands modes. Users can configure the command of a type in the corresponding command mode.
- Users can use shortcut keys to execute commands.
- Users can check or execute a history command by checking command history. The last 20 history commands can be saved on the ISCOM2600G series switch.
- Users can enter a question mark (?) to obtain online help.
- The ISCOM2600G series switch supports multiple intelligent analysis methods, such as fuzzy match and context association.

1.1.2 Privileges

The ISCOM2600G series switch uses hierarchical protection methods to divide commands into 16 privileges in an ascending order.

- Viewing level: users can execute viewing commands, such as the **ping**, **clear**, and **history** commands.
- Monitoring level: users can execute monitoring commands, such as the **show** command.
- Configuring level: users can execute commands for configuring different services, such as Virtual Local Area Network (VLAN) and Internet Protocol (IP).
- Administering level: users can execute basic commands for administering the system.

1.1.3 Modes

Command line mode is the CLI environment. All system commands are registered in one (or multiple) command line mode, the command can only run in the corresponding mode.

Establish a connection with the ISCOM2600G series switch. If the ISCOM2600G series switch is in default configuration, it will enter user EXEC mode, and the screen will display:

```
Raisecom#
```

In privileged EXEC mode, use the **config** command to enter global configuration mode.

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

Note

- The CLI prompts that Raisecom is a default host name. You can modify it by using the **hostname** *name* command in privileged EXEC mode.
- Commands executed in global configuration mode can also be executed in other modes. The functions vary on command modes.
- You can use the **exit** or **quit** command to return to the upper command mode.
- You can execute the **end** command to return to privileged EXEC mode from any modes but privileged EXEC mode.

The ISCOM2600G series switch supports the following command line modes:

Copyright © Raisecom Technology Co., Ltd.

Mode	Enter method	Description
Privileged EXEC	After logging in to the device, at the "Login:" prompt, use the user name and password.	`Raisecom#`
Global configuration	In privileged EXEC mode, use the **config terminal** command.	`Raisecom(config)#`
Physical interface configuration	In global configuration mode, use the **interface** { **gigaethernet** | **tengigabitethernet** } *unit/slot/interface* command.	`Raisecom(config-gigaethernet1/1/`*`interface`*`)#` `Raisecom(config-tengigabitethernet1/1/`*`interface`*`)#`
SNMP interface configuration	In global configuration mode, use the **interface fastethernet 1/0/1** command.	`Raisecom(config-fastethernet1/0/1)#`
Loopback interface configuration	In global configuration mode, use the **interface loopback** *lb-number* command.	`Raisecom(config-loopback*)#`
VLAN configuration	In global configuration mode, use the **vlan** *vlan-id* command.	`Raisecom(config-vlan*)#`
Aggregation group configuration	In global configuration mode, use the **interface port-channel** *channel-number* command.	`Raisecom(config-port-channel)#`
Traffic classification configuration	In global configuration mode, use the **class-map** *class-map-name* command.	`Raisecom(config-cmap)#`
Traffic policy configuration	In global configuration mode, use the **policy-map** *policy-map-name* command.	`Raisecom(config-pmap)#`
Traffic policy configuration binding with traffic classification	In floe policy configuration mode, use the **class-map** *class-map-name* command.	`Raisecom(config-pmap-c)#`
Basic IP ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. In this command, *acl-number* ranges from 1000 to 1999.	`Raisecom(config-acl-ip-std)#`
Extended IP ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. In this command, *acl-number* ranges from 2000 to 2999.	`Raisecom(config-acl-ip-ext)#`
MAC ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. In this command, *acl-number* ranges from 3000 to 3999.	`Raisecom(config-acl-mac)#`

Copyright © Raisecom Technology Co., Ltd.

Mode	Enter method	Description
User ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. In this command, *acl-number* ranges from 5000 to 5999.	`Raisecom(config-acl-udf)#`
Advanced ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. The *acl-number* ranges from 7000 to 7999.	`Raisecom(config-acl-advanced)#`
MST region configuration	In global configuration mode, use the **spanning-tree region-configuration** command.	`Raisecom(config-region)#`
Profile configuration	In global configuration mode, use the **igmp filter profile** *profile-number* command.	`Raisecom(config-igmp-profile)#`
cos-remark configuration	In global configuration mode, use the **mls qos mapping cos-remark** *profile-id* command.	`Raisecom(cos-remark)#`
cos-to-pri configuration	In global configuration mode, use the **mls qos mapping cos-to-local-priority** *profile-id* command.	`Raisecom(cos-to-pri)#`
dscp-mutation configuration	In global configuration mode, use the **mls qos mapping dscp-mutation** *profile-id* command.	`Raisecom(dscp-mutation)#`
dscp-to-pri configuration	In global configuration mode, use the **mls qos mapping dscp-to-local-priority** *profile-id* command.	`Raisecom(dscp-to-pri)#`
SRED profile configuration	In global configuration mode, use the **mls qos sred profile** *profile-id* command.	`Raisecom(sred)#`
Traffic monitoring profile configuration	In global configuration mode, use the **mls qos policer-profile** *policer-name* command.	`Raisecom(traffic-policer)#`
Remote configuration	In physical interface configuration mode, use the **remote-device** command.	`Raisecom(config-remote)#`
Remote interface configuration	In remote configuration mode, use the **interface client** *client-id* command.	`Raisecom(config-remoteport)#`
Chinese prompt	In any configuration mode, use the **language chinese** command.	`Raisecom#`
English prompt	In any configuration mode, use the **language english** command.	`Raisecom#`

Copyright © Raisecom Technology Co., Ltd.

1.1.4 Shortcut keys

The ISCOM2600G series switch supports the following shortcut keys.

Shortcut key	Description
Up Arrow (↑)	Show the previous command if there is any command entered earlier; the displayed command does not change if the current command is the earliest one in history records.
Down Arrow (↓)	Show the next command if there is any newer command. The displayed command does not change if the current command is the newest one in history records.
Left Arrow (←)	Move the cursor leftward by one character. The displayed command does not change if the cursor is already at the beginning of the command.
Right Arrow (→)	Move the cursor rightward by one character. The displayed command does not change if the cursor is already at the end of the command.
Backspace	Delete the character before the cursor. The displayed command does not change if the cursor is already at the beginning of the command.
Tab	Press **Tab** after entering a complete keyword, and the cursor will automatically appear a space to the end. Press **Tab** again, and the system will show the follow-up available keywords. Press **Tab** after entering an incomplete keyword, and the system automatically executes partial helps: • When only one keyword matches the entered incomplete keyword, the system takes the complete keyword to replace the entered incomplete keyword and leaves one space between the cursor and end of the keyword. • When no keyword or multiple keywords match the entered incomplete keyword, the system displays the prefix, and you can press **Tab** to check words circularly. In this case, there is no space from the cursor to the end of the keyword. Press **Space bar** to enter the next word. • If you enter an incorrect keyword, pressing **Tab** will move the cursor to the next line and the system will prompt an error. In this case, the entered keyword does not change.
Ctrl+A	Move the cursor to the beginning of the command.
Ctrl+B	Identical to the **Left Arrow** key.
Ctrl+C	Interrupt the ongoing command, such as **ping** and **traceroute**. This short key combination takes effect only when page-break is enabled.
Ctrl+D or **Delete**	Delete the character at the cursor.
Ctrl+E	Move the cursor to the end of the command.
Ctrl+F	Identical to the Right Arrow key
Ctrl+K	Delete all characters from the cursor to the end of the command.

Copyright © Raisecom Technology Co., Ltd.

Shortcut key	Description
Ctrl+L	Clear screen information.
Ctrl+S	Identical to the **Down Arrow** key
Ctrl+W	Identical to the **Up Arrow** key
Ctrl+X	Delete all characters before the cursor (except the cursor location).
Ctrl+Y	Show history commands.
Ctrl+Z	Return to privileged EXEC mode from the current mode.
Space bar or **Y**	Scroll down one screen.
Enter	Scroll down one line.

1.1.5 Acquiring help

Complete help

You can acquire complete help under following three conditions:

- You can enter a question mark (?) at the system prompt to display a list of commands and brief descriptions available for each command mode.

```
Raisecom#?
```

The command output is as below.

```
aaa             Authentication, Authorization, Accounting
boot            system boot
bootrom          Bootrom
clear           Reset functions
clock           System time and date
config          Configuration from terminal interface
console          Console
copy            load configuration information
debug           Debugging functions (see also 'undebug')
delete           Delete flash file
……
```

- After you enter a keyword, press **Space bar** and enter a question mark (?), all correlated commands and their brief descriptions are displayed if the question mark (?) matches another keyword.

```
Raisecom(config)#ntp ?
```


Copyright © Raisecom Technology Co., Ltd.

The command output is as below.

```
authenticate        Authenticate function
authentication-keyid  Authentication keyid
peer               Configure NTP peer
refclock-master      Set local clock as reference clock
server             Configure NTP server
trust-keyid         Trusted authenticate keyid
```

- After you enter a keyword, press **Space bar** and enter a question mark (?), the value range and descriptions are displayed if the question mark (?) matches a parameter.

```
Raisecom(config)#interface vlan ?
```

The command output is as below.

```
vlan1
 <1-4094>  vlan number
```

Incomplete help

You can acquire incomplete help under following three conditions:

- After you enter part of a particular character string and a question mark (?), a list of commands that begin with a particular character string is displayed.

```
Raisecom(config)#c?
```

The command output is as below.

```
class-map   Set class map
clear      Clear buffer content
command-log  Log the command to the file
console     console
cpu        Configure cpu parameters
cpu-protect  Config cpu protect information
create      Create static VLAN
```

- After you enter a command, press **Space bar**, and enter a particular character string and a question mark (?), a list of commands that begin with a particular character string is displayed.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config)#show li?
```

The command output is as below.

```
link-state-tracking  Fault tracking
link-trace         Link trace
```

- After you enter a partial command name and press **Tab**, the full form of the keyword is displayed if there is a unique match command. Otherwise, press **Tab** continuously to display different keywords and then you can select the required one.

Error messages

The ISCOM2600G series switch prints out the following error messages according to error type when you enter incorrect commands:

Error message	Description
% Incomplete command.	The user has entered an incomplete command.
Error input in the position marked by '^'.	The keyword marked "^" is invalid.
Ambiguous input in the position marked by '^'	The keyword marked "^" is not clear.

Note

If there is an error message mentioned above, use CLI help information to solve the problem.

1.1.6 Display information

Display features

The CLI provides the following display features:

- The help information and prompt messages displayed at the CLI are in English.
- When messages are displayed at more than one screen, you can suspend displaying them with one of the following operations, as listed in Table 1-1.

Table 1-1 Shortcut keys for display features

Shortcut key	Description
Press **Space bar** or **Y**	Scroll down one screen.
Press **Enter**	Scroll down one line.
Press any letter key (except **Y**)	Stop displaying and executing commands.

Copyright © Raisecom Technology Co., Ltd.

Filtering displayed information

The ISCOM2600G series switch supports a series of commands starting with **show**, to check device configurations, operation and diagnostic information. Generally, these commands can output more information, and then you need to add filtering rules to filter out unnecessary information.

The **show** command on the ISCOM2600G series switch supports three kinds of filter modes:

- | **begin** *string*: show all lines starting from the assigned string. Case-sensitivity is optional.
- | **exclude** *string*: show all lines mismatching the assigned string. Case-sensitivity is optional.
- | **include** *string*: show all lines only matching the assigned string. Case-sensitivity is optional.

Step	Command	Description
1	`Raisecom#show command-string | { begin | include | exclude } expression [ igncase ]`	Configure whether to distinguish upper case and lower case when showing configurations, running status, and diagnosis information about the device. • command-string: command string • expression: key word to be filtered, a string, optionally case sensitive • begin: show all lines starting from the line matching the specified string. • exclude: show all lines mismatching the specified string. • include: show all lines matching the specified string. • igncase: ignore case-sensitivity.

Page-break

Page-break is used to suspend displaying messages when they are displayed at more than one screen. After page-break is enabled, you can use shortcut keys listed in Table 1-1. If page-break is disabled, all messages are displayed when they are displayed at more than one screen.

By default, page-break is enabled.

Configure terminal page-break for the ISCOM2600G series switch as below.

Step	Command	Description

1	`Raisecom#terminal page-break { enable | disable }`
	Example:
	`Raisecom#terminal page-break enable`
		Enable or disable terminal page-break.
		• enable: enable terminal page-break.
		• disable: disable terminal page-break.

1.1.7 Command history

The history commands can be automatically saved at the CLI. You can use the up arrow (↑) or down arrow (↓) to schedule a history command. By default, the last 20 history commands are saved. You can configure the number of commands to be saved at the CLI.

Copyright © Raisecom Technology Co., Ltd.

Configure the ISCOM2600G series switch as below.

Step	Command	Description

1	`Raisecom#terminal history number`
	Example:
	`Raisecom#terminal history 10`
		(Optional) configure the number of history commands saved in the system.
		• number: the number of displayed commands, an integer, ranging from 1 to 20

2	`Raisecom#terminal time-out second`
	Example:
	`Raisecom#terminal time-out 20`
		(Optional) configure the Console terminal timeout period.
		• second: logout waiting time of terminal timeout, an integer, ranging from 0 to 6553, in units of second

3	`Raisecom#history`	Show history commands entered by the user.
4	`Raisecom#show terminal`	Show terminal configurations of the user.

1.1.8 Restoring default value of command line

The default value of command line can be restored by **no** form or **enable | disable** form.

- **no** form: be provided in front of a command and used to restore the default value, disable some feature, or delete a configuration. It is used to perform an operation that is opposite to the command. Therefore, the command with a **no** form is also called a reverse command.
- **enable | disable** form: be provided behind a command or in the middle of a command. The **enable** parameter is used to enable some feature or function while the **disable** parameter is used to disable some feature or function.

For example:

- In physical interface configuration mode, the **description** *string* command is used to modify descriptions about an interface while the **no description** command is used to delete descriptions about the interface and restore to the default values.
- In physical interface configuration mode, the **shutdown** command is used to disable an interface while the **no shutdown** command is used to enable an interface.
- In global configuration mode, the **terminal page-break enable** command is used to enable page-break while the **terminal page-break disable** command is used to disable terminal page-break.

Note

Most configuration commands have default values, which often are restored by the **no** form.

1.1.9 Logging commands

Configure command log for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#command-log { enable | disable }`
	Example:
	`Raisecom(config)#command-log enable`
		Enable or disable command logging.
		• enable: enable command loging.
		• disable: disable command loging.

1.2 Accessing device

1.2.1 Introduction

The ISCOM2600G series switch can be configured and managed in Command Line Interface (CLI) mode or NView NNM network management mode.

The ISCOM2600G series switch CLI mode has a variety of configuration modes:

- Console mode: it must use Console mode in the first configuration.
- Telnet mode: log on through the Console mode, open Telnet service on the Switch, configure the IP address of the VLAN interface, configure the user name and password, and then take remote Telnet configuration.
- SSH mode: before accessing the ISCOM2600G series switch through SSH, you need to log in to the ISCOM2600G series switch and start SSH services through the Console interface.

When configuring the ISCOM2600G series switch in network management mode, you must first configure the IP address of the VLAN interface on CLI, and then configure the ISCOM2600G series switch through the NView NNM system.

1.2.2 Accessing through Console interface

Introduction

The Console interface is commonly used to connect the network device with a PC running terminal emulation programs. You can use this interface to configure and manage local devices. In this management mode, devices can communicate with each other independent from the network, so it is called out-of-band management. You can also perform configuration and management on the ISCOM2600G series switch through the Console interface when the network fails.

In the following two conditions, you can only log in to the ISCOM2600G series switch and configure it through the Console interface:

- The ISCOM2600G series switch is powered on to start for the first time.
- Accessing the ISCOM2600G series switch through Telnet fails.

Accessing device through RJ45 Console interface

If you want to access the ISCOM2600G series switch through PC through RJ45 Console interface, connect Console interface and PC RS-232 serial port, as shown in Figure 1-1; then

Copyright © Raisecom Technology Co., Ltd.

run the terminal emulation program in PC to configure communication parameters as shown in Figure 1-2, and then log in to the ISCOM2600G series switch.

Figure 1-1 Accessing device through PC connected with RJ45 Console interface

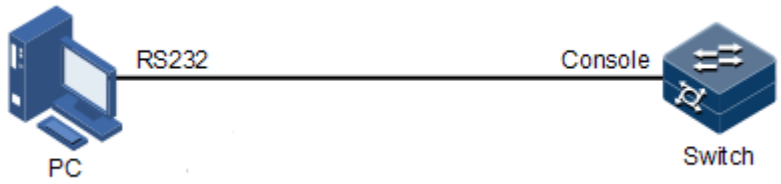
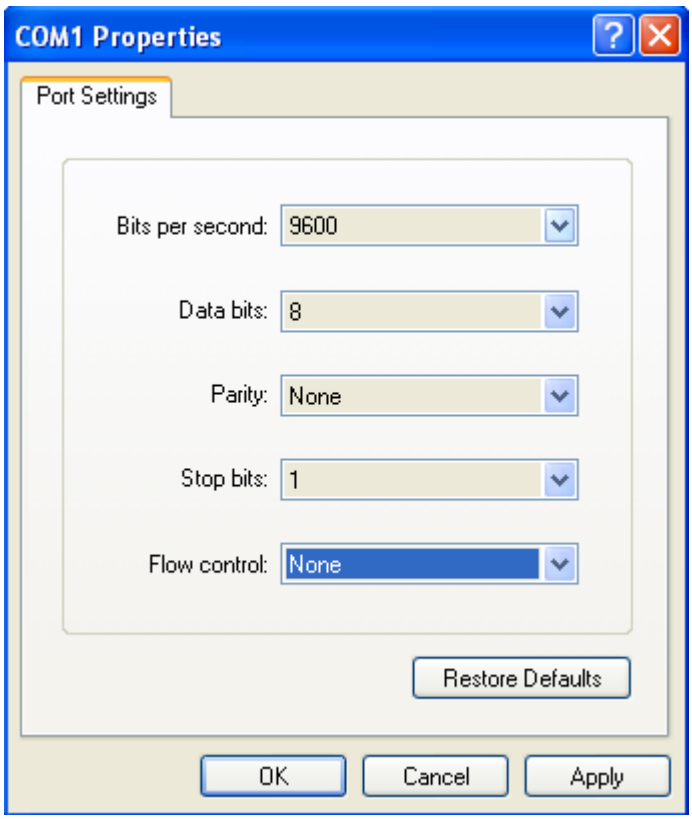


Figure 1-2 Configuring communication parameters in Hyper Terminal



Note

By default, the baud rate of the serial interface is 9600.

Configure the baud rate of the serial interface for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

1	`Raisecom#config`
	`Raisecom(config)#console baud-rate { 115200 | 19200 | 38400 | 9600 }`
	`Example:`
	`Raisecom(config)#console baud-rate 9600`
		Modify the baud rate of the serial interface to 115200, 19200, 38400, or 9600.
		• baud-rate: baud rate of the Console interface
		• 115200: configure the baud rate of the Console interface to 115200 baud.
		• 19200: configure the baud rate of the Console interface to 19200 baud.
		• 38400: configure the baud rate of the Console interface to 38400 baud.
		• 9600: configure the baud rate of the Console interface to 9600 baud.

1.2.3 Accessing through Telnet

Note

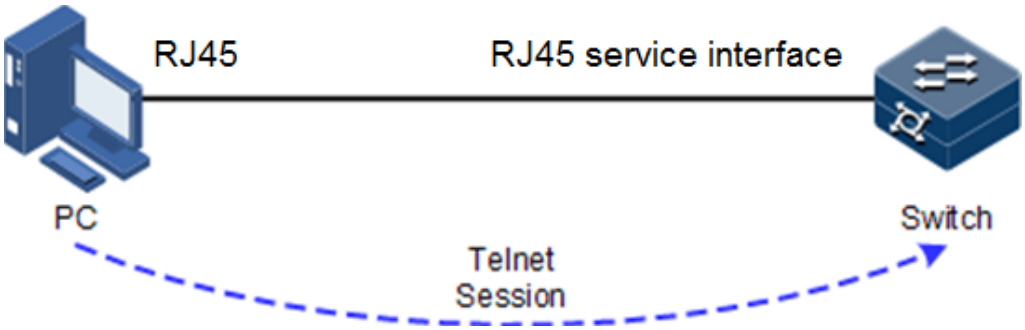
By default, the default management IP address of the out-of-band management interface (SNMP interface: fastethernet 1/0/1), and the subnet mask is 255.255.255.0. To modify the IP address, log in to the ISCOM2600G series switch and configure it. Both the default user name and password are raisecom. In Telnet connection status, if you enter the password incorrectly for three 3 times, the Telnet connection will be automatically disconnected.

You can use a PC to log in to the ISCOM2600G series switch remotely through Telnet. You can log in to an ISCOM2600G series switch from PC at first, then Telnet another ISCOM2600G series switch on the network. You do not need to connect a PC to each ISCOM2600G series switch.

Telnet services provided by the ISCOM2600G-HI series switch are as below:

- Telnet Server: run the Telnet client program on a PC to log in to the ISCOM2600G series switch, and take configuration and management. As shown in Figure 1-3, the ISCOM2600G series switch is providing Telnet Server service at this time.

Figure 1-3 Networking with device as Telnet server



Before accessing the ISCOM2600G series switch through Telnet, you need to log in to the ISCOM2600G series switch through the Console interface and start the Telnet service. Take the following configurations on the ISCOM2600G series switch that needs to start Telnet service.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface fastethernet 1/0/1`	Enter out-of-band network management interface configuration mode
3	`Raisecom(config-fastethernet1/0/1)#ip address` *ip-address* [*ip-mask*] **Example:** `Raisecom(config-fastethernet1/0/1)#ip address 192.168.0.1 255.255.255.0`	Configure the IP address of the out-of-band network management interface. By default, it is 192.168.0.1. Both the default user name and password are raisecom. • ip-address: IP address, in dotted decimal notation, such as 10.0.0.1 • ip-mask: mask of IP address, in dotted decimal notation, such as 255.0.0.0
4	`Raisecom(config)#telnet-server accept` *interface-type interface-number* **Example:** `Raisecom(config)#telnet-server accept gigaethernet 1/1/1`	(Optional) configure the interface in support of Telnet function. • interface-type: interface type • interface-number: interface ID. The form and value range depend on the interface type.
5	`Raisecom(config)#telnet-server close terminal-telnet` *session-number* **Example:** `Raisecom(config)#telnet-server close terminal-telnet 1`	(Optional) release the specified Telnet connection. • session-number: session number, an integer, ranging from 1 to 10
6	`Raisecom(config)#telnet-server max-session` *session-number* **Example:** `Raisecom(config)#telnet-server max-session 5`	(Optional) configure the maximum number of Telnet sessions supported by the ISCOM2600G series switch. By default, it is 10. • session-number: maximum number of connections, an integer, ranging from 0 to 10
7	`Raisecom(config)#telnet-server access-list` { *ip-access-list-number* | *ipv6-access-list-number* } **Example:** `Raisecom(config)#telnet-server access-list 1001`	(Optional) configure the ACL number of the Telnet. • ip access-list number: IPv4 standard ACL number, an integer, ranging from 1000 to 1999; IPv4 ACL number, an integer, ranging from 2000 to 2999 • ipv6 access-list number: IPv6 ACL number, an integer, ranging from 6000 to 6999

8	`Raisecom(config)#telnet-server { enable | disable }`
	Example:
	`Raisecom(config)#telnet-server disable`
		(Optional) enable or disable Telnet Server. At the same time, the corresponding port number will be disabled.
		• enable: enable Telnet server.
		• disable: disable Telnet server.

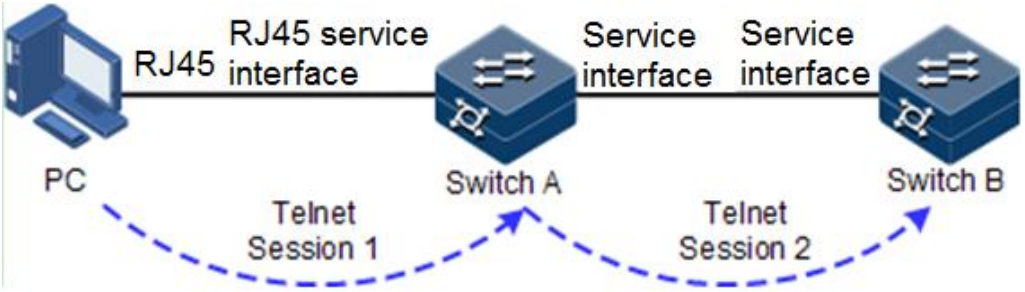
Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

9	`Raisecom(config)#telnet-server port port-id`
	Example:
	`Raisecom(config)#telnet-server port 2000`
		(Optional) configure the Telnet listening port number.
		• port-id: Telnet listening port number, an integer, ranging from 1 to 65535

- Telnet Client: when you connect to the ISCOM2600G series switch through the PC terminal emulation program or Telnet client program on a PC, then telnet other ISCOM2600G series switch and configure/manage them. As shown in Figure 1-4, Switch A not only acts as Telnet server but also provides Telnet client service.

Figure 1-4 Networking with device as Telnet client



Configure Telnet Client device as below.

Step	Command	Description

1	`Raisecom#telnet { ipv4-address | ipv6-address } [ port port-id ]`
	`Raisecom#telnet ipv4-address [ port port-id ] [ sourceip source-ip-address ]`
	Example:
	`Raisecom#telnet 192.168.1.1`
		Log in to another device through Telnet.
		• ipv4-address: IPv4 address of the remote destination host, in dotted decimal notation, such as 10.10.1.1
		• ipv6-address: IPv6 address of the remote destination host, in form of A:B::C:D/M
		• port-id: TCP port number corresponding to Telnet service which is provided by the remote destination device, an integer, ranging from 1 to 65535
		• source-ip-address: source IPv4 address, in dotted decimal notation, such as 10.10.1.1

1.2.4 Accessing through SSH

Telnet is lack of security authentication and it transports messages through Transmission Control Protocol (TCP) which exists with big potential security hazard. Telnet service may cause hostile attacks, such as Deny of Service (DoS), host IP spoofing, and routing spoofing.

The traditional Telnet and File Transfer Protocol (FTP) transmit password and data in plain text, which cannot satisfy users' security demands. SSHv2 is a network security protocol, which can effectively prevent the disclosure of information in remote management through data encryption, and provides greater security for remote login and other network services in network environment.

Copyright © Raisecom Technology Co., Ltd.

SSHv2 allows data to be exchanged through TCP and it establishes a secure channel over TCP. Besides, SSHv2 supports other service ports besides standard port 22, avoiding illegal attacks from the network.

Before accessing the ISCOM2600G series switch through SSHv2, you must log in to the ISCOM2600G series switch through the Console interface and start SSH service.

Default configurations for accessing the ISCOM2600G series switch through SSHv2 are as below.

Function	Default value
SSH server status	Disable
Local SSH key pair length	512 bits
Key renegotiation period	0h
SSH authentication method	password
SSH authentication timeout	600s
Allowable failure times for SSH authentication	20
SSH snooping port number	22
SSH session status	Disable
SSH version	v2

Configure SSH services for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#generate ssh-key [ length ]`
	Example:
	`Raisecom(config)#generate ssh-key 512`
		Generate local SSHv2 key pair and designate its length.
		By default, the length is 512 bits.
		• length: key pair length of the SSH server, an integer, ranging from 512 to 2048, in units of bit

3	`Raisecom(config)#ssh2 server`	Start the SSH server. By default, it is not started. Use the **no ssh2 server** command to shut down the SSH server. (Optional) configure SSH key renegotiation period.

4	`Raisecom(config)#ssh2 server authentication { password | rsa-key }`
	Example:
	`Raisecom(config)#ssh2 server authentication password`
		(Optional) configure SSHv2 authentication mode.
		By default, it is password.
		• password: use local user name and password to authenticate SSH clients.
		• rsa-key: use "host key pairs + local user name and password" to authenticate SSH clients.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config)#**ssh2 server authentication** *public-key-name* **public-key** [*publickey*] **Example:** Raisecom(config)#ssh2 server authentication aa public-key	(Optional) record the public key of the client on the ISCOM2600G series switch in rsa-key authentication mode. • public-key-name: public key name • publickey: public key contents, a string of 10 characters
6	Raisecom(config)#**ssh2 server authentication-timeout** *second* **Example:** Raisecom(config)#ssh2 server authentication-timeout 100	(Optional) configure the SSHv2 authentication timeout. The ISCOM2600G series switch refuses to authenticate the client and then closes the connection when the client authentication time exceeds this upper limit. By default, it is 600s. • second: SSH authentication timeout, an integer, ranging from 100 to 65535, in units of second
7	Raisecom(config)#**ssh2 server authentication-retries** *times* **Example:** Raisecom(config)#ssh2 server authentication-retries 20	(Optional) configure the allowable failure times for SSHv2 authentication. The ISCOM2600G series switch refuses to authenticate the client and then closes the connection when the number of client authentication failure times exceeds the upper limit. By default, it is 20. • times: number of failures allowed in SSH authentication, an integer, ranging from 1 to 100
8	Raisecom(config)#**ssh2 server port** *port-number* **Example:** Raisecom(config)#ssh2 server port 20	(Optional) configure SSHv2 snooping port number. By default, it is 22. • port-id: SSH listening port number, an integer, ranging from 1 to 65535 **Note** When configuring SSHv2 snooping port number, the entered parameter cannot take effect until SSH is restarted.
9	Raisecom(config)#**ssh2 server max-session** *session-number* **Example:** Raisecom(config)#ssh2 server max-session 1	(Optional) configure the maximum number of SSHv2 sessions. • session-number: maximum number of sessions, an integer, ranging from 0 to 10

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
10	Raisecom(config)#**ssh2 access-list** { *ip-access-list-number* | *ipv6-access-list-number* } **Example:** Raisecom(config)#ssh2 access-list 1001	(Optional) configure the ACL number. • ip access-list number: IPv4 standard ACL number, an integer, ranging from 1000 to 1999; IPv4 extended ACL number, an integer, ranging from 2000 to 2999 • ipv6 access-list number: IPv6 ACL number, an integer, ranging from 6000 to 6999
11	Raisecom(config)#**ssh2 server rekey-interval** *value* **Example:** Raisecom(config)#ssh2 server rekey-interval 10	(Optional) configure the SSH renegotiation time. • value: renegotiation time, an integer, ranging from 1 to 24
12	Raisecom(config)#**ssh2 server close session** *session-number* **Example:** Raisecom(config)#ssh2 server close session 5	(Optional) close the specified SSHv2 session. • session-number: SSH2 session ID, an integer, ranging from 1 to 10

1.2.5 Managing users

Introduction

When you start the ISCOM2600G series switch for the first time, connect the PC through Console interface to the ISCOM2600G series switch, enter the initial user name and password in HyperTerminal to log in and configure the ISCOM2600G series switch.

Note

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

If there is no privilege restriction, any remote user can log in to the ISCOM2600G series switch through Telnet or access network by establishing a Point to Point Protocol (PPP) connection when service interfaces are configured with IP addresses. This is unsafe to the ISCOM2600G series switch and network. Creating user accounts for the ISCOM2600G series switch and configuring password and privilege help manage login users and ensures network and device security.

Default configurations of user management

Default configurations of user management are as below.

Function	Default value
Local user information	• User name: raisecom • Password: raisecom • Privilege: 15
New user privilege	15

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
New user activation status	Activate
New user service type	N/A
Login password	raisecom
User login authentication mode	local-user
Password valid period check	Disable
Password valid period	90 days
Number of days for reminding prior to password invalidity	30 days
Login and logout alarm status	Disable
Password check strength	simple

Configuring local user management

Configure local user management for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**user name** *user-name* **password** [**cipher** | **simple**] *password* [**confirm**] Raisecom#**no username** *user-name* **Example:** Raisecom#user name user1 password aaAA1234@ Raisecom#no username raisecom	Create or modify the user name and password for login. Use the **no** form of this command to delete a user account. • user-name: user name, a string of 1 to 16 characters • password password: login password, a string of characters with the length depending on the password check mode • simple: plaintext password • cipher: ciphertext password • confirm: confirm
2	Raisecom#**user name** *user-name* **privilege** *privilege-level* **Example:** Raisecom#user name user1 privilege 5	Configure the login user privilege. • user-name: user name, a string of 1 to 16 characters • privilege-level: user privilege, an integer, ranging from 1 to 15
3	Raisecom#**user name** *user-name* **state** { **active** | **inactive** } **Example:** Raisecom#user name user1 state active	(Optional) configure the status of a login user. • user-name: user name, a string of 1 to 16 characters • active: the user is in active status. • inactive: the user is in inactive status.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom#**user** *user-name* { **allow-exec** | **disallow-exec** } *first-keyword* [*second-keyword*] [**confirm**] **Example:** Raisecom#user raisecom1 allow-exec write	(Optional) configure the priority rule for login user to perform the command line. • user-name: user name, a string of 1 to 16 characters • allow-exec: allow users to execute commands with priorities higher than theirs. • disallow-exec: disallow users execute commands with priorities lower than theirs. • first-keyword: first keyword of the command • second-keyword: second keyword of the command • confirm: confirm
5	Raisecom#**user** *user-name* **service-type** { **lan-access** | **ssh** | **telnet** | **web** | **console** | **all** } **Example:** Raisecom#user raisecom1 service-type telnet	(Optional) configure the service type supported by the user. • user-name: user name, a string of 1 to 16 characters • lan-access: LAN access • ssh: SSH session • telnet: Telnet session • web: Web connection • console: Console connection • all: All service types
6	Raisecom#**user login** { **console** | **telnet** | **ssh** | **web** } { **local-radius** | **local-user** | **radius-local** [**server-no-response**] | **radius-user** | **local-tacacs** | **tacacs-local** [**server-no-response**] | **tacacs-user** } **Example:** Raisecom#user login local-radius	(Optional) configure the authentication mode for different user login modes. • console: Console interface login • telnet: Telnet login • ssh: SSH login • web: Web login • local-radius: when local authentication coexist with RADIUS authentication, use local authentication in preference to RADIUS. • local-user: sse local authentication. • radius-local: when local authentication coexist with RADIUS authentication concurrently, use RADIUS authentication in preference to local authentication. • radius-user: use RADIUS authentication. • local-tacacs: when local authentication coexist with TACACS+ authentication, use local authentication in preference to TACACS+ authentication. • tacacs-local: when local authentication coexist with TACACS+ authentication, use TACACS+ authentication in preference to local authentication. • tacacs-user: use TACACS+ authentication. • server-no-response: use local authentication if the server stops responding.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
7	Raisecom#**enable** [*privilege*] **Example:** Raisecom#enable 11	(Optional) configure the user privilege. • privilege: user privilege, an integer, ranging from 1 to 15
8	Raisecom#**logout**	Exit the system.
9	Raisecom#**config**	Enter global configuration mode.
10	Raisecom(config)#**login -trap** { **enable** | **disable** }	(Optional) configure the login/logout alarm status.

Note

- Besides the default user raisecom, you can create up to 9 local user accounts.
- A local user with a level lower than 15, unless allowed to execute the command to modify the login password, is not allowed to modify the login password.

1.2.6 Configuring local password management

Configure local password management for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**enable password** [**cipher** *password*] **Example:** Raisecom#enable password Please input password(Not exceed 16 and more than 8 characters): Please input password again(Not exceed 16 and more than 8 characters): Set successfully	Modify the password for entering privileged EXEC mode. The user with the privilege under 11 does not need the password for entering privileged EXEC mode. • password: ciphertext password, a string of 1 to 36 characters
2	Raisecom#**password check** { **complex** | **none** | **simple** } **Example:** Raisecom#password check complex	Configure the password check strength. • simple: simple mode check • none: none mode check • complex: complex mode check
3	Raisecom#**password expire** { **enable** | **disable** } **Example:** Raisecom#password expire enable	Configure the password valid period check. • enable: enable password valid period check. • disable: disable password valid period check.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom#**password expire day** *time* **Example:** Raisecom#password expire day 100	Configure the password valid period. • time: password valid period, an integer, ranging from 1 to 999, in units of day
5	Raisecom#**password expire alert day** *time* **Example:** Raisecom#password expire alert day 10	Configure the number of days for reminding prior to password invalidity. • time: number of days for reminding prior to password invalidity, an integer, ranging from 1 to 999, in units of day

Note

The length of the login password depends on the password check mode:

- In complex mode, it is 8–16 characters, mandatorily including digits, lower-case letters, and upper-case letters.
- In simple mode, it is 8–16 characters.
- In none mode, it is 1–16 characters.

1.2.7 Configuring login through serial cable

After login through the serial cable is enabled on the Console interface, only the linear user on the Console interface can log in; in other words, the user logging in on the Console interface need to enter the linear password only, without the user name.

Configuring login through serial cable for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**line password** *password*	Configure the plaintext password for logging through the serial interface.
2	Raisecom#**line encrypt-password** *password*	Configure the ciphertext password for logging through the serial interface.
3	Raisecom#**console login line**	Configure the login mode on the Console interface to login through the serial interface.

1.2.8 Checking configurations

Use the following commands to check the configuration results.

No.	Command	Description
1	Raisecom#**show user table** [**detail**]	Show login user information.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
2	`Raisecom#show user active`	Show information about users logged in to the ISCOM2600G series switch.
3	`Raisecom#show user password expire`	Show configurations of the user valid period.
4	`Raisecom#show telnet-server`	Show configurations of the Telnet server.
5	`Raisecom#show ssh2 public-key [ authentication | rsa ]`	Show the public key used for SSH authentication on the ISCOM2600G series switch and client.
6	`Raisecom#show ssh2 { server | session }`	Show SSHv2 server or session information.
7	`Raisecom#show privilege`	Show the privilege of the current user.

1.2.9 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
`Raisecom#delete user-file` **Example:** `Raisecom#delete user-file`	Delete the user file. **Caution** This command is applicable to the device that is customized with the user password loss function.

1.2.10 Example for configuring user management

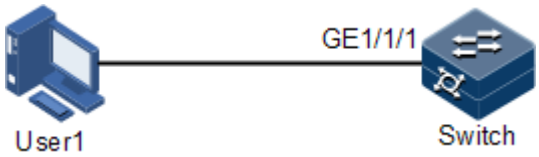
Networking requirements

As shown in Figure 1-5, to prevent malicious users from logging in to the ISCOM2600G series switch and to eliminate risks on the ISCOM2600G series switch, configure user management as below:

- Configure the user login mode to local-user.
- Create a local user user1 with plain password of aaAA123@.
- Configure the user1 privilege to privilege 10.
- Configure the user1 service type to Telnet.

Copyright © Raisecom Technology Co., Ltd.

Figure 1-5 User management networking



Configuration steps

Step 1 Configure user login authentication mode.

```
Raisecom#user login local-user
```

Step 2 Create a local user user1.

```
Raisecom#user name user1 password simple aaAA123@
```

Step 3 Configure the user privilege.

```
Raisecom#user user1 privilege 10
```

Step 4 Configure the service type of the user.

```
Raisecom#no user user1 service-type all
Raisecom#user user1 service-type telnet
```

Checking results

Use the **show user table detail** command to show configurations of local users.

```
Raisecom#show user table detail
Default Login:local-user

Username:raisecom
Priority:15
Server:Local
Login   :console
Status  :online
Service type: telnet
User State  :active

Username:user1
```


Copyright © Raisecom Technology Co., Ltd.

```
Priority:10
Server:Local
Login   :--
Status  :offline
Service type:console telnet ssh web lan-access
User State  :active
```

Use the newly-created user name user1 and password aaAA123@ to log in to the ISCOM2600G series switch, and check whether the user privilege is correctly configured.

```
Login:user1
Password:

Raisecom#config
Raisecom(config)#arp 192.168.0.2 000E.5E12.3456
Set successfully.
```

To delete the default raisecom account, use the following command:

```
Raisecom#no username raisecom
```

1.2.11 Example for configuring SSH login

Networking requirements

As shown in Figure 1-6, when a user logs in to the switch remotely from a PC through an insecure network, you must configure SSH Server and RSA authentication on the switch to guarantee security of data exchange to the maximum extent, with detailed requirements as below:

- Configure the SSH authentication timeout to 400s and allowed authentication failure times to 3.
- Configure the public key name of SSH authentication to raisecom and mode to rsa-key.
- Configure the name for SSH login to the default name raisecom.

Figure 1-6 Configuring SSH login

Copyright © Raisecom Technology Co., Ltd.

Configuration steps

Step 1 Configure a routing protocol to make the route between the switch and PC available.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 172.16.70.134
Raisecom(config-vlan1)#exit
```

Step 2 Generate a local SSH key pair, and enable SSH Server.

```
Raisecom(config)#generate ssh-key
Raisecom(config)#ssh2 server
```

Step 3 Configure the SSH authentication timeout to 400s and allowed authentication failure times to 3.

```
Raisecom(config)#ssh2 server authentication-timeout 400
Raisecom(config)#ssh2 server authentication-retries 3
```

Step 4 Generate a SSH key pair for login, including the server public key and server private key. Save the server private key on the SSH client. This step is performed in a terminal emulation program, such as SecureCRT.

Step 5 Write the server public key of the client to the switch. Copy the server public key generated in step 4, paste it in the terminal emulation program, and press **Ctrl+S** to save the public key.

```
Raisecom(config)#ssh2 server authentication raisecom public-key
(Ctrl+s) for save input and return
(Ctrl+z) for discard input and return.
-------------------------------------------------------------.
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCwMf+rJOF3cccsbU9NnVSVKqlvvFDOJqYX
kwvMIzCmz1qKhhbguUxHTPnuuOyLbA9Yz+AFeaCdWxxdKvNCFXBJvu2pHjTZcJxm
cThqD3kvvRKnR3BjV9HioBjGHPO1gni2Bqc1z91/RoZ6oaNoQfN885SgwigbGt6K
eei/I8pJgQ==
```

Step 6 Configure the SSH authentication mode to rsa-key.

```
Raisecom(config)#ssh server authentication rsa-key
```

Step 7 Establish a SSH session. Log in to the switch in SSH mode.

Copyright © Raisecom Technology Co., Ltd.

Checking results

Use the following command to view configurations of SSH Server.

```
Raisecom#show ssh2 server
SSH server information:
------------------------
State:   Enable
Version:  sshv2
Authentication method(default:local user-password ):  rsa-key
Authentication timeout(default 600):               400s
Authentication retries(default 20):                3
Rekey interval time(default 0):                   0h
Max client count(default 10):                     10
Current client count:                            0
Current channel count:                           0
Listen port on (default 22):                      22
```

Use the following command to view the SSH public key.

```
Raisecom#show ssh2 public-key
RSA public key :
---- BEGIN SSH PUBLIC KEY ----
Comment: "rsa-key"
AAAAB3NzaC1yc2EAAAADAQABAAAAQwDG0mZvhPtWd5zo6naC6Vrz4cK4QEoj
01+WlD94RmPyF/atwjzH0jQOB63J3tg/vcazH2nNVG3jwu912u1cuYTsZWE=
Fingerprint: md5 b6:1b:e8:88:73:1b:11:a9:af:9f:7b:e6:08:b8:b8:9c
---- END SSH PUBLIC KEY ----


Authentication public key :
---- BEGIN SSH PUBLIC KEY ----
Comment: "rsa-key"

Public-key name: raisecom
Public-key:
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCwMf+rJOF3cccsbU9NnVSVKqlvvFDO
JqYXkwvMIzCmz1qKhhbguUxHTPnuuOyLbA9Yz+AFeaCdWxxdKvNCFXBJvu2p
HjTZcJxmcThqD3kvvRKnR3BjV9HioBjGHPO1gni2Bqc1z91/RoZ6oaNoQfN8
85SgwigbGt6Keei/I8pJgQ==

---- END SSH PUBLIC KEY ----
```

Use the following command to view information about the SSH session. SSH session 1 is established.

```
Raisecom#show ssh2 session
ID  Ver  Cipher(IN/OUT)      Auth-Type        Con-Time    State
UserId    Ip
```


Copyright © Raisecom Technology Co., Ltd.

```
-----------------------------------------------------------------------
 1  2.0  aes/aes   rsa   0h:0m:23s   OK(1channels)   raisecom  172.16.70.110
 2  --   --/--            --             --        Closed        --
--
 3  --   --/--            --             --        Closed        --
--
 4  --   --/--            --             --        Closed        --
--
 5  --   --/--            --             --        Closed        --
--
 6  --   --/--            --             --        Closed        --
--
 7  --   --/--            --             --        Closed        --
--
 8  --   --/--            --             --        Closed        --
--
 9  --   --/--            --             --        Closed        --
--
 10 --   --/--            --             --        Closed        --
--
```

1.3 File management

1.3.1 Managing BootROM files

In Boot mode, you can do the following operations.

Operation	Description
t	Update system software to the ISCOM2600G series switch.
m	Update the boot file to the ISCOM2600G series switch.
b	Read system software from the ISCOM2600G series switch, and load it.
s	Specify the sequence of system software to be loaded upon startup.
e	Clear environment variables.
r	Restart the ISCOM2600G series switch.
p	Configure the BootROM password.
?/h	Show information about system files and help.

Configure the ISCOM2600G series switch as below.

All the following steps are optional and in any sequence.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**upload bootstrap** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*] **Example:** Raisecom#upload bootstrap tftp 10.1.1.1 config	(Optional) upload the BootROM file through FTP, SFTP, or TFTP. • bootstrap: upload the bootstrap file. • tftp: upload the file through TFTP. • ftp: upload the file through FTP. • sftp: upload the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the server • password: password of the server • file-name: name of the uploaded file • dir: file path
2	Raisecom#**download bootstrap** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password* [**unit** *unit-id*] *file-name* | **tftp** { *ipv4-address* | *ipv6-address* } [**unit** *unit-id*] *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password* [**unit** *unit-id*] *file-name* } [*dir*] **Example:** Raisecom#download bootstrap tftp 10.1.1.1 config	(Optional) download the BootROM file through FTP, SFTP, or TFTP. • bootstrap: download the bootstrap file. • tftp: upload the file through TFTP. • ftp: upload the file through FTP. • sftp: upload the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the server • password: password of the server • file-name: name of the downloaded file • dir: file path • unit-id: specified unit ID, an integer, ranging from 1 to 9
3	Raisecom#**erase** *file-name* **Example:** Raisecom#erase text	(Optional) delete files saved in the Flash. • file-name: file name. If you do not configure the parameter, the startup configuration file startup_config.conf will be deleted by default.
4	Raisecom#**bootrom password** *word* **Example:** Raisecom#bootrom password raisecom	(Optional) configure the BootROM password. • word: BootROM password, a string of characters

1.3.2 Managing system files

System files are the files needed for system operation (such as system startup software and configuration file). These files are usually saved in the memory. The ISCOM2600G series switch manages them through a file system to facilitate managing the memory. The file system can create, delete, and modify the file and directory.

In addition, the ISCOM2600G series switch supports dual-system. There are 2 independent sets of system software saved at the memory. When the ISCOM2600G series switch fails to work due to upgrade failure, you can use the other set to boot the ISCOM2600G series switch.

Manage system files for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Raisecom#**download system-boot** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password* [**unit** *unit-id*] *file-name* | **tftp** { *ipv4-address* | *ipv6-address* } [**unit** *unit-id*] *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password* [**unit** *unit-id*] *file-name* } [**system1.z** | **system2.z**] **Example:** Raisecom#download system-boot tftp 10.1.1.1 config	(Optional) download the system boot file through FTP, SFTP, or TFTP to the device. • tftp: download the file through TFTP. • ftp: download the file through FTP. • sftp: download the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the server • password: password of the server • file-name: name of the downloaded file • unit-id: specified unit ID, an integer, ranging from 1 to 9
2	Raisecom#**erase** *file-name* **Example:** Raisecom#erase text	(Optional) delete files saved in the Flash. • file-name: file name. If you do not configure the parameter, the startup configuration file startup_config.conf will be deleted by default.
3	Raisecom#**upload system-boot** { **ftp** { *ipv4-address* |*ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* |*ipv6-address* } *file-name* | **sftp** { *ipv4-address* |*ipv6-address* } *user-name password file-name* } [**system1.z** | **system2.z**] **Example:** Raisecom#upload system-boot tftp 10.1.1.1 config	(Optional) upload the system boot file through FTP, SFTP, or TFTP to the local device. • tftp: upload the file through TFTP. • ftp: upload the file through FTP. • sftp: upload the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the server • password: password of the server • file-name: name of the uploaded file

1.3.3 Managing configuration files

Configuration files are loaded after starting the system; different files are used in different scenarios to achieve different service functions. After starting the system, you can configure the ISCOM2600G series switch and save the configuration files. New configurations will take effect in next boot.

The configuration file has a suffix ".cfg", and can be opened by the text book program in Windows system. The contents are in the following format:

- Be saved in the mode+command format.
- Just keep the non-default parameters to save space (see the command reference manual for default values of configuration parameters).

Copyright © Raisecom Technology Co., Ltd.

- Use the command mode for basic frame to organize commands. Put parameters of one mode together to form a section, and the sections are separated by the exclamation mark (!).

The ISCOM2600G series switch starts initialization by reading configuration files from the memory after being powered on. Thus, the configurations in configuration files are called the default configurations. If there is no configuration file in the memory, the ISCOM2600G series switch uses the default parameters for initialization.

The configuration that is currently used by the ISCOM2600G series switch is called the running configuration.

You can modify the running configuration of ISCOM2600G series switch through CLI. The running configuration can be used as initial configuration upon next power-on. You must use the **write** command to save running configurations in the memory and form a configuration file.

Manage configuration files for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**download startup-config** { **ftp** { *ipv4-address* |*ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* |*ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } } [*dir*] **Example:** Raisecom#download startup-config tftp 10.1.1.1 config	(Optional) download the startup configuration file through FTP, SFTP, or TFTP. • tftp: download the file through TFTP. • ftp: download the file through FTP. • sftp: download the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the server • password: password of the server • file-name: name of the downloaded file • dir: file path
2	Raisecom#**download backup-config** { **ftp** { *ipv4-address* |*ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* |*ipv6-address* } *file-name* | **sftp** { *ipv4-address* |*ipv6-address* } *user-name password file-name* } [*dir*] **Example:** Raisecom#download backup-config tftp 10.1.1.1 config	(Optional) download the backup configuration file through FTP, SFTP, or TFTP. • backup-config: backup configuration file • tftp: download the file through TFTP. • ftp: download the file through FTP. • sftp: download the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the server • password: password of the server • file-name: name of the downloaded file • dir: file path

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom#**download dhcplease** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*] **Example:** Raisecom#download dhcplease tftp 10.1.1.1 config	(Optional) download the DHCP lease file through FTP, SFTP, or TFTP. • tftp: download the file through TFTP. • ftp: download the file through FTP. • sftp: download the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the server • password: password of the server • file-name: name of the downloaded file • dir: file path
4	Raisecom#**download dhcpsnooping-binding** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*] **Example:** Raisecom#download dhcpsnooping-binding tftp 10.1.1.1 config	(Optional) download the DHCP Snooping binding table file through FTP, SFTP, or TFTP. • tftp: download the file through TFTP. • ftp: download the file through FTP. • sftp: download the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the server • password: password of the server • file-name: name of the downloaded file • dir: file path
5	Raisecom#**erase** *file-name* **Example:** Raisecom#erase text	(Optional) delete files saved in the Flash. • file-name: file name. If you do not configure the parameter, the startup configuration file startup_config.conf will be deleted by default.
6	Raisecom#**upload startup-config** { **ftp** { *ipv4-address* |*ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* |*ipv6-address* } *file-name* | **sftp** { *ipv4-address* |*ipv6-address* } *user-name password file-name* } } [*dir*] **Example:** Raisecom#upload startup-config tftp 10.1.1.1 config	(Optional) upload the startup configuration file through FTP or TFTP. • backup-config: backup configuration file • tftp: upload the file through TFTP. • ftp: upload the file through FTP. • sftp: upload the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the server • password: password of the server • file-name: name of the uploaded file • dir: file path

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
7	Raisecom#**upload backup-config** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*] **Example:** Raisecom#upload backup-config tftp 10.1.1.1 config	(Optional) upload the backup configuration file through FTP, SFTP, or TFTP. • backup-config: backup configuration file • tftp: upload the file through TFTP. • ftp: upload the file through FTP. • sftp: upload the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the FTP server • password: password of the FTP server • file-name: name of the uploaded file • dir: file path
8	Raisecom#**upload command-log** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*] **Example:** Raisecom#upload command-log tftp 10.1.1.1 config	(Optional) upload the command line logging file and system logs through FTP, SFTP, or TFTP. • command-log: command line logging file • tftp: upload the file through TFTP. • ftp: upload the file through FTP. • sftp: upload the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the server • password: password of the server • file-name: name of the uploaded file • dir: file path
9	Raisecom#**upload logging-file** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*] **Example:** Raisecom#upload logging-file tftp 10.1.1.1 config	(Optional) upload the system log file through FTP, SFTP, or TFTP. • Logging-file: syslog file • tftp: upload the file through TFTP. • ftp: upload the file through FTP. • sftp: upload the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the FTP server • password: password of the FTP server • file-name: name of the uploaded file • dir: file path

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
10	Raisecom#**upload running-config** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*] **Example:** Raisecom#upload running-config tftp 10.1.1.1 config	(Optional) upload the running configuration file through FTP, SFTP, or TFTP. • running-config: running configuration file • tftp: download the file through TFTP. • ftp: download the file through FTP. • sftp: download the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the server • password: password of the server • file-name: name of the uploaded file • dir: file path
11	Raisecom#**upload license** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*] **Example:** Raisecom#upload license tftp 10.1.1.1 config	(Optional) upload the License file through FTP, SFTP, or TFTP. • tftp: upload the file through TFTP. • ftp: upload the file through FTP. • sftp: upload the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the server • password: password of the server • file-name: name of the uploaded file • dir: file path
12	Raisecom#**upload dhcpLease** { **ftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* | **tftp** { *ipv4-address* | *ipv6-address* } *file-name* | **sftp** { *ipv4-address* | *ipv6-address* } *user-name password file-name* } [*dir*] **Example:** Raisecom#upload dhcpLease tftp 10.1.1.1 config	(Optional) upload the DHCP lease file through FTP, SFTP, or TFTP. • tftp: upload the file through TFTP. • ftp: upload the file through FTP. • sftp: upload the file through SFTP. • ipv4-address: IPv4 address of the server • ipv6-address: IPv6 address of the server • user-name: user name of the server • password: password of the server • file-name: name of the uploaded file • dir: file path

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

13	`Raisecom#upload dhcpsnooping-binding { ftp { ipv4-address | ipv6-address } user-name password file-name | tftp { ipv4-address | ipv6-address } file-name | sftp { ipv4-address | ipv6-address } user-name password file-name } [ dir ]`
	Example:
	`Raisecom#upload dhcpsnooping-binding tftp 10.1.1.1 config`
		(Optional) upload the DHCP Snooping binding file through FTP, SFTP, or TFTP.
		• tftp: upload the file through TFTP.
		• ftp: upload the file through FTP.
		• sftp: upload the file through SFTP.
		• ipv4-address: IPv4 address of the server
		• ipv6-address: IPv6 address of the server
		• user-name: user name of the server
		• password: password of the server
		• file-name: name of the uploaded file
		• dir: file path

14	`Raisecom#write`	(Optional) save the running configuration file in the Flash.

1.3.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show startup-config`	Show configurations loaded upon device startup.
2	`Raisecom#show running-config`	Show running configurations.
3	`Raisecom#show backup-config`	Show backup configurations upon device startup.

1.3.5 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description

`Raisecom#write [ backup-config ]`
Example:
`Raisecom#write backup-config`
	Save running configurations as a startup configuration file which can take effect upon next startup.
	• backup-config: save running configurations as a backup configuration file.
	Caution
	When you save running configurations as a startup configuration file, the file will overwrite the original startup configuration file; therefore back up the original one in advance.

Copyright © Raisecom Technology Co., Ltd.

Command	Description
`Raisecom#dir`	Show names of system files. You can view the remaining size of the Flash.

`Raisecom#erase [ file-name | backup-config ]`
Example:
`Raisecom#erase text`
	Delete a specified system file. If the file-name parameter is not configured, this configuration will delete the startup configuration file.
	• file-name: file name. If you do not configure the parameter, the startup configuration file startup_config.conf will be deleted by default.
	• backup-config: backup configuration file
	Caution
	After a file is deleted through this command, it cannot be restored. Use this command with caution.

`Raisecom(config)#syslog save`	Save log files.
`Raisecom#startup-config write`	Save configurations.

1.4 Loading and upgrade

1.4.1 Introduction

Loading

Traditionally, configuration files are loaded through the serial interface, which takes a long time due to low rate and unavailable remote loading. FTP and TFTP loading modes can solve those problems and make operation more convenient.

The ISCOM2600G series switch supports TFTP auto-loading mode.

TFTP auto-loading refers that you can obtain the configuration files from a server and then configure the ISCOM2600G series switch. Auto-loading allows configuration files to contain loading related commands for multiple configurations loading to meet file auto-loading requirements in complex network environment.

The ISCOM2600G series switch provides several methods to confirm configuration file name on the TFTP server, such as manually entering, obtaining through DHCP, and using default name of the configuration file. Besides, you can assign certain naming conventions for configuration files, and then the ISCOM2600G series switch confirms the name according to naming conventions and its attributes (device type, MAC address, software version, and so on).

Upgrade

The ISCOM2600G series switch needs to be upgraded if you want to add new features, optimize functions, or fix bugs in the current software version.

Copyright © Raisecom Technology Co., Ltd.

The ISCOM2600G series switch supports the following two upgrade modes:

- Upgrade through BootROM
- Upgrade through CLI

Note

We recommend upgrading the BootROM under instructions of professional technical engineers.

1.4.2 Upgrading system software through BootROM

You need to upgrade system software through BootROM under the following conditions:

- A system file is damaged.
- The card is started improperly.

Before upgrading system software through BootROM, you should establish a TFTP environment, and use the PC as the TFTP server and the ISCOM2600G series switch as the client. Basic requirements are as below.

- Configure the TFTP server. Ensure that the TFTP server is available.
- Configure the IP address of the TFTP server; keep it in the same network segment with that of the ISCOM2600G series switch.
- Connect the Ethernet interface on the TFTP server to the SNMP interface on the ISCOM2600G series switch. The default IP address of the SNMP interface is 192.168.0.1 by default.

Upgrade system software through BootROM for the ISCOM2600G series switch as below.

Step	Operation
1	Log in to the ISCOM2600G series switch through serial interface as the administrator, enter Privileged EXEC mode, and restart the ISCOM2600G series switch with the **reboot** command. `Raisecom#reboot`

2	When the system successfully loads the big BootROM, and it displays "Press space to enter big boot menu", press **Space bar** to enter the interface starting with [raisecom]. The command list is displayed as below:
	
	`BOOT`
	`**********`
	`t: Update system from tftp.`
	`m: Update boot from tftp.`
	`b: Boot system from flash.`
	`e: Erase bootline para.`
	`s: Select system image to boot.`
	`p: Password setting.`
	`r: Reboot.`
	`?/h: Help menu.`
	`[Raisecom]:`

Copyright © Raisecom Technology Co., Ltd.

Step	Operation

3	Type "t" to upgrade system software to the ISCOM2600G series switch.
	
	`[Raisecom]:t`
	`ipaddr: 192.168.5.100`
	`serverip: 192.168.5.1`
	`filename: uImage`
	
	`Current system partiton info:`
	`Partition number  Name  Size`
	`----------`
	`1  iscom2600_image  16320072`
	`2  None  0`
	
	`Please input system partition number for upgrading(1-2):1`

4	Type "r" to rapidly execute the big BootROM file. The ISCOM2600G series switch is restarted and will load the downloaded startup file.

1.4.3 Upgrading system software through CLI

Before upgrading system software through CLI, you should establish a TFTP environment, and use a PC as the TFTP server and the ISCOM2600G series switch as the client. Basic requirements are as below.

- Connect the Ethernet interface on the TFTP server to the SNMP interface on the ISCOM2600G series switch. The default IP address of the SNMP interface is 192.168.0.1 by default.
- Configure the TFTP server, and ensure that the server is available.
- Configure the IP address of the TFTP server; keep it in the same network segment with that of the ISCOM2600G series switch so that the ISCOM2600G series switch can access the TFTP server.

Upgrade system software through CLI for the ISCOM2600G series switch as below.

Step	Command	Description

1	`Raisecom#download system-boot { ftp { ipv4-address | ipv6-address } user-name password file-name | tftp { ipv4-address | ipv6-address } file-name | sftp { ipv4-address | ipv6-address } user-name password file-name } [ system1.z | system2.z ]`
	Example:
	`Raisecom#download system-boot tftp 10.10.10.1 config`
		Download the system boot file through FTP, SFTP, or TFTP. This command supports the IPv6 address.
		• system-file: system boot file
		• tftp: download the file through TFTP.
		• ftp: download the file through FTP.
		• sftp: download the file through SFTP.
		• ipv4-address: IPv4 address of the server
		• ipv6-address: IPv6 address of the server
		• user-name: user name of the server
		• password: password of the server
		• file-name: name of the downloaded file
		• unit-id: specified unit ID, an integer, ranging from 1 to 9

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	`Raisecom#boot sequence`	(Optional) configure the sequence for loading system software.

3	`Raisecom#reboot [ now | in time ]`
	Example:
	`Raisecom#reboot now`
		Restart the ISCOM2600G series switch, and it will automatically load the downloaded system boot file.
		• now: immediately restart the device without confirmation.
		• in: restart the device after a specified period.
		• time: delay period for restarting the device, an integer, ranging from 1 to 1440, in units of minute

1.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show startup-config`	Show information about the startup configuration file.
2	`Raisecom#show running-config`	Show information about the running configuration file.
3	`Raisecom#show version`	Show system version.

1.5 Time management

1.5.1 Introduction

With development and extension of Internet in all aspects, multiple applications involved in time need accurate and reliable time, such as online realtime transaction, distributed network calculation and processing, transport and flight management, and data management.

To ensure precise system time, the ISCOM2600G series switch provides complete time management functions, including manually configuring system time and time zone, manually configuring Daylight Saving Time (DST), Network Time Protocol (NTP), and Simple Network Time Protocol (SNTP).

Time and time zone

The device time is usually configured to the local time of the device while the time zone is configured to the local time zone based on Greenwich Mean Time (GMT) (for example, China Beijing is in the eastern eight zone based on GMT, so its time zone is configured to +08:00).

Copyright © Raisecom Technology Co., Ltd.

The ISCOM2600G series switch supports displaying time in the format of "year-month-day hour:minute:second" and offset of the time zone. You can manually configure the time and time zone of the ISCOM2600G series switch.

DST

DST is a kind of artificially regulated local time system for saving energy. Time is usually advanced one hour in summer to make people sleep early and rise early to save energy, but different countries have different stipulations for DST. In this case, you should consider local conditions when configuring DST.

The ISCOM2600G series switch supports configuring the start time, end time, offset of the DST.

NTP

Network Time Protocol (NTP) is a standard Internet protocol for time synchronization, used to synchronize time between the distributed time servers and clients. NTP transmits data based on UDP, using UDP port 123 and guaranteeing high precision (error around 10ms).

Figure 1-7 shows basic principles of NTP. Clock synchronization works as below:

Step 1 Switch A sends Switch B a NTP message which carries the timestamp of leaving Switch A. The timestamp is 10:00:00am and recorded as t1.

Step 2 When the message reaches Switch B, it is added with the timestamp of reaching Switch B, which is 11:00:01am and recorded as t2.

Step 3 When the message leaves Switch B, it is added with the timestamp of leaving Switch B, which is 11:00:02am and recorded as t3.

Step 4 When switch A receives the response message, it adds a new timestamp, which is 11:00:03am and recorded as t4.

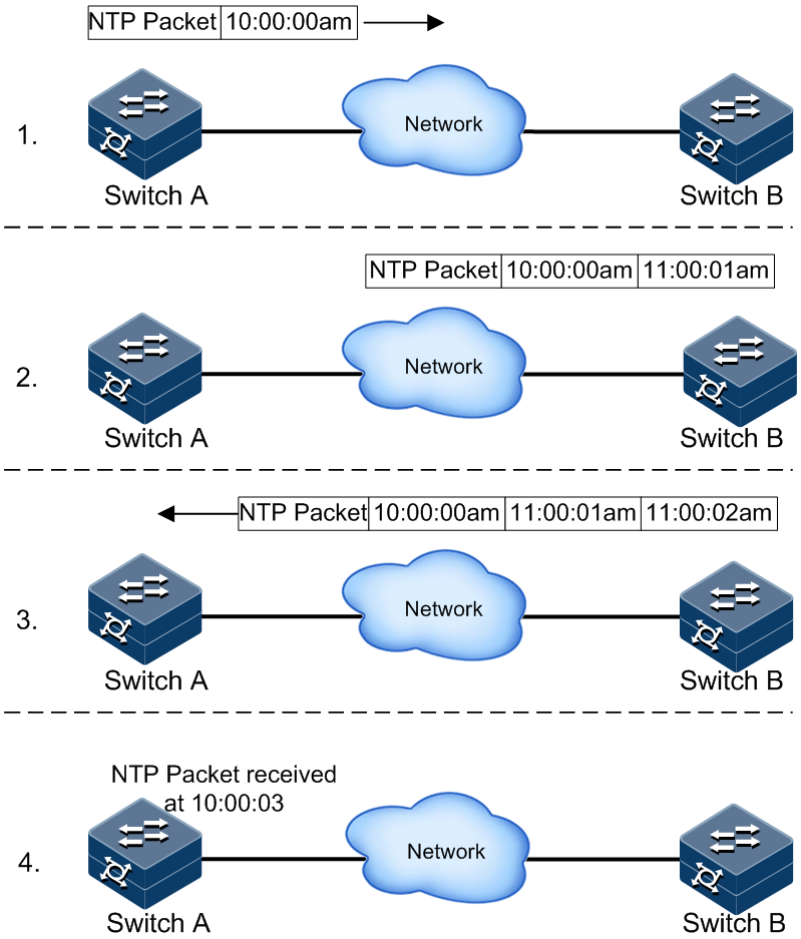
At present, Switch A has enough information to calculate two important parameters:

- Round-trip delay of the NTP message: delay = (t4 - t1) - (t3 - t2)
- Time offset between Switch A and Switch B: offset = ((t2 - t1) + (t3 - t4))/2

Switch A configures its clock based on previous two parameters to synchronize clock with Switch B.

Copyright © Raisecom Technology Co., Ltd.

Figure 1-7 Basic principles of NTP



The ISCOM2600G series switch adopts multiple NTP working modes for time synchronization:

- Client/Server mode

In this mode, the client sends clock synchronization messages to different servers. The servers work in server mode automatically after receiving the synchronization message and sending response messages. The client receives response messages, performs clock filtering and selection, and is synchronized to the preferred server.

In this mode, the client can be synchronized to the server but the server cannot be synchronized to the client. The ISCOM2600G series switch can work as a client or server.

- Symmetric mode

In this mode, you can configure the passive peer on the active peer. The active peer sends a clock synchronization message to the passive peer. The passive peer works in passive mode automatically after receiving the message and sends the answering message back. By exchanging messages, the two peers establish the symmetric peer mode. The peer with fewer stratum synchronizes time with the one with more stratum. The active and passive peers in this mode can synchronize each other.

Copyright © Raisecom Technology Co., Ltd.

SNTP

Simple Network Time Protocol (SNTP) is used to synchronize the system time of the ISCOM2600G series switch to the GMT and transmit the GMT to local time according to the system settings of time zone. When the SNTP client and server are in different time zones, the SNTP client will be synchronized to the GMT and then translated into the local time according to system settings of time zone.

The SNTP client obtains time in two modes: actively sending a request packet or passively monitoring the packet. They are implemented as below:

- Unicast mode: the SNTP client actively sends a request packet. After being configured with the IP address of the SNTP unicast server, the device tries to obtain clock signals every 10s from the SNTP server. The maximum timeout for obtaining clock signals from the SNTP server is 60s.
- Multicast or broadcast mode: SNTP client passively monitors the packet.
  - After being configured to multicast mode, the device monitors the multicast IP address of 224.0.1.1 in real time and obtain clock signals from the SNTP multicast server. The maximum timeout for obtaining clock signals from the SNTP server is 60s.
  - After being configured to broadcast mode, the device monitors the broadcast IP address of 255.255.255.255 in real time and obtain clock signals from the SNTP broadcast server. The maximum timeout for obtaining clock signals from the SNTP server is 60s.

1.5.2 Preparing for configurations

Scenario

Configure the system time of the ISCOM2600G series switch, and guarantee precision of the system time.

- The time and time zone that is manually configured take effect immediately.
- After NTP or SNTP is enabled, the synchronized time will override the current system time after a synchronization period.
- NTP and SNTP are mutually exclusive, so they cannot be concurrently configured.

Prerequisites

N/A

1.5.3 Default configurations of time management

Time and time zone

Default configurations of time and time zone are as below.

Function	Default value
Time zone offset	+08:00-CCT
Display mode of the system clock	Default

Copyright © Raisecom Technology Co., Ltd.

Note

China Coast Time (CCT) is the standard time code. Several countries define their local time by reference to GMT by advancing or adjusting backward several hours on the basis of GMT and their longitudes or time zones. To be convenient, establish a series of standard time codes, including:

- China Coast Time (CCT): GMT +8:00
- Eastern Daylight Time (EDT): GMT +4:00
- Eastern Standard Time (EST): GMT +5:00
- Central Daylight Time (CDT): GMT -5:00
- Central Standard Time (CST): GMT -6:00
- Mountain Daylight Time (MDT): GMT -6:00
- Mountain Standard Time (MST): GMT -7:00
- Pacific Daylight Time (PDT): GMT -7:00
- Pacific Standard Time (PDT): GMT -8:00

DST

Default configurations of DST are as below.

Function	Default value
DST status	Disable

NTP

Default configurations of NTP are as below.

Function	Default value
Whether the device is NTP master clock	No
Global NTP server	Inexistent
Global NTP equity	Inexistent
Reference clock source	0.0.0.0
Identity authentication	Disable
Identity authentication key ID	N/A
Trusted key	N/A

SNTP

Default configurations of SNTP are as below.

Function	Default value
IP address of the SNTP server	N/A

Copyright © Raisecom Technology Co., Ltd.

1.5.4 Configuring time and time zone

Configure the time and time zone for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**clock set** *hour minute second year month day* **Example:** Raisecom#clock set 8 0 0 2013 1 1	Configure the system time. • hour: hour, an integer, ranging from 0 to 23 • minute: minute, an integer, ranging from 0 to 59 • second: second, an integer, ranging from 0 to 59 • year: year, an integer, ranging from 2000 to 2037 • month: month, an integer, ranging from 1 to 12 • day: day, an integer, ranging from 1 to 31
2	Raisecom#**clock timezone** { **+** | **-** } *hour minute timezone-name* **Example:** Raisecom#clock timezone – 5 40 CCT	Configure the local time zone. • +: time zones in the Eastern Hemisphere • -: time zones in the Western Hemisphere • Hour: time zone offset hour, an integer, ranging from 0 to 11 • Minute: time zone offset minute, an integer, ranging from 0 to 59 • timezone-name: time zone name, a string of 1 to 7 characters
3	Raisecom#**clock display** { **default** | **utc** } **Example:** Raisecom#clock display utc	Configure the system clock display mode. • Default: default mode • utc: UTC mode

1.5.5 Configuring DST

Configure DST for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**clock summer-time { enable | disable }** **Example:** Raisecom#clock summer-time enable	Enable or disable DST. • enable: enable DST. • disable: disable DST.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom#**clock summer-time recurring** { *start-week* | **last** } { **sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat** } *start-month hour minute* { *end-week* | **last** } { **sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat** } *end-month hour minute offset* **Example:** Raisecom#clock summer-time recurring 2 sun 4 2 0 2 sun 9 2 0 60	Configure calculation period for system DST. • start-week: week when DST begins, an integer, ranging from 1 to 4 • last: DST begins or ends in the last week of a month. • sun: DST begins or ends on Sunday of a week. • mon: DST begins or ends on Monday of a week. • tue: DST begins or ends on Tuesday of a week. • wed: DST begins or ends on Wednesday of a week. • thu: DST begins or ends on Thursday of a week. • fri: DST begins or ends on Friday of a week. • sat: DST begins or ends on Saturday of a week. • start-month: month when DST begins, an integer, ranging from 1 to 12 • hour: hour when DST begins or ends, an integer, ranging from 0 to 23 • minute: minute when DST begins or ends, an integer, ranging from 0 to 59 • end-week: week of the month when : DST ends, an integer, ranging from 1 to 4 • end-month: month when DST ends, an integer, ranging from 1 to 12 • offset: time offset of DST, an integer, ranging from 1 to 1440, in units of second **Note** Underlined command lines indicate the termination DST.

Note

- When you configure system time manually, if the system uses DST, such as DST from 2 A.M. on the second Sunday, April to 2 A.M. on the second Sunday, September every year, you have to adjust the clock one hour forward during this period, configure time offset as 60 minutes, and the period from 2 A.M. to 3 A.M. on the second Sunday, April each year is inexistent. The time setting by manual operation during this period shows failure.
- The summer time in southern hemisphere is opposite to the northern hemisphere, which is from September to April of next year. If you configure the start time later than the end time, the system will suppose that it is in the Southern Hemisphere. In other words, the summer time is from the start time this year to the ending time of next year.

1.5.6 Configuring NTP

Configure NTP for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**ntp server** { *ipv4-address* | *ipv6-address* } [**version** *version-number*] [**key** *key-id*] **Example:** Raisecom(config)#ntp server 10.0.0.1	(Optional) configure the IP address of the NTP server for the client working in client/server mode. • ipv4-address: IP address of the remote peer, in dotted decimal notation, such as 10.10.1.1 • ipv6-address: IPv6 address of the remote peer, in colon decimal notation, such as 2001::3 • version-number: version number, the value is v1, v2, v3, or v4. • key key-id: key ID, an integer, ranging from 1 to 4294967295
3	Raisecom(config)#**ntp peer** { *ipv4-address* | *ipv6-address* } [**version** *version-number*] [**key** *key-id*] **Example:** Raisecom(config)#ntp peer 10.0.0.1	(Optional) configure the IP address of the NTP peer for the ISCOM2600G series switch working in symmetric peer mode. • ipv4-address: IP address of the remote peer, in dotted decimal notation, such as 10.10.1.1 • ipv6-address: IPv6 address of the remote peer, in colon decimal notation, such as 2001::3 • version-number: version number, the value is v1, v2, v3, or v4. • key key-id: key ID, an integer, ranging from 1 to 4294967295
4	Raisecom(config)#**ntp refclock-master** [*ip-address*] [*stratum*] **Example:** Raisecom(config)#ntp refclock-master	Configure the clock of the ISCOM2600G series switch as the NTP reference clock source for the ISCOM2600G series switch. • ip-address: IP address of the local reference clock, in dotted decimal notation, with IP address ranging from 127.127.1.0 to 127.127.1.2. Take the local clock as the NTP master clock. The defaulted value should be local clock 127.127.1.0 if the parameter is not configured. • stratum: the layer of the tree-type NTP network topology in which the device is, ranging from 2 to 15. The lower the layer is, the more accurate the clock is. The default value is 8 if the parameter is not configured.

Note

If the ISCOM2600G series switch is configured as the NTP reference clock source, it cannot be configured as the NTP server or NTP symmetric peer; vice versa.

Configuring NTP identity authentication

A network with high requirements for security requires identity authentication when NTP is used. After enabled with identity authentication, a NTP client synchronizes with the NTP server that passes identity authentication, thus guaranteeing network security. Only after the NTP client is enabled with identity authentication can it authenticate the NTP server. If it is disabled with identity authentication, it will directly synchronize time with the NTP server without authentication regardless of that the NTP server carries key information.

Copyright © Raisecom Technology Co., Ltd.

Configure NTP identity authentication for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#ntp authenticate { enable | disable }`
	Example:
	`Raisecom(config)#ntp authenticate enable`
		Enable identity authentication on the NTP client/server.
		• enable: enable identity authentication.
		• disable: disable identity authentication.

3	`Raisecom(config)#ntp authentication-keyid key-id md5 password`
	Example:
	`Raisecom(config)#ntp authentication-keyid 1 md5 atestkey`
		Configure the key ID and key password for identity authentication on the NTP client/server.

4	`Raisecom(config)#ntp trust-keyid key-id`
	Example:
	`Raisecom(config)#ntp trust-keyid 1`
		Configure the key ID for identity authentication on the NTP client/server as a trusted ID.
		Note
		Only after the NTP client is enabled with identity authentication can it authenticate the NTP server, and can it synchronize time with the NTP server that provides a trusted key.

1.5.7 Configuring SNTP

Configuring unicast feature of SNTP client

Configure unicast feature of SNTP client for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#sntp server { ipv4-address | ipv6-address } [ version version-number ]`
	Example:
	`Raisecom(config)#sntp server 10.0.0.1`
		Configure the IP address of the SNTP unicast server.
		After the SNTP server is configured with an IP address, the ISCOM2600G series switch tries to get the clock information from the SNTP server every 10s. In addition, the maximum timeout is 60s.
		• ipv4-address: IP address of the server, in dotted decimal notation, such as 10.10.1.1
		• ipv6-address: IPv6 address of the server, in colon decimal notation, such as 2001::3
		• version: SNTP version
		• version-number: version, being v1, v2, v3, or v4

Copyright © Raisecom Technology Co., Ltd.

1.5.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show clock [ summer-time-recurring ]`	Show configurations of the time zone and DST.
2	`Raisecom#show sntp`	Show SNTP configurations.
3	`Raisecom#show ntp status`	Show NTP configurations.
4	`Raisecom#show ntp associations [ detail ]`	Show information about NTP connection.
5	`Raisecom#show ntp authentication`	Show information about NTP identity authentication.

1.5.9 Example for configuring NTP

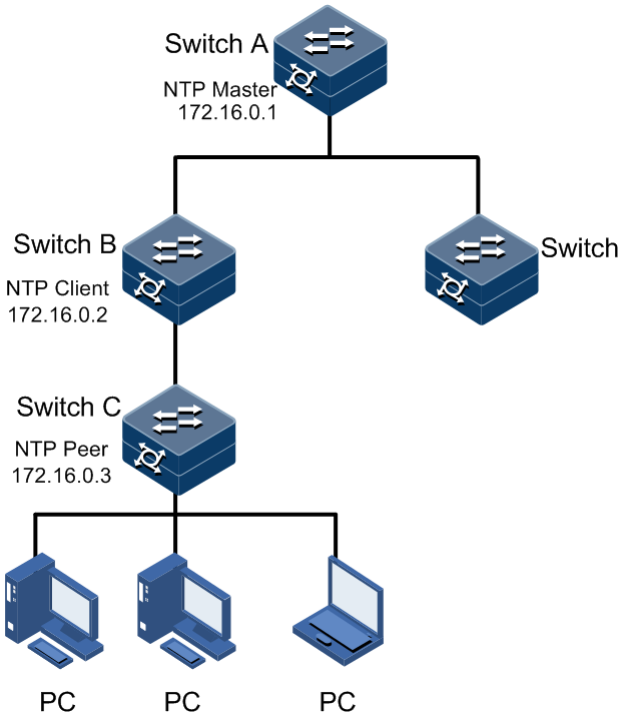
Networking requirements

Establish a clock synchronization system in a company to keep consistency and precision of the system time. Basic planning is as below:

- Configure Switch A as the master clock source of the clock synchronization system.
- Configure Switch B as the client of the clock synchronization system. Configure the upper-layer Switch A as the NTP server.
- Configure Switch C as the NTP entity of Switch B so that Switch C receives downlink synchronization data from Switch B.

Copyright © Raisecom Technology Co., Ltd.

Figure 1-8 NTP networking



Configuration steps

Step 1 Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#ntp refclock-master
```

Step 2 Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#ntp server 172.16.0.1
SwitchB(config)#ntp peer 172.16.0.3
```

Checking results

- Check Switch A.

Use the **show ntp status** command to view configurations of Switch A.

```
SwitchA#show ntp status
Clock status    :synchronized
```


Copyright © Raisecom Technology Co., Ltd.

```
NTP peer      :0.0.0.0
NTP version    :3
NTP mode      :ntpMaster
Leap         :0
Poll         :6
Stratum       :8
Precision      :2**-16
Reference clock :127.127.1.0
Reference time  :00000000.00000000(Thu 1970-01-01,08:00:00)
Current time   :5333d6de.33428f00(Thu 2014-03-27,15:45:44.070)
Root delay     :0.000000
Root dispersion :0.000000
```

- Check Switch B.

Use the **show ntp status** command to view configurations of Switch B.

```
SwitchB#show ntp status
Clock status   :synchronized
NTP peer      :172.16.0.1
NTP version    :3
NTP mode      :ntpSlave
Leap         :0
Poll         :6
Stratum       :9
Precision      :2**-16
Reference clock :172.16.0.1
Reference time  :5333d671.383980f6(Thu 2014-03-27,15:44:58.466)
Current time   :5333d697.0a917f54(Thu 2014-03-27,15:45:58.765)
Root delay     :0.000000
Root dispersion :0.010004
```

Use the **show ntp associations** command to view information about NTP sessions of Switch B.

```
SwitchB#show ntp associations
Server(ip)       refid         stratum  poll  when      delay
offset      dispersion   mode reach
-----------------------------------------------------------------------
----------------------------------------
(s)172.16.0.1   127.127.1.0    8       6    55        0.000000     -
1.965874    14.875517    4   255
Peer(ip)         refid         stratum  poll  when      delay
offset      dispersion   mode reach
-----------------------------------------------------------------------
----------------------------------------
(u)172.16.0.3   0.0.0.0        16      6    125       0.000000
0.000000     16.000000    0   0
```

- Check Switch C.

Use the **show ntp status** command to view configurations of Switch C.

```
Raisecom#show ntp status
Clock status :     synchronized
NTP peer :        172.16.0.2
NTP version :      3
NTP mode :        ntpSlave
Leap :           0
Poll :           6
Stratum :         10
Precision :       2**-22
Reference clock :  172.16.0.2
Reference time :   4d62a905.00000000(Mon 2011-02-22,02:03:49)
Current time :     5333dd97.00000000(Thu 2014-03-27,16:13:11)
Root delay :      4.154726
Root dispersion :  14.034068
```

Use the **show ntp associations** command to view information about NTP sessions of Switch C.

```
Raisecom#show ntp associations
Active(IP)       refid      stratum poll  when      delay       offset
dispersion   mode reach
-------------------------------------------------------------------------
----------------------------------------
(s)172.16.0.2  172.16.0.1         9         6     97596571    4.154726
13447.112484  0.000930     1   6
```

1.6 Interface management

1.6.1 Introduction

Ethernet is a very important LAN networking technology which is flexible, simple, and easy to implement. The Ethernet interface includes the Ethernet electrical interface and Ethernet optical interface.

The ISCOM2600G series switch supports both Ethernet electrical and optical interfaces.

Auto-negotiation

Auto-negotiation is used to make the devices at both ends of a physical link automatically choose the same working parameters by exchanging information. The auto-negotiation parameters include duplex mode, interface rate, and flow control. Once successful in negotiation, the devices at both ends of the link can work in the same duplex mode and interface rate.

Copyright © Raisecom Technology Co., Ltd.

Cable connection

Generally, the Ethernet cable can be categorized as the Medium Dependent Interface (MDI) cable and Medium Dependent Interface crossover (MDI-X) cable. MDI provides physical and electrical connection from terminal to network relay device while MDI-X provides connection between devices of the same type (terminal to terminal). Hosts and routers use MDI cables while hubs and switches use MDI-X interfaces. Usually, the connection of different devices should use the MDI cable while devices of the same type should use the MDI-X cable. Devices in auto-negotiation mode can be connected by the MDI or MDI-X cable.

The Ethernet cable of the ISCOM2600G series switch supports auto-MDI/MDIX.

1.6.2 Default configurations of interface management

Default configurations of interface management are as below.

Function	Default value
Maximum forwarding frame length of interface	2000 bytes
Duplex mode of interface	Auto-negotiation
Interface rate	Auto-negotiation
Interval for monitoring the interface rate	5s
Interface rate statistics status	Disable
Interval of interface dynamic statistics	5s
Interface flow control status	Disable
Interface status	Enable
L2protocol peer stp status	Disable

1.6.3 Configuring basic attributes of interfaces

The interconnected devices cannot communicate normally if their interface attributes (such as MTU, duplex mode, and rate) are inconsistent, and then you have to adjust the interface attributes to make the devices at both ends match each other.

The Ethernet physical layer works in three modes as below:

- Half duplex: devices can receive or send messages at a time.
- Full duplex: devices can receive and send messages concurrently.
- Auto-negotiation: devices can automatically choose duplex mode by exchanging information. Once successful in negotiation, the devices at both ends of the link can work in the same duplex mode, interface rate, and flow control mode.

Configure the basic attributes of interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID. The form and value range depend on the interface type.
3	Raisecom(config-gigaethernet1/1/port)#**duplex** { **full** | **half** | **auto** } **Example:** Raisecom(config-gigaethernet1/1/1)#duplex half	(Optional) configure the duplex mode of the interface. • full: forced full duplex mode • half: forced half duplex mode • auto: auto-negotiation
4	Raisecom(config-gigaethernet1/1/port)#**speed** { **auto** | **10** | **100** | **1000** } **Example:** Raisecom(config-gigaethernet1/1/1)#speed 10	Configure the duplex mode of the interface. The rate of an optical interface also depends on parameters of the optical module. When there is no 10 Gbit/s optical interface on the device, its interface does not support being configured to 10 Gbit/s. • auto: auto-negotiation • 10: forcible 10 Mbit/s • 100: forcible 100 Mbit/s • 1000: forcible 1000 Mbit/s
5	Raisecom(config-gigaethernet1/1/port)#**tpid** { **8100** | **9100** | **88a8** } **Example:** Raisecom(config-gigaethernet1/1/1)#tpid 88a8	(Optional) configure the interface TPID. By default, it is 0x8100. • 8100: configure the TPID to 0x8100. • 9100: configure the TPID to 0x9100. • 88a8: configure the TPID to 0x88a8.
6	Raisecom(config-gigaethernet1/1/port)#**jumboframe** *frame-size* **Example:** Raisecom(config-gigaethernet1/1/1)#jumboframe 2046	(Optional) configure the MTU on the interface. The device supports configuring MTU on interfaces in batches. • frame-size: maximum length of frame, an integer, ranging from 1522 to 12288 bytes, in units of bytes.
7	Raisecom(config-gigaethernet1/1/port)#**mdi** { **xover** | **auto** | **normal** } **Example:** Raisecom(config-gigaethernet1/1/1)#mdi xover	(Optional) configure the MDI/MDIX mode of the electrical interface. • xover: forcible crossover mode • auto: auto-MDI/MDIX mode • normal: forcible straight-through mode
8	Raisecom(config-gigaethernet1/1/port)#**vibration-suppress peroid** *value* **Example:** Raisecom(config-gigaethernet1/1/1)#vibration-suppress period 20	(Optional) configure the period for suppressing vibration on the interface. • value: period for suppressing vibration, an integer, ranging from 1 to 600, in units of second

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

9	`Raisecom(config-gigaethernet1/1/port)#eee { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#eee enable`
		(Optional) enable interface EEE.
		Use the **no** form of this command to disable this function.
		• enable: enable interface EEE.
		• disable: disable interface EEE.

10	`Raisecom(config)#interface tunnel interface-number`
	Example:
	`Raisecom(config)#interface tunnel 1/1/1`
		Create a Tunnel interface.
		• interface-number: the slot is the number of slot which houses the interface, an integer, with the value being 1; the port is the interface ID, an integer, with value ranging from 1 to 100.

11	`Raisecom(config-tunnel1/1/1)#tunnel source ip-address`
	Example:
	`Raisecom(config-tunnel1/1/1)#tunnel source 172.31.128.255`
		Configure the source IP address of the Tunnel interface.
		• ip-address: IP address, in dotted decimal notation, a unicast IP address

12	`Raisecom(config-tunnel1/1/1)#tunnel destination ip-address`
	Example:
	`Raisecom(config-tunnel1/1/1)#tunnel destination 172.31.128.255`
		Configure the destination IP address of the Tunnel interface.
		• ip-address: IP address, in dotted decimal notation, a unicast IP address

13	`Raisecom(config-tunnel1/1/1)#tunnel mode ipv6ip` **Example:** `Raisecom(config-tunnel1/1/1)#tunnel mode ipv6ip`	Configure the encapsulation type of the Tunnel. • ipv6ip: configure the Tunnel type to IPv6 over IPv4.

1.6.4 Configuring interface rate statistics

Configure interface rate statistics for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#dynamic statistics time time-value`
	Example:
	`Raisecom(config)#dynamic statistics time 100`
		(Optional) configure the period for dynamic statistics.
		• time time-value: interval, an integer, ranging from 3 to 300, in units of second

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

3	`Raisecom(config)#interface statistic period value`
	Example:
	`Raisecom(config)#interface statistic period 100`
		(Optional) configure the period for gathering statistics about interfaces.
		• value: interval, an integer, ranging from 3 to 300, in units of second

4	`Raisecom(config)#interface vlan vlan-id`
	Example:
	`Raisecom(config)#interface vlan 1`
		Enter VLAN interface configuration mode.
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094

5	`Raisecom(config-vlan*)#statistics enable`	(Optional) enable interface statistics.
6	`Raisecom(config-vlan*)#clear interface statistics`	Clear statistics about the interface rate.

1.6.5 Configuring flow control on interfaces

IEEE 802.3x is a flow control method for full duplex on the Ethernet data layer. When the client sends a request to the server, it will send the PAUSE frame to the server if there is system or network jam. Then, it delays data transmission from the server to the client.

Configure flow control on interfaces for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID. The form and value range depend on the interface type.

3	`Raisecom(config-gigaethernet1/1/port)#flowcontrol { receive | send } { off | on }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#flowcontrol receive on`
		Enable/Disable interface flow control over 802.3x packets.
		By default, it is disabled.
		• receive: received flow control
		• send: sent flow control
		• off: disable flow control.
		• on: enable flow control.

1.6.6 Shutting down/Restarting interface

Shut down/Restart an interface for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID. The form and value range depend on the interface type.
3	`Raisecom(config-gigaethernet1/1/port)#shutdown`	Shut down the current interface. Use the **no shutdown** command to re-enable the disabled interface.

1.6.7 Configuring Combo interface

Configure the Combo interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/25`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.

3	`Raisecom(config-gigaethernet1/1/port)#medium-priority { copper | fiber }`
	Example:
	`Raisecom(config-gigaethernet1/1/25)#medium-priority fiber`
		(Optional) configure the priority of the Combo interface; in other words, configure the optical interface or electrical interface preferentially to be used. By default, the optical interface prevails.
		• cooper: electrical interface
		• fiber: optical interface

4	`Raisecom(config-tengigabitethernet1/1/port)#medium-type { auto | fiber | copper }`
	Example:
	`Raisecom(config-gigaethernet1/1/25)#medium-type fiber`
		(Optional) configure the mode for selecting the optical interface or electrical interface of the Combo interface.
		• auto: automatic selection mode
		• fiber: forcibly choosing the optical interface
		• copper: forcibly choosing the electrical interface

Note

The previous commands are applicable to the device that has a Combo interface.

1.6.8 Configuring Console interface

Configure the Console interface for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#console open`	(Optional) enable the Console interface. Use this command in non-Console command lines only. **Caution** If you use the **console close** command to disable the Console interface, this will cause the ISCOM2600G series switch to be out of control. Use it with caution.
3	`Raisecom(config)#login-trap enable`	(Optional) enable Trap sending upon user login or exit.

1.6.9 Configuring VLAN interface

Configure the VLAN interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface vlan` *`vlan-id`* **Example:** `Raisecom(config)#interface vlan 1`	Enter VLAN interface configuration mode. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
3	`Raisecom(config-vlan1)#mtu` *`max-frame-length`* **Example:** `Raisecom(config-vlan1)#mtu 1800`	(Optional) configure the maximum transmission unit of the interface. • max-frame-length: maximum framelength, an integer, ranging from 46 to 9600, in units of byte

1.6.10 Configuring SNMP interface

Note

By default, the IP address of the SNMP interface is 192.168.0.1 and the subnet mask is 255.255.255.0.

Configure the SNMP interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface fastethernet 1/0/1`	Enter SNMP interface configuration mode. The device supports shutdown.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-fastethernet1/0/1)#**ip address** *ip-address* [*ip-mask*] **Example:** Raisecom(config-fastethernet1/0/1)#ip address 10.2.2.2	Configure the IPv4 address of the SNMP interface. • ip-address: IP address, in dotted decimal notation, such as 10.0.0.1 • ip-mask: mask of IP address, in dotted decimal notation, such as 255.0.0.0
4	Raisecom(config-fastethernet1/0/1)#**ipv6 address** *ipv6-address/prefix-length* [**eui-64**] Raisecom(config-fastethernet1/0/1)#**ipv6 address** *ipv6-address* **link-local** **Example:** Raisecom(config-fastethernet1/0/1)#ipv6 address 1030:0::48AA:1A2B/60	Configure the IPv6 address of the SNMP interface. • ipv6-address/prefix-length: IPv6 address with prefix length, in form of A:B::C:D/M • ipv6-address: IPv6 address, in colon hexadecimal notation • eui-64: IPv6 local link address. The eui-64 is the interface ID. • link-local: IPv6 local link address
5	Raisecom(config-fastethernet1/0/1)#**ip dhcp server**	(Optional) enable DHCP Server on the SNMP interface.
6	Raisecom(config-fastethernet1/0/1)#**ip dhcp client** { **class-id** *class-id* | **client-id** *client-id* | **hostname** *hostname* } **Example:** Raisecom(config-fastethernet1/0/1)#ip dhcp client hostname myhost	(Optional) configure information about the DHCP client on the SNMP interface, including the class ID, client ID, and host name. • host-name: host name, a string of 1 to 64 characters • class-id: Class-ID, a string of 1 to 64 characters • client-id: Client-ID, a string of 1 to 64 characters
7	Raisecom(config-fastethernet1/0/1)#**ip dhcp client renew**	(Optional) configure the IP address to be renewed for the SNMP interface.

1.6.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show interface** [**range**] [*interface-type interface-number*]	Show the interface status. The device supports showing blocked VLANs.
2	Raisecom#**show interface** *interface-type interface-number* **statistics** [**dynamic**] [**detail**] Raisecom#**show interface statistics dynamic** [**detail**]	Show interface statistics.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
3	`Raisecom#show interface brief`	Show the interface list.
4	`Raisecom#show interface [ interface-type interface-number ] configuration`	Show the interface summary.
5	`Raisecom#show interface [ interface-type interface-number ] description`	Show the interface description.
6	`Raisecom#show port split`	Show the status of interface split.

1.7 Configuring basic information

Configure basic information for the ISCOM2600G series switch as below.

Step	Command	Description

1	`Raisecom#hostname name`
	Example:
	`Raisecom#hostname A`
		(Optional) configure the device name.
		By default, the device name is Raisecom.
		The system supports changing device name to make users distinguish different devices on the network. Once the device name changes, it can be seen in terminal prompt.
		• name: device name, a string of 1 to 64 characters, supporting special characters, such as space, \, ', <, >, &

2	`Raisecom#language { chinese | english }`
	Example:
	`Raisecom#language english`
		(Optional) configure language mode.
		By default, the language is English.
		• english: show descriptions of command lines in English.
		• chinese: show descriptions of command lines in Chinese.

3	`Raisecom#write`	(Optional) save configurations. Save configurations to the ISCOM2600G series switch after configurations, and the new configurations will overwrite the original configurations. If new configurations are not saved, they will be lost after restarting, and the ISCOM2600G series switch will continue to working with the original configurations. **Caution** Use the **erase** *file-name* command to delete the configuration file. This operation cannot be rolled back, so use this command with caution.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom#**reboot** [**now**]	(Optional) configure restart options. When the ISCOM2600G series switch fails, restart it to try to solve the problem according to actual condition.
5	Raisecom#**show** { **assert** | **bootlog** | **exception** | **memory_errors** | **ros_errors** } [**last** [*count*]]	Show displayed information or logs.
6	Raisecom#**clear** [**all** | **assert** | **bootlog** | **exception** | **memory_errors** | **ros_errors**] **Example:** Raisecom#clear exception	Clear displayed information or logs. • all: clear all errored logs. • assert: clear assertion information. • bootlog: clear boot logs. • exception: clear abnormal logs. • memory_errors: clear memory errors. • ros_errors: clear errors.
7	Raisecom#**show loadcfg**	Show cache configurations.
8	Raisecom#**show tech-support**	Show common system information, such as the CPU, memory, terminal connection status, and DDM.
9	Raisecom#**show semaphore** [*semaphore-id*]	Show information about the semaphore on the platform.
10	Raisecom#**show timer** [*timer-id*]	Show timer information.
11	Raisecom#**show twltimer** [*timer-level*]	Show time information on the platform.

Caution

- Restarting the ISCOM2600G series switch interrupts services, so use the command with caution.
- Save configurations before restarting to avoid loss of configurations.

1.8 Task scheduling

1.8.1 Introduction

To use some commands periodically or at a specified time, configure task scheduling.

The ISCOM2600G series switch supports scheduling tasks by combining the program list with command lines. You just need to specify the start time of the task, period, and end time in the program list, and then bind the program list to command lines to implement the periodic execution of command lines.

Copyright © Raisecom Technology Co., Ltd.

1.8.2 Configuring task scheduling

Configure task scheduling for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**schedule-list** *list-number* **start date-time** { *mm-dd-yyyy hh:mm:ss* [**every** { **day** | **week** } **stop** *mm-dd-yyyy hh:mm:ss*] | **every** *days-interval time-interval* [**stop** *mm-dd-yyyy hh:mm:ss*] } Raisecom(config)#**schedule-list** *list-number* **start date-time** *mm-dd-yyyy hh:mm:ss* **every weekday-list** { **fri** | **mon** | **off-day** | **sta** | **sun** | **thu** | **tue** | **wed** | **working-day** | *weekday-list* } Raisecom(config)#**schedule-list** *list-number* **start up-time** *days-after-startup hh:mm:ss* [**every** *days-interval time-interval* [**stop** *days-after-startup hh:mm:ss*]]	Create a scheduling list, and configure it. • list-number: schedule number, an integer, ranging from 0 to 99 • start: time when schedule begins, start executing certain command. • stop: time when schedule ends, stop executing certain command. • date-time: absolute time, start or end scheduling when the system time is the same as the configured time. • up-time: relative time, start timing after the system is started and start or end scheduling after a period of configured time. • mm-dd-yyyy: date of absolute time in a format of month-day-year, such as 01-02-2011. • hh:mm:ss: time of absolute time in a format of hour-minute-second, such as 23:01:10. • days-after-startup: relative period, an integer, ranging from 0 to 365, in units of day, it means that after how long you can start or end scheduling since the system is started. • every: schedule period, the frequency of scheduling • day: once a day • week: once a week • days-interval: interval, an integer, ranging from 0 to 365, in units of day, the frequency of scheduling • time-interval: time interval, in form of hh:mm:ss, perform scheduling every how many days and hours • command: delete schedule information of specified commands from the schedule list. It means this command is not used for scheduling. If you do not choose this parameter, the entire schedule list will be deleted. • command-number: command number, an integer, ranging from 0 to 99
3	Raisecom(config)#*command-string* **schedule-list** *list-number* Example: Raisecom(config)#clear mac-address all schedule-list 2	Bind the command line which needs periodical execution and supports the scheduling list to the scheduling list. • command-string: command line character string • list-number: schedule list number, an integer, ranging from 0 to 99

Copyright © Raisecom Technology Co., Ltd.

1.8.3 Checking configurations

Use the following command to check configuration results.

No.	Command	Description
1	`Raisecom#show schedule-list [ list-number ]`	Show configurations of the scheduling list.

1.9 Watchdog

1.9.1 Introduction

The external electromagnetic field interferes with the working of the Microcontroller Unit (MCU), and causes program elapsing and endless loop; consequently the system fails to work normally. To monitor the realtime running status of the MCU, a program is specially used, which is commonly known as Watchdog.

The ISCOM2600G series switch will be restarted when it fails to work due to task suspension or endless loop, and it neither sends signals to restart the waterdog timer.

Watchdog can prevent the system program from endless loop due to uncertain fault, thus improving system stability.

1.9.2 Preparing for configurations

Scenario

By configuring Watchdog, you can prevent the system program from endless loop due to uncertain fault, thus improving system stability.

Prerequisite

N/A

1.9.3 Default configurations of Watchdog

Default configurations of Watchdog are as below.

Function	Default value
Watchdog status	Enable

1.9.4 Configuring Watchdog

Configure Watchdog for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

1	`Raisecom#watchdog { enable | disable }`
	Example:
	`Raisecom#watchdog enable`
		Enable or disable Watchdog.
		• enable: enable Watchdog.
		• disable: disable Watchdog.

1.9.5 Checking configurations

Use the following command to check configuration results.

Step	Command	Description
1	`Raisecom#show watchdog`	Show Watchdog status.

1.10 Configuring Banner

1.10.1 Preparing for configurations

Scenario

Banner is a message to display when you log in to or exit the ISCOM2600G series switch, such as the precautions or disclaimer.

You can configure the Banner of the ISCOM2600G series switch as required. In addition, the ISCOM2600G series switch provides the Banner switch. After Banner display is enabled, the configured Banner information appears when you log in to or exit the ISCOM2600G series switch.

After configuring Banner, use the **write** command to save configurations. Otherwise, Banner information will be lost when the ISCOM2600G series switch is restarted.

Prerequisite

N/A

1.10.2 Configuring Banner

Configure Banner for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#banner login` *w* `Press Enter.`
	`message w`
	`Example:`
	`Raisecom(config)#banner login @`
	`Enter text message followed by the character '@' to finish.User can stop configuration by inputing 'Ctrl+c';`
	`Welcome To Raisecom @`
		Configure the Banner contents. Enter the **banner login** and *w*, press **Enter**, enter the Banner contents, and then end with the *w* character.
		• *w:* a character with the length of 1. It is the beginning and end marker of the Banner contents. These 2 marks must be the identical character. We recommend selecting the specified character that will not occur at the *message*.
		• message: Banner contents. Up to 2560 characters are supported.

3	`Raisecom(config)#clear banner login`	(Optional) clear contents of the Banner.

1.10.3 Enabling Banner display

Enable Banner display for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#banner { enable | disable }`
	`Example:`
	`Raisecom(config)#banner enable`
		Enable or disable Banner display.
		By default, Banner display is disabled.
		• enable: enable Banner display.
		• disable: disable Banner display.

1.10.4 Checking configurations

Use the following commands to check configurations.

No.	Command	Description
1	`Raisecom#show banner login`	Show Banner status and contents of the configured Banner.

Copyright © Raisecom Technology Co., Ltd.

2 Ethernet

This chapter describes basic principles and configuration procedures for Ethernet, and provides related configuration examples, including the following sections:

- MAC address table
- VLAN
- PVLAN
- QinQ
- VLAN mapping
- STP/RSTP
- MSTP
- Loop detection
- Interface protection
- Port mirroring
- L2CP
- Voice VLAN
- GARP/GVRP

2.1 MAC address table

2.1.1 Introduction

The MAC address table records mappings between MAC addresses and interfaces. It is the basis for an Ethernet device to forward packets. When the Ethernet device forwards packets on Layer 2, it searches the MAC address table for the forwarding interface, implements expedited forwarding of packets, and reduces broadcast traffic.

The MAC address table contains the following information:

- Destination MAC address
- Destination MAC address related interface ID
- Interface VLAN ID
- Flag bits

Copyright © Raisecom Technology Co., Ltd.

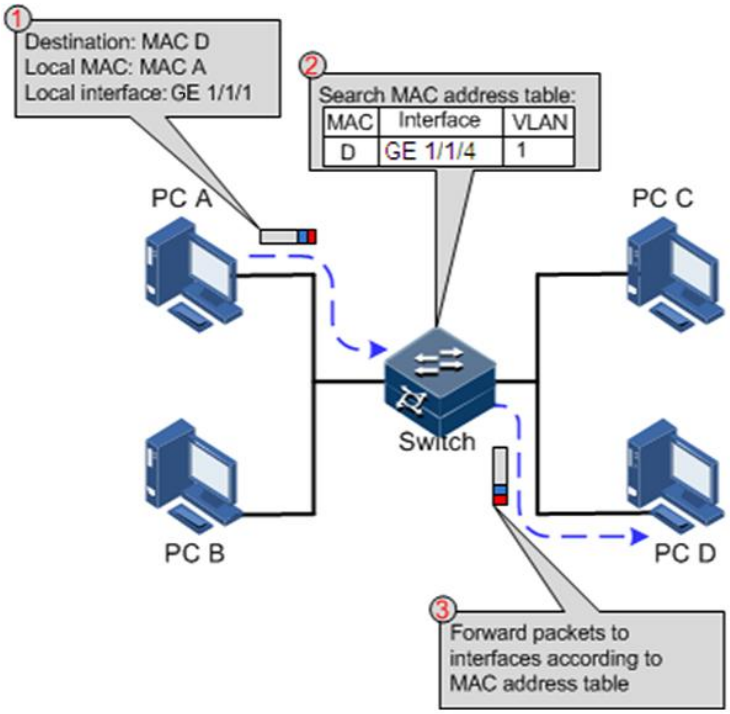
The ISCOM2600G series switch supports showing MAC address information by device, interface, or VLAN.

Forwarding modes of MAC addresses

When forwarding packets, based on the information about MAC addresses, the ISCOM2600G series switch adopts the following modes:

- Unicast: when a MAC address entry, related to the destination MAC address of a packet, is listed in the MAC address table, the ISCOM2600G series switch will directly forward the packet to the receiving interface through the egress interface of the MAC address entry. If the entry is not listed, the ISCOM2600G series switch broadcasts the packet to all interfaces except the receiving interface, as shown in Figure 2-1.

Figure 2-1 Forwarding packets according to the MAC address table



- Multicast: when the ISCOM2600G series switch receives a packet of which the destination MAC address is a multicast address, it will broadcast the packet. If multicast is enabled and storm control over unknown packets is also enabled, the packet will be sent to the specified Report interface. If no Report interface is specified, the packet will be discarded.
- Broadcast: when the ISCOM2600G series switch receives an all-F packet, or the MAC address is not listed in the MAC address table, the ISCOM2600G series switch forwards the packet to all interfaces except the interface that receives this packet. Broadcast addresses are special multicast addresses.

Classification of MAC addresses

MAC address table is divided into static address entry and dynamic address entry.

- Static MAC address entry: also called permanent address, added and removed by the user manually, not aged with time. For a network with small changes of devices, adding

Copyright © Raisecom Technology Co., Ltd.

static address entry manually can reduce the network broadcast flow, improve the security of the interface, and prevent entries from being lost after the system is reset.

- Dynamic MAC address entry: the ISCOM2600G series switch can add dynamic MAC address entries through MAC address learning. The entries are aged according to the configured aging time, and will be empty after the system is reset.

Aging time of MAC addresses

There is limit on the capacity of the MAC address table on the ISCOM2600G series switch. To maximize the use of the MAC address table, the ISCOM2600G series switch uses the aging mechanism to update the MAC address table. For example, when the ISCOM2600G series switch creates a dynamic entry, it starts the aging timer. If it does not receive packets from the MAC address in the entry during the aging time, the ISCOM2600G series switch will delete the entry.

The ISCOM2600G series switch supports automatic aging of MAC addresses. The aging time ranges from 10s to 1000000s and can be 0. The value 0 indicates no aging.

Note

The aging mechanism takes effect on dynamic MAC addresses.

Forwarding policies of MAC addresses

The MAC address table has two forwarding policies:

When receiving packets on an interface, the ISCOM2600G series switch searches the MAC address table for the interface related to the destination MAC address of packets.

- If successful, it forwards packets on the related interface, records the source MAC addresses of packets, interface ID of ingress packets, and VLAN ID in the MAC address table. If packets from other interface are sent to the MAC address, the ISCOM2600G series switch can send them to the related interface.
- If failed, it broadcasts packets to all interfaces except the source interface, and records the source MAC address in the MAC address table.

MAC address limit

The MAC address limit is used to limit the number of MAC addresses, avoid extending the searching time of forwarding entry caused by a too large MAC address table and degrading the forwarding performance of the Ethernet switch, and it is effective to manage the MAC address table.

The MAC address limit improves the speed of forwarding packets.

2.1.2 Preparing for configurations

Scenario

Configure the static MAC address table in the following situations:

- The static MAC address can be configured for a fixed server, special persons (manager, financial staff), fixed and important hosts to ensure that all data flow forwarding to these MAC addresses are forwarded from static MAC address related interface in priority.

Copyright © Raisecom Technology Co., Ltd.

- For the interface with fixed static MAC address, you can disable MAC address learning to avoid other hosts visiting LAN data from the interface.

Configure the aging time of dynamic MAC addresses to avoid saving excessive MAC address entries in the MAC address table and running out of MAC address table resources, and to achieve aging of dynamic MAC addresses.

Prerequisite

N/A

2.1.3 Default configurations of MAC address table

Default configurations of the MAC address table are as below.

Function	Default value
MAC address learning status	Enable
MAC address aging time	300s
MAC address limit	Unlimited
Suppression of MAC address flapping	Disable
MAC address flapping alarm	Disable

2.1.4 Configuring static MAC address

Configure static MAC address as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mac-address static unicast` *`mac-address`* `vlan` *`vlan-id interface-type interface-number`* **Example:** `Raisecom(config)#mac-address static unicast 0001.0001.0001 vlan 1 gigaethernet 1/1/1`	Configure static unicast MAC addresses. • mac-address: MAC address, in dotted hexadecimal notation • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • interface-type: interface type • interface-number: interface ID

Note

The MAC address of the source device, multicast MAC address, FFFF.FFFF.FFFF, and 0000.0000.0000 cannot be configured as static unicast MAC address.

2.1.5 Configuring blackhole MAC address

Configure blackhole MAC addresses as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-address blackhole** *mac-address* **vlan** *vlan-id* **Example:** Raisecom(config)#mac-address blackhole 000e.5e12.3456 vlan 3	Configure blackhole MAC addresses. • mac-address: MAC address, in dotted hexadecimal notation • vlan vlan-id: VLAN ID, an integer, ranging from 1 to 4094

2.1.6 Filtering unknown multicast packets

Filter unknown multicast packets for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-address multicast drop-unknown [reserved-address | vlan** *vlan-list* **]** **Example:** Raisecom(config)#mac-address multicast drop-unknown reserved-address	(Optional) filter unknown multicast packets. • reserved-address: contain reserved address. • vlan-list: forward unregistered multicast packets within VLAN. The vlan-list is an integer ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

2.1.7 Configuring MAC address learning

Configure MAC address learning for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.
3	Raisecom(config-config-gigaethernet1/1/por)#**mac-address learning { enable | disable }** **Example:** Raisecom(config-(config-gigaethernet1/1/por)#mac-address learning enable	Enable or disable MAC address learning. • enable: enable MAC address learning on the physical interface. • disable: disable MAC address learning on the physical interface.

Copyright © Raisecom Technology Co., Ltd.

2.1.8 Configuring MAC address limit

Configure the MAC address limit for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID. The form and value range depend on the interface type.
3	`Raisecom(config-gigaethernet1/1/port)#mac-address threshold` *`threshold-value`* **Example:** `Raisecom(config-gigaethernet1/1/1)#mac-address threshold 200`	Configure interface-based MAC address limit. • threshold: threshold-value: threshold of dynamic MAC address learning, an integer, ranging from 1 to 16383

2.1.9 Configuring aging time of MAC addresses

Configure the aging time of MAC addresses for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#mac-address aging-time { 0 | time }`
	Example:
	`Raisecom(config)#mac-address aging-time 600`
		Configure the aging time of MAC addresses.
		• time: aging time, an integer, being 0 or ranging from 10 to 1000000 among which 0 means no aging, in units of second

2.1.10 Enabling suppression of MAC address flapping

Enable suppression of MAC address flapping for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#mac-address move-restrain { enable | disable }`
	Example:
	`Raisecom(config)#mac-address move-restrain enable`
		Enable or disable global suppression of MAC address flapping.
		• enable: enable global suppression of MAC address flapping.
		• disable: disable global suppression of MAC address flapping.

Copyright © Raisecom Technology Co., Ltd.

2.1.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show mac-address** { **all** | **static** | **dynamic** | **blackhole** | *mac-address* } [**vlan** *vlan-id*] [*interface-type interface-number* | **vlan** *vlan-id*]]	Show information about MAC address entries.
2	Raisecom#**show mac-address multicast** [**vlan** *vlan-id*] [**count**]	Show Layer 2 multicast addresses or the number of existing multicast MAC address.
3	Raisecom#**show mac-address blackhole**	Show the blackhole MAC address.
4	Raisecom#**show mac-address threshold** [*interface-type interface-number* | **vlan** *vlan-list*]	Show the dynamic MAC address limit.
5	Raisecom#**show mac-addres aging-timemac-move**	Show the aging time of dynamic MAC addresses.
6	Raisecom#**show mac-address learning** [*interface-type interface-list*][*number* | **vlan**]	Show status of MAC address learning.
7	Raisecom#**show mac-address count** [**vlan** *vlan-id*] [*interface-type interface-number*]	Show the number of MAC address entries.

2.1.12 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
Raisecom(config)#**clear mac-address** [{ **all** | *mac-address*]{ **all** | **dynamic** | **blackhole** | **static** } [**vlan** *vlan-id*] [*interface-type interface-number*] **Example:** Raisecom(config)#clear mac-address all	Clear MAC addresses. • all: Clear all MAC address entries. • blackhole: clear blackhole MAC address entries. • static: clear static MAC address entries. • mac-address: unicast MAC address, in dotted hexadecimal notation, such as "000E.5E12.3456" • vlan vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • interface-type: interface type • interface-number: interface ID. The form and value range depend on the interface type.

Copyright © Raisecom Technology Co., Ltd.

Command	Description

`Raisecom(config)#clear mac-address { all | dynamic | static } [[ mac-address ][ vlan vlan-id ] [ interface-type interface-number ]`
Example:
`Raisecom(config)#clear mac-address all gigaethernet 1/1/1dynamic`
	Clear dynamic MAC addresses.
	• dynamic: clear dynamic MAC address entries.
	• mac-address: unicast MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456
	• vlan vlan-id: VLAN ID, an integer, ranging from 1 to 4094
	• interface-type: interface type
	• interface-number: interface ID. The form and value range depend on the interface type.

`Raisecom(config)#search mac-address mac-address { all | dynamic | static } [ interface-type interface-number ] [ vlan vlan-id ]`
Example:
`Raisecom(config)#search mac-address F04D.A22D.7805 all`
	Search for a MAC address.
	• mac-address: MAC address, in dotted hexadecimal notation
	• all: queue all MAC address entries.
	• dynamic: queue dynamic MAC address entries.
	• dynamic: queue dynamic MAC address entries.
	• interface-type: interface type
	• interface-number: interface ID. The form and value range depend on the interface type.
	• vlan: query the MAC address entry of the specified VLAN.
	• vlan-id: VLAN ID, an integer, ranging from 1 to 4094

2.1.13 Example for configuring MAC address table

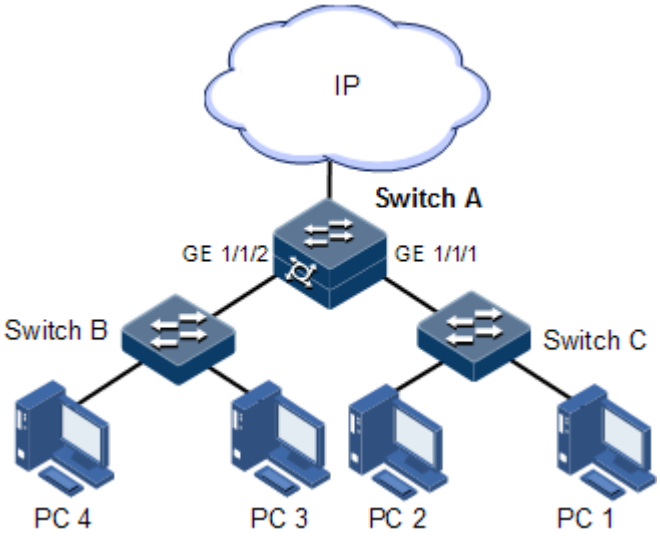
Networking requirements

As shown in Figure 2-2, configure Switch A as below:

- Configure a static unicast MAC address 0001.0203.0405 on GE 1/1/2 and configure its VLAN to VLAN 10.
- Configure the aging time to 500s.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-2 MAC networking



Configuration steps

Step 1 Create VLAN 10, and activate it, and add GE 1/1/2 to VLAN 10.

```
Raisecom#config
Raisecom(config)#create vlan 10 active
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode access
Raisecom(config-gigaethernet1/1/2)#switchport access vlan 10
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 2 Configure a static unicast MAC address 0001.0203.0405 on GE 1/1/2, which belongs to VLAN 10.

```
Raisecom(config)#mac-address static unicast 0001.0203.0405 vlan 10
gigaethernet 1/1/2
```

Step 3 Configure the aging time to 500s.

```
Raisecom(config)#mac-address aging-time 500
```

Checking results

Use the **show mac-address** to show configurations of MAC addresses.

```
Raisecom#show mac-address all gigaethernet 1/1/2
```


Copyright © Raisecom Technology Co., Ltd.

```
Aging time: 500 seconds

Mac Address       Port                        Vlan/Vxlan     Flag

-----------------------------------------------------------------

0001.0203.0405    gigaethernet1/1/2             10            static
```

2.2 VLAN

2.2.1 Introduction

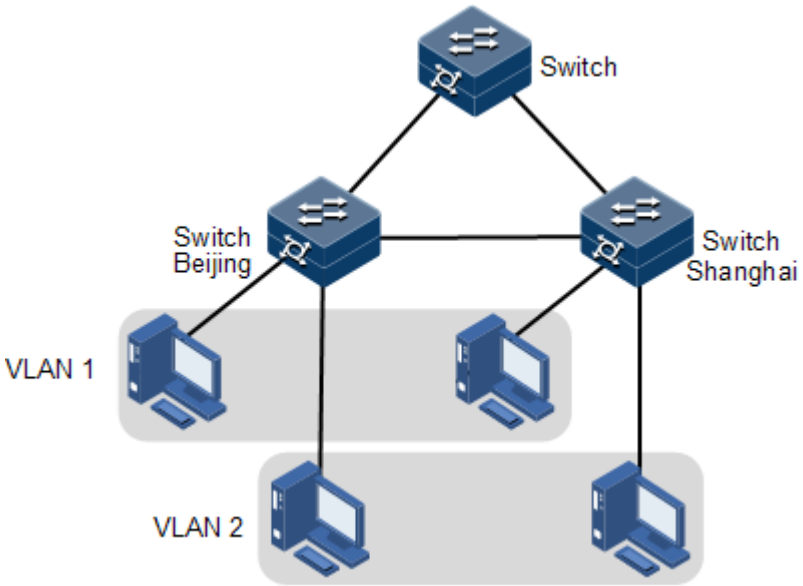
Overview

Virtual Local Area Network (VLAN) is a protocol to solve Ethernet broadcast and security problem. It is a Layer 2 isolation technique that partitions a LAN into different broadcast domains logically rather than physically, and then the different broadcast domains can work as virtual groups without any influence from one another. In terms of functions, VLAN has the same features as LAN, but members in one VLAN can access one another without restriction by physical location.

VLAN partitions

There are multiple ways of VLAN partitions, such as by interface, by MAC address, by IP subnet, and by protocol, as shown in Figure 2-3.

Figure 2-3 VLAN partitions



VLAN technique can partition a physical LAN into different broadcast domains logically. Hosts without intercommunication requirements can be isolated by VLAN, so VLAN partitions improve network security, and reduce broadcast flow and broadcast storm.

Copyright © Raisecom Technology Co., Ltd.

The ISCOM2600G series switch complies with IEEE 802.1Q standard VLAN and supports 4094 concurrent VLANs.

- VLAN partitions by interface

The ISCOM2600G series switch supports VLAN partitions by interface. The ISCOM2600G series switch has two interface modes: Access mode and Trunk mode. The method for processing packets for the two modes is shown as below.

Table 2-1 Interface mode and packet processing

Interface type	Processing ingress packets		Processing egress packets
	Untagged packets	Tagged packets	
Access	Add the Access VLAN Tag to the packet.	• If the VLAN ID of the packet is equal to the Access VLAN ID, the interface will receive the packet. • If the VLAN ID of the packet is not equal to the Access VLAN ID, the interface will discard the packet.	• If the VLAN ID of the packet is equal to the Access VLAN ID, the interface will remove the Tag and send the packet. • If the VLAN ID of the packet is excluded from the list of VLANs of which packets are allowed to pass by the interface, the interface will discard the packet.
Trunk	Add the Native VLAN Tag to the packet.	• If the VLAN ID of the packet is included in the list of VLANs of which packets are allowed to pass by the interface, the interface will receive the packet. • If the VLAN ID of the packet is excluded from the list of VLANs of which packets are allowed to pass by the interface, the interface will discard the packet.	• If the VLAN ID of the packet of the packet is equal to the Native VLAN ID, the interface will remove the Tag and send the packet. • If the VLAN ID of the packet is not equal to the Native VLAN ID and the interface allows packets of the VLAN to pass, the interface will keep the original Tag and send the packet.

- VLAN partitions by MAC address

This refers to VLAN partitions by the source MAC address of the packet.

  - When an interface receives an untagged packet, it matches the source MAC address of the packet with the VLAN MAC addresses. If they are the same, the match is successful. In this case, the interface adds the VLAN ID specified by VLAN MAC addresses, and forwards the packet. If they are different, the interface continues to match the packet with the IP address-based VLAN and interface-based VLAN in descending order.

Copyright © Raisecom Technology Co., Ltd.

  - When a tagged packet reaches an interface, if its VLAN ID is in the VLAN ID list allowed to pass by the interface, the interface receives it. Otherwise, the interface discards it.

- VLAN partitions by IP subnet

This refers to VLAN partitions by the source IP subnet of the packet.

  - When an interface receives an untagged packet, it determines the VLAN of the packet by the source IP subnet of the packet, and then transmits the packet in the specified VLAN.
  - When a tagged packet reaches an interface, if its VLAN ID is in the VLAN ID list allowed to pass by the interface, the interface receives it. Otherwise, the interface discards it.

- VLAN partitions by protocol

This refers to VLAN partitions by the protocol type carried in the packet received by the interface and assigning different VLAN IDs for packets. The protocol VLAN is defined by the protocol profile. One interface can be associated with multiple protocol profiles. After an interface is associated with protocol VLANs, it will process packets as below:

- After receiving an untagged packet from an interface, the device adds the VLAN Tag of the protocol VLAN defined by the protocol profile if the packet matches the protocol profile, or adds the default VLAN Tag if the packet does not match the protocol profile.
- When receiving a tagged packet from an interface, the device receives the packet if the VLAN ID is in the list of VLANs of which packets are allowed to pass by the interface, or discards the packet if the VLAN ID is not in the list of VLANs of which packets are allowed to pass by the interface.

2.2.2 Preparing for configurations

Scenario

The main function of VLAN is to partition logic network segments. There are 2 typical application modes:

- One kind is that in a small LAN several VLANs are created on a device, the hosts that connect to the device are divided by VLAN. So hosts in the same VLAN can communicate, but hosts between different VLANs cannot communicate. For example, the financial department needs to be separated from other departments and they cannot access each other. Generally, the interface to connect host is in Access mode.
- The other kind is that in bigger LAN or enterprise network multiple devices connect to multiple hosts and the devices are cascaded, and data packets carry VLAN Tag for forwarding. The interfaces in the same VLAN on multiple devices can communicate, but the interfaces in different VLANs cannot communicate. This mode is used in enterprise that has many employees and needs a large number of hosts, in the same department but different position, the hosts in one department can access one another, so users have to partition VLANs on multiple devices. Layer 3 devices, such as routers, are required if users want to communicate among different VLANs. The cascaded interfaces among devices are configured in Trunk mode.

When configuring the IP address for VLAN, you can associate a Layer 3 interface for it. Each Layer 3 interface corresponds to one IP address and one VLAN.

Copyright © Raisecom Technology Co., Ltd.

Prerequisite

N/A

2.2.3 Default configurations of VLAN

Default configurations of VLAN are as below.

Function	Default value
Create VLAN	VLAN 1 and VLAN 4093
Active status of static VLAN	Active
Interface mode	Access
Access VLAN	VLAN 1
Native VLAN of Trunk interface	VLAN 1
Allowable VLAN in Trunk mode	VLAN 1
Allowable untagged VLAN in Trunk mode	VLAN 1
VLAN mapping table ID	VLAN ID

2.2.4 Configuring VLAN attributes

Configure VLAN attributes for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#create vlan vlan-list active`
	Example:
	`Raisecom(config)#create vlan 4 active`
		Create a VLAN.
		The command can also be used to create VLANs in batches.
		• vlan-list: an integer ranging from 1 to 4094. It supports specific values, such as "2,3,4"; it also supports a range, such as "2-4".

3	`Raisecom(config)#vlan vlan-id`
	Example:
	`Raisecom(config)#vlan 100`
		Enter VLAN configuration mode.
		vlan-id: VLAN ID, an integer, ranging from 1 to 4094

4	`Raisecom(config-vlan)#name vlan-name`
	Example:
	`Raisecom(config-vlan)#name HR`
		(Optional) configure the VLAN name.
		• vlan-name: VLAN name, a string of 1 to 32 characters

Note

- The VLAN created by the **vlan** *vlan-id* command is in active status.

Copyright © Raisecom Technology Co., Ltd.

- All configurations of VLAN do not take until the VLAN is activated.

2.2.5 Configuring interface mode

Configure the interface mode for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID. The form and value range depend on the interface type.
3	`Raisecom(config-gigaethernet1/1/port)#switchport mode { access | trunk }`	Configure the interface to Access or Trunk mode. • access: configure the interface to Access mode. • trunk: configure the interface to Trunk mode.

2.2.6 Configuring VLAN on Access interface

Configure the VLAN on the Access interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#switchport mode access`
	`Raisecom(config-gigaethernet1/1/port)#switchport access vlan` *`vlan-id`*
	Example:
	`Raisecom(config-gigaethernet1/1/1)#switchport access vlan 100`
		Configure the interface to Access mode, and add the Access interface to the VLAN.
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

4	`Raisecom(config-gigaethernet1/1/port)#switchport access egress-allowed vlan { all | [ add | remove ] vlan-list } [ confirm ]`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#switchport access egress-allowed vlan 100,200`
		(Optional) configure the VLAN allowed to pass by the Access interface.
		• all: the access interface allows all VLANs to pass.
		• vlan-list: VLAN list allowed to pass by the Access interface, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
		• confirm: confirmed
		• add: add VLANs which are allowed to pass through the interface to the old VLAN list.
		• remove: delete VLANs which are allowed to pass through the interface from the old VLAN list.

Note

- The interface allows Access VLAN packets to pass regardless of configuration for VLAN allowed by the Access interface. The forwarded packets do not carry the VLAN Tag.
- When configuring the Access VLAN, the system creates and activates a VLAN automatically if you have not created and activated a VLAN in advance.
- If you delete the Access VLAN manually, the system will automatically configure the interface Access VLAN as the default VLAN.
- When you configure the interface Access VLAN as the non-default Access VLAN, the default Access VLAN 1 is the VLAN allowed by the Access the egress interface, you can delete Access VLAN 1 from the allowed VLAN list of the egress Access interface.
- If the configured Access VLAN is not the default VLAN and there is no default VLAN in the allowed VLAN list of the Access interface, the interface does not allow packets of the default VLAN to pass.
- The allowed VLAN list of the Access interface is effective to static VLANs only, and ineffective to cluster VLAN, GVRP dynamic VLAN, and so on.

2.2.7 Configuring VLAN on Trunk interface

Configure the VLAN on the Trunk interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-gigaethernet1/1/port)#**switchport mode trunk**	Configure the interface to Trunk mode.
4	Raisecom(config-gigaethernet1/1/port)#**switchport trunk native vlan** *vlan-id* **Example:** Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan 100	Configure the Native VLAN of the interface. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
5	Raisecom(config-gigaethernet1/1/port)#**switchport trunk allowed vlan** { **all** | [**add** | **remove**] *vlan-list* } [**confirm**] **Example:** Raisecom(config-gigaethernet1/1/1)#switchport trunk allowed vlan 100,200	(Optional) configure VLANs allowed to pass by the Trunk interface. • all: the access interface allows all VLANs to pass. • vlan-list: VLAN list allowed to pass by the Access interface, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • confirm: confirmed • add: add VLANs which are allowed to pass through the interface to the old VLAN list. • remove: delete VLANs which are allowed to pass through the interface from the old VLAN list.
6	Raisecom(config-gigaethernet1/1/port)#**switchport trunk untagged vlan** { **all** | [**add** | **remove**] *vlan-list* } [**confirm**] **Example:** Raisecom(config-gigaethernet1/1/1)#switchport trunk untagged vlan 100,200	(Optional) configure VLANs from which the Trunk interface can remove Tag. • all: the access interface allows all VLANs to pass. • vlan-list: VLAN list allowed to pass by the Access interface, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • confirm: confirmed • add: add VLANs which are allowed to pass through the interface to the old VLAN list. • remove: delete VLANs which are allowed to pass through the interface from the old VLAN list.
7	Raisecom(config-gigaethernet1/1/port)#**switchport trunk native vlan** { **tagged** | **untagged** } **Example:** Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan tagged	(Optional) configure the Tag attribute of the Native VLAN egress interface of the Trunk interface. • Tagged: the Tag attribute of the egress interface is tagged. • Untagged: the Tag attribute of the egress interface is untagged.

Copyright © Raisecom Technology Co., Ltd.

Note

- The system will create and activate the VLAN if no VLAN is created and activated in advance when configuring the Native VLAN.
- The system configures the interface Trunk Native VLAN as default VLAN if you have deleted or blocked Native VLAN manually.
- The interface allows incoming and outgoing VLAN packet allowed by the Trunk interface. If the VLAN is Trunk untagged VLAN, the VLAN Tag is removed from the packets at the egress interface. Otherwise the packets are not modified.
- When configuring Trunk untagged VLAN list, the system automatically adds all untagged VLAN to the VLAN allowed by the Trunk interface.
- The VLAN list and untagged VLAN list allowed by the Trunk interface are only effective to static VLAN, and ineffective for cluster VLAN, GVRP dynamic VLAN.

2.2.8 Configuring VLAN based on MAC address

Configure the VLAN based on MAC address for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#mac-vlan` *`mac-address`* `[ mask` *`mac-address-mask`* `] vlan` *`vlan-id`* `[ priority` *`value`* `]`
	Example:
	`Raisecom(config)#mac-vlan 0001.0001.0001 vlan 2`
		Associate a MAC address with a VLAN.
		• mac-address: MAC address, in dotted hexadecimal notation
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094
		• mac-address-mask: MAC address mask, in dotted hexadecimal notation
		• value: VLAN priority, an integer, ranging from 0 to 7

3	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID. The form and value range depend on the interface type.

4	`Raisecom(config-gigaethernet1/1/port)#mac-vlan { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#mac-vlan enable`
		Enable or disable MAC-VLAN.
		• enable: enable MAC-VLAN.
		• disable: disable MAC-VLAN.

5	`Raisecom(config-gigaethernet1/1/port)#vlan precedence { mac-vlan | ip-subnet-vlan }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#vlan precedence mac-vlan`
		(Optional) configure priorities of MAC-VLAN and IP subnet VLAN.
		• mac-vlan: high priority of MAC-based VLAN
		• ip-subnet-vlan: high priority of IP-based VLAN

Copyright © Raisecom Technology Co., Ltd.

Caution

- If the IP address or subnet mask is invalid, the configuration will fail.
- If you associate a created IP subnet to a VLAN but this association conflict with an existing association (for example, the IP subnet or VLAN is already associated), the association will fail.

2.2.9 Configuring VLAN based on IP subnet

Configure the VLAN based on IP subnet for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#ip-subnet-vlan ip-address [ ip-mask ] vlan vlan-id [ priority value ]`
	Example:
	`Raisecom(config)#ip-subnet-vlan 192.168.1.5 255.255.255.0 vlan 2`
		Associate a MAC address with an IP subnet.
		• ip-address: IP address, in dotted decimal notation, such as "10.0.0.1"
		• ip-mask: IP address mask, in dotted decimal notation, such as "255.0.0.0"
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094
		• priority value: VLAN priority value, an integer, ranging from 0 to 7

3	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID. The form and value range depend on the interface type.

4	`Raisecom(config-gigaethernet1/1/port)#ip-subnet-vlan { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#ip-subnet-vlan enable`
		Enable VLAN partitions based on IP subnet.
		• enable: enable IP subnet-based VLAN partitions.
		• disable: disable IP subnet-based VLAN partitions.

5	`Raisecom(config-gigaethernet1/1/port)#vlan precedence { mac-vlan | ip-subnet-vlan }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#vlan precedence ip-subnet-vlan`
		(Optional) configure priorities of MAC-VLAN and IP subnet VLAN.
		• mac-vlan: high priority of MAC-based VLAN
		• ip-subnet-vlan: high priority of IP-based VLAN

Caution

- If the IP address or subnet mask is invalid, the configuration will fail.

Copyright © Raisecom Technology Co., Ltd.

- If you associate a created IP subnet to a VLAN but this association conflict with an existing association (for example, the IP subnet is associated with different VLANs), the association will fail.

2.2.10 Configuring VLAN based on protocol

Configure the VLAN based on protocol for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#protocol-vlan protocol-index { ipv4 | ipv6 | ethertype protocol-id }`
	Example:
	`Raisecom(config)#protocol-vlan 1 ipv4`
		Configure the rule for associating the protocol VLAN with Ethernet packets.
		• protocol-index: protocol template index, an integer, ranging from 1 to 16
		• ethertype protocol-id: support the associated Ethernet packet protocol ID, an integer, ranging from 0x600–ffff (excluding 800, 809b, 8137, and 86dd)

3	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID. The form and value range depend on the interface type.

4	`Raisecom(config-gigaethernet1/1/port)#switchport protocol-vlan protocol-index vlan vlan-id`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#switchport protocol-vlan 1 vlan 100`
		Configure the rule for associating the interface with the protocol VLAN.
		• vlan vlan-id: VLAN ID, an integer, ranging from 1 to 4094
		• protocol-index: protocol template index, an integer, ranging from 1 to 16

2.2.11 Configuring VLAN filtering in egress direction

Configure VLAN filtering in the egress direction for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

3	`Raisecom(config-gigaethernet1/1/port)#egress-filtering vlan vlan-list`
	Example:
	`Raisecom(config-gigaethernet1/1/1)# egress-filtering vlan 100`
		Configure VLAN filtering in the egress direction. After VLAN filtering in the egress direction is configured in Layer 2 interface configuration mode, the device will discard traffic of the VLAN in the egress direction.
		• vlan-list: VLAN list. The vlan-list is an integer, ranging from 2 to 4094. It supports specific values, such as "2,3,4"; it also supports a range, such as "2-4".

2.2.12 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show vlan [ vlan-list | static | dynamic ] [ detail ]`	Show VLAN configurations.
2	`Raisecom#show vlan precedence`	Show priorities of the MAC-VLAN and IP subnet VLAN.
3	`Raisecom#show mac-vlan [ mask | efficient ] { all | vlan vlan-id }`	Show MAC VLAN configurations.
4	`Raisecom#show mac-vlan aging-time`	Show the aging time of MAC VLANs.
5	`Raisecom#show switchport interface interface-type interface-number`	Show configurations of switching on the interface.
6	`Raisecom#show protocol-vlan all`	Show configurations of all protocol VLANs.
7	`Raisecom#show protocol-vlan interface [ interface-type interface-number ]`	Show configurations of the protocol VLAN on the interface.
8	`Raisecom#show ip-subnet-vlan { all | vlan vlan-id }`	Show configurations of the IP subnet VLAN.
9	`Raisecom#show egress-filtering`	Show configurations of VLAN filtering in the egress direction.

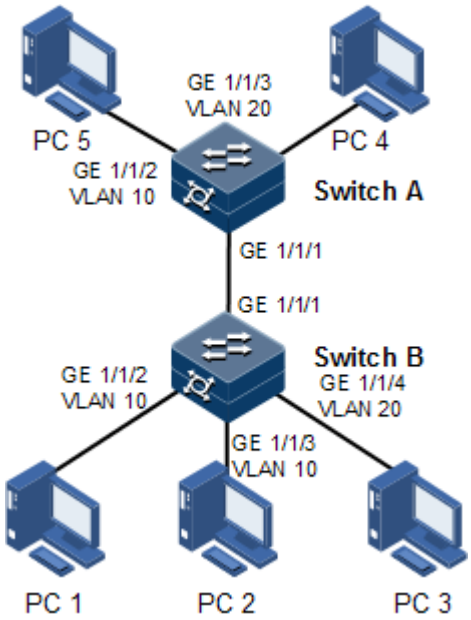
2.2.13 Example for configuring VLAN

Networking requirements

As shown in Figure 2-4, PC 1, PC 2, and PC 5 belong to VLAN 10, PC 3 and PC 4 belong to VLAN 20; Switch A and Switch B are connected by the Trunk interface; PC 3 and PC 4 cannot communicate because VLAN 20 is not allowed to pass in the link; PC 1 and PC 2 under the same Switch B are enabled with interface protection function so that they cannot communicate with each other, but can respectively communicate with PC 5.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-4 VLAN and interface protection networking



Configuration steps

Step 1 Create VLAN 10 and VLAN 20 on the two switches respectively, and activate them.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 10,20 active
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#create vlan 10,20 active
```

Step 2 Add GE 1/1/2 and GE 1/1/3 in Access mode on Switch B to VLAN 10, add GE 1/1/4 as Access mode to VLAN 20, configure GE 1/1/1 to Trunk mode, and allow VLAN 10 to pass.

```
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode access
SwitchB(config-gigaethernet1/1/2)#switchport access vlan 10
SwitchB(config-gigaethernet1/1/2)#exit
SwitchB(config)#interface gigaethernet 1/1/3
SwitchB(config-gigaethernet1/1/3)#switchport mode access
SwitchB(config-gigaethernet1/1/3)#switchport access vlan 10
SwitchB(config-gigaethernet1/1/3)#exit
```


Copyright © Raisecom Technology Co., Ltd.

```
SwitchB(config)#interface gigaethernet 1/1/4
SwitchB(config-gigaethernet1/1/4)#switchport mode access
SwitchB(config-gigaethernet1/1/4)#switchport access vlan 20
SwitchB(config-gigaethernet1/1/4)#exit
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#switchport trunk allowed vlan 10
confirm
SwitchB(config-gigaethernet1/1/1)#exit
```

Step 3 Add GE 1/1/2 as Access mode on Switch A to VLAN 10, add GE 1/1/3 as Access mode to VLAN 20, configure GE 1/1/1 to Trunk mode, and allow VLAN 10 to pass.

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode access
SwitchA(config-gigaethernet1/1/2)#switchport access vlan 10
SwitchA(config-gigaethernet1/1/2)#exit
SwitchA(config)#interface gigaethernet 1/1/3
SwitchA(config-gigaethernet1/1/3)#switchport mode trunk
SwitchA(config-gigaethernet1/1/3)#switchport trunk native vlan 20
SwitchA(config-gigaethernet1/1/3)#exit
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 10
confirm
```

Checking results

Use the **show vlan** command to show VLAN configurations.

Take Switch B for example.

```
SwitchB#show vlan
Switch Mode: --
VLAN Name          State   Status  Priority Member-Ports
---------------------------------------------------------------------
1   Default        active  static  --       gigaethernet1/1/1
10  VLAN0010       active  static  --       gigaethernet1/1/2
gigaethernet1/1/3
20  VLAN0020       active  static  --       gigaethernet1/1/4
```

Use the **show switchport interface** *interface-type interface-number* command to show configurations of the interface VLAN.

Take Switch B for example.

```
SwitchB#show switchport interface gigaethernet 1/1/2
```


Copyright © Raisecom Technology Co., Ltd.

```
Interface: gigaethernet1/1/2
Switch Mode: switch
Reject frame type: none
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 10
Administrative Access Egress VLANs:
Operational Access Egress VLANs: 10
Trunk Native Mode VLAN: 1
Trunk Native VLAN: untagged
Administrative Trunk Allowed VLANs:
Operational Trunk Allowed VLANs: 1
Administrative Trunk Untagged VLANs:
Operational Trunk Untagged VLANs: 1
Administrative private-vlan host-association:  1
Administrative private-vlan mapping: 1
Operational private-vlan: --
```

Check whether the Trunk interface permitting VLAN passing is correct by making PC 1 ping PC 5, PC 2 ping PC 5, and PC 3 ping PC 4.

- PC 1 can ping through PC 5, so VLAN 10 communication is normal.
- PC 2 can ping through PC 5, so VLAN 10 communication is normal.
- PC 3 fails to ping through PC 4, so VLAN 20 communication is abnormal.

2.3 PVLAN

2.3.1 Introduction

Private VLAN (PVLAN) provides Layer 2 isolation between interfaces in a VLAN, and it is effective to distribute VLAN resources.

PVLAN type

VLANs are divided into two types: primary VLAN and secondary VLAN. The primary VLAN and secondary VLAN form a PVLAN domain. The primary VLAN can communicate both in and out of PVLANs, but the secondary VLAN can communicate in the PVLAN only.

- Primary VLAN: each PVLAN can be configured with only one primary VLAN. Interface of all types in PVLAN are members of primary VLAN.
- Secondary VLAN: it can be divided into isolated VLAN and community VLAN according to the different forwarding and isolation rules.
  - Isolated VLAN: each PVLAN can be configured with only one isolated VLAN.
  - Community VLAN: each PVLAN can be configured with multiple community VLANs.

Interface modes of PVLAN

The interface to be able to communicate with the external network is called the Promiscuous interface. The interface in the secondary VLAN is the Host interface.

Copyright © Raisecom Technology Co., Ltd.

- Promiscuous interface: it belongs to all PVLANs in the PVLAN domain. It can communicate with all interfaces.
- Isolated interface: isolated interfaces cannot communicate with each other, but they can communicate with the Promiscuous interface and Trunk interface.
- Community interface: community interfaces in a community can communicate with each other, but community interfaces in different communities cannot communicate with each other. All community interfaces can communicate with the Promiscuous interface and Trunk interface.

2.3.2 Preparing for configuration

Scenario

PVLAN, used on an enterprise Intranet, allows devices inside the VPLAN to communicate with the default gateway only rather than the Intranet.

Prerequisite

Create a static VLAN and activate it.

2.3.3 Default configurations of PVLAN

Default configurations of PVLAN are as below.

Function	Default value
PVLAN mode on the interface	Access mode

2.3.4 Configuring PVLAN type

Configure the PVLAN type for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#private-vlan { primary vlan vlan-id | isolated vlan vlan-id | community vlan vlan-list }`
	Example:
	`Raisecom(config)#private-vlan primary vlan 3`
		Configure the PVLAN type.
		• primary: primary VLAN type of a PVLAN
		• isolated: isolated VLAN of PVLAN
		• vlan-id: VLAN ID, an integer, ranging from 2 to 4094
		• vlan-list: VLAN list. The vlan-list is an integer, ranging from 2 to 4094. It supports specific values, such as "2,3,4"; it also supports a range, such as "2-4".

Caution

- Up to 32 primary VLANs and 2048 secondary VLANs are allowed.

Copyright © Raisecom Technology Co., Ltd.

- If the VLAN is associated, its PVLAN type cannot be modified nor deleted.

2.3.5 Configuring PVLAN association

Configure PVLAN association for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#private-vlan { primary vlan vlan-id | isolated vlan vlan-id | community vlan vlan-list }`
	Example:
	`Raisecom(config)#private-vlan primary vlan 3`
		Configure the PVLAN type.
		• primary: primary VLAN type of a PVLAN
		• isolated: isolated VLAN of PVLAN
		• vlan-id: VLAN ID, an integer, ranging from 2 to 4094
		• vlan-list: VLAN list. The vlan-list is an integer, ranging from 2 to 4094. It supports specific values, such as "2,3,4"; it also supports a range, such as "2-4".

3	`Raisecom(config)#private-vlan association primary-vlan-list [ add | remove ] secondary-vlan-list`
	Example:
	`Raisecom(config)#private-vlan association 2 3`
		Configuration association of the primary VLAN and secondary VLANs.
		• primary-vlan-list: primary VLAN ID. The vlan-list is an integer, ranging from 2 to 4094.
		• secondary-vlan-list: secondary VLAN ID. The vlan-list is an integer, ranging from 2 to 4094.
		• add: add secondary VLAN ID list.
		• remove: delete secondary VLAN ID list.

Caution

- Before configuring VLAN association, create a VLAN and activate it, configure PVLAN type, configure the primary VLAN and secondary VLANs, and choose the correct association type. Otherwise, VLAN association cannot be configured.
- The primary VLAN and secondary VLANs cannot be configured to the default VLAN 1. If VLAN 2 is the cluster VLAN, it cannot be configured as the PVLAN.
- A secondary VLAN can be added to only one PVLAN.
- A primary VLAN can be associated with only one isolated VLAN, or up to 64 secondary VLANs.

2.3.6 Configuring PVLAN mode on interface

The VLAN of the ISCOM2600G series switch supports Access and Trunk interface modes, and the PVLAN supports promiscuous interface mode and host interface mode.

Caution

- The promiscuous interface mode and host interface mode can be configured with association or mapping which already exists. Otherwise, the configuration will fail.
- When an interface is configured to the host interface mode or promiscuous interface mode without being associated with or mapped to a primary VLAN or secondary VLAN, the interface allows untagged packets to enter.

Copyright © Raisecom Technology Co., Ltd.

- IGMP runs on the primary VLAN only. The VLANs to data flow to pass in uplink and downlink of PVLAN are different, so you cannot configure IGMP Snooping to implement multicast; instead, you need to configure IGMP MVR.

Configure the PVLAN mode on the interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface`** *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID. The form and value range depend on the interface type.

3	`Raisecom(config-gigaethernet1/1/port)#`**`switchport mode private-vlan`** `{` **`host`**`|` **`promiscuous`** `}`
	Example:
	`Raisecom(config)#switchport mode private-vlan host`
		Configure the PVLAN mode on the interface.
		• host: host interface mode
		• promiscuous: promiscuous interface mode

4	`Raisecom(config-gigaethernet1/1/port)#`**`switchport private-vlan host-association`** *`primary-vlan-id secondary-vlan-id`* **Example:** `Raisecom(config-gigaethernet1/1/1)#switchport private-vlan host-association 2 3`	Associate the primary VLAN of the host interface with the secondary VLAN. Use the **no switchport private-vlan host-association** command to delete the association between the primary VLAN of the host interface with the secondary VLAN. • primary-vlan-id: primary VLAN ID. The vlan-list is an integer, ranging from 2 to 4094. • secondary-vlan-id: secondary VLAN ID. The vlan-list is an integer, ranging from 2 to 4094.
5	`Raisecom(config-gigaethernet1/1/port)#`**`switchport private-vlan trunk host-association`** *`secondary-vlan-id`* **Example:** `Raisecom(config-gigaethernet1/1/1)#switchport private-vlan trunk host-association 3`	Configure the host interface associated with the secondary VLAN to be able to forward tagged packets. Use the **no switchport private-vlan trunk host-association** command to delete this configuration. • secondary-vlan-id: secondary VLAN ID. The vlan-list is an integer ranging from 2 to 4094.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

6	`Raisecom(config-gigaethernet1/1/port)#switchport private-vlan mapping primary-vlan-id [ add | remove ] secondary-vlan-id`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#switchport private-vlan mapping 2 3`
		Configure the mapping of the primary VLAN and secondary VLANs on the promiscuous interface.
		Use the **no switchport private-vlan mapping** command to delete the association between the primary VLAN of the promiscuous interface with the secondary VLAN.
		• primary-vlan-id: primary VLAN ID. The vlan-list is an integer, ranging from 2 to 4094.
		• secondary-vlan-list: secondary VLAN ID. The vlan-list is an integer, ranging from 2 to 4094.

7	`Raisecom(config-gigaethernet1/1/port)#switchport private-vlan trunk mapping primary-vlan-id`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#switchport private-vlan trunk mapping 2`
		Configure the interface mapped with the primary VLAN to be able to forward tagged packets.
		Use the **no switchport private-vlan trunk mapping** command to delete this configuration.
		• primary-vlan-id: primary VLAN ID. The vlan-list is an integer ranging from 2 to 4094.

2.3.7 Checking configuration

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show vlan private-vlan [ vlan vlan-id ] [ type { primary | community | isolated } ]`	Show PVLAN configurations.

2.3.8 Example for configuring PVLAN

Networking requirements

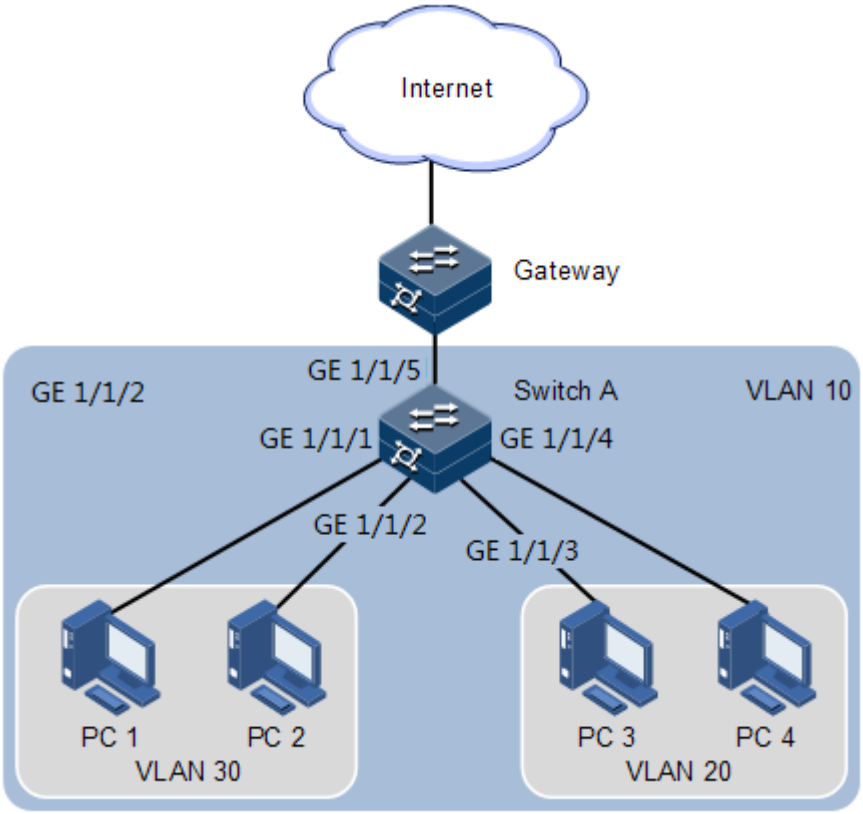
To effectively distribute VLAN resources, you need to properly partition and configure VLANs. As shown in Figure 2-5, on Switch A, configure VLAN 10 as the primary VLAN, VLAN 20 as the isolated VLAN, and VLAN 30 as the community VLAN. The detailed configurations are as below:

- Configure GE 1/1/1 and GE 1/1/2 as community interfaces. Associate primary VLAN 10 with secondary VLAN 30.
- Configure GE 1/1/3 and GE 1/1/4 as isolated interfaces. Associate primary VLAN 10 with secondary VLAN 20.

Copyright © Raisecom Technology Co., Ltd.

- Configure GE 1/1/5 as the promiscuous interface. Map PVLAN with VLAN 10, VLAN 20, and VLAN 30.
- Connect PC 1 and PC 2 to community interfaces GE 1/1/1 and GE 1/1/2 respectively, and they can communicate with these two interfaces and the promiscuous interface GE 1/1/5.
- Connect PC 3 and PC 4 to isolated interfaces GE 1/1/3 and GE 1/1/4respectively, and they can communicate with the promiscuous interface GE 1/1/5 only.

Figure 2-5 Networking with PVLAN



Configuration steps

Step 1 Configure the PVLAN type.

```
Raisecom#config
Raisecom(config)#create vlan 10,20,30 active
Raisecom(config)#private-vlan primary vlan 10
Raisecom(config)#private-vlan community vlan 30
Raisecom(config)#private-vlan isolated vlan 20
Raisecom(config)#private-vlan association 10 20,30
```

Step 2 Configure the promiscuous interface mode and mapping of the primary VLAN and secondary VLAN on the promiscuous interface.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config)#interface gigaethernet 1/1/5
Raisecom(config-gigaethernet1/1/5)#switchport mode private-vlan
promiscuous
Raisecom(config-gigaethernet1/1/5)#switchport private-vlan mapping 10
20,30
Raisecom(config-gigaethernet1/1/5)#exit
```

Step 3 Configure the host interface mode and association of the primary VLAN with the secondary VLAN on the host interface.

Configuration on GE 1/1/1 and GE 1/1/2, GE 1/1/3 and GE 1/1/4 are identical. Take GE 1/1/1 and GE 1/1/3 for example.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode private-vlan host
Raisecom(config-gigaethernet1/1/1)#switchport private-vlan host-
association 10 30
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#switchport mode private-vlan host
Raisecom(config-gigaethernet1/1/3)#switchport private-vlan host-
association 10 20
```

Checking results

Use the **show vlan private-vlan** command to show PVLAN configurations on the ISCOM2600G series switch.

```
Raisecom#show vlan private-vlan
VLAN ID: 10
Pvlan type: primary
Associated-isolated vlan: 20
Associated-community vlan: 30
Member Port-list:
         gigaethernet1/1/1         gigaethernet1/1/3
         gigaethernet1/1/5
Untag Port-list:
         gigaethernet1/1/1         gigaethernet1/1/3
         gigaethernet1/1/5

VLAN ID: 20
Pvlan type: isolated
Associated-primary vlan: 10
Member Port-list:
         gigaethernet1/1/3         gigaethernet1/1/5
Untag Port-list:
         gigaethernet1/1/3         gigaethernet1/1/5

VLAN ID: 30
Pvlan type: community
```


Copyright © Raisecom Technology Co., Ltd.

```
Associated-primary vlan: 10
Member Port-list:
        gigaethernet1/1/1         gigaethernet1/1/5
Untag Port-list:
        gigaethernet1/1/1         gigaethernet1/1/5
```

2.4 QinQ

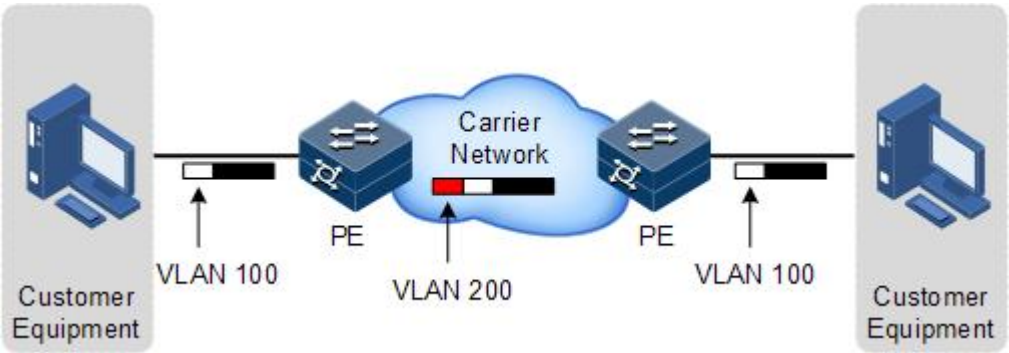
2.4.1 Introduction

QinQ (also known as Stacked VLAN or Double VLAN) technique is an extension to 802.1Q defined in IEEE 802.1ad standard.

Basic QinQ

Basic QinQ is a simple Layer 2 VPN tunnel technique, which encapsulates outer VLAN Tag for user private network packets at carrier access end, then the packet with double VLAN Tag traverse backbone network (public network) of the carrier. On the public network, packets are transmitted according to outer VLAN Tag (namely, the public network VLAN Tag), the user private network VALN Tag is transmitted as data in packets.

Figure 2-6 Principles of basic QinQ



Typical networking of basic QinQ is shown as Figure 2-6; the ISCOM2600G series switch is the PE.

Packets are transmitted from the user device to the PE, and the VLAN ID of packet tag is 100. Packet will be added with outer tag with VLAN 1000 when traversing from the PE device at the network side interface to the carrier network.

Packets with the VLAN 1000 outer Tag are transmitted to PE device on the other side by the carrier, and then the PE will remove the outer tag VLAN 1000 and send packets to the user device. Now the packets return to carrying only one tag VLAN 100.

This technique can save public network VLAN ID resources. You can plan private network VLAN ID to avoid conflict with public network VLAN ID.

Copyright © Raisecom Technology Co., Ltd.

Selective QinQ

Selective QinQ is an enhancement to basic QinQ, which classifies flow according to user data features, then encapsulates different types flow into different outer VLAN Tags. This technique is implemented through combination of interface and VLAN. Selective QinQ can perform different actions on different VLAN Tags received by one interface and add different outer VLAN IDs for different inner VLAN IDs. According to configured mapping rules for inner and outer Tags, you can encapsulate different outer Tags for different inner tagged packets.

Selective QinQ makes structure of the carrier network more flexible. You can classify different terminal users on the access device interface by VLAN Tag and then, encapsulate different outer Tags for users in different classes. On the public network, you can configure QoS policy according to outer Tag and configure data transmission priority flexibly to make users in different classes receive corresponding services.

2.4.2 Preparing for configurations

Scenario

Basic QinQ configuration and selective QinQ configuration for the ISCOM2600G series switch are based on different service requirements.

- Basic QinQ

With application of basic QinQ, you can add outer VLAN Tag to plan the private VLAN ID freely to make the user device data at both ends of carrier network transparently transmitted without conflicting with VLAN ID on the service provider network.

- Selective QinQ

Different from basic QinQ, outer VLAN Tag of selective QinQ can be selectable according to different services. There are multiple services and different private VLAN ID on the user network which are divided by adding different outer VLAN Tag for voice, video, and data services, then implementing different distributaries and inner and outer VLAN mapping for forwarding different services.

Prerequisite

- Connect the interface.
- Configure its physical parameters to make it Up.
- Create VLANs.

Note

- Basic QinQ and 1:1 VLAN mapping can be concurrently configured. VLAN mapping functions normally before or after basic QinQ is enabled.
- Selective QinQ and 1:1 VLAN mapping can be concurrently configured. When they are concurrently configured, they function normally. They also function normally when basic QinQ is enabled or disable. When one of them is disabled, other configurations function normally.
- Basic QinQ, selective QinQ, and 2:2 VLAN mapping are mutually exclusive. When selective QinQ and 1:1 VLAN mapping are configurrently configured, their matching VLANs cannot be the same, and VLANs after mapping cannot be the same.

Copyright © Raisecom Technology Co., Ltd.

2.4.3 Default configurations of QinQ

Default configurations of QinQ are as below.

Function	Default value
Outer VLAN Tag TPID	0x8100
Basic QinQ status	Disable
Selective QinQ status	Disable

2.4.4 Configuring basic QinQ

Configure basic QinQ on the ingress interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#dot1q-tunnel`	Enable basic QinQ on the interface. The device supports this configuration on the LAG interface or in ISF mode.

4	`Raisecom(config-gigaethernet1/1/port)#switchport qinq default-cvlan vlan-id`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#switchport qinq default-cvlan 2`
		Configure basic QinQ, add double Tags, and specify the PVID used by the CVLAN and SVLAN.
		• vlan-id: user VLAN ID, an integer, ranging from 1 to 4094

5	`Raisecom(config-gigaethernet1/1/port)#switchport reject-frame { tagged | untagged }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#switchport reject-frame tagged`
		Configure the types of packets disallowed to be forwarded.
		• tagged: packets with Tags
		• untagged: packets without Tags

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	`Raisecom(config-gigaethernet1/1/port)#`**`dot1q-tunnel tpid`** *`tpid`* **`Example:`** `Raisecom(config-gigaethernet1/1/1)#dot1q-tunnel tpid 9100`	Configure the TPID of the inner VLAN Tag on the interface. It is used identify the inner VLAN, or is used to identify the outer VLAN when QinQ is enabled. • tpid: TPID, in hexadecimal notation, an integer, being 0x8100, 0x88a8, or 0x9100
7	`Raisecom(config-gigaethernet1/1/port)#`**`dot1q-tunnel trust port-priority`** **`Example:`** `Raisecom(config-gigaethernet1/1/1)#dot1q-tunnel trust port-priority`	Configure the trust mode of basic QinQ to interface priority trust mode.

Note

- To use basic QinQ functions on an interface, configure its attributes first by configuring it to the Access or Trunk interface and configuring the default VLAN.
- When basic QinQ is enabled on the interface, all packets are processed as untagged packets. If you configure the untagged packets to be discarded, tagged packets are also discarded.
- VLAN mapping based on VLAN+CoS and VLAN mapping based on VLAN cannot be concurrently configured.

2.4.5 Configuring selective QinQ

Configure selective QinQ on the ingress interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface`** *`interface-type interface-number`* **`Example:`** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	`Raisecom(config-gigaethernet1/1/port)#`**`switchport vlan-mapping-miss discard`**	Configure the interface to discard tagged packets that fail to match selective QinQ or VLAN mapping rules.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-gigaethernet1/1/port)#**switchport vlan-mapping ethertype** { **arp** | **eapol** | **ip** | **ipv6** | **loopback** | **mpls** | **mpls-mcast** | **pppoe** | **pppoedisc** | **user-define** *protocol-id* | **x25** | **x75** } **add-outer** *outer-vlan-id* **Example:** Raisecom(config-gigaethernet1/1/1)#switchport vlan-mapping ethertype arp add-outer 2	Configure EtherType selective QinQ, and add mapping rules for Tag VLAN. • arp: address resolution protocol • eapol: EAPOL PAE/802.1x protocol • ip: Internet protocol • ipv6: IPv6 • loopback: loop protocol • mpls: MPLS unicast protocol • mpls-mcast: MPLS multicast protocol • pppoe: PPPOE session protocol • pppoedisc: PPPOE discovery protocol • x25: X.25 Layer 3 protocol • x75: X.75 interconnection protocol • user-define protocol id: user-defined protocol number • add-outer outer-vlan-id: ID of the added outer VLAN, an integer, ranging from 1 to 4049
5	Raisecom(config-gigaethernet1/1/1)#**switchport vlan-mapping both priority-tagged translate** *vlan-id* Raisecom(config-gigaethernet1/1/1)#**switchport vlan-mapping both vlan** *custom-vlan-id* [**cos** *cos-value*] **add-outer** *outer-vlan-id* Raisecom(config-gigaethernet1/1/1)#**switchport vlan-mapping both untag add-outer** *outer-vlan-id* **Example:** Raisecom(config-gigaethernet1/1/1)#switchport vlan-mapping both priority-tagged translate 10	(Optional) configure bidirectional selective QinQ, and add outer VLAN rules. The device supports this configuration on the LAG or in ISF mode. • vlan custom-vlan-list: customer VLAN list, an integer, ranging from 1 to 4094 • cos cos-value: customer Tag CoS, an integer, ranging from 0 to 7 • add-outer outer-vlan-id: ID of the outer VLAN to be added, an integer, ranging from 1 to 4094 • translate vlan-id: ID of the inner VLAN Tag to be modified, an integer, ranging from 1 to 4094 • untag: without tags • priority-tagged: match tagged packets with priority

Note

- Selection QinQ and 1:1 VLAN mapping can be concurrently configured on the same interface.
- Double-tagged VLAN mapping cannot be concurrently configured with basic QinQ or tagged CVLAN/Priority-tagged VLAN mapping on the same interface.

Copyright © Raisecom Technology Co., Ltd.

2.4.6 Configuring network-side interface to Trunk mode

Configure the network-side interface to Trunk mode for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	`Raisecom(config-gigaethernet1/1/port)#switchport mode trunk`	Configure interface trunk mode, permit double-tagged packet to pass.

2.4.7 Configuring TPID

Configure the TPID on the network side interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	`Raisecom(config-gigaethernet1/1/port)#tpid` *`tpid`* **Example:** `Raisecom(config-gigaethernet1/1/1)#tpid 9100`	Configure the TPID of the outer VLAN Tag on the interface. • tpid: TPID value, in dotted hexadecimal notation, an integer, being 0x8100, 0x88a8, or 0x9100

2.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show dot1q-tunnel`	Show configurations of basic QinQ.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
2	`Raisecom#show vlan-mapping both interface interface-type interface-number`	Show configurations of selective QinQ.
3	`Raisecom#show vlan-mapping interface interface-type interface-number add-outer`	Show configurations of selective QinQ of EtherType on the interface.

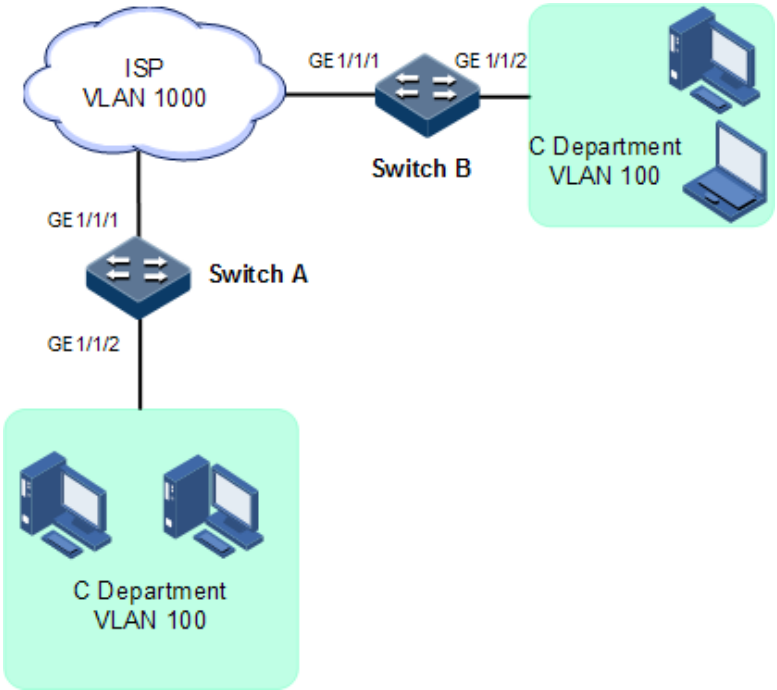
2.4.9 Example for configuring basic QinQ

Networking requirements

As shown in Figure 2-7, Switch A and Switch B are connected to two branches of Department C, which are in different locations. Department C uses VLAN 100, and needs to communicate through VLAN 1000 of the carrier network. The carrier TPID is 9100.

Configure basic QinQ on Switch A and Switch B to enable normal communication inside a department through the carrier's network.

Figure 2-7 Basic QinQ networking



Configuration steps

Configure Switch A and Switch B.

Configurations of Switch A are the same with those of Switch B. Take Switch A for example.

Step 1 Create VLAN 100 and VLAN 1000, and activate them. TPID is 9100.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#config
Raisecom(config)#create vlan 100,1000 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk allowed vlan 1000
Raisecom(config-gigaethernet1/1/1)#tpid 9100
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 2 Configure basic QinQ on the interface.

```
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#switchport trunk native vlan 1000
Raisecom(config-gigaethernet1/1/2)#dot1q-tunnel
Raisecom(config-gigaethernet1/1/2)#switchport qinq 100
Raisecom(config-gigaethernet1/1/2)#exit
```

Checking results

Use the **show dot1q-tunnel** command to show QinQ configurations.

```
Raisecom#show dot1q-tunnel
Interface          QinQ Status  Outer TPID on port  Cos override Vlan-
map-miss drop
-------------------------------------------------------
gigaethernet1/1/1     -              0x9100          -      disable
gigaethernet1/1/2  Dot1q-tunnel      0x8100          -      disable
```

2.4.10 Example for configuring selective QinQ

Networking requirements

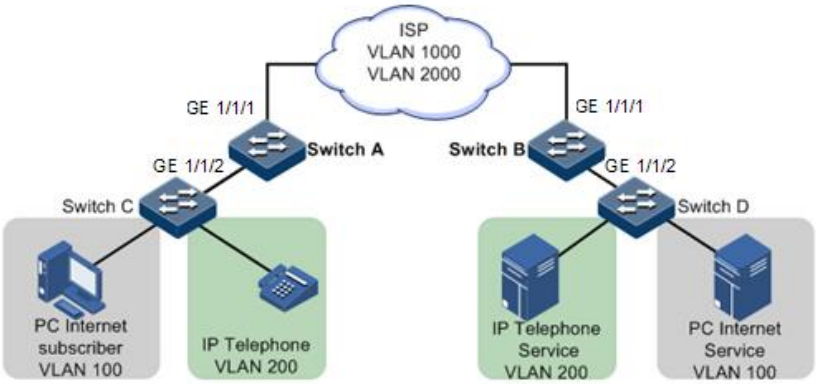
As shown in Figure 2-8, the carrier network contains common PC Internet access services and IP phone services. PC Internet access services are assigned to VLAN 1000, and IP phone services are assigned to VLAN 2000.

Configure Switch A and Switch B as below to make the user and server communicate through the carrier network:

- Add outer Tag VLAN 1000 to VLAN 100 assigned to PC Internet access services.
- Add outer Tag 2000 to VLAN 200 for IP phone services.
- The carrier TPID is 9100.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-8 Selective QinQ networking



Configuration steps

Configure Switch A and Switch B.

Configurations of Switch A are the same with those of Switch B. Take Switch A for example.

Step 1 Create and activate VLAN 100, VLAN 200, VLAN 1000, and VAN 2000. The TPID is 9100.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100,200,1000,2000 active
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 1000,2000
SwitchA(config-gigaethernet1/1/1)#tpid 9100
SwitchA(config-gigaethernet1/1/1)#exit
```

Step 2 Enable selective QinQ on GE 1/1/2.

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#switchport trunk allowed vlan
100,200,1000,2000
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping both vlan 100
add-outer 1000
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping both vlan 200
add-outer 2000
SwitchA(config-gigaethernet1/1/2)#exit
```

Checking results

Use the following command to show configurations of selective QinQ.

Take Switch A for example.

Copyright © Raisecom Technology Co., Ltd.

```
SwitchA#show vlan-mapping both interface gigaethernet 1/1/2
Both Direction VLAN QinQ mapping rule:
Interface  : GE1/1/2
Default cvlan: --
--------------------------------
Original Outer VLANs: --
Original Outer COS:   --
Original Inner VLANs: 100
Original Inner COS:   --
Vlan mapping Mode:    S-ADD
New Outer-VID:       1000
New Outer-COS:       --
New Inner-VID:       --
New Inner-COS:       --
---------------------------
Original Outer VLANs: --
Original Outer COS:   --
Original Inner VLANs: 200
Original Inner COS:   --
Vlan mapping Mode:    S-ADD
New Outer-VID:       2000
New Outer-COS:       --
New Inner-VID:       --
New Inner-COS:       --
---------------------------
```

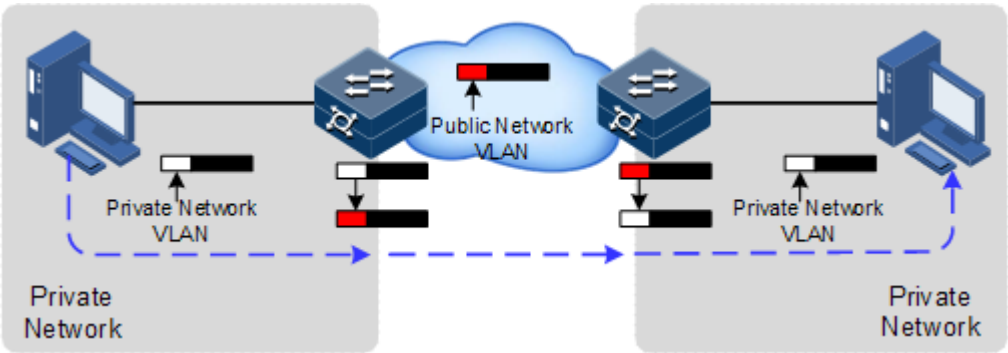
2.5 VLAN mapping

2.5.1 Introduction

VLAN mapping is used to replace the private VLAN Tag of Ethernet packets with carrier's VLAN Tag, making packets transmitted according to carrier's VLAN forwarding rules. When packets are sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Therefore packets are correctly sent to the destination.

Figure 2-9 shows principles of VLAN mapping.

Figure 2-9 Principles of VLAN mapping



After receiving a user private network packet with a VLAN Tag, the ISCOM2600G series switch matches the packet according to configured VLAN mapping rules. If successful, it maps the packet according to configured VLAN mapping rules.

By supporting 1: 1 VLAN mapping, the ISCOM2600G series switch replaces the VLAN Tag carried by a packet from a specified VLAN to the new VLAN Tag.

Different from QinQ, VLAN mapping does not encapsulate packets with multiple layers of VLAN Tags, but needs to modify VLAN Tag so that packets are transmitted according to the carrier's VLAN forwarding rule.

2.5.2 Preparing for configurations

Scenario

Different from QinQ, VLAN mapping is used to change the VLAN Tag without encapsulating multilayer VLAN Tag so that packets are transmitted according to the carrier's VLAN mapping rules. VLAN mapping does not increase the frame length of the original packet. It can be used in the following scenarios:

- A user service needs to be mapped to a carrier's VLAN ID.
- Multiple user services need to be mapped to a carrier's VLAN ID.

Prerequisite

- Connect the interface.
- Configure its physical parameters to make it Up.
- Create VLANs.

2.5.3 Default configurations of VLAN mapping

Default configurations of VLAN mapping are as below.

Function	Default value
VLAN mapping status	Disable

2.5.4 Configuring VLAN mapping

Configure VLAN mapping for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **`Example:`** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-gigaethernet1/1/port)#**switchport vlan-mapping both outer** *outer-vlan-id* **translate** *outer-vlan-id* Raisecom(config-gigaethernet1/1/port)#**switchport vlan-mapping both outer** *outer-vlan-id* **inner** *inner-vlan-id* **translate outer** *outer-vlan-id* **inner** *inner-vlan-id* Raisecom(config-gigaethernet1/1/port)#**switchport vlan-mapping both outer** *outer-vlan-id* **cos** *cos-value* **translate** *outer-vlan-id* **Example:** Raisecom(config-gigaethernet1/1/1)#switchport vlan-mapping both outer 50 translate 100	Configure the VLAN mapping rule based on outer and inner VLAN Tag in both the ingress and egress directions of the interface. • outer-vlan-id: outer VLAN ID, an integer, ranging from 1 to 4094 • inner-vlan-id: inner VLAN ID, an integer, ranging from 1 to 4094 • cos-value: outer Tag CoS, an integer, ranging from 0 to 7
4	Raisecom(config-gigaethernet1/1/port)#**switchport vlan-mapping both** *vlan-list* **translate** *vlan-id* **Example:** Raisecom(config-gigaehternet1/1/1)#switchport vlan-mapping both 5-10 translate 100	Configure the bidirectional N:1 VLAN mapping rule. • vlan-list: customer VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • vlan-id: inner VLAN ID, an integer, ranging from 1 to 4094

Note

- Basic QinQ and 1:1 VLAN mapping can be concurrently configured. VLAN mapping functions normally before or after basic QinQ is enabled.
- Selective QinQ and 1:1 VLAN mapping can be concurrently configured. When they are concurrently configured, they function normally. They also function normally when basic QinQ is enabled or disable. When one of them is disabled, other configurations function normally.
- Basic QinQ, selective QinQ, and 2:2 VLAN mapping are mutually exclusive. When selective QinQ and 1:1 VLAN mapping are configurrently configured, their matching VLANs cannot be the same, and VLANs after mapping cannot be the same.
- To concurrently configure N:1 VLAN mapping and VLAN Copy, configure VLAN Copy, and then configure N:1 VLAN mapping.

2.5.5 Checking configurations

Use the following commands to check configuration results.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
1	`Raisecom#show vlan-mapping both interface interface-type interface-number`	Show configurations of VLAN mapping.
2	`Raisecom#show vlan-mapping interface interface-type interface-number both translate`	Show configurations of N:1 VLAN mapping on the interface.

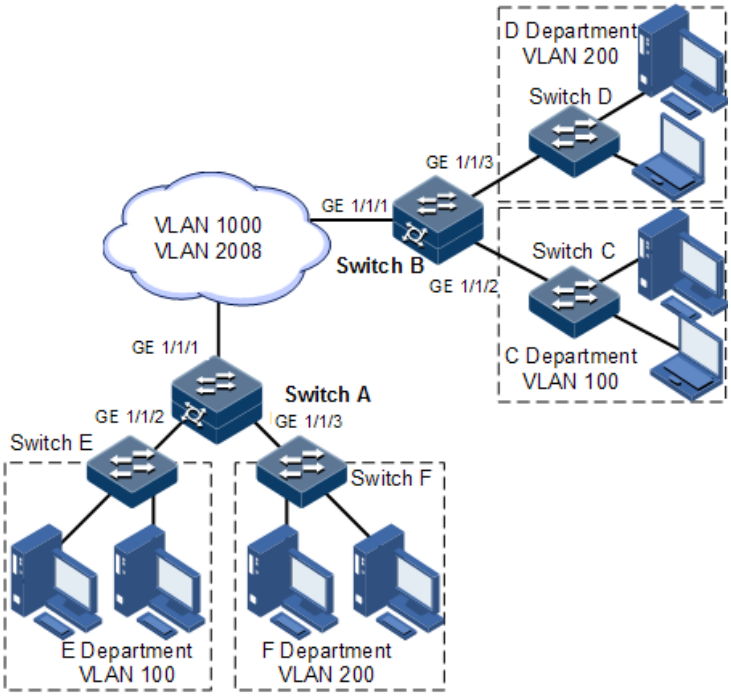
2.5.6 Example for configuring VLAN mapping

Scenario

As shown in Figure 2-10, GE 1/1/2 and GE 1/1/3 on Switch A are connected to Department E using VLAN 100 and Department F using VLAN 200; GE 1/1/2 and GE 1/1/3 on Switch A are connected to Department C using VLAN 100 and Department D using VLAN 200. The carrier's network uses VLAN 1000 to transmit services between Department E and Department C and uses VLAN 2008 to transmit services between Department F and Department D.

Configure 1:1 VLAN mapping between Switch A and Switch B to implement normal communication inside each department.

Figure 2-10 VLAN mapping networking



Configuration steps

Configure Switch A and Switch B.

Configuration steps for Switch A and Switch B are the same. Take Switch A for example.

Copyright © Raisecom Technology Co., Ltd.

Step 1 Create VLANs 100, 200, 1000, and 2008, and activate them.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100,200,1000,2008 active
```

Step 2 Configure GE 1/1/1 to Trunk mode, allowing packets of VLAN 1000 and VLAN 2008 to pass.

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 1000,2008
confirm
SwitchA(config-gigaethernet1/1/1)#exit
```

Step 3 Configure GE 1/1/2 to Trunk mode, allowing packets of VLAN 100 to pass. Configure VLAN mapping rules.

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#switchport trunk allowed vlan 100
confirm
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping both outer 100
translate 1000
SwitchA(config-gigaethernet1/1/2)#exit
```

Step 4 Configure GE 1/1/3 to Trunk mode, allowing packets of VLAN 200 to pass. Configure VLAN mapping rules.

```
SwitchA(config)#interface gigaethernet 1/1/3
SwitchA(config-gigaethernet1/1/3)#switchport mode trunk
SwitchA(config-gigaethernet1/1/3)#switchport trunk allowed vlan 200
confirm
SwitchA(config-gigaethernet1/1/3)#switchport vlan-mapping bother outer
200 translate 2008
```

Checking results

Use the **show vlan-mapping both interface** command to show configurations of 1:1 VLAN mapping.

```
SwitchA#show vlan-mapping both interface gigaethernet 1/1/2
Both Direction VLAN QinQ mapping rule:
Interface  : GE 1/1/2
```


Copyright © Raisecom Technology Co., Ltd.

```
Default cvlan: --
----------------------------
Original Outer VLANs: 100
Original Outer COS:   --
Original Inner VLANs: --
Original Inner COS:   --
Vlan mapping Mode:    S-TRANS
New Outer-VID:       1000
New Outer-COS:       --
New Inner-VID:       --
New Inner-COS:       --

-------------------------

SwitchA#show vlan-mapping both interface gigaethernet 1/1/3
Both Direction VLAN QinQ mapping rule:
Interface  : GE 1/1/3
Default cvlan: --
----------------------------
Original Outer VLANs: 200
Original Outer COS:   --
Original Inner VLANs: --
Original Inner COS:   --
Vlan mapping Mode:    S-TRANS
New Outer-VID:       2008
New Outer-COS:       --
New Inner-VID:       --
New Inner-COS:       --
----------------------------
```

2.6 STP/RSTP

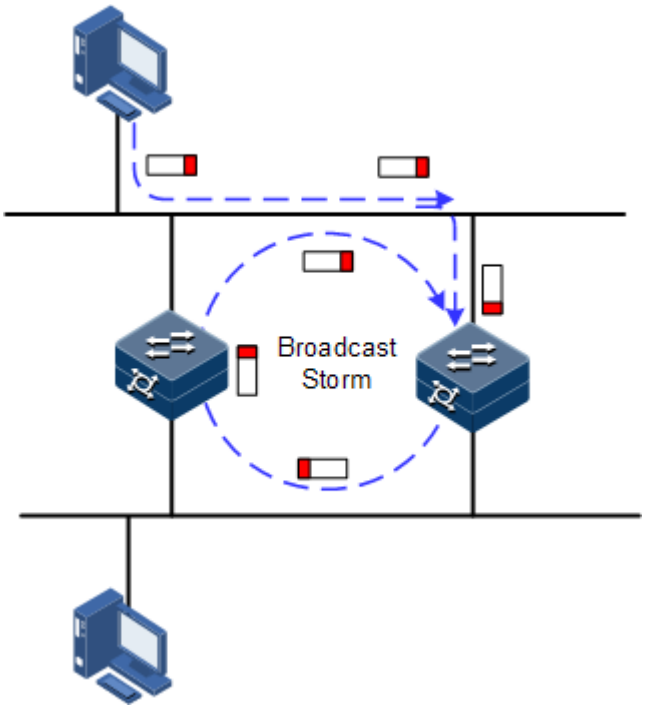
2.6.1 Introduction

STP

With the increasing complexity of network structure and growing number of switches on the network, the Ethernet network loops become the most prominent problem. Because of the packet broadcast mechanism, a loop causes the network to generate storms, exhaust network resources, and have serious impact to forwarding normal data. The network storm caused by the loop is shown in Figure 2-11.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-11 Network storm due to loopback



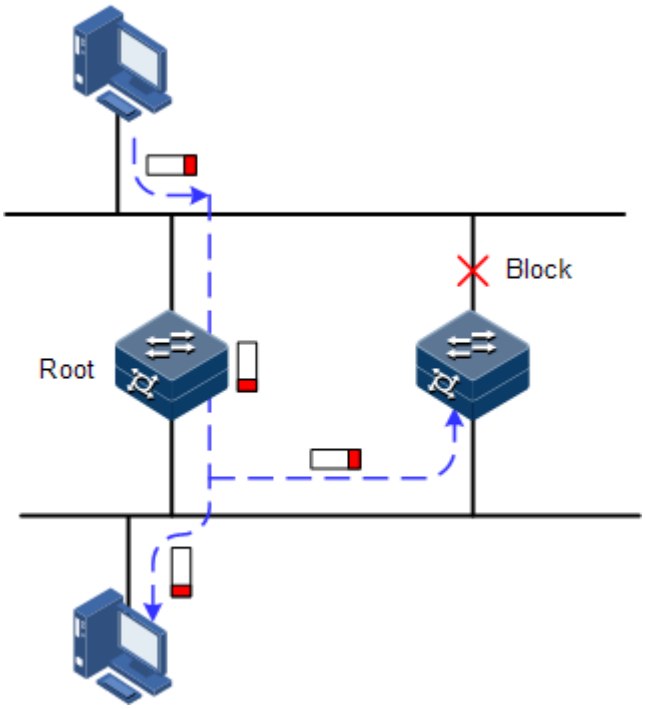
Spanning Tree Protocol (STP) is compliant to IEEE 802.1d standard and used to remove data physical loop in data link layer in the LAN.

The ISCOM2600G series switch running STP can process Bridge Protocol Data Unit (BPDU) with each other for the election of root switch and selection of root port and designated port. It also can block loop interface on the ISCOM2600G series switch logically according to the selection results, and finally trims the loop network structure to tree network structure without loop which takes an ISCOM2600G series switch as root. This prevents the continuous proliferation and limitless circulation of packet on the loop network from causing broadcast storms and avoids declining packet processing capacity caused by receiving the same packets repeatedly.

Figure 2-12 shows loop networking with STP.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-12 Loop networking with STP



Although STP can eliminate loop network and prevent broadcast storm well, its shortcomings are still gradually exposed with thorough application and development of network technology.

The major disadvantage of STP is the slow convergence speed.

RSTP

For improving the slow convergent speed of STP, IEEE 802.1w establishes Rapid Spanning Tree Protocol (RSTP), which increases the mechanism to change interface blocking state to forwarding state, speed up the topology convergence rate.

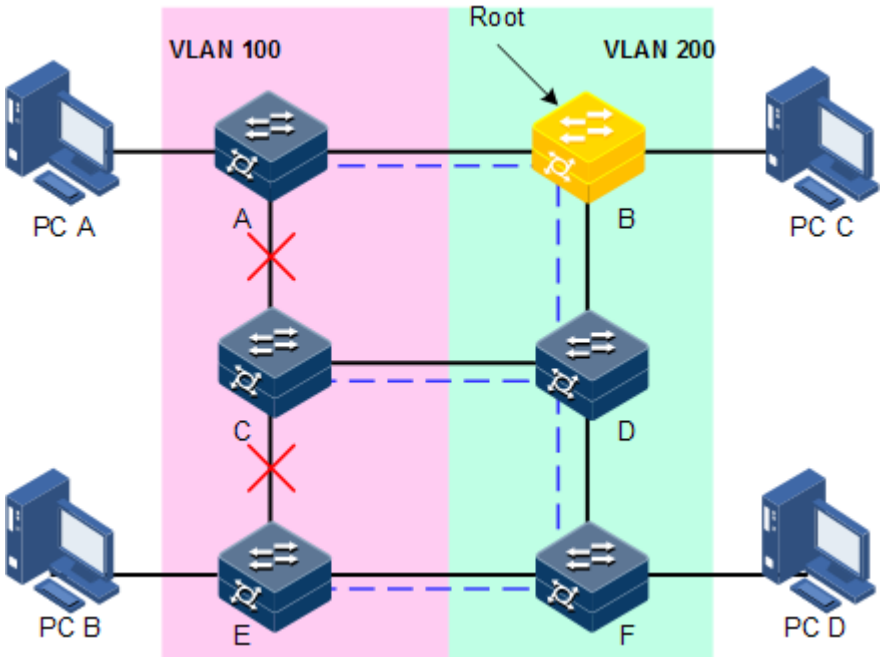
The purpose of STP/RSTP is to simplify a bridged LAN to a unitary spanning tree in logical topology and to avoid broadcast storm.

The disadvantages of STP/RSTP are exposed with the rapid development of VLAN technology. The unitary spanning tree simplified from STP/RSTP leads to the following problems:

- The whole switching network has only one spanning tree, which will lead to longer convergence time on a larger network.
- After a link is blocked, it does not carry traffic any more, causing waste of bandwidth.
- Packet of partial VLAN cannot be forwarded when network structure is unsymmetrical. As shown in Figure 2-13, Switch B is the root switch; RSTP blocks the link between Switch A and Switch C logically and makes that the VLAN 100 packet cannot be transmitted and Switch A and Switch C cannot communicate.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-13 Failure in forwarding VLAN packets due to RSTP



2.6.2 Preparation for configuration

Networking situation

In a big LAN, multiple devices are concatenated for accessing each other among hosts. They need to be enabled with STP to avoid loop among them, MAC address learning fault, and broadcast storm and network down caused by quick copy and transmission of data frame. STP calculation can block one interface in a broken loop and ensure that there is only one path from data flow to the destination host, which is also the best path.

Preconditions

N/A

2.6.3 Default configurations of STP

Default configurations of STP are as below.

Function	Default value
Global STP status	Disable
Interface STP status	Enable
STP priority of device	32768
STP priority of interface	128
Path cost of interface	0
Max Age timer	20s
Hello Time timer	2s

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
Forward Delay timer	15s

2.6.4 Enabling STP

Enable STP for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#spanning-tree { enable | disable }`
	Example:
	`Raisecom(config)#spanning-tree enable`
		Enable or disable global STP.
		• enable: enable STP.
		• disable: disable STP.

3	`Raisecom(config)#spanning-tree mode { stp | rstp | mrstp }`
	Example:
	`Raisecom(config)#spanning-tree mode stp`
		Configure spanning tree mode.
		• STP: the device is working in the global STP-compatible mode.
		• RSTP: the device is working in the global RSTP mode.
		• MRSTP: the device is working in the global MRSTP mode.

4	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

5	`Raisecom(config-gigaethernet1/1/port)#spanning-tree { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/port)#spanning-tree enable`
		Enable interface STP.
		• enable: enable STP.
		• disable: disable STP.

2.6.5 Configuring STP parameters

Configure STP parameters for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**spanning-tree [instance** *instance-id* **] priority** *priority-value* **Example:** Raisecom(config)#spanning-tree instance 1 priority 8192	(Optional) configure device priorities. • instance-id: MSTI ID, an integer, ranging from 0 to 4095 • priority-value: priority. The system priority ranges from 0 to 61440 in step of 4096, such as 0, 4096, and 8192. The interface priority ranges from 0 to 240 in step of 16, such as 0, 16, and 32.
3	Raisecom(config)#**spanning-tree** [**instance** *instance-id*] **root** { **primary** | **secondary** } **Example:** Raisecom(config)#spanning-tree root primary	(Optional) configure the device as the root or backup device. • instance-id: MSTI number, an integer, ranging from 1 to 4095 • primary: configure the device as the primary root device. • secondary: configure the device as the backup root device.
4	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-gigaethernet1/1/port)#**spanning-tree [instance** *instance-id* **] priority** *priority-value* **Example:** Raisecom(config-gigaethernet1/1/1)#spanning-tree priority 64	(Optional) configure interface priorities on the device. • instance-id: MSTI ID, an integer, ranging from 0 to 4095 • priority-value: priority. The system priority ranges from 0 to 61440 in step of 4096, such as 0, 4096, and 8192. The interface priority ranges from 0 to 240 in step of 16, such as 0, 16, and 32.
5	Raisecom(config-gigaethernet1/1/port)#**spanning-tree extern-path-cost** *cost* Raisecom(config-gigaethernet1/1/port)#**exit** **Example:** Raisecom(config-gigaethernet1/1/1)#spanning-tree extern-path-cost 10	(Optional) configure the path cost of the external interface on the device. • cost: path cost value, an integer, ranging from 0 to 200000000
6	Raisecom(config-gigaethernet1/1/port)#**spanning-tree** [**instance** *instance-id*] **inter-path-cost** *cost* **Example:** Raisecom(config-gigaethernet1/1/1)#spanning-tree instance 1 inter-path-cost 10	(Optional) configure the path cost of the internal interface on the device. • instance-id: MSTI ID, an integer, ranging from 0 to 4095 • cost: path cost value, an integer, ranging from 0 to 200000000
7	Raisecom(config)#**spanning-tree hello-time** *period* **Example:** Raisecom(config)#spanning-tree hello-time 3	(Optional) configure the value of Hello Time. • period: interval for sending BPDUs, an integer, ranging from 1 to 10, in units of second

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
8	Raisecom(config)#**spanning-tree transmit-limit** *max-num* **Example:** Raisecom(config)#spanning-tree transmit-limit 10	(Optional) configure the maximum transmission rate of the interface. • max-num: maximum number of packets, an integer, ranging from 1 to 10
9	Raisecom(config)#**spanning-tree forward-delay** *period* **Example:** Raisecom(config)#spanning-tree forward-delay 10	(Optional) configure forward delay. • period: forward-delay period, an integer, ranging from 4 to 30, in units of second
10	Raisecom(config)#**spanning-tree max-age** *period* **Example:** Raisecom(config)#spanning-tree max-age 30	(Optional) configure the maximum age. • period: time value, an integer, ranging from 6 to 40, in units of second
11	Raisecom(config)#**spanning-tree pathcost-standard** { **dot1d-1998** | **dot1t** } **Example:** Raisecom(config)#spanning-tree pathcost-standard dot1t	(Optional) configure the standard for calculating path cost of the panning tree. • dot1d-1998: the standard for calculating path cost of the panning tree is dot1d-1998. • dot1t: the standard for calculating path cost of the panning tree is dot1t.

2.6.6 Configuring edge interface

The edge interface indicates that the interface neither directly connects to any devices nor indirectly connects to any device through the network.

The edge interface can change the interface status to forward quickly without any waiting time. You had better configure the Ethernet interface connected to user client as edge interface to make it quick to change to forward status.

The edge interface attribute depends on actual condition when it is in auto-detection mode; the real port will change to false edge interface after receiving BPDU when it is in force-true mode; when the interface is in force-false mode, whether it is true or false edge interface in real operation, it will maintain the force-false mode until the configuration is changed.

By default, all interfaces on the ISCOM2600G series switch are configured in auto-detection attribute.

Configure the edge interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config-gigaethernet1/1/port)#**spanning-tree edged-port** { **auto** | **force-true** | **force-false** } **Example:** Raisecom(config-gigaethernet1/1/1)#spanning-tree edged-port force-true	Configure attributes of the RSTP edge interface. • auto: automatically detect whether it is an edge interface • force-true: forced to be an edge interface • force-false: forced to be a non-edge interface

2.6.7 Configuring link type

Two interfaces connected by a point-to-point link can quickly transit to forward status by transmitting synchronization packets. By default, MSTP configures the link type of interfaces according to duplex mode. The full duplex interface is considered as the point-to-point link, and the half duplex interface is considered as the shared link.

You can manually configure the current Ethernet interface to connect to a point-to-point link, but the system will fail if the link is not point to point. Generally, we recommend configuring this item in auto status and the system will automatically detect whether the interface is connected to a point-to-point link.

Configure the link type for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config-gigaethernet1/1/port)#**spanning-tree link-type** { **auto** | **point-to-point** | **shared** } **Example:** Raisecom(config-gigaethernet1/1/1)#spanning-tree link-type point-to-point	Configure the link type for interface. • auto: automatically detect whether the link connected to the interface is a point-to-point link. • point-to-point: the link connected to the current interface is a point-to-point link. • shared: the link connected to the current interface is a shared link.

Copyright © Raisecom Technology Co., Ltd.

2.6.8 Configuring BPDU filtering

After being enabled with BPDU filtering, the edge interface does not send BPDUs nor process received BPDUs.

Configure BPDU filtering for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#spanning-tree edged-port bpdu-filter { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#spanning-tree edged-port bpdu-filter enable`
		Enable or disable BPDU filtering on the edge interface.
		• enable: enable the BPDU filter on the edge interface.
		• disable: disable the BPDU filter on the edge interface.

2.6.9 Configuring BPDU Guard

Generally, on a switch, interfaces are directly connected with terminals (such as a PC) or file servers are configured to an edge interfaces. Therefore, these interfaces can be transferred quickly.

In normal status, these edge interfaces will not receive BPDUs. If somebody attacks the switch by forging the BPDU, the device will configure these edge interfaces to non-edge interfaces when these edge interfaces receive the forged BPDU and re-perform spanning tree calculation. This may cause network vibration.

BPDU Guard provided by MSTP can prevent this attack. After BPDU Guard is enabled, edge interfaces can avoid attack from forged BPDUs.

After BPDU Guard is enabled, the device will shut down the edge interfaces if they receive BPDUs and notify the NView NNM system of the case. The blocked edge interface is restored only by the administrator through the CLI.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#spanning-tree bpduguard { enable | disable }`
	Example:
	`Raisecom(config)#spanning-tree bpduguard enable`
		Enable BPDU Guard.
		• enable: enable BPDU Guard.
		• disable: disable BPDU Guard.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

3	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

4	`Raisecom(config-gigaethernet1/1/port)#no spanning-tree bpduguard shutdown port`	Manually restore interfaces that are shut down by BPDU Guard.

Note

When the edge interface is enabled with BPDU filtering and the device is enabled with BPDU Guard, BPDU Guard takes effect first. Therefore, an edge interface is shut down if it receives a BPDU.

2.6.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show spanning-tree [ instance instance-id ] [ detail ]`	Show basic configurations of STP.
2	`Raisecom#show spanning-tree [ instance instance-id ] interface-type interface-list [ detail ]`	Show configurations of the spanning tree on the interface.

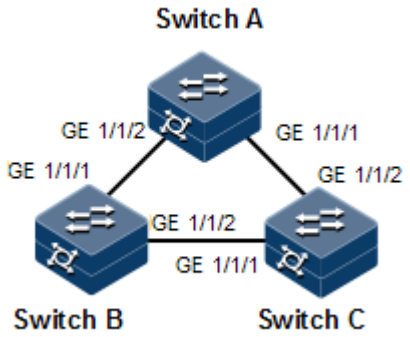
2.6.11 Example for configuring STP

Networking requirements

As shown in Figure 2-14, Switch A, Switch B, and Switch C form a ring network, so the loop must be eliminated in the situation of a physical link forming a ring. Enable STP on them, configure the priority of Switch A to 0, and path cost from Switch B to Switch A to 10.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-14 STP networking



Configuration steps

Step 1 Enable STP on Switch A, Switch B, and Switch C.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree mode stp
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree mode stp
```

Configure Switch C.

```
Raisecom#hostname SwitchC
SwitchC#config
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree mode stp
```

Step 2 Configure interface modes on three switches.

Configure Switch A.

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#exit
```


Copyright © Raisecom Technology Co., Ltd.

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#exit
```

Configure Switch B.

```
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#exit
```

Configure Switch C.

```
SwitchC(config)#interface gigaethernet 1/1/1
SwitchC(config-gigaethernet1/1/1)#switchport mode trunk
SwitchC(config-gigaethernet1/1/1)#exit
SwitchC(config)#interface gigaethernet 1/1/2
SwitchC(config-gigaethernet1/1/2)#switchport mode trunk
SwitchC(config-gigaethernet1/1/2)#exit
```

Step 3 Configure priority of spanning tree and interface path cost.

Configure Switch A.

```
SwitchA(config)#spanning-tree priority 0
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#spanning-tree extern-path-cost 10
```

Configure Switch B.

```
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#spanning-tree extern-path-cost 10
```

Checking results

Use the **show spanning-tree** command to show bridge status.

Take Switch A for example.

```
SwitchA#show spanning-tree
```


Copyright © Raisecom Technology Co., Ltd.

```
Spanning-tree admin state: enable
Spanning-tree protocol mode: STP

Spanning-tree pathcost-standard: Dot1t
BridgeId:    Mac 000E.5EAB.CDEF  Priority 0
Root:       Mac 000E.5EAB.CDEF  Priority 0     RootCost 0
Operational:  HelloTime 2   ForwardDelay 15  MaxAge 20
Configured:   HelloTime 2   ForwardDelay 15  MaxAge 20  TransmitLimit 3
           MaxHops   20  Diameter 7
```

Use the **show spanning-tree port-list** *port-list* command to show interface status.

Take Switch A for example.

```
SwitchA#show spanning-tree gigaethernet 1/1/1
GE1/1/1
PortProtocolEnable: admin: enable oper: enable
Rootguard:  disable
Loopguard:  disable
Bpduguard:  disable
TcRejection:disable
ExternPathCost:20000
Partner STP Mode: stp
Bpdus send:   48    (TCN<0>  Config<48>  RST<0>  MST<0>)
Bpdus received:0     (TCN<0>  Config<0>  RST<0>  MST<0>)
State:forwarding  Role:designated  Priority:128    Cost: 20000
Root:           Mac 5051.5051.5053  Priority 0      RootCost       0
DesignatedBridge: Mac 5051.5051.5053  Priority 0      DesignatedPort
33041
```

2.7 MSTP

2.7.1 Introduction

Multiple Spanning Tree Protocol (MSTP) is defined by IEEE 802.1s. Recovering the disadvantages of STP and RSTP, the MSTP implements fast convergence and distributes different VLAN flow following its own path to provide an excellent load balancing mechanism.

MSTP divides a switch network into multiple regions, called MST region. Each MST region contains several spanning trees but the trees are independent from each other. Each spanning tree is called a Multiple Spanning Tree Instance (MSTI).

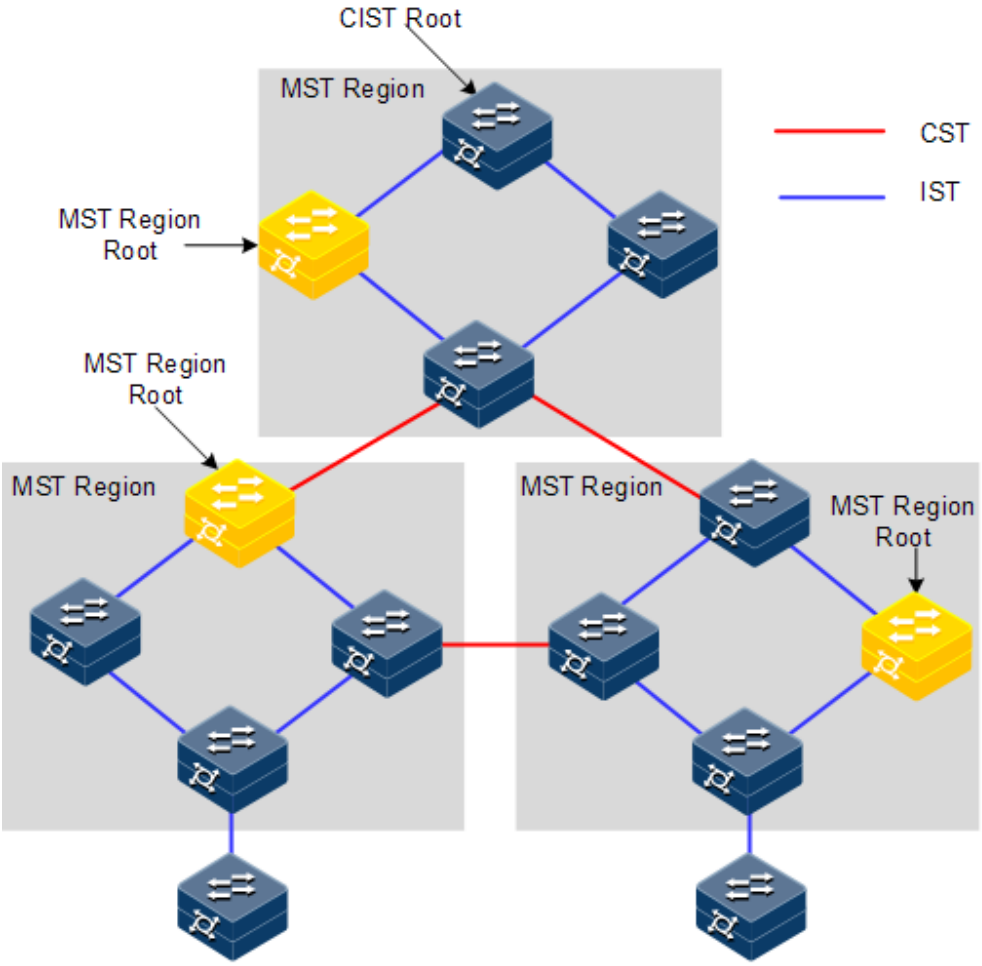
MSTP protocol introduces Common Spanning Tree (CST) and Internal Spanning Tree (IST) concepts. CST refers to taking MST region as a whole to calculate and generating a spanning tree. IST refers to generating spanning tree in internal MST region.

Compared with STP and RSTP, MSTP also introduces total root (CIST Root) and region root (MST Region Root) concepts. The total root is a global concept; all switches running STP/RSTP/MSTP can have only one total root, which is the CIST Root. The region root is a

Copyright © Raisecom Technology Co., Ltd.

local concept, which is relative to an instance in a region. As shown in Figure 2-15, all connected devices only have one total root, and the number of region root contained in each region is associated with the number of instances.

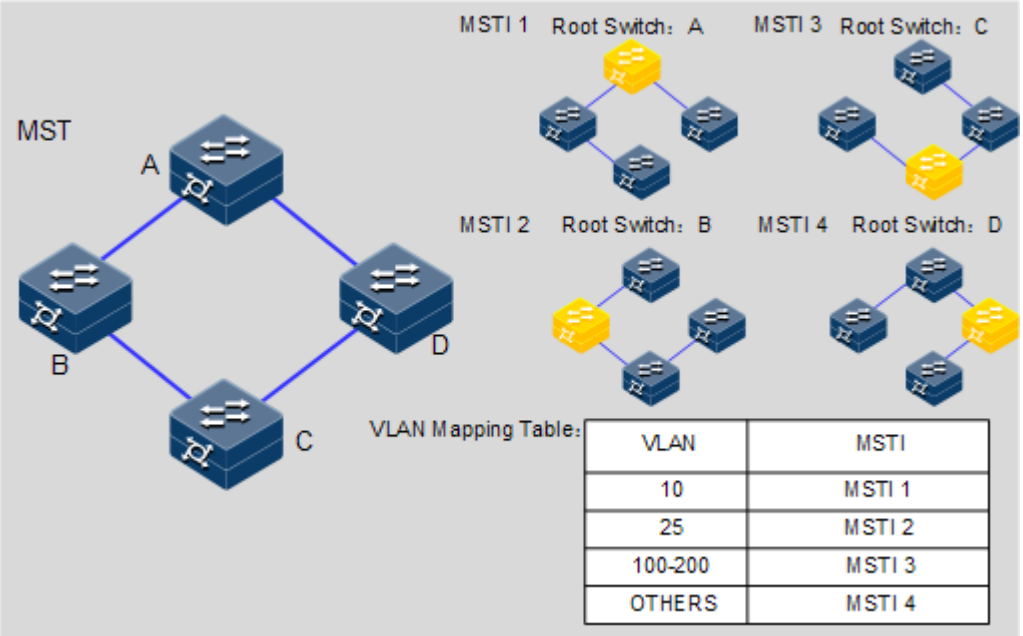
Figure 2-15 Basic concepts of the MSTI network



There can be different MST instance in each MST region, which associates VLAN and MSTI by configuring the VLAN mapping table (relationship table of VLAN and MSTI). The concept sketch map of MSTI is shown in Figure 2-16.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-16 MSTI concepts



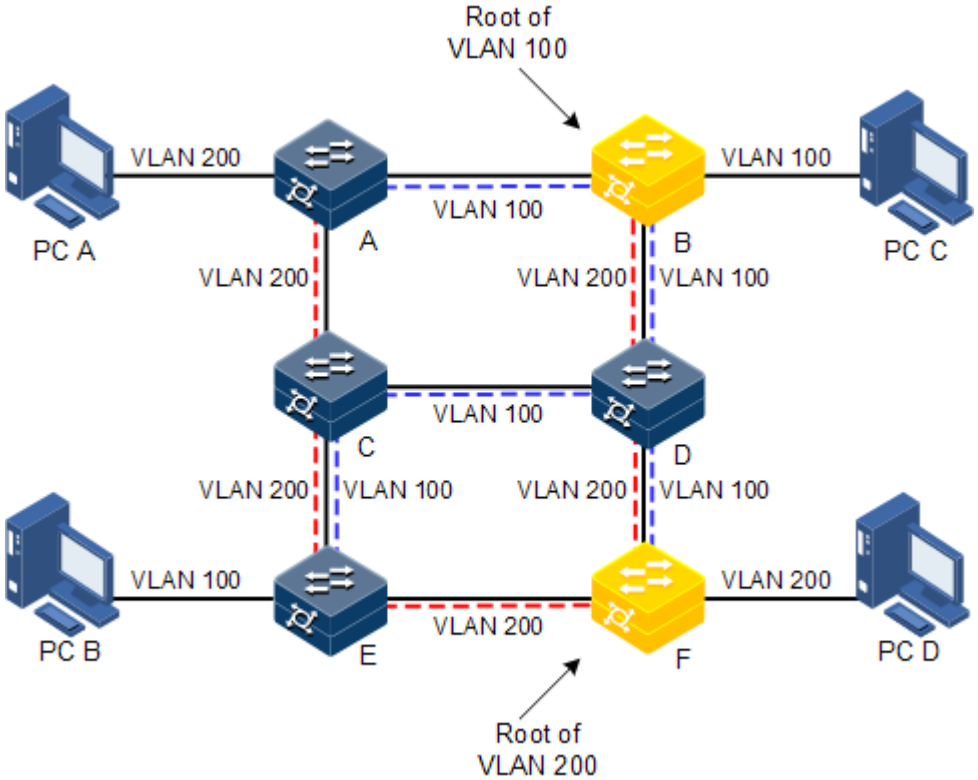
Note

Each VLAN can map to one MSTI; in other words, data of one VLAN can only be transmitted in one MSTI but one MSTI may correspond to several VLANs.

Compared with STP and RSTP mentioned previously, MSTP has obvious advantages, including cognitive ability of VLAN, load balancing, similar RSTP interface status switching, and binding multiple VLAN to one MST instance, to reduce resource occupancy rate. In addition, devices running MSTP on the network are also compatible with the devices running STP and RSTP.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-17 Networking with multiple spanning trees instances in MST region



Apply MSTP to the network as shown in Figure 2-17. After calculation, there are two spanning trees generated at last (two MST instances):

- MSTI 1 takes B as the root switch, forwarding packet of VLAN 100.
- MSTI 2 takes F as the root switch, forwarding packet of VLAN 200.

In this case, all VLANs can communicate internally, different VLAN packets are forwarded in different paths to share loading.

2.7.2 Preparation for configuration

Scenario

In a big LAN or residential region aggregation, the aggregation devices make up a ring for link backup, avoiding loop and realizing load balancing. MSTP can select different and unique forwarding paths for each one or a group of VLANs.

Prerequisite

N/A

2.7.3 Default configurations of MSTP

Default configurations of MSTP are as below.

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
Global MSTP status	Disable
Interface MSTP status	Enable
Maximum number of hops in the MST region	20
MSTP priority of the device	32768
MSTP priority of the interface	128
Path cost of the interface	0
Maximum number of packets sent within each Hello time	3
Max Age timer	20s
Hello Time timer	2s
Forward Delay timer	15s
Revision level of the MST region	0

2.7.4 Enabling MSTP

Enable MSTP for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#spanning-tree mode mstp`	Configure spanning tree for MSTP.

3	`Raisecom(config)#spanning-tree { enable | disable }`
	Example:
	`Raisecom(config)#spanning-tree enable`
		Enable or disable global or interface STP.
		• enable: enable MSTP.
		• disable: disable MSTP.

4	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

5	`Raisecom(config-gigaethernet1/1/port)#spanning-tree { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/port)#spanning-tree enable`
		Enable or disable interface STP. The device supports this configuration on the LAG interface.
		• enable: enable MSTP.
		• disable: disable MSTP.

Copyright © Raisecom Technology Co., Ltd.

2.7.5 Configuring MST region and its maximum number of hops

You can configure region information about the ISCOM2600G series switch when it is running in MSTP mode. The device MST region is determined by the region name, VLAN mapping table and configuration of MSTP revision level. You can configure current device in a specific MST region through following configuration.

The MST region scale is restricted by the maximum number of hops. Starting from the root bridge of spanning tree in the region, the number of forwarding hops decreases by 1 when the configuration message (BPDU) passes a device; the ISCOM2600G series switch discards the configuration message whose number of hops is 0. The device exceeding the maximum number of hops cannot join spanning tree calculation, so the MST region scale is restricted.

Configure MSTP region and its maximum number of hops for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#spanning-tree region-configuration`	Enter MST region configuration mode.

3	`Raisecom(config-region)#name name`
	Example:
	`Raisecom(config-region)#name mst1`
		Configure the MST region name.
		• name: MST region name, a string of 1 to 32 characters

4	`Raisecom(config-region)#revision-level level`
	Example:
	`Raisecom(config-region)#revision-level 20`
		Configure the revision level for the MST region.
		• level: revision level, an integer, ranging from 0 to 65535

5	`Raisecom(config-region)#instance instance-id vlan vlan-list`
	`Raisecom(config-region)#exit`
	Example:
	`Raisecom(config-region)#instance 1 vlan 100-200`
		Configure mapping from the MST region VLAN to instance.
		• instance-id: MSTI ID, an integer, ranging from 1 to 4095
		• vlan-list: VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". While using the no form of this command, the MSTI will be deleted if the parameter is not configured; if the parameter is configured, certain VLAN corresponding to the MSTI will be deleted.

6	`Raisecom(config)#spanning-tree max-hops hops`
	Example:
	`Raisecom(config)#spanning-tree max-hops 10`
		Configure the maximum number of hops for the MST region.
		• hops: maximum number of hops, an integer, ranging from 1 to 40

Copyright © Raisecom Technology Co., Ltd.

Note

Only when the configured device is the region root can the configured maximum number of hops be used as the maximum number of hops for MST region; other non-region root cannot be configured this item.

2.7.6 Configuring root/backup bridge

Two methods for MSTP root selection are as below:

- To configure device priority and calculated by STP to confirm STP root bridge or backup bridge
- To assign MSTP root directly by a command

When the root bridge has a fault or is powered off, the backup bridge can replace the root bridge of related instance. In this case, if a new root bridge is assigned, the backup bridge will not become the root bridge. If several backup bridges for a spanning tree are configured, once the root bridge stops working, MSTP will choose the backup root with the lowest MAC address as the new root bridge.

Note

We do not recommend modifying the priority of any device on the network if you directly assign the root bridge. Otherwise, the assigned root bridge or backup bridge may be invalid.

Configure the root bridge or backup bridge for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#spanning-tree [ instance instance-id ] root { primary | secondary }`
	Example:
	`Raisecom(config)#spanning-tree root primary`
		Configure the ISCOM2600G series switch as the root bridge or backup bridge of a STP instance.
		• instance-id: MSTI ID, an integer, ranging from 0 to 4095
		• primary: configure the device as the primary root device.
		• secondary: configure the device as the backup root device.

Note

- You can confirm the effective instance of the root bridge or backup bridge through the **instance** *instance-id* parameter. The current device will be assigned as the root bridge or backup bridge of CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.
- The roots in device instances are mutually independent; in other words, they cannot only be the root bridge or backup bridge of one instance, but also the root bridge or backup bridge of other spanning tree instances. However, in a spanning tree instance, a device cannot be used as the root bridge and backup bridge concurrently.

Copyright © Raisecom Technology Co., Ltd.

- You cannot assign two or more root bridges for one spanning tree instance, but can assign several backup bridges for one spanning tree. Generally, you had better assign one root bridge and several backup bridges for a spanning tree.

2.7.7 Configuring interface priority and system priority

Whether the interface is elected as the root interface depends on interface priority. Under the same condition, the interface with smaller priority will be elected as the root interface. An interface may have different priorities and play different roles in different instances.

The Bridge ID determines whether the ISCOM2600G series switch can be elected as the root of the spanning tree. Configuring smaller priority helps obtain smaller Bridge ID and designate the ISCOM2600G series switch as the root. If priorities of two ISCOM2600G series switch devices are identical, the ISCOM2600G series switch with lower MAC address will be elected as the root.

Similar to configuring root and backup root, priority is mutually independent in different instances. You can confirm priority instance through the **instance** *instance-id* parameter. Configure bridge priority for CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.

Configure the interface priority and system priority for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#spanning-tree [ instance instance-id ] priority priority-value`
	`Raisecom(config-gigaethernet1/1/port)#exit`
	Example:
	`Raisecom(config-gigaethernet1/1/port)#spanning-tree priority 64`
		Configure the interface priority for a STP instance.
		• instance-id: MSTI ID, an integer, ranging from 0 to 4095
		• priority-value: priority. The system priority ranges from 0 to 61440 in step of 4096, such as 0, 4096, and 8192. The interface priority ranges from 0 to 240 in step of 16, such as 0, 16, and 32.

4	`Raisecom(config)#spanning-tree [ instance instance-id ] priority priority-value`
	Example:
	`Raisecom(config)#spanning-tree instance 1 priority 8192`
		Configure the system priority for a STP instance.
		• instance-id: MSTI ID, an integer, ranging from 0 to 4095
		• priority-value: priority. The system priority ranges from 0 to 61440 in step of 4096, such as 0, 4096, and 8192. The interface priority ranges from 0 to 240 in step of 16, such as 0, 16, and 32.

Copyright © Raisecom Technology Co., Ltd.

Note

The value of priorities must be multiples of 4096, such as 0, 4096, and 8192. It is 32768 by default.

2.7.8 Configuring network diameter for switch network

The network diameter indicates the number of nodes on the path that has the most devices on a switching network. In MSTP, the network diameter is valid only to CIST, and invalid to MSTI instance. No matter how many nodes in a path in one region, it is considered as just one node. Actually, network diameter should be defined as the region number in the path crossing the most regions. The network diameter is 1 if there is only one region on the entire network.

The maximum number of hops of the MST region is used to measure the region scale, while network diameter is a parameter to measure the whole network scale. The greater the network diameter is, the larger the network scale is.

Similar to the maximum number of hops of the MST region, only when the ISCOM2600G series switch is configured as the CIST root device can this configuration take effect. MSTP will automatically configure the Hello Time, Forward Delay and Max Age parameters to a privileged value through calculation when configuring the network diameter.

Configure the network diameter for the switching network as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#spanning-tree bridge-diameter` *`bridge-diameter-value`* **`Example:`** `Raisecom(config)#spanning-tree bridge-diameter 5`	Configure the network diameter for the switching network. • bridge-diameter-value: network diameter, an integer, ranging from 2 to 7

2.7.9 Configuring internal path cost of interface

When selecting the root interface and designated interface, the smaller the interface path cost is, the easier it is to be selected as the root interface or designated interface. Inner path costs of interface are independently mutually in different instances. You can configure internal path cost for instance through the **instance** *instance-id* parameter. Configure internal path cost of interface for CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.

By default, interface cost often depends on the physical features:

- 10 Mbit/s: 2000000
- 100 Mbit/s: 200000
- 1000 Mbit/s: 20000
- 10 Gbit/s: 2000

Configure the internal path cost for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example • interface-type: interface type • interface-number: interface ID
3	`Raisecom(config-gigaethernet1/1/port)#spanning-tree [ instance` *`instance-id`* `] inter-path-cost` *`cost`* **Example:** `Raisecom(config-gigaethernet1/1/1)#spanning-tree instance 1 inter-path-cost 10`	Configure the internal path cost of the interface. • instance-id: MSTI ID, an integer, ranging from 0 to 4095 • cost: path cost value, an integer, ranging from 0 to 200000000

2.7.10 Configuring external path cost of interface

The external path cost is the cost from the device to the CIST root, which is equal in the same region.

Configure the external path cost for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	`Raisecom(config-gigaethernet1/1/port)#spanning-tree extern-path-cost` *`cost`* **Example:** `Raisecom(config-gigaethernet1/1/1)#spanning-tree extern-path-cost 10`	Configure the external path cost of the interface. • cost: path cost value, an integer, ranging from 0 to 200000000

2.7.11 Configuring maximum transmission rate on interface

The maximum transmission rate on an interface means the maximum number of transmitted BPDUs allowed by MSTP in each Hello Time. This parameter is a relative value and of no unit. The greater the parameter is configured, the more packets are allowed to be transmitted

Copyright © Raisecom Technology Co., Ltd.

in a Hello Time, the more device resources it takes up. Similar with the time parameter, only the configurations on the root device can take effect.

Configure the maximum transmission rate on the interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#spanning-tree transmit-limit max-num`
	Example:
	`Raisecom(config)#spanning-tree transmit-limit 10`
		Configure the maximum transmission rate on the interface.
		• max-num: maximum number of packets, an integer, ranging from 1 to 10

2.7.12 Configuring MSTP timer

- Hello Time: the interval for the ISCOM2600G series switch to send BPDUs. It is used to detect whether a link fails on the ISCOM2600G series switch. The ISCOM2600G series switch sends Hello packets to other devices around in the Hello time to check if there is fault in the link. The default value is 2s. You can adjust the interval value according to network conditions. Reduce the interval when network link changes frequently to enhance the stability of STP. However, increasing the interval reduces CPU utilization rate for STP.
- Forward Delay: the time parameter to ensure the safe transit of device status. Link fault causes the network to recalculate spanning tree, but the new configuration message recalculated cannot be transmitted to the whole network immediately. There may be temporary loop if the new root interface and designated interface start transmitting data at once. This protocol adopts status remove system: before the root interface and designated interface starts forwarding data, it needs a medium status (learning status); after delay for the interval of Forward Delay, it enters forwarding status. The delay guarantees the new configuration message to be transmitted through whole network. You can adjust the delay according to actual condition; in other words, reduce it when network topology changes infrequently and increase it under opposite conditions.
- Max Age: the bridge configurations used by STP have a life time that is used to judge whether the configurations are outdated. The ISCOM2600G series switch will discard outdated configurations and STP will recalculate spanning tree. The default value is 20s. Over short age may cause frequent recalculation of the spanning tree, while a too great age value will make STP not adapt to network topology change timely.

All devices in the whole switching network adopt the three time parameters on CIST root device, so only the root device configuration is valid.

Configure the MSTP timer for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#spanning-tree hello-time period`
	Example:
	`Raisecom(config)#spanning-tree hello-time 3`
		Configure the Hello Time.
		• period: interval for sending BPDUs, an integer, ranging from 1 to 10, in units of second

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

3	`Raisecom(config)#spanning-tree forward-delay period`
	Example:
	`Raisecom(config)#spanning-tree forward-delay 10`
		Configure the Forward Delay.
		• period: forward-delay period, an integer, ranging from 4 to 30, in units of second

4	`Raisecom(config)#spanning-tree max-age period`
	Example:
	`Raisecom(config)#spanning-tree max-age 30`
		Configure the Max Age.
		• period: time value, an integer, ranging from 6 to 40, in units of second

2.7.13 Configuring edge interface

The edge interface indicates the interface neither directly connecting to any devices nor indirectly connecting to any device through the network.

The edge interface can change the interface status to forward quickly without any waiting time. You had better configure the Ethernet interface connected to user client as edge interface to make it quick to change to forward status.

The edge interface attribute depends on actual condition when it is in auto-detection mode; the real port will change to false edge interface after receiving BPDU when it is in force-true mode; when the interface is in force-false mode, whether it is true or false edge interface in real operation, it will maintain the force-false mode until the configuration is changed.

By default, all interfaces on the ISCOM2600G series switch are configured in auto-detection attribute.

Configure the edge interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#spanning-tree edged-port { auto | force-true | force-false }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#spanning-tree edged-port force-true`
		Configure attributes of the RSTP edge interface.
		• auto: automatically detect whether it is an edge interface.
		• force-true: forced to be an edge interface
		• force-false: forced to be a non-edge interface

Copyright © Raisecom Technology Co., Ltd.

2.7.14 Configuring BPDU filtering

After being enabled with BPDU filtering, the edge interface does not send BPDU packets nor process received BPDU packets.

Configure BPDU filtering for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#spanning-tree edged-port bpdu-filter { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#spanning-tree edged-port bpdu-filter enable`
		Enable BPDU filtering on the edge interface.
		• enable: enable BPDU filtering on the edge interface.
		• disable: disable BPDU filtering on the edge interface.

2.7.15 Configuring BPDU Guard

On a switch, interfaces directly connected with non-switch devices, such as terminals (such as a PC) or file servers, are configured as edge interfaces to implement fast transition of these interfaces.

In normal status, these edge interfaces do not receive BPDUs. If forged BPDU attacks the switch, the switch will configure these edge interfaces to non-edge interfaces when these edge interfaces receive forged BPDUs and re-perform spanning tree calculation. This may cause network vibration.

BPDU Guard provided by MSTP can prevent this type of attacks. After BPDU Guard is enabled, edge interfaces can avoid attacks from forged BPDU packets.

After BPDU Guard is enabled, the switch will shut down the edge interfaces if they receive BPDUs and notify the NView NNM system of the case. The blocked edge interface is restored only by the administrator through the CLI.

Configure BPDU Guard for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#spanning-tree bpduguard { enable | disable }`
	Example:
	`Raisecom(config)#spanning-tree bpduguard enable`
		Enable BPDU Guard.
		• enable: enable BPDU Guard on the ring interface.
		• disable: disable BPDU Guard on the ring interface.

3	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

4	`Raisecom(config-gigaethernet1/1/port)#no spanning-tree bpduguard shutdown port`	Manually restore interfaces that are shut down by BPDU Guard.

Note

When the edge interface is enabled with BPDU filtering and the device is enabled with BPDU Guard, BPDU Guard takes effect first. Therefore, an edge interface is shut down if it receives a BPDU.

2.7.16 Configuring STP/RSTP/MSTP mode switching

When STP is enabled, three spanning tree modes are supported as below:

- STP compatible mode: the ISCOM2600G series switch does not implement fast switching from the replacement interface to the root interface and expedited forwarding by a specified interface; instead it sends STP configuration BPDU and STP Topology Change Notification (TCN) BPDU. After receiving MST BPDU, it discards unidentifiable part.
- RSTP mode: the ISCOM2600G series switch implements fast switching from the replacement interface to the root interface and expedited forwarding by a specified interface. It sends RST BPDUs. After receiving MST BPDUs, it discards unidentifiable part. If the peer device runs STP, the local interface is switched to STP compatible mode. If the peer device runs MSTP, the local interface remains in RSTP mode.
- MSTP mode: the ISCOM2600G series switch sends MST BPDU. If the peer device runs STP, the local interface is switched to STP compatible mode. If the peer device runs MSTP, the local interface remains in RSTP mode, and process packets as external information of region.

Configure the STP/RSTP/MSTP mode switching for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#spanning-tree mode { stp | rstp | mstp }`
	Example:
	`Raisecom(config)#spanning-tree mode mstp`
		Configure the spanning tree mode.
		• STP: the device is working in global STP-compatible mode.
		• RSTP: the device is working in global RSTP mode.
		• MRSTP: the device is working in global MRSTP mode.

3	`Raisecom(config-gigaethernet1/1/port)#spanning-tree mcheck`	(Optional) forcibly configure the interface to MSTP mode.

2.7.17 Configuring link type

Two interfaces connected by a point-to-point link can quickly transit to forward status by transmitting synchronization packets. By default, MSTP configures the link type of interfaces according to duplex mode. The full duplex interface is considered as the point-to-point link, and the half duplex interface is considered as the shared link.

You can manually configure the current Ethernet interface to connect to a point-to-point link, but the system will fail if the link is not point to point. Generally, we recommend configuring this item in auto status and the system will automatically detect whether the interface is connected to a point-to-point link.

Configure the link type for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#spanning-tree link-type { auto | point-to-point | shared }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#spanning-tree link-type point-to-point`
		Configure the link type of the interface.
		• auto: automatically detect whether the link connected to the interface is a point-to-point link.
		• point-to-point: the link connected to the current interface is a point-to-point link.
		• shared: the link connected to the current interface is a shared link.

2.7.18 Configuring root interface protection

The bridge will re-elect a root interface when it receives a packet with higher priority, which influents network connectivity and also consumes CPU resource. For the MSTP network, if

Copyright © Raisecom Technology Co., Ltd.

someone sends BPDUs with higher priority, the network may become unstable due to continuous election.

Generally, priority of each bridge has already been configured in network planning phase. The nearer a bridge is to the edge, the lower the bridge priority is. So the downlink interface cannot receive the packets higher than bridge priority unless under someone attacks. For these interfaces, you can enable rootguard to refuse to process packets with priority higher than bridge priority and block the interface for a period to prevent other attacks from attacking sources and damaging the upper layer link.

Configure root interface protection for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.

3	`Raisecom(config-gigaethernet1/1/port)#spanning-tree rootguard { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#spanning-tree rootguard enable`
		Enable/Disable root interface protection.
		• enable: enable BPDU Guard.
		• disable: disable BPDU Guard.

2.7.19 Configuring interface loopguard

The spanning tree has two functions: loopguard and link backup. Loopguard requires carving up the network topology into tree structure. There must be redundant links in the topology if link backup is required. Spanning tree can avoid loop by blocking the redundant link and enable link backup function by opening redundant link when the link breaks down.

The spanning tree module exchanges packets periodically, and the link has failed if it has not received packet in a period. Then select a new link and enable backup interface. In actual networking, the cause to failure in receiving packets may not link fault. In this case, enabling the backup interface may lead to loop.

Loopguard is used to keep the original interface status when it cannot receive packet in a period.

Note

Loopguard and link backup are mutually exclusive; in other words, loopguard is implemented on the cost of disabling link backup.

Configure interface loop protection for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface

3	`Raisecom(config-gigaethernet1/1/port)#spanning-tree loopguard { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#spanning-tree loopguard enable`
		Configure interface loopguard attributes.
		• enable: enable BPDU Guard.
		• disable: disable BPDU Guard.

2.7.20 Configuring TC packet suppression

When the topology of the user access network changes, the forward address of the core network will be updated. When the topology becomes unstable, it will affect the core network. To avoid unstable topology, you can configure TC packet suppression on the interface. In this case, after the interface receives a TC packet, it will not forward the TC packet to other interfaces.

Configure TC packet suppression for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#spanning-tree tc-rejection { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/port)#spanning-tree tc-rejection enable`
		Configure TC packet suppression.
		• enable: enable TC packet suppression.
		• disable: disable TC packet suppression.

2.7.21 Checking configurations

Use the following commands to check configuration results.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
1	Raisecom#**show spanning-tree** [**instance** *instance-id*] [**detail**]	Show basic configurations of STP.
2	Raisecom#**show spanning-tree** [**instance** *instance-id*] *interface-type interface-list* [**detail**]	Show configurations of spanning tree on the interface.
3	Raisecom#**show spanning-tree region-operation**	Show operation information about the MST region.
4	Raisecom(config-region)#**show spanning-tree region-configuration**	Show configurations of the MST region.

2.7.22 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
Raisecom(config-gigaethernet1/1/port)#**spanning-tree clear statistics**	Clear statistics about spanning tree on the interface.

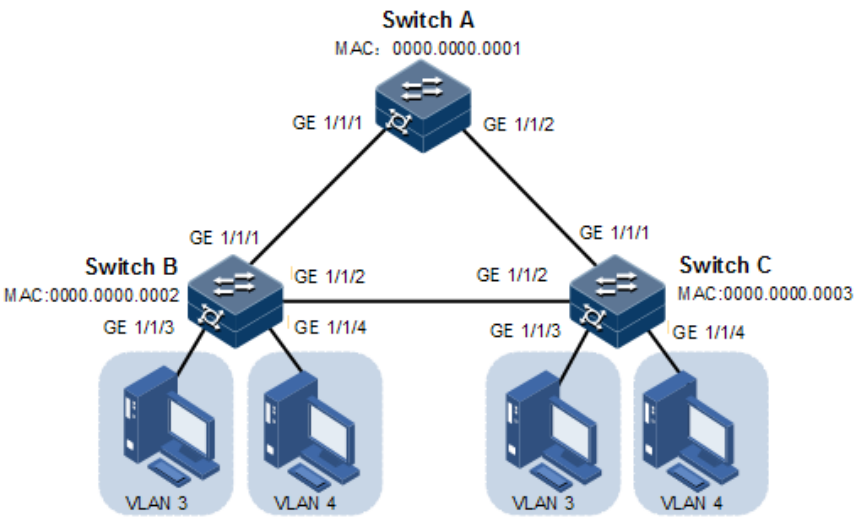
2.7.23 Example for configuring MSTP

Networking requirements

As shown in Figure 2-18, three ISCOM2600G series switch devices are connected to form a ring network through MSTP, with the region name aaa. Switch B, connected with a PC, belongs to VLAN 3. Switch C, connected with another PC, belongs to VLAN 4. Instant 3 is associated with VLAN 3. Instant 4 is associated with VLAN 4. Configure the path cost of instance 3 on Switch B so that packets of VLAN 3 and VLAN 4 are forwarded respectively in two paths, which eliminates loops and implements load balancing.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-18 MSTP networking



Configuration steps

Step 1 Create VLAN 3 and VLAN 4 on Switch A, Switch B, and switch C respectively, and activate them.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 3,4 active
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#create vlan 3,4 active
```

Configure Switch C.

```
Raisecom#hostname SwitchC
SwitchC#config
SwitchC(config)#create vlan 3,4 active
```

Step 2 Configure GE 1/1/1 and GE 1/1/2 on Switch A to allow packets of all VLAN to pass in Trunk mode. Configure GE 1/1/1 and GE 1/1/2 on Switch B to allow packets of all VLANs to pass in Trunk mode. Configure GE 1/1/1 and GE 1/1/2 on Switch C to allow packets of all VLANs

Copyright © Raisecom Technology Co., Ltd.

to pass in Trunk mode. Configure GE 1/1/3 and GE 1/3/4 on Switch B and Switch C to allow packets of VLAN 3 and VLAN 4 to pass in Access mode.

Configure Switch A.

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#exit
```

Configure Switch B.

```
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#exit
SwitchB(config)#interface gigaethernet 1/1/3
SwitchB(config-gigaethernet1/1/3)#switchport access vlan 3
SwitchB(config-gigaethernet1/1/3)#exit
SwitchB(config)#interface gigaethernet 1/1/4
SwitchB(config-gigaethernet1/1/4)#switchport access vlan 4
SwitchB(config-gigaethernet1/1/4)#exit
```

Configure Switch C.

```
SwitchC(config)#interface gigaethernet 1/1/1
SwitchC(config-gigaethernet1/1/1)#switchport mode trunk
SwitchC(config-gigaethernet1/1/1)#exit
SwitchC(config)#interface gigaethernet 1/1/2
SwitchC(config-gigaethernet1/1/2)#switchport mode trunk
SwitchC(config-gigaethernet1/1/2)#exit
SwitchC(config)#interface gigaethernet 1/1/3
SwitchC(config-gigaethernet1/1/3)#switchport access vlan 3
SwitchC(config-gigaethernet1/1/3)#exit
SwitchC(config)#interface gigaethernet 1/1/4
SwitchC(config-gigaethernet1/1/4)#switchport access vlan 4
SwitchC(config-port)#exit
```

Step 3 Configure spanning tree mode of Switch A, Switch B, and Switch C to MSTP, and enable STP. Enter MSTP configuration mode, and configure the region name to aaa and revision version to 0. Map instance 3 to VLAN 3, and instance 4 to VLAN 4. Exist from MST configuration mode.

Configure Switch A.

Copyright © Raisecom Technology Co., Ltd.

```
SwitchA(config)#spanning-tree mode mstp
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree region-configuration
SwitchA(config-region)#name aaa
SwitchA(config-region)#revision-level 0
SwitchA(config-region)#instance 3 vlan 3
SwitchA(config-region)#instance 4 vlan 4
```

Configure Switch B.

```
SwitchB(config)#spanning-tree mode mstp
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree region-configuration
SwitchB(config-region)#name aaa
SwitchB(config-region)#revision-level 0
SwitchB(config-region)#instance 3 vlan 3
SwitchB(config-region)#instance 4 vlan 4
SwitchB(config-region)#exit
```

Configure Switch C.

```
SwitchC(config)#spanning-tree mode mstp
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree region-configuration
SwitchC(config-region)#name aaa
SwitchC(config-region)#revision-level 0
SwitchC(config-region)#instance 3 vlan 3
SwitchC(config-region)#instance 4 vlan 4
```

Step 4 Configure the internal path cost of GE 1/1/3 of spanning tree instance 3 to 500000 on Switch B.

```
SwitchB(config)#interface gigaethernet 1/1/3
SwitchB(config-gigaethernet1/1/3)#spanning-tree instance 3 inter-path-
cost 500000
```

Checking results

Use the **show spanning-tree region-operation** command to show configurations of the MST region.

Take Switch A for example.

```
SwitchA#show spanning-tree region-operation
```


Copyright © Raisecom Technology Co., Ltd.

```
Operational Information:
-----------------------------------------------
Name: aaa
Revision level: 0
Instances running: 3
Digest: 0X024E1CF7E14D5DBBD9F8E059D2C683AA
Instance  Vlans Mapped
--------  ------------------------------
1-2,5-4094
3
4
```

Use the **show spanning-tree instance 3** command to show basic information about spanning tree instance 3.

Take Switch A for example.

```
SwitchA#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
Spanning-tree pathcost-standard: Dot1t

MST ID: 3
------------------------------------------------------------
BridgeId:    Mac 5051.5051.5053  Priority 32768
RegionalRoot: Mac 5051.5051.5053  Priority 32768  InternalRootCost 0
Port     PortState   PortRole   PathCost  PortPriority  LinkType
-----------------------------------------------------------------
```

Use the **show spanning-tree instance 4** command to show basic information about spanning tree instance 4.

Take Switch A for example.

```
SwitchA#show spanning-tree instance 4
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
Spanning-tree pathcost-standard: Dot1t

MST ID: 4
------------------------------------------------------------
BridgeId:    Mac 5051.5051.5053  Priority 32768
RegionalRoot: Mac 5051.5051.5053  Priority 32768  InternalRootCost 0
Port     PortState   PortRole   PathCost  PortPriority  LinkType
```


Copyright © Raisecom Technology Co., Ltd.

2.8 Loop detection

2.8.1 Introduction

Loop detection can address the influence on network caused by a loop, providing the self-detection, fault-tolerance, and robustness.

During loop detection, an interface enabled with loop detection periodically sends loop detection packets (Hello packets). Under normal conditions, the edge interface should not receive any loop detection packets because loop detection is applied to the edge interface. However, if the edge interface receives a loop detection packet, it is believed that a loop occurs on the network. There are two conditions that an edge interface receives a loop detection packet: receiving a loop detection packet from itself or receiving a loop detection packet from other devices, which can be told by comparing the MAC address of the device and the MAC address carried in the packet.

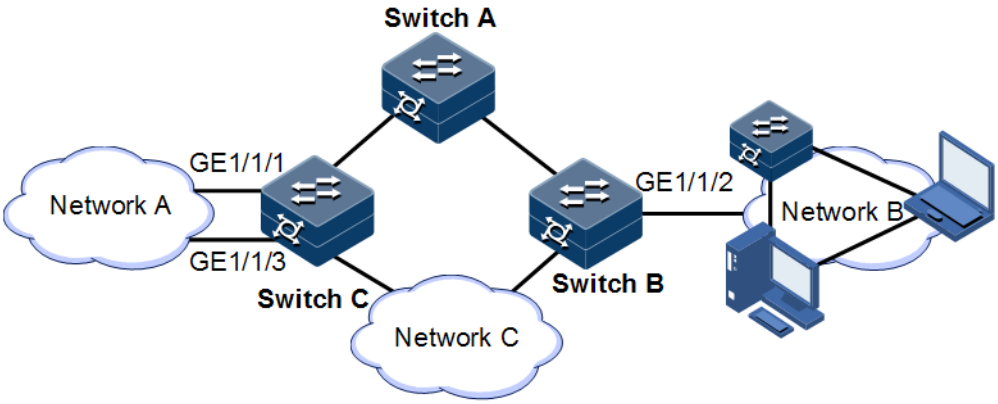
Loop types

Common loop types include self-loop and inner loop.

As shown in Figure 2-19, Switch B and Switch C are connected to the user network.

- Self-loop: a user loop on the same Ethernet interface of the same device. User network B has a loop, which forms self-loop on GE 1/1/2 on Switch B.
- Inner loop: a loop forming on different Ethernet interfaces of the same device. GE 1/1/1 and GE 1/1/3 on Switch C forms an inner loop with the user network A.

Figure 2-19 Loop detection networking



Principles for processing loops

The ISCOM2600G series switch processes loops as below:

- If the device sending the loop detection packet is the one receiving the packet but the interface sending the packet and the interface receiving the packet are different, process the interface with the smaller interface ID to eliminate the loop (inner loop).
- If the interface sending the packet and the interface receiving the packet are the same, process the interface to eliminate the loop (self-loop).

In Figure 2-19, assume that both Switch B and Switch C connect user network interfaces enabled with loop detection. The system processes loops for the three loop types as below:

Copyright © Raisecom Technology Co., Ltd.

- Self-loop: the interface sending the packet and the interface receiving the packet on Switch B are the same, the configured loop detection action will be taken to eliminate the loop on GE 1/1/2.
- Inner loop: Switch C receives the loop detection packets sent by it and the interface sending the packet and the interface receiving the packet are the same, the configured loop detection action will be taken to eliminate the loop on the interface with a bigger interface ID, namely, GE 1/1/1.

Action for processing loops

The action for processing loops is the method for the ISCOM2600G series switch to use upon loop detection. You can define different actions on the specified interface according to actual situations, including:

- Block: block the interface and send a Trap.
- Trap-only: send Trap only.
- Shutdown: shut down the interface and send a Trap.

Loop detection modes

The loop detection mode is port mode.

When a loop occurs, the system blocks the interface and sends Trap in the loopback processing mode of Block, or shuts down the physical interface and sends Trap information in the loopback processing mode of shutdown.

If the loop detection processing mode is Trap-only, the ISCOM2600G series switch sends Traps only.

Loop restoration

After an interface is blocked or shut down, you can configure it, such as no automatic restoration and automatic restoration after a specified period.

- If an interface is configured as automatic restoration after a specified period, the system will start loop detection after the period. If the loop disappears, the interface will be restored. Otherwise, it will be kept in blocking or shutdown status.
- If an interface is configured as no automatic restoration, in other words, the automatic restoration time is infinite, it will not be automatically restored.

2.8.2 Preparing for configurations

Scenario

On the network, hosts or Layer 2 devices connected to access devices may form a loop intentionally or involuntarily. Enable loop detection on downlink interfaces on all access devices to avoid the network congestion generated by unlimited copies of data traffic. Once a loopback is detected on an interface, the interface will be blocked.

Prerequisite

Loopback interface, interface backup, STP, and G.8032 affect each other. We do not recommend configuring two or more of them concurrently.

Copyright © Raisecom Technology Co., Ltd.

2.8.3 Default configurations of loop detection

Default configurations of loop detection are as below.

Function	Default value
Loop detection status	Disable
Automatic recovery time for the blocked interface	Infinite, namely, no automatic recovery
Mode for processing detected loops	trap-only
Loop detection period	4s
Loop detection mode	port mode

2.8.4 Configuring loop detection

Note

- Loop detection and STP are exclusive, so only one can be enabled at a time.
- Loop detection cannot be concurrently enabled on both two directly-connected devices.

Configure loop detection based on interface+VLAN for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-gigaethernet1/1/port)# **loopback-detection** [**pkt-vlan** { **untag** | *vlan-id* }] [**hello-time** *second*] [**restore-time** *second*] [**action** { **block** | **trap-only** | **shutdown** | **shutdown-restore** }] [**log-interval** *log-interval time*] **Example:** Raisecom(config-gigaethernet1/1/1)#loopback-detection pkt-vlan 5 hello-time 3 restore-time 15 action block	Enable loop detection on the interface. Configure the VLAN for sending loop detection packets. (Optional) configure the period for sending Hello packets. (Optional) configure the time for automatically restoring the blocked interface due to loop detection and the action for processing loops. • untag: specify packets to not carry Tag. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • hello-time second: loop detection period, an integer, ranging from 1 to 3600, in units of second • restore-time second: lLoop recovery time, an integer, ranging from 1 to 18000, in units of second • block: send alarms and block the interface upon detection of a loop. After the loop is eliminated, the interface will be Up when the recovery time elapses. • trap-only: send alarms only upon detection of a loop. After the loop is eliminated, the interface will be Up when the recovery time elapses. • shutdown: send alarms and shut down the interface upon detection of a loop. After the loop is eliminated, the interface will be Up when the recovery time elapses. • shutdown-restore: when a loop is detected, the alarm information is sent and the interface is closed. The restore time is calculated from the detection of the loop. When the recovery time elapses, the interface will be Up. • log-interval time: log time interval, an integer, ranging from 0 to 1440, in units of minute, with the value 0 indicating no periodic report
4	Raisecom(config-gigaethernet1/1/port)# **loopback-detection manual restore**	Manually restore the interface blocked due to loop detection.

2.8.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show loopback-detection** [*interface-type interface-number*] [**detail**]	Show configurations and status of loop detection.

Copyright © Raisecom Technology Co., Ltd.

2.8.6 Maintenance

Use the following commands to maintain the ISCOM2600G series switch.

Command	Description

`Raisecom(config)#clear loopback-detection statistic [ interface-type interface-number ]`
Example:
`Raisecom(config)#clear loopback-detection statistic`
	Clear statistics about loop detection.
	• interface-type: interface type
	• interface-number: in the form of unit/slot/port. The value range depends on the interface type.

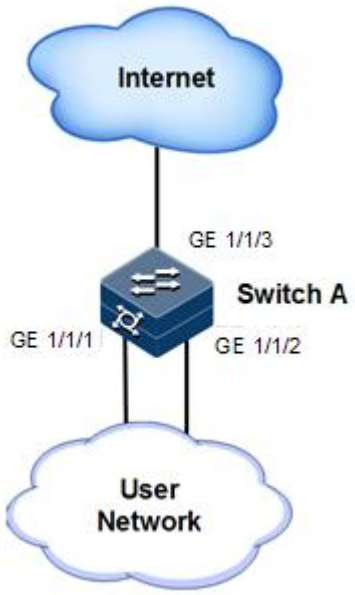
2.8.7 Example for configuring inner loop detection

Networking requirements

As shown in Figure 2-20, GE 1/1/2 and GE 1/1/3 on Switch A are connected to the user network. To avoid loops on the user network, enable loop detection on Switch A to detect loops on user network, and then take actions accordingly. Detailed requirements are as below:

- Enable loop detection on GE 1/1/2 and GE 1/1/3.
- Configure the interval for sending loop detection packets to 3s.
- Configure the VLAN for sending loop detection packets to VLAN 3.
- Configure the loop detection processing action to discarding, namely, sending Trap and blocking the interface.

Figure 2-20 Loop detection networking



Copyright © Raisecom Technology Co., Ltd.

Configuration steps

Step 1 Create VLAN 3, and add interfaces to VLAN 3.

```
Raisecom#config
Raisecom(config)#create vlan 3 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport access vlan 3
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport access vlan 3
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 2 Configure the VLAN for sending loop detection packets, action taken for detected loops, and period for sending loop detection packets.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#loopback-detection  pkt-vlan 3 hello-
time 3 action block
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#loopback-detection  pkt-vlan 3 hello-
time 3 action block
```

Checking results

Use the **show loopback-detection** command to show loop detection status. GE 1/1/1 is already blocked because of its smaller interface ID, so the loop is eliminated.

```
Raisecom#show loopback-detection
Interface  pktVlan  detect-vlanlist    hellotime  restoretime  loop-act
log-interval  Status   loop-srcMAC      loop-srcPort   loop-Duration  loop-
vlanlist

---------------------------------------------------------------------------
---------------------------------------------------------------------------
-----------------

GE1/1/1   3      --              3        15         block          0
yes     000E.5E55.0001   GE1/1/2       121          --


GE1/1/2   3      --              3        15         block          0
no      --             --           --           --
```


Copyright © Raisecom Technology Co., Ltd.

2.9 Interface protection

2.9.1 Introduction

With interface protection, you can add an interface, which needs to be controlled, to an interface protection group, isolating Layer 2/Layer 3 data in the interface protection group. This can provide physical isolation between interfaces, enhance network security, and provide flexible networking scheme for users.

After being configured with interface protection, interfaces in an interface protection group cannot transmit packets to each other. Interfaces in and out of the interface protection group can communicate with each other. So do interfaces out of the interface protection group.

2.9.2 Preparing for configurations

Scenario

Interface protection can implement mutual isolation of interfaces in the same VLAN, enhance network security and provide flexible networking solutions for you.

Prerequisite

N/A

2.9.3 Default configurations of interface protection

Default configurations of interface protection are as below.

Function	Default value
Interface protection status of each interface	Disable

2.9.4 Configuring interface protection

Caution

Interface protection is unrelated with the VLAN to which the interface belongs.

Configure interface protection for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	`Raisecom(config-gigaethernet1/1/port)#` **`switchport protect`**	Enable interface protection. Interface isolation is supported across devices in the ISF. Interface isolation can be implemented based on LAG interface, namely, between LAG interfaces, and between a LAG interface and common interface.

2.9.5 Configuring interface isolation

Configure interface isolation for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.

2	`Raisecom(config)#`**`protect-group`** *`group-id`* **`vlan`** *`vlan-id`* `interface-type` *`interface-number`* `[` **`add`** `|` **`remove`** `]`
	Example:
	`Raisecom(config)#protect-group 1 vlan 1 gigaethernet 1/1/1`
		Create an interface isolation group. Configure isolation VLANs associated with the group and the list of isolated interfaces.
		• group-id: isolated group ID, an integer, ranging from 1 to 256
		• vlan-id: isolated VLAN associated with the isolated group, an integer, ranging from 1 to 4094
		• interface-type: interface type
		• interface-number: in the form of unit/slot/port. The value range depends on the interface type.
		• add: add an isolated interface.
		• remove: delete an isolated interface.

2.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show switchport protect`**	Show configurations of interface protection.
2	`Raisecom#`**`show protect-group`** `{` **`all`** `|` *`group-id`* `}`	Show configurations of interface isolation.

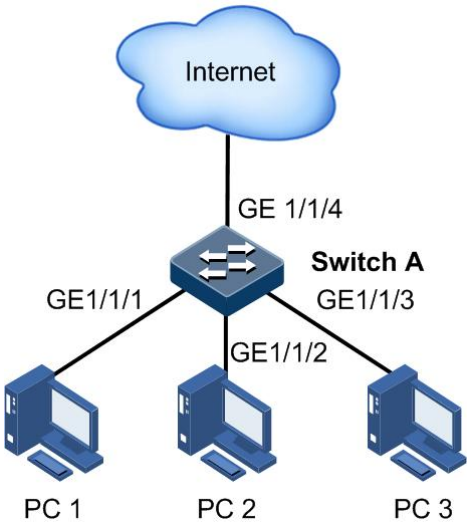
2.9.7 Example for configuring interface protection

Networking requirements

As shown in Figure 2-21, to prevent PC 1 and PC 2 from interconnecting with each other and to enable them to interconnect with PC 3 respectively, enable interface protection on GE 1/1/1 and GE 1/1/2 on Switch A.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-21 Interface protection networking



Configuration steps

Step 1 Enable interface protection on the GE 1/1/1.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport protect
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 2 Enable interface protection on the GE 1/1/2.

```
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport protect
```

Checking results

Use the **show switchport protect** command to show configurations of interface protection.

```
Raisecom#show switchport protect
Port              Protected State
--------------------------
gigaethernet1/1/1   enable
gigaethernet1/1/2   enable
gigaethernet1/1/3   disable
gigaethernet1/1/4   disable
gigaethernet1/1/5   disable
gigaethernet1/1/6   disable
……
```


Copyright © Raisecom Technology Co., Ltd.

Check whether PC 1 and PC 2 can ping PC 3 successfully.

- PC 1 can ping PC 3 successfully.
- PC 2 can ping PC 3 successfully.

Check whether PC 1 can ping PC 2 successfully.

PC 1 fails to ping PC 3, so interface protection has taken effect.

2.10 Port mirroring

2.10.1 Introduction

Port mirroring refers to mirroring some packets from a specified source port to the destination port, namely, the monitor port, without affecting normal packet forwarding. You can monitor the sending and receiving status of packets on a port through this function and analyze the related network conditions.

Figure 2-22 Principles of port mirroring

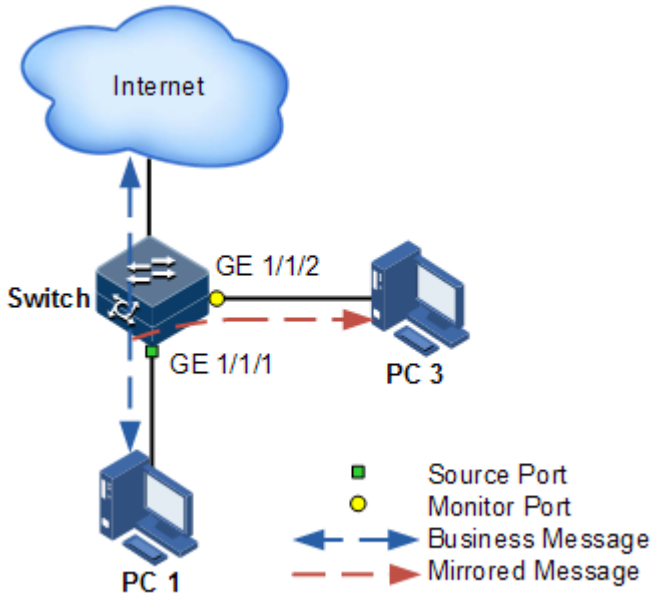


Figure 2-22 shows principles of port mirroring. PC 1 is connected to the external network by the GE 1/1/1; PC 3 is the monitor PC, connecting the external network by GE 1/1/2.

When monitoring packets from the PC 1, you need to assign GE 1/1/1 to connect to PC 1 as the mirror source port, enable port mirroring on the ingress port and assign GE 1/1/2 as monitor port to mirror packets to destination port.

When service packets from PC 1 enter the ISCOM2600G series switch, the ISCOM2600G series switch will forward and copy them to monitor port (GE 1/1/2). The monitor device connected to the monitor port can receive and analyze these mirrored packets.

The ISCOM2600G series switch supports traffic mirroring on the ingress port and egress port. The packets on the ingress/egress mirroring port will be copied to the monitor port after the

Copyright © Raisecom Technology Co., Ltd.

switch is enabled with port mirroring. The monitor port and mirroring port cannot be the same one.

2.10.2 Preparing for configurations

Scenario

Port mirroring is used to monitor the type and flow of network data regularly for the network administrator.

Port mirroring copies the port flow monitored to a monitor port or CPU to obtain the ingress/egress port failure or abnormal flow of data for analysis, discovers the root cause, and solves them timely.

Prerequisite

N/A

2.10.3 Default configurations of port mirroring

Default configurations of port mirroring are as below.

Function	Default value
Port mirroring status	Disable
Mirroring the source port	N/A

2.10.4 Configuring port mirroring on local port

Configure local port mirroring for the ISCOM2600G series switch as below.

Step	Configure	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#mirror-group group-id`
	Example:
	`Raisecom(config)#mirror-group 1`
		Create a port mirroring group.
		• group-id: mirroring group ID, an integer, ranging from 1 to 4

3	`Raisecom(config)#mirror-group group-id remote-vlan vlan-id`
	Example:
	`Raisecom(config)#mirror-group 1 remote-vlan 2`
		Configure the remote mirroring VLAN for the mirroring group.
		• group-id: mirroring group ID, an integer, ranging from 1 to 4
		• vlan-id: remote mirror VLAN ID, an integer, ranging from 1 to 4094

Copyright © Raisecom Technology Co., Ltd.

Step	Configure	Description
4	Raisecom(config)#**mirror-group** *group-id* **reflector-port** *interface-type interface-number* **Example:** Raisecom(config)#mirror-group 1 reflector-port gigaethernet 1/1/1	Configure the reflector interface for the mirroring group. • group-id: mirroring group ID, an integer, ranging from 1 to 4 • interface-type: interface type • interface-number: in the form of unit/slot/port. The form and value range depend on the interface type.
5	Raisecom(config)#**interface** interface-type interface-number **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The form and value range depend on the interface type.
6	Raisecom(config-gigaethernet1/1/port)#**mirror-group** *group-id* **monitor-port** **Example:** Raisecom(config-gigaethernet1/1/1)#mirror-group 1 monitor-port	Configure the monitor port for mirroring. • group-id: mirroring group ID, an integer, ranging from 1 to 4
7	Raisecom(config-gigaethernet1/1/port)#**mirror-group** *group-id* **source-port** [**ingress** | **egress**] **Example:** Raisecom(config-gigaethernet1/1/1)#mirror-group 1 source-port ingress	Configure the mirroring port of port mirroring, and designate the mirroring rule for port mirroring. Port mirroring supports mirroring packets in both the ingress and egress directions of the port. • group-id: mirroring group ID, an integer, ranging from 1 to 4 • ingress: ingress direction • egress: egress direction
8	Raisecom(config-gigaethernet1/1/port)#**exit** Raisecom(config)#**mirror-group** *group-id* **source-cpu** [**ingress** | **egress**] **Example:** Raisecom(config)#mirror-group 1 source-cpu ingress	Configure port mirroring to mirror packets to or from the CPU. • group-id: mirroring group ID, an integer, ranging from 1 to 4 • ingress: ingress direction • egress: egress direction

2.10.5 Checking configurations

Use the following commands to check configuration results.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
1	`Raisecom#show mirror-group [ group-id ]`	Show configurations of port mirroring.

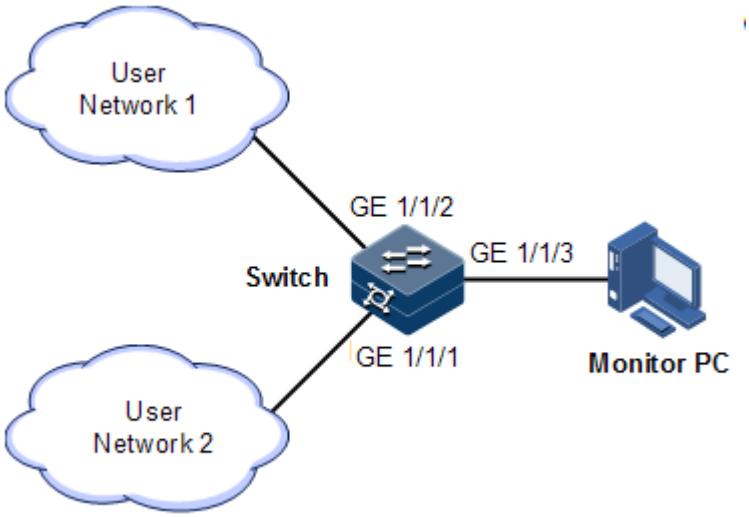
2.10.6 Example for configuring port mirroring

Networking requirements

As shown in Figure 2-23, the network administrator wants to monitor user network 1 through the monitor device, then to catch the fault or abnormal data flow for analyzing and discovering faults and then solve them in time.

The ISCOM2600G series switch is disabled with storm control and automatic packets sending. User network 1 accesses the ISCOM2600G series switch through GE 1/1/1, user network 2 accesses the ISCOM2600G series switch through GE 1/1/2, and the data monitor device is connected to GE 1/1/3.

Figure 2-23 Port mirroring networking



Configuration steps

Enable port mirroring on the Switch.

```
Raisecom#config
Raisecom(config)#mirror-group 1
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#mirror-group 1 monitor-port
Raisecom(config-gigaethernet1/1/3)#exit
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#mirror-group 1 source-port ingress
```


Copyright © Raisecom Technology Co., Ltd.

Checking results

Use the **show mirror** command to show configurations of port mirroring.

```
Raisecom#show mirror-group
Mirror Group 1:
Monitor Port:
   gigaethernet1/1/3
Source Port:
   gigaethernet1/1/1           : ingress
Reflector Port:
Remote Vlan:
```

2.11 L2CP

2.11.1 Introduction

Metro Ethernet Forum (MEF) introduces service concepts, such as EPL, EVPL, EP-LAN, and EVP-LAN. Different service types have different processing modes for Layer 2 Control Protocol (L2CP) packets.

MEF6.1 defines processing modes for L2CP as below.

- Discard: discard the packet, by applying the configured L2CP profile on the ingress interface of the ISCOM2600G series switch, to complete configuring processing mode.
- Peer: send packets to the CPU in the same way as the discard action.
- Tunnel: send packets to the MAN. It is more complex than discard and peer mode, requiring cooperating profile at network side interface and carrier side interface tunnel terminal to allow packets to pass through the carrier network.

2.11.2 Preparing for configurations

Scenario

On the access device of MAN, you can configure profile on user network interface according to services from the carrier to configure L2CP of the user network.

Prerequisite

N/A

2.11.3 Defaul configurations of L2CP

Default configurations of L2CP are as below.

Function	Default value
Global L2CP status	Disable

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
Applying the profile on the interface	Disable
Destination MAC address of transparently transmitted packets	010E.5E00.0003
Description of the L2CP profile	N/A
Channel type of transparently transmitted packets	none

2.11.4 Configuring global L2CP

Configure global L2CP for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#l2cp-process tunnel destination-address` *`mac-address`* **Example:** `Raisecom(config)#l2cp-process tunnel destination-address 0180.c300.0001`	(Optional) configure the destination MAC address for transparently transmitted packets. It must be a multicast address that does not start with 0180.c200 or 010E.5E00, but its default value is 010E.5E00.0003.

3	`Raisecom(config)#l2cp-process user-defined-protocol` *`name`* `protocol-mac` *`mac-address`* `encaptype { ethernetI` *`ethertype`* `| llc dsap` *`dsap value`* `ssap` *`ssap value`* `}`
	Example:
	`Raisecom(config)#l2cp-process user-defined-protocol aa protocol-mac 0180.c200.0001 encaptype ethernetI 0x0601`
		Configure user-defined MAC address rules.
		• name: name of the user default protocol, a string of 1 to 16 characters
		• mac-address: protocol MAC address, in dotted hexadecimal notation, being 0180.c200.0000–0180.c200.00ff, 010e.5e00.0000–010e.5eff.ffff, or 0100.0c00.00000–0100.0cff.fff
		• ethertype: IEEE 802.3 protocol type, ranging from 0x0600 to 0xffff
		• dsap value: LLC DSAP, used to identify the type of upper layer data carried by Ethernet frames, ranging from 0 to 0x05ff
		• ssap value: LLC SSAP, used to identify the type of upper layer data carried by Ethernet frames, ranging from 0 to 0x05ff

2.11.5 Configuring L2CP profile

Configure the L2CP profile for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**l2cp-process profile** *profile-number* **Example:** Raisecom(config)#l2cp-process profile 4	Create and enter the L2CP profile. • profile-number: L2CP profile ID, an integer, ranging from 1 to 32. L2CP profiles 1 and 2 are default profiles, so they cannot be created, deleted, and modified.
3	Raisecom(config-l2cp-profile)#**name** *string* **Example:** Raisecom(config-l2cp-profile)#name epl	(Optional) add the profile description. • string: description of the L2CP profile, a character string starting with a letter or number, with length ranging from 0 to 16
4	Raisecom(config-l2cp-profile)#**l2cp-process protocol** { **stp** |**lacp**| **lamp** |**oam** | **esmc** | **dot1x** | **elmi** | **lldp** | **gvrp** | **gmrp** | **cdp** | **vtp** | **pvst** | **udld** | **pagp** | **all** } **action** { **tunnel** | **drop** | **peer** } **Example:** Raisecom(config-l2cp-profile)#l2cp-process protocol all action peer	(Optional) configure the mode for processing L2CP packets. • stp: STP packets • lacp: LACP packets • lamp: Lamp packets • oam: OAM packets • esmc: ESMC packets • Dot1x: Dot1x packets • elmi: ELMI packets • lldp: LLDP packets • gvrp: GVRP packets • gmrp: GMRP packets • cdp: CDP packets • vtp: VTPtp packets • pvst: PVST packets • udld: UDLD packets • pagp: PAGP packets • all: all L2CP packets (excluding self-defined protocol packets) • drop: discard packets. • peer: submit packets to the CPU. • tunnel: transparently transmit packets.
5	Raisecom(config-l2cp-profile)#**tunnel vlan** *vlan-id* **Example:** Raisecom(config-l2cp-profile)#tunnel vlan 20	(Optional) configure the specified VLAN for transparent transmission. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
6	Raisecom(config-l2cp-profile)#**tunnel** *interface-type interface-number* **Example:** Raisecom(config-l2cp-profile)#tunnel gigaethernet 1/1/1	(Optional) configure the specified egress interface for transparent transmission. • interface-type: interface type • interface-number: interface ID. The range depends on the device type.
7	Raisecom(config-l2cp-profile)#**tunnel tunnel-type mac**	(Optional) configure the type of the tunnel for transparent transmission.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

8	`Raisecom(config-l2cp-profile)#tunnel cos cos-value`
	Example:
	`Raisecom(config-l2cp-profile)#tunnel cos 1`
		(Optional) configure the CoS of encapsulated packets. It is the CoS priority in the header of 802.1q packets, an integer, ranging from 0 to 7.

2.11.6 Configuring L2CP profile on interface

Configure the L2CP profile on the interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#l2cp-process profile profile-number`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#l2cp-process profile 1`
		Apply the L2CP profile on the interface.
		• profile-number: L2CP profile ID, an integer, ranging from 1 to 32

Note

Only when global L2CP is enabled can the profile applied to the interface take effect. You can configure global L2CP but it will not take effect if it is disabled.

2.11.7 Checking configurations

Use the following commands check configuration results.

No.	Command	Description
1	`Raisecom#show l2cp-process profile [ profile-number ]`	Show information about the created L2CP profile.
2	`Raisecom#show l2cp-process [interface-type interface-number ]`	Show configurations of L2CP on the interface.
3	`Raisecom#show l2cp-process [ tunnel statistics ] [ interface-type interface-number]`	Show statistics about L2CP packets on the interface.

Copyright © Raisecom Technology Co., Ltd.

2.11.8 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description

`Raisecom(config)#clear l2cp-process tunnel statistics [interface-type interface-number ]`
Example:
`Raisecom(config)#clear l2cp-process tunnel statistics`
	Clear statistics about L2CP packets on the interface.
	• interface-type: interface type
	• interface-number: interface ID. The range depends on the device type.

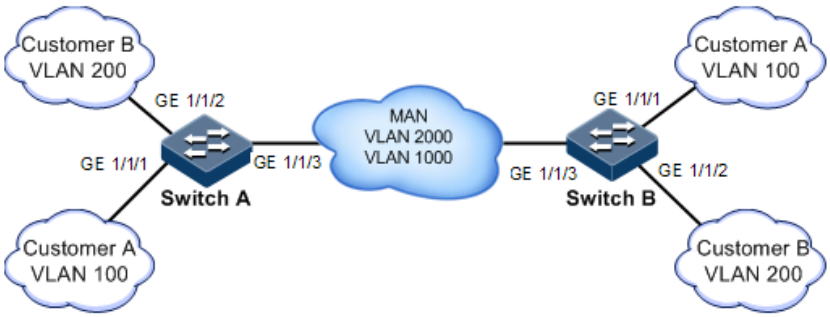
2.11.9 Example for configuring L2CP

Networking requirements

As shown in Figure 2-24, configure L2CP on Switch A and Switch B as below.

- Specify the multicast destination MAC address of them to 0100.1234.1234.
- Configure the STP packets of Customer A to traverse the MAN, and discard other packets.
- Configure the STP and VTP packets of Customer B to traverse the MAN, send elmi packets to the CPU, and discard other packets.

Figure 2-24 L2CP networking



Configuration steps

Configure Switch A and Switch B.

Configurations of Switch A and Switch B are identical. Take Switch A for example.

Step 1 Configure the switch name.

```
Raisecom#hostname SwitchA
```

Step 2 Configure the specified multicast destination MAC address.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config)#l2cp-process tunnel destination-address 0100.1234.1234
```

Step 3 Configure L2CP profile 1, and apply the profile to GE 1/1/1 for Customer A.

```
Raisecom(config)#l2cp-process profile 1
Raisecom(config-l2cp-profile)#name CustomerA
Raisecom(config-l2cp-profile)#l2cp-process protocol all action drop
Raisecom(config-l2cp-profile)#l2cp-process protocol stp action tunnel
Raisecom(config-l2cp-profile)#exit
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#l2cp-process profile 1
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 4 Configure L2CP profile 2, and apply the profile to GE 1/1/2 for Customer B.

```
Raisecom(config)#l2cp-process profile 2
Raisecom(config-l2cp-proflie)#name CustomerB
Raisecom(config-l2cp-proflie)#l2cp-process protocol all action drop
Raisecom(config-l2cp-proflie)#l2cp-process protocol stp action tunnel
Raisecom(config-l2cp-proflie)#l2cp-process protocol vtp action tunnel
Raisecom(config-l2cp-proflie)#l2cp-process protocol elmi action peer
Raisecom(config-l2cp-proflie)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#l2cp-process profile 2
Raisecom(config-gigaethernet1/1/2)#exit
```

Checking results

Use the **show l2cp-profile** command to show L2CP configurations.

```
Raisecom#show l2cp-process profile
Destination MAC Address for Encapsulated Packets: 0100.1234.1234
ProfileId: 1
Name: customerA
BpduType   Mac-address     l2cp-process  Mac-vlan  EgressPort  tunneltype
-------------------------------------------------------------------------
-------------
stp        0180.C200.0000   tunnel       --                 none
dot1x      0180.C200.0003   drop         --                 none
lacp       0180.C200.0002   drop         --                 none
oam        0180.C200.0002   drop         --                 none
cdp        0100.0CCC.CCCC   drop         --                 none
vtp        0100.0CCC.CCCC   drop         --                 none
pvst       0100.0CCC.CCCD   drop         --                 none
lldp       0180.C200.000E   drop         --                 none
elmi       0180.C200.0007   drop         --                 none
udld       0100.0CCC.CCCC   drop         --                 none
```


Copyright © Raisecom Technology Co., Ltd.

```
pagp       0100.0CCC.CCCC   drop        --                 none
ProfileId: 2
Name: customerB
BpduType    Mac-address     l2cp-process  Mac-vlan  EgressPort  tunneltype
-----------------------------------------------------------------------
-------------
stp        0180.C200.0000   tunnel       --                 none
dot1x      0180.C200.0003   drop         --                 none
lacp       0180.C200.0002   drop         --                 none
oam        0180.C200.0002   drop         --                 none
cdp        0100.0CCC.CCCC   drop         --                 none
vtp        0100.0CCC.CCCC   tunnel       --                 none
pvst       0100.0CCC.CCCD   drop         --                 none
lldp       0180.C200.000E   drop         --                 none
elmi       0180.C200.0007   peer         --                 none
udld       0100.0CCC.CCCC   drop         --                 none
pagp       0100.0CCC.CCCC   drop         --                 none
…
```

Use the **show l2cp-process** command to show interface configurations.

```
Raisecom#show l2cp-process
L2CP running informatiom
Port     ProfileID   BpduType   mac-address     l2cp-process
-----------------------------------------------------------------------
-----
GE1/1/1   1          stp        0180.C200.0000   tunnel
                   dot1x      0180.C200.0003   drop
                   lacp       0180.C200.0002   drop
                   oam        0180.C200.0002   drop
                   cdp        0100.0CCC.CCCC   drop
                   vtp        0100.0CCC.CCCC   drop
                   pvst       0100.0CCC.CCCD   drop
                   lldp       0180.C200.000E   drop
                   elmi       0180.C200.0007   drop
                   udld       0100.0CCC.CCCC   drop
                   pagp       0100.0CCC.CCCC   drop
GE1/1/2   2          stp        0180.C200.0000   tunnel
                   dot1x      0180.C200.0003   drop
                   lacp       0180.C200.0002   drop
                   oam        0180.C200.0002   drop
                   cdp        0100.0CCC.CCCC   drop
                   vtp        0100.0CCC.CCCC   tunnel
                   pvst       0100.0CCC.CCCD   drop
                   lldp       0180.C200.000E   drop
                   elmi       0180.C200.0007   peer
                   udld       0100.0CCC.CCCC   drop
                   pagp       0100.0CCC.CCCC   drop
GE1/1/3   --         --         --             --
GE1/1/4   --         --         --             --
GE1/1/5   --         --         --             --
…
```


Copyright © Raisecom Technology Co., Ltd.

2.12 Voice VLAN

2.12.1 Introduction

With increasing growth of voice technologies, voice devices are more and more widely used, especially in broadband residential communities. The network usually transmits voice traffic and data traffic concurrently, but voice traffic requires a higher priority than data traffic in transmission to avoid delay and packet loss.

A voice VLAN is especially partitioned for voice traffic of users. By partitioning voice VLANs and add interfaces of the voice device to voice VLANs, you can configure QoS of voice traffic to increase the priority of transmitting voice traffic and guarantee call quality.

Compared with other methods for managing voice traffic, the voice VLAN has the following advantages:

- Easy configuration: after you configure the voice device in global configuration mode and interface configuration mode and enable the voice VLAN, the voice device can classify and process voice traffic.
- Easy maintenance: you can modify rules (voice VLAN OUI address) for matching voice traffic in global configuration mode. When a new IP voice device joins the network, its interfaces can rapidly identify voice traffic by updated matching rules.
- Flexible implementation: The voice VLAN supports safe mode and common mode in global configuration mode and automatic mode and manual mode on the interface, so it is flexible in implementation. You can combine these modes as required to meet users' requirements to the maximum extent.
  - Secure mode: in the voice VLAN, the packets mismatching OUI are discarded while the packets matching OUI are modified with the priority and then forwarded.
  - Common mode: in the voice VLAN, the packets mismatching OUI are not modified with the priority and are normally forwarded while the packets matching OUI are modified with the priority and then forwarded.
  - Automatic mode: in this mode, the interface automatically joins the voice VLAN. You do not need to add the interface to the voice LAN; when the switch receives voice packets, it will automatically add the interface to the voice VLAN. When the interface fails to receive voice packets for a specified period, it will automatically quit the voice VLAN.
  - Manual mode: in this mode, you need to manually add the interface to the voice VLAN. The interface does not automatically join and leave the voice VLAN.

The ISCOM2600G series switch supports the following two networking modes.

Figure 2-25 shows the networking mode for IP phone (with its interfaces transmitting voice traffic only) to connect to the switch. This mode enables these interfaces to transmit voice traffic only, thus minimizing the impact on voice traffic from data traffic.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-25 Networking for IP phone to connect to switch

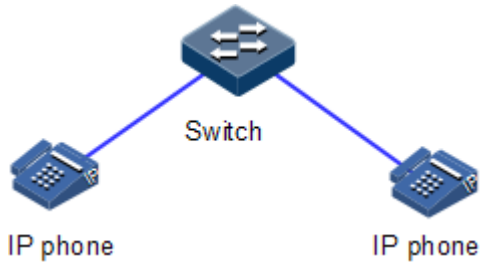
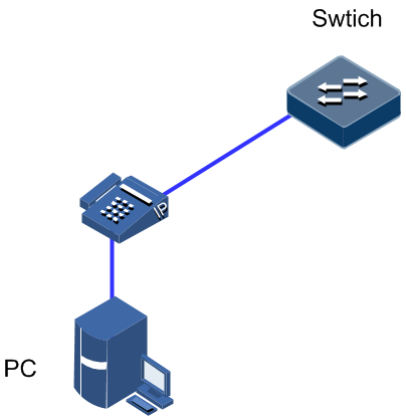


Figure 2-26 shows the networking mode for the IP phone to connect the PC to the switch (transmitting voice packets only), so the link transmits both voice traffic and data traffic. In this networking mode, voice traffic and data traffic are transmitted in the voice VLAN and data VLAN respectively with affecting each other. When office staff need data communication through PCs and also need voice communication through IP phones, you can adopt this networking mode.

Figure 2-26 Networking for IP phone to connect PC to the switch



2.12.2 Preparing for configurations

Scenario

The voice VLAN can transmit voice traffic. You can choose one of the following networking schemes according to whether voice packets are tagged or not:

- If the IP phone sends untagged voice packets, see section Example for adding interface to voice VLAN and configuring it to work in manual mode.
- If the IP phone supports obtaining the voice VLAN configured on the switch through LLDP, it will send tagged voice packets. For details, see section 2.12.9 Example for configuring IP phone to access voice VLAN packets through LLDP.

Prerequisite

Create a VLAN, and configure its parameters.

2.12.3 Default configurations of voice VLAN

Default configurations of Organizationally Unique Identifier (OUI) of the voice VLAN are as below.

Copyright © Raisecom Technology Co., Ltd.

OUI-Address	Mask address	Description
0001.E300.0000	FFFF.FF00.0000	Siemens-phone
0003.6B00.0000	FFFF.FF00.0000	Cisco-phone
0004.0D00.0000	FFFF.FF00.0000	Avaya-phone
00D0.1E00.0000	FFFF.FF00.0000	Pingtel-phone
0060.B900.0000	FFFF.FF00.0000	Philips/NEC-phone
00E0.7500.0000	FFFF.FF00.0000	Verilink-phone
00E0.BB00.0000	FFFF.FF00.0000	NBX-phone

Other default configurations of the voice VLAN are as below.

Function	Default value
Voice VLAN	Disable
Voice VLAN secure working mode	Disable
Voice VLAN common working mode	Enable
Automatic mode for the interface to join the voice VLAN	Disable
Manual mode for the interface to join the voice VLAN	Enable
CoS and DSCP of Voice VLAN packets	6 and 46 respectively
QoS trust priority of Voice VLAN	N/A

2.12.4 Configuring QoS of voice VLAN

Configure the QoS of the voice VLAN for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **`Example:`** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID, in the form of unit/slot/port. The range depends on the device type.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-gigaethernet1/1/port)#**voice-vlan qos cos** *cos-value* **dscp** *dscp-value* **Example:** Raisecom(config-gigaethernet1/1/1)#voice-vlan qos cos 2 dscp 10	Configure CoS and DSCP of voice VLAN packets. • cos-value: CoS priority in the 802.1Q packet header, an integer, ranging from 0 to 7 • dscp-value: DSCP priority in the 802.1Q packet header, an integer, ranging from 0 to 63
4	Raisecom(config-gigaethernet1/1/port)#**voice-vlan qos trust**	Configure QoS trust priority of the voice VLAN. Then, the interface does not modify the priority of voice VLAN packets.

2.12.5 Enabling voice VLAN

Enable the voice VLAN for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID, in the form of unit/slot/port. The value range depends on the interface type.
3	Raisecom(config-gigaethernet1/1/port)#**voice-vlan** *vlan-id* **{ enable | disable }** [**include-untagged**] **Example:** Raisecom(config-gigaethernet1/1/1)#voice-vlan 3 enable	Enable or disable the voice VLAN. • enable: enable the Voice VLAN. • disable: disable the Voice VLAN. • vlan-id: VLAN ID, an integer, ranging from 2 to 4094 • include-untagged: add Voice VLAN Tags to untagged packets which match the OUI.
4	Raisecom(config-gigaethernet1/1/port)#**voice-vlan auto** { **enable** | **disable** } **Example:** Raisecom(config-gigaethernet1/1/1)#voice-vlan auto disable	Configure the working mode for the interface to join the voice VLAN. • enable: the Voice VLAN works in automatic mode. • disable: the Voice VLAN works in manual mode.
5	Raisecom(config)#**voice-vlan aging-time** *time* **Example:** Raisecom(config)#voice-vlan aging-time 600	Configure the aging time for the interface to leave the voice VLAN in automatic mode. • time: aging time, an integer, ranging from 30 to 1440, in units of minute

Copyright © Raisecom Technology Co., Ltd.

2.12.6 Configuring OUI address

Configure the OUI address for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#voice-vlan mac-address` *`mac-address`* `[` *`mask address`* `]` `[ description` *`word`* `]`
	Example:
	`Raisecom(config)#voice-vlan mac-address 0001.E300.0000 FFFF.FF00.0000 description siemens`
		Configure the OUI of the voice VLAN.
		• mac-address: MAC address, in dotted hexadecimal notation
		• mask-address: MAC address mask, ranging from 0x0000.0000.0000 to 0xFFFF.FFFF.FFFF
		• word: description of the OUI address

2.12.7 Checking configurations

Use the following commands check configuration results.

No.	Command	Description
1	`Raisecom#show voice-vlan mac-address`	Show the OUI address, its mask, and description.
2	`Raisecom#show voice-vlan status`	Show the status of the voice VLAN on the current device.
3	`Raisecom#show voice-vlan auto`	Show the automatic mode of the voice VLAN on the current device.

2.12.8 Example for adding interface to voice VLAN and configuring it to work in manual mode

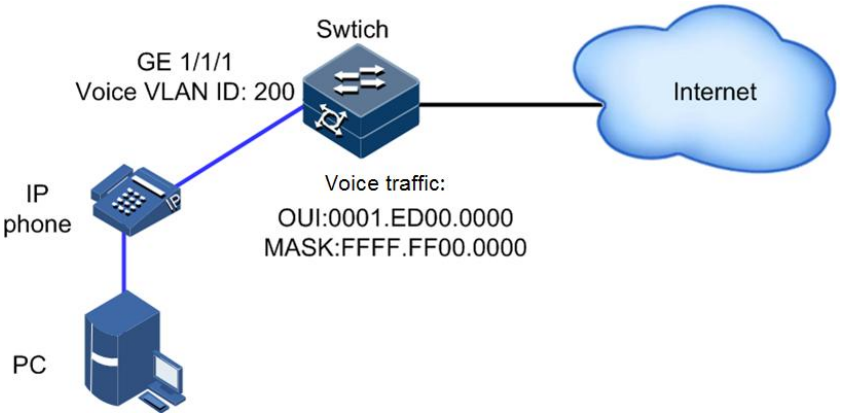
Networking requirements

GE 1/1/1 on the Switch connects the IP phone and PC to the Internet. It is required to concurrently forward and isolate voice traffic and data traffic.

You can configure GE 1/1/1 as a Trunk interface, making the Native VLAN forward data traffic and voice VLAN forward voice traffic. The PC sends untagged packets which are transmitted in the Native VLAN of GE 1/1/1. Configure VLAN 100 as the Native VLAN to transmit data traffic sent from the PC. The IP phone also sends untagged packets. Configure the source MAC address to the OUI address of the voice VLAN so that the device can add voice VLAN Tag when these packets pass the voice VLAN interface. Configure VLAN 200 as the voice VLAN to transmit voice traffic sent from the IP phone.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-27 Networking with adding interface to voice VLAN and configuring it to work in manual mode



Configuration steps

Step 1 Create VLAN 100 and VLAN 200, activate them, and configure VLAN 200 as the voice VLAN.

```
Raisecom(config)#create vlan 100,200 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan 100
Raisecom(config-gigaethernet1/1/1)#switchport trunk untag vlan 200
Raisecom(config-gigaethernet1/1/1)#voice-vlan 200 enable include-untagged
```

Step 2 Configure the MAC address (supporting the mask) of the IP phone as the OUI address of the voice VLAN on the switch, namely, 0001.ED00.0000. Configure the mask to FFFF.FF00.0000. For the OUI supported by the device by default, see section 2.12.3 Default configurations of voice VLAN.

```
Raisecom(config)#voice-vlan mac-address 0001.ED00.0000 FFFF.FF00.0000
```

Step 3 (Optional) by default, the interface modifies the CoS and DSCP of voice packets to 6 and 46 respectively. To modify them to other values, you should use the following command in the interface view before the voice VLAN is enabled on the interface.

```
Raisecom(config-gigaethernet1/1/1)#voice-vlan qos cos 6 dscp 46
```

Step 4 (Optional) by default, the interface modifies the CoS and DSCP of voice packets to 6 and 46 respectively. To prevent the interface from modifying them, you should use the following command:

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config-gigaethernet1/1/1)#voice-vlan qos trust
```

Checking configurations

Use the **show voice-vlan status** command to view the current status of the voice VLAN.

Use the **show voice-vlan mac-address** command to view the OUI address of the voice VLAN.

```
Raisecom(config)#show voice-vlan mac-address
OUI-Address         Mask             Description
-------------------------------------------------------------
0001.E300.0000       FFFF.FF00.0000     Siemens-phone
0003.6B00.0000       FFFF.FF00.0000     Cisco-phone
0004.0D00.0000       FFFF.FF00.0000     Avaya-phone
00D0.1E00.0000       FFFF.FF00.0000     Pingtel-phone
0060.B900.0000       FFFF.FF00.0000     Philips/NEC-phone
00E0.7500.0000       FFFF.FF00.0000     Verilink-phone
00E0.BB00.0000       FFFF.FF00.0000     NBX-phone
0001.ED00.0000      FFFF.FF00.0000
```

2.12.9 Example for configuring IP phone to access voice VLAN packets through LLDP

Networking requirements

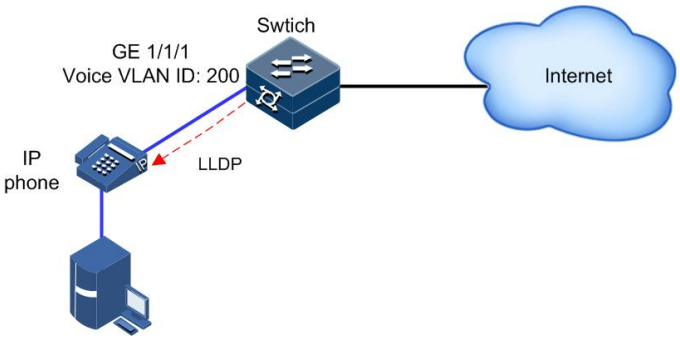
As shown in Figure 2-28, when the IP phone supports LLDP, it can obtain the voice VLAN through LLDP. You can configure LLDP and voice VLAN on the switch to connect the IP phone. Configure LLDP on the switch to advertise the voice VLAN of the interface to the IP phone. To guarantee call quality, configure the voice VLAN to prioritize voice packets.

GE 1/1/1 on the Switch connects the IP phone and PC to the Internet. It is required to concurrently forward and isolate voice traffic and data traffic.

You can configure GE 1/1/1 as a Trunk interface, making the Native VLAN forward data traffic and voice VLAN forward voice traffic. The PC sends untagged packets which are transmitted in the Native VLAN of GE 1/1/1. Configure VLAN 100 as the Native VLAN to transmit data traffic sent from the PC. Configure VLAN 200 as the voice VLAN to transmit voice traffic sent from the IP phone. The IP phone obtains the voice VLAN through LLDP and sends packets with the voice VLAN Tag.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-28 Configuring IP phone to access voice VLAN packets through LLDP



Configuration steps

Step 1 Create VLAN 100 and VLAN 200, activate them, and configure VLAN 200 as the voice VLAN.

```
Raisecom(config)#create vlan 100,200 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan 100
Raisecom(config-gigaethernet1/1/1)#voice-vlan 200 enable
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 2 Enable global LLDP and interface LLDP to advertise the voice VLAN of the interface to the IP phone.

```
Raisecom(config)#lldp enable
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#lldp enable
```

Step 3 Configure the MAC address (supporting the mask) of the IP phone as the OUI address of the voice VLAN on the switch, namely, 0001.ED00.0000. Configure the mask to FFFF.FF00.0000. For the OUI supported by the device by default, see section 2.12.3 Default configurations of voice VLAN.

```
Raisecom(config)#voice-vlan mac-address 0001.ED00.0000 FFFF.FF00.0000
```

Step 4 (Optional) by default, the interface modifies the CoS and DSCP of voice packets to 6 and 46 respectively. To modify them to other values, you should use the following command in the interface view before the voice VLAN is enabled on the interface.

```
Raisecom(config-gigaethernet1/1/1)#voice-vlan qos cos 6 dscp 46
```


Copyright © Raisecom Technology Co., Ltd.

Step 5 (Optional) by default, the interface modifies the CoS and DSCP of voice packets to 6 and 46 respectively. To prevent the interface from modifying them, you should use the following command:

```
Raisecom(config-gigaethernet1/1/1)#voice-vlan qos trust
```

Checking configurations

Use the **show voice-vlan mac-address** command to view the OUI address of the voice VLAN.

```
Raisecom(config)#show voice-vlan mac-address
OUI-Address         Mask             Description
-----------------------------------------------------------------
0001.E300.0000      FFFF.FF00.0000     Siemens-phone
0003.6B00.0000      FFFF.FF00.0000     Cisco-phone
0004.0D00.0000      FFFF.FF00.0000     Avaya-phone
00D0.1E00.0000      FFFF.FF00.0000     Pingtel-phone
0060.B900.0000      FFFF.FF00.0000     Philips/NEC-phone
00E0.7500.0000      FFFF.FF00.0000     Verilink-phone
00E0.BB00.0000      FFFF.FF00.0000     NBX-phone
0001.ED00.0000     FFFF.FF00.0000
```

2.13 GARP/GVRP

2.13.1 Introduction

Generic Attribute Registration Protocol (GARP) provides a mechanism to help GARP members in the same LAN to distribute, broadcast, and register information (such as VLAN and multicast information).

GARP is not an entity on a device. Those applications complying with GARP are called GARP applications. GARP VLAN Registration Protocol (GVRP) is a GARP application. When a GARP application entity is connected to an interface of a device, the interface is mapped into the GARP application entity.

Packets of the GARP application entity use a specific multicast MAC address as its destination MAC address. When receiving packets of the GARP application entity, a device distinguishes them by the destination MAC address and transmits them to different GARP applications (such as GAVP) for processing.

GARP messages

GARP members exchange data by transmitting messages, including the following three types of messages:

- Join message: a GARP application entity sends a Join message when:
  - It needs another device to register its attributes (such as VLAN information).

Copyright © Raisecom Technology Co., Ltd.

  - It receives a Join message from other entities; or it has been statically configured with some parameters, and needs another GARP application entity to register.
- Leave message: a GARP application entity sends a Leave message when:
  - It needs another device to register its attributes.
  - It receives a Join message from other entities to deregister its attributes or it statically deregisters its attributes.
- LeaveAll message: when the GARP application entity is started, the LeaveAll timer starts. It sends a LeaveAll message when this timer expires. The LeaveAll message is used to deregister all attributes so that other GARP application entities can register all attributes of the GARP application entity. When the GARP application entity receives a LeaveAll message from the peer, its LeaveAll time is restored and then starts.
- The Leave message or LeaveAll message cooperates with the Join message to deregister or reregister attributes. Through message exchange, all attributes to be registered can be transmitted to all GARP entities in the same LAN.

GARP timer

The interval for sending the GARP message is controlled by timers. GARP defines three timers to control the interval.

- Join timer: if no message is replied to the first Join message sent by the GARP application entity, this entity will send another Join message to ensure secure transmission. The interval between sending these two messages is controlled by the Join timer. If the entity has received reply from other GARP application entities, it will not send the Join message.
- Leave timer: when a GARP application entity needs to deregister an attribute, it sends a Leave message to another GARP application entity which will later start a Leave timer. It deregisters the attribute if failing to receive the Join message to deregister the attribute before the Leave timer expires.
- LeaveAll timer: when a GARP application entity starts, its LeaveAll timer also starts. When the LeaveAll timer expires, the GARP application entity sends a LeaveAll message so that other GARP application entities can register all attributes of the GARP application entity. Then, the LeaveAll timer is restored and starts retiming.

GVRP

GARP VLAN Registration Protocol (GVRP) is a GARP application. Based on GARP working mechanism, it maintains VLAN dynamic registration information of the switch, and sends the information to other switches.

All GVRP-supportive switches can receive VLAN registration information from other switches, and dynamically update local VLAN registration information. In addition, all GVRP-supportive switches can send local VLAN registration information to other switches so that they have consistent VLAN registration information in the same VLAN. VLAN registration information sent by GVRP includes manually configured local static registration information and dynamic registration information from other switches.

GVRP has three registration modes:

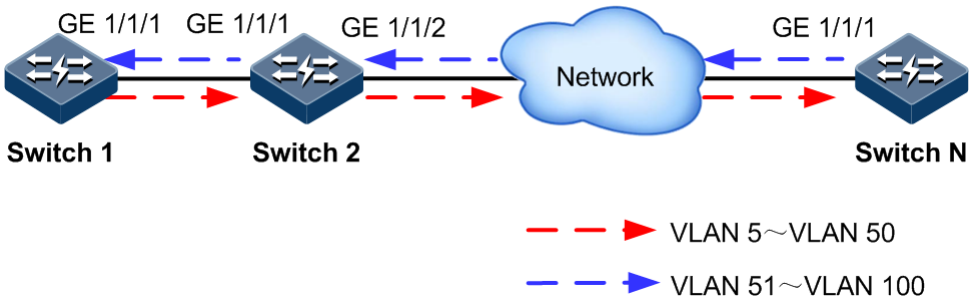
- Normal: in this mode, GVRP allows dynamic registration and deregistration of VLANs, and sends dynamic and static VLAN information.
- Fixed: in this mode, GVRP forbids dynamic registration and deregistration of VLANs, and sends static VLAN information rather than dynamic VLAN information.

Copyright © Raisecom Technology Co., Ltd.

- Forbidden: in this mode, GVRP forbids dynamic registration and deregistration of VLANs, forbids creating static VLANs on the interface, deletes all VLANs except VLAN 1, allows packets of the default VLAN (VLAN 1) to pass, and transmits packets of the default VLAN to other GARP members.

As shown in Figure 2-29, to configure VLANs on multiple devices on a network and allow packets of the specified VLAN to pass are complex. By using GVRP to dynamically register and transmit the specified VLAN, the network administrator can improve working efficiency and accuracy.

Figure 2-29 Principles of GVRP



As shown in Figure 2-29, GE 1/1/1 on Switch 1, GE 1/1/1 and GE 1/1/2 on Switch 2, and GE 1/1/1 on Switch N are Trunk interfaces. Create VLANs 5–50 on Switch 1, and then these VLANs will be dynamically registered on the Rx interface along the red direction until Switch N is registered. Create VLANs 51–100 on Switch N, and then these VLANs will be dynamically registered on the Rx interface along the blue direction so that each switch can completely process packets of VLANs 5–100.

2.13.2 Preparing for configurations

Scenario

GARP enables configurations of a GARP member to fast spread to all GARP-enabled devices in the LAN.

The values of the Join timer, Leaver timer, and LeaveAll timer configured through GARP will be applied to all GARP applications in the LAN, including GVRP and GMRP features.

Prerequisite

N/A

2.13.3 Default configurations of GARP

Default configurations of GARP are as below.

Function	Default value
GARP Join timer	20 (in units of 10ms)
GARP Leave timer	600 (in units of 10ms)
GARP LeaveAll timer	1000 (in units of 10ms)

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
Global GVRP status	Enable
Interface GVRP status	Disable
GVRP registration mode	Normal
Global GMRP status	Disable
Interface GMRP status	Disable
GMRP registration mode	Normal

2.13.4 Configuring basic functions of GARP

Configure basic functions of GARP for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface`** *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID, in the form of unit/slot/port. The value range depends on the interface type.
3	`Raisecom(config-gigaethernet1/1/port)#`**`garp timer`** { **`join`** | **`leave`** | **`leaveall`** } *`time-value`* **Example:** `Raisecom(config-gigaethernet1/1/1)#garp timer join 60`	Configure the GARP timer. • join time-value: configure the Join timer. The time-value refers to the timer value, which is an integer, ranging from 20 to 20000, in units of 10ms. • leave time-value: configure the Leave timer. The time-value refers to the timer value, which is an integer, ranging from 60 to 20000, in units of 10ms. • leaveall time-value: configure the LeaveAll timer. The time-value refers to the timer value, which is an integer, ranging from 500 to 20000, in units of 10ms.

Caution

- The value of the Join timer must be smaller than half of that of the Leave timer.
- The value of the Leave timer must be greater than twice of that of the Join timer, and smaller than that of the LeaveAll timer.
- The value of the LeaveAll timer must be greater than that of the Leave timer.
- In actual networking, we recommend configuring the Join timer, Leave timer, and LeaveAll timer to 3000, 15000, and 20000, in units of 10ms.

Copyright © Raisecom Technology Co., Ltd.

2.13.5 Configuring GVRP

Configure GVRP for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#gvrp { enable | disable }`
	Example:
	`Raisecom(config)#gvrp enable`
		Enable or enable global GVRP.
		• enable: enable GVRP.
		• disable: disable GVRP.

3	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID, in the form of unit/slot/port. The value range depends on the interface type.

4	`Raisecom(config-gigaethernet1/1/port)#switchport mode trunk`	Configure the interface to Trunk mode.

5	`Raisecom(config-gigaethernet1/1/port)#gvrp registration { fixed | forbidden | normal }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#gvrp registration fixed`
		(Optional) configure GVRP registration mode.
		• fixed: fixed mode
		• forbidden: forbidden mode
		• normal: normal mode

6	`Raisecom(config-gigaethernet1/1/port)#gvrp { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/port)#gvrp enable`
		Enable or disable interface GVRP.
		• enable: enable GVRP.
		• disable: disable GVRP.

Caution

- Interface GVRP can be enabled only after the interface is configured to Trunk mode.
- We do not recommend enabling GVRP on a LAG member interface.

2.13.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show garp [ interface-type interface-number]`	Show configurations of the GARP timer.
2	`Raisecom#show garp [ interface-type interface-number] statistics`	Show GARP statistics.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
3	`Raisecom#show gvrp [ interface-type interface-number]`	Show GVRP configurations.
4	`Raisecom#show gvrp [ interface-type interface-number] statistics`	Show GVRP statistics.
5	`Raisecom#show gvrp local-vlan interface-type interface-number`	Show the local VLAN of GMRP.

2.13.7 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description

`Raisecom(config)#clear gvrp [ interface-type interface-number ] statistics`
Example:
`Raisecom(config)#clear gvrp statistics`
	Clear GVRP statistics.
	• interface-type: interface type
	• interface-number: interface ID. The value range depends on the interface type.

2.13.8 Example for configuring GVRP

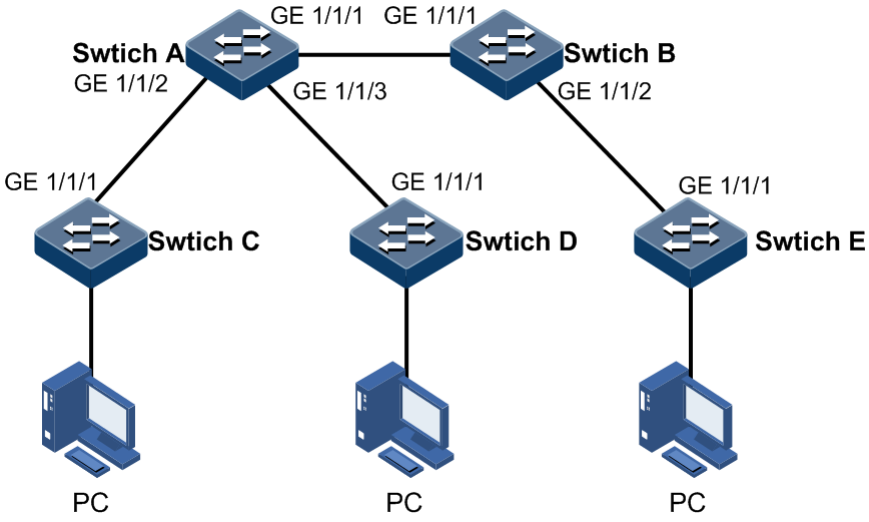
Networking requirements

As shown in Figure 2-30, to dynamically register, deregister, and update VLAN information between switches, configure GVRP on these switches. Detailed requirements are as below:

- Configure static VLANs 5–10 on Switch A and Switch C.
- Configure static VLANs 15–20 on Switch D.
- Configure static VLANs 25–30 on Switch E.
- Configure the interfaces that are connected to other switches to Trunk mode, and enable GVRP on these interfaces.
- Configure the Join timer, Leave timer, and LeaveAll timer of GARP on each interface to 3000, 15000, and 20000, in units of 10ms.

Copyright © Raisecom Technology Co., Ltd.

Figure 2-30 GVRP networking



Configuration steps

Step 1 Create VLANs and enable global GVRP.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 5-10 active
SwitchA(config)#gvrp enable
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#gvrp enable
```

Configure Switch C.

```
Raisecom#hostname SwitchC
SwitchC#config
SwitchC(config)#create vlan 5-10 active
SwitchC(config)#gvrp enable
```

Configure Switch D.

```
Raisecom#hostname SwitchD
```


Copyright © Raisecom Technology Co., Ltd.

```
SwitchD#config
SwitchD(config)#create vlan 15-20 active
SwitchD(config)#gvrp enable
```

Configure Switch E.

```
Raisecom#hostname SwitchE
SwitchE#config
SwitchE(config)#create vlan 25-30 active
SwitchE(config)#gvrp enable
```

Step 2 Configure GE 1/1/1, GE 1/1/2, and GE 1/1/3 on Switch A, GE 1/1/1, GE 1/1/2, and GE 1/1/3 on Switch B, GE 1/1/1 on Switch C, and GE 1/1/1 on Switch D to Trunk mode, and enable GVRP on them. Take GE 1/1/1 on Switch A for example. Configurations of other interfaces are the same.

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#gvrp enable
SwitchA(config-gigaethernet1/1/1)#exit
```

Step 3 Configure GARP timers of GE 1/1/1, GE 1/1/2, and GE 1/1/3 on Switch A, GE 1/1/1, GE 1/1/2, and GE 1/1/3 on Switch B, GE 1/1/1 on Switch C, and GE 1/1/1 on Switch D, and enable GVRP on them. Take GE 1/1/1 on Switch A for example. Configurations of other interfaces are the same.

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#garp timer leaveall 20000
SwitchA(config-gigaethernet1/1/1)#garp timer leave 15000
SwitchA(config-gigaethernet1/1/1)#garp timer join 3000
```

Checking results

Use the **show gvrp** command to show GVRP configurations on the interface.

Take Switch A for example.

```
SwitchA#show gvrp gigaethernet 1/1/1
Gvrp Globle Status: Enable
Port     PortStatus     RegMode
-------------------------------------------------
GE1/1/1  Enable       Normal
GE1/1/2  Enable       Normal
GE1/1/3  Enable       Normal
```


Copyright © Raisecom Technology Co., Ltd.

```
GE1/1/4   Disable       Normal
GE1/1/5   Disable       Normal
GE1/1/6   Disable       Normal
GE1/1/7   Disable       Normal
GE1/1/8   Disable       Normal
GE1/1/9   Disable       Normal
GE1/1/10  Disable       Normal
```

Use the **show vlan** command to view information about VLANs on the device. Take Switch A for example.

```
SwitchA#show vlan
VLAN Name                        State   Status       Priority Member-
Ports
---------------------------------------------------------------------------
-----------------------------------------------------
1    Default                     active  static       --
gigaethernet1/1/1         gigaethernet1/1/2
5    VLAN0005                    active  static       --
6    VLAN0006                    active  static       --
7    VLAN0007                    active  static       --
8    VLAN0008                    active  static       --
9    VLAN0009                    active  static       --
10   VLAN0010                    active  static       --
15   VLAN0015                    active  dynamic-gvrp  --
gigaethernet1/1/3

16   VLAN0016                    active  dynamic-gvrp  --
gigaethernet1/1/3

17   VLAN0017                    active  dynamic-gvrp  --
gigaethernet1/1/3

18   VLAN0018                    active  dynamic-gvrp  --
gigaethernet1/1/3

19   VLAN0019                    active  dynamic-gvrp  --
gigaethernet1/1/3

20   VLAN0020                    active  dynamic-gvrp  --
gigaethernet1/1/3
--More--
```


Copyright © Raisecom Technology Co., Ltd.

3 IP services

This chapter describes basic principles and configuration procedures for IP services, and provides related configuration examples, including the following sections:

- IP basis
- Loopback interface
- Interface loopback
- ARP
- NDP
- Static route
- Routing policy

3.1 IP basis

3.1.1 Introduction

The IP interface is the virtual interface based on VLAN. Configuring Layer 3 interface is generally used for network management or routing link connection of multiple devices.

The ISCOM2600G series switch supports double-tagged management VLAN packets; in other words, it can send and process double-tagged packets.

3.1.2 Preparing for configurations

Scenario

Configure the IP address of each VLAN interface and loopback interface.

Prerequisite

- Create VLANs.
- Activate them.

3.1.3 Default configurations of Layer 3 interface

Default configurations of the Layer 3 interface are as below.

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
Management VLAN inner TPID	0x8100
Management VLAN inner VLAN	1
Management VLAN CoS	0

3.1.4 Configuring IPv4 adress of VLAN interface

Configure the IPv4 address of the VLAN interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface vlan vlan-id`
	Example:
	`Raisecom(config)#interface vlan 1`
		Enter VLAN interface configuration mode.
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094

3	`Raisecom(config-vlan*)#ip address ip-address [ ip-mask ] [ sub ]`
	Example:
	`Raisecom(config-vlan1)#ip address 192.168.11.101 255.255.0.0`
		Configure the IP address of the VLAN interface.
		Use the **no ip address** *ip-address* command to delete configuration of the IP address.
		• ip-address: IP address, in dotted decimal notation, such as 10.0.0.1
		• ip-mask: mask of IP address, in dotted decimal notation, such as 255.0.0.0
		• sub: sub-IP address

3.1.5 Configuring IPv6 address of VLAN interface

Configure the IPv6 address of the VLAN interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface vlan vlan-id`
	Example:
	`Raisecom(config)#interface vlan 1`
		Enter Layer 3 interface configuration mode.
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-vlan*)#**ipv6 address** *ipv6-address* **link-local** Raisecom(config-vlan*)#**ipv6 address** *ipv6-address/prefix-length* **[eui-64]** **Example:** Raisecom(config-vlan1)#ipv6 address 1030:0::48AA:1A2B/60	Configure the IPv6 address of the VLAN interface. • ipv6-address/prefix-length: IPv6 address with prefix length, in form of A:B::C:D/M • eui-64: IPv6 local link address. The eui-64 is the interface ID. • ipv6-address: IPv6 address, in colon hexadecimal notation • link-local: IPv6 local link address

3.1.6 Configuring basic attributes

Configure basic attributes for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface vlan** *vlan-id* **Example:** Raisecom(config)#interface vlan 1	Enter VLAN interface configuration mode. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlan*)#**ip management-traffic cos** *cos-value* **Example:** Raisecom(config-vlan1)#ip management-traffic cos 2	Configure CoS of the management VLAN. By default, it is 6. • cos-value: outer CoS, an integer, ranging from 0 to 7
4	Raisecom(config-vlan*)#**ip management-traffic mode double-tagging** [**inner-vlan** *vlan-id*] [**inner-cos** *cos-id*] **Example:** Raisecom(config-vlan1)#ip management-traffic mode double-tagging	Configure the double-tagged mode for management packets. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • cos-id: inner CoS, an integer, ranging from 0 to 7
5	Raisecom(config-vlan*)#**exit**	Exit global configuration mode.
6	Raisecom(config)#**ip dest-address illegal syslog** { **enable** | **disable** }	Enable or disable the function of processing IP packets of which destination addresses include illegal addresses.
7	Raisecom(config)#**ip packet unknown forward**	Configure the device to forward IP packets of unknown types.
8	Raisecom(config)#**icmp unreach send**	Enable the function of sending ICMP unreachable packets.
9	Raisecom(config)#**exit**	Return to privileged EXEC mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

10	`Raisecom#ip soft-forward { enable | disable }`
	Example:
	`Raisecom#ip soft-forward enable`
		Enable the device to forward generated control packets.
		Use the **disable** form of this command to disable this function.
		• enable: enable the device to forward generated control packets.
		• disable: disable the device to forward generated control packets.

3.1.7 Checking configurations

Use the following commands to check configuration results.

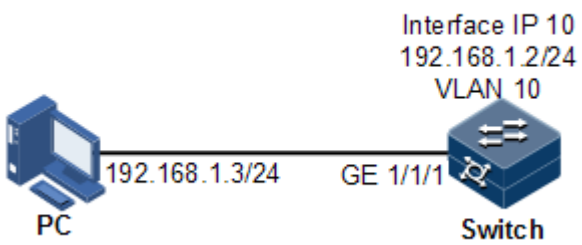
No.	Command	Description
1	`Raisecom#show ip interface brief`	Show configurations of the IP address of the VLAN interface.
2	`Raisecom#show ipv6 interface brief`	Show configurations of the IPv6 address of the VLAN interface.
3	`Raisecom#show ip management-traffic`	Show information about management packets on the VLAN interface.

3.1.8 Example for configuring VLAN interface to interconnect with host

Networking requirements

As shown in Figure 3-1, configure the VLAN interface to the switch so that the host and the ISCOM2600G series switch can ping each other.

Figure 3-1 VLAN interface networking



Configuration steps

Step 1 Create a VLAN and add the interface to the VLAN.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#config
Raisecom(config)#create vlan 10 active
```

Step 2 Configure Layer 3 interface on the ISCOM2600G series switch, configure its IP address, and associate the interface with the VLAN.

```
Raisecom(config)#interface vlan 10
Raisecom(config-vlan10)#ip address 192.168.1.2 255.255.255.0
```

Checking results

Use the **show vlan** command to show mapping between the physical interface and VLAN.

```
Raisecom#show vlan 10
VLAN Name              State      Status   Priority   Member-Ports
-----------------------------------------------------------------------
10   VLAN0010          active     static   --
```

Use the **show ip interface brief** to show configurations of the Layer 3 interface.

```
Raisecom#show ip interface brief
VRF                  IF                        Address       NetMask
Catagory
-----------------------------------------------------------------------
-----------------------------
Default-IP-Routing-Table  fastethernet1/0/1  192.168.0.1    255.255.255.0
primary
Default-IP-Routing-Table  vlan10            192.168.1.2    255.255.255.0
primary
```

Use the **ping** command to check whether the ISCOM2600G series switch and PC can ping each other.

```
Raisecom#ping 192.168.1.3
Type CTRL+C to abort
Sending 5, 8-byte ICMP Echos to 192.168.1.3, timeout is 3 seconds:
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms

---- PING Statistics----
5 packets transmitted, 5 packets received,
```


Copyright © Raisecom Technology Co., Ltd.

```
Success rate is 100 percent(5/5),
round-trip (ms)  min/avg/max = 0/0/0.
```

3.2 Loopback interface

3.2.1 Introduction

The loopback interface is a virtual interface and can be classified into two types:

- Loopback interface automatically created by the system: the IP address is fixed to 127.0.0.1. This type of interfaces receives packets sent to the device. It does not broadcast packets through routing protocols.
- Loopback interface created by users: without affecting physical interface configurations, configure a local interface with a specified IP address, and make the interface Up permanently so that packets can be broadcasted through routing protocols.

The loopback interface status is independent from the physical interface status (Up/Down). As long as the ISCOM2600G series switch is working normally, the loopback interface will not become Down. Thus, it is used to identify the physical device as a management address.

3.2.2 Preparing for configurations

Scenario

Use the IP address of the loopback interface to log in through Telnet so that the Telnet operation does not become Down due to change of physical status. To enable the PC to ping through the IP address of the loopback interface, configure the corresponding static route entry on the PC. The loopback interface ID is also used as the router ID of dynamic routing protocols, such as OSPF, to uniquely identify a device.

Prerequisite

N/A

3.2.3 Default configurations of loopback interface

N/A

3.2.4 Configuring IP address of loopback interface

Configure the IP address of the loopback interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**interface loopback** *loopback-number* **Example:** Raisecom(config)#interface loopback 0	Enter loopback interface configuration mode. • loopback-number: loopback interface ID, an integer, ranging from 0 to 128
3	Raisecom(config-loopback*)#**ip address** *ip-address* [*ip-mask*] [**sub**] **Example:** Raisecom(config-loopback0)#ip address 192.168.1.1	Configure the IP address of the loopback interface. • ip-address: IP address, in dotted decimal notation • ip-mask: IP subnet mask, in dotted decimal notation • sub: sub IP address
4	Raisecom(config-loopback*)#**ipv6 address** *ipv6-address* **link-local** Raisecom(config-loopback*)#**ipv6 address** *ipv6-address/prefix-length* [**eui-64**] **Example:** Raisecom(config-loopback0)#ipv6 address 1030:0::48AA:1A2B/60	Configure the IPv6 address of the loopback interface. • ipv6-address/prefix-length: IPv6 address with prefix length, such as A:B::C:D/M • eui-64: IPv6 local link address • ipv6-address: IPv6 address, in colon hexadecimal notation

3.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show interface loopback**	Show configurations of the loopback interface.

3.3 Interface loopback

3.3.1 Introduction

Interface loopback (local loopback) refers to sending packets, which comply with user-defined loopback rules and parameter requirements according to these rules, by the receiving interface to the sending device at the peer end, thus checking communication of the network.

Interface loopback is executed without affecting services; in other words, packets that comply with rules are looped back and concurrently forwarded or sent to the CPU.

As shown in Figure 3-2, the customer configures loopback rules on GE 1/1/1 on Switch A. When packets sent by GE 1/1/2 on Switch B reaches GE 1/1/1 on Switch A, Switch A checks whether these packets comply with current loopback rules.

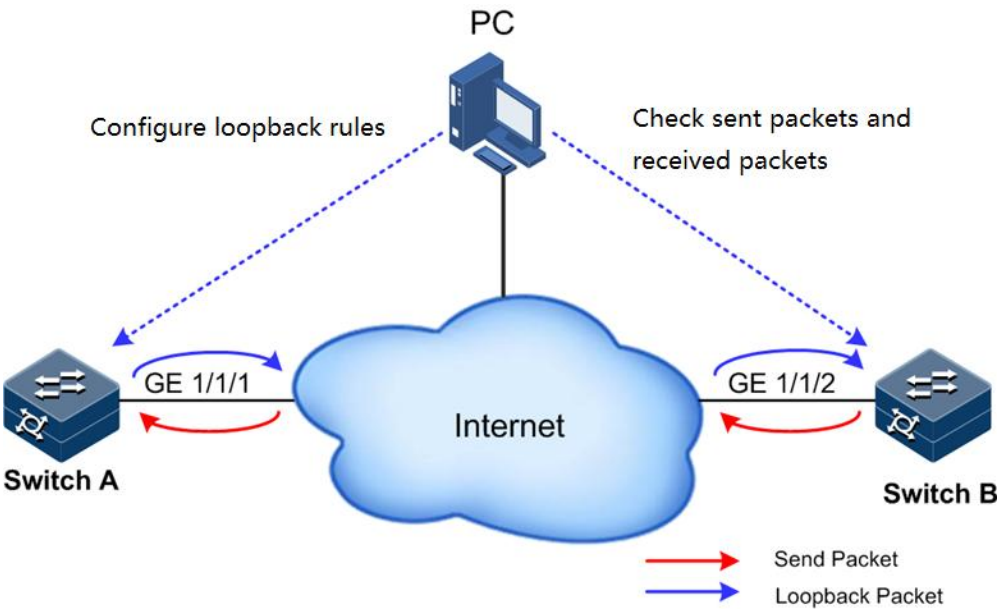
- If yes, Switch A loops back these packets through its GE 1/1/1 to GE 1/1/2 on Switch B.

Copyright © Raisecom Technology Co., Ltd.

- If no, Switch A normally forwards them or sends them to the CPU.

The customer can check communication of the network by comparing packets sent by Switch B with those received by switch B.

Figure 3-2 Interface loopback



3.3.2 Preparing for configurations

Scenario

Interface loopback refers to sending packets, which comply with user-defined loopback rules and parameter requirements according to these rules, by the receiving interface to the sending device at the peer end, thus checking communication of the network.

Prerequisites

N/A

3.3.3 Default configurations of interface loopback

N/A

3.3.4 Configuring interface loopback

Configure interface loopback for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID, in the form of unit/slot/port. The value range depends on the interface type.
3	Raisecom(config-gigaethernet1/1/port)#**loopback external** [**cvlan** *vlan-id* [**cos** *cos-value*]] [**svlan** *vlan-id* [**cos** *cos-value*]] [**dmac** *mac-address*] [**smac** *mac-address*][**swap smac** *mac-address*] [**swap dmac-disable**] **Example:** Raisecom(config-gigaethernet1/1/1)#loopback external dmac 0001.0002.0003 smac 0005.0002.0001 swap smac 0002.0003.0004 swap dmac-disable	Configure interface loopback. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • cos-value: CoS priority, an integer, ranging from 0 to 7 • mac-address: MAC address, in dotted decimal notation

3.3.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show loopback** [*interface-type interface-number*]	Show configurations of interface loopback.
2	Raisecom#**show loopback-statistics** [*interface-type interface-number*]	Show statistics on loopback packets.

3.3.6 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
Raisecom(config)#**clear loopback-statistics** [*interface-type interface-number*] **Example:** Raisecom(config)#clear loopback-statistics	Clear statistics on loopback packets. • interface-type: interface type • interface-number: interface ID. The form and value range depend on the interface type.

Copyright © Raisecom Technology Co., Ltd.

3.4 ARP

3.4.1 Introduction

In TCP/IP network environment, each host is assigned with a 32-bit IP address that is a logical address used to identify hosts between networks. To transmit packets in physical link, you must know the physical address of the destination host, which requires mapping the IP address to the physical address. In Ethernet environment, the physical address is 48-bit MAC address. The system has to transfer the 32-bit IP address of the destination host to the 48-bit Ethernet address for transmitting packet to the destination host correctly. Then Address Resolution Protocol (ARP) is applied to resolve IP address to MAC address and configure mapping between IP address and MAC address.

The ARP address table contains the following two types:

- Static entry: bind the IP address and MAC address to avoid ARP dynamic learning cheating.
  - The static ARP address entry needs to be added/deleted manually.
  - The static ARP address entry is not aged.
- Dynamic entry: MAC address automatically learned through ARP.
  - This dynamic ARP address entry is automatically generated by switch. You can adjust partial parameters of it manually.
  - The dynamic ARP address entry will be aged after the aging time if not used.

The ISCOM2600G series switch supports the following two modes of dynamically learning ARP address entries:

- Learn-all: in this mode, the ISCOM2600G series switch learns both ARP request packets and response packets. When device A sends its ARP request, it writes mapping between its IP address and physical address in ARP request packets. When device B receives ARP request packets from device A, it learns the mapping in its address table. In this way, device B will no longer send ARP request when sending packets to device A.
- learn-reply-only mode: in this mode, the ISCOM2600G series switch learns ARP response packets with corresponding ARP request only sent by itself. For ARP request packets from other devices, it responds with ARP response packets only rather than learning ARP address mapping entry. In this way, network load is heavier but some network attacks based on ARP request packets can be prevented.

3.4.2 Preparing for configurations

Scenario

The mapping of IP address and MAC address is saved in the ARP address table.

Generally, the ARP address table is dynamically maintained by the ISCOM2600G series switch. The ISCOM2600G series switch searches for the mapping between IP address and MAC address automatically according to ARP. You just need to configure the ISCOM2600G series switch manually for preventing ARP dynamic learning from cheating and adding static ARP address entries.

Prerequisite

N/A

Copyright © Raisecom Technology Co., Ltd.

3.4.3 Default configurations of ARP

Default configurations of ARP are as below.

Function	Default value
Static ARP entry	N/A
Dynamic ARP entry learning mode	learn-all
Aging time of dynamic ARP entries	1200s
Dynamic ARP entry learning on the interface	Enable
Local proxy ARP	Disable
Maximum number of dynamically learnt ARP entries	4096
Gratuitous ARP packet learning on the interface	Enable

3.4.4 Configuring static ARP entries

Caution

- The IP address in static ARP entry must belong to the IP network segment of Layer 3 interface on the switch.
- The static ARP entry needs to be added and deleted manually.

Configure static ARP entries for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#arp` *`ip-address mac-address`* **`Example:`** `Raisecom(config)#arp 192.168.27.26 000e.5e12.3456`	Configure static ARP entry. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1 • mac-address: MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456

3.4.5 Configuring dynamic ARP entries

Configure dynamic ARP entries for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**arp mode** { **learn-all** | **learn-reply-only** } **Example:** Raisecom(config)#arp mode learn-all	Configure the aging time of dynamic ARP entries. • learn-all: learn MAC addresses contained in the reply packets of all hosts. • learn-reply-only: learn the MAC address contained in the reply packet from the requested host.
3	Raisecom(config)#**arp aging-time** *time* **Example:** Raisecom(config)#arp aging-time 1500	(Optional) configure the aging time of dynamic ARP entries. • time: aging time, an integer, ranging from 60 to 2147483, in units of second
4	Raisecom(config)#**arp max-learning-num** *number* **Example:** Raisecom(config)#arp max-learning-num 100	(Optional) configure the maximum number of dynamic ARP entries allowed to learn on the Layer 3 interface. • number: maximum number, an integer, ranging from 1 to 4096
5	Raisecom(config)#**interface vlan** *vlan-id* **Example:** Raisecom(config)#interface vlan 1	Enter VLAN interface configuration mode. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
6	Raisecom(config-vlan*)#**arp learning** [**strict**]{ **enable** | **disable** } **Example:** Raisecom(config-vlan1)#arp learning disable	(Optional) configure dynamic ARP learning. • strict: strictly learn ARP entries. • enable: enable dynamic ARP learning on the interface. • disable: disable dynamic ARP learning on the interface.
7	Raisecom(config-vlan*)#**gratuitous-arp-learning** { **enable** | **disable** } **Example:** Raisecom(config-vlan1)#gratuitous-arp-learning disable	(Optional) configure gratuitous ARP packet learning. • enable: enable gratuitous ARP packet learning. • disable: disable gratuitous ARP packet learning.

3.4.6 Configuring proxy ARP

Configure proxy ARP for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#interface vlan vlan-id`
	Example:
	`Raisecom(config)#interface vlan 1`
		Enter VLAN interface configuration mode.
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094

3	`Raisecom(config-vlan*)#arp local-proxy { enable | disable }`
	Example:
	`Raisecom(config-vlan1)#arp local-proxy enable`
		Enable local proxy ARP.
		• enable: enable local proxy ARP.
		• disable: disable local proxy ARP.

3.4.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show arp [ ip-address | interface vlan vlan-id [ valid ] | static | valid ]`	Show information about entries in the ARP address table.
2	`Raisecom#show arp local-proxy [ interface vlan vlan-id ]`	Show information about local proxy ARP.

3.4.8 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description

`Raisecom(config)#clear arp[ ip-address | interface vlan vlan-id ]`
Example:
`Raisecom(config)#clear arp`
	Clear all entries in the ARP address table.
	• ip-address: IP address, in dotted decimal notation, such as 10.10.10.1
	• vlan-id: VLAN ID, an integer, ranging from 1 to 4094

3.4.9 Example for configuring ARP

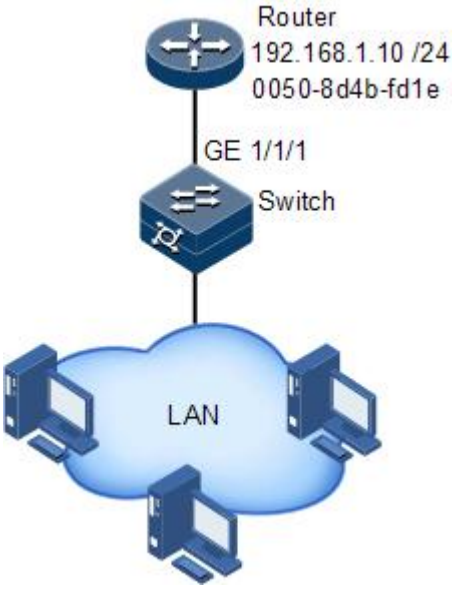
Networking requirements

As shown in Figure 3-3, the ISCOM2600G series switch is connected to the host, and is also connected to the upstream Router through GE 1/1/1. For the Router, the IP address and submask are 192.168.1.10/24, and the MAC address is 0050-8d4b-fd1e.

To improve communication security between the Switch and Router, you need to configure related static ARP entry on the ISCOM2600G series switch.

Copyright © Raisecom Technology Co., Ltd.

Figure 3-3 Configuring ARP networking



Configuration steps

Add a static ARP entry.

```
Raisecom#config
Raisecom(config)#arp 192.168.1.10 0050.8d4b.fd1e
```

Checking results

Use the **show arp** command to show configurations of the ARP address table.

```
Raisecom#show arp
ARP aging-time: 1200 seconds(default: 1200s)
ARP mode: Learn all
ARP table:
Total: 1    Static: 1    Dynamic: 0
IP Address     Mac Address      Interface  vlan  Type     Age(s)   status
-----------------------------------------------------------------------------
192.168.1.10   0050.8D4B.FD1E   vlan10     10   static   --     PERMANENT
```

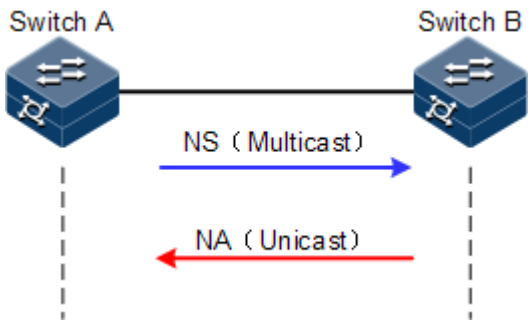
3.5 NDP

3.5.1 Introduction

Neighbor Discovery Protocol (NDP) is a neighbor discovery mechanism used on IPv6 devices in the same link. It is used to discover neighbors, obtain MAC addresses of neighbors, and maintain neighbor information.

NDP obtains data link layer addresses of neighbor devices in the same link, namely, MAC address, through the Neighbor Solicitation (NS) message and Neighbor Advertisement (NA) message.

Figure 3-4 Principles of NDP address resolution



As shown in Figure 3-4, take Switch A for example. Switch A obtains the data link layer address of Switch B as below:

Step 1 Switch A sends a NS message in multicast mode. The source address of the NS message is the IPv6 address of Layer 3 interface on Switch A, and the destination address of the NS message is the multicast address of the requested node of the Switch B. The NS message even contains the data link layer address of Switch A.

Step 2 After receiving the NS message, Switch B judges whether the destination address of the NS message is the multicast address of the request node corresponding to the IPv6 address of Switch B. If yes, Switch B can obtain the data link layer address of Switch A, and sends a NA message which contains its data link layer address in unicast mode.

Step 3 After receiving the NA message from Switch B, Switch A obtains the data link layer address of Switch B.

By sending ICMPv6 message, IPv6 NDP even has the following functions:

- Verify whether the neighbor is reachable.
- Detect duplicated addresses.
- Discover routers or prefix.
- Automatically configure addresses.
- Support redirection.

3.5.2 Preparing for configurations

Scenario

IPv6 NDP not only implements IPv4 ARP, ICMP redirection, and ICMP device discovery, but also supports detecting whether the neighbor is reachable.

Copyright © Raisecom Technology Co., Ltd.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.
- Configure the IPv6 address of the Layer 3 interface.

3.5.3 Default configurations of NDP

Default configurations of NDP are as below.

Function	Default value
Times of sending NS messages for detecting duplicated addresses	1
Maximum number of NDPs allowed to learn	2048
Aging time of dynamic NDPs	1200s

3.5.4 Configuring static neighbor entries

To resolute the IPv6 address of a neighbor into the data link layer address, you can use the NS message and NA message, or manually configure static neighbor entries.

Configure static neighbor entries for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#ipv6 neighbor ipv6-address mac-address`
	Example:
	`Raisecom(config)#ipv6 neighbor 2001::3 000E.5E12.3456`
		Configure static neighbor entries.
		• ipv6-address: IPv6 unicast address, in colon hexadecimal notation
		• mac-address: MAC address, in dotted hexadecimal notation. It should not be a multicast MAC address or an all-0 address.

3.5.5 Configuring aging time of dynamic NDPs

NDP entries are not permanently valid but valid for only a period. After the period expires, a NDP entry will be deleted if it is not updated. The period is called the aging time.

Configure the aging time of dynamic NDPs for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#ipv6 neighbor aging-time time`
	Example:
	`Raisecom(config)#ipv6 neighbor aging-time 1500`
		Configure the aging time of dynamic NDPs.
		• Time: aging time, an integer, ranging from 60 to 2147483, in units of second

3.5.6 Configuring times of sending NS messages for detecting duplicated addresses

Configure times of sending NS messages for detecting duplicated addresses for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#ipv6 nd dad attempts value`
	Example:
	`Raisecom(config)#ipv6 nd dad attempts 5`
		Configure times of sending NS messages for detecting duplicated addresses.
		• value: times for sending NS, an integer, ranging from 0 to 600 where the value 0 means forbidding checking whether the address is occupied

Note

When the ISCOM2600G series switch obtains an IPv6 address, it uses the duplicated address detection function to determine whether the IPv6 address is already used by another device. After sending NS messages for a specified times and receiving no response, it determines that the IPv6 address is not duplicated and thus can be used.

3.5.7 Configuring maximum number of NDPs allowed to be learnt

Configure the maximum number of NDPs allowed to be learnt on the Layer 3 interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#ipv6 neighbors max-learning-num number`
	Example:
	`Raisecom(config)#ipv6 neighbors max-learning-num 4`
		Configure the maximum number of NDPs allowed to be learnt on the Layer 3 interface.
		• number: maximum number of NDPs, an integer, ranging from 1 to 2048

Copyright © Raisecom Technology Co., Ltd.

3.5.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show ipv6 neighbors**	Show all NDP neighbor information.
2	Raisecom#**show ipv6 neighbors** *ipv6-address*	Show neighbor information about a specified IPv6 address.
3	Raisecom#**show ipv6 neighbors vlan** *vlan-id*	Show neighbor information about a specified layer 3 interface.
4	Raisecom#**show ipv6 neighbors static** [**count**]	Show information about IPv6 static neighbor.
5	Raisecom#**show ipv6 neighbors** *interface-type interface-number*	Show neighbor information about a specified interface.
6	Raisecom#**show ipv6 neighbors dynamic count**	Show the number of dynamic IPv6 neighbors.
7	Raisecom#**show ipv6 neighbors all count**	Show the number of all IPv6 neighbors.
8	Raisecom#**show ipv6 interface nd** [*interface-type interface-number*]	Show ND information configured on the interface.
9	Raisecom#**show ipv6 interface prefix** [*interface-type interface-number*]	Show the prefix of the IPv6 address.

3.5.9 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
Raisecom(config)#**clear ipv6 neighbors**	Clear information about all IPv6 neighbors.

3.6 Static route

3.6.1 Introduction

A route is required for communication among different devices in one VLAN, or different VLANs. The route is used to transmit packets through network to destination, which adopts routing table for forwarding packets.

Copyright © Raisecom Technology Co., Ltd.

Default route

The default route is a special route that can be used only when there is no matched item in the routing table. The default route appears as a route to network 0.0.0.0 (with mask 0.0.0.0) in the routing table. You can show configurations of the default route by using the **show ip route** command. If the ISCOM2600G series switch has not been configured with default route and the destination IP of the packet is not in the routing table, the ISCOM2600G series switch will discard the packet and return an ICMP packet to the Tx end to inform that the destination address or network is unavailable.

Static route

A static route is the route configured manually, thus bringing low requirements on the system. It is available to simple, small, and stable network. The disadvantage is that it cannot adapt to network topology changes automatically and needs manual intervention.

3.6.2 Preparing for configurations

Scenario

Configure the static route for simple network topology manually to establish an intercommunication network.

Prerequisite

Configure the IP address of the VLAN interface correctly.

3.6.3 Configuring static route

Configure the static route for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**ip route** *ip-address ip-mask* { *next-hop-ip-address* [*interface-type interface-num*]| **NULL 0** } [**distance** *distance-num*] [**description** *description-text*] [**tag** *tag-id*] [**track bfd-session** *session-id*] Raisecom(config)#**ip route** *ip-address/mask-length* { *next-hop-ip-address* / **NULL 0** } [**distance** *distance-num*] [**description** *description-text*] [**tag** *tag-id*] [**track bfd-session** *session-id*] **Example:** Raisecom(config)#ip route 10.0.0.0 255.0.0.0 10.0.1.2	Configure the IPv4 static route. The device supports BFD. When the interface is Down, BFD becomes Down and the static route is deleted. When the interface is Up, BFD becomes Up and the static route is added to the routing table. • ip-address: destination IP address, in dotted decimal notation, such as 10.0.0.1 • ip-address/mask-length: destination IP address/mask length, such as 192.168.1.0/24. The mask length is an integer, ranging from 0 to 32. • ip-mask: mask length, in dotted decimal notation, such as 255.255.255.255 • next-hop-ip-address: next-hop IP address, in dotted decimal notation, such as 10.0.0.1 • interface-type: interface type • interface-num: interface ID • distance distance-num: administrative distance of static route. The distance is the administrative distance, which is an integer, ranging from 1 to 255. • Description description-text: description of the static route. The description is the description, a string of 1 to 60 characters. • tag-id: identification of static route. The tag-id is the identification ID, an integer, ranging from 1 to 4294967295. • session-id: ID of the BFD session to be added to the static route, an integer, ranging from 1 to 64 • NULL0: NULL interface
	Raisecom(config)#**ipv6 route** { *ipv6-address/prefix-length* | *ipv6-address/0* }{ *next-hop-ipv6-address* | **NULL 0** } [**distance** *distance-num*] [**description** *text*] [**tag** *tag-id*] **Example:** Raisecom(config)#ipv6 route 1:123::1:1/96 1:123::0:1 distance 100 description route1 tag 20	Configure the IPv6 static route. • ipv6-address/prefix-length: IPv6 router prefix, in IPv6 address with prefix length, such as 1:123::0:1/96. • ipv6-address/0: default IPv6 address, with prefix of 0, such as 1:123::0:1/0 • ipv6-address: IPv6 address of next hop, such as 1:123::0:1 • distance-num: administrative distance of the static route, an integer, ranging from 1 to 255. When this parameter is not selected, use the **ip route static distance** command to configure the default administrative distance. • text: description of the static route. The description is a string of 1 to 60 characters. • tag-id: Tag of the static route. The tag-id is the tag ID, an integer, ranging from 1 to 4294967295. • NULL0: NULL interface

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**ip route static distance** *distance-num* **Example:** Raisecom(config)#ip route static distance 2	(Optional) configure the default administrative distance of the IPv4 static route. • Distance-num: administrative distance of the static route, an integer, ranging from 1 to 255
	Raisecom(config)#**ipv6 route static distance** *distance-num* **Example:** Raisecom(config)#ipv6 route static distance 2	(Optional) configure the default administrative distance of the IPv6 static route. • Distance-num: administrative distance of the static route, an integer, ranging from 1 to 255

3.6.4 Configuring route mangement

Configure route management for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router id** *router-id* **Example:** Raisecom(config)#router id 192.168.1.2	Configure the router ID. By default, it is 192.168.1.1. • router-id: routing device ID, identifying a router device, in dotted decimal notation, such as 10.10.10.1. IP addresses starting with 0 and 127, D type IP addresses, and E type IP addresses are not allowed to be configured.
3	Raisecom(config)#**route recursive-lookup tunnel** [**ip-prefix** *list-name*] **Example:** Raisecom(config)#route recursive-lookup tunnel	Configure non-labeled public network routes to be recursive to a LSP tunnel. • ip-prefix list-name: specify the IP prefix names to limit the route ranges which will be iterated to tunnels. The list-name is a string of 1 to 20 characters.

3.6.5 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Raisecom#**show router id**	Show information about IPv4 routes.
2	Raisecom#**show ip route protocol** { **static** | **connected** | **bgp** | **ospf** | **isis** | **rip** } [**detail**]	Show information about the routing table.

Copyright © Raisecom Technology Co., Ltd.

No.	Item	Description
	Raisecom#**show ipv6 route** [[**all**] **protocol** { **static** | **connected** | **bgp** | **ospf** | **isis** | **rip** }] [**detail**]	
3	Raisecom#**show ip route** *ip-address1* [*mask-address1*] *ip-address2* [*mask-address2*] [**detail**]	Show information about routes between two IP addresses.
4	Raisecom#**show** { **ip** | **ipv6** } **route summary**	Show route statistics.
5	Raisecom#**show ip route** *ip-address* [*mask-address*] [**longer-prefixes**]	Show information about a route to a destination.
6	Raisecom#**show ip fib** [*ip-address* | **nexthop** *ip-address*]	Show information about FIB entries.
	Raisecom#**show ipv6 fib** [*ipv6-address* | **nexthop** *ipv6-address*]	
7	Raisecom#**show ip fib summary**	Show statistics in the routing table.
	Raisecom#**show ipv6 fib summary**	

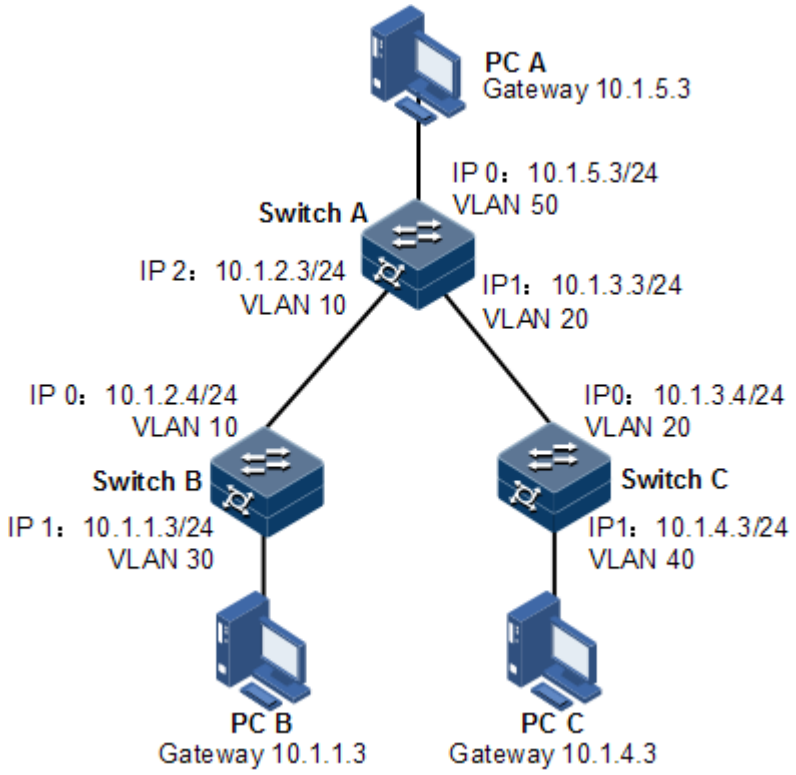
3.6.6 Example for configuring static route

Networking requirements

Configure the static route to enable any two hosts or ISCOM2600G series switch devices successfully to ping through each other, as shown in Figure 3-5.

Copyright © Raisecom Technology Co., Ltd.

Figure 3-5 Configuring static route



Configuration steps

Step 1 Configure the IP address of each device. Detailed configurations are omitted.

Step 2 Configure the static route on Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.4
SwitchA(config)#ip route 10.1.4.0 255.255.255.0 10.1.3.4
```

Step 3 Configure the default gateway on Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#ip route 0.0.0.0 0.0.0.0 10.1.2.3
```

Step 4 Configure the default gateway on Switch C.

```
Raisecom#hostname SwitchC
SwitchC#config
SwitchC(config)#ip route 0.0.0.0 0.0.0.0 10.1.3.3
```


Copyright © Raisecom Technology Co., Ltd.

Step 5 Configure the default gateway of host A to 10.1.5.3. Detailed configurations are omitted.

Configure the default gateway of host B to 10.1.1.3. Detailed configurations are omitted.

Configure the default gateway of host C to 10.1.4.3. Detailed configurations are omitted.

Checking results

Use the **ping** command to check whether any two of all devices can ping through each other.

```
SwitchA#ping 10.1.1.3
Type CTRL+C to abort
Sending 5, 8-byte ICMP Echos to 10.1.1.3, timeout is 3 seconds:
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms
Reply from 10.1.1.3: time<1ms

---- PING Statistics----
5 packets transmitted, 5 packets received,
Success rate is 100 percent(5/5),
round-trip (ms)  min/avg/max = 0/0/0.
```

3.7 Routing policy

3.7.1 Configuring IP prefix list

Configure the IP prefix list for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip prefix-list` *`prefix-name`* `[ seq` *`seq-number`* `] { deny | permit } any`	Create an IP prefix list or add a node to the IP prefix list.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	`Raisecom(config)#`**`ip prefix-list`** *`prefix-name`* [**`seq`** *`seq-number`*] { **`deny`** | **`permit`** } *`ip-address/mask`* [**`ge`** *`min-length`*] [**`le`** *`max-length`*] **Example:** `Raisecom(config)#ip prefix-list pre1 seq 2 permit 172.16.0.0/16`	If no prefix list ID (*seq-number*) is configured, the system will generate a prefix list ID automatically. The generated pre-fix list ID has 5 digits. • prefix-name: name of the prefix list, a string of 1 to 20 characters • seq seq-number: sequence of the prefix list. The seq-number is an integer, ranging from 1 to 4294967295. • deny: deny the access to the route that matches conditions. • permit: permit the access to the route that matches conditions. • any: match any IP address. • ip-address: matching IP address, in dotted decimal notation, such as 10.10.10.1 • mask: length of the mask of the matching IP address, an integer, ranging from 1 to 32 • ge min-length: minimum length of the mask of the matching IP address. The min-length is an integer, ranging from 0 to 32. • le max-length: maximum length of the mask of the matching IP address. The max-length is an integer, ranging from 0 to 32.
3	`Raisecom(config)#`**`ip prefix-list`** *`prefix-name`* **`description`** *`string`* **Example:** `Raisecom(config)#ip prefix-list pre01 description test`	Configure the description of the IP prefix list. If the length of descriptions exceeds 80 characters, the configuration will not take effect. • prefix-name: name of the prefix list, a string of characters • string: description, a string of 1 to 80 characters. If the description contains spaces, use quotation marks to embrace it.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config)#**ipv6 prefix-list** *prefix-name* **seq** *seq-number* { **deny** | **permit** } **any** Raisecom(config)#**ipv6 prefix-list** *prefix-name* **seq** *seq-number* { **deny** | **permit** } *ipv6-address/mask* [**ge** *min-length*] [**le** *max-length*] **Example:** Raisecom(config)#ipv6 prefix-list pre1 seq 2 permit 3FFE::2/128	Create an IPv6 prefix list, or add a node to it. • prefix-name: name of the prefix list, a string of 1 to 20 characters • seq seq-number: sequence of the prefix list. The seq-number is an integer, ranging from 1 to 4294967295. • deny: deny the access to the route that matches conditions. • permit: permit the access to the route that matches conditions. • any: match any IP address. • Ipv6-address: matching IPv6 address, in colon hexadecimal notation, such as 3001::1 • mask: length of the mask of the matching IPv6 address, an integer • ge min-length: minimum length of the mask of the matching IPv6 address. The min-length is an integer, ranging from 0 to 128. • le max-length: maximum length of the mask of the matching IPv6 address. The max-length is an integer, ranging from 0 to 128.
5	Raisecom(config)#**ipv6 prefix-list** *prefix-name* **description** *string* **Example:** Raisecom(config)#ipv6 prefix-list pre01 description test	Configure the description of the IPv6 prefix list. • prefix-name: name of the prefix list, a string of characters • string: description, a string of 1 to 80 characters. If the description contains spaces, use quotation marks to embrace it.

Note

- If one record is the **permit** type, all mismatched routes are the **deny** type by default. Only matched routes can pass filtering of the IP prefix list.
- If one record is the **deny** type, all mismatched routes are the **deny** type by default. Even matched routes cannot pass filtering of the IP prefix list. Therefore, you need to add a **permit** record after multiple **deny** records to allow other routes to pass.
- If there are multiple records in the IP prefix list, there must be a record of the **permit** type.

3.7.2 Configuring routing table

Configure the routing table for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**route-map** *map-name* { **permit** | **deny** } *number* **Example:** Raisecom(config)#route-map map1 permit 1	Create a routing table, and enter route mapping configuration mode. • map-name: name of the routing table, a string of 1 to 20 characters • permit: permit the access to the route that matches conditions. • deny: deny the access to the route that matches conditions. • number: number of the node in the routing table, an integer, ranging from 1 to 65535
3	Raisecom(config-route-map)#**description** *string* **Example:** Raisecom(config-route-map)#description test	(Optional) configure the description of the routing table. • string: description, a string of 1 to 80 characters. If the description contains spaces, use quotation marks to embrace it.
4	Raisecom(config-route-map)#**on-match next**	(Optional) configure the on-match clause to continue to match at the next node. By default, the process is finished after matching.
5	Raisecom(config-route-map)#**on-match goto** *number* **Example:** Raisecom(config-route-map)#on-match goto 10	(Optional) configure the on-match clause to continue to match at some node. By default, the process is finished after matching. • number: number of the node in the routing table, an integer, ranging from 1 to 65535
6	Raisecom(config-route-map)#**call** *map-name* **Example:** Raisecom(config-route-map)#call map2	(Optional) continue to match routes by scheduling other routing table after matching the route. By default, the process is finished after matching. • map-name: name of the routing table, a string of 1 to 20 characters
7	Raisecom(config-route-map)#**match ip next-hop** *acl-number* **Example:** Raisecom(config-route-map)#match ip next-hop 2982	(Optional) configure the match clause to match the next hop based on extended IP ACL. • acl-number: advanced IP ACL number, an integer, ranging from 2000 to 2999
8	Raisecom(config-route-map)#**match ip next-hop prefix-list** *prefix-name* **Example:** Raisecom(config-route-map)#match ip next-hop prefix-list pre01	(Optional) configure the match clause to match the next hop based on IP prefix list. • prefix-name: name of the prefix list, a string of 1 to 20 characters

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
9	Raisecom(config-route-map)#**match ip address** *acl-number* **Example:** Raisecom(config-route-map)#match ip address 2002	(Optional) configure the match clause to matching the IP address based on extended IP ACL. • acl-number: advanced IP ACL number, an integer, ranging from 2000 to 2999
10	Raisecom(config-route-map)#**match ip address prefix-list** *prefix-name* **Example:** Raisecom(config-route-map)#match ip address prefix-list pre02	(Optional) configure the match clause to matching the IP address based on IP prefix list. • prefix-name: name of the prefix list, a string of 1 to 20 characters
11	Raisecom(config-route-map)#**match interface** *name* **Example:** Raisecom(config-route-map)#match interface port1	(Optional) configure the match clause to matching the interface name. • name: interface name, a string of characters
12	Raisecom(config-route-map)#**match metric** *metric-value* **Example:** Raisecom(config-route-map)#match metric 1000	(Optional) configure the match clause to the matching rule that is based on route metric value. • metric-value: route metric, an integer, ranging from 4294967295
13	Raisecom(config-route-map)#**match tag** *tag-id* **Example:** Raisecom(config-route-map)#match tag 5	(Optional) configure the match clause to the matching rule that is based on Tag field of the route tagging. • tag-id: route Tag value, an integer, ranging from 1 to 4294967295
14	Raisecom(config-route-map)#**set metric** [+ | -] *metric-value* **Example:** Raisecom(config-route-map)#set metric 20	(Optional) configure the match clause to the BGP routing information matching rule that is based on prefix list matching with source address of the route. • metric-value: route metric, an integer, ranging from 4294967295 • +: increase the route metric. • -: decrease the route metric.
15	Raisecom(config-route-map)#**set metric-type** { **type-1** | **type-2** } **Example:** Raisecom(config-route-map)#set metric-type type-1	(Optional) configure the set clause to modifying the route metric value after matching. • type-1: OSPF external metric type 1 • type-2: OSPF external metric type 2
16	Raisecom(config-route-map)#**set src** *ip-address* **Example:** Raisecom(config-route-map)#set src 172.16.20.1	(Optional) configure the set clause to modifying the route metric type after matching. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
17	Raisecom(config-route-map)#**set ip next-hop** *ip-address* **Example:** Raisecom(config-route-map)#set ip next-hop 172.16.20.3	(Optional) configure the set clause to modifying the source IP address after matching. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1
18	Raisecom(config-route-map)#**set tag** *tag-id* **Example:** Raisecom(config-route-map)#set tag 10	(Optional) configure the set clause to modifying the next-hop IP address of the route after matching. • tag-id: route Tag value, an integer, ranging from 1 to 4294967295

3.7.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show ip prefix-list** [*prefix-name*] [**seq** *seq-number*] Raisecom#**show ip prefix-list** *prefix-name ip-address/mask* { **longer** | **first-match** }	Show information about the IP prefix list.
2	Raisecom#**show ip prefix-list** [**summary** *prefix-name*]	Show summary of the IP prefix list.
3	Raisecom#**show ip prefix-list detail** [*prefix-name*]	Show statistics on the IP prefix list.
4	Raisecom#**show ipv6 prefix-list** [*prefix-name*] [**seq** *seq-number*] Raisecom#**show ipv6 prefix-list** *prefix-name ipv6-address/mask* { **longer** | **first-match** }	Show information about the IPv6 prefix list.
5	Raisecom#**show ipv6 prefix-list summary** [*prefix-name*]	Show summary of the IPv6 prefix list.
6	Raisecom#**show ipv6 prefix-list detail** [*prefix-name*]	Show statistics on the IPv6 prefix list.
7	Raisecom#**show route-map** [*map-name*]	Show configurations of the routing table.

3.7.4 Maintenance

Maintain the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Command	Description
Rasiecom#**clear ip prefix-list** [*prefix-name* [*ip-address/mask*]] **Example:** Rasiecom#clear ip prefix-list	Clear information about all IPv6 neighbors. • prefix-name: name of the prefix list, a string of 1 to 20 characters • ip-address: matching IP address, in dotted decimal notation, such as 10.10.10.1 • mask: length of the mask of the matching IP address, an integer, ranging from 1 to 32
Rasiecom#**clear ipv6 prefix-list** [*prefix-name* [*ipv6-address/mask*]] **Example:** Rasiecom#clear ipv6 prefix-list	Clear statistics on the IPv6 prefix list. • prefix-name: name of the prefix list, a string of 1 to 20 characters • ipv6-address: matching IPv6 address, in colon hexadecimal notation, such as 3001::1 • mask: length of the mask of the matching IPv6 address, an integer

Copyright © Raisecom Technology Co., Ltd.

4 PoE

This chapter describes basic principles and configuration procedures of PoE, and provides related configuration examples, including the following sections:

- Introduction
- Configuring PoE
- Configuring Smart PoE
- Example for configuring PoE power supply

Note

This chapter is supported by PoE switches only. PoE switches support uninterrupted power supply during hot restart. Save running configurations before restart, otherwise PoE parameters will be restored to default values and thus power supply will fail to meet requirements.

4.1 Introduction

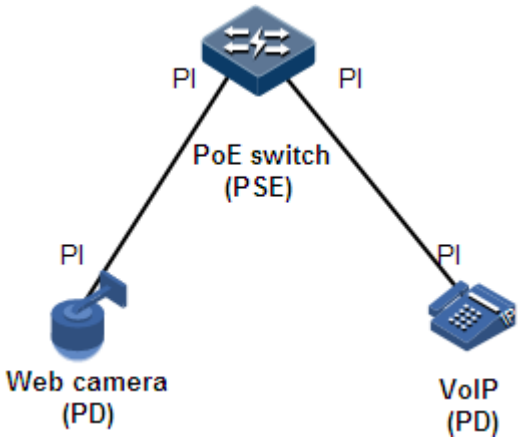
4.1.1 Principles of PoE

Power over Ethernet (PoE) means that the Power Sourcing Equipment (PSE) both supplies power and transmits data to the remote Power Device (PD) through the Ethernet cable and Power Interface (PI).

Figure 4-1 shows principles of PoE.

Copyright © Raisecom Technology Co., Ltd.

Figure 4-1 Principles of PoE



4.1.2 PoE modules

The PoE system consists of the following modules:

- PSE: consist of the power module and PSE functional module. The PSE can detect PDs, obtain PD power information, remotely supply power, monitor power supply, and power off PDs.
- PD: supplied with power by the PSE. There are standard PDs and non-standard PDs. Standard PDs must comply with IEEE 802.3af or IEEE 802.3at, such as the IP phone and web camera.
- PI: the interface connecting the PSE/PD to the Ethernet cable, namely, the RJ45 interface

4.1.3 PoE advantages

PoE has the following advantages:

- Reliability: a centralized PSE supplies power with convenient backup, uniform management of power modules, and high security.
- Convenient connection: the network terminal does not need an external power supply; instead, it needs only one Ethernet cable connected to the PoE interface.
- Standardization: PoE complies with IEEE 802.3at and uses globally uniform power interface.
- Wide applications: applicable to IP phones, wireless Access Point (AP), portable device charger, credit card reader, web camera, and data collection system.

4.1.4 PoE concepts

- Maximum output power of PoE

It is the maximum output power output by the interface to the connected PD.

- Priority of PoE

There are three levels of priorities for power supply: critical, high, and low. The PSE supplies power to the PD connected to the PI with critical priority preferentially, the PD connected to the PI with the high priority, and finally the PD connected to the PI with the low priority.

- Overtemperature protection

Copyright © Raisecom Technology Co., Ltd.

When the current temperature exceeds the overtemperature threshold, overtemperature alarms occur and the system sends Trap to the Network Management System (NMS).

- Global Trap

When the current temperature exceeds the overtemperature threshold, the current PSE power utilization rate exceeds the threshold, or the status of PoE changes, the ISCOM2600G series switch sends Trap to the NMS.

- PSE power utilization rate threshold

When the PSE power utilization rate exceeds the threshold for the first time, the system sends Trap.

4.1.5 Smart PoE

Compared with common PoE, Smart PoE supports smarter device management features as below:

- Support PD active detection to detect whether PDs are active.
- Support PoE scheduling to periodically restart PDs.
- Support PoE scheduling to supply power in the specified period.
- Support monitoring status, including PoE status, power, current, voltage, and Trap sending status.

Through linktrace, PD Active check monitors in realtime whether PDs are active. It will generate an alarm or restart the PoE interface according to configured action if a PD fails to respond.

PoE scheduling enables a PoE interface to supply power in the specified period to save power and money for the enterprise, or restarts the PoE interface at a specified interval to minimize possibility of PD damage or buffer overflowing.

A PoE scheduling profile is a set of configurations. If you apply the PoE scheduling profile to multiple PoE interfaces, these PoE interfaces will have the same PoE features. If a PoE interface needs to be replaced, apply the PoE scheduling profile, which was applied to the original PoE interface, to the new PoE interface, without configuring the new PoE interface parameter by parameter. In this way, the network management staff can easily configure PoE.

The ISCOM2600G series switch supports multiple PoE scheduling profiles. Save different PoE configurations for different PDs in different PoE scheduling profiles, and apply the corresponding PoE scheduling profile on the PoE interface. By configuring PoE scheduling, you can specify PoE parameters on the PoE interface, such as the start time and restart interval, to enable the ISCOM2600G series switch to intelligently supply power and to control when to shut down the PoE interface.

4.2 Configuring PoE

4.2.1 Preparing for configurations

Scenario

When the remotely connected PE is inconvenient to take power, it needs to take power from the Ethernet electrical interface to concurrently transmit power and data.

Copyright © Raisecom Technology Co., Ltd.

Prerequisite

N/A

4.2.2 Default configurations of PoE

Default configurations of PoE are as below.

Function	Default value
PI PoE status	Enable
Non-standard PD identification	Enable
Maximum output power of PoE	30000 mW
Power supply management mode	Auto
PoE priority	Low
Overtemperature protection status	Enable
Power supply global Trap switch status	Enable
PSE power utilization rate threshold	99%

4.2.3 Enabling interface PoE

Enable interface PoE for the ISCOM2600G series switch as below:

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#poe { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#poe enable`
		Enable or disable interface PoE.
		• enable: enable interface PoE.
		• disable: disable interface PoE.

4.2.4 Configuring maximum output power of PoE

Configure the maximum output power of PoE for the ISCOM2600G series switch as below:

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#poe max-power max-power-value`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#poe max-power 6050`
		Configure the maximum output power of PoE.
		• max-power-value: maximum output power, an integer, ranging from 4000 to 30000, in units of mW

4.2.5 Configuring maximum output power of device

Configure the maximum output power of the device for the ISCOM2600G series switch as below:

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#poe pse max-power max-power-value`
	Example:
	`Raisecom(config)#poe pse max-power 300`
		Configure the maximum output power of the device.
		• max-power-value: maximum output power of the device, an integer, ranging from 0 to 600, in units of W

4.2.6 Configuring priority of PoE

Configure the priority of PoE for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#poe priority { critical | high | low }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#poe priority high`
		Configure the priority of PoE.
		• critical: critical priority
		• high: high priority
		• low: low priority

Copyright © Raisecom Technology Co., Ltd.

4.2.7 Configuring PSE power utilization rate threshold

Configure the PSE power utilization rate threshold for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#poe pse power-threshold` *`percent`* **Example:** `Raisecom(config)#poe pse power-thredshold 60`	Configure the PSE power utilization rate threshold. • percent: threshold ratio, an integer, ranging from 1 to 99, indicating 1% to 99%

4.2.8 Configuring identification of non-standard PDs

Caution

To use other non-standard PD, confirm its power consumption, voltage, and current in advance to properly configure the maximum output power on the PSE and to avoid damaging the PD due to too high output power.

Configure identification of non-standard PDs for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#poe legacy { enable | disable }`
	Example:
	`Raisecom(config)#poe legacy enable`
		Enable or disable the PSE to identify non-standard PDs.
		• enable: enable the PSE to identify the non-standard PD.
		• disable: disable the PSE to identify the non-standard PD.

4.2.9 Enabling forcible power supply on interface

Caution

When using the ISCOM2600G series switch to supply power for a remote PD, we recommend using a standard PD, pre-standard PD, or Cisco-primate standard PD. To use other non-standard PD in forcible power supply mode, confirm its power consumption, voltage, and current in advance to properly set the maximum output power on the PSE and to avoid damaging the PD due to too high output power.

Enable forcible power supply on interfaces for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config-gigaethernet1/1/port)#**poe force-power**	Enable forcible PoE power supply on the interface.

4.2.10 Enabling overtemperature protection

Enable overtemperature protection for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**poe temperature-protection { enable | disable }** **Example:** Raisecom(config)#poe temperature-protection enable	Enable or disable overtemperature protection. • enable: enable overtemperature protection. • disable: disable overtemperature protection.

4.2.11 Enabling global Trap

Enable global Trap for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**poe pse trap { enable | disable }** **Example:** Raisecom(config)#poe pse trap enable	Enable or disable global Trap. • enable: enable global Trap • disable: disable global Trap

4.2.12 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show poe interface** *interface-type interface-number* [**detail**]	Show power supply status on specified interfaces.
2	Raisecom#**show poe pse** [**detail**]	Show PSE configurations and realtime operating information.

Copyright © Raisecom Technology Co., Ltd.

4.3 Configuring Smart PoE

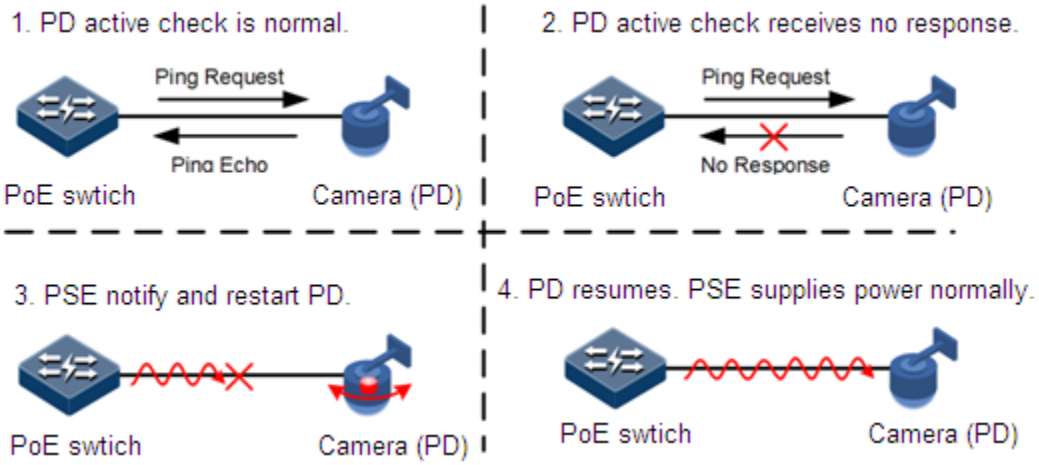
4.3.1 Preparing for configurations

Scenario

Through linktrace, PD Active check monitors in realtime whether PDs are active. It will generate an alarm or restart the PoE interface according to configured action if a PD fails to respond. You can configure the PoE interface and PD linktrace on this page.

As shown in Figure 4-2, by configuring PD Active check, you can monitor PD active status through realtime ping operations. When a PD fails to respond, the PoE switch will restart the corresponding PoE interface to resume the PD. PD Active check can improve reliability of PoE power supply and lower cost on device management.

Figure 4-2 PD Active check



PoE scheduling enables a PoE interface to supply power in the specified period to save power and money for the enterprise, or restarts the PoE interface at a specified interval to minimize possibility of PD damage or buffer overflow.

By configuring PoE scheduling profiles and applying them to specified PoE interfaces, you can configure PoE interfaces in batches, thus simplifying your operations.

By configuring PoE scheduling, you can specify PoE parameters on the PoE interface, such as the start time and restart interval, to enable the ISCOM2600G series switch to intelligently supply power and to control when to shut down the PoE interface.

Prerequisite

N/A

4.3.2 Default configurations of PoE

Default configurations of PoE are as below.

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
PD Active check	Enable
PD check action	N/A
Restart interval	N/A

4.3.3 Configuring PoE scheduling profile for interface

Configure the PoE scheduling profile for the interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
3	`Raisecom(config-gigaethernet1/1/port)#poe schedule profile` *`profile`* **Example:** `Raisecom(config-gigaethernet1/1/1)#poe schedule profile 2`	Configure the PoE scheduling profile for the interface. • profile: PoE scheduling profile ID, an integer, ranging from 1 to 4
4	`Raisecom(config-profile1)#rule` *`rule-id`* `{ reboot-time | start-time | end-time }` *`week hour minute`* **Example:** `Raisecom(config-profile1)#rule 1 reboot-time 1 10 20`	Configure rules for the PoE scheduling profile. • rule-id: rule ID of the schedule profile, an integer, ranging from 1 to 8 • reboot-time: reboot time on PoE interface • start-time: power supply start time on the PoE interface • end-time: power supply end time on the PoE interface • week: week, an integer, ranging from 1 to 7 • hour: hour, ranging from 0 to 23 • minute: minute, ranging from 0 to 59

4.3.4 Configuring linktrace

Linktrace is used to detect whether the destination host is reachable, so it can help you judge network connection. For example, you can apply it to the PoE for PD active check.

Configure linktrace for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#linktrace track track-id`
	Example:
	`Raisecom(config)#linktrace track 1`
		Configure the linktrace ID.
		• track-id: track ID, an integer, ranging from 1 to 128

3	`Raisecom(config-linktrace)#icmp ip-address { interface-type interface-number | source ip source-ip-address }`
	Example:
	`Raisecom(config-linktrace)#icmp 192.168.1.100 source ip 192.168.1.200`
		Configure the destination IP address of linktrace, and specify the linktrace type.
		• ip-address: configure the linktrace destination IP address, in dotted decimal notation.
		• interface-type: interface type
		• interface-number: linktrace source interface
		• source-ip-address: configure the linktrace type as the interface and specify the linktrace source IP address in dotted decimal notation.

4	`Raisecom(config-linktrace)#icmp interval time`
	Example:
	`Raisecom(config-linktrace)#icmp interval 10`
		Configure the period for sending linktrace packets.
		• time: ICMP interval, an integer, in units of second, ranging from 1 to 3600

5	`Raisecom(config-linktrace)#icmp retry count number`
	Example:
	`Raisecom(config-linktrace)#icmp retry count 2`
		Configure the maximum number of retry times for linktrace.
		• count number: retry times of Linktrace, an integer ranging from 1 to 5

4.3.5 Configuring PD active check

Configure PD active check for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-gigaethernet1/1/port)#**poe alive check { enable | disable }** **Example:** Raisecom(config-gigaethernet1/1/1)#poe alive check enable	Enable or disable PD active check. • enable: enable PD active check. • disable: disable PD active check.
4	Raisecom(config-gigaethernet1/1/port)#**poe alive action** { **reboot** | **reboot-alarm** | **alarm** } **Example:** Raisecom(config-gigaethernet1/1/1)#poe alive action reboot	Configuring the action for PD active check. • reboot: reboot the device. • reboot-alarm: reboot the device and send an alarm. • alarm: send an alarm.
5	Raisecom(config-gigaethernet1/1/port)#**poe reboot interval** *period* **Example:** Raisecom(config-gigaethernet1/1/1)#poe reboot interval 100	Configure the restart interval. • period: PD check reboot interval, an integer, ranging from 30 to 300, in units of second
6	Raisecom(config-gigaethernet1/1/port)#**poe linktrace track** *track-id* **Example:** Raisecom(config-gigaethernet1/1/1)#poe linktrace track 1	Bind a PoE interface with the specified linktrace ID. • track id: track ID, an integer, ranging from 1 to 128

Note

Before configuring linktrace for PD active check, create a linktrace of the corresponding PD, and then bind the PoE interface with the linktrace ID.

4.3.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show poe profile** { **all** | *profile* }	Show rules of the PoE scheduling profile.
2	Raisecom#**show poe interface** *interface-type interface-number* [**detail**]	Show the power supply status of the specified PoE interface.
3	Raisecom#**show linktrace**	Show linktrace configurations.

Copyright © Raisecom Technology Co., Ltd.

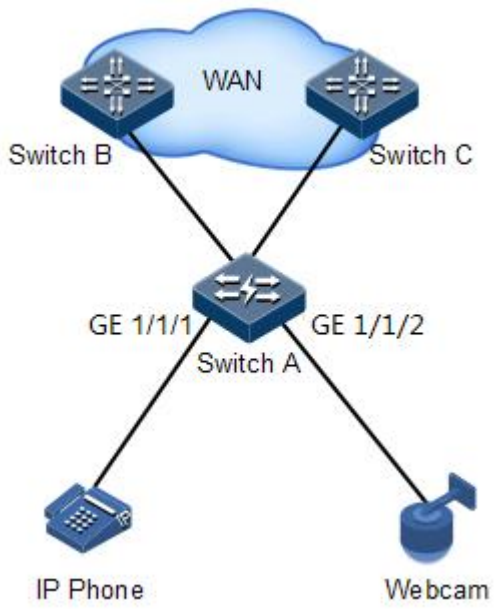
4.4 Example for configuring PoE power supply

Networking requirements

As shown in Figure 4-3, both Switch B and Switch C connect Switch A to the WAN, and PoE-supportive Switch A is used to supply power to an IP phone and a monitor camera. Switch A is required to supply power to the monitor camera preferentially when it runs at full load. Detailed requirements are as below:

- Configure the maximum output power of GE 1/1/1 and GE 1/1/2 to 30000 mW.
- Enable overtemperature protection on Switch A.
- Enable Trap for power supply on Switch A.
- Configure the priorities of GE 1/1/2 and GE 1/1/1 to high and low respectively.

Figure 4-3 PoE switch power supply networking



Configuration steps

Step 1 Enable PoE on GE 1/1/1 and GE 1/1/2.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#poe enable
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#poe enable
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 2 Configure the maximum output power of GE 1/1/1 and GE 1/1/2 to 30000 mW.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#poe max-power 30000
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#poe max-power 30000
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 3 Enable overtemperature protection.

```
Raisecom(config)#poe temperature-protection enable
```

Step 4 Enable global Trap.

```
Raisecom(config)#poe pse trap enable
```

Step 5 Configure priorities of GE 1/1/2 and GE 1/1/1 to high and low respectively.

```
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#poe priority high
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#poe priority low
```

Checking results

Use the **show poe interface gigaethernet 1/1/1 detail** and **show interface poe gigaethernet 1/1/2 detail** commands to show PoE configurations on GE 1/1/2 and GE 1/1/1.

```
Raisecom#show poe interface gigaethernet 1/1/1 detail
Port: gigaethernet 1/1/1
-------------------------------------------------
POE administrator status: Enable
POE operation status: Enable
Power detection status:Searching
POE Power Pairs mode:Signal
PD power classification:Class0
POE power Priority:Low
POE power max:30000 (mW)
POE power output:0 (mW)
POE power average:0 (mW)
POE power peak:0 (mW)
POE current output:0 (mA)
POE voltage output:0 (mV)
```


Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#show poe interface gigaethernet 1/1/2 detail
Port: gigaethernet 1/1/1
-----------------------------------------------
POE administrator status: Enable
POE operation status: Enable
Power detection status:Searching
POE Power Pairs mode:Signal
PD power classification:Class0
POE power Priority:High
POE power max:30000 (mW)
POE power output:0 (mW)
POE power average:0 (mW)
POE power peak:0 (mW)
POE current output:0 (mA)
POE voltage output:0 (mW)
```


Copyright © Raisecom Technology Co., Ltd.

5 DHCP

This chapter describes basic principles and configurations procedures of DHCP, and providing related configuration examples, including the following sections:

- DHCP Client
- Zero-configuration
- DHCP Snooping
- DHCP Options
- DHCP Server
- DHCP Relay

5.1 DHCP Client

5.1.1 Introduction

Dynamic Host Configuration Protocol (DHCP) refers to the protocol which assigns configurations, such as the IP address, to users on the TCP/IP network. Based on BOOTP (Bootstrap Protocol) protocol, it has additional features, such as automatically assigning available network addresses, reusing network addresses, and other extended configuration features.

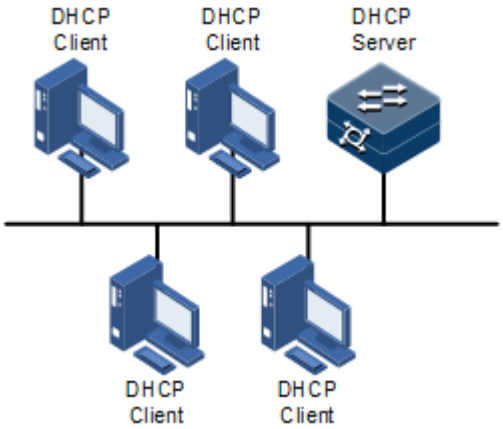
With the enlargement of network scale and development of network complexity, the number of PCs on a network usually exceeds the maximum number of distributable IP addresses. Meanwhile, the widely use of laptops and wireless networks lead to frequent changes of locations and also related IP addresses must be updated frequently. As a result, network configurations become more and more complex. DHCP is developed to solve these problems.

DHCP adopts client/server communication mode. A client applies for configurations to the server (including the IP address, subnet mask, and default gateway), and the server replies with IP address to the client and other related configurations to implement dynamic configurations.

Typical applications of DHCP usually include a set of DHCP server and multiple clients (such as the PC or laptop), as shown in Figure 5-1.

Copyright © Raisecom Technology Co., Ltd.

Figure 5-1 DHCP typical networking



DHCP ensures rational allocation, avoid waste, and improve the utilization rate of IP addresses on the entire network.

Figure 5-2 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 5-2 Structure of DHCP packet

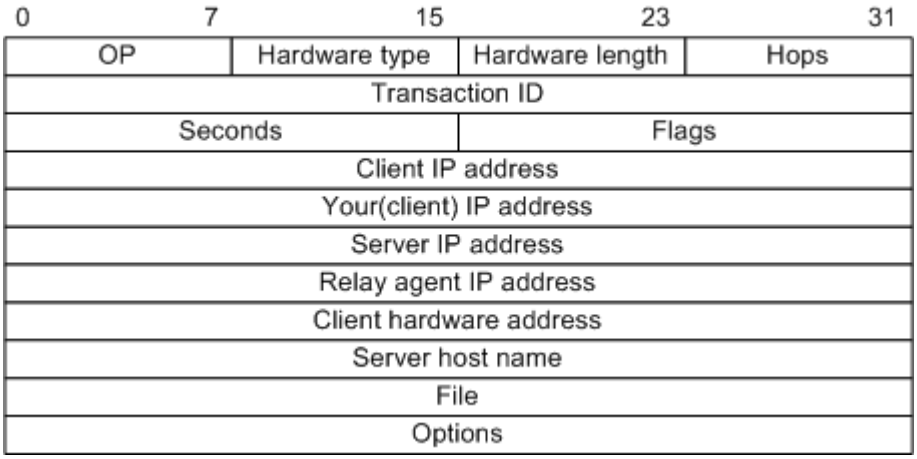


Table 5-1 describes fields of DHCP packets.

Table 5-1 Fields of a DHCP packet

Field	Length	Description
OP	1	Packet type • 1: a request packet • 2: a reply packet
Hardware type	1	Hardware address type of a DHCP client
Hardware length	1	Hardware address size of a DHCP client
Hops	1	Number of DHCP hops passed by a DHCP packet This field increases by 1 every time the DHCP request packet passes a DHCP hop.

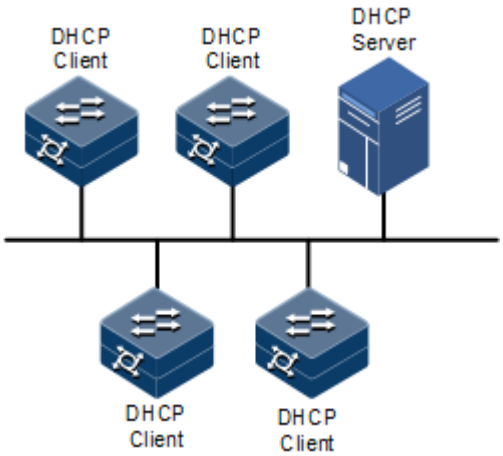
Copyright © Raisecom Technology Co., Ltd.

Field	Length	Description
Transaction ID	4	The client chooses a number at random when starting a request, used to mark process of address request.
Seconds	2	Passing time for the DHCP client after starting DHCP request. It is unused now, fixed as 0.
Flags	2	Bit 1 is the broadcast reply flag, used to mark whether the DHCP server replies packets in unicast or broadcast mode. • 0: unicast • 1: broadcast Other bits are reserved.
Client IP address	4	DHCP client IP address, only filled when the client is in bound, updated or re-bind status, used to reply ARP request.
Your (client) IP address	4	IP address of the client distributed by the DHCP server
Server IP address	4	IP address of the DHCP server
Relay agent IP address	4	IP address of the first DHCP hop after the DHCP client sends request packets.
Client hardware address	16	Hardware address of the DHCP client
Server host name	64	Name of the DHCP server
File	128	Name of the startup configuration file of the DHCP client and path assigned by the DHCP server
Options	Modifiable	A modifiable option field, including packet type, available lease period, IP address of the DNS server, and IP address of the WINS server

The ISCOM2600G series switch can be used as a DHCP client to obtain the IP address from the DHCP server for future management, as shown in Figure 5-3.

Copyright © Raisecom Technology Co., Ltd.

Figure 5-3 DHCP Client networking



5.1.2 Preparing for configurations

Scenario

As a DHCP client, the ISCOM2600G series switch obtains the IP address from the DHCP server.

The IP address assigned by the DHCP client is limited with a certain lease period when adopting dynamic assignment of IP addresses. The DHCP server will take back the IP address when it is expired. The DHCP client has to renew the IP address for continuous use. The DHCP client can release the IP address if it does not want to use the IP address before expiration.

We recommend configuring the number of DHCP relay devices smaller than 4 if the DHCP client needs to obtain IP address from the DHCP server through multiple DHCP relay devices.

Prerequisite

- Create VLANs
- DHCP Snooping is disabled.
- FE 1/0/1 supports obtaining the IP address through DHCP or zero-configuration.

5.1.3 Default configurations of DHCP Client

Default configurations of DHCP Client are as below.

Function	Default value
hostname	Raisecom
class-id	Raisecom-ROS
client-id	Raisecom-SYSMAC-IF0

Copyright © Raisecom Technology Co., Ltd.

5.1.4 Configuring DHCP Client

Before a DHCP client applies for an IP address, you must create a VLAN. Meanwhile you must configure the DHCP server, otherwise the interface will fail to obtain the IP address through DHCP.

Note

- By default, the ISCOM2600G series switch is enabled with DHCP Client. Use the **no ip address dhcp** command to disable DHCP Client.
- If the ISCOM2600G series switch obtains the IP address from the DHCP server through DHCP previously, it will restart the application process for IP address if you use the **ip address dhcp** command to modify the IP address of the DHCP server.

Configure DHCP Client for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface vlan vlan-id`
	Example:
	`Raisecom(config)#interface vlan 1`
		Enter VLAN interface configuration mode.
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094

3	`Raisecom(config-vlan*)#ip dhcp client { class-id class-id | client-id client-id | hostname host-name }`
	Example:
	`Raisecom(config-vlan1)#ip dhcp client hostname myhost`
		(Optional) configure DHCP client information, including the type identifier, client identifier, and host name.
		• host-name: host name, a string of 1 to 64 characters
		• class-id: class-ID, a string of 1 to 64 characters
		• client-id: client-ID, a string of 1 to 64 characters
		Caution
		After the IP address is obtained by a DHCP client, client information cannot be modified.

4	`Raisecom(config-vlan*)#ip address dhcp [ server-ip ip-address ]` `Raisecom(config-vlan1)#ip address dhcp server-ip 10.0.0.1`	Configure the DHCP client to obtain IP address through DHCP. • server-ip: IP address of the specified DHCP server. Only the specified server assigns IP address if the parameter is configured. • ip-address: IP address, in dotted decimal notation, such as 10.0.0.1
5	`Raisecom(config-vlan*)#ip dhcp client renew`	(Optional) renew the IP address. If the Layer 3 interface of the DHCP client has obtained an IP address through DHCP, the IP address will automatically be renewed when the lease period expires.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	`Raisecom(config-vlan*)#no ip address dhcp`	(Optional) release the IP address.

5.1.5 Configuring DHCPv6 Client

Configure the DHCPv6 client for the ISCOM2600 series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface vlan vlan-id`
	Example:
	`Raisecom(config)#interface vlan 1`
		Enter VLAN interface configuration mode.
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094

3	`Raisecom(config-vlan*)#ipv6 address dhcp [ server-ip ipv6-address ]`
	Example:
	`Raisecom(config-vlan1)#ipv6 address dhcp server-ip 2000::3`
		Configure applying for IPv6 address through DHCPv6.
		If the ISCOM2600G series switch has obtained an IP address from the DHCP server through DHCPv6 before, it will restart the application process for the IP address if you use the command to modify the IPv6 address of the DHCP server.
		• server-ip: IP address of the specified DHCP server. Only the specified server assigns IP addresses if the parameter is configured.
		• ipv6-address: ipv6 address, in colon hexadecimal notation, such as 3001::1

4	`Raisecom(config-vlan*)#ipv6 dhcp client renew`	(Optional) renew the IPv6 address. If the Layer 3 interface on the ISCOM2600G series switch has obtained an IP address through DHCP, the IPv6 address will automatically be renewed when the lease period expires.
5	`Raisecom(config-vlan*)#ipv6 dhcp client rapid-commit`	(Optional) enable DHCPv6 Client to apply for rapid interaction.

5.1.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show ip dhcp client [ fastethernet 1/0/1 | vlan vlan-id ]`	Show configurations of DHCP Client.

Copyright © Raisecom Technology Co., Ltd.

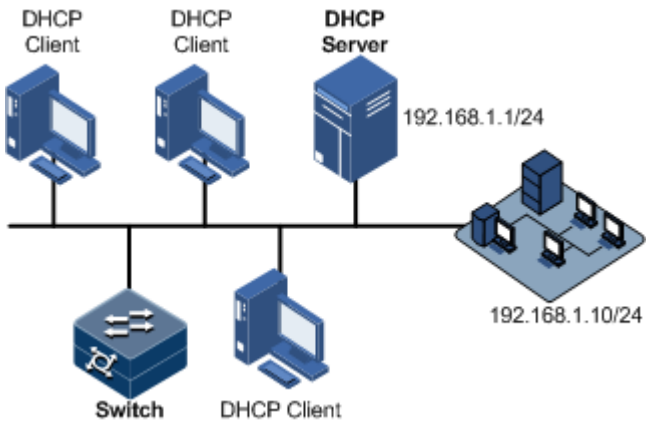
No.	Command	Description
2	`Raisecom#show ipv6 dhcp client [ interface { interface-type interface-number | vlan vlan-id } ]`	Show configurations of DHCPv6 Client.

5.1.7 Example for configuring DHCP Client

Networking requirements

As shown in Figure 5-4, the Switch is used as a DHCP client, and the host name is raisecom. The Switch is connected to the DHCP server and NMS. The DHCP server should assign IP addresses to the SNMP interface on the Switch and make NMS manage the Switch.

Figure 5-4 DHCP Client networking



Configuration steps

Step 1 Configure the DHCP client.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip dhcp client hostname raisecom
```

Step 2 Configure applying for IP address through DHCP.

```
Raisecom(config-vlan1)#ip address dhcp server-ip 192.168.1.1
```

Checking results

Use the **show ip dhcp client** command to show configurations of DHCP Client.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#show ip dhcp client
DHCP Client Mode:             Normal Mode
  Interface :                 vlan1
  Hostname:                   Raisecom
  Class-ID:                   Raisecom-ROS_5.2.1
  Client-ID:                  Raisecom-000e5e112233-IF0
  DHCP Client Is Requesting For A Lease.
  Assigned IP Addr:            0.0.0.0
  Subnet Mask:                0.0.0.0
  Default Gateway:             --
  Client Lease Starts:          Jan-01-1970 08:00:00
  Client Lease Ends:           Jan-01-1970 08:00:00
  Client Lease Duration:        0(sec)
  DHCP Server:                0.0.0.0
  TFTP Server Name:            --
  TFTP Server IP Addr:          --
  Bootfile Filename:           --
  NTP Server IP Addr:          --
  Root Path:                  --

  DHCP Client Mode:            Normal Mode
  Interface :                 vlan10
  Hostname:                   Raisecom
  Class-ID:                   Raisecom-ROS_5.2.1
  Client-ID:                  Raisecom-000e5e112233-IF0
  DHCP Client Is Disabled.
  Assigned IP Addr:            0.0.0.0
  Subnet Mask:                0.0.0.0
  Default Gateway:             --
  Client Lease Starts:          Jan-01-1970 08:00:00
  Client Lease Ends:           Jan-01-1970 08:00:00
  Client Lease Duration:        0(sec)
  DHCP Server:                0.0.0.0
  TFTP Server Name:            --
  TFTP Server IP Addr:          --
  Bootfile Filename:           --
  NTP Server IP Addr:          --
  Root Path:                  --
```

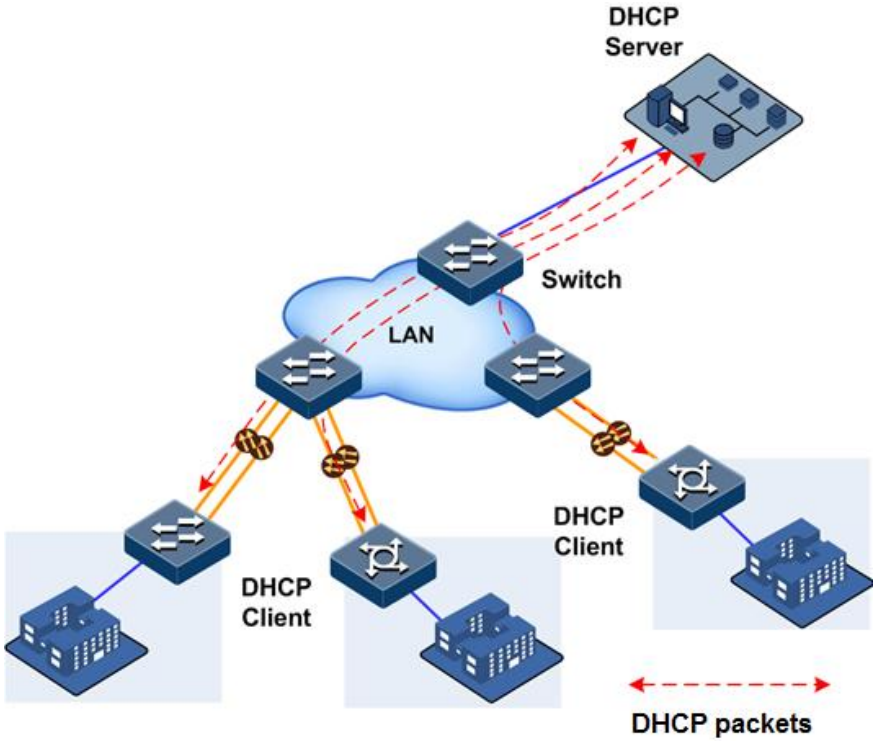
5.2 Zero-configuration

5.2.1 Introduction

Zero-configuration refers to that the device needs no manual configurations; it automatically sends DHCP packets for applying for an IP address to the zero-configuration server, and automatically downloads the configurations file from the zero-configuration server to update its configurations after obtaining the IP address from the zero-configuration server. Figure 5-5 shows zero-configuration server networking.

Copyright © Raisecom Technology Co., Ltd.

Figure 5-5 Zero-configuration server networking



Caution

By default, zero-configuration is enabled on the device. To disable it, configure the device to common client mode.

5.2.2 Default configurations of zero-configuration

Default configurations of zero-configuration are as below.

Function	Default value
Zero-configuration polling period	2h
Zero-configuration mode	Enable

5.2.3 Preparing for configuration

Scenario

To enable the remote device to automatically apply for the IP address after being powered on, configure zero-configuration. To configure zero-configuration parameters, see the following section.

Prerequisite

- Connect the device to the DHCP server correctly. Configure the DHCP server correctly.

Copyright © Raisecom Technology Co., Ltd.

- Configure the interface connected to the zero-configuration server to be Up.
- Configure the upstream switch to allow packets of a VLAN of the remote device to pass.
- Out-of-band interface FE 1/0/1 supports obtaining the IP address through DHCP or zero-configuration.

5.2.4 Configuring DHCP Client

Configure DHCP Client for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#ip dhcp client mode { zeroconfig | normal }`
	Example:
	`Raisecom(config)#ip dhcp client mode normal`
		Configure the DHCP client to work in zero-configuration mode or common client mode.
		By default, it works in zero-configuration mode.
		• zeroconfig: zero-configuation mode
		• normal: normal DHCP client mode
		Caution
		To disable zero-configuration, use the command to configure the DHCP client to common client mode.

5.2.5 (Optional) configuring zero-configuration polling

Configure zero-configuration polling for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#ip dhcp client zeroconfig polling period hour`
	Example:
	`Raisecom(config)#ip dhcp client zeroconfig polling period 3`
		Configure the zero-configuration polling period, in units of hour, ranging from 1 to 24.
		By default, it is 2h.
		• hour: polling period, an integer, ranging from 1 to 24, in units of hour

5.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show ip dhcp client [ fastethernet 1/0/1 | vlan vlan-id ]`	Show configurations and information automatically obtained by the DHCP client.

Copyright © Raisecom Technology Co., Ltd.

5.3 DHCP Snooping

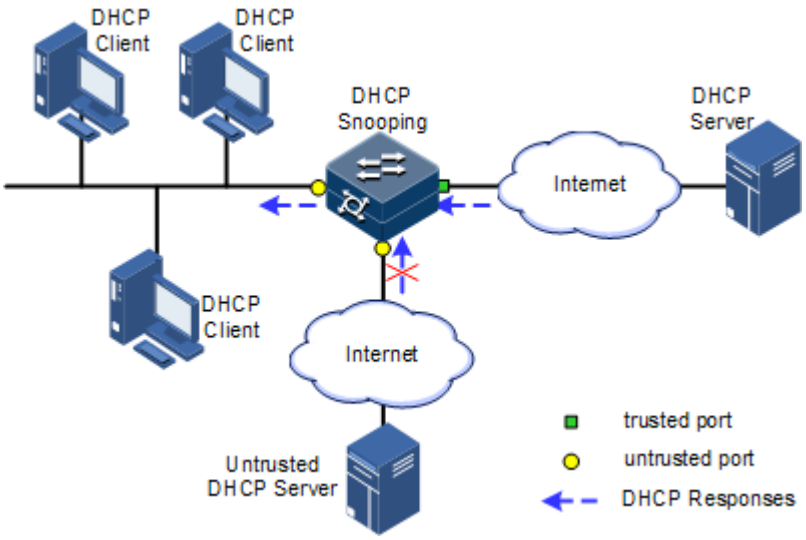
5.3.1 Introduction

DHCP Snooping is a security feature of DHCP with the following functions:

- Make the DHCP client obtain the IP address from a legal DHCP server.

If a false DHCP server exists on the network, the DHCP client may obtain incorrect IP address and network configuration parameters, but cannot communicate normally. As shown in Figure 5-6, to make DHCP client obtain the IP address from a legal DHCP server, the DHCP Snooping security system permits you to configure an interface as the trusted interface or untrusted interface: the trusted interface forwards DHCP packets normally; the untrusted interface discards reply packets from the DHCP server.

Figure 5-6 DHCP Snooping



- Record mapping between DHCP client IP address and MAC address.

DHCP Snooping records entries through monitor request and reply packets received by the trusted interface, including client MAC address, obtained IP address, DHCP client connected interface and VLAN of the interface. Then implement following by the record information:

  - ARP detection: judge legality of a user that sends ARP packet and avoid ARP attack from illegal users.
  - IP Source Guard: filter packets forwarded by interfaces by dynamically getting DHCP Snooping entries to avoid illegal packets to pass the interface.
  - VLAN mapping: modify mapped VLAN of packets sent to users to original VLAN by searching IP address, MAC address, and original VLAN information in DHCP Snooping entry corresponding to the mapped VLAN.

The Option field in DHCP packet records position information of DHCP clients. The Administrator can use this Option filed to locate DHCP clients and control client security and accounting.

If the ISCOM2600G series switch is configured with DHCP Snooping to support Option function:

Copyright © Raisecom Technology Co., Ltd.

- When the ISCOM2600G series switch receives a DHCP request packet, it processes packets according to Option field included or not, filling mode, and processing policy configured by user, then forwards the processed packet to DHCP server.
- When the ISCOM2600G series switch receives a DHCP reply packet, it deletes the Optional field and forwards the rest part of the packet to the DHCP client if the packet contains the Option field, or it forwards the packet directly if the packet does not contain the Option field.

5.3.2 Preparing for configurations

Scenario

DHCP Snooping is a security feature of DHCP, used to make DHCP client obtain its IP address from a legal DHCP server and record mapping between IP address and MAC address of a DHCP client.

The Option field of a DHCP packet records location of a DHCP client. The administrator can locate a DHCP client through the Option field and control client security and accounting. The device configured with DHCP Snooping and Option can perform related process according to Option field status in the packet.

Prerequisite

N/A

5.3.3 Default configurations of DHCP Snooping

Default configurations of DHCP Snooping are as below.

Function	Default value
Global DHCP Snooping status	Disable
Interface DHCP Snooping status	Enable
Interface trusted/untrusted status	Untrust
DHCP Snooping in support of Option 82	Disable

5.3.4 Configuring DHCP Snooping

Generally, you must ensure that the ISCOM2600G series switch interface connected to DHCP server is in trusted status while the interface connected to the user is in untrusted status.

If enabled with DHCP Snooping but without the feature of DHCP Snooping supporting DHCP Option, the ISCOM2600G series switch will do nothing to Option fields in packets. For packets without Option fields, the ISCOM2600G series switch does not conduct the insertion operation.

By default, DHCP Snooping is enabled on all interfaces, but only when global DHCP Snooping is enabled can interface DHCP Snooping take effect.

Configure DHCP Snooping for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip dhcp snooping`	Enable global DHCP Snooping.

3	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

4	`Raisecom(config-gigaethernet1/1/port)#ip dhcp snooping`	(Optional) enable interface DHCP Snooping. The device supports this configuration on the QinQ interface.
5	`Raisecom(config-gigaethernet1/1/port)#ip dhcp snooping trust`	Configure the trusted interface of DHCP Snooping.

6	`Raisecom(config-gigaethernet1/1/port)#ip dhcp snooping binding max number`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#ip dhcp snooping binding max 100`
		Configure the maximum number of entries in the DHCP Snooping binding table.
		• number: maximum number of entries in the DHCP Snooping binding table, an integer, ranging from 1 to 512

7	`Raisecom(config-gigaethernet1/1/port)#ip dhcp snooping outer vlan-id inner vlan-list`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#ip dhcp snooping outer 1 inner 1`
		(Optional) enable DHCP Snooping based on interface or double VLAN Tags.
		• vlan-id: outer VLAN ID, an integer, ranging from 1 to 4094
		• vlan-list: inner VLAN ID, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

8	`Raisecom(config)#ip dhcp snooping option client-id`	(Optional) configure DHCP Snooping to support Option 61 field.

9	`Raisecom(config)#ip dhcp snooping autosave { enable | disable }`
	Example:
	`Raisecom(config)#ip dhcp snooping autosave enable`
		(Optional) enable or disable auto-saving of the DHCP Snooping binding table.
		• enable: enable auto-saving of the DHCP Snooping binding table.
		• disable: disable auto-saving of the DHCP Snooping binding table.

10	`Raisecom(config)#ip dhcp snooping autosave write-interval time`
	Example:
	`Raisecom(config)#ip dhcp snooping autosave write-interval 360`
		(Optional) configure the interval for automatically saving the DHCP Snooping binding table.
		• time: interval for automatically saving the DHCP Snooping binding table, an integer, ranging from 60 to 157680000, in units of second

Copyright © Raisecom Technology Co., Ltd.

5.3.5 Configure DHCP Snooping to support Option 82

Configure DHCP Snooping to support Option 82 for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip dhcp snooping information option`	Configure global DHCP Snooping to support Option 82.

3	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

4	`Raisecom(config-gigaethernet1/1/port)#ip dhcp snooping information option vlan-list vlan-list`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#ip dhcp snooping information option vlan-list 1`
		(Optional) configure the lists of VLANs that support Option 82 through interface DHCP Snooping.
		• vlan-list: VLAN ID, an integer, ranging from 1 to 4094

5.3.6 Configuring DHCPv6 Snooping

Configure DHCPv6 Snooping for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ipv6 dhcp snooping`	Enable global DHCPv6 Snooping.

3	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

4	`Raisecom(config-gigaethernet1/1/port)#ipv6 dhcp snooping`	(Optional) enable interface DHCPv6 Snooping.

5	`Raisecom(config-gigaethernet1/1/port)#ipv6 dhcp snooping trust[ access-list acl-number ]`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#ipv6 dhcp snooping trust`
		Configure the trusted interface of DHCPv6 Snooping.
		• access-list acl-number: ACL number, an integer, ranging from 6000 to 6999

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config-gigaethernet1/1/port)#**ipv6 dhcp snooping vlan** *vlan-id* **Example:** Raisecom(config-gigaethernet1/1/1)#ipv6 dhcp snooping vlan 2	Enable IPv6 DHCP Snooping on the specified interface and in the specified VLAN. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
7	Raisecom(config-gigaethernet1/1/port)#**ipv6 dhcp snooping binding max** *number* **Example:** Raisecom(config-gigaethernet1/1/1)#ipv6 dhcp snooping binding max 100	Configure the maximum number of entries in the DHCPv6 Snooping binding table. • number: maximum number of entries in the DHCP Snooping binding tables, an integer, ranging from 1 to 512
8	Raisecom(config-gigaethernet1/1/port)#**exit** Raisecom(config)#**ipv6 dhcp snooping option** *number* **Example:** Raisecom(config)#ipv6 dhcp snooping option 30	(Optional) configure DHCPv6 Snooping to support user-defined Options. number: ID of user-defined Option supported, an integer, ranging from 1 to 254
9	Raisecom(config)#**ipv6 dhcp snooping option interface-id**	(Optional) configure DHCP Snooping to support Option 18. • interface-id: enable DHCP Snooping to support Option 18.
10	Raisecom(config)#**ipv6 dhcp snooping option remote-id**	(Optional) configure DHCPv6 Snooping to support Option 37. • remote-id: enable DHCP Snooping to support Option 37.

5.3.7 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom#**show ip dhcp snooping**	Show configurations of DHCP Snooping.
2	Raisecom#**show ip dhcp snooping binding**	Show configurations of the DHCP Snooping binding table.
3	Raisecom#**show ipv6 dhcp snooping**	Show configurations of DHCPv6 Snooping.
4	Raisecom#**show ipv6 dhcp snooping binding** [**prefix**]	Show configurations of the DHCPv6 Snooping binding table.
5	Raisecom#**show ip dhcp snooping autosave**	Show auto-saving status of the DHCP Snooping binding table.

Copyright © Raisecom Technology Co., Ltd.

5.3.8 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description

`Raisecom(config)#clear ip dhcp snooping binding [ interface-type interface-number | vlan vlan-id | ip-address ip-address ]`
Example:
`Rasiecom(config)#clear ip dhcp snooping binding`
	Clear information about the IPv4 binding table.
	• interface-type: interface type
	• interface-number: interface ID. The form and value range depend on the interface type.
	• vlan vlan-id: VLAN ID, an integer, ranging from 1 to 4094
	• ip-address ip-address: IP address, in dotted decimal notation, such as 10.10.10.1

`Raisecom(config)#clear ipv6 dhcp snooping binding [ interface-type interface-number | vlan vlan-id | ipv6-address ipv6-address | ipv6-prefix ipv6-address/prefix-length ]`
Example:
`Raisecom(config)#clear ipv6 dhcp snooping binding`
	Clear information about the IPv6 binding table.
	• interface-type: interface type
	• interface-number: interface ID. The form and value range depend on the interface type.
	• vlan vlan-id: VLAN ID, an integer, ranging from 1 to 4094
	• ipv6-address ipv6-address: IPv6 address, in colon hexadecimal notation, such as 3001::1
	• ipv6-prefix ipv6-address/prefix-length: IPv6 address with a prefix, such as 1:123::0:1/96

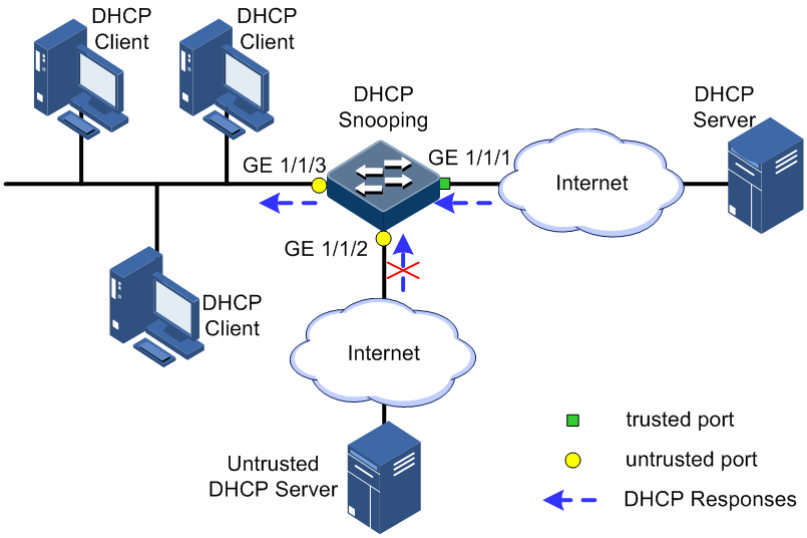
5.3.9 Example for configuring DHCP Snooping

Networking requirements

As shown in Figure 5-7, the Switch is used as the DHCP Snooping device. The network requires DHCP clients to obtain the IP address from a legal DHCP server and support Option 82 to facilitate client management. You can configure padding information of about circuit ID sub-option to raisecom on GE 1/1/3, and padding information about remote ID sub-option to user01.

Copyright © Raisecom Technology Co., Ltd.

Figure 5-7 DHCP Snooping networking



Configuration steps

Step 1 Configure global DHCP Snooping.

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

Step 2 Configure the trusted interface.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#ip dhcp snooping
Raisecom(config-gigaethernet1/1/1)#ip dhcp snooping trust
Raisecom(config-gigaethernet1/1/1)#quit
```

Step 3 Configure DHCP Relay to support Option 82 field and configure Option 82 field.

```
Raisecom(config)#ip dhcp snooping information option
Raisecom(config)#ip dhcp information option remote-id string user01
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#ip dhcp information option circuit-id
raisecom
```

Checking results

Use the **show ip dhcp snooping** command to show configurations of DHCP Snooping.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#show ip dhcp snooping
DHCP Snooping: Enabled
DHCP Option 82: Enabled
Port                        vlan         Enabled Status  Trusted Status
Option82 Vlanlist
-------------------------------------------------------------------------
------------------------
gigaethernet1/1/1             --           enabled       yes           1-
4094
gigaethernet1/1/2             --           enabled       no            1-
4094
gigaethernet1/1/3             --           enabled       no            1-
4094
gigaethernet1/1/4             --           enabled       no            1-
4094
gigaethernet1/1/5             --           enabled       no            1-
4094
gigaethernet1/1/6             --           enabled       no            1-
4094
……
```

5.4 DHCP Options

5.4.1 Introduction

DHCP transmits control information and network configuration parameters through Option field in packet to dynamically assign addresses to provide abundant network configurations for clients. DHCP has 255 types of options, with the final option as Option 255. Table 5-2 lists frequently used DHCP options.

Table 5-2 Common DHCP options

Options	Description
3	Router option, used to assign the gateway address of DHCP clients
6	DNS server option, used to specify the IP address of the DNS server assigned for DHCP clients
18	IPv6 DHCP client flag option, used to specify interface information about DHCP clients
37	IPv6 DHCP client flag option, used to specify device information about DHCP clients
51	IP address lease option
53	DHCP packet type option, used to mark the type of DHCP packets
55	Request parameter list option, used to indicate network configuration parameters to be obtained from the server, containing values of these parameters

Copyright © Raisecom Technology Co., Ltd.

Options	Description
61	DHCP client flag option, used to assign device information for DHCP clients
66	TFTP server name option, used to specify the domain name of the TFTP server assigned for DHCP clients
67	Startup file name option, used to specify the name of the startup file assigned for DHCP clients
82	DHCP client flag option, user-defined, used to mark the position of DHCP clients, including Circuit ID and remote ID
150	TFTP server address option, used to specify the IP address of the TFTP server assigned for DHCP clients
184	DHCP reserved option. At present Option 184 is used to carry information required by voice calling. Through Option 184, the DHCP server can distribute IP addresses for DHCP clients with voice function and meanwhile provide information about voice calling.
255	Complete option

Options 18, 37, 61, and 82 in DHCP Option are relay information options in DHCP packets. When a DHCP client sends request packets to the DHCP server by passing a DHCP Relay or DHCP Snooping device, the DHCP Relay or DHCP Snooping device will add Option fields to the request packets.

Options 18, 37, 61, and 82 implement recording of information about DHCP clients on the DHCP server. By cooperating with other software, it can implement functions, such as limit on IP address distribution and accounting. For example, by cooperating with IP Source Guard, Options 18, 61, 82 can defend deceiving through IP address+MAC address.

Option 82 can include up to 255 sub-options. If the Option 82 field is defined, at least one sub-option must be defined. The ISCOM2600G series switch supports the following two sub-options:

- Sub-Option 1 (Circuit ID): it contains the interface ID, interface VLAN, and additional information about request packets of the DHCP client.
- Sub-Option 2 (Remote ID): it contains interface MAC address (DHCP Relay), or bridge MAC address (DHCP Snooping device) of the ISCOM2600G series switch, or user-defined string in request packets of the DHCP client.

5.4.2 Preparing for configurations

Scenario

Options 18, 37, 61, and 82 in DHCP Option are relay information options in DHCP packets. When request packets from DHCP clients reach the DHCP server, DHCP Relay or DHCP Snooping added Option field into request packets if request packets pass the DHCP relay device or DHCP snooping device is required.

Options 18, 37, 61, and 82 are used to record DHCP client information on the DHCP server. By cooperating with other software, it can implement functions such as limit on IP address distribution and accounting.

Copyright © Raisecom Technology Co., Ltd.

Prerequisite

N/A

5.4.3 Default configurations of DHCP Option

Default configurations of DHCP Option are as below.

Function	Default value
attach-string in global configuration mode	N/A
remote-id in global configuration mode	Switch-mac
circuit-id in interface configuration mode	N/A

5.4.4 Configuring DHCP Option field

Configure DHCP Option field for the ISCOM2600G series switch as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#ip dhcp information option attach-string attach-string`
	Example:
	`Raisecom(config)#ip dhcp information option attach-string raisecom`
		(Optional) configure additional information for Option 82 field.
		• attach-string: attached string, a string of 1 to 32 characters

	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

	`Raisecom(config-gigaethernet1/1/port)#ip dhcp information option circuit-id circuit-id [ prefix-mode ]`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#ip dhcp information option circuit-id 10`
		(Optional) configure circuit ID sub-option information for Option 82 field on the interface.
		• circuit-id: circuit ID, a string of 1 to 64 characters
		• prefix-mode: prefix mode

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	`Raisecom(config-gigaethernet1/1/port)#`**`ip dhcp option vlan`** *`vlan-id`* **`description`** *`string`* `Raisecom(config-gigaethernet1/1/port)#`**`exit`** **`Example:`** `Raisecom(config-gigaethernet1/1/1)#ip dhcp option vlan 10 description raisecom`	(Optional) configure the interface or VLAN description to be padded into Option 82 fields. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • string: description of the interface and VLAN, a string up to 64 characters.
	`Raisecom(config)#`**`ip dhcp information option attach-string`** *`attach-string`* **`Example:`** `Raisecom(config)#ip dhcp information option attach-string raisecom`	(Optional) configure the attached string in Option 82 of DHCP packets. • attach-string: attached string, a string of 1 to 32 characters

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

	`Raisecom(config)#ip dhcp information option circuit-id { mac-format | format | hex } string`
	Example:
	`Raisecom(config)#ip dhcp information option circuit-id mac-format hhhh.hhhh.hhhh`
		(Optional) configure the format for padding the sub-option in the Circuit ID in Option 82 of DHCP packets.
		• mac-format string: MAC address format, a string, supporting the following types:
		– hhhhhhhhhhhh
		– hhhh.hhhh.hhhh
		– hhhh-hhhh-hhhh
		– hhhh:hhhh:hhhh
		– hh.hh.hh.hh.hh.hh
		– hh-hh-hh-hh-hh-hh
		– hh:hh:hh:hh:hh:hh
		• format string: string format:
		– %h: HostName
		– %s: Slot
		– %v: SVLAN
		– %c: CVLAN
		– %p: Port
		– %m: Local MAC
		– %r: Remote MAC
		– %i: IP Address
		– %u: Unit
		– %d: Port-Description
		– %bd: Bussiness-Description
		• hex string: hexadecimal string:
		– %h: HostName
		– %s: Slot
		– %v: SVLAN
		– %c: CVLAN
		– %p: Port
		– %m: Local MAC
		– %r: Remote MAC
		– %i: IP Address
		– %u: Unit
		– %d: Port-Description
		– %bd: Bussiness-Description

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config)#**ip dhcp information option remote-id** { **client-mac** | **client-mac-string** | **hostname** | **string** *string* | **switch-mac** | **switch-mac-string** } Raisecom(config)#**ip dhcp information option remote-id extend** { **client-mac** | **client-mac-string** | **switch-mac** | **switch-mac-string** } **Example:** Raisecom(config)#ip dhcp information option remote-id switch-mac-string	(Optional) configure remote ID sub-option information for Option 82 field. DHCP Relay supports the Remote ID of Option 82 to be compatible with the Huawei Default mode. • client-mac: the remote ID is the MAC address of the user device, sent in binary form. • client-mac-string: the remote ID is the MAC address of the user device, sent in form of a string of characters. • hostname: the remote ID is the host name, sent in form of a string of characters. • string: value of the user-defined remote ID, with the length no more than 64 bytes: – %h: HostName – %s: Slot – %v: SVLAN – %c: CVLAN – %p: Port – %m: Local MAC – %r: Remote MAC – %i: IP Address – %u: Unit – %d: Port-Description – %bd: Bussiness-Description • switch-mac: the remote ID is the MAC address of the device, sent in binary form. • switch-mac-string: the remote ID is the MAC address of the device, sent in form of a string of characters. • extend: extended format, compatible with Huawei default mode
3	Raisecom(config)#**ipv4 dhcp option** *option-id* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* } **Example:** Raisecom(config)#ipv4 dhcp option 100 ip-address 10.0.0.1	(Optional) create user-defined Option based on IPv4. • option-id: relay agent option, an integer, ranging from 1 to 254 • ascii-string: a string, in units of byte, sent in form of ASCII code • hex-string: a string, sent in form of hexadecimal code. The device will add 0 to the header of the character string if the bytes of the character string are odd numbered. • ip-address: in dotted decimal notation, sent in form of IP address

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
	Raisecom(config-gigaethernet1/1/port)#**ipv4 dhcp option** *option-id* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* } **Example:** Raisecom(config-gigaethernet1/1/1)#ipv4 dhcp option 100 ip-address 10.0.0.1	(Optional) create user-defined Option field information on the interface. • option-id: relay agent option, an integer, ranging from 1 to 254 • ascii-string: a string, in units of byte, sent in form of ASCII code • hex-string: a string, sent in form of hexadecimal code. The device will add 0 to the header of the character string if the bytes of the character string are odd numbered. • ip-address: in dotted decimal notation, sent in form of IP address
4	Raisecom(config-gigaethernet1/1/port)#**exit** Raisecom(config)#**ipv4 dhcp option client-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* } **Example:** Raisecom(config)#ipv4 dhcp option client-id ip-address 10.0.0.1	(Optional) configure Option 61 field information. • ascii-string: a string, in units of byte, sent in form of ASCII code • hex-string: a string, sent in form of hexadecimal code • ip-address: in dotted decimal notation, sent in form of IP address
	Raisecom(config-gigaethernet1/1/port)#**ipv4 dhcp option client-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* } **Example:** Raisecom(config-gigaethernet1/1/1)#ipv4 dhcp option client-id ip-address 10.0.0.1	(Optional) configure Option61 field information on the interface. • ascii-string: a string, in units of byte, sent in form of ASCII code • hex-string: a string, sent in form of hexadecimal code • ip-address: in dotted decimal notation, sent in form of IP address

5.4.5 Configuring DHCP Option 18 over IPv6

Configure DHCP Option 18 over IPv6 for the ISCOM2600G series switch as below.

Option 18 over IPv6 should be configured on the device that is enabled with DHCP Snooping.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**ipv6 dhcp option interface-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ipv6-address* } **Example:** Raisecom(config)#ipv6 dhcp option interface-id ascii raisecom	(Optional) configure information about Option 18. • ascii-string: a string, in units of byte, sent in form of ASCII code • hex-string: a string, sent in form of hexadecimal code • ipv6-address: in colon hexadecimal notation, sent in form of IP address
3	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
	Raisecom(config-gigaethernet1/1/port)#**ipv6 dhcp option interface-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ipv6-address* } **Example:** Raisecom(config-gigaethernet1/1/1)#ipv6 dhcp option interface-id ascii raisecom	(Optional) configure information about Option 18 on the interface. • ascii-string: a string, in units of byte, sent in form of ASCII code • hex-string: a string, sent in form of hexadecimal code • ipv6-address: in colon hexadecimal notation, sent in form of IP address

5.4.6 Configuring DHCP Option 37 over IPv6

Configure DHCP Option 37 over IPv6 for the ISCOM2600G series switch as below.

Option 37 over IPv6 should be configured on the device that is enabled with DHCP Snooping.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#ipv6 dhcp option remote-id { ascii | hex } string`
	Example:
	`Raisecom(config)#ipv6 dhcp option remote-id ascii raisecom`
		(Optional) configure information about Option 37.
		• ascii: a string of characters
		• hex: in hexadecimal notation
		• string: value of the user-defined remote ID, with the length no more than 64 bytes:
		– %h: HostName
		– %s: Slot
		– %v: SVLAN
		– %c: CVLAN
		– %p: Port
		– %m: Local MAC
		– %r: Remote MAC
		– %i: IP Address
		– %u: Unit
		– %d: Port-Description
		– %bd: Bussiness-Description

3	`Raisecom(config)#ipv6 dhcp option remote-id mac-format string`
	Example:
	`Raisecom(config)#ipv6 dhcp option remote-id mac-format hhhh.hhhh.hhhh`
		(Optional) configure the format of the MAC address of the Remote ID variable in Option 37 in DHCPv6 packets.
		• string: MAC address format, a string, supporting the following types:
		– hhhhhhhhhhhh
		– hhhh.hhhh.hhhh
		– hhhh-hhhh-hhhh
		– hhhh:hhhh:hhhh
		– hh.hh.hh.hh.hh.hh
		– hh-hh-hh-hh-hh-hh
		– hh:hh:hh:hh:hh:hh

5.4.7 Configuring user-defined DHCP Option over IPv6

Configure user-defined DHCP Option over IPv6 for the ISCOM2600G series switch as below.

User-defined Option over IPv6 should be configured on the device that is enabled with DHCP Snooping.

All the following steps are optional and in any sequence.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**ipv6 dhcp option** *number* { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ipv6-address* } **Example:** Raisecom(config)#ipv6 dhcp option 10 ascii raisecom	(Optional) create user-defined Option information over IPv6. • number: relay agent option, an integer, ranging from 1 to 254. Specify the number which supports self-defined Option. • ascii-string: a string, in units of byte, sent in form of ASCII code • hex-string: a string, sent in form of hexadecimal code • ipv6-address: in colon hexadecimal notation, sent in form of IP address
3	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
	Raisecom(config-gigaethernet1/1/port)#**ipv6 dhcp option** *number* { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ipv6-address* } **Example:** Raisecom(config-gigaethernet1/1/1)#ipv6 dhcp option 10 ascii raisecom	(Optional) create user-defined Option information over IPv6 on the interface. • number: relay agent option, an integer, ranging from 1 to 254. Specify the number which supports self-defined Option. • ascii-string: a string, in units of byte, sent in form of ASCII code • hex-string: a string, sent in form of hexadecimal code • ipv6-address: in colon hexadecimal notation, sent in form of IP address

5.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show ip dhcp information option**	Show configurations of DHCP Option fields.
2	Raisecom#**show ip dhcp option port vlan description**	Show the interface or VLAN description to be padded into Option 82 fields.

Copyright © Raisecom Technology Co., Ltd.

5.5 DHCP Server

5.5.1 Introduction

Dynamic Host Configuration Protocol (DHCP) refers to assigning IP address configurations dynamically for users on the TCP/IP network. It is based on BOOTP (Bootstrap Protocol) protocol, and automatically adds the specified available network address, network address re-use, and other extended configuration options over BOOTP protocol.

With the enlargement of network scale and development of network complexity, the number of PCs on a network usually exceeds the maximum number of distributable IP addresses. Meanwhile, the widely use of laptops and wireless networks lead to frequent change of PC positions and also related IP addresses must be updated frequently. As a result, network configurations become more and more complex. DHCP is developed to solve these problems.

DHCP adopts client/server communication mode. A client applies configuration to the server (including IP address, subnet mask, and default gateway), and the server replies with an IP address for the client and other related configurations to implement dynamic configurations of IP address.

In DHCP Client/Server communication mode, a specific host is configured to assign IP addresses, and send network configurations to related hosts. The host is called the DHCP server.

DHCP application

Under normal circumstances, use the DHCP server to assign IP addresses in following situations:

- The network scale is large. It requires much workload for manual configurations, and is difficult to manage the entire network intensively.
- The number of hosts on the network is greater than that of IP addresses, which makes it unable to assign a fixed IP address for each host and restricts the number of users connected to network simultaneously.
- Only the minority of hosts on the network need fixed IP addresses, most of hosts have no requirement for fixed IP address.

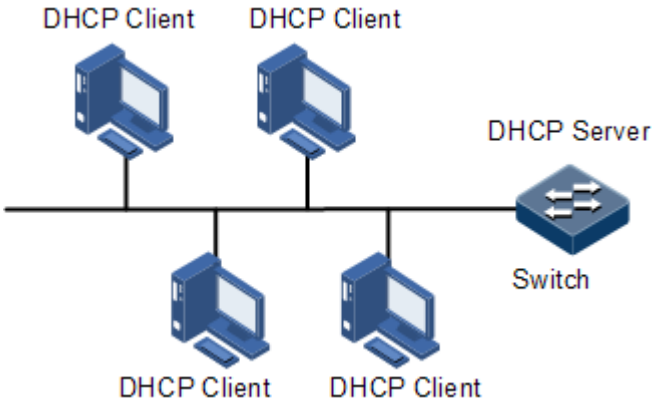
After a DHCP client obtains the IP address from the DHCP server, it cannot use the IP address permanently but in a fixed period, which is called the lease period. You can specify the duration of the lease period.

DHCP ensures rational allocation, avoids waste of IP addresses, and improves the utilization rate of IP addresses on the entire network.

The ISCOM2600G series switch, as the DHCP server, assigns dynamic IP addresses to clients, as shown in Figure 5-8.

Copyright © Raisecom Technology Co., Ltd.

Figure 5-8 DHCP Server and Client networking



DHCP packets

Figure 5-9 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 5-9 Structure of a DHCP packet

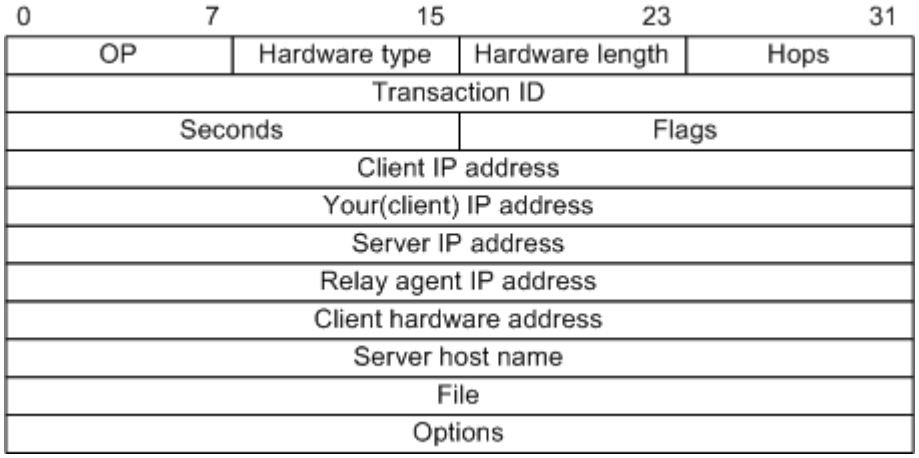


Table 5-3 describes fields of a DHCP packet.

Table 5-3 Fields of a DHCP packet

Field	Length	Description
OP	1	Packet type • 1: a request packet • 2: a reply packet
Hardware type	1	Hardware address type of a DHCP client
Hardware length	1	Hardware address length of a DHCP client
Hops	1	Number of DHCP hops passing by the DHCP packet This field increases 1 every time the DHCP request packet passes a DHCP relay.

Copyright © Raisecom Technology Co., Ltd.

Field	Length	Description
Transaction ID	4	A random number selected by the client to initiate a request, used to identify an address request process
Seconds	2	Duration after the DHCP request for the DHCP client, fixed to 0, being idle currently
Flags	2	Bit 1 is the broadcast reply flag, used to mark that the DHCP server response packet is transmitted in unicast or broadcast mode. • 0: unicast • 1: broadcast Other bits are reserved.
Client IP address	4	IP address of the DHCP client, only filled when the client is in bound, updated or re-bound status, used to respond to ARP request
Your (client) IP address	4	IP address of the DHCP client assigned by the DHCP server
Server IP address	4	IP address of the DHCP server
Relay agent IP address	4	IP address of the first DHCP relay passing by the request packet sent by the DHCP client
Client hardware address	16	Hardware address of the DHCP client
Server host name	64	Name of the DHCP server
File	128	Startup configuration file name and path assigned by the DHCP server to the DHCP client
Options	Modifiable	A modifiable option field, including packet type, available lease period, IP address of the DNS server, IP address of the WINS

5.5.2 Preparing for configurations

Scenario

When working as the DHCPv4 server, the ISCOM2600G series switch can assign IP addresses to DHCPv4 clients.

Prerequisite

- Disable DHCPv4 Client on the ISCOM2600G series switch.
- The DHCP server is a common one.

Copyright © Raisecom Technology Co., Ltd.

5.5.3 Creating and configuring IPv4 address pool

Configure the IPv4 address pool for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#ip dhcp server pool pool-name`
	Example:
	`Raisecom(config)#ip dhcp server pool pool`
		Create an IPv4 address pool, and enter address pool configuration mode.
		• pool-name: IP address pool, a string of 1 to 16 characters

3	`Raisecom(config-pool)#address start-ip-address end-ip-address mask { mask | mask-length }`
	Example:
	`Raisecom(config-pool)#address 172.31.0.1 172.31.0.10 mask 255.255.255.0`
		Configure the range of IP addresses in the IPv4 address pool. The mask length ranges from 1 to 30.
		• start-ip-address: start IP address of address pool, in dotted decimal notation, such as 10.10.10.1
		• end-ip-address: end IP address of address pool, in dotted decimal notation, such as 10.10.10.1
		• mask: mask of IP address, in dotted decimal notation, such as 255.0.0.0
		• mask-length: mask length of IP address, 16-bit mask is supported, an integer, ranging from 1 to 30

4	`Raisecom(config-pool)#excluded-ip-address start-ip-address [ end-ip-address ]`
	Example:
	`Raisecom(config-pool)#excluded-ip-address 172.31.0.2`
		Configure the range of excluded IP addresses in the IPv4 address pool.
		• start-ip-address: start IP address of address pool, in dotted decimal notation, such as 10.10.10.1
		• end-ip-address: end IP address of address pool, in dotted decimal notation, such as 10.10.10.1

5	`Raisecom(config-pool)#lease expired { minute | infinite }`
	Example:
	`Raisecom(config-pool)#lease expired 600`
		Configure the lease period for the IPv4 address pool.
		• minute: lease time, an integer, ranging from 30 to 10080, in units of minute
		• infinite: infinite lease time

6	`Raisecom(config-pool)#dns-server ip-address [ secondary ]`
	Example:
	`Raisecom(config-pool)#dns-server 192.168.100.1`
		Configure the DNS server address of the IPv4 address pool.
		• ip-address: IPv4 address. The ip-address is in dotted decimal notation, such as 10.10.10.1.
		• secondary: specify the IP address of the backup DNS server.

7	`Raisecom(config-pool)#gateway ip-address`
	Example:
	`Raisecom(config-pool)#gateway 192.168.1.1`
		Configure the default gateway of the IPv4 address pool.
		• ip-address: IP address, in dotted decimal notation, such as 10.10.10.1

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
8	`Raisecom(config-pool)#`**`option 60`** *`string`* **Example:** `Raisecom(config-pool)#option 60 Raisecom001`	Configure information carried by Option 60. • string: Option 60 value, a string of 1 to 16 characters
9	`Raisecom(config-pool)#`**`option 43 [ sub-option`** *`option-code`* **`] { ascii`** *`ascii-string`* **`| hex`** *`hex-string`* **`}`** **Example:** `Raisecom(config-pool)#option 43 ascii raisecom`	Configure information carried by Option 43. • sub-option option-code: sub-field of Option 43, an integer, ranging from 1 to 254 **Note** • If there is no configured sub-option, the default sub-option is 0. • There is no conflict from 1 to 254; namely, there can be multiple sub-options (except sub-option 0). • If commands without sub-option are configured, configuring command with sub-option from 1 to 254 will cause the previous configuration to be deleted. • ascii ascii-string: sent in ASCII. The ascii-string is a string of characters. • hex hex-string: sent in hexadecimal notation. The hex-string is a string of characters.
10	`Raisecom(config-pool)#`**`tftp-server`** *`ip-address`* **Example:** `Raisecom(config-pool)#tftp-server 192.168.1.201`	Configure the TFTP server of the IPv4 address pool. • ip-address: IP address, in dotted decimal notation, such as 10.10.10.1
11	`Raisecom(config-pool)#`**`trap server-ip`** *`ip-address`* **Example:** `Raisecom(config-pool)#trap server-ip 192.168.1.201`	Configure the Trap server of the IPv4 address pool. ip-address: IP address, in dotted decimal notation, such as 10.10.10.1

5.5.4 Enabling DHCP Server on VLAN interface

Only when global DHCP Server and Layer 3 interface DHCP Server are enabled can the Layer 3 interface receive and process DHCP request packets from clients.

Enable DHCPv6 Server on the VLAN interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#interface vlan vlan-id`
	Example:
	`Raisecom(config)#interface vlan 1`
		Enter VLAN interface configuration mode.
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094

3	`Raisecom(config-vlan*)#ip dhcp server`	Enable DHCP Server on the VLAN interface.

5.5.5 (Optional) recycling IP address or adress pool

Recycle the IP address or adress pool for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#ip dhcp address ip-address release`
	`Raisecom(config)#ip dhcp address release [ pool pool-name ]`
	Example:
	`Raisecom(config)#ip dhcp address 192.168.1.1 release`
		Configure DHCP Server to support Option 82.
		• ip-address: IP address to be recycled, in dotted decimal notation, such as 10.0.0.1
		• pool-name: IP address pool to be recycled, a string of 1 to 16 characters

5.5.6 Configuring DHCP Server to support Option 82

Configure DHCP Server to support Option 82 for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip dhcp server information option`	Configure DHCP Server to support Option 82.

5.5.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom(config)#show ip dhcp server`	Show configurations of DHCP Server.
2	`Raisecom(config)#show ip dhcp server lease`	Show assigned IPv4 addresses and clients information.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
3	`Raisecom(config)#show ip dhcp server statistics`	Show packet statistics on the DHCPv4 Server.
4	`Raisecom(config)#show ip dhcp static-bind`	Show information about DHCPv4 static binding.
5	`Raisecom(config)#show ip server pool [ excluded-ip-address ] [ statistics ] [ pool-name ]`	Show configurations of the address pool of DHCPv4 Server.

5.5.8 Maintenance

Maintain the ISCOM2600G series switch as below.

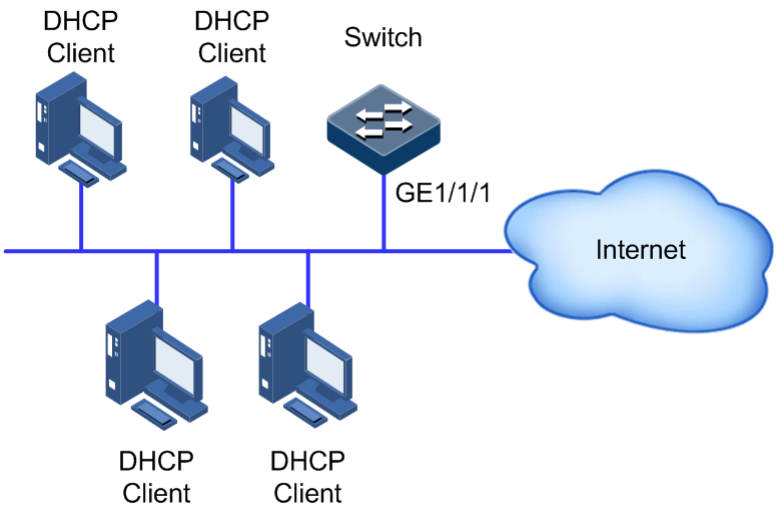
Command	Description
`Rasiecom(config)#clear ip dhcp server statistics`	Clear statistics on DHCP Server.

5.5.9 Example for configuring DHCPv4 Server

Networking requirements

As shown in Figure 5-10, the switch as a DHCP server assigns IP addresses to DHCP clients. The lease period is 8h. The name of the IP address pool is pool. The range of IP addresses is 172.31.1.2–172.31.1.100. The IP address of the DNS server is 172.31.100.1.

Figure 5-10 DHCP Server networking



Configuration steps

Step 1 Create an IP address pool, and configure it.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#config
Raisecom(config)#ip dhcp server pool pool
Raisecom(config-pool)#address 172.31.1.2 172.31.1.100 mask 24
Raisecom(config-pool)#lease expired 480
Raisecom(config-pool)#dns-server 172.31.100.1
Raisecom(config-pool)#exit
```

Step 2 Configure interface DHCP Server.

```
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 172.31.1.1 255.255.255.0
Raisecom(config-vlan1)#ip dhcp server
```

Checking results

Use the **show ip dhcp server** command to show configurations of DHCP Server.

```
Raisecom#show ip dhcp server
Interface                 Status
------------------------------------
vlan 1                   Enable
```

Use the **show ip server pool** command to show configurations of the address pool of the DHCP server.

```
Raisecom#show ip server pool
Pool Name          :      pool
pool type          :      DHCP
Address Range       :      172.31.1.2~172.31.1.100
Address Mask        :      255.255.255.0
Gateway            :      0.0.0.0
DNS Server         :      172.31.100.1
Secondary DNS       :      0.0.0.0
Tftp Server        :      0.0.0.0
Lease time         :      480  minutes
Trap Server        :      0.0.0.0
interface          :      vlan1
option60           :
```


Copyright © Raisecom Technology Co., Ltd.

5.6 DHCP Relay

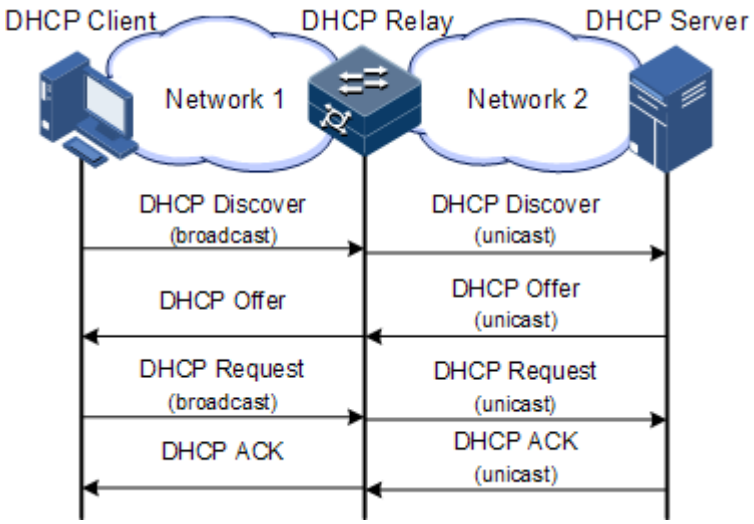
5.6.1 Introduction

At the beginning, DHCP requires the DHCP server and clients to be in the same segment, instead of different segments. As a result, a DHCP server is configured for all segments for dynamic host configuration, which is not economic.

DHCP Relay is introduced to solve this problem. It can provide relay service between DHCP clients and the DHCP server that are in different segments. It relays packets across segments to the DHCP server or clients.

Figure 5-11 shows typical application of DHCP Relay.

Figure 5-11 Typical application of DHCP Relay



When a DHCP client sends a request packet to the DHCP server through a DHCP relay, the DHCP relay processes the request packet and sends it to the DHCP server in the specified segment. The DHCP server sends required information to the DHCP client through the DHCP relay according to the request packet, thus implementing dynamic configuration of the DHCP client.

5.6.2 Preparing for configurations

Scenario

When DHCP Client and DHCP Server are not in the same segment, you can use DHCP Relay function to make DHCP Client and DHCP Server in different segments carry relay service, and relay DHCP protocol packets across segment to destination DHCP server, so that DHCP Client in different segments can share the same DHCP server.

Prerequisite

N/A

Copyright © Raisecom Technology Co., Ltd.

5.6.3 Default configurations of DHCP Relay

Default configurations of DHCP Relay are as below.

Function	Default value
Global DHCP Relay	Disable
Interface DHCP Relay	Disable

5.6.4 Configuring global DHCP Relay

Configure global DHCP Relay for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip dhcp relay`	Enable global DHCP Relay.

5.6.5 Configuring DHCP Relay on VLAN interface

Configure DHCP Relay on the VLAN interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface vlan` *`vlan-id`* **Example:** `Raisecom(config)#interface vlan 1`	Enter VLAN interface configuration mode. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
3	`Raisecom(config-vlan*)#ip dhcp relay`	Enable DHCP Relay on the VLAN interface.
4	`Raisecom(config-vlan*)#ip dhcp relay target-ip` *`ip-address`* **Example:** `Raisecom(config-vlan1)#ip dhcp relay target-ip 192.168.12.34`	Configure the destination IP address for forwarding packets. • ip-address: destination IP address, in dotted decimal notation

5.6.6 Configuring global DHCPv6 Relay

Configure global DHCPv6 Relay for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ipv6 dhcp relay`	Enable global DHCPv6 Relay.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**ipv6 dhcp relay option interface-id**	Enable DHCPv6 Relay to support Option 18.
4	Raisecom(config)#**ipv6 dhcp relay option remote-id**	Enable DHCPv6 Relay to support Option 37.

5.6.7 Configuring DHCPv6 Relay on VLAN interface

Configure DHCPv6 Relay on the VLAN interface for forwarding packets for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface vlan** *vlan-id* **Example:** Raisecom(config)#interface vlan 1	Enter VLAN interface configuration mode. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlan*)#**ipv6 dhcp relay**	Enable DHCPv6 Relay on the VLAN interface.
4	Raisecom(config-vlan*)#**ipv6 dhcp relay target-ip** *ipv6-address* [**vlan** *vlan-id*] **Example:** Raisecom(config-vlan1)#ipv6 dhcp relay target-ip 3001::1	Configure the destination IPv6 address for forwarding packets. • ipv6-address: IPv6 address, in colon hexadecimal notation • vlan-id: VLAN ID, an integer, ranging from 1 to 4094

5.6.8 (Optional) configuring DHCP Relay to support Option 82

Configure DHCP Relay to support Option 82 for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp relay information option**	Configure DHCP Relay to support Option 82. DHCP Relay supports the Remote ID of Option 82 and is compatible with Huawei Default mode.
3	Raisecom(config)#**ip dhcp relay information policy** { **drop** | **keep** | **replace** } **Example:** Raisecom(config)#ip dhcp relay information policy keep	Configure the policy for DHCP Relay to process Option 82 request packets. • drop: discard Option 82 packets. • keep: directly forward Option 82 packets. • replace: replace the Option 82 field and then transmit the packet.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

4	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or VLAN interface configuration mode. Take physical interface configuration mode for example .
		• interface-type: interface type
		• interface-number: interface ID

5	`Raisecom(config-gigaethernet1/1/port)#ip dhcp relay information trusted`	Configure the trusted interface of DHCP Relay.

5.6.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show ip dhcp relay`	Show configurations of DHCP Relay.
2	`Raisecom#show ip dhcp relay binding`	Show binding information about DHCP Relay.
3	`Raisecom#show ip dhcp relay information`	Show information about Option 82 supported by DHCP Relay.
4	`Raisecom#show ip dhcp relay statistics`	Show static information about DHCP Relay.
5	`Raisecom#show ipv6 dhcp relay`	Show configurations of DHCPv6 Relay.

5.6.10 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
`Rasiecom#clear ip dhcp relay statistics`	Clear statistics on DHCP Relay.

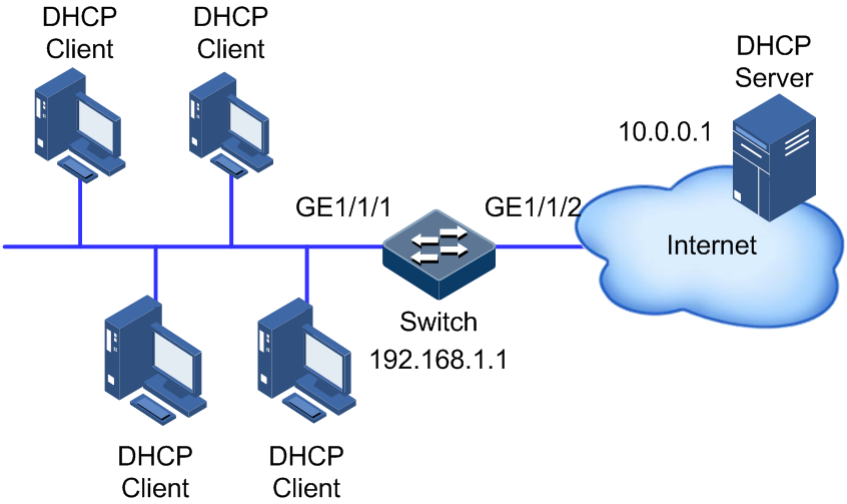
5.6.11 Example for configuring DHCPv4 Relay

Networking requirements

As shown in Figure 5-12, the switch works as the DHCP relay device. The host name is raisecom. The switch is connected to the DHCP server through a service interface. The DHCP server assigns IP addresses to clients so that the NMS can discover and manage these clients.

Copyright © Raisecom Technology Co., Ltd.

Figure 5-12 DHCP Relay networking



Configuration steps

Step 1 Enable global DHCP Relay.

```
Raisecom#config
Raisecom(config)#ip dhcp relay
Raisecom(config)#create vlan 2,3 active
Raisecom(config)#interface vlan 2
Raisecom(config-vlan2)#ip dhcp relay relay-ip 192.168.1.1
Raisecom(config-vlan2)#exit
Raisecom(config)#interface vlan 3
Raisecom(config-vlan3)#ip dhcp relay relay-ip 192.168.1.1
Raisecom(config-vlan3)#exit
```

Step 2 Configure the destination IP address of DHCP Relay.

```
Raisecom(config)#interface vlan 2
Raisecom(config-vlan2)#ip dhcp relay target-ip 10.0.0.1
```

Checking results

Use the **show ip dhcp relay** command to show configurations of DHCP Relay.

```
Raisecom#show ip dhcp relay
DHCP Relay Global Status: Enable
Interface                 Status        Relay Address      Target Address
------------------------------------------------------------------------
-------
vlan2                    Enable        192.168.1.1        10.0.0.1
```

```
vlan3                    Enable       192.168.1.1       --
```


Copyright © Raisecom Technology Co., Ltd.

6 QoS

This chapter describes basic principles and configuration procedures for QoS, and provides related configuration examples, including the following sections:

- Introduction
- Configuring priority
- Configuring congestion management
- Configuring congestion avoidance
- Configuring traffic classification and traffic policy
- Configuring traffic shaping and rate limiting
- Bandwidth rate limiting
- Configuration examples

6.1 Introduction

When network applications become more and more versatile, users bring forward different Quality of Service (QoS) requirements on them. In this case, the network should distribute and schedule resources for different network applications as required. When network is overloaded or congested, QoS can ensure service timeliness and integrity and make the entire network run efficiently.

QoS is composed of a group of flow management technologies:

- Service model
- Priority trust
- Traffic classification
- Traffic policy
- Priority mapping
- Congestion management

6.1.1 Service model

QoS technical service models:

- Best-effort Service

Copyright © Raisecom Technology Co., Ltd.

- Differentiated Services (DiffServ)

Best-effort

Best-effort service is the most basic and simplest service model on the Internet (IPv4 standard) based on storing and forwarding mechanism. In Best-effort service model, the application can send a number of packets at any time without being allowed in advance and notifying the network. For the Best-effort service, the network will send packets as possible as it can, but it does not guarantee the delay and reliability.

Best-effort is the default Internet service model now, suitable to most network applications, such as FTP and Email. It is implemented by First In First Out (FIFO) queue.

DiffServ

The DiffServ model is a multi-service model, which can satisfy different QoS requirements.

The DiffServ model does not need to maintain state for each flow. It provides differentiated services according to the QoS classification of each packet. Many different methods can be used for classifying QoS packets, such as IP packet priority (IP precedence), the packet source address or destination address.

Generally, DiffServ is used to provide end-to-end QoS services for a number of important applications, which is implemented through the following techniques:

- Committed Access Rate (CAR): CAR refers to classifying the packets according to the preconfigured packet matching rules, such as IP packets priority, the packet source address or destination address. The system continues to send the packets if the flow complies with the rules of token bucket. Otherwise, it discards the packets or remarks IP precedence, DSCP, EXP CAR can not only control the flows, but also mark and remark the packets.
- Queuing technology: the queuing technologies of SP, WRR, DRR, SP+WRR, and SP+DRR cache and schedule the congestion packets to implement congestion management.

6.1.2 Priority trust

Priority trust means that the ISCOM2600G series switch uses priority of packets for classification and performs QoS management.

The ISCOM2600G series switch supports packet priority trust based on interface, including:

- Differentiated Services Code Point (DSCP) priority
- Class of Service (CoS) priority
- ToS priority

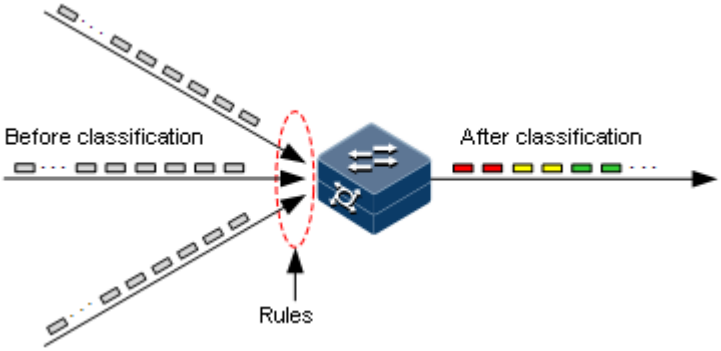
6.1.3 Traffic classification

Traffic classification refers to identifying certain packets according to specified rules and performing different QoS policies on packets matched with different rules. Traffic classification is the premise and basis for differentiated services.

The ISCOM2600G series switch supports traffic classification based on ToS priority, DSCP, and CoS over IP packets, and classification based on Access Control List (ACL) rules and VLAN ID. The traffic classification procedure is shown in Figure 6-1.

Copyright © Raisecom Technology Co., Ltd.

Figure 6-1 Traffic classification



IP precedence and DSCP

Figure 6-2 shows the structure of the IP packet header. The head contains an 8-bit ToS field. Defined by RFC 1122, IP priority (IP Precedence) uses the highest 3 bits (0–3) with value range of 0–7; RFC2474 defines ToS field again, and applies the first 6 bits (0–5) to DSCP with value ranging from 0 to 63, the last 2 bits (bit-6 and bit-7) are reserved. Figure 6-3 shows the structure of ToS and DSCP.

Figure 6-2 Structure of an IP packet header

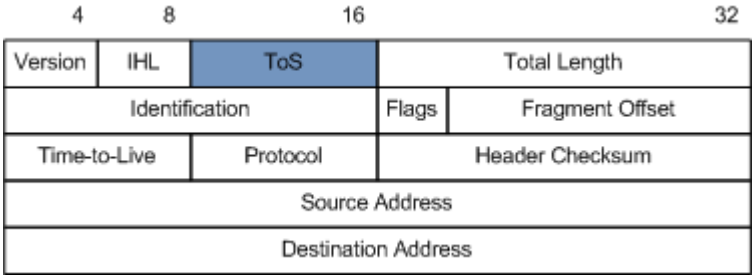
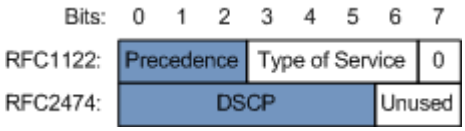


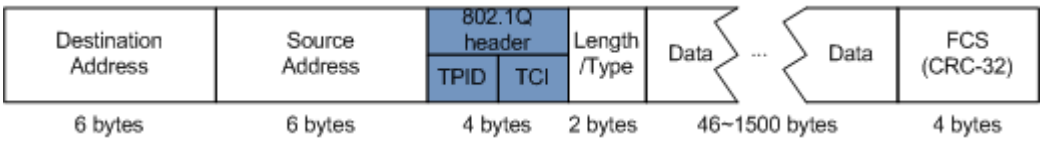
Figure 6-3 Structures of the ToS priority and DSCP



CoS

IEEE802.1Q-based VLAN packets are modifications of Ethernet packets. A 4-byte 802.1Q header is added between the source MAC address and protocol type, as shown in Figure 6-4. The 802.1Q header consists of a 2-byte Tag Protocol Identifier (TPID, valuing 0x8100) filed and a 2-byte Tag Control Information (TCI) field.

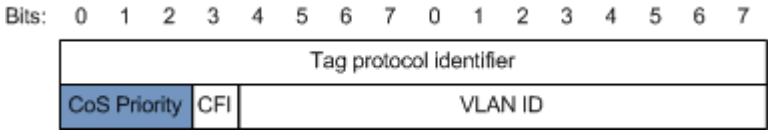
Figure 6-4 Structure of a VLAN packet



Copyright © Raisecom Technology Co., Ltd.

The first 3 bits of the TCI field represent CoS, which ranges from 0 to 7, as shown in Figure 6-5. CoS is used to guarantee QoS on the Layer 2 network.

Figure 6-5 Structure of CoS



6.1.4 Traffic policy

After performing traffic classification on packets, you need to perform different operations on packets of different categories. A traffic policy is formed when traffic classifiers are bound to traffic behaviours.

Rate limiting based on traffic policy

Rate limiting refers to controlling network traffic, monitoring the rate of traffic entering the network, and discarding overflow part, so it controls ingress traffic in a reasonable range, thus protecting network resources and carrier interests.

The ISCOM2600G series switch supports rate limiting based on traffic policy in the ingress direction on the interface.

The ISCOM2600G series switch supports using token bucket for rate limiting, including single-token bucket and dual-token bucket.

Redirection

Redirection refers to redirecting packets to a specified interface, instead of forwarding packets according to the mapping between the original destination address and interface, thus implementing policy routing.

The ISCOM2600G series switch supports redirecting packets to the specified interface for forwarding in the ingress direction of the interface.

Remarking

Remarking refers to configuring some priority fields in packets again and then classifying packets by user-defined standards. Besides, downstream nodes on the network can provide differentiated QoS service according to remarking information.

The ISCOM2600G series switch supports remarking packets by the following priority fields:

- IP precedence
- DSCP
- CoS

Traffic statistics

Traffic statistics is used to gather statistics about data packets of a specified service flow; in other words, the number of packets and bytes matching traffic class that pass the network or are discarded.

Copyright © Raisecom Technology Co., Ltd.

Traffic statistics is not a QoS control measure, but can be used in combination with other QoS actions to improve network supervision.

6.1.5 Priority mapping

Priority mapping refers to sending packets to different queues with different local priorities according to pre-configured mapping from external priority to local priority. Therefore, packets in different queues can be scheduled on the egress interface.

The ISCOM2600G series switch supports performing priority mapping based on DSCP of IP packets or CoS of VLAN packets. The Traffic-Class field of IPv6 packets corresponds to DSCP of IPv4 packets. The mapping from DSCP to local priority is applicable to IPv6 packets. Take the first 6 bits of the Traffic-Class field for use.

By default, the mapping from the DSCP or CoS to local priority of the ISCOM2600G series switch is listed in Table 6-1 and Table 6-2.

Table 6-1 Mapping from DSCP or CoS to local priority

Local priority	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
CoS	0	1	2	3	4	5	6	7

Local priority refers to a kind of packet priority with internal meaning assigned by the ISCOM2600G series switch and is the priority corresponding to queue in QoS queue scheduling.

Local priority ranges from 0 to 7. Each interface of the ISCOM2600G series switch supports 8 queues. Local priority and interface queue are in one-to-one mapping. The packet can be sent to the assigned queue according to the mapping between local priority and queue, as shown in Table 6-2.

Table 6-2 Mapping between local priority and queue

Local priority	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

6.1.6 Queue scheduling

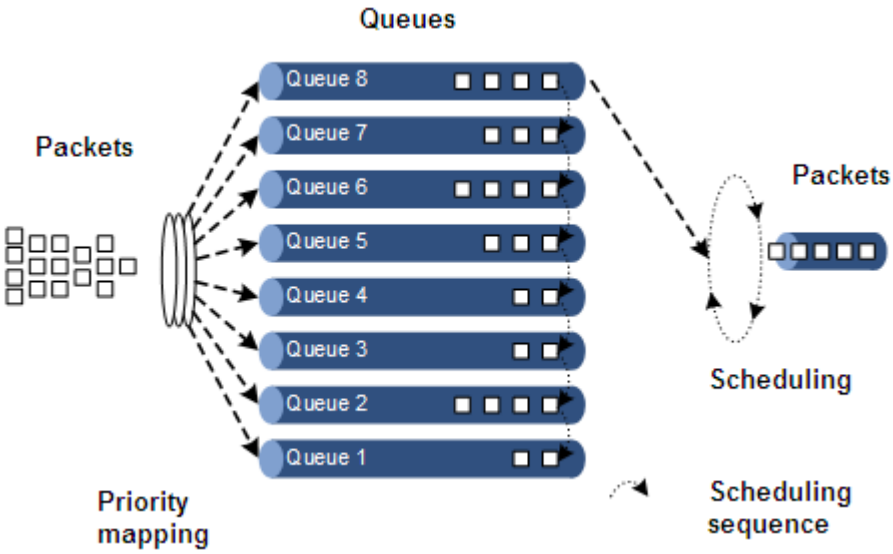
The ISCOM2600G series switch needs to perform queue scheduling when delay-sensitive services need better QoS services than non-delay-sensitive services and when the network is congested once in a while.

Queue scheduling adopts different scheduling algorithms to send packets in a queue. Scheduling algorithms supported by the ISCOM2600G series switch include Strict-Priority (SP), Weight Round Robin (WRR), Deficit Round Robin (DRR), SP+WRR, and SP+DRR. All scheduling algorithms are designed for addressing specified traffic problems. And they have different effects on bandwidth distribution, delay, and jitter.

Copyright © Raisecom Technology Co., Ltd.

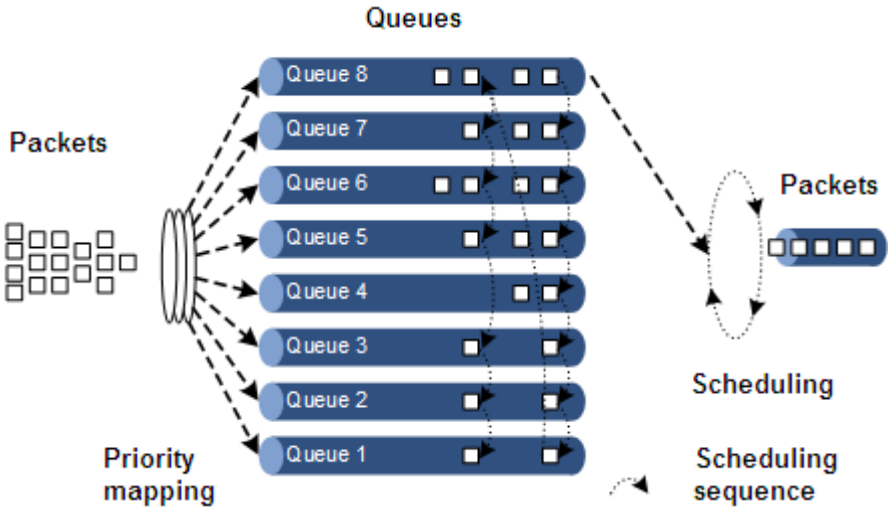
- SP: the ISCOM2600G series switch strictly schedules packets in a descending order of priority. Packets with lower priority cannot be scheduled until packets with higher priority are scheduled, as shown in Figure 6-6.

Figure 6-6 SP scheduling



- WRR: on the basis of scheduling packets in a polling manner according to the priority, the ISCOM2600G series switch schedules packets according to the weight (based on bytes) of the queue, as shown in Figure 6-7.

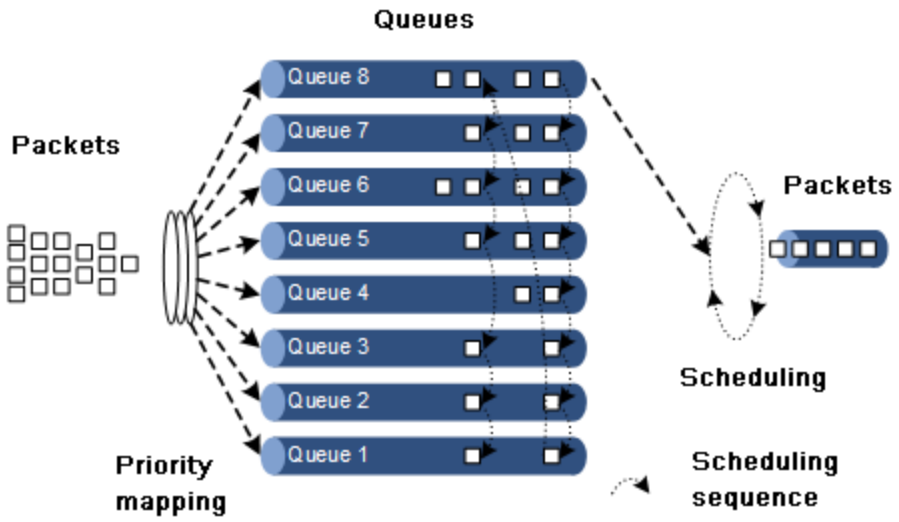
Figure 6-7 WRR scheduling



- DRR: similar with WRR, on the basis of scheduling packets in a polling manner according to the scheduling sequence, the ISCOM2600G series switch schedules packets according to the weight of the queue (based on packet), as shown in DRR scheduling

Copyright © Raisecom Technology Co., Ltd.

Figure 6-8 DRR scheduling



- SP+WRR: a scheduling mode combining the SP scheduling and WRR scheduling. In this mode, queues on an interface are divided into 2 groups. You can specify the queues where SP scheduling/WRR scheduling is performed.
- SP+DRR: a scheduling mode combining the SP scheduling and DRR scheduling. In this mode, queues on an interface are divided into 2 groups. You can specify the queues where SP scheduling/DRR scheduling is performed.

6.1.7 Congestion avoidance

By monitoring utilization of network resources (queues/memory buffer), congestion avoidance can discard packets actively when congestion occurs or network traffic increases. It is a traffic control mechanism that is used to resolve network overload by adjusting network traffic.

The traditional packet loss policy uses the Tail-Drop mode to process all packets equally without differentiating class of services. When congestion occurs, packets at the end of a queue are discarded until congestion is resolved.

This Tail-Drop policy may cause TCP global synchronization, making network traffic change between heavy and low and affecting link utilization.

RED

Random Early Detection (RED) discards packets randomly and prevents multiple TCP connection from reducing transmission rate simultaneously to avoid TCP global synchronization.

The RED algorithm configures a minimum threshold and maximum threshold for length of each queue. In addition:

- Packets are not discarded when the queue length is smaller than the minimum threshold.
- All received packets are discarded when the queue length is greater than the maximum threshold.
- Packets to be received are discarded randomly when the queue length is between the minimum and maximum thresholds. The greater the queue size is, the higher the packet drop probability is.

Copyright © Raisecom Technology Co., Ltd.

6.1.8 Traffic shaping

When the rate of the interface on the downstream device is smaller than that of the interface on the upstream device, traffic congestion may occur on the interface on the downstream device. In this case, you can configure traffic shaping in the egress direction of the interface on the upstream device to shape the irregular traffic from the upstream device and to output a regular traffic, thus avoiding traffic congestion on the downstream device.

Traffic shaping is a traffic control technology applied to queues on the interface. It can limit the rate of all packets on the specified queue on the interface. It caches excess packets when the configured bandwidth is exceeded, and forwards them when the bandwidth for these packets is available. It discards packets if all packets exceed the length of the cached queue.

6.1.9 Rate limiting based on interface and VLAN

The ISCOM2600G series switch supports rate limiting both based on traffic policy, interface, or VLAN ID. Similar to rate limiting based on traffic policy, the ISCOM2600G series switch discards the excess traffic.

6.1.10 QoS enhancement

QoS enhancement is a subfunction of QoS and is more flexible than basic QoS. It is widely used on switches.

QoS enhancement has the following functions:

- Ingress interface
  - Bandwidth guarantee: QoS enhancement implements the bandwidth service based on interface or flow. It also supports hierarchical bandwidth guarantee and refining bandwidth of different service flows.
  - Awaring: this function determines whether to conduct color-aware of packets when a flow enters the bandwidth-guaranteed interface.
- Egress interface
  - Bandwidth guarantee: bandwidth service based on interface or flow is implemented. QoS enhancement does not support hierarchical bandwidth guarantee.
  - Marking: this function determines whether to mark a packet with color when a flow leaves the bandwidth-guaranteed interface.

Bandwidth guarantee

The bandwidth guarantee function guarantees that the traffic entering the network is within the defined range, and it discards or schedules packets. Bandwidth guarantee can meet users' requirements on service bandwidth, and also protect network resources and carriers' benefits.

By configuring the bandwidth guarantee profile and applying it to an interface, you can mark different flows green, yellow, and red. The ISCOM2600G series switch takes different actions over flows of different colors: forward green flows, schedule yellow flows, and discard red flows.

Hierarchical bandwidth guarantee

Hierarchical bandwidth guarantee is a more flexible bandwidth guarantee. You can configure guaranteed bandwidth for each flow independently and even configure guaranteed bandwidth for sum of multiple flows through hierarchical bandwidth guarantee.

Copyright © Raisecom Technology Co., Ltd.

Color-aware and marking

If enabled with color-aware, the ISCOM2600G series switch is in color-aware status, in which it can identify whether the ingress flow is marked with color. If disabled with color-aware, the ISCOM2600G series switch is in color-blind status, in which it can neglect whether the ingress flow is marked with color, but identify the flow color again.

The function of color marking judges the color of a flow according to Committed Information Rate (CIR), Committed Burst Size (CBS), Excess Information Rate (EIR), and Excess Burst Size (EBS) configured in the bandwidth guarantee profile, and modifies the flag bit to mark it with color according to the packet format defined in IEEE 802.1ad.

6.2 Configuring priority

6.2.1 Preparing for configurations

Scenario

You can choose to trust the priority carried by packets from an upstream device, or process packets with untrusted priority through the traffic class and traffic policy. After being configured to priority trust mode, the ISCOM2600G series switch processes packets according to their priorities and provides services accordingly.

To specify local priority for packets is the prerequisite for queue scheduling. For packets from the upstream device, you can not only map the external priority carried by packets to different local priorities, but also configure local priority for packets based on interface. Then the ISCOM2600G series switch will conduct queue scheduling according to local priority of packets. Generally, IP packets need to be configured with mapping from IP precedence/DSCP to local priority; while VLAN packets need to be configured with mapping from CoS to local priority.

Prerequisite

N/A

6.2.2 Default configurations of basic QoS

Default configurations of basic QoS are as below.

Function	Default value
Global QoS status	Enable
Interface trust priority type	Trust CoS
Mapping from CoS to local priority	See Table 6-3.
Mapping from DSCP to local priority	See Table 6-4.
Mapping from local priority to CoS	See Table 6-5.
Interface priority	0

Copyright © Raisecom Technology Co., Ltd.

Table 6-3 Default mapping from CoS to local priority

CoS	0	1	2	3	4	5	6	7
Local priority	0 (green)	1 (green)	2 (green)	3 (green)	4 (green)	5 (green)	6 (green)	7 (green)

Table 6-4 Default mapping from DSCP to local priority

DSCP	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
Local priority	0 (green)	1 (green)	2 (green)	3 (green)	4 (green)	5 (green)	6 (green)	7 (green)

Table 6-5 Default mapping from local priority to CoS

Local priority	0	1	2	3	4	5	6	7
CoS	0	1	2	3	4	5	6	7

6.2.3 Configuring types of priorities trusted by interface

Configure types of priorities trusted by interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#mls qos trust { cos | dscp | dscp-or-cos | port-priority }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#mls qos trust dscp`
		Configure types of priorities trusted by interface.
		• cos: trust CoS priority which exists in the header of the 802.1Q packet.
		• dscp: trust DSCP priority which exists in the header of the IP packet.
		• dscp-or-cos: trust DSCP priority of CoS priority. Layer 3 packets trust DSCP priority and Layer 2 packets trust CoS priority.
		• port-priority: priority trusted by the interface

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-gigaethernet1/1/port)#**mls qos priority** priority-*value* **Example:** Raisecom(config-gigaethernet1/1/1)#mls qos priority 2	Configure the interface priority. • priority-value: interface priority, an integer, ranging from 0 to 7

6.2.4 Configuring mapping from CoS to local priority

Configure the mapping from CoS to local priority and color for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping cos-to-local-priority** *profile-id* **Example:** Raisecom(config)#mls qos mapping cos-to-local-priority 1	Create a profile of mapping from CoS to local priority and color, and enter cos-to-pri configuration mode. • profile-id: profile ID, an integer, ranging from 1 to 7
3	Raisecom(cos-to-pri)#**cos** *cos-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }] **Example:** Raisecom(cos-to-pri)#cos 2 to local-priority 3 color red	(Optional) modify the profile of mapping from CoS to local priority and color. • cos-value: CoS priority, an integer, ranging from 0 to 7 • localpri-value: local priority, an integer, ranging from 0 to 7 • green: specify the green. • red: specify the red. • yellow: specify the yellow.
4	Raisecom(cos-to-pri)#**exit** Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config-gigaethernet1/1/port)#**mls qos cos-to-local-priority** *profile-id* [**dei** { **enable** | **disable** }] **Example:** Raisecom(config-gigaethernet1/1/1)#mls qos cos-to-local-priority 1	Apply the profile of mapping from CoS to local priority and color on the interface. • profile-id: profile ID, an integer, ranging from 1 to 7 • enable: enable the function of marking egress packets with a color on the interface. • disable: disable the function of marking egress packets with a color on the interface.

6.2.5 Configuring mapping from DSCP to local priority and color

Configure the mapping from DSCP to local priority and color for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping dscp-to-local-priority** *profile-id* **Example:** Raisecom(config)#mls qos mapping dscp-to-local-priority 1	Create a profile of mapping from DSCP to local priority and color, and enter dscp-to-pri configuration mode. • profile-id: profile ID, an integer, ranging from 1 to 7
3	Raisecom(dscp-to-pri)#**dscp** *dscp-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }] **Example:** Raisecom(dscp-to-pri)#dscp 2 to local-priority 3 color red	(Optional) modify the profile of mapping from DSCP to local priority and color. • dscp-value: DSCP priority, an integer, ranging from 0 to 63 • localpri-value: local priority, an integer, ranging from 0 to 7 • green: specify the green. • red: specify the red. • yellow: specify the yellow.
4	Raisecom(cos-to-pri)#**exit** Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config-gigaethernet1/1/port)#**mls qos dscp-to-local-priority** *profile-id* **Example:** Raisecom(config-gigaethernet1/1/1)#mls qos dscp-to-local-priority 1	Apply the profile of mapping from DSCP to local priority and color on the interface. The profile used in this configuration is the same profile used by DSCP mutation. • profile-id: profile ID, an integer, ranging from 1 to 7

6.2.6 Configuring DSCP mutation

Configure DSCP mutation for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping dscp-mutation** *profile-id* **Example:** Raisecom(config)#mls qos mapping dscp-mutation 1	Create a DSCP mutation mapping profile, and enter dscp mutation configuration mode. • profile-id: profile ID, an integer, ranging from 1 to 7
3	Raisecom(dscp-mutation)#**dscp** *dscp-value* **to new-dscp** *dscp-value* **Example:** Raisecom(dscp-mutation)#dscp 2 to new-dscp 20	(Optional) modify the DSCP mutation profile. The profile used in this configuration is the same profile used by the mapping from DSCP to local priority. • dscp-value: DSCP priority, an integer, ranging from 0 to 63
4	Raisecom(cos-to-pri)#**exit** Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
5	Raisecom(config-gigaethernet1/1/port)#**mls qos dscp-mutation** *profile-id* **Example:** Raisecom(config-gigaethernet1/1/1)#mls qos dscp-mutation 1	Apply the DSCP mutation profile on the interface. • profile-id: profile ID, an integer, ranging from 1 to 7

6.2.7 Configuring CoS remarking

Configure CoS remarking for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config-gigaethernet1/1/port)#**mls qos cos-remark-mapping { enable | disable }** [**dei** { **enable** | **disable** }] Raisecom(config-gigaethernet1/1/port)#**exit** **Example:** Raisecom(config-gigaethernet1/1/1)#mls qos cos-remark-mapping enable	Enable or disable mapping from local priority to CoS. • enable: enable mapping from local priority to CoS. • disable: disable mapping from local priority to CoS. • dei enable: enable the function of marking egress packets with a color on the interface. • dei disable: disable the function of marking egress packets with a color on the interface.
4	Raisecom(config)#**mls qos mapping cos-remark** *profile-id* **Example:** Raisecom(config)#mls qos mapping cos-remark 1	Create a CoS remarking profile, and enter cos-remark configuration mode. • profile-id: profile ID, an integer, ranging from 1 to 7
5	Raisecom(cos-remark)#**local-priority** *localpri-value* **to cos** *cos-value* **Example:** Raisecom(cos-remark)#local-priority 2 to cos 3	Modify the CoS remarking profile. • localpri-value: local priority, an integer, ranging from 0 to 7 • cos-value: CoS priority, an integer, ranging from 0 to 7
6	Raisecom(cos-to-pri)#**exit** Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
7	Raisecom(config-gigaethernet1/1/port)#**mls qos cos-remark** *profile-id* **Example:** Raisecom(config-gigaethernet1/1/1)#mls qos cos-remark 1	Apply the DSCP remarking profile on the interface. profile-id: profile ID, an integer, ranging from 1 to 7

6.2.8 Checking configurations

Use the following commands to check configuration results.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
1	Raisecom#**show mls qos interface** [*interface-type interface-number*]	Show QoS priority, trust mode, and scheduling mode on the interface.
2	Raisecom#**show mls qos mapping cos-to-local-priority** [**default** | *profile-id*]	Show information about mapping from CoS to local priority and color profile.
3	Raisecom#**show mls qos mapping dscp-to-local-priority** [**default** | *profile-id*]	Show information about mapping from DSCP to local priority and color profile.
4	Raisecom#**show mls qos mapping dscp-mutation** [*profile-id*]	Show mapping information about the DHCP mutation profile
5	Raisecom#**show mls qos mapping cos-remark** [**default** | *profile-id*]	Show information about the CoS remarking profile.

6.3 Configuring congestion management

6.3.1 Preparing for configurations

Scenario

When the network is congested, you can configure queue scheduling if you want to:

- Balance delay and delay jitter of various packets, preferentially process packets of key services (such as video and voice).
- Fairly process packets of secondary services (such as Email) with identical priority.
- Process packets of different priorities according to respective weight values.

The scheduling algorithm to be chosen depends on the current service condition and customer requirements.

Prerequisite

Enable global QoS.

6.3.2 Default configurations of congestion management

Default configurations of congestion management are as below.

Function	Default value
Queue scheduling mode	SP
Queue weight	• WRR weight for scheduling 8 queues is 1. • DRR weight for scheduling 8 queues is 81.

Copyright © Raisecom Technology Co., Ltd.

6.3.3 Configuring SP queue scheduling

Configure SP queue scheduling for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#mls qos queue scheduler sp`	Configure queue scheduling mode as SP on the interface.

6.3.4 Configuring WRR or SP+WRR queue scheduling

Configure WRR or SP+WRR for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#mls qos queue scheduler wrr weigh1 weight2 weight3…weight8`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#mls qos queue scheduler wrr 1 1 1 1 1 1 1 1`
		Configure queue scheduling mode as WRR on the interface and the weight for each queue.
		• weight1–weight8: weight, an integer, ranging from 0 to 127, with the value 0 indicating the SP queue

6.3.5 Configuring DRR or SP+DRR queue scheduling

Configure DRR or SP+DRR for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config-gigaethernet1/1/port)#**mls qos queue scheduler drr** *weigh1 weight2 weight3…weight8* **Example:** Raisecom(config-gigaethernet1/1/1)#mls qos queue scheduler drr 1 1 1 1 1 1 1 1	Configure queue scheduling mode as DRR, and configure weight for various queues. Conduct SP scheduling when priority of a queue is 0. • weight1–weight8: weight, an integer, ranging from 0 to 127

6.3.6 Configuring queue bandwidth guarantee

Configure queue bandwidth guarantee for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config-gigaethernet1/1/port)#**mls qos queue** *queue-id* **shaping cir** *cir-value* **pir** *pir-value* **Example:** Raisecom(config-gigaethernet1/1/1)#mls qos queue 2 shaping cir 20 pir 200	(Optional) configure queue bandwidth guarantee on the interface and configure burst size. • queue-id: queue ID, an integer, ranging from 1 to 8 • cir-value: CIR, an integer, ranging from 0 to 10485760, in units of kbit/s • pir-value: PIR, an integer, ranging from 0 to 10485760, in units of kbit/s

6.3.7 Checking configurations

Use the following commands to check configuration results.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
1	`Raisecom#show mls qos queue interface interface-type interface-number`	Show the weight of queues on the interface.
2	`Raisecom#show mls qos queue statistics interface interface-type interface-number`	Show statistics about queues on the interface.
3	`Raisecom#show mls qos queue shaping interface interface-type interface-list`	Show queue shaping on the interface.

6.4 Configuring congestion avoidance

6.4.1 Preparing for configurations

Scenario

To avoid network congestion and solve the problem of TCP global synchronization, you can configure congestion avoidance to adjust network flow and relieve network overload.

The ISCOM2600G series switch conducts congestion avoidance based on WRED.

Prerequisite

Enable global QoS.

6.4.2 Default configurations of congestion avoidance

Default configurations of congestion avoidance are as below.

Function	Default value
Global WRED status	Enable

6.4.3 Configuring SRED

Configure SRED for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#mls qos sred profile profile-id`
	Example:
	`Raisecom(config)#mls qos sred profile 1`
		Create a SRED profile, and enter SRED configuration mode.
		• profile-id: SRED profile ID, an integer, ranging from 1 to 8

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(sred)#**sred** [**color** { **red** | **yellow** }] **start-drop-threshold** *start-drop-value* **drop-probability** *drop-probability-value* **Example:** Raisecom(sred)#sred start-drop-threshold 20 drop-probability 5	Modify the SRED profile. • red: red packets • yellow: yellow packets • start-drop-value: start-drop threshold, ranging from 0 to 100 • drop probability value: discard probability, an integer, ranging from 0 to 7
4	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
5	Raisecom(config-gigaethernet1/1/port)#**mls qos queue** *queue-id* **sred** *sredprofile-num* **Example:** Raisecom(config-gigaethernet1/1/1)#mls qos queue 2 sred 1	Apply the SRED profile to the interface. • queue-id: queue ID, an integer, ranging from 1 to 8 • sredprofile-num: SRED profile ID, an integer, ranging from 1 to 8

6.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show mls qos sred profile** [*profile-list*]	Show information about the SRED profile.
2	Raisecom#**show mls qos queue sred interface** *interface-type interface-number*	Show SRED information about the interface.

6.5 Configuring traffic classification and traffic policy

6.5.1 Preparing for configurations

Scenario

Traffic classification is the basis of QoS. You can classify packets from the upstream device according to the priorities and ACL rules. After classification, the ISCOM2600G series switch can perform corresponding operations on packets in different categories and provide corresponding services.

Copyright © Raisecom Technology Co., Ltd.

A traffic classification rule will not take effect until it is bound to a traffic policy. You should apply traffic policy according to current network loading conditions and period. Usually, the ISCOM2600G series switch limits the rate for transmitting packets according to CIR when packets enter the network, and remarks priority according to service feature of packets.

Prerequisite

Enable global QoS.

6.5.2 Default configurations of traffic classification and traffic policy

Default configurations of traffic classification and traffic policy are as below.

Function	Default value
Traffic policy status	Disable
Traffic policy statistics status	Disable

6.5.3 Creating traffic class

Create a traffic class for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#class-map` *`class-map-name`* `[ match-all | match-any ]`
	Example:
	`Raisecom(config)#class-map class1 match-all`
		Create a traffic class and enter traffic classification cmap configuration mode.
		• class-map: name of the traffic class, a string of 1 to 16 characters
		• match-all: specify match type to satisfy all defined classification rules.
		• match-any: specify match type to satisfy one defined or more defined classification rules.

3	`Raisecom(config-cmap)#description` *`string`* **Example:** `Raisecom(config-cmap)#description this-is-a-test-class-map`	(Optional) configure the description of the traffic class. • string: description, a string of 1 to 255 characters

6.5.4 Configuring traffic classification rules

Configure traffic classification rules for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**class-map** *class-map-name* [**match-all** | **match-any**] **Example:** Raisecom(config)#class-map class1 match-all	Create a traffic class and enter traffic classification cmap configuration mode. • class-map: name of the traffic class, a string of 1 to 16 characters • match-all: specify match type to satisfy all defined classification rules. • match-any: specify match type to satisfy one defined or more defined classification rules.
3	R Raisecom(config-cmap)#**match access-list** { *acl-number* | **name** *word* } Raisecom(config-cmap)#**exit** **Example:** Raisecom(config-cmap)#match access-list 1001	(Optional) configure the traffic classification based on the ACL rule. The ACL rule must be defined firstly and the type must be permit. • acl-number: number of ACL list, in form of integer – When the value ranges from 1000 to 1999, it means basic IP ACL. – When the value ranges from 2000 to 2999, it means extended IP ACL. – When the value ranges from 3000 to 3999, it means MAC ACL. – When the value ranges from 5000 to 5999, it means MAP ACL. – When the value ranges from 6000 to 6999, it means IPv6 ACL. – When the value ranges from 7000 to 7999, it means IPv6 extended ACL. • name word: ACL name
4	Raisecom(config-cmap)#**match cos** *cos-value* **Example:** Raisecom(config-cmap)#match cos 1	(Optional) configure the traffic class based on CoS of packets. • cos-value: classify packets based on CoS values. The cos-value indicates the CoS value. It is an integer ranging from 0 to 7.
5	Raisecom(config-cmap)#**match inner-vlan** *inner-vlan-value* **Example:** Raisecom(config-cmap)#match inner-vlan 2	(Optional) configure the traffic class based on inner VLAN of packets. • inner-vlan-value: classify packets based on inner and outer VLANs. The inner-vlan-value indicates the inner VLAN ID. It is an integer ranging from 1 to 4094.
6	Raisecom(config-cmap)#**match vlan** *vlan-id* [vlan-mask] **Example:** Raisecom(config-cmap)#match vlan 3	(Optional) configure the traffic class based on VLANs of packets. • vlan-id: classify packets based on VLANs. The vlan-id indicates VLAN ID. It is an integer ranging from 1 to 4094. • vlan-mask: VLAN mask, in hexadecimal notation
7	Raisecom(config-cmap)#**match dscp** *dscp-value* **Example:** Raisecom(config-cmap)#match dscp 4	(Optional) configure the traffic class based on DSCP rule. • dscp-value: classify packets based on DSCP values. The dscp-value indicates the DSCP value. It is an integer ranging from 0 to 63.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

8	`Raisecom(config)#policy-map policy-map-name`
	`Raisecom(config-pmap)#class-map class-map-name`
	Example:
	`Raisecom(config)#policy-map policy1`
	`Raisecom(config-pmap)#class-map class1`
		(Optional) configure the traffic class based on traffic policy.
		The traffic policy must have been created, and it matching type must be consistent with the matching type of the traffic class.
		• policy-map-name: name of the traffic policy, a string of 1 to 16 characters
		• class-map-name: name of the traffic class, a string of 1 to 16 characters

Note

- Traffic classification rules must be created for the traffic class; in other words, the **match** parameter must be configured.
- For the traffic class quoted by a traffic policy, do not modify the traffic classification rule; in other words, do not modify the **match** parameter of the traffic class.

6.5.5 Creating rate limiting rule and shapping rule

To limit rate of packets based on traffic policy, create a token bucket, configure rate limiting and shaping rules on the token bucket, quote these rules to the traffic class bound to the traffic policy.

Create rate limiting rules and shaping rule for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#mls qos policer-profile policer-name [ single | hierarchy | aggregate ]`
	Example:
	`Raisecom(config)#mls qos policer-profile tb single`
		Create a traffic policer profile, and enter traffic-policer configuration mode.
		• policer-name: name of traffic policing profile, a string of 1 to 16 characters
		• single: specify the traffic regulation mode as single.
		• aggregate: specify the traffic regulation mode as aggregate token bucket.
		• hierarchy: specify the traffic regulation mode as hierarchy token bucket.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

3	`Raisecom(traffic-policer)#cir cir cbs cbs`
	Example:
	`Raisecom(traffic-policer)#cir 20 cbs 30`
		(Optional) configure flow mode token bucket parameters.
		• cir: committed information rate. The cir is an integer ranging from 1 to 10485760, in units of kbit/s.
		• cbs: committed burst size. The cbs is an integer ranging from 1 to 262144, in units of Kbyte.
		Note
		Flow mode token bucket is single token bucket, only supporting to configure red and green packets operation.

4	`Raisecom(traffic-policer)#cir cir cbs cbs ebs ebs`
	Example:
	`Raisecom(traffic-policer)#cir 20 cbs 30 ebs 30`
		(Optional) configure RFC2697 mode token bucket parameters.
		• cir: committed information rate. The cir is an integer ranging from 1 to 10485760, in units of kbit/s.
		• cbs: committed burst size. The cbs is an integer ranging from 1 to 262144, in units of Kbyte.
		• ebs: excess burst size. The ebs is an integer ranging from 1 to 262144, in units of Kbyte.

5	`Raisecom(traffic-policer)#cir cir cbs cbs pir pir pbs pbs`
	Example:
	`Raisecom(traffic-policer)#cir 20 cbs 30 pir 20 pbs 30`
		(Optional) configure RFC2698 mode token bucket parameters.
		• cir: committed information rate. The cir is an integer ranging from 1 to 10485760, in units of kbit/s.
		• cbs: committed burst size. The cbs is an integer ranging from 1 to 262144, in units of Kbyte.
		• pir: peak information rate. The pir is an integer ranging from 1 to 10485760, in units of Kbyte.
		• pbs: peak burst size. The pbs is an integer ranging from 1 to 262144, in units of Kbyte.

6	`Raisecom(traffic-policer)#cir cir cbs cbs eir eir ebs ebs [ coupling ]`
	Example:
	`Raisecom(traffic-policer)#cir 20 cbs 30 eir 20 ebs 30`
		(Optional) configure RFC4115 mode or MEF token bucket parameters.
		• cir: committed information rate. The cir is an integer ranging from 1 to 10485760, in units of kbit/s.
		• cbs: committed burst size. The cbs is an integer ranging from 1 to 262144, in units of Kbyte.
		• eir: excess information rate. The eir is an integer ranging from 1 to 10485760, in units of kbit/s.
		• ebs: excess burst size. The ebs is an integer ranging from 1 to 262144, in units of Kbyte.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
7	Raisecom(traffic-policer)#**color-mode** { **aware** | **blind** } **Example:** Raisecom(traffic-policer)#color-mode blind	(Optional) configure the color mode of the token bucket. • aware: color aware mode • blind: color blind mode
8	Raisecom(traffic-policer)#**drop-color** { **red** [**yellow**] | **yellow** } **Example:** Raisecom(traffic-policer)#drop-color red	(Optional) configure the token bucket to discard packets with any color. • red: discard red packets. • yellow: discard yellow packets
9	Raisecom(traffic-policer)#**recolor** { **green-recolor** { **yellow** | **red** } | **red**[**yellow-recolor** { **green** | **yellow** } | **yellowred** }] [**red-recolor** { **green** | **red** } }**yellow** }] Raisecom(traffic-policer)#**recolor red-recolor** { **green** | **yellow** } Raisecom(traffic-policer)#**recolor yellow-recolor** { **green** | **red** } [**red-recolor** { **green** | **yellow** }] **Example:** Raisecom(traffic-policer)#recolor green-recolor red	(Optional) configure packet recoloring. • green-recolor: recolor green packets. • red-recolor: recolor red packets. • yellow-recolor: recolor yellow packets. • red: recolor packets with red. • green: recolor packets with green. • yellow: recolor packets with yellow.
10	Raisecom(traffic-policer)#**set-cos** { **green** *cos* | **red** *cos* |[**yellow** *cos*] [**red** *cos*] | **red** *cos* | **yellow** *cos* [**red** *cos*] } **Example:** Raisecom(traffic-policer)#set-cos red 2	(Optional) configure the mapping from packets color to CoS. • green cos: specify the CoS value mapped to green packets. It is an integer ranging from 0 to 7. • red cos: specify the CoS value mapped to red packets. It is an integer ranging from 0 to 7. • yellow cos: specify the CoS value mapped to yellow packets. It is an integer ranging from 0 to 7.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
11	Raisecom(traffic-policer)#**set-dscp** { **green** *green-value* | **red** *red-value* |[**yellow** *yellow-value*] [**red** *red-value*] | **red** *red-value* | **yellow** *yellow-value* [**red** *red-value*] } **Example:** Raisecom(traffic-policer)#set-dscp red 2	(Optional) configure the mapping from packets color to DSCP. • green-value: specify the DSCP value mapped to green packets. It is an integer ranging from 0 to 63. • red-value: specify the DSCP value mapped to red packets. It is an integer ranging from 0 to 63. • yellow-value: specify the DSCP value mapped to yellow packets. It is an integer ranging from 0 to 63.
12	Raisecom(traffic-policer)#**set-pri** { **green** *green-value* | **red** *red-value* |[**yellow** *yellow-value*] [**red** *red-value*] | **red** *red-value* | **yellow** *yellow-value* [**red** *red-value*] } **Example:** Raisecom(traffic-policer)#set-pri red 2	(Optional) configure the mapping from packets color to local priority. • green-value: specify the local priority mapped to green packets. It is an integer ranging from 0 to 7. • red-value: specify the local priority mapped to red packets. It is an integer ranging from 0 to 7. • yellow-value: specify the local priority mapped to yellow packets. It is an integer ranging from 0 to 7.

6.5.6 Creating traffic policy

Create a traffic policy for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**policy-map** *policy-map-name* **Example:** Raisecom(config)#policy-map policy1	Create a traffic policy, and enter traffic policy pmap configuration mode. • policy-map-name: name of the traffic policy, a string of 1 to 16 characters
3	Raisecom(config-pmap)#**description** *string* **Example:** Raisecom(config-pmap)#description this-is-a-test-policy-map	(Optional) configure the description of the traffic policy. • string: description, a string of 1 to 255 characters

Copyright © Raisecom Technology Co., Ltd.

6.5.7 Defining traffic policy mapping

Note

Define one or more defined traffic classes to one traffic policy.

Define traffic policy mapping for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`policy-map`** *`policy-map-name`* **Example:** `Raisecom(config)#policy-map policy1`	Create a traffic policy, and enter traffic policy pmap configuration mode. • policy-map-name: name of the traffic policy, a string of 1 to 16 characters
3	`Raisecom(config-pmap)#`**`class-map`** *`class-map-name`* **Example:** `Raisecom(config-pmap)#class-map class1`	Bind a traffic class with a traffic policy. The traffic policy is applied to the packets matching the traffic class. • class-map-name: name of the traffic class, a string of 1 to 16 characters **Note** At least one rule is required for the traffic class to be bount with a traffic policy, otherwise the binding will fail.

6.5.8 Defining traffic policy operation

Note

Define different operations to different flows in policy.

Define a traffic policy operation for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`policy-map`** *`policy-map-name`* **Example:** `Raisecom(config)#policy-map policy1`	Create a traffic policy, and enter traffic policy pmap configuration mode. • policy-map-name: name of the traffic policy, a string of 1 to 16 characters

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	`Raisecom(config-pmap)#`**`class-map`** *`class-map-name`* **Example:** `Raisecom(config-pmap)#class-map class1`	Bind a traffic class with a traffic policy. The traffic policy is applied to the packets matching the traffic class. • class-map-name: name of the traffic class, a string of 1 to 16 characters **Note** At least one rule is required for the traffic class to be bound with the traffic policy, otherwise the binding will fail.

4	`Raisecom(config-pmap-c)#`**`police`** *`policer-name`* `[` **`hierarchy-police`** *`hierarchy-police-name`* **`mode`** `{` **`and`** `|` **`or`** `}` `]`
	Example:
	`Raisecom(config-pmap-c)#police policer1`
		(Optional) apply the token bucket on traffic policy and conduct rate limiting and shaping.
		• policier-name: name of the traffic policier, a string of 1 to 16 characters
		• hierarchy-police hierarchy-police-name: name of the hierarchical policier, a string of 1 to 16 characters
		• mode: hierarchical token bucket mode
		• and: the hierarchical token bucket mode is and.
		• or: the hierarchical token bucket mode is or.
		Note
		The token bucket needs to be created in advance and be configured with rate limiting and shaping rules. Otherwise, the operation will fail.

5	`Raisecom(config-pmap-c)#`**`redirect-to`** *`interface-type interface-number`* `|` **`next-hop`** *`next-hop-ipaddress`* `}`
	Example:
	`Raisecom(config-pmap-c)#redirect-to gigaethernet 1/1/1`
		(Optional) configure redirection rules under the traffic class, forwarding classified packets from assigned interface.
		• interface-type: interface type
		• interface-number: interface ID. The type and value range depend on the interface type.
		• next-hop next-hop-ipaddress: IP address of the next hop, in dotted decimal notation, such as 10.1.1.1

6	`Raisecom(config-pmap-c)#`**`set`** `{` **`cos`** *`cos-value`* `|` **`dscp`** *`dscp-value`* `|` **`local-priority`** *`value`* `}`
	Example:
	`Raisecom(config-pmap-c)#set cos 5`
		(Optional) configure remarking rules under the traffic class, modify packet CoS, local priority, inner VLAN, DSCP, IP precedence, and VLAN ID.
		• cos-value: new CoS priority. The cos-value is an integer ranging from 0 to 7.
		• dscp-value: new DSCP. The dscp-value is an integer ranging from 0 to 63.
		• value: new local priority. The value is an integer ranging from 0 to 7.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
7	Raisecom(config-pmap-c)#**copy-to-mirror** *group-id* **Example:** Raisecom(config-pmap-c)#copy-to-mirror 1	(Optional) configure traffic mirroring to the monitor interface. • group-id: ID of the port mirroring group, an integer, ranging from 1 to 4
8	Raisecom(config-pmap-c)#**statistics { enable | disable }** **Example:** Raisecom(config-pmap-c)#statistics enable	(Optional) configure traffic statistic rules under the traffic class, statistic packets for the matched traffic class. • enable: enable traffic statistics. • disable: disable traffic statistics.
9	Raisecom(config-pmap-c)#**forward-to-cpu**	(Optional) configure traffic to be forwarded to the CPU.

6.5.9 Applying traffic policy to interfaces

Apply a traffic policy to the interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, VLAN interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config-gigaethernet1/1/port)#**service-policy ingress** *policy-map-name* **Example:** Raisecom(config-gigaethernet1/1/1)#service-policy ingress policy1	Apply the configured traffic policy to the ingress or egress direction of the interface. • policy-map-name: policy name, a string of 1 to 16 characters

6.5.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show service-policy statistics interface** { *interface-type interface-number* | **vlan** *vlan-id* } **ingress** [**class-map** *class-map-name*]	Show statistics about applied traffic policy.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
2	Raisecom#**show service-policy interface** [*interface-type interface-number* [**ingress**] | **vlan** *vlan-id* [**ingress**]]	Show information about the applied traffic policy.
3	Raisecom#**show class-map** [*class-map-name*]	Show information about the traffic class.
4	Raisecom#**show policy-map** [*policy-map-name*]	Show information about traffic policy.
5	Raisecom#**show policy-map** [*policy-map-name*] [**class** *class-map-name*]	Show information about the traffic class in the traffic policy.
6	Raisecom#**show mls qos policer** [*policer-name*]	Show information about the assigned token bucket (rate limiting and shaping).

6.5.11 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
Raisecom(config)#**clear service-policy statistics interface** *interface-type interface-number* **ingress** **Example:** Raisecom(config)#clear service-policy statistics interface gigaethernet 1/1/1 ingress	Clear statistics on QoS packets. • interface-type: interface type • interface-number: interface ID • ingress: clear statistics on traffic policies in the ingress direction of the interface.

6.6 Configuring traffic shaping and rate limiting

6.6.1 Preparing for configurations

Scenario

When the network is congested, you want to restrict burst flow on an interface or VLAN to make packets transmitted at a well-proportioned rate to remove network congestion. In this case, you need to configure rate limiting.

When the rate of the interface on the downstream device is smaller than that of the interface on the upstream device, traffic congestion may occur on the interface on the downstream device. In this case, you can configure traffic shaping in the egress direction of the interface on the upstream device.

Copyright © Raisecom Technology Co., Ltd.

Prerequisite

N/A

6.6.2 Configuring rate limiting based on interface

Configure rate limiting based on interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#rate-limit { ingress | egress } cir cir-value cbs cbs-value`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#rate-limit egress cir 100 cbs 20`
		Configure rate limiting based on interface.
		• egress: rate limiting in the egress direction
		• ingress: rate limiting in the ingress direction
		• cir-value: committed information rate. The cir-value is an integer ranging from 1 to 10485760, in units of kbit/s.
		• cbs-value: committed burst size. The cbs-value is an integer ranging from 1 to 16384, in units of Kbytes.

4	`Raisecom(config)#rate-limit mode { l1 | l2 }`
	Example:
	`Raisecom(config)#rate-limit mode l1`
		Configure the rate limiting mode.
		• l1: physical layer mode
		• l2: data link layer mode

Note

- By default, no interface-based rate limiting is configured.
- Adopt the drop processing mode for packets on the ingress interface if they exceed the configured rate limit.
- When you configure the rate limit and burst for an interface, the burst value should not be much greater if the configured rate limit is smaller than 256 kbit/s. Otherwise, packets may be inconsecutive.
- When the rate limit is too small, we recommend that the burst value is 4 times greater than then rate limit. If packets are inconsecutive, reduce the burst value or increase the rate limit.
- Packets discarded due to rate limiting on the egress interface are included in statistics about packet loss of the ingress interface.

6.6.3 Configuring rate limiting based on VLAN

Configure rate limiting based on VLAN for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface vlan vlan-id`
	Example:
	`Raisecom(config)#interface vlan 1`
		Enter VLAN interface configuration mode.
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094

3	`Raisecom(config-vlan*)#rate-limit ingress cir cir-value cbs cbs-value`
	Example:
	`Raisecom(config-vlan1)#rate-limit ingress cir 100 cbs 20`
		Configure rate limiting based on VLAN.
		• ingress: rate limiting in the ingress direction
		• cir-value: committed information rate. The cir-value is an integer ranging from 1 to 10485760, in units of kbit/s.
		• cbs-value: committed burst size. The cbs-value is an integer ranging from 1 to 16384, in units of Kbyte.

6.6.4 Configuring traffic shaping

Configure traffic shaping for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter VLAN interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#mls qos shaping { ingress | egress } pir pir-value [ pbs pbs-value ]`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#mls qos shaping ingress pir 20 pbs 200`
		Configure traffic shaping on queues of the interface.
		• ingress: traffic shaping in the ingress direction
		• egress: traffic shaping in the egress direction
		• pir pir-value: peak information rate. The pir-value is an integer ranging from 1 to 10485760, in units of kbit/s.
		• pbs pbs-value: peak burst size. The pbs-value is an integer ranging from 1 to 16384, in units of Kbyte.

6.6.5 Checking configurations

Use the following commands to check configuration results.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
1	`Raisecom#show rate-limit interface`	Show configurations of rate limiting on interfaces.
	`Raisecom#show rate-limit interface vlan vlan-id [ ingress ]`	
	`Raisecom#show rate-limit interface interface-type interface-number [ ingress | egress ]`	
2	`Raisecom#show rate-limit mode`	Show the rate limiting mode on the interface.
3	`Raisecom#show mls qos shaping interface [ interface-type interface-number [ ingress | egress ] ]`	Show information about traffic shaping on the interface.

6.7 Bandwidth rate limiting

6.7.1 Introduction

Bandwidth rate limiting is a subfunction of QoS and is more flexible than basic QoS.

Bandwidth rate limiting has the following functions:

- Ingress interface
  - Bandwidth guarantee: bandwidth rate limiting implements the bandwidth service based on interface or flow. It also supports hierarchical bandwidth guarantee and refining bandwidth of different service flows.
  - Awaring: this function determines whether to be aware of packet color when a flow enters the bandwidth-guaranteed interface.
- Egress interface
  - Bandwidth guarantee: bandwidth service based on interface or flow is implemented. Bandwidth rate limiting does not support hierarchical bandwidth guarantee.

Bandwidth guarantee

The bandwidth guarantee function guarantees that the traffic entering the network is within the defined range, and it discards or schedules packets. Bandwidth guarantee can meet users' requirements on service bandwidth, and also protect network resources and carriers' benefits.

By configuring the bandwidth guarantee profile and applying it to an interface, you can mark different flows green, yellow, and red. The ISCOM2600G series switch takes different actions over flows of different colors: forward green flows, schedule yellow flows, and discard red flows.

Hierarchical bandwidth guarantee

Hierarchical bandwidth guarantee is more flexible. You can configure the token bucket action or aggregation token bucket for each flow independently and then configure hierarchical token buckets to limit the sum of multiple flows.

Copyright © Raisecom Technology Co., Ltd.

Color-aware and marking

If enabled with color-aware, the ISCOM2600G series switch is in color-aware status, in which it can identify whether the ingress flow is marked with color. If disabled with color-aware, the ISCOM2600G series switch is in color-blind status, in which it can neglect whether the ingress flow is marked with color, but identify the flow color again.

The function of color marking judges the color of a flow according to Committed Information Rate (CIR), Committed Burst Size (CBS), Excess Information Rate (EIR), and Excess Burst Size (EBS) configured in the bandwidth guarantee profile, and modifies the flag bit to mark it with color according to the packet format defined in IEEE 802.1ad.

6.7.2 Preparing for configurations

Scenario

Bandwidth rate limiting is used to guarantee service bandwidth for users and protect network resources and carriers' profits.

Prerequisite

N/A

6.7.3 Default configurations of bandwidth rate limiting

Default configurations of bandwidth rate limiting are as below.

Function	Default value
Color awaring	Disable

6.7.4 Configuring bandwidth guarantee

Creating bandwidth guarantee profile

Create a bandwidth guarantee profile for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**bandwidth -profile** *bwp-profile-id* **cir** *cir* **cbs** *cbs* [**color-aware**] Raisecom(config)#**bandwidth -profile** *bwp-profile-id* **cir** *cir* **cbs** *cbs* **eir** *eir* **ebs** *ebs* [**color-aware** [**coupling**]] **Example:** Raisecom(config)#bandwidth -profile 1 cir 20 cbs 30 eir 20 ebs 30 color-aware	Create a bandwidth guarantee profile. • bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128 • cir: committed information rate, an integer, ranging from 1 to 10485760, in units of kbit/s • cbs: committed burst size, an integer, ranging from 1 to 262144, in units of Kbyte • eir: excess information rate, an integer, ranging from 1 to 10485760, in units of kbit/s • ebs: excess burst size, an integer, ranging from 1 to 262144, in units of Kbyte • color-aware: packet color identification mode • coupling: bucket coupling
3	Raisecom(config)#**bandwidth -profile** *bwp-profile-id* **description** *word* **Example:** Raisecom(config)#bandwidth -profile 1 description profile1	Configure the description of the bandwidth guarantee profile. • bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128 • word: description, a string of 1–32 characters
4	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
5	Raisecom(config-gigaethernet1/1/port)#**band width ingress** *bwp-profile-id* **Example:** Raisecom(config-gigaethernet1/1/1)#bandwid th ingress 2	Apply the bandwidth guarantee profile on the interface. • ingress: ingress direction • bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128
6	Raisecom(config-gigaethernet1/1/port)#**band width color-aware** { **enable** | **disable** } **Example:** Raisecom(config-gigaethernet1/1/1)#bandwid th color-mode enable	Enable color-aware on packets in the ingress direction of the bandwidth guarantee interface. Use the **disable** form of this command to disable this function. • enable: enable color-aware on packets in the ingress direction of the bandwidth guarantee interface. • disable: disable color-aware on packets in the ingress direction of the bandwidth guarantee interface.

Copyright © Raisecom Technology Co., Ltd.

Configuring bandwidth guarantee based on interface+VLAN

Configure bandwidth guarantee based on interface+VLAN for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#bandwidth-profile` *`bwp-profile-id`* `cir` *`cir`* `cbs` *`cbs`* `[ eir` *`eir`* `ebs` *`ebs`* `] [ color-aware [ coupling ] ]`
	Example:
	`Raisecom(config)#bandwidth-profile 1 cir 20 cbs 30 eir 20 ebs 30 color-aware`
		Create a bandwidth guarantee profile.
		• bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128
		• cir: committed information rate, an integer, ranging from 1 to 10485760, in units of kbit/s
		• cbs: committed burst size, an integer, ranging from 1 to 262144, in units of Kbyte
		• eir: excess information rate, an integer, ranging from 1 to 10485760, in units of kbit/s
		• ebs: excess burst size, an integer, ranging from 1 to 262144, in units of Kbyte
		• color-aware: packet color identification mode
		• coupling: bucket coupling

3	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
4	`Raisecom(config-gigaethernet1/1/port)#bandwidth ingress vlan` *`vlan-id bwp-profile-id`* **Example:** `Raisecom(config-gigaethernet1/1/1)#bandwidth ingress vlan 3 2`	Apply the bandwidth guarantee profile on the interface+VLAN. • ingress: ingress direction • vlan-id: VLAN list, an integer, ranging from 1 to 4094 • bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128

Configuring bandwidth guarantee based on interface+VLAN+CoS

Configure bandwidth guarantee based on interface+VLAN+CoS for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**bandwidth-profile** *bwp-profile-id* **cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**color-aware** [**coupling**]] **Example:** Raisecom(config)#bandwidth-profile 1 cir 20 cbs 30 eir 20 ebs 30 color-aware	Create a bandwidth guarantee profile. • bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128 • cir: committed information rate, an integer, ranging from 1 to 10485760, in units of kbit/s • cbs: committed burst size, an integer, ranging from 1 to 262144, in units of Kbyte • eir: excess information rate, an integer, ranging from 1 to 10485760, in units of kbit/s • ebs: excess burst size, an integer, ranging from 1 to 262144, in units of Kbyte • color-aware: packet color identification mode • coupling: bucket coupling
3	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
4	Raisecom(config-gigaethernet1/1/port)#**bandwidth ingress vlan** *vlan-id* **coslist** *cos-value-list bwp-profile-id* **Example:** Raisecom(config-gigaethernet1/1/1)#bandwidth ingress vlan 3 coslist 1-3 2	Apply the bandwidth guarantee profile on the interface+VLAN+CoS. • ingress: ingress direction • vlan-id: VLAN list, an integer, ranging from 1 to 4094 • cos-value-list: CoS value list, an integer, ranging from 0 to 7. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128

Note

If a bandwidth guarantee profile is used by other profiles or applied, it cannot be deleted.

Configuring bandwidth guarantee based on VLAN interface

Configure bandwidth guarantee based on VLAN interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#bandwidth-profile bwp-profile-id cir cir cbs cbs [ eir eir ebs ebs ] [ color-aware [ coupling ] ]`
	Example:
	`Raisecom(config)#bandwidth-profile 1 cir 20 cbs 30 eir 20 ebs 30 color-aware`
		Create a bandwidth guarantee profile.
		• bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128
		• cir: committed information rate, an integer, ranging from 1 to 10485760, in units of kbit/s
		• cbs: committed burst size, an integer, ranging from 1 to 262144, in units of Kbyte
		• eir: excess information rate, an integer, ranging from 1 to 10485760, in units of kbit/s
		• ebs: excess burst size, an integer, ranging from 1 to 262144, in units of Kbyte
		• color-aware: packet color identification mode
		• coupling: bucket coupling

3	`Raisecom(config)#interface vlan vlan-id`
	Example:
	`Raisecom(config)#interface vlan 1`
		Enter VLAN interface configuration mode.
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094

4	`Raisecom(config-vlan*)#bandwidth ingress bwp-profile-id`
	Example:
	`Raisecom(config-vlan1)#bandwidth ingress 2`
		Apply the bandwidth guarantee profile on the VLAN interface.
		• ingress: ingress direction
		• bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128

5	`Raisecom(config-vlan*)#bandwidth ingress coslist cos-value-list bwp-profile-id`
	Example:
	`Raisecom(config-vlan1)#bandwidth ingress coslist 3 2`
		Apply the bandwidth guarantee profile on the interface+VLAN.
		• ingress: ingress direction
		• cos-value-list: CoS value list, an integer, ranging from 0 to 7. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
		• bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128

6.7.5 Configuring hierarchical bandwidth guarantee

Creating hierarchical CoS bandwidth guarantee

Create a hierarchical CoS bandwidth guarantee for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**bandwidth -profile** *bwp-profile-id* **cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**color-aware** [**coupling**]] **Example:** Raisecom(config)#bandwidth -profile 1 cir 20 cbs 30 eir 20 ebs 30 color-aware	Create a bandwidth guarantee profile. • bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128 • cir: committed information rate, an integer, ranging from 1 to 10485760, in units of kbit/s • cbs: committed burst size, an integer, ranging from 1 to 262144, in units of Kbyte • eir: excess information rate, an integer, ranging from 1 to 10485760, in units of kbit/s • ebs: excess burst size, an integer, ranging from 1 to 262144, in units of Kbyte • color-aware: packet color identification mode • coupling: bucket coupling
3	Raisecom(config)#**hierarchy -cos bandwidth-profile** *hc-profile-id* **Example:** Raisecom(config)#hierarchy -cos bandwidth-profile 3	Create a hierarchical CoS profile, and enter HCoS configuration mode. • hc-profile-id: hierarchical CoS profile ID, an integer, ranging from 1 to 128
4	Raisecom(config-hcos)#**bandwidth coslist** *cos-list bwp-profile-id* Raisecom(config-hcos)#**exit** **Example:** Raisecom(config-hcos)#bandwidth coslist 2 2	Configure the hierarchical CoS profile. • cos-list: CoS list value, an integer, ranging from 0 to 7. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128
5	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
6	Raisecom(config-gigaethernet1/1/port)#**band width ingress vlan** *vlan-id bwp-profile-id* **hierarchy-cos** *hc-profile-id* **Example:** Raisecom(config-gigaethernet1/1/1)#bandwid th ingress vlan 1 2 hierarchy-cos 2	Apply the hierarchical CoS profile on the ingress interface+VLAN. • ingress: ingress direction • vlan-id: VLAN list, an integer, ranging from 1 to 4094 • bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128 • hc-profile-id: hierarchical CoS profile ID, an integer, ranging from 1 to 128

Copyright © Raisecom Technology Co., Ltd.

Configuring hierarchical VLAN bandwidth guarantee

Create a hierarchical VLAN bandwidth guarantee for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#bandwidth-profile bwp-profile-id cir cir cbs cbs [ eir eir ebs ebs ] [ color-aware [ coupling ] ]`
	Example:
	`Raisecom(config)#bandwidth-profile 1 cir 20 cbs 30 eir 20 ebs 30 color-aware`
		Create a bandwidth guarantee profile.
		• bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128
		• cir: committed information rate, an integer, ranging from 1 to 10485760, in units of kbit/s
		• cbs: committed burst size, an integer, ranging from 1 to 262144, in units of Kbyte
		• eir: excess information rate, an integer, ranging from 1 to 10485760, in units of kbit/s
		• ebs: excess burst size, an integer, ranging from 1 to 262144, in units of Kbyte
		• color-aware: packet color identification mode
		• coupling: bucket coupling

3	`Raisecom(config)#hierarchy-vlan bandwidth-profile hv-profile-id`
	Example:
	`Raisecom(config)#hierarchy-vlan bandwidth-profile 4`
		Create a hierarchical VLAN profile, and enter Hvlan configuration mode.
		• hv-profile-id: hierarchical VLAN profile ID, an integer, ranging from 1 to 128

4	`Raisecom(config-hvlan)#bandwidth vlanlist vlan-list profile-id`
	`Raisecom(config-hvlan)#exit`
	Example:
	`Raisecom(config-hvlan)#bandwidth vlanlist 2-4 2`
		Configure the hierarchical VLAN profile.
		• vlan-list: VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
		• bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128

5	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

6	`Raisecom(config-gigaethernet1/1/port)#bandwidth ingress bwp-profile-id hierarchy-vlan hv-profile-id`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#bandwidth ingress 2 hierarchy-vlan 2`
		Apply the hierarchical VLAN profile to the ingress or egress interface.
		• ingress: ingress direction
		• bwp-profile-id: bandwidth guarantee profile ID, an integer, ranging from 1 to 128
		• hv-profile-id: hierarchical VLAN profile ID, an integer, ranging from 1 to 128

Copyright © Raisecom Technology Co., Ltd.

Note

If a hierarchical bandwidth guarantee profile is applied, it cannot be deleted or modified.

6.7.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show bandwidth-profile [ bwp-profile-id ]`	Show information about the bandwidth guarantee profile.
2	`Raisecom#show bandwidth interface interface-type interface-number`	Show information about the bandwidth guarantee profile on the interface.
3	`Raisecom#show hierarchy-cos-bandwidth profile [ hc-profile-id ]`	Show information about the hierarchical CoS bandwidth guarantee profile.
4	`Raisecom#show hierarchy-vlan-bandwidth profile [ hv-profile-id ]`	Show information about the hierarchical VLAN bandwidth guarantee profile.

6.8 Configuration examples

6.8.1 Example for configuring congestion management

Networking requirements

As shown in Figure 6-9, the user uses voice, video and data services.

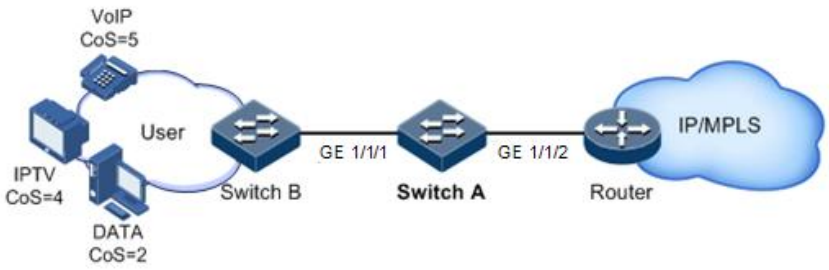
The CoS of voice services is 5, the CoS of video services is 4, and the CoS of data services is 2. The local priorities for these three types of services are mapping 6, 5, and 2 respectively.

Congestion can easily occur on Switch A. To reduce network congestion, make the following rules according to different services types:

- For voice services, perform SP scheduling to assign voice services with a high priority.
- For video services, perform WRR scheduling, with weight of 50.
- For data services, perform WRR scheduling, with weight of 20.

Copyright © Raisecom Technology Co., Ltd.

Figure 6-9 Queue scheduling networking



Configuration steps

Step 1 Configure interface priority trust mode.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#mls qos trust cos
SwitchA(config-gigaethernet1/1/2)#quit
```

Step 2 Configure the profile for mapping from CoS to local priority.

```
SwitchA(config)#mls qos mapping cos-to-local-priority 1
SwitchA(cos-to-pri)#cos 5 to local-priority 6
SwitchA(cos-to-pri)#cos 4 to local-priority 5
SwitchA(cos-to-pri)#cos 2 to local-priority 2
SwitchA(cos-to-pri)#quit
```

Step 3 Apply the profile for mapping from CoS to local priority on GE 1/1/2.

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#mls qos cos-to-local-priority 1
SwitchA(config-gigaethernet1/1/2)#quit
```

Step 4 Conduct SP+WRR queue scheduling in the egress direction of GE 1/1/1.

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#mls qos queue scheduler wrr 1 1 20 1 1
50 0 0
SwitchA(config-gigaethernet1/1/1)#quit
```


Copyright © Raisecom Technology Co., Ltd.

Checking results

Use the following command to show priority trust mode on the interface.

```
Raisecom#show mls qos interface
Interface                 TrustMode  Priority    Cos-PriProfile Dscp-
PriProfile Dscp-Mutation Cos-Remark DEI-Status
---------------------------------------------------------------------
---------------------------------------------
gigaethernet1/1/1          cos      untagged 0   0           0
0          0        --
gigaethernet1/1/2          cos      untagged 0   1           0
0          0        --
```

Use the following command to show configurations of mapping from CoS to local priority

```
Raisecom#show mls qos mapping cos-to-local-priority
G:GREEN
Y:YELLOW
R:RED
cos-to-localpriority(color)
Index Description    Ref   CoS:          0     1     2     3     4
5     6     7
---------------------------------------------------------------------
--------------------------------
1                  1    localpri(color) :0(G)   1(G)   2(G)   3(G)   5(G)
6(G)   6(G)   7(G)
```

Use the following command to show configurations of queue scheduling on the interface.

```
Raisecom#show mls qos queue interface gigaethernet 1/1/1
gigaethernet1/1/1
Queue    Weight(WRR)
-------------------------
  2       1
  3       20
  4       1
  5       1
  6       50
  7       0
  8       0
```


Copyright © Raisecom Technology Co., Ltd.

6.8.2 Example for configuring rate limiting based on traffic policy

Networking requirements

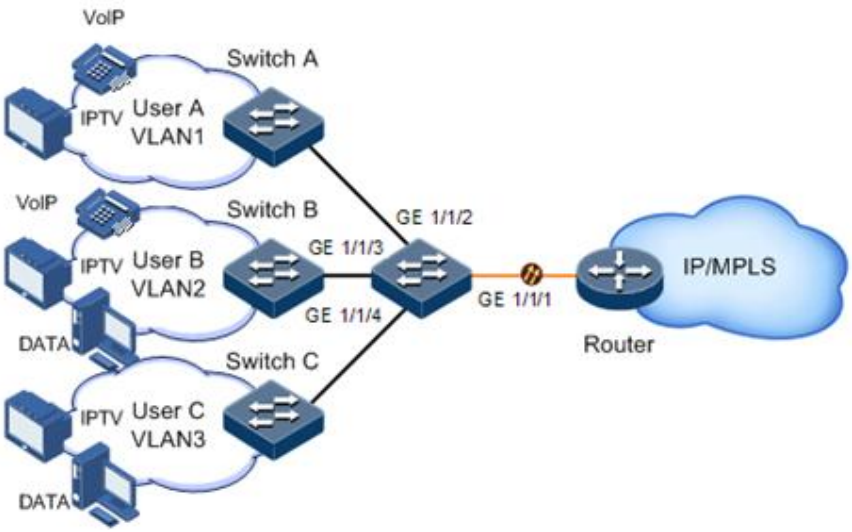
As show in Figure 6-10, User A, User B, and User C respectively belong to VLAN 1, VLAN 2, and VLAN 3, and are connected to the ISCOM2600G series switch by Switch A, Switch B, and Switch C.

User A uses voice and video services, User B uses voice, video and data services, and User C uses video and data services.

According to service requirements, user needs to make rules as below.

- Provide User A with 25 Mbit/s guaranteed bandwidth, permitting burst flow of 100 Kbytes and discarding excess flow.
- Provide User B with 35 Mbit/s guaranteed bandwidth, permitting burst flow of 100 Kbytes and discarding excess flow.
- Provide User C with 30 Mbit/s guaranteed bandwidth, permitting burst flow of 100 Kbytes and discarding excess flow.

Figure 6-10 Rate limiting based on traffic policy



Configuration steps

Step 1 Create and configure the traffic class, and classify users by VLAN ID.

```
Raisecom#config
Raisecom(config)#class-map usera match-any
Raisecom(config-cmap)#match vlan 1
Raisecom(config-cmap)#quit
Raisecom(config)#class-map userb match-any
Raisecom(config-cmap)#match vlan 2
Raisecom(config-cmap)#quit
Raisecom(config)#class-map userc match-any
Raisecom(config-cmap)#match vlan 3
```


Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config-cmap)#quit
```

Step 2 Create rate limiting rules.

```
Raisecom(config)#mls qos policer-profile usera single
Raisecom(traffic-policer)#cir 25000 cbs 100
Raisecom(traffic-policer)#drop-color red
Raisecom(traffic-policer)##quit
Raisecom(config)#mls qos policer-profile userb single
Raisecom(traffic-policer)#cir 35000 cbs 100
Raisecom(traffic-policer)#drop-color red
Raisecom(traffic-policer)##quit
Raisecom(config)#mls qos policer-profile userc single
Raisecom(traffic-policer)#cir 30000 cbs 100
Raisecom(traffic-policer)#drop-color red
Raisecom(traffic-policer)##quit
```

Step 3 Create and configure the traffic policy.

```
Raisecom(config)#policy-map usera
Raisecom(config-pmap)#class-map usera
Raisecom(config-pmap-c)#police usera
Raisecom(config-pmap-c)#quit
Raisecom(config-pmap)#quit
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#service-policy ingress usera
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#policy-map userb
Raisecom(config-pmap)#class-map userb
Raisecom(config-pmap-c)#police userb
Raisecom(config-pmap-c)#quit
Raisecom(config-pmap)#quit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#service-policy ingress userb
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#policy-map userc
Raisecom(config-pmap)#class-map userc
Raisecom(config-pmap-c)#police userc
Raisecom(config-pmap-c)#quit
Raisecom(config-pmap)#quit
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#service-policy userc ingress 4
Raisecom(config-gigaethernet1/1/1)#exit
```

Checking results

Use the **show class-map** command to show configurations of traffic classification.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#show class-map usera
Class Map match-any usera (id 0)(ref 1)
    Match vlan 1
Raisecom#show class-map userb
 Class Map match-any userb (id 1)(ref 1)
    Match vlan 2
Raisecom#show class-map userc
 Class Map match-any userb (id 2)(ref 1)
    Match vlan 3
```

Use the **show mls qos policer** command to show configurations of rate limiting rules.

```
Raisecom(config)#show mls qos policer
single-policer: USERC        mode:flow   color:blind
cir: 30000 kbps  cbs: 100 kB

single-policer: usera        mode:flow   color:blind
cir: 25000 kbps  cbs: 100 kB

single-policer: userb        mode:flow   color:blind
cir: 35000 kbps  cbs: 100 kB
```

Use the **show policy-map** command to show configurations of traffic policy.

```
Raisecom(config)#show policy-map
  Policy Map usera
    Class usera
        police usera

  Policy Map userb
    Class userb
        police userb

  Policy Map userc
    Class userc
        police userc
```

6.8.3 Example for configuring rate limiting based on interface

Networking requirements

As shown in Figure 6-11, User A, User B, and User C are respectively connected to the ISCOM2600G series switch by Switch A, Switch B, and Switch C.

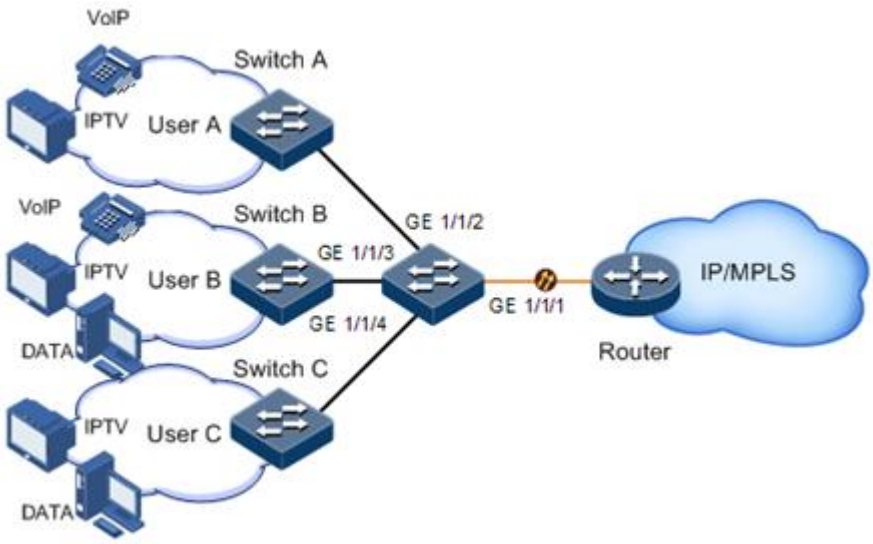
User A uses voice and video services. User B uses voice, video and data services. User C uses video and data services.

According to service requirements, make rules as below.

Copyright © Raisecom Technology Co., Ltd.

- Provide User A with 25 Mbit/s guaranteed bandwidth, permitting burst flow of 100 Kbytes and discarding excess flow.
- Provide User B with 35 Mbit/s guaranteed bandwidth, permitting burst flow of 100 Kbytes and discarding excess flow.
- Provide User C with 30 Mbit/s guaranteed bandwidth, permitting burst flow of 100 Kbytes and discarding excess flow.

Figure 6-11 Rate limiting based on interface



Configuration steps

Configure rate limiting based on interface.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#rate-limit ingress cir 25000 cbs 100
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#rate-limit ingress cir 35000 cbs 100
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#rate-limit ingress cir 30000 cbs 100
Raisecom(config-gigaethernet1/1/3)#exit
```

Checking results

Use the **show rate-limit port-list** command to show configurations of rate limiting based on interface.

```
Raisecom(config)#show rate-limit interface
Interface            Direction Cir(kbps)        Cbs(kb)
CirOper(kbps)         CbsOper(kb)
```

```
-----------------------------------------------------------------------
---------------------------------------
gigaethernet1/1/1     ingress   25000           100           25024
101
gigaethernet1/1/2     ingress   35000           100           30016
101
gigaethernet1/1/3     ingress   30000           100           30016
101
```


Copyright © Raisecom Technology Co., Ltd.

7 Multicast

This chapter describes basic principles and configuration procedures for multicast, and provides related configuration examples, including the following sections:

- Multicast
- Basic functions of Layer 2 multicast
- IGMP Snooping
- IGMP Querier
- IGMP MVR
- IGMP filtering
- Multicast VLAN copy

7.1 Multicast

With the continuous development of Internet, more and more interactive data, voice, and video of various types emerge on the network. On the other hand, the emerging e-commerce, online meetings, online auctions, video on demand, remote learning, and other services also rise gradually. These services bring higher requirements on network bandwidth, information security, and paid feature. Traditional unicast and broadcast cannot meet these requirements well, while multicast has met them timely.

Multicast is a point-to-multipoint data transmission method. The method can effectively solve the single point sending and multipoint receiving problems. During transmission of packets on the network, multicast can save network resources and improve information security.

Comparison among unicast, broadcast, and multicast

Multicast is a kind of packets transmission method which is parallel with unicast and broadcast.

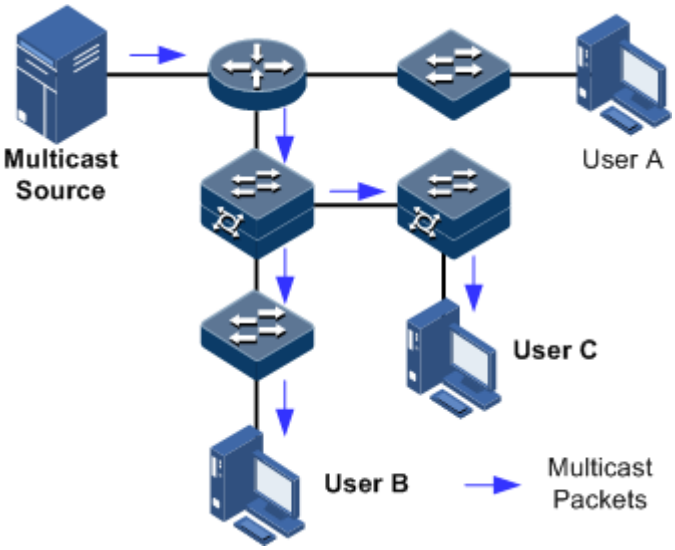
- Unicast: the system establishes a data transmission path for each user who needs the information, and sends separate copy information about them. Through unicast, the amount of information transmitted over the network is proportional to the number of users, so when the number of users becomes huge, there will be more identical information on the network. In this case, bandwidth will become a bottleneck, and unicast will not be conducive to transmission of large-scale information.

Copyright © Raisecom Technology Co., Ltd.

- Broadcast: the system sends information to all users regardless of whether they need or not, so any user will receive it. Through broadcast, the information source delivers information to all users in the segment, which fails to guarantee information security and paid service. In addition, when the number of users who require this kind of information decreases, the utilization of network resources will be very low, and the bandwidth will be wasted seriously.
- Multicast: when some users in the network need specific information, the sender only sends one piece of information, then the transmitted information can be reproduced and distributed in fork junction as far as possible.

As shown in Figure 7-1, assume that User B and User C need information, you can use multicast transmission to combine User B and User C to a receiver set, then the information source just needs to send one piece of information. Each switch on the network will establish their multicast forwarding table according to IGMP packets, and finally transmits the information to the actual receiver User B and User C.

Figure 7-1 Multicast transmission networking



In summary, the unicast is for a network with sparse users and broadcast is for a network with dense users. When the number of users in the network is uncertain, unicast and broadcast will present low efficiency. When the number of users are doubled and redoubled, the multicast mode does not need to increase backbone bandwidth, but sends information to the user in need. These advantages of multicast make itself become a hotspot in study of the current network technology.

Advantages and application of multicast

Compared with unicast and broadcast, multicast has the following advantages:

- Improve efficiency: reduce network traffic, relieve server and CPU load.
- Optimize performance: reduce redundant traffic and guarantee information security.
- Support distributed applications: solve the problem of point-point data transmission.

The multicast technology is used in the following aspects:

- Multimedia and streaming media, such as, network television, network radio, and realtime video/audio conferencing

Copyright © Raisecom Technology Co., Ltd.

- Training, cooperative operations communications, such as: distance education, telemedicine
- Data warehousing and financial applications (stock)
- Any other point-to-multipoint applications

Basic concepts in multicast

- Multicast group

A multicast group refers to the recipient set using the same IP multicast address identification. Any user host (or other receiving device) will become a member of the group after joining the multicast group. They can identify and receive multicast data with the destination address as IP multicast address.

- Multicast group members

Each host joining a multicast group will become a member of the multicast group. Multicast group members are dynamic, and hosts can join or leave multicast group at any time. Group members may be widely distributed in any part of the network.

- Multicast source

A multicast source refers to a server which regards multicast group address as the destination address to send IP packet. A multicast source can send data to multiple multicast groups; multiple multicast sources can send to a multicast group.

- Multicast router

A multicast router is a router that supports Layer 3 multicast. The multicast router can achieve multicast routing and guide multicast packet forwarding, and provide multicast group member management to distal segment connecting with users.

- Routed interface

A routed interface refers to the interface towards the multicast router between a multicast router and a host. The ISCOM2600G series switch receives multicast packets from this interface.

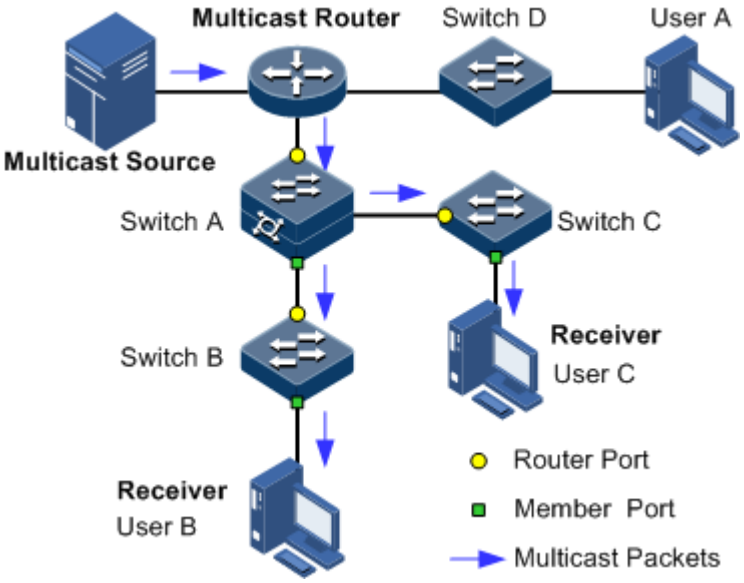
- Member interface

Known as the Rx interface, a member interface is the interface towards the host between multicast router and the host. The ISCOM2600G series switch sends multicast packets from this interface.

Figure 7-2 shows basic concepts in multicast.

Copyright © Raisecom Technology Co., Ltd.

Figure 7-2 Basic concepts in multicast



Multicast address

To make multicast source and multicast group members communicate across the Internet, you need to provide network layer multicast address and link layer multicast address, namely, the IP multicast address and multicast MAC address.

- IP multicast address

Internet Assigned Numbers Authority (IANA) assigns Class D address space to IPv4 multicast; the IPv4 multicast address ranges from 224.0.0.0 to 239.255.255.255.

- Multicast MAC address

When the Ethernet transmits unicast IP packets, it uses the MAC address of the receiver as the destination MAC address. However, when multicast packets are transmitted, the destination is no longer a specific receiver, but a group with an uncertain number of members, so the Ethernet needs to use the multicast MAC address.

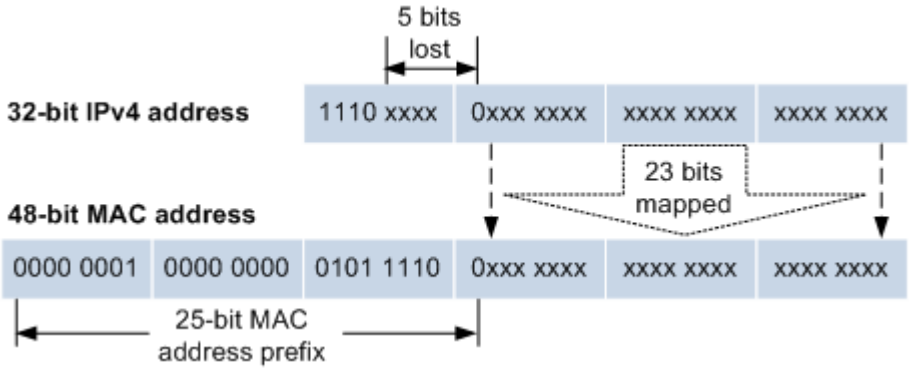
The multicast MAC address identifies receivers of the same multicast group on the link layer.

According to IANA, high bit 24 of the multicast MAC address are 0x01005E, bit 25 is fixed to 0, and the low bit 23 corresponds to low bit 23 of the IPv4 multicast address.

Figure 7-3 shows mapping between the IPv4 multicast address and MAC address.

Copyright © Raisecom Technology Co., Ltd.

Figure 7-3 Mapping between IPv4 multicast address and multicast MAC address



The first 4 bits of IP multicast address are 1110, indicating multicast identification. In the last 28 bits, only 23 bits are mapped to the multicast MAC address, and the missing of 5 bits makes 32 IP multicast addresses mapped to the same multicast MAC address. Therefore, in Layer 2, the ISCOM2600G series switch may receive extra data besides IPv4 multicast group, and these extra multicast data needs to be filtered by the upper layer on the ISCOM2600G series switch.

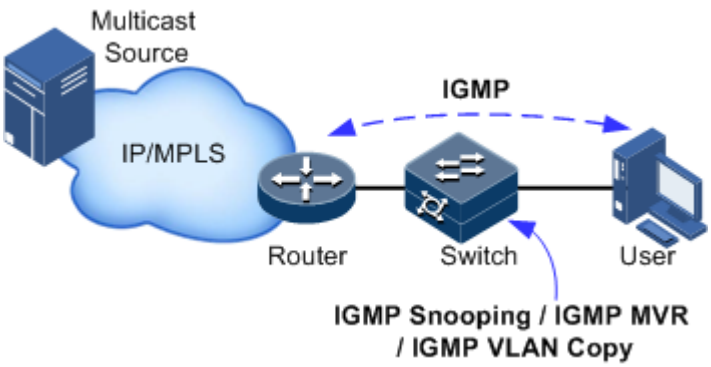
Basis of multicast protocol

To implement complete set of multicast services, you need to deploy a variety of multicast protocols in various positions of network and make them cooperate with each other.

Typically, IP multicast working at network layer is called Layer 3 multicast, so the corresponding multicast protocol is called Layer 3 multicast protocol, including Internet Group Management Protocol (IGMP). IP multicast working at data link layer is called Layer 2 multicast, so the corresponding multicast protocol is called Layer 2 multicast protocol, including Internet Group Management Protocol (IGMP) Snooping.

Figure 7-4 shows operating of IGMP and Layer 2 multicast features.

Figure 7-4 Operating of IGMP and Layer 2 multicast features



IGMP, a protocol in TCP/IP protocol suite, is responsible for managing IPv4 multicast members. IGMP runs between the multicast router and host, defines the establishment and maintenance mechanism of multicast group membership between hosts and the multicast router. IGMP is not involved in transmission and maintenance of group membership between multicast routers, which is completed by the multicast routing protocol.

Copyright © Raisecom Technology Co., Ltd.

IGMP manages group members through interaction of IGMP packets between the host and multicast router. IGMP packets are encapsulated in IP packets, including Query packets, Report packets, and Leave packets. Basic functions of IGMP are as below:

- The host sends Report packets to join the multicast group, sends Leave packets to leave the multicast group, and automatically determines which multicast group packets to receive.
- The multicast router sends Query packets periodically, and receives Report packets and Leave packets from hosts to understand the multicast group members in connected segment. The multicast data will be forwarded to the segment if there are multicast group members, and not forward if there are no multicast group members.

Up to now, IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3. The newer version is fully compatible with the older version. Currently the most widely used version is IGMPv2, while IGMPv1 does not support the Leave packet.

Layer 2 multicast runs on Layer 2 devices between the host and multicast router.

Layer 2 multicast manages and controls multicast groups by monitoring and analyzing IGMP packets exchanged between hosts and multicast routers to implement forwarding multicast data at Layer 2 and suppress multicast data diffusion at Layer 2.

Supported multicast features

The ISCOM2600G series switch supports the following multicast features:

- Basic functions of IGMP
- IGMP Snooping
- IGMP Multicast VLAN Registration (MVR)
- IGMP filtering

Note

- Any two of IGMP Snooping, IGMP MVR, and multicast VLAN copy cannot be concurrently enabled in the same multicast VLAN. Multicast VLAN copy and IGMP MVR cannot be enabled concurrently in the same multicast group of the same multicast VLAN.
- The ISCOM2600G series switch supports IGMPv2 and IGMPv3.

7.2 Basic functions of Layer 2 multicast

7.2.1 Introduction

Basic IGMP functions are as below:

- Assign the multicast router interface.
- Enable immediate leave.
- Configure multicast forwarding entries and the aging time of router interfaces.
- Enable IGMP ring network forwarding.

Basic functions of Layer 2 multicast provide Layer 2 multicast common features, which must be used on the ISCOM2600G series switch enabled with IGMP Snooping or IGMP MVR.

Copyright © Raisecom Technology Co., Ltd.

Note

Configurations of basic function take effect on IGMP Snooping or IGMP MVR concurrently.

The concepts related to IGMP basic functions are as below.

Multicast router interface

The router interface can be learnt dynamically (learnt through IGMP query packets, on the condition that the multicast routing protocol is enabled on multicast routers) on Layer 2 multicast switch, or configured manually to forward downstream multicast report and leave packets to the router interface.

The router interface learnt dynamically has an aging time, while the router interface configured manually will not be aged.

Aging time

The configured aging time takes effect on both multicast forwarding entries and the router interface.

On Layer 2 switch running multicast function, each router interface learnt dynamically starts a timer, of which the expiration time is the aging time of IGMP Snooping. The router interface will be deleted if no IGMP Query packets are received in the aging time. The timer of the router interface will be updated when an IGMP Query packet is received.

Each multicast entry starts a timer, namely, the aging time of a multicast member. The expiration time is IGMP Snooping aging time. The multicast member will be deleted if no IGMP Report packets are received in the aging time. Update timeout for multicast entry when receiving IGMP Report packets. The timer of the multicast entry will be updated when an IGMP Report packet is received.

Immediate leave

On Layer 2 switch running multicast function, the system will not delete the corresponding multicast entry immediately, but wait until the entry is aged after sending Leave packets. You can enable this function to delete the corresponding multicast entry quickly when there are a large number of downstream users and adding or leaving is more frequently required.

Note

IGMPv2/v3 supports immediate leave.

IGMP ring network forwarding

On Layer 2 switch running multicast function, IGMP ring network forwarding can be enabled on any type of interfaces.

Enabling IGMP ring network forwarding can implement multicast backup protection on the ring network, make multicast services more stable, and prevent link failure from causing multicast service failure.

IGMP ring network forwarding can be applied to the RRPS ring, STP/RSTP/MSTP ring, and G.8032 ring.

Copyright © Raisecom Technology Co., Ltd.

7.2.2 Preparing for configurations

Scenario

Basic functions of Layer 2 multicast provide common features of Layer 2 multicast, and must be used on the ISCOM2600G series switch enabled with IGMP Snooping or IGMP MVR.

Prerequisite

- Disable IGMP MVR and multicast VLAN copy in the Snooping multicast VLAN.
- Add related interfaces to VLANs.

7.2.3 Default configurations of Layer 2 multicast basic functions

Default configurations of Layer 2 multicast basic functions are as below.

Function	Default value
IGMP immediate leave status	Disable
Aging time of multicast entries	260s
Interface IGMP ring network forwarding status	Disable

7.2.4 Configuring basic functions of Layer 2 multicast

Configure basic functions of Layer 2 multicast for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`igmp mrouter vlan`** *`vlan-id interface-type interface-number`* **Example:** `Raisecom(config)#igmp mrouter vlan 10 gigaethernet 1/1/1`	(Optional) configure the multicast router interface. • vlan-id: ID of the VLAN to which the specified multicast router interface attached, an integer, ranging from 1 to 4094 • interface-type: interface type • interface-number: interface ID
3	`Raisecom(config)#`**`igmp member-timeout {`** *`seconds`* **`| infinite }`** **Example:** `Raisecom(config)#igmp member-timeout 100`	(Optional) configure the aging time of IGMP members. • seconds: start time, in units of minute, an integer, ranging from 5 to 3600 • infinite: never aged
4	`Raisecom(config)#`**`igmp ring`** *`interface-type interface-number-list`* **Example:** `Raisecom(config)#igmp ring gigaethernet 1/1/1`	(Optional) enable IGMP ring network forwarding on the interface. • interface-type: interface type • interface-number: interface ID

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	`Raisecom(config)#igmp report-suppression`	(Optional) enable Report suppression.

6	`Raisecom(config)#igmp version { 2 | 3 }`
	Example:
	`Raisecom(config)#igmp version 3`
		(Optional) configure the IGMP version.
		• 2|3: IGMP version
		– 2 refers to version 2.
		– 3 refers to version 3.

7	`Raisecom(config)#igmp snooping mrouter vlan vlan-list priority priority-number`
	Example:
	`Raisecom(config)#igmp snooping mrouter vlan 1 priority 1`
		(Optional) configure the CoS priority of the IGMP route VLAN.
		• vlan-list: VLAN of the multicast router interface, an integer, ranging from 1 to 4094. It supports specific values, such as "2,3,4"; it also supports a range, such as "2-4".
		• priority-number: CoS priority, an integer, ranging from 0 to 7

8	`Raisecom(config)#igmp unknown forward-router`	(Optional) enable the function of forwarding unknown IGMP multicast packets to the router interface. Use the **no** form of this command to disable this function.
9	`Raisecom(config)#igmp forward-router`	(Optional) enable the function of forwarding known IGMP multicast packets to the router interface. Use the **no** form of this command to disable this function.

10	`Raisecom(config-gigaethernet1/1/port)#igmp immediate-leave vlan [ vlan vlan-list | user-mac ]`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#igmp immediate-leave vlan 100`
		(Optional) configure immediate leave.
		If immediate leave is disabled on the downlink interface, the router interface, after receiving a Leave packet, will calculate the aging time according to robust factor and configure the expiration time for a member to leave the group as Group Membership Interval (GMI). GMI = robust - value*lastmember - queryinterval.
		• vlan-list: VLAN of the multicast router interface, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
		• user-mac: MAC address based on user

7.2.5 Checking configurations

Use the following commands to check configuration results.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
1	Raisecom#**show igmp configuration**	Show IGMP basic configurations.
2	Raisecom#**show igmp mrouter**	Show configurations of the multicast route interface.
3	Raisecom#**show igmp immediate-leave** [*interface-type interface-number*]	Show configuration of immediate leave on Layer 2 multicast.
4	Raisecom#**show igmp statistics** [*interface-type interface-number*]	Show Layer 2 multicast statistics.
5	Raisecom#**show igmp snooping mrouter vlan-priority**	Show the CoS priority of the IGMP route VLAN.
6	Raisecom#**show igmp ring**	Show information about the IGMP ring network.
7	Raisecom#**show igmp user-mac** [*interface-type interface-number* | **user-vlan** *vlan-id*]	Show information about user MAC addresses of IGMP.
8	Raisecom#**show igmp user-mac count** [*interface-type interface-number* | **vlan** *vlan-id*]	Show the number of user MAC addresses of IGMP.

7.2.6 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
Raisecom(config)#**clear igmp statistics** [*interface-type interface-number*] **Example:** Raisecom(config)#clear igmp statistics	Clear statistics about Layer 2 multicast IGMP. • interface-type: interface type • interface-number: interface ID
Raisecom(config)#**no igmp member** *interface-type interface-number* **Example:** Raisecom(config)#no igmp member gigaethernet 1/1/1	Delete a specified multicast entry. • interface-type: interface type • interface-number: interface ID

7.3 IGMP Snooping

7.3.1 Introduction

IGMP Snooping is a multicast constraining mechanism running on Layer 2 devices, used for managing and controlling multicast groups, and implementing Layer 2 multicast.

IGMP Snooping allows the ISCOM2600G series switch to monitor IGMP sessions between the host and multicast router. When monitoring the IGMP Report packet from the host to a

Copyright © Raisecom Technology Co., Ltd.

group, the ISCOM2600G series switch will add host-related interface to the forwarding entry of this group. Similarly, when a forwarding entry reaches the aging time, the ISCOM2600G series switch will delete host-related interface from the forwarding table.

IGMP Snooping forwards multicast data through Layer 2 multicast entry. When receiving multicast data, the ISCOM2600G series switch will forward them directly according to the corresponding receiving interface of the multicast entry, instead of flooding them to all interfaces, to save bandwidth of the ISCOM2600G series switch effectively.

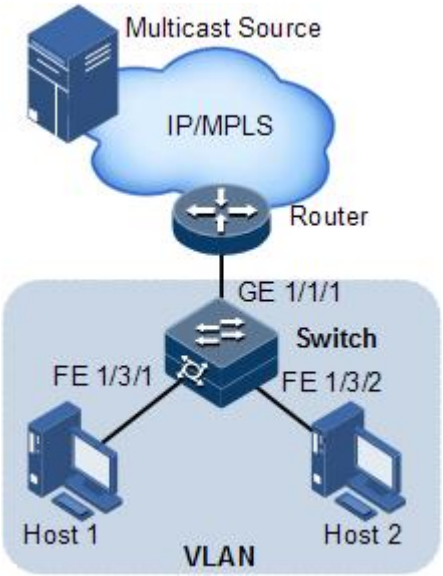
IGMP Snooping establishes a Layer 2 multicast forwarding table, of which entries can be learnt dynamically or configured manually.

7.3.2 Preparing for configurations

Scenario

As shown in Figure 7-5, multiple hosts belonging to a VLAN receive data from the multicast source. You can enable IGMP Snooping on the Switch that connects the multicast router and hosts. By listening IGMP packets transmitted between the multicast router and hosts, creating and maintaining the multicast forwarding table, you can implement Layer 2 multicast.

Figure 7-5 IGMP Snooping networking



Prerequisite

- Disable multicast VLAN copy on the ISCOM2600G series switch.
- Create VLANs.
- Add related interfaces to the VLANs.

7.3.3 Default configurations of IGMP Snooping

Default configurations of IGMP Snooping are as below.

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
Global IGMP Snooping status	Disable
VLAN IGMP Snooping status	Disable
IGMP robustness	2

7.3.4 Configuring IGMP Snooping

Configure IGMP Snooping for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`igmp snooping`**	Enable global IGMP Snooping.
3	`Raisecom(config)#`**`igmp member-timeout {`** *`seconds`* **`| infinite }`** **Example:** `Raisecom(config)#igmp member-timeout 100`	(Optional) configure the aging time of IGMP members. • seconds: timeout, in units of second, an integer, ranging from 5 to 3600 • infinite: never aged
4	`Raisecom(config)#`**`igmp snooping vlan`** *`vlan-list`* **Example:** `Raisecom(config)#igmp snooping vlan 2-3`	(Optional) enable IGMP Snooping on all VLANs. • vlan-list: VLAN enabled with IGMP Snooping, an integer, ranging from 1 to 4094. It supports specific values, such as "2,3,4"; it also supports a range, such as "2-4".
5	`Raisecom(config)#`**`vlan`** *`vlan-id`* **Example:** `Raisecom(config)#vlan 2`	Enter VLAN configuration mode.
6	`Raisecom(config-vlan)#`**`igmp snooping static`** *`ip-address interface-type interface-number`* **Example:** `Raisecom(config-vlan)#igmp snooping static 224.0.1.10 gigaethernet 1/1/1`	(Optional) configure static members of IGMP Snooping in VLAN mode. • ip-address: multicast group address, multicast IP address, with IPv4 ranging from 224.0.1.0 to 239.255.255.255 • interface-type: interface type • interface-number: interface ID
7	`Raisecom(config)#`**`interface`** *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical layer configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

8	`Raisecom(config-gigaethernet1/1/port)#igmp snooping host-join group-address vlan vlan-id`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#igmp snooping host-join 224.0.1.10 vlan 2`
		Configure the host joining function.
		• group-address: multicast group member IP address, in dotted decimal notation
		• vlan-id: VLAN enabled with IGMP Snooping, an integer, ranging from 1 to 4094

Note

- IGMP Snooping and IGMP MVR cannot be enabled concurrently in the same multicast VLAN. Otherwise, the configuration will fail.
- IGMP Snooping and multicast VLAN copy cannot be enabled concurrently in the same multicast VLAN. Otherwise, the configuration will fail.

7.3.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show igmp snooping`	Show configurations of IGMP Snooping.
2	`Raisecom#show igmp snooping member [ interface-type interface-number | vlan vlan-id ]`	Show information about multicast group members of IGMP Snooping.
3	`Raisecom#show igmp snooping member count [ interface-type interface-number | vlan vlan-id ]`	Show the number of multicast group members of IGMP Snooping.
4	`Raisecom#show igmp snooping vlan vlan-id`	Show configurations of IGMP Snooping in the specified VLAN.

7.3.6 Example for applying multicast on ring network

Networking requirements

Configure IGMP ring forwarding on single Ethernet ring to make multicast service more stable and prevent multicast service from being disrupted by link failure.

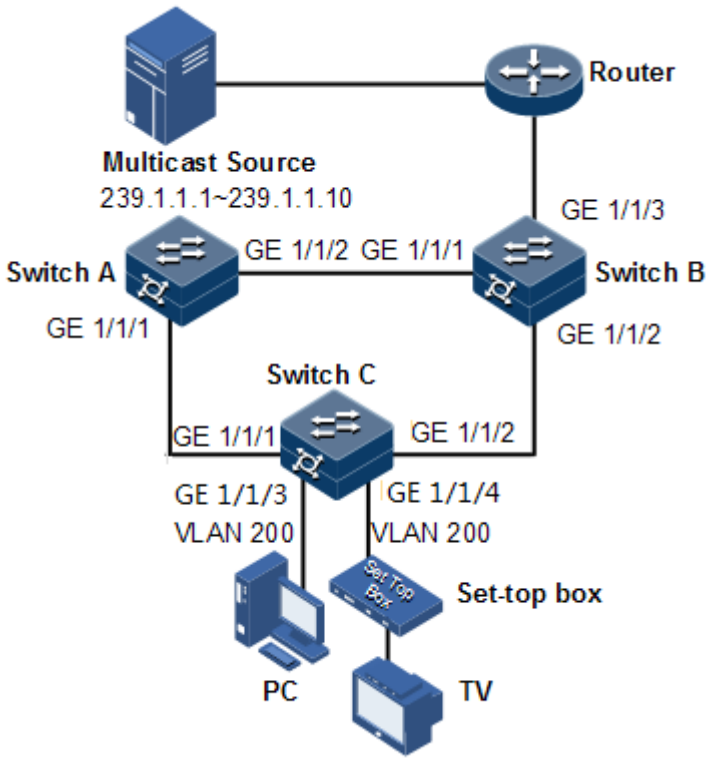
As shown in Figure 7-6, GE 1/1/1 and GE 1/1/2 on Switch A, GE 1/1/1 and GE 1/1/2 on Switch B, GE 1/1/1 and GE 1/1/2 on Switch C form a physical ring. Multicast traffic is input from GE 1/1/1 on Switch B. The customer demands multicast traffic through GE 1/1/3 and GE 1/1/4 on Switch C. This networking does not affect the customer's on-demand multicast traffic whichever link fails on the switch.

When using single Ethernet ring to provide multicast services, you can adopt IGMP MVR or IGMP Snooping to receive the multicast traffic.

Copyright © Raisecom Technology Co., Ltd.

The following example shows that STP provides ring network detection and IGMP Snooping provides multicast function.

Figure 7-6 Ring network multicast networking



Configuration steps

Step 1 Enable STP, create a VLAN, and add interfaces to the VLAN.

Configure Switch A.

```
SwitchA#config
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree mode stp
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk native vlan 200
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#switchport trunk native vlan 200
```

Configure Switch B.

```
SwitchB#config
```

```
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree mode stp
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#switchport trunk native vlan 200
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#switchport trunk native vlan 200
```

Configure Switch C.

```
SwitchC#config
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree mode stp
SwitchC(config)#interface gigaethernet 1/1/1
SwitchC(config-gigaethernet1/1/1)#switchport mode trunk
SwitchC(config-gigaethernet1/1/1)#switchport trunk native vlan 200
SwitchC(config-gigaethernet1/1/1)#exit
SwitchC(config)#interface gigaethernet 1/1/2
SwitchC(config-gigaethernet1/1/2)#switchport mode trunk
SwitchC(config-gigaethernet1/1/2)#switchport trunk native vlan 200
```

Step 2 Enable IGMP Snooping and IGMP ring network forwarding on the interface.

Configure Switch A.

```
SwitchA(config)#igmp ring gigaethernet 1/1/1
SwitchA(config)#igmp ring gigaethernet 1/1/2
SwitchA(config)#igmp snooping
SwitchA(config)#igmp snooping vlan 200
```

Configure Switch B.

```
SwitchB(config)#igmp ring gigaethernet 1/1/1
SwitchB(config)#igmp ring gigaethernet 1/1/2
SwitchB(config)#igmp snooping
SwitchB(config)#igmp snooping vlan 200
```

Configure Switch C.

```
SwitchC(config)#igmp ring gigaethernet 1/1/1
SwitchC(config)#igmp ring gigaethernet 1/1/2
SwitchC(config)#igmp snooping
```


Copyright © Raisecom Technology Co., Ltd.

Checking results

Disconnect any link in the ring, and check whether the multicast flow can be received normally.

7.4 IGMP Querier

7.4.1 Introduction

MVR Querier is an MVR protocol proxy mechanism. It runs on Layer 2 devices to assist in managing and controlling multicast groups. MVR Querier will terminate IGMP packets. It can agent host functions upstream and also proxy multicast router functions downstream. The Layer 2 network device enabled with MVR Querier has two roles:

- At the user side, it is a query builder and undertakes the role of the server, sending Query packets and periodically checking user information, and processing the Report and Leave packets from users.
- At the network routing side, it is a host and undertakes the role of the client, responding the multicast router Query packet and sending Report and Leave packets. It sends the user information to the network as required.

The proxy mechanism can control and access user information effectively, and reduce the network side protocol packet and network load.

IGMP Querier establishes a multicast packet forwarding list by intercepting IGMP packets between the user and multicast routers.

Note

IGMP Querier is used in cooperation with IGMP Snooping/MVR.

The following concepts are related to IGMP Querier.

- IGMP packet suppression

IGMP packet suppression means that the switch filters identical Report packets. When receiving multiple Report packets from a multicast group member in a query interval, the switch sends the first Report packet to the multicast router only while it suppresses other identical Report packets, to reduce packet quantity on the network.

Note

When IGMP Snooping, IGMP MVR, or multicast VLAN copy is enabled, IGMP packet suppression can be enabled or disabled respectively.

- IGMP Querier

If a switch is enabled with this function, it can actively send IGMP Query packets to query information about multicast members on the interface. If it is disabled with this function, it only forwards IGMP Query packets from routers.

Note

When IGMP Snooping, IGMP MVR, or multicast VLAN copy is enabled, IGMP Querier can be enabled or disabled respectively.

Copyright © Raisecom Technology Co., Ltd.

- Source IP address of Query packets sent by IGMP Querier

IGMP querier sends the source IP address of Query packets. By default, the IP address of IP interface 0 is used. If the IP address is not configured, 0.0.0.0 is used. When receiving Query packets with IP address of 0.0.0.0, some hosts take it illegal and do not respond. Thus, specifying the IP address for the Query packet is recommended.

- Query interval

It is the query interval for common groups. The query message of common group is periodically sent by the switch in multicast mode to all hosts in the shared network segment, to query which multicast groups have members.

- Maximum response time for Query packets

The maximum response time for Query packets is used to control the deadline for reporting member relations by a host. When the host receives Query packets, it starts a timer for each added multicast group. The value of the timer is between 0 and maximum response time. When the timer expires, the host sends the Report packet to the multicast group.

- Interval for the last member to send Query packets

It is also called the specified group query interval. It is the interval for the switch continues to send Query packets for the specified group when receiving IGMP Leave packet for a specified group by a host.

The Query packet for the specified multicast group is sent to query whether the group has members on the interface. If yes, the members must send Report packets within the maximum response time; after the switch receives Report packets in a specie period, it continues to maintain multicast forwarding entries of the group; If the members fail to send Report packets within the maximum response time, the switch judges that the last member of the multicast group has left and thus deletes multicast forwarding entries.

7.4.2 Preparing for configurations

Scenario

On a network with multicast routing protocol widely applied, multiple hosts and client subnets receive multicast information. Enable IGMP Querier on the switch connecting the multicast router and hosts to block IGMP packets between hosts and the multicast router and relieve the network load.

Configure IGMP Querier to relieve configuration and management of client subnet for the multicast router and to implement multicast connection with the client subnet.

IGMP Querier is used in cooperation with IGMP Snooping/MVR.

Prerequisite

- Create VLANs.
- Add related interfaces to VLANs.

7.4.3 Default configurations of IGMP Querier

Default configurations of IGMP Querier area as below.

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
IGMP Querier status	Disable
IGMP packet suppression status	Disable
Source IP address for IGMP Querier to send packets	Use the IP address of IP address 0. If IP interface 0 is not configured, use 0.0.0.0.
IGMP query interval	125s
Maximum response time to send Query packets	10s
Interval for the last member to send Query packets	1s

7.4.4 Configuring IGMP Querier

Configure IGMP Querier for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp querier`	Enable IGMP Querier.
3	`Raisecom(config)#igmp source-ip` *`ip-address`* **Example:** `Raisecom(config)#igmp source-ip 10.0.0.1`	(Optional) configure the source IP address for the IGMP querier to send Query packets. • ip-address: source IP address, in dotted decimal notation, such as 10.0.0.1
4	`Raisecom(config)#igmp query-interval` *`period`* **Example:** `Raisecom(config)#igmp query-interval 20`	(Optional) configure the IGMP query interval. • period: interval for general groups to send Query packets, an integer, ranging from 10 to 3600, in units of second
5	`Raisecom(config)#igmp query-max-response-time` *`period`* **Example:** `Raisecom(config)#igmp query-max-response-time 20`	(Optional) configure the maximum response time to send Query packets. • period: maximum response time for general groups to send Query packets, an integer, ranging from 1 to 25, in units of second
6	`Raisecom(config)#igmp last-member-query-interval` *`period`* **Example:** `Raisecom(config)#igmp last-member-query-interval 10`	(Optional) configure the interval for the last member to send Query packets. • period: specified interval, an integer, ranging from 1 to 25, in units of second
7	`Raisecom(config)#igmp proxy`	Configure IGMP proxy.

Copyright © Raisecom Technology Co., Ltd.

Note

- When IGMP Querier is disabled, the following parameters can be configured: source IP address, query interval, maximum response time to send Query packets, and interval for the last member to send Query packets. After IGMP Querier is enabled, these configurations will take effect immediately.
- Though IGMP Snooping or IGMP MVR is enabled, IGMP Querier can be still enabled.
- IGMP Proxy and IGMP Querier are mutually exclusive. IGMP Proxy and IGMP report suppression are mutually exclusive.

7.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show igmp querier`	Show configurations of IGMP Querier.

7.4.6 Example for configuring IGMP Snooping and IGMP Querier

Networking requirements

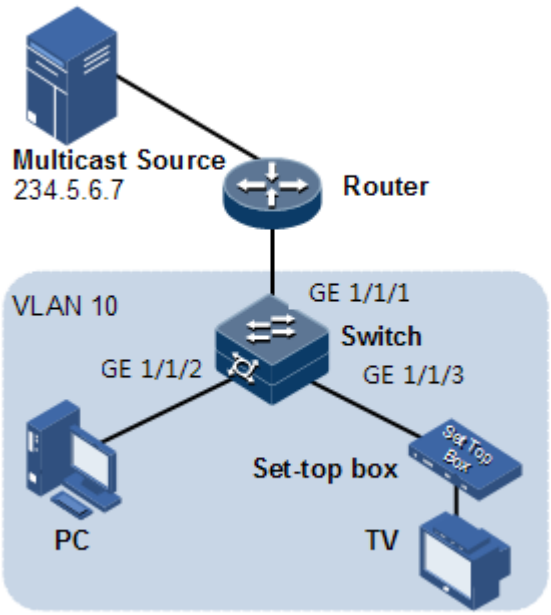
As shown in Figure 7-7, GE 1/1/1 on the switch is connected to the multicast router; GE 1/1/2 and GE 1/1/3 are connected to users. All multicast users belong to the same VLAN 10; you need to configure IGMP Snooping on the switch to receive multicast data with the address 234.5.6.7.

Enable the IGMP Querier on the switch to reduce communication between the hosts and multicast routers and implement the multicast function.

When the PC and set-top box are added to the same multicast group, the switch receives two IGMP Report packets and only sends one of them to the multicast router. The IGMP Query packet sent by the multicast router is not forwarded downstream, but the switch periodically sends IGMP Query packets.

Copyright © Raisecom Technology Co., Ltd.

Figure 7-7 IGMP Snooping networking



Configuration steps

Step 1 Create VLANs and add interfaces to VLANs.

```
Raisecom#config
Raisecom(config)#create vlan 10 active
Raisecom(config)#interface gigaethernet  1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#switchport trunk native vlan 10
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#switchport access vlan 10
Raisecom(config-gigaethernet1/1/3)#exit
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport access vlan 10
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 2 Enable IGMP Snooping.

```
Raisecom(config)#igmp snooping
Raisecom(config)#igmp snooping vlan 10
```

Step 3 Configure IGMP Querier.

```
Raisecom(config)#igmp querier
Raisecom(config)#igmp source-ip 192.168.1.2
```


Copyright © Raisecom Technology Co., Ltd.

Checking results

Use the following command to show configurations of IGMP Snooping.

```
Raisecom#show igmp snooping
  IGMP snooping              :Enable
  IGMP report-suppression      :Disable
  IGMP version               :v2
  IGMP snooping active vlan    :10
  IGMP aging-time(s)          :260
  IGMP ring                  :--
```

Use the following command to show information about IGMP Snooping multicast group members.

```
Raisecom#show igmp snooping member vlan 10
R- ring port   D - Dynamic   S - Static
Vlan   Group                                Port       Live-time(s)  Flag
-----------------------------------------------------------------------
10    234.5.6.7                             GE1/1/1          --
D
```

Use the following command to show configurations of IGMP Querier.

```
Raisecom#show igmp querier
Global IGMP querier configuration:
----------------------------------
Querier Status               : Enable
Querier Source Ip            : 192.168.1.2
Query Interval(s)            :125
Query Max Response Interval(s)  :10
Last Member Query Interval(s)   :1
Robust Count                :2
Next General Query(s)         :--
```

7.5 IGMP MVR

7.5.1 Introduction

IGMP Multicast VLAN Registration (MVR) is multicast constraining mechanism running on Layer 2 devices, used for multicast group management and control and achieve Layer 2 multicast.

IGMP MVR adds member interfaces belonging to different user VLAN in switch to multicast VLAN by configuring multicast VLAN and makes different VLAN user uses one common

Copyright © Raisecom Technology Co., Ltd.

multicast VLAN, then the multicast data will be transmitted only in one multicast VLAN without copying one for each user VLAN, thus saving bandwidth. At the same time, multicast VLAN and user VLAN are completely isolated which also increases the security.

Both IGMP MVR and IGMP Snooping can implement Layer 2 multicast, but the difference is that the multicast VLAN in IGMP Snooping is the same as the customer VLAN while the multicast VLAN in IGMP MVR can be different from the customer VLAN.

Note

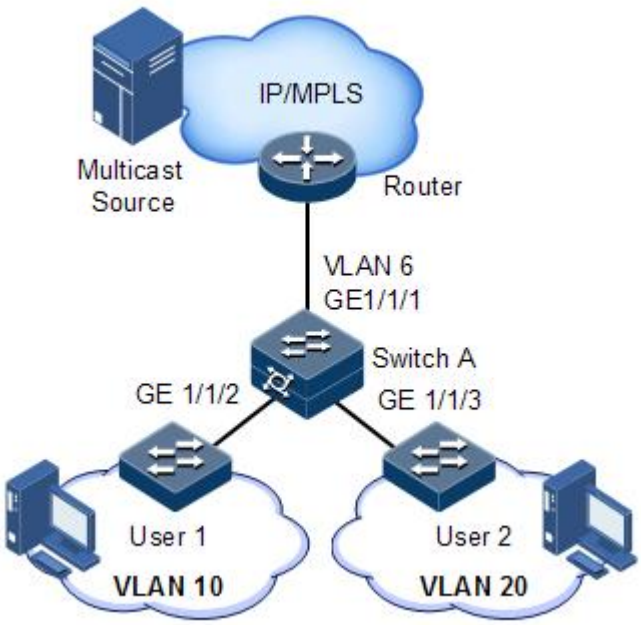
One switch can configure up to 10 multicast VLAN, at least one multicast VLAN and group addresses. The supported maximum number of multicast groups is 1024.

7.5.2 Preparing for configurations

Scenario

As shown in Figure 7-8, multiple users receive data from the multicast source. These users and the multicast router belong to different VLAN. Enable IGMP MVR on Switch A, and configure multicast VLAN. In this way, users in different VLAN can share a multicast VLAN to receive the same multicast data, and bandwidth waste is reduced.

Figure 7-8 IGMP MVR networking



Prerequisite

- Disable multicast VLAN copy.
- Create VLANs.
- Add related interfaces to the VLANs.

Copyright © Raisecom Technology Co., Ltd.

7.5.3 Default configurations of IGMP MVR

Default configurations of MVR are as below.

Function	Default value
Global IGMP MVR status	Disable
Interface IGMP MVR status	Disable
Multicast VLAN and group address set	N/A

7.5.4 Configuring IGMP MVR

Configure IGMP MVR for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`igmp mvr`**	Enable global IGMP MVR.

3	`Raisecom(config)#`**`igmp mvr mcast-vlan`** *`vlan-id`* **`group`** `{` *`start-ip-address`* `[` *`end-ip-address`* `] |` **`any`** `}`
	Example:
	`Raisecom(config)#igmp mvr mcast-vlan 10 group 224.0.1.1 224.0.1.10`
		Configure the group address set for multicast VLAN.
		• vlan-id: multicast VLAN, VLAN to which the multicast routing interface is attached, an integer, ranging from 1 to 4094
		• group: configure the multicast source group address contained in multicast VLAN.
		• start-ip-address: start IP multicast address, in dotted decimal notation, ranging from 224.0.0.1 to 239.255.255.255
		• end-ip-address: end IP multicast address, in dotted decimal notation, ranging from 224.0.0.1 to 239.255.255.255
		• any: any multicast address
		Note
		After IGMP MVR is enabled, you need to configure multicast VLAN and bind group address set. If the received IGMP Report packet does not belong to a group address set of any VLAN, it is not processed and the user cannot make multicast traffic on demand.

4	`Raisecom(config)#`**`interface`** *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config-gigaethernet1/1/port)#**igmp mvr mcast-vlan** *vlan-id* **static** *ip-address* **[user-vlan** *vlan-id* **]** **Example:** Raisecom(config-gigaethernet1/1/1)#igmp mvr mcast-vlan 2 static 224.0.1.1 user-vlan 10	(Optional) configure static multicast members of MVR for a specified customer VLAN. • vlan-id: multicast VLAN, VLAN to which the multicast router interface belongs, an integer, ranging from 1 to 4094 • ip-address: IP multicast address, in dotted decimal notation, ranging from 224.0.0.1 to 239.255.255.255 • user-vlan vlan-id: user VLAN, an integer, ranging from 1 to 4094
6	Raisecom(config-gigaethernet1/1/port)#**igmp mvr user-vlan** *vlan-id* **Example:** Raisecom(config-gigaethernet1/1/1)#igmp mvr user-vlan 1	(Optional) configure the range for multicast inter-VLAN copy to take effect. • vlan-id: user VLAN, an integer, ranging from 1 to 4094
7	Raisecom(config-gigaethernet1/1/port)#**igmp mvr mcast-vlan** *vlan-id* **host-join** *ip-address* **[user-vlan** *vlan-id* **]** **Example:** Raisecom(config-gigaethernet1/1/1)#igmp mvr mcast-vlan 2 host-join 224.0.1.1	(Optional) configure the host joining function of MVR. • mcast-vlan vlan-id: multicast VLAN, an integer, ranging from 1 to 4094 • ip-address: IP multicast address, in dotted decimal notation, ranging from 224.0.0.1 to 239.255.255.255 • user-vlan vlan-id: user VLAN, an integer, ranging from 1 to 4094

Note

- IGMP Snooping and IGMP MVR cannot be enabled concurrently in the same multicast VLAN. Otherwise, the configuration will fail.
- IGMP Snooping and multicast VLAN copy cannot be enabled concurrently in the same multicast VLAN. Otherwise, the configuration will fail.

7.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show igmp mvr**	Show configurations of IGMP MVR.
2	Raisecom#**show igmp mvr** { **interface** | *interface-type interface-number* }	Show configurations of IGMP MVR on the specified interface.
3	Raisecom#**show igmp mvr member** [*interface-type interface-number* | **user-vlan** *vlan-id*]	Show information about multicast group members of IGMP MVR.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
4	`Raisecom#show igmp mvr member count [ interface-type interface-number | user-vlan vlan-id ]`	Show the number of multicast group members of IGMP MVR.
5	`Raisecom#show igmp mvr vlan-group [ mcast-vlan vlan-id ]`	Show multicast VLAN and its group address set.

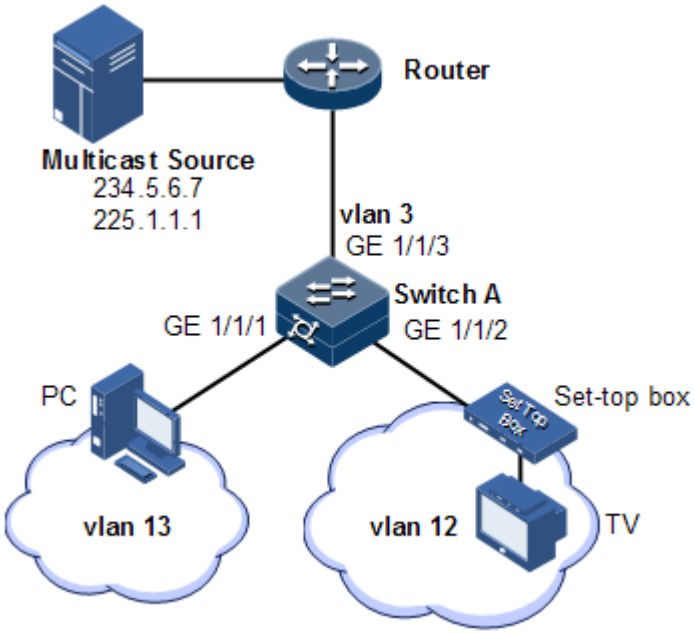
7.5.6 Example for configuring IGMP MVR

Networking requirements

As shown in Figure 7-9, GE 1/1/1 on Switch A connects with the multicast router, and GE 1/1/2 and GE 1/1/3 connect with users in different VLANs to receive data from multicast addresses 234.5.6.7 and 225.1.1.1.

Configure IGMP MVR on Switch A to specify VLAN 3 as a multicast VLAN, and then the multicast data needs to be duplicated with one copy in the multicast VLAN instead of copying for each customer VLAN, thus saving bandwidth.

Figure 7-9 MVR networking



Configuration steps

Step 1 Create VLANs on Switch A and add interfaces to them.

```
Raisecom(config)#config
Raisecom(config)#create vlan 3,12,13 active
```


Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan 13
Raisecom(config-gigaethernet1/1/1)#switchport trunk untagged vlan 12
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#switchport trunk native vlan 12
Raisecom(config-gigaethernet1/1/2)#switchport trunk untagged vlan 13
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#switchport mode trunk
Raisecom(config-gigaethernet1/1/3)#switchport trunk native vlan 3
Raisecom(config-gigaethernet1/1/3)#switchport trunk untagged vlan 12,13
Raisecom(config-gigaethernet1/1/3)#exit
```

Step 2 Configure IGMP MVR on Switch A.

```
Raisecom(config)#igmp mvr
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#igmp mvr
Raisecom(config-gigaethernet1/1/1)#igmp mvr user-vlan 13
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#igmp mvr
Raisecom(config-gigaethernet1/1/2)#igmp mvr user-vlan 12
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#igmp mvr mcast-vlan 3 group 234.5.6.7
Raisecom(config)#igmp mvr mcast-vlan 3 group 225.1.1.1
```

Checking results

Use the following command to show IGMP MVR configurations on Switch A.

```
Raisecom#show igmp mvr
igmp mvr running             :Enable
igmp mvr port               :GE1/1/1 GE1/1/2
igmp mvr multicast vlan(ref)   :3(2)
igmp aging time(s)           :260
igmp ring                   :--
```

Use the following command to show information about the multicast VLAN and group address.

```
Raisecom#show igmp mvr vlan-group
----------------------------------------------------
Raisecom(config)#show igmp mvr vlan-group
```


Copyright © Raisecom Technology Co., Ltd.

```
Mcast-vlan     Start-group    End-group
-------------------------------------------
3            225.1.1.1      225.1.1.1
3            234.5.6.7      234.5.6.7
```

7.6 IGMP filtering

7.6.1 Introduction

To control user access, you can configure IGMP filtering. IGMP filtering includes limiting the range of accessible multicast groups by using the filtering profile and limiting the maximum number of multicast groups.

- IGMP filtering profile

To ensure information security, the administrator needs to limit the multicast users, such as what multicast data are allowed to receive and what are not.

You can configure IGMP Profile filtering profile to control the interface. One IGMP Profile can be configured one or more multicast group access control restrictions and access the multicast group according to the restriction rules (**permit** and **deny**). If a rejected IGMP Profile filtering profile is applied to the interface, the interface will discard the IGMP report packet from this group directly once receiving it and disallow the interface to receive this group of multicast data.

IGMP filtering profile can be configured on an interface or interface+VLAN.

IGMP Profile only applies to dynamic multicast groups, but not static ones.

- Limit to the maximum number of multicast groups

You can configure the maximum number of multicast groups allowed to join based on interface or interface+VLAN and the rules to restrict the maximum number.

The maximum group number rule defines the actions to be taken for reaching the maximum number of multicast groups jointed by users, namely, disallowing new users to join the multicast group or overriding a joined group.

Note

IGMP filtering is generally used with IGMP Snooping/IGMP MVR/multicast VLAN copy.

7.6.2 Preparing for configurations

Scenario

Different users in the same multicast group receive different multicast requirements and permissions. You can configure filtering rules on the switch which connects the multicast router and user host to restrict multicast users. You also can configure the maximum number of multicast groups jointed by users. IGMP Proxy is generally used with IGMP Snooping or IGMP MVR.

Copyright © Raisecom Technology Co., Ltd.

Prerequisite

- Create VLANs.
- Add related interfaces to the VLANs.

7.6.3 Default configurations of IGMP filtering

Default configurations of IGMP filtering are as below.

Function	Default value
Global IGMP filtering	Disable
IGMP filtering profile Profile	N/A
IGMP filtering profile action	Refuse
IGMP filtering under interface	No maximum group limit, the largest group action is drop, no application filtering profile
IGMP filtering under interface+VLAN	No maximum group limit, the largest group action is drop, no application filtering profile

7.6.4 Enabling global IGMP filtering

Enable global IGMP filtering for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode
2	`Raisecom(config)#igmp filter`	Enable global IGMP filtering

Note

When configuring IGMP filtering profile or the maximum group number, use the **igmp filter** command to enable global IGMP filtering.

7.6.5 Configuring IGMP filtering profile

The IGMP filtering profile can be used to interface or interface+VLAN.

Configure the IGMP filtering profile for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#igmp filter profile profile-number`
	Example:
	`Raisecom(config)#igmp filter profile 1`
		Create IGMP Profile and enter Profile configuration mode.
		• profile-number: number of the filtering profile, an integer, ranging from 1 to 100

3	`Raisecom(config-igmp-profile)#{ permit | deny }`
	Example:
	`Raisecom(config-igmp-profile)#permit`
		Configure the IGMP Profile action.
		• permit: permit users to receive data from the filtered multicast address.
		• deny: deny users to receive data from the filtered multicast address.

4	`Raisecom(config-igmp-profile)#range range-id start-ip-address [ end-ip-address ]`
	Example:
	`Raisecom(config-igmp-profile)#range 1 224.0.1.1 224.0.10.1`
		Configure the IP multicast address or rang under access control.
		• range-id: index number of the specified multicast address range, an integer, ranging from 1 to 10
		• start-ip-address: start IP address of the multicast address range, in dotted decimal notation, within the range of multicast address, ranging from 224.0.0.1 to 239.255.255.255
		• end-ip-address: end IP address of the multicast address range, in dotted decimal notation, within the range of multicast address, ranging from 224.0.0.1 to 239.255.255.255. If this parameter is not selected, the filtered address is a multicast address, namely, the start-ip-address, instead of an address range.

5	`Raisecom(config-igmp-profile)#exit`
	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
	`Raisecom(config)#interface port-channel 1`
		Enter physical interface configuration mode or aggregation group configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

6	`Raisecom(config-gigaethernet1/1/port)#igmp filter profile profile-number [ vlan vlan-list ]`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#igmp filter profile 1`
		Configure IGMP Profile filtering profile to physical interface or interface+VLAN.
		• profile-number: number of the filtering profile, an integer, ranging from 1 to 100
		• vlan-list: specified VLAN, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". If this parameter is selected, the IGMP filtering profile will be applied to interface+VLAN. If this parameter is not selected, the IGMP filtering profile will be applied to interface.

	`Raisecom(config-port-channel*)#igmp filter profile profile-number [ vlan vlan-list ]`
	`Raisecom(config-port-channel*)#exit`
	Example:
	`Raisecom(config-port-channel1)#igmp filter profile 1`
		Configure IGMP Profile filtering profile to LAG interface or interface+VLAN.
		• profile-number: number of the filtering profile, an integer, ranging from 1 to 100
		• vlan-list: specified VLAN, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". If this parameter is selected, the IGMP filtering profile is applied to interface+VLAN. If this parameter is not selected, the IGMP filtering profile is applied to interface.

7	`Raisecom(config-gigaethernet1/1/port)#igmp drop { query | report }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#igmp drop query`
		(Optional) enable IGMP to filter query packets from the user interface or join or leave packets from the upstream interface.
		• query: query packets
		• report: join packets

Note

Use the **igmp filter profile** *profile-number* command in interface configuration mode to make the created IGMP profile apply to the specified interface. One IGMP profile can be applied to multiple interfaces, but each interface can have only one IGMP profile.

7.6.6 Configuring maximum number of multicast groups

You can add the maximum number of multicast groups applied to interface or interface+VLAN.

Configure the maximum number of multicast groups for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode

2	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*
	`Example:`
	`Raisecom(config)#interface gigaethernet 1/1/1`
	`Raisecom(config)#interface port-channel 1`
		Enter physical interface configuration mode or aggregation group configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#`**`igmp filter max-groups`** *`group-number`* `[` **`vlan`** *`vlan-list`* `]`
	`Example:`
	`Raisecom(config-gigaethernet1/1/1)#igmp filter max-groups 10`
		Configure the maximum number of multicast groups to physical interface or interface+VLAN.
		• group-number: maximum number of multicast groups, an integer, ranging from 1 to 1024
		• vlan-list: specified VLAN, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". If this parameter is selected, the maximum number of multicast groups allowed to join based on interface+VLAN is configured. If this parameter is not selected, the maximum number of multicast groups allowed to join based on interface is configured.

	`Raisecom(config-port-channel*)#`**`igmp filter max-groups`** *`group-number`* `[` **`vlan`** *`vlan-list`* `]`
	`Example:`
	`Raisecom(config-port-channel1)#igmp filter max-groups 10`
		Configure the maximum number of multicast groups to LAG interface or interface+VLAN.
		• group-number: maximum number of multicast groups, an integer, ranging from 1 to 1024
		• vlan-list: specified VLAN, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". If this parameter is selected, the maximum number of multicast groups allowed to join based on interface+VLAN is configured. If this parameter is not selected, the maximum number of multicast groups allowed to join based on interface is configured.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-gigaethernet1/1/port)#**igmp filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*] **Example:** Raisecom(config-gigaethernet1/1/1)#igmp filter max-groups action drop vlan 10	(Optional) configure the action upon reach of the maximum number of multicast groups in physical interface or interface+VLAN. • drop: new multicast groups are not allowed to be added to the interface or interface+VLAN. • replace: the multicast group with the shortest Time-to-leave time overrides the new multicast group. • vlan-list: specified VLAN, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". If this parameter is selected, the action upon reach of the maximum number of multicast groups allowed to join based on interface+VLAN is configured. If this parameter is not selected, the action upon reach of the maximum number of multicast groups allowed to join based on interface is configured.
	Raisecom(config-port-channel*)#**igmp filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*] **Example:** Raisecom(config-port-channel1)#igmp filter max-groups action drop vlan 10	(Optional) configure the action upon reach of the maximum number of multicast groups in LAG interface or interface+VLAN. • drop: new multicast groups are not allowed to be added to the interface or interface+VLAN. • replace: the multicast group with the shortest Time-to-leave time overrides the new multicast group. • vlan-list: specified VLAN, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". If this parameter is selected, the action upon reach of the maximum number of multicast groups allowed to join based on interface+VLAN is configured. If this parameter is not selected, the action upon reach of the maximum number of multicast groups allowed to join based on interface is configured.

7.6.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show igmp filter** [{ **interface** | *interface-type interface-number* } [**vlan** [*vlan-id*]]]	Show configurations of IGMP filtering.
2	Raisecom#**show igmp filter profile** [*profile-number*]	Show information about the IGMP profile.

Copyright © Raisecom Technology Co., Ltd.

7.6.8 Example for applying IGMP filtering on interface

Networking requirements

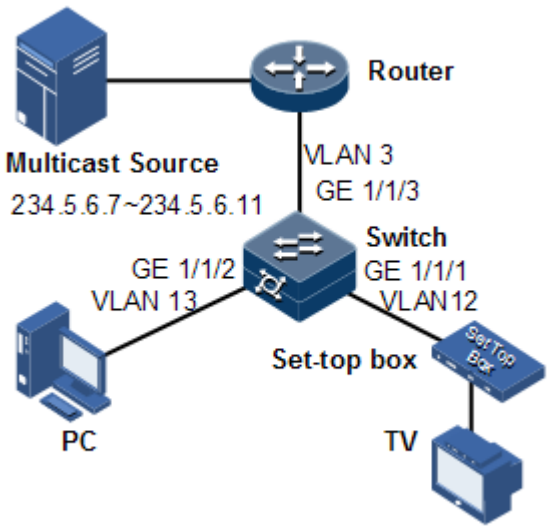
Enable IGMP filtering on the switch. Add filtering rules on the interface to filter multicast users.

As shown in Figure 7-10,

- Create an IGMP filtering rule Profile 1, and configure the action to pass for the multicast group ranging from 234.5.6.7 to 234.5.6.10.
- Apply filtering rule on GE 1/1/1, allow the STB to join the 234.5.6.7 multicast group, forbid it to join the 234.5.6.11 multicast group.
- Apply no filtering rule on Port 3, and allow PCs to join the 234.5.6.11 multicast group.

Configure the maximum number of multicast groups on GE 1/1/1. After the STB is added to the 234.5.6.7 multicast group, add it to the 234.5.6.8 multicast group while it quits the 234.5.6.7 multicast group.

Figure 7-10 Applying IGMP filtering on interface



Configuration steps

Step 1 Create VLANs, and add interfaces to VLANs.

```
Raisecom#config
Raisecom(config)#create vlan 3,12,13 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan 12
Raisecom(config-gigaethernet1/1/1)#switchport trunk untagged vlan 3
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
```


Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#switchport trunk native vlan 13
Raisecom(config-gigaethernet1/1/2)#switchport trunk untagged vlan 3
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#switchport mode trunk
Raisecom(config-gigaethernet1/1/3)#switchport trunk native vlan 3
Raisecom(config-gigaethernet1/1/3)#switchport trunk untagged vlan 12,13
Raisecom(config-gigaethernet1/1/3)#exit
```

Step 2 Enable IGMP MVR.

```
Raisecom(config)#igmp mvr
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#igmp mvr
Raisecom(config-tengigabitethernet1/1/1)#igmp mvr user-vlan 12
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#igmp mvr
Raisecom(config-tengigabitethernet1/1/2)#igmp mvr user-vlan 13
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#igmp mvr mcast-vlan 3 group any
```

Step 3 Configure the IGMP filtering profile.

```
Raisecom(config)#igmp filter profile 1
Raisecom(config-igmp-profile)#permit
Raisecom(config-igmp-profile)#range 1 234.5.6.7 234.5.6.10
Raisecom(config-igmp-profile)#exit
```

Step 4 Configure the STB to apply the IGMP filtering profile.

```
Raisecom(config)#igmp filter
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#igmp filter profile 1
```

Step 5 Configure the maximum number of multicast groups on the STB interface.

```
Raisecom(config-gigaethernet1/1/1)#igmp filter max-groups 1
Raisecom(config-gigaethernet1/1/1)#igmp filter max-groups action replace
```


Copyright © Raisecom Technology Co., Ltd.

Checking results

Use the following command to show configurations of IGMP filtering on the interface.

```
Raisecom#show igmp filter gigaethernet 1/1/1
profile:  1
max group:      1
current group:  0
action:       replace
```

7.7 Multicast VLAN copy

7.7.1 Introduction

Multicast VLAN copy refers to specifying different VLANs as one user VLAN of the multicast VLAN when different user VLANs require the same multicast source on the switch. After multicast VLAN copy is enabled, the upper layer device copies multicast data in the multicast VLAN, instead of copying multicast data for each user VLAN, thus saving bandwidth. The system searches for the egress interface according to the multicast VLAN and multicast group address, and copies multicast data for each user VLAN on the egress interface.

Both multicast VLAN copy and IGMP MVR can implement multicast functions when user VLANs and the multicast VLAN are in different VLANs. Their difference is that multicast data of IGMP MVR can be forwarded in a multicast VLAN but multicast VLAN copy is used to copy multicast data to each user VLAN.

IGMP MVR transmits data in a way as shown in Figure 7-11 while multicast VLAN copy transmits data in a way as shown in Figure 7-12.

Copyright © Raisecom Technology Co., Ltd.

Figure 7-11 Data transmission of IGMP MVR

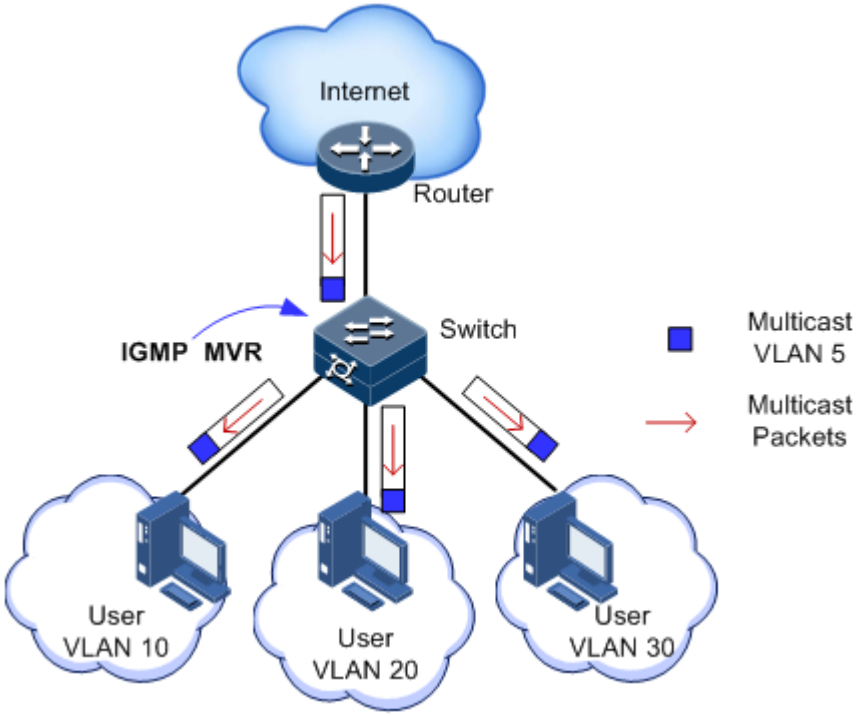
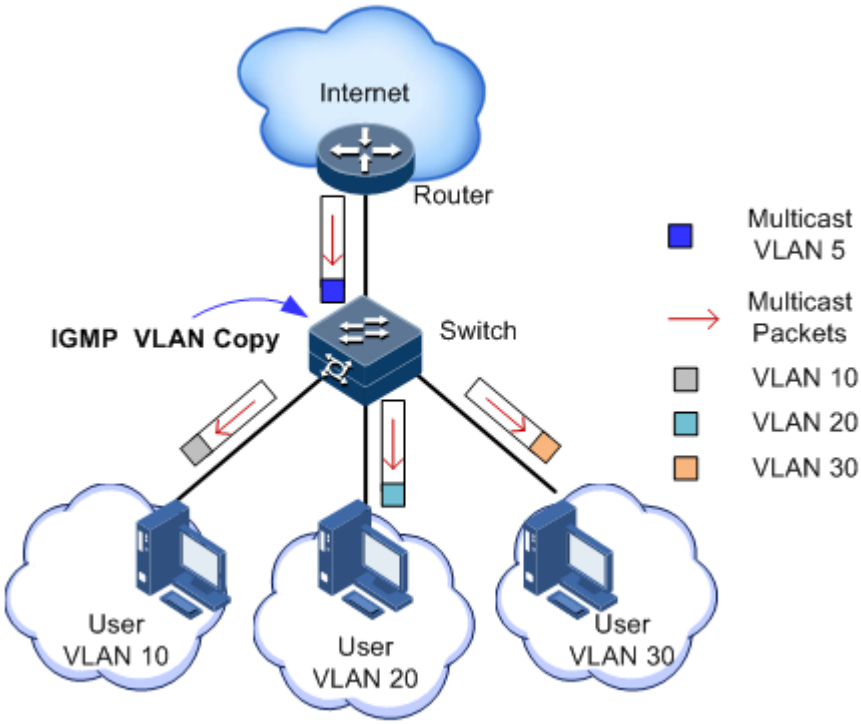


Figure 7-12 Data transmission of multicast VLAN copy



Note

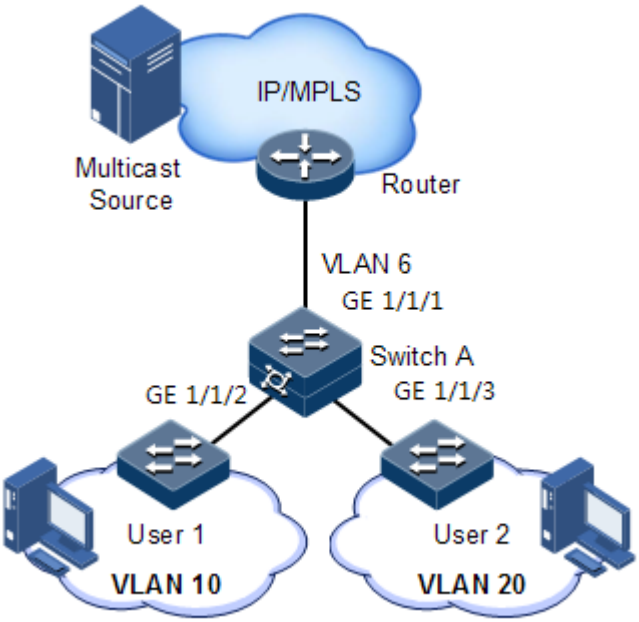
The ISCOM2600G series switch can be configured with 1–10 multicast VLANs and at least one multicast VLAN and corresponding group address set. It supports up to 1024 multicast groups.

7.7.2 Preparing for configurations

Scenario

As shown in Figure 7-13, multiple hosts belonging to different VLANs receive data of the multicast source. Enable multicast VLAN copy on Switch B and configure multicast VLAN so that multicast data is copied on the receiving interface to the user VLAN and users of different VLANs can share a multicast VLAN to receive the same multicast data and reduce waste of bandwidth.

Figure 7-13 Multicast VLAN copy networking



Prerequisite

Create VLANs, and add related interfaces to VLANs.

7.7.3 Default configurations of multicast VLAN copy

Default configurations of multicast VLAN copy are as below.

Function	Default value
Global multicast VLAN copy status	Disable
Interface multicast VLAN copy status	Disable

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
Multicast VLAN and group address set	N/A

Note

- To concurrently configure N:1 VLAN mapping and VLAN copy, you must configure VLAN copy and then configure N:1 VLAN mapping.
- To concurrently configure N:1 VLAN mapping and PIM, you must configure PIM and then configure N:1 VLAN mapping.

7.7.4 Configuring multicast VLAN copy

Configure multicast VLAN copy for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp vlan-copy`	Enable global multicast VLAN copy.

3	`Raisecom(config)#igmp vlan-copy mcast-vlan vlan-id group { start-ip [ end-ip ] | any }`
	Example:
	`Raisecom(config)#igmp vlan-copy mcast-vlan 10 group 224.0.1.1 224.0.1.10`
		Configure the group address set of the multicast VLAN.
		• vlan-id: multicast VLAN, an integer, ranging from 1 to 4094, namely, the VLAN from the multicast route interface
		• group: multicast source group address of multicast VLAN
		• start-ip: start IP multicast address, in dotted decimal notation, ranging from 224.0.0.1 to 239.255.255.255
		• end-ip: end IP multicast address, in dotted decimal notation, ranging from 224.0.0.1 to 239.255.255.255
		• any: any multicast address
		Note
		After multicast VLAN copy is enabled, you need to configure the multicast VLAN and bound group address set. If the received IGMP Report packet does not belong to a group address set of any VLAN, it is not processed and the user cannot make multicast traffic on demand.

4	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	`Raisecom(config-gigaethernet1/1/port)#igmp vlan-copy`	Enable multicast VLAN copy in interface configuration mode.

7.7.5 Configuring static multicast members of VLAN copy

Configure static multicast members of VLAN copy for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	`Raisecom(config-gigaethernet1/1/port)#igmp vlan-copy mcast-vlan` *`vlan-id`* `static` *`ip-address`* `user-vlan` *`vlan-id`* **Example:** `Raisecom(config-gigaethernet1/1/1)#igmp vlan-copy mcast-vlan 2 static 224.0.1.1 user-vlan 10`	Configure static multicast members of VLAN copy. • vlan-id: multicast VLAN, an integer, ranging from 1 to 4094, namely, the VLAN from the multicast route interface • ip-address: multicast address, in dotted decimal notation, ranging from 224.0.0.1 to 239.255.255.255 • user-vlan vlan-id: user VLAN, an integer, ranging from 1 to 4094

Note

- IGMP Snooping and IGMP MVR cannot be enabled concurrently in the same multicast VLAN, otherwise the configuration will fail.
- IGMP Snooping and multicast VLAN copy cannot be enabled concurrently in the same multicast VLAN, otherwise the configuration will fail.

7.7.6 Configuring customer VLAN of VLAN copy

Configure the customer VLAN of VLAN copy for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config-gigaethernet1/1/port)#**igmp vlan-copy user-vlan** *vlan-id* **Example:** Raisecom(config-gigaethernet1/1/1)#igmp vlan-copy user-vlan 2	Configure the customer VLAN of multicast VLAN copy. • vlan-id: customer VLAN, an integer, ranging from 1 to 4094

7.7.7 Configuring host joining function of VLAN copy

Configure the host joining function of VLAN copy for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config-gigaethernet1/1/port)#**igmp vlan-copy mcast-vlan** *vlan-id* **host-join** *ip-address* [**user-vlan** *vlan-id*] **Example:** Raisecom(config-gigaethernet1/1/1)#igmp vlan-copy mcast-vlan 2 host-join 224.0.1.1	Configure the host joining function of multicast VLAN copy. • mcast-vlan vlan-id: multicast VLAN, VLAN to which the multicast router interface belongs, an integer, ranging from 1 to 4094 • ip-address: multicast IP address, in dotted decimal notation, ranging from 224.0.0.1 to 239.255.255.255 • user-vlan vlan-id: user VLAN, an integer, ranging from 1 to 4094

7.7.8 Checking configurations

Use the following commands to check configuration results.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
1	Raisecom#**show igmp vlan-copy**	Show configurations of multicast VLAN copy.
2	Raisecom#**show igmp vlan-copy** { **interface** | *interface-type interface-number* }	Show configurations of multicast VLAN copy on the specified interface.
3	Raisecom#**show igmp vlan-copy member**	Show information about multicast group members of multicast VLAN copy.
4	Raisecom#**show igmp vlan-copy member** *interface-type interface-number*	Show information about multicast group members of multicast VLAN copy on the specified interface.
5	Raisecom#**show igmp vlan-copy member user-vlan** *vlan-id*	Show information about multicast group members of multicast VLAN copy in the specified user VLAN.
6	Raisecom#**show igmp vlan-copy member count** { *interface-type interface-number* | **user-vlan** *vlan-id* }	Show the number of members in the multicast group of multicast VLAN copy.
7	Raisecom#**show igmp vlan-copy vlan-group** [**mcast-vlan** *vlan-id*]	Show the multicast VLAN and bound group address set of multicast VLAN copy.

Copyright © Raisecom Technology Co., Ltd.

8 OAM

This chapter describes basic principles and configuration procedures for OAM and provide related configuration examples, including the following sections:

- Introduction
- EFM

8.1 Introduction

Initially, Ethernet is designed for LAN. Operation, Administration and Maintenance (OAM) is weak because of its small size and a NE-level administrative system. With continuous development of Ethernet technology, the application scale of Ethernet in Telecom network becomes wider and wider. Compared with LAN, the link length and network size of Telecom network is bigger and bigger. The lack of effective management and maintenance mechanism has seriously obstructed Ethernet technology applying to the Telecom network.

To confirm connectivity of Ethernet virtual connection, effectively detect, confirm, and locate faults on network, balance network utilization, measure network performance, and provide service according Service Level Agreement (SLA), implementing OAM on Ethernet has becoming an inevitable developing trend.

Working mode

An interface enabled with EFM OAM is called an OAM entity. EFM OAM supports the following two working modes:

- Active mode: initialized by the OAM entity that is in active mode
- Passive mode: the OAM entity in passive mode just waits for connection request of the active OAM entity. If OAM entities of both ends of a link are in passive mode, the OAM link cannot be established.

OAM discovery

The Ethernet OAM connection process is the OAM discovery phase, where an OAM entity discovers a remote OAM entity and establishes a session with it.

This phase is initiated by an OAM entity that is in active mode. One ends informs the other of its Ethernet OAM configurations and Ethernet OAM capabilities supported by the local node

Copyright © Raisecom Technology Co., Ltd.

by exchanging OAM PDU. Both ends determine whether to establish OAM connection. If yes, Ethernet OAM protocol will work on the link layer.

Only the OAM entity in active mode can initiate OAM connection.

After the OAM connection is established, both ends keep connected by exchanging OAM PDU. If one end fails to receive OAM PDU within the timeout time, it believes that connection expires and reconnection is required.

Monitoring link

In the OAM connection, an OAM entity keeps sending Information OAM PDUs. The local OAM entity can inform the peer OAM entity of threshold events through Information OAM PDUs. In this way, the network administrator can learn the link state and take actions accordingly.

The network administrator monitors Ethernet OAM through the Event Notification OAM PDU. When a link fails, the passive OAM entity detects the failure, and actively sends Event Notification OAM PDU to the peer active OAM entity to inform the following threshold events. By default, 3 Dying Gasp Traps are sent. Therefore, the network administrator can dynamically master the network status through the link monitoring process.

- Error frame event: the number of error frames exceeds the threshold in a time unit.
- Error frame period event: the number of error frames exceeds the threshold in a period (specified N frames).
- Error frame second event: the number of error frames in M seconds exceeds the threshold. The second when an errored frame is generated is called the errored frame second.
- Error symbol period event: the number of error symbols received in a period (monitor window) exceeds the threshold.

Informing of peer fault

When a device is faulty or fails, it may cause network failure. Thus a flag is defined in OAM PDU packet to allow an OAM entity to transmit fault information to the peer. The flag may stand for the following threshold events:

- Link fault: signals from the peer are lost. OAM PDUs are sent every 1s.
- Dying gasp: an unpredictable event occurs which causes the system to be irrevocable, such as power failure. In this case, OAM PDUs are sent ceaselessly.
- Critical event: an uncertain critical event occurs, such as abnormal temperature. In this case, OAM PDUs are sent ceaselessly,

Remote loopback

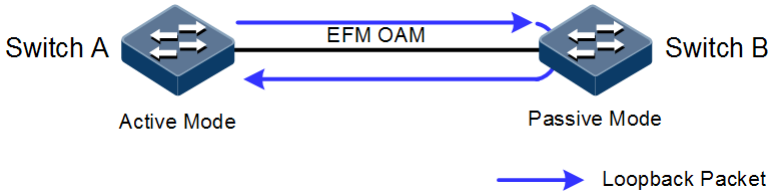
Remote loopback is used to locate the area with the fault and help you test link quality with instruments. Periodical loop detection helps you find network faults in time and segmental loop detection helps you locate the specified area with the fault and clear the fault.

OAM loopback occurs only after the Ethernet OAM connection is established. When connected, the active OAM entity initiates the OAM loopback command, and the peer OAM entity responds to the command. When the peer OAM entity is in loopback mode, all packets except OAM PDU will be retraced.

Copyright © Raisecom Technology Co., Ltd.

Switch A, in active mode, determines link status through returned packets, as shown in Figure 8-1.

Figure 8-1 OAM loopback



8.2 EFM

8.2.1 Introduction

Complying with IEEE 802.3ah protocol, Ethernet in the First Mile (EFM) is a link-level Ethernet OAM technology. It provides link connectivity detection, link fault monitoring, and remote fault notification for a link between two directly connected devices. EFM is mainly used for Ethernet links on edges of the network accessed by users.

8.2.2 Preparing for configurations

Scenario

Deploying EFM feature between directly connected devices can efficiently improve Ethernet link management and maintenance capability and ensure stable network operation.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.

8.2.3 Default configurations of EFM

Default configurations of EFM are as below.

Function	Default value
EFM working mode	Passive mode
Interval for sending messages	10 × 100ms
Link timeout	5s
OAM	Disable
Remote OAM event alarm	Enable
EFM remote loopback status	Not response
Monitor window of errored frame event	1s
Monitor threshold of errored event	1 errored frame

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
Monitor window of errored frame period event	1000ms
Monitor threshold of errored frame period event	1 errored frame
Monitor window of link errored frame second statistics event	60s
Monitor threshold of link errored frame second statistics event	1s
Monitor window of link errored coding statistics event	1s
Monitor threshold of errored coding statistic event	1s
Fault indication	Enable
Local OAM event alarm	Enable

8.2.4 Configuring basic functions of EFM

Configure basic functions of EFM for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface`** *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
3	`Raisecom(config-gigaethernet1/1/port)#`**`oam { active | passive }`** `Raisecom(config-gigaethernet1/1/port)#`**`exit`** **Example:** `Raisecom(config-gigaethernet1/1/1)#oam active`	Configure the working mode of EFM OAM. At least one end should be in active mode, otherwise link detection will fail. • active: active mode. An interface sends OAM Protocol Data Unit (PDU) initiating peer discovery or remote loopback. • passive: passive mode. An interface waits for receiving the peer OAM PDU.
4	`Raisecom(config)#`**`oam send-period`** *`period-number`* **`timeout`** *`time`* **Example:** `Raisecom(config)#oam send-period 20 timeout 10`	(Optional) configure the period for sending OAM PDUs. • period-number: period of sending OAM PDU, an integer, ranging from 1 to 100, in units of 100ms • time: timeout, an integer, ranging from 1 to 50, in units of second
5	`Raisecom(config)#`**`interface`** *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type interface-number: interface ID

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

6	`Raisecom(config-gigaethernet1/1/port)#oam { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#oam enable`
		Enable interface OAM.
		• enable: enable EFM OAM of links.
		• disable: disable EFM OAM of links.

7	`Raisecom(config-gigaethernet1/1/port)#exit`	(Optional) enter global configuration mode.
8	`Raisecom(config)#ip oam server pool` *pool-name* **Example:** `Raisecom(config)#ip oam server pool pool`	(Optional) create an address pool based on OAM, and define attributes of the address pool so that it can be used in assigning IP addresses for interfaces. • pool pool-name: IP address pool. The pool-name is a string of 1 to 16 characters.

8.2.5 Configuring active functions of EFM

Note

The active function of EFM OAM can be configured only when the ISCOM2600G series switch is in active mode.

Configuring OAM remote loopback

OAM provides a link-layer remote loopback mechanism for locating link faults and measuring performance and quality. In link loopback status, the ISCOM2600G series switch sends back all packets except OAM packets received by the link to the peer device. The local device initiates or disables remote loopback through the OAM remote loopback command. The remote device, through the loopback configuration command, controls whether to respond to the loopback command.

Configure OAM remote loopback for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
3	`Raisecom(config-gigaethernet1/1/port)#oam remote-loopback`	Configure the interface to start EFM OAM remote loopback. Only the active OAM end can initiate remote loopback.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-gigaethernet1/1/port)#**oam loopback timeout** *time* **Example:** Raisecom(config-gigaethernet1/1/1)#oam loopback timeout 5	(Optional) configure the timeout for remote loopback. If the remote end fails to respond within the timeout time, the local end will retry. After the local end fails in retry, it will send a timeout alarm. • time: timeout, an integer, ranging from 1 to 50, in units of second
5	Raisecom(config-gigaethernet1/1/port)#**oam loopback retry** *times* **Example:** Raisecom(config-gigaethernet1/1/1)#oam loopback retry 3	(Optional) configure the retry times for remote loopback. • times: retry times, an integer, ranging from 1 to 10
6	Raisecom(config-gigaethernet1/1/port)#**no oam remote-loopback**	(Optional) disable remote loopback. After loop detection is complete, disable remote loopback in time.

Configuring peer OAM event alarm

Configure the peer OAM event alarm for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config-gigaethernet1/1/port)#**oam peer event trap { enable | disable }** **Example:** Raisecom(config-gigaethernet1/1/1)#oam peer event trap enable	Enable peer OAM event alarm to send link monitoring events to the NMS. • enable: enable peer OAM link event Trap. • disable: disable peer OAM link event Trap.

(Optional) configuring OAM variable obtaining

OAM variable obtaining is a link monitoring method. By obtaining the current variable of the peer, you can learn status of current link. IEEE802.3 Clause 30 defines and explains supported variable and its denotation obtained by OAM in details. The variable takes object as the maximum unit. Each object contains Package and Attribute. A package contains several attributes. Attribute is the minimum unit of a variable. When getting an OAM variable, it defines object, package, branch, and leaf description of attributes by Clause 30 to describe

Copyright © Raisecom Technology Co., Ltd.

requesting object, and the branch and leaf are followed by variable to denote object responds variable request.

The ISCOM2600G series switch supports obtaining OAM information and interface statistics.

Configure OAM variable obtaining for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#show oam peer { link-statistic | oam-info } [ interface-type interface-number ]`	Obtain EFM OAM information about the peer device or interface statistical variable.

Note

Peer variable cannot be obtained until EFM is connected.

8.2.6 Configuring EFM passive function

Note

The EFM passive function can be configured regardless the ISCOM2600G series switch is in active or passive mode.

Configuring device to respond with EFM remote loop

Configure the ISCOM2600G series switch to respond with EFM remote loop as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#oam loopback { ignore | process }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#oam loopback process`
		Configure the Layer 2 physical interface to ignore or process EFM remote loopback.
		• ignore: ignore the remote loopback command sent by the peer end.
		• process: process the remote loopback command sent by the peer end.

Caution

Only when the local end is configured with remote loopback response can EFM OAM remote loopback of the peer end take effect.

Copyright © Raisecom Technology Co., Ltd.

Configuring OAM link monitoring

OAM link monitoring is used to detect and report link error in different conditions. When the detection link has a fault, the ISCOM2600G series switch notifies the peer of the error generated time, window and threshold by OAM event, the peer receives event notification and reports the NView NNM system through SNMP Trap. Besides, the local device can directly report events from a specified interface to the NView NNM system center through SNMP Trap.

Configure OAM link monitoring for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface`** *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
3	`Raisecom(config-gigaethernet1/1/port)#`**`oam errored-frame window`** *`framewindow`* **`threshold`** *`framethreshold`* **Example:** `Raisecom(config-gigaethernet1/1/1)#oam errored-frame window 20 threshold 100`	Configure errored frame monitor window and threshold. • errored-frame: errored frame event. It will produce error event when the number of error frames exceeds the threshold in monitoring window. • framewindow: errored frame event window, an integer, ranging from 1 to 60, in units of second • framethreshold: errored frame threshold, an integer, ranging from 1 to 65535
4	`Raisecom(config-gigaethernet1/1/port)#`**`oam errored-frame-period window`** *`frameperiodwindow`* **`threshold`** *`frameperiodthreshold`* **Example:** `Raisecom(config-gigaethernet1/1/1)#oam errored-frame-period window 20 threshold 100`	Configure errored frame period event monitor window and threshold. • errored-frame-period: errored frame period event, generated when the number of error frames exceeds the threshold in a period • frameperiodwindow: errored frame period event window, an integer, ranging from 1 to 600, in units of 100ms • frameperiodthreshold: errored frame period event threshold, an integer, ranging from 1 to 65535
5	`Raisecom(config-gigaethernet1/1/port)#`**`oam errored-frame-seconds window`** *`framesecswindow`* **`threshold`** *`framesecsthreshold`* **Example:** `Raisecom(config-gigaethernet1/1/1)#oam errored-frame-seconds window 200 threshold 100`	Configure link errored frame second window and threshold. • errored-frame-seconds: errored frame second event, generated when the number of error frame seconds exceeds the threshold. • framesecswindow: errored frame second event window, an integer, ranging from 10 to 900, in units of second • framesecsthreshold: errored frame second event threshold, an integer, ranging from 1 to 65535

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

6	`Raisecom(config-gigaethernet1/1/port)#oam errored-symbol-period window symperiodwindow threshold symperiodthreshold`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#oam errored-symbol-period window 20 threshold 100`
		Configure errored code window and threshold.
		• errored-symbol-period: errored symbol period event, generated when the number of error symbols received in a period (monitor window) exceeds the threshold
		• symperiodwindow: errored symbol period event window, an integer, ranging from 1 to 60, in units of second
		• symperiodthreshold: errored symbol period event threshold, ranging from 1 to 65535, an integer

(Optional) configuring OAM fault indication

OAM fault indication is used by the local device to inform the peer device of local abnormalities, such as link fault, power failure, abnormal temperature, which cause faulty link and device restart.

You can enable or disable fault indications except link fault which must be sent to the peer end.

Configure OAM fault indication for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-gigaethernet1/1/port)#**oam notify** { **critical-event** | **dying-gasp** | **errored-frame** | **errored-frame-period** | **errored-frame-seconds** | **errored-symbol-period** } { **enable** | **disable** } **Example:** Raisecom(config-gigaethernet1/1/1)#oam notify errored-frame disable	Enable the OAM fault notification to notify the peer device of local fault. • critical-event: when detecting critical faults such as abnormal temperature and voltage, the interface notifies the peer. • dying-gasp: when detecting power failure, the interface notifies the peer. • errored-frame: when detecting errored frame events, the interface notifies the peer. • errored-frame-period: when detecting errored frame period events, the interface notifies the peer. • errored-frame-seconds: when detecting errored frame second events, the interface notifies the peer. • errored-symbol-period: when detecting errored symbol period events, the interface notifies the peer. • enable: enable notification of faults and OAM link events. • disable: disable notification of faults and OAM link events.

Configuring local OAM event Trap

Configure local OAM event alarm for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config-gigaethernet1/1/port)#**oam event trap** { **enable** | **disable** } **Example:** Raisecom(config-gigaethernet1/1/1)#oam event trap enable	Enable local OAM event Trap to report link monitoring events to the NView NNM system immediately. • enable: enable OAM link event Trap. • disable: disable OAM link event Trap.

8.2.7 Checking configurations

Use the following commands to check configuration results.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
1	Raisecom#**show oam** [**gigaethernet** *interface-number*]	Show basic configurations of EFM OAM.
2	Raisecom#**show oam event** [**gigaethernet** *interface-number*] [**critical**]	Show remote loopback configurations of EFM OAM.
3	Raisecom#**show oam loopback** [**gigaethernet** *interface-number*]	Show configurations of link monitoring and fault indication of EFM OAM.
4	Raisecom#**show oam notify** [**gigaethernet** *interface-number*]	Show statistics on EFM OAM packets.
5	Raisecom#**show oam peer event** [**gigaethernet** *interface-number*] [**critical**]	Show configurations of EFM OAM event Trap.
6	Raisecom#**show oam peer link-statistic** [**gigaethernet** *interface-number*]	Show information about local critical faults detected by the EFM OAM interface.
7	Raisecom#**show oam statistics** [**gigaethernet** *interface-number*]	Show information about the peer EFM OAM device.
8	Raisecom#**show oam trap** [**gigaethernet** *interface-number*]	Show information about the peer EFM OAM and interface statistical variable.

8.2.8 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
Raisecom(config-gigaethernet1/1/*)#**clear oam statistics**	Clear statistics on links of the EFM OAM interface.
Raisecom(config-gigaethernet1/1/*)#**clear oam event**	Clear EFM OAM link events.
Raisecom(config)#**clear oam config**	Clear EFM OAM configurations.

Copyright © Raisecom Technology Co., Ltd.

9 Security

This chapter describes basic principles and configuration procedures for security, and provides related configuration examples, including the following sections.

- ACL
- Port security MAC
- Dynamic ARP inspection
- RADIUS
- TACACS+
- Storm control
- 802.1x
- IP Source Guard
- PPPoE+
- Configuring CPU protection
- Configuring ARP attack protection
- ND Snooping

9.1 ACL

9.1.1 Introduction

Access Control List (ACL) is a set of ordered rules, which can control the ISCOM2600G series switch to receive or refuse some data packets.

You need to configure rules on the network to prevent illegal packets from affecting network performance and determine the packets allowed to pass. These rules are defined by ACL.

ACL is a series of rule composed of permit | deny sentences. The rules are described according to source address, destination address, and port number of data packets. The ISCOM2600G series switch judges receiving or rejecting packets according to the rules.

Copyright © Raisecom Technology Co., Ltd.

9.1.2 Preparing for configurations

Scenario

ACL can help a network device recognize filter data packets. The device recognizes special objects and then permits/denies packets to pass according to the configured policy.

ACL is divided into the following types:

- Basic IPv4 ACL: define classification rules according to attributes carried in the header of IP packets, such as the source IP address and destination IP address.
- Extended IPv4 ACL: define classification rules according to attributes carried in the header of IP packets, such as the source IP address, destination IP address, bearing protocol type, and TCP or UDP port number (being 0 by default). This type can restrict Telnet/SSH login.
- MAC ACL: define classification rules according to attributes carried in the header of Layer 2 frames, such as the source MAC address, destination MAC address, and Layer 2 protocol type. When ACL denies packets with a destination MAC address, the device will not learn and show the source MAC address.
- User ACL: this type can perform the AND operation with the mask from a specified byte in the packet header or IP header, compares the character string extracted from the packet with the user-defined character string, and thus find matching packets. This type supports matching any field in the first 64 bytes of the Ethernet frame.
- IPv6 ACL: define classification rules according to attributes carried in the header of IP packets, such as the source IPv6 address, destination IPv6 address, IPv6 bearing protocol type, and TCP or UDP port number (being 0 by default). This type can restrict Telnet/SSH login.
- Advanced ACL: define classification rules according to attributes carried in the header of Layer 2 frames, such as the source MAC address and destination MAC address, and attributed carried in the header of IP packets, such as the source IP address and destination IP address.

There are 4 ACL modes according to different application environments:

- ACL based on device
- ACL based on interface
- ACL based on flow from the ingress interface to egress interface
- ACL based on VLAN

Prerequisite

N/A

9.1.3 Configuring MAC ACL

Configure MAC ACL for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#access-list acl-number [ name acl-name ]`
	Example:
	`Raisecom(config)#access-list 2001`
		Create an ACL, and enter ACL configuration mode.
		• acl-number: ACL number, an integer
		– When the ACL number is 1000–1999, this configuration enters basic IP ACL configuration mode.
		– When the ACL number is 2000–2999, this configuration enters extended IP ACL configuration mode.
		– When the ACL number is 3000–3999, this configuration enters MAC ACL configuration mode.
		– When the ACL number is 5000–5999, this configuration enters User ACL configuration mode.
		– When the ACL number is 6000–6999, this configuration enters IPv6 ACL configuration mode.
		– When the ACL number is 7000–7999, this configuration enters advanced ACL configuration mode.
		• acl-name: ACL name, a string of 1 to 32 characters

3	`Raisecom(config-acl-ip-std)#rule [ rule-id ] { deny | permit } { source-ip-address source-ip-mask | any } [ time-range time-range-name ]`
	Example:
	`Raisecom(config-acl-ip-std)#rule permit 192.168.27.27 255.255.255.0`
		(Optional) configure the matching rule for basic IP ACL.
		• rule-id: rule ID, an integer, ranging from 1 to 65535
		• deny: deny access when the rule is matched.
		• permit: allow access when the rule is matched.
		• source-ip-address: source IP address of the packet, in dotted decimal notation, such as 10.10.10.1
		• source-ip-mask: source IP mask of the packet, in dotted decimal notation, such as 255.255.255.0
		• any: match any IP address.
		• time-range time-range-name: time range, a string of characters

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-acl-ip-ext)#**rule** [*rule-id*] { **deny** | **permit** } { *protocol-id* | **icmp** | **igmp** | **ip** } { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** } [**dscp** *dscp-value*] [**ttl** *ttl-value*] [**fragment**] [**icmp-type** *icmp-type-value*] [[*icmp-message-code*]] [**igmp-type** *igmp-type-value*] [**igmp-group** *igmp-ip-address igmp-ip-mask*] [**dscp** *dscp-value* | **precedence** *precedence-value*] [| **tos** *tos-value*] [**ttl** *ttl-value*] [**fragment**] [**time-range** *time-range-name*] **Example:** Raisecom(config-acl-ip-ext)#rule permit icmp 192.168.27.27 255.255.255.0 192.168.27.28 255.255.255.0	(Optional) configure the matching rule for extended IP ACL. • rule-id: rule ID, an integer, ranging from 1 to 65535 • deny: deny access when the rule is matched. • permit: allow access when the rule is matched. • protocol-id: protocol ID, an integer, ranging from 1 to 255 • icmp: ICMP • igmp: IGMP • ip: IP address • source-ip-address: source IP address of the packet, in dotted decimal notation, such as 10.10.10.1 • source-ip-mask: source IP mask of the packet, in dotted decimal notation, such as 255.255.255.0 • any: match any IP address. • destination-ip-address: destination IP address of the packet, in dotted decimal notation, such as 10.10.10.1 • destination-ip-mask: destination IP mask

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config-acl-ip-ext)#**rule** [*rule-id*] { **deny** | **permit** } { **tcp** | **udp** } { *source-ip-address source-ip-mask* | **any** } [*source-port*] [**range** *minimum-source-port maximum-source-port*] { *destination-ip-address destination-ip-mask* | **any** } [*destination-port*] [**ack** *ack-value*] [**dscp** *dscp-value*] [**fin** *fin-value*] [**fragment**] [**precedence** *precedence-value*] [**psh** *psh-valu*e] [**range** *minimum-source-port maximum-source-port*] [**ack** *ack-value*] [**fin** *fin-value*] [**psh** *psh-valu*e] [**rst** *rst-value*] [**syn** *syn-value*] [**urg** *urg-value*] [**tos** *tos-value*] [**urg** *urg***dscp** *dscp-value*] [| **precedence** *precedence-value* | **ttl** *ttl-value*] [**fragment**] [**time-range** *time-range-name*] **Example:** Raisecom(config-acl-ip-ext)#rule permit tcp 192.168.27.27 255.255.255.0 10000 192.168.27.28 255.255.255.0 10000	of the packet, in dotted decimal notation, such as 255.255.255.0 • ack ack-value: match ACK bit, an integer, ranging from 0 to 1. • fin fin-value: match FIN bit, an integer, ranging from 0 to 1 • psh psh-value: match PSH bit, an integer, ranging from 0 to 1. • rst rst-value: match RST bit, an integer, ranging from 0 to 1. • syn syn-value: match SYN bit, an integer, ranging from 0 to 1. • urg urg-value: match URG bit, an integer, ranging from 0 to 1. • dscp dscp-value: DSCP priority, an integer, ranging from 0 to 63 • ttl ttl-valuePacket lifetime, an integer, ranging from 1 to 255 • icmp-type icmp-type-value: ICMP type, an integer, ranging from 0 to 255 • icmp-message-code: ICMP message code, an integer, ranging from 0 to 255 • igmp-type igmp-type-value: IGMP type, an integer, ranging from 0 to 255 • igmp-group igmp-ip-address: IP address of the IGMP group, in dotted decimal notation, such as 10.10.10.1 • igmp-ip-mask: mask of the IP address of the IGMP group, in dotted decimal notation, such as 255.255.255.0 • precedence precedence-value: priority used to match the packet, an integer, ranging from 0 to 7 • tos tos-value: TOS used to match the packet, an integer, ranging from 0 to 15 • fragment: fragment • tcp: TCP • udp: UDP • source-port: source interface of the packet, an integer, ranging from 1 to 65535 • destination-port: destination of the port, an integer, ranging from 1 to 65535 • range minimum-source-port: maximum source interface: source port batch configuration mode, used to configure the minimum and maximum number of source interfaces. The minimum number of source interfaces is an integer, ranging from 1 to 65535. The maximum number of source interfaces is an integer, ranging from 1 to 65535. • time-range time-range-name: period, a string of characters

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config-acl-mac)#**rule** [*rule-id*] { **deny** | **permit** } { *source-mac-address source-mac-mask* | **any** } { *destination-mac-address destination-mac-mask* | **any** } [**ethertype** { *ethertype* [*ethertype-mask*] | **ip** | **arp** }] [**svlan** *svlanid*] [**cvlan** *cvlanid*] [**cos** *cos-value*] [**inner-cos** *inner-cos-value*] [**time-range** *time-range-name*] **Example:** Raisecom(config-acl-mac)#rule 1 permit 000E.5E12.3456 FFFF.FFFF.FFFF 000E.5E34.5678 FFFF.FFFF.FFFF ethertype ip	(Optional) configure the matching rule for MAC ACL. • rule-id: rule ID, an integer, ranging from 1 to 65535 • deny: deny access when the rule is matched. • permit: allow access when the rule is matched. • source-mac-address: source MAC address of physical frame, in dotted hexadecimal notation, such as 000E.5E12.3456 • source-mac-mask: source MAC mask of physical frame, in dotted hexadecimal notation, such as FFFF.FFFF.FFFF • any: match any MAC address • destination-mac-address: destination MAC address of physical frame, in dotted hexadecimal notation, such as 000E.5E12.3456 • destination-mac-mask: destination MAC mask of physical frame, in dotted hexadecimal notation, such as FFFF.FFFF.FFFF • ethertype ethertype: Ethernet frame type, in hexadecimal notation, ranging from 0x0000 to 0xFFFF • ethertype-mask: Ethernet frame type mask, in hexadecimal notation, ranging from 0x0000 to 0xFFFF • ip: IP • arp: ARP • svlan svlanid: SVLAN ID, an integer, ranging from 1 to 4094 • cos cos-value: CoS priority of SVLAN. The cos-value is an integer, ranging from 0 to 7. • cvlan cvlanid: CVLAN ID, an integer, ranging from 1 to 4094 • inner-cos inner-cos-value: CoS priority of CVLAN. The inner-cos-value is an integer, ranging from 0 to 7. • time-range time-range-name: period, a string of characters

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	`Raisecom(config-acl-udf)#rule [rule-id] { deny | permit } { layer2 | l2-head } rule-string rule-mask offset [second rule-string rule-mask offset] [third rule-string rule-mask offset] [fourth rule-string rule-mask offset] [fifth rule-string rule-mask offset] [sixth rule-string rule-mask offset] [seventh rule-string rule-mask offset] [time-range time-range-name]` `Raisecom(config-acl-udf)#rule [rule-id] { deny | permit } ipv4 rule-string rule-mask offsets [second rule-string rule-mask offsets] [third rule-string rule-mask offsets] [fourth rule-string rule-mask offsets] [fifth rule-string rule-mask offsets] [sixth rule-string rule-mask offsets] [seventh rule-string rule-mask offsets] [time-range time-range-name]` **Example:** `Raisecom(config-acl-udf)#rule 1 permit layer2 2D FF 22`	(Optional) configure the matching rule for User ACL. • rule-id: rule ID, an integer, ranging from 1 to 65535 • deny: deny access when the rule is matched. • permit: allow access when the rule is matched. • ipv4: offset starts from IPv4 packet head+20 bytes • layer2: offset starts from protocol field • l2-head: offset starts from the header field of the L2 packet • second: match the second field. • third: match the third field. • fourth: match the fourth field. • fifth: match the fifth field. • sixth: match the sixth field. • seventh: match the seventh field. • rule-string: user-defined string, in hexadecimal notation, with even characters • rule-mask: user-defined string mask, in hexadecimal notation, with even characters • offset: beginning field of the user-defined string, starting from the physical frame, an integer, being 4n + 2 (n = 0, 1, 2, and 3...), ranging from 0 to 115 • offsets: beginning field of the user-defined string, starting from the physical frame, an integer, being 4n + 2 (n = 0, 1, 2, and 3...), ranging from 0 to 93 • time-range: time period, a string of no more than 32 characters

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
7	Raisecom(config-acl-ipv6)#**rule** [*rule-id*] { **deny** | **permit** } { *protocol-id* | **ipv6** | **icmpv6** } { *source-ipv6-address/prefix* | **any** } { *destination-ipv6-address/prefix* | **any** } [**icmpv6-type** *icmp-type-value* [*icmp-message-code*]] [**dscp** *dscp-value*] [**fragment**] [**flow-label** *flow-label-value*] [**fragment**] [**time-range** *time-range-name*] Raisecom(config-acl-ipv6)#**rule** [*rule-id*] { **deny** | **permit** } { **tcp** | **udp** } { *source-ipv6-address/prefix*| **any** } [*source-ip-mask* | **any** }*port*] { *destination-ipv6-address/prefix* | **any** } [*destination-port*] [**ack** *ack-value*] [**dscp** *dscp-value*] [**fin** *fin-value*] [**fragment**] [**flow-label** *flow-label-value*] [**psh** *psh-value*] [**rst** *rst-value*] [**syn** *syn-value*] [**urg** *urg-value*] [**dscp** *dscp-value*] [**flow-label** *flow-label-value*] [**fragment**] [**time-range** *time-range-name*] **Example:** Raisecom(config-acl-ipv6)#rule 1 permit ipv6 1030:0::48AA:1A2B/60 any	(Optional) configure the matching rule for IPv6 ACL. • rule-id: rule ID, an integer, ranging from 1 to 65535 • deny: deny access when the rule is matched. • permit: allow access when the rule is matched. • protocol-id: protocol ID, an integer, ranging from 1 to 255 • ipv6: IPv6 • igmpv6: IGMPv6 • source-ipv6-address/prefix: source IPv6 address and prefix length of the packet, in colon hexadecimal notation • any: match any IP address. • destination-ipv6-address/prefix: destination IPv6 address of the packet, in colon hexadecimal notation • icmpv6-type icmp-type-value: type value of the ICMP message, an integer, ranging from 0 to 255 • icmp-message-code: code of the ICMP message, an integer, ranging from 0 to 255 • ack ack-value: match ACK bit, an integer, ranging from 0 to 1. • fin fin-value: match FIN bit, an integer, ranging from 0 to 1 • psh psh-value: match PSH bit, an integer, ranging from 0 to 1. • rst rst-value: match RST bit, an integer, ranging from 0 to 1. • syn syn-value: match SYN bit, an integer, ranging from 0 to 1. • urg urg-value: match URG bit, an integer, ranging from 0 to 1. • dscp dscp-value: match packets with DSCP. The dscp-value is an integer, ranging from 0 to 63. • flow-label flow label-value: flow label, an integer, ranging from 0 to 1048575 • fragment: fragment • tcp: TCP • udp: UDP • source-port: source port of the packet, an integer, ranging from 1 to 65535 • destination-port: destination port of the packet, an integer, ranging from 1 to 65535 • time-range time-range-name: period, a string of characters

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
8	Raisecom(config-acl-advanced)#**rule** [*rule-id*] { **deny** | **permit** } { *source-mac-address source-mac-mask* | **any** } { *destination-mac-address destination-mac-mask* | **any** } [**svlan** *svlanid*] [**cvlan** *cvlanid*] [**cos** *cos-value*] [**cvlan** *cvlanid*] [**inner-cos** *inner-cos-value*] { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** }[} [**dscp** *dscp-value*] [**ttl** *ttl-value*] [**fragment**] [| **precedence** *precedence-value*] [| **tos** *tos-value*] [**ttl** *ttl-value*] [**fragment**] [**time-range** *time-range-name*] Raisecom(config-acl-advanced)#**exit** **Example:** Raisecom(config-acl-advanced)#rule 1 permit 000E.5E12.3456 FFFF.FFFF.FFFF 000E.5E34.5678 FFFF.FFFF.FFFF 192.168.1.2 255.255.255.0 192.168.1.5 255.255.255.0	(Optional) configure the matching rule for advanced ACL. • rule-id: rule ID, an integer, ranging from 1 to 65535 • deny: deny access when the rule is matched. • permit: allow access when the rule is matched. • source-mac-address: source MAC address of physical frame, in dotted hexadecimal notation, such as 000E.5E12.3456 • source-mac-mask: source MAC address mask of physical frame, in dotted hexadecimal notation, such as FFFF.FFFF.FFFF • any: match any MAC address • destination-mac-address: destination MAC address of physical frame, in dotted hexadecimal notation, such as 000E.5E12.3456 • destination-mac-mask: destination MAC address mask of physical frame, in dotted hexadecimal notation, such as FFFF.FFFF.FFFF • svlan svlanid: SVLAN ID, an integer, ranging from 1 to 4094 • cos cos-value: SVLAN CoS priority. The cos-value is an integer, ranging from 0 to 7. • cvlan cvlanid: CVLAN ID, an integer, ranging from 1 to 4094 • inner-cos inner-cos-value: CVLAN CoS priority. The inner-cos-value is an integer, ranging from 0 to 7. • source-ip-address: source IP address of the packet, in dotted decimal notation such as 10.10.10.1 • source-ip-mask: source IP address mask of the packet, in dotted decimal notation, such as 255.255.255.0 • dscp dscp-value: match packets with DSCP. The dscp-value is an integer, ranging from 0 to 63. • ttl ttl-value: packet lifetime, an integer, ranging from 1 to 255 • precedence precedence-value: priority used to match packet, an integer, ranging from 0 to 7 • tos tos-value: ToS priority used to match packet, an integer, ranging from 0 to 15 • fragment: fragment • time-range time-range-name: period, a string of characters

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
9	Raisecom(config)#**interface vlan** *vlan-id* **Example:** Raisecom(config)#interface vlan 1	Enter VLAN interface mode. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
10	Raisecom(config-vlan*)#**local-access access-list** *acl-number* **Example:** Raisecom(config-vlan1)#local-access access-list 1001	(Optional) configure the SNMP ACL IP. • acess-list acl-number: ACL number, an integer – When the rangg is 1000 to 1999, enter standard IP ACL configuration mode. – When the range is 6000 to 6999, enter IPv6 ACL configuration mode.

9.1.4 Configuring ACL period

Configure the ACL period for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**time-range** *time-range-name* { *hour minute seconds* **to** *hour minute seconds* { *weekday-list* | **sun** | **mon** | **tue** | **wed** | **thu** | **fri** | *sat***sta** | **off-day** | **working-day** | **daily** } [**from** *hour minute seconds month-day-year*] [**to** *hour minute seconds month-day-year*] | **from** *hour minute seconds month-day-year* [**to** *hour minute seconds month-day-year*] | **to** *hour minute seconds month-day-year* } **Example:** Raisecom(config)#time-range a 1:00:00 to 3:00:00 mon	Create a period for applying ACL rules. • time-range-name: period, a string of characters • hour minute seconds: hour, minute, second, an integer • weekday-list: weekday list, an integer, ranging from 0 to 6 • sun: Sunday • mon: Monday • tue: Tuesday • wed: Wednesday • thu: Thursday • fri: Friday • sta: Saturday • off-day: Saturday and Sunday • working-day: Monday to Friday • daily: Monday to Saturday • month-day-year: month, day, year, an integer. Month ranges from 1 to 12. Day ranges from 1 to 31. Year ranges from 2000 to 2099.

9.1.5 Configuring filter

Configure the filter for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode, or VLAN interface configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	`Raisecom(config-gigaethernet1/1/port)#filter ingress access-list` { *`acl-number`* | **`name`** *`acl-name`* } [**`statistics`**] [**`statistics`**] **Example:** `Raisecom(config-gigaethernet1/1/1)#filter ingress access-list 1001`	Apply ACL to the interface. • ingress: apply ACL to the ingress direction. • access-list acl-number: access control list number, an integer – When the range is 1000 to 1999, enter standard IP ACL configuration mode. – When the range is 2000 to 2999, enter extended IP ACL configuration mode. – When the range is 3000 to 3999, enter MAC ACL configuration mode. – When the range is 5000 to 5999, enter user ACL configuration mode. – When the range is 6000 to 6999, enter IPv6 ACL configuration mode. – When the range is 7000 to 7999, enter advanced ACL configuration mode. • statistics: enable ACL statistics. • name acl-name: ACL name, a string of 1 to 32 characters
4	`Raisecom(config-gigaethernet1/1/port)#exit`	Return to global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config)#**filter ingress access-list** { *acl-number* | **name** *acl-name* } **vlanlist** *vlan-list* [**statistics**] **Example:** Raisecom(config)#filter ingress access-list 2001 vlanlist 2	Apply ACL to the VLAN. • ingress: apply ACL to the ingress direction. • access-list acl-number: access control list number, an integer – When the range is 1000 to 1999, enter standard IP ACL configuration mode. – When the range is 2000 to 2999, enter extended IP ACL configuration mode. – When the range is 3000 to 3999, enter MAC ACL configuration mode. – When the range is 5000 to 5999, enter user ACL configuration mode. – When the range is 6000 to 6999, enter IPv6 ACL configuration mode. – When the range is 7000 to 7999, enter advanced ACL configuration mode. • name acl-name: ACL name, a string of 1 to 32 characters • vlan-list: VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". • statistics: enable ACL statistics.

9.1.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show access-list** [*acl-number* | **name** *acl-name*]	Show ACL configurations.
2	Raisecom#**show acl resource ingress**	Show resources used by ACL.
3	Raisecom#**show filter interface**	Show filter configurations.
	Raisecom#**show filter interface** *interface-type interface-number* [**ingress**]	
	Raisecom#**show filter statistics interface** *interface-type interface-number* [**ingress** [**access-list** { *acl-number* | **name** *acl-name* }]	
	Raisecom#**show filter vlanlist** [*vlan-list*]	
4	Raisecom#**show local-access access-list**	Show information about authentication by the SNMP server.
5	Raisecom#**show time-range** [*time-range-name*]	Show configurations of the time range.

Copyright © Raisecom Technology Co., Ltd.

9.1.7 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description

`Raisecom(config)#clear filter statistics interface { interface-type interface-number | vlan vlan-id } ingress [ access-list { acl-number | name acl-name } ]`
Example:
`Raisecom(config)#clear filter statistics interface gigaethernet 1/1/1 ingress`
	Clear statistics on ACL filter configurations.
	• interface-type: interface type
	• interface-number: interface ID. The form and value range depend on the interface type.
	• vlan vlan-id: VLAN ID, an integer, ranging from 1 to 4094
	• ingress: apply ACL to the ingress direction.
	• access-list acl-number: access control list number, an integer
	– When the range is 1000 to 1999, enter standard IP ACL configuration mode.
	– When the range is 2000 to 2999, enter extended IP ACL configuration mode.
	– When the range is 3000 to 3999, enter MAC ACL configuration mode.
	– When the range is 5000 to 5999, enter user ACL configuration mode.
	– When the range is 6000 to 6999, enter IPv6 ACL configuration mode.
	– When the range is 7000 to 7999, enter advanced ACL configuration mode.
	• name acl-name: ACL name, a string of 1 to 32 characters

9.2 Port security MAC

9.2.1 Introduction

Port security MAC is used for the switching device on the edge of the network user side. It can ensure security of accessed data on an interface, and control the incoming packets according to the source MAC address.

You can enable port security MAC to limit and distinguish which users can access the network through secure interfaces. Only secure MAC addresses can access the network, unsecure MAC addresses will be dealt with as configured interface access violation mode.

Secure MAC address classification

Secure MAC addresses supported by the device are divided into the following three categories:

- Static secure MAC address

The static secure MAC address is configured by user on secure interface manually; this MAC address will take effect when port security MAC is enabled. Static secure MAC address does not age and supports loading configuration.

- Dynamic secure MAC address

Copyright © Raisecom Technology Co., Ltd.

The dynamic secure MAC address is learnt by the device. You can configure the learnt MAC address to secure MAC address in the range of the maximum number of learnt MAC address. The dynamic secure MAC addresses are aged and does not support configuration load.

The dynamic secure MAC address can be converted to the sticky secure MAC address if necessary, so as not to be aged and supports auto-loading.

- Sticky secure MAC address

The sticky secure MAC address is generated from the manual configuration of user in secure interface or converted from dynamic secure MAC address. Different from static secure MAC address, the sticky secure MAC address needs to be used in conjunction with sticky learning:

- When sticky learning is enabled, the sticky secure MAC address will take effect and this address will not be aged.
- When sticky learning is disabled, the sticky secure MAC address will become invalid and be saved only in the system.

Note

- When sticky learning is enabled, all dynamic secure MAC addresses learnt from an interface will be converted to sticky secure MAC addresses.
- When sticky learning is disabled, all sticky secure MAC addresses on an interface will be converted to dynamic secure MAC addresses.

Processing mode for violating port security MAC

When the number of secure MAC addresses has already reached the maximum number, inputting of packets from a strange source MAC address will be regarded as a violation operation. For the illegal user access, there are different processing modes for configuring the switch according to secure MAC violation policy:

- Protect mode: for illegal access users, the secure interface will discard the user's packets directly.
- Restrict mode: for illegal access users, the secure interface will discard the user's packets, and the console will print Syslog information and send an alarm to the NMS.
- Shutdown mode: for illegal access users, the secure interface will discard the user's packets, and the console will print Syslog information, send an alarm to the NMS, and then shut down the secure interface.

Caution

When the MAC address is flapping, in other words, secure interface A is accessed by a user corresponding to a secure MAC address that is already on secure interface B, secure interface A will process the access as violation.

9.2.2 Preparing for configurations

Scenario

To ensure the security of data accessed by the interface of the switch, you can control the incoming packets according to source MAC address. With port security MAC, you can configure the feature of permitting specified users to access the interface, or permitting specified number of users to access from this interface only. However, when the number of

Copyright © Raisecom Technology Co., Ltd.

users exceeds the limit, the accessed packets will be processed in accordance with port security MAC violation policies.

Prerequisite

N/A

9.2.3 Default configurations of port security MAC

Default configurations of port security MAC are as below.

Function	Default value
Interface secure MAC	Disable
Aging time of dynamic secure MAC address	300s
Aging type of dynamic secure MAC address	Absolute
Restoration time of port security MAC	Disable, namely, no restoration
Dynamic secure MAC sticky learning	Disable
Port secure MAC Trap	Disable
Port secure MAC violation processing mode	Protect
Maximum number of port security MAC	1024

9.2.4 Configuring basic functions of port security MAC

Caution

- We do not recommend enabling port security MAC on member interfaces of the LAG.
- We do not recommend using the MAC address management function to configure static MAC addresses when port security MAC is enabled.
- When the 802.1x interface adopts a MAC address-based authentication mode, port security MAC and 802.1x are mutually exclusive. We do not recommend co-configuring them concurrently.
- Port security MAC and interface-/interface VLAN-based MAC number limit are mutually exclusive, which cannot be configured concurrently.

Configure basic functions of port security MAC for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-gigaethernet1/1/port)#**switch port port-security**	Enable port security MAC.
4	Raisecom(config-gigaethernet1/1/port)#**switch port port-security maximum** *maximum-number* **Example:** Raisecom(config-gigaethernet1/1/1)#switchport port-security maximum 10	(Optional) configure the maximum number of secure MAC addresses. • maximum-number: maximum number of secure MAC addresses, an integer, ranging from 1 to 1024
5	Raisecom(config-gigaethernet1/1/port)#**switch port port-security violation** { **protect** | **restrict** | **shutdown** } **Example:** Raisecom(config-gigaethernet1/1/1)#switchport port-security violation restrict	(Optional) configure secure MAC violation mode. • protect: protect the interface. The secure port will discard packets from unauthorized users. • restrict: restrict packets. The secure port will discard packets from unauthorized users, print Syslog at console, and send a trap to the NMS. • shutdown: shut down the interface. The secure port will discard packets from unauthorized users, print Syslog information at console, send a trap to the NMS, and shut down the interface.
6	Raisecom(config-gigaethernet1/1/port)#**no port-security shutdown** Raisecom(config-gigaethernet1/1/port)#**exit**	(Optional) re-enable the interface which is shut down due to violating port security MAC.
7	Raisecom(config)#**port-security recovery-time** *second* **Example:** Raisecom(config)#port-security recovery-time 30	(Optional) configure the restoration time of port security MAC. • second: recovery time, an integer, ranging from 30 to 86400, in units of second

Note

When secure MAC violation policy is in Shutdown mode, you can use this command to re-enable this interface which is shut down due to violating port security MAC. When the interface is Up, the configured secure MAC violation mode will continue to be valid.

9.2.5 Configuring static secure MAC address

Configure the static secure MAC address for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.
3	`Raisecom(config-gigaethernet1/1/port)#switchport port-security`	Enable port security MAC.
4	`Raisecom(config-gigaethernet1/1/port)#switchport port-security mac-address` *`mac-address`* `vlan` *`vlan-id`* **Example:** `Raisecom(config-gigaethernet1/1/1)#switchport port-security mac-address 0000.0000.0001 vlan 1`	Configure the static secure MAC address. • mac-address: MAC address, in dotted hexadecimal notation • vlan-id: VLAN ID, an integer, ranging from 1 to 4094

9.2.6 Configuring dynamic secure MAC address

Configure the dynamic secure MAC address for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#port-security aging-time` *`period`* **Example:** `Raisecom(config)#port-security aging-time 10`	(Optional) configure the aging time of dynamic secure MAC address. • period: aging time, an integer, ranging from 0 to 1440s, in units of second
3	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.

4	`Raisecom(config-gigaethernet1/1/port)#switchport port-security aging-type { absolute | inactivity }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#switchport port-security aging-type inactivity`
		(Optional) configure the aging type of secure MAC addresses.
		• absolute: be aged after absolute period.
		• inactivity: be aged when there is no traffic on the interface.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	`Raisecom(config-gigaethernet1/1/port)#switchport port-security`	(Optional) enable port dynamic security MAC learning.

6	`Raisecom(config-gigaethernet1/1/port)#switchport port-security trap { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#switchport port-security trap enable`
		(Optional) enable port security MAC Trap.
		• enable: enable port security MAC learning Trap
		• disable: disable port security MAC learning Trap

7	`Raisecom(config-gigaethernet1/1/port)#switchport port-security trap period value`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#switchport port-security trap period 60`
		(Optional) configure the period for sending Traps on the interface.
		• value: Trap interval, an integer, ranging from 1 to 60 seconds

Note

The **switchport port-security** command can enable port security MAC and dynamic secure MAC learning at the same time.

9.2.7 Configuring sticky secure MAC address

Caution

We do not recommend configuring sticky secure MAC addresses when port sticky security MAC is disabled. Otherwise, port sticky security MAC may malfunction.

Configure the sticky secure MAC address for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: in the form of unit/slot/port. The value range depends on the interface type.

3	`Raisecom(config-gigaethernet1/1/port)#switchport port-security`	Enable port security MAC.
4	`Raisecom(config-gigaethernet1/1/port)#switchport port-security mac-address sticky`	Enable sticky secure MAC learning.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

5	`Raisecom(config-gigaethernet1/1/port)#switchport port-security mac-address sticky mac-address vlan vlan-id`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#switchport port-security mac-address sticky 0000.0000.0001 vlan 1`
		(Optional) manually configure sticky secure MAC addresses.
		• mac-address: MAC address, in dotted hexadecimal notation
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094

Note

After sticky secure MAC address learning is enabled, the dynamic secure MAC address will be converted to the sticky secure MAC address; the manually configured sticky secure MAC address will take effect.

9.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show port-security [ interface-type interface-number ]`	Show configurations of port security MAC.
2	`Raisecom#show port-security mac-address [interface-type interface-number ]`	Show configurations of secure MAC address and secure MAC address learning.

9.2.9 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description

`Raisecom(config-gigaethernet1/1/port)#clear port-security { all | configured | dynamic | sticky }`
Example:
`Raisecom(config-gigaethernet1/1/1)#clear port-security all`
	Clear a specified type of secure MAC addresses on a specified interface.
	• all: all secure MAC addresses
	• configured: configured MAC addresses
	• dynamic: dynamic MAC addresses
	• sticky: sticky MAC addresses

Copyright © Raisecom Technology Co., Ltd.

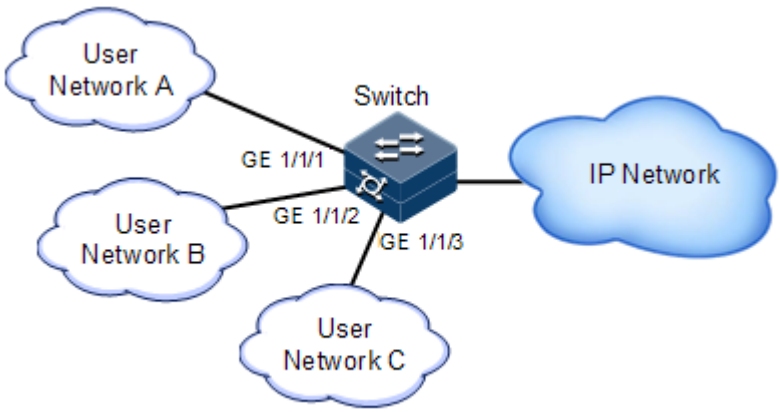
9.2.10 Example for configuring port security MAC

Networking requirements

As shown in Figure 9-1, the Switch connects 3 user networks. To ensure security of data accessed from the interface, configure the Switch as below.

- GE 1/1/1 allows up to 3 users to access the network. One of specified user MAC addresses is 0000.0000.0001. The other two users are in dynamic learning mode. The NMS can receive Trap information once the user learns a MAC address. The violation mode is Protect mode and the aging time of the two learning user MAC addresses is 10min.
- GE 1/1/2 allows up to 2 users to access the network. MAC addresses of the 2 users are determined through learning; once they are learnt, they will not be aged. The violation mode is Restrict mode.
- GE 1/1/3 allows up to 1 user to access the network. The specified user MAC address is 0000.0000.0002. Whether MAC addresses are aged can be controlled. The violation mode is Shutdown mode.

Figure 9-1 Port security MAC networking



Configuration steps

Step 1 Configure the secure MAC address on GE 1/1/1.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport port-security
Raisecom(config-gigaethernet1/1/1)#switchport port-security maximum 3
Raisecom(config-gigaethernet1/1/1)#switchport port-security mac-address
0000.0000.0001 vlan 1
Raisecom(config-gigaethernet1/1/1)#switchport port-security violation
protect
Raisecom(config-gigaethernet1/1/1)#switchport port-security trap enable
Raisecom(config-gigaethernet1/1/1)#switchport port-security trap period
10
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#port-security aging-time 10
```


Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config)#
```

Step 2 Configure the secure MAC address on GE 1/1/2.

```
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport port-security
Raisecom(config-gigaethernet1/1/2)#switchport port-security maximum 2
Raisecom(config-gigaethernet1/1/2)#switchport port-security mac-address
sticky
Raisecom(config-gigaethernet1/1/2)#switchport port-security violation
restrict
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 3 Configure the secure MAC address for GE 1/1/3.

```
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#switchport port-security
Raisecom(config-gigaethernet1/1/3)#switchport port-security maximum 1
Raisecom(config-gigaethernet1/1/3)#switchport port-security mac-address
sticky 0000.0000.0002 vlan 1
Raisecom(config-gigaethernet1/1/3)#switchport port-security mac-address
sticky
Raisecom(config-gigaethernet1/1/3)#switchport port-security violation
shutdown
```

Checking results

Use the **show port-security** command to show configurations of port security MAC.

```
Raisecom#show port-security
Port security aging time:10 (mins)
Port security recovery time:Disable (s)
port                     status    Max-Num   Cur-Num  His-MaxNum  vio-
Count vio-action Dynamic-Trap Aging-Type trap-period
---------------------------------------------------------------------------
-----------------------------------------------------
gigaethernet1/1/1          Enable    3        1      1          0
protect   Enable     Absolute  10
gigaethernet1/1/2          Enable    2        0      0          0
restrict  Disable    Absolute  0
gigaethernet1/1/3          Enable    1        1      1          0
shutdown  Disable    Absolute  0
```

Use the **show port-security mac-address** command to show configurations and learning of secure MAC addresses.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#show port-security mac-address
VLAN  Security-MAC-Address  Flag           Port                  Age(min)
-----------------------------------------------------------------------------
1    0000.0000.0001      Security-static  gigaethernet1/1/1       --
1    0000.0000.0002      sticky          gigaethernet1/1/3       --
```

9.3 Dynamic ARP inspection

9.3.1 Introduction

Dynamic ARP inspection is used for ARP protection of unsecure interface and prevents from responding ARP packets which do not meet the requirements, thus preventing ARP spoofing attack on the network.

There are 2 modes for dynamic ARP inspection:

- Static binding mode: configure the binding manually.
- Dynamic binding mode: in cooperation with the DHCP snooping to generate dynamic binding. When DHCP Snooping entry is changed, the dynamic ARP inspection will also update dynamic binding entry synchronously.

The ARP inspection table, which is used for preventing ARP attacks, consists of DHCP snooping entries and statically configured ARP inspection rules, including IP address, MAC address, and VLAN binding information. In addition, the ARP inspection table associates this information with specific interfaces. The dynamic ARP inspection binding table supports the combination of following entries:

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

Dynamic ARP inspection interfaces are divided into the following two types according to trust status:

- Trusted interface: the interface will stop ARP inspection, which conducts no ARP protection on the interface. All ARP packets are allowed to pass.
- Untrusted interface: the interface takes ARP protection. Only ARP packets that match the binding table rules are allowed to pass. Otherwise, they are discarded.

Copyright © Raisecom Technology Co., Ltd.

Figure 9-2 Principles of dynamic ARP inspection

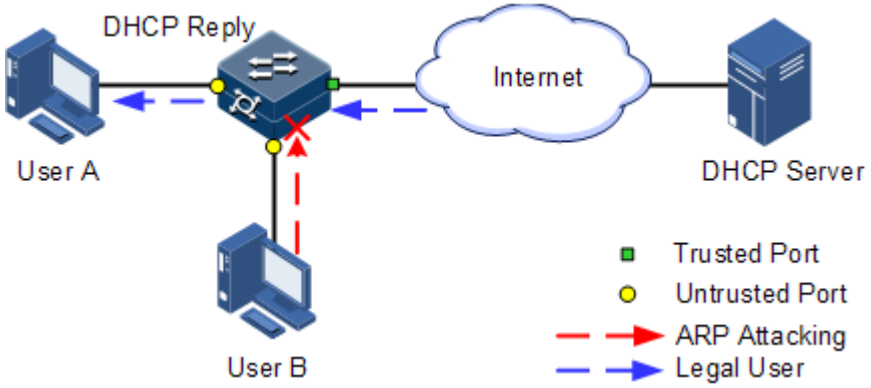


Figure 9-2 shows principles of dynamic ARP inspection. When the ISCOM2600G series switch receives an ARP packet, it compares the source IP address, source MAC address, interface ID, and VLAN information of the ARP packet with the DHCP Snooping entry information. If matched, it indicates that it is a legal user and the ARP packets are permitted to pass. Otherwise, it is an ARP attack and the ARP packet is discarded.

Dynamic ARP inspection also provides rate limiting on ARP packets to prevent unauthorized users from attacking the ISCOM2600G series switch by sending a large number of ARP packets to the ISCOM2600G series switch.

- When the number of ARP packets received by an interface per second exceeds the threshold, the system will determine that the interface encounters ARP attacks, and then discard all received ARP packets to avoid ARP attacks.
- The system provides auto-recovery and supports configuring the recovery time. The interfaces, where the number of received ARP packets is greater than the threshold, will recover to normal Rx/Tx status automatically after the recovery time expires.

Dynamic ARP inspection can also protect the specified VLAN. After the protection VLAN is configured, the ARP packets in specified VLAN on an untrusted interface will be protected. Only the ARP packets, which meet binding table rules, are permitted to pass. Other packets are discarded.

9.3.2 Preparing for configurations

Scenario

Dynamic ARP inspection is used to prevent common ARP spoofing attacks on the network, which isolates ARP packets from unsafe sources. Whether to trust ARP packets depend on the trusting status of an interface while ARP packets meet requirements depends on the ARP binding table.

Prerequisite

Enable DHCP Snooping if there is a DHCP user.

9.3.3 Default configurations of dynamic ARP inspection

Default configurations of dynamic ARP inspection are as below.

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
Dynamic ARP inspection interface trust status	Untrusted
Dynamic ARP inspection static binding	Disable
Dynamic ARP inspection dynamic binding	Disable
Dynamic ARP inspection static binding table	N/A
Dynamic ARP inspection protection VLAN	All VLANs
Interface rate limiting on ARP packets	60 pps
Limit on the number of binding tables on the interface	No limit

9.3.4 Configuring trusted interfaces of dynamic ARP inspection

Configure trusted interfaces of dynamic ARP inspection for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface`** *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.
3	`Raisecom(config-gigaethernet1/1/port)#`**`ip arp-inspection trust`**	Configure the interface as a trusted interface. Use the **no ip arp-inspection trust** command to configure the interface to an untrusted interface; in other words, the interface does not trust the ARP packet.

9.3.5 Configuring static binding of dynamic ARP inspection

Configure static binding of dynamic ARP inspection for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`ip arp-inspection static-config`**	Enable global static ARP binding.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

3	`Raisecom(config)#ip arp-inspection binding ip-address [ ip-mask ] [ mac-address ] [ vlan vlan-id ] interface-type interface-number`
	Example:
	`Raisecom(config)#ip arp-inspection binding 10.0.0.1 vlan 10 gigaethernet 1/1/1`
		Configure the static binding.
		• ip-address: bound IP address, in dotted decimal notation, such as 10.0.0.1
		• ip mask: bound IP address mask, in dotted decimal notation, such as 255.255.255.0
		• mac-address: binding MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456
		• vlan vlan-id: binding VLAN ID, an integer, ranging from 1 to 4094
		• interface-type: interface type
		• interface-number: interface ID. The form and value range depend on the interface type.

9.3.6 Configuring dynamic binding of dynamic ARP inspection

Caution

Before enabling dynamic binding of dynamic ARP inspection, you need to use the **ip dhcp snooping** command to enable DHCP Snooping.

Configure dynamic binding of dynamic ARP inspection for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip arp-inspection dhcp-snooping`	Enable global dynamic ARP binding.

9.3.7 Configuring protection VLAN of dynamic ARP inspection

Configure protection VLAN of dynamic ARP inspection for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#ip arp-inspection binding dhcp-snooping { auto-update | static }`
	Example:
	`Raisecom(config)#ip arp-inspection binding dhcp-snooping auto-update`
		Configure ARP entry conversion.
		• auto-update: automatically converted into static entries
		• static: converted into static entries

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

3	`Raisecom(config)#ip arp-inspection vlan vlan-list`
	Example:
	`Raisecom(config)#ip arp-inspection vlan 1-3`
		Configure the protection VLAN of dynamic ARP inspection.
		• vlan-list: protection VLAN ID list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".

9.3.8 Configuring rate limiting on ARP packets on interface

Configure rate limiting on ARP packets on the interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: in the form of unit/slot/port. The value range depends on the interface type.

3	`Raisecom(config-gigaethernet1/1/port)#ip arp-rate-limit rate rate-value`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#ip arp-rate-limit rate 200`
		Configure the rate limit of ARP packets on the interface.
		• rate-value: threshold, an integer, ranging from 1 to 1000, in units of packet/s

9.3.9 Configuring number of binding tables on interface

Configure the number of binding tables on the interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter global configuration mode.
		• interface-type: interface type
		• interface-number: in the form of unit/slot/port. The value range depends on the interface type.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	`Raisecom(config-gigaethernet1/1/port)#ip arp-inspection binding-number` *number* **Example:** `Raisecom(config-gigaethernet1/1/1)#ip arp-inspection binding-number 100`	Configure the number of binding tables on the interface, including static binding tables and DHCP Snooping binding tables. • number: number of binding tables, an integer, ranging from 1 to 512

9.3.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show ip arp-inspection`	Show configurations of dynamic ARP inspection.
2	`Raisecom#show ip arp-inspection binding [` *interface-type interface-number* `]`	Show information about the dynamic ARP inspection binding table.
3	`Raisecom#show ip arp-rate-limit`	Show configurations of rate limiting on ARP packets.

9.3.11 Example for configuring dynamic ARP inspection

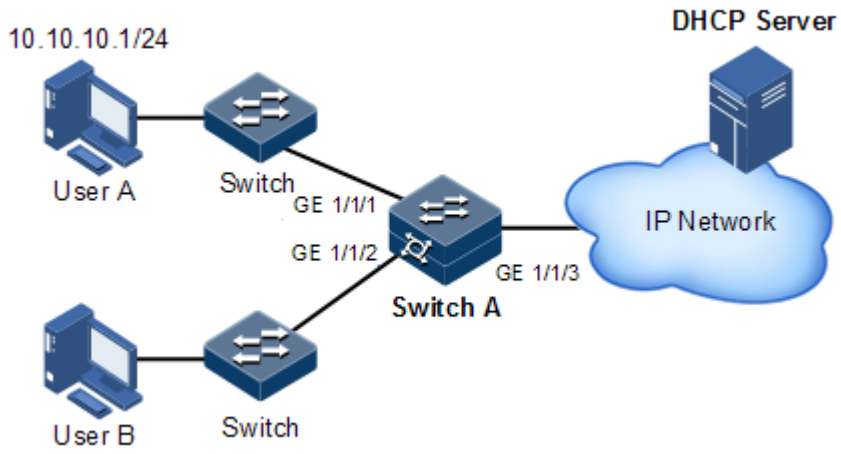
Networking requirements

To prevent ARP attacks, configure dynamic ARP inspection on Switch A, as shown in Figure 9-3.

- Uplink GE 1/1/3 allows all ARP packets to pass.
- Downlink GE 1/1/1 allows ARP packets with specified IP address 10.10.10.1 to pass.
- Other interfaces allow ARP packets complying with dynamic binding learnt by DHCP Snooping to pass.
- Configure rate limiting on ARP packets on downlink GE 1/1/2. The rate threshold is configured to 20 pps.

Copyright © Raisecom Technology Co., Ltd.

Figure 9-3 Configuring dynamic ARP inspection



Configuration steps

Step 1 Configure GE 1/1/3 as the trusted interface.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#ip arp-inspection trust
Raisecom(config-gigaethernet1/1/3)#exit
```

Step 2 Configure static binding.

```
Raisecom(config)#ip arp-inspection static-config
Raisecom(config)#ip arp-inspection binding 10.10.10.1 gigaethernet 1/1/1
```

Step 3 Enable dynamic ARP inspection binding.

```
Raisecom(config)#ip dhcp snooping
Raisecom(config)#ip arp-inspection dhcp-snooping
```

Step 4 Configure rate limiting on ARP packets on the interface.

```
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#ip arp-rate-limit rate 20
Raisecom(config-gigaethernet1/1/2)#exit
```


Copyright © Raisecom Technology Co., Ltd.

Checking results

Use the **show ip arp-inspection** command to show configurations of interface trust status and static/dynamic ARP binding.

```
Raisecom#show ip arp-inspection
Static Config ARP Inspection: Enable
DHCP Snooping ARP Inspection: Enable
ARP Inspection Protect Vlan : 1-4094
Bind Rule Num            : 1
Vlan Rule Num            : 0
Bind Acl Num             : 1
Vlan Acl Num             : 0
Remained Rule Num         : 511
Remained Acl Num          : 511

Port                        Trust
----------------------------------------
gigaethernet1/1/1              no
gigaethernet1/1/2              no
gigaethernet1/1/3              yes
gigaethernet1/1/4              no
gigaethernet1/1/5              no
gigaethernet1/1/6              no
gigaethernet1/1/7              no
……
```

Use the **show ip arp-inspection binding** command to show information about the dynamic ARP binding table.

```
Raisecom#show ip arp-inspection binding
Current Rules Num    : 1
History Max Rules Num : 1
Ip Address    Mask        Mac Address  VLAN   Port            Type    Inhw
------------------------------------------------------------------------
-----------------------------------------
10.10.10.1   255.255.255.255   --       --  gigaethernet1/1/1  static   yes
```

Use the **show ip arp-rate-limit** command to show configurations of rate limiting on the interface and auto-recovery time for rate limiting.

```
Raisecom#show ip arp-rate-limit
Port                       Rate(Num/Sec)
---------------------------------------------
gigaethernet1/1/1             --
gigaethernet1/1/2            20
gigaethernet1/1/3             --
gigaethernet1/1/4             --
gigaethernet1/1/5             --
```


Copyright © Raisecom Technology Co., Ltd.

```
gigaethernet1/1/6            --
gigaethernet1/1/7            --
gigaethernet1/1/8            --
gigaethernet1/1/9            --
```

9.4 RADIUS

9.4.1 Introduction

Remote Authentication Dial In User Service (RADIUS) is a standard communication protocol that provides centralized authentication of remote access users. RADIUS uses UDP as the transmission protocol (port 1812 and port 1813) which has a good instantaneity; at the same time, RADIUS features good reliability by supporting retransmission mechanism and standby server mechanism.

RADIUS authentication

RADIUS adopts client/server mode. The network access device is used as client of RADIUS server. The RADIUS server receives user connection requests, authenticates users, and replies them with configurations for providing services. In this way, RADIUS can control user to access devices and network, thus improving network security.

Communication between clients and RADIUS server is authenticated by the shared key, which will not be transmitted on the network. Besides, any user password to be transmitted between clients and RADIUS server must be encrypted to prevent it from being intercepted through sniffing through any insecure network.

RADIUS accounting

RADIUS accounting is used on users that have passed RADIUS authentication. When a user logs in, the device sends an Account-Start packet to the RADIUS accounting server. During user login, the device sends Account-Update packets to the RADIUS accounting server according to the accounting policy. When the user logs off, the device sends an Account-Stop packet, which contains user online time, to the RADIUS accounting server. The RADIUS accounting server can record the access time and operations of each user through these packets.

9.4.2 Preparing for configurations

Scenario

You can deploy the RADIUS server on the network to conduct authentication and accounting to control users to access to the ISCOM2600G series switch and network. The ISCOM2600G series switch can be used as agent of the RADIUS server, which authorizes user to access according to feedback from RADIUS.

Prerequisite

N/A

Copyright © Raisecom Technology Co., Ltd.

9.4.3 Default configurations of RADIUS

Default configurations of RADIUS are as below.

Function	Default value
IP address of the RADIUS server	0.0.0.0
Timeout of the RADIUS server	3s
IP address of the RADIUS accounting server	0.0.0.0
Port number of the RADIUS authentication server	1812
Port number of the RADIUS accounting server	1813
Shared key for communicating with the RADIUS accounting server	N/A
Processing policy for accounting failure	Online
Period for sending Account-Update packets	0
AAA accounting	Disable
AAA authorization through CLI	Disable
AAA accounting through CLI	Enable

9.4.4 Configuring basic functions of AAA

Configure basic functions of AAA for the ISCOM2600G series switch as below.

Step	Command	Description

1	`Raisecom#aaa command authorize { enable | disable }`
	Example:
	`Raisecom#aaa command authorize enable`
		Enable/Disable AAA authorization through CLI.
		• enable: enable AAA authorization through CLI.
		• disable: disable AAA authorization through CLI.

2	`Raisecom#aaa command accounting { enable | disable }`
	Example:
	`Raisecom#aaa command accounting enable`
		Enable/Disable AAA accounting through CLI.
		• enable: enable AAA accounting through CLI.
		• disable: disable AAA accounting through CLI.

3	`Raisecom#aaa accounting login { enable | disable }`
	Example:
	`Raisecom#aaa accounting login enable`
		Enable/Disable RADIUS accounting.
		• enable: enable AAA accounting through CLI.
		• disable: disable AAA accounting through CLI.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

4	`Raisecom#aaa accounting fail { offline | online }`
	Example:
	`Raisecom#aaa accounting fail offline`
		Configure the processing policy for accounting failure.
		• online: allow login.
		• offline: disallow login.

5	`Raisecom#aaa accounting update minute`
	Example:
	`Raisecom#aaa accounting update 10`
		Configure the period for sending Account-Update packets. If it is configured to 0, no Account-Update packet will be sent.
		• Minute: sending period, an integer, ranging from 0 to 300, in units of minute
		Note
		The accounting server can record access time and operation for each user through Account-Start packets, Account-Update packets, and Account-Stop packets.

9.4.5 Configuring RADIUS authentication

Configure RADIUS authentication for the ISCOM2600G series switch as below.

Step	Command	Description

1	`Raisecom#radius [ backup ] { ipv4-address | ipv6-address } [ auth-port port-id ]`
	Example:
	`Raisecom#radius 10.0.0.1 auth-port 1000`
		Assign the IP address and port number for RADIUS authentication server. Configure the **backup** parameter to assign the backup RADIUS authentication server.
		• backup: if this parameter is selected, the IP address of the backup RADIUS authentication server will be configured. If this parameter is not selected, the IP address of the master RADIUS authentication server will be configured.
		• ipv4-address: IPv4 address, in dotted decimal notation, such as 10.10.1.1
		• auth-port port-id: authentication interface ID, an integer, ranging from 1 to 65535

2	`Raisecom#radius-key string`
	Example:
	`Raisecom#radius-key raisecom`
		Configure the shared key for RADIUS authentication.
		• string: key string, a string of 1 to 100 characters

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom#**radius-encrypt-key** *word* **Example:** Raisecom#radius-encrypt-key Q3koBSbi4CrD	Configure the RADIUS authentication server to encrypt data in cyphertext mode. • word: key string, a string of 1 to 270 characters
4	Raisecom#**radius backup key** *word* **Example:** Raisecom#radius backup key WinRadius	Configure the shared key for the backup RADIUS authentication server. • word: public key string of the RADIUS server, no more than 100 characters
5	Raisecom#**radius backup encrypt-key** *word* **Example:** Raisecom#radius backup encrypt-key /vxmfY8GI13rmJQ8GomEoGM=	Configure the backup RADIUS authentication server to encrypt data in cyphertext mode. • word: public key string of the RADIUS server, no more than 270 characters
6	Raisecom#**user login** { **local-radius** | **radius-local** [**server-no-response**] | **radius-user** } **Example:** Raisecom#user login local-radius	Configure users to perform login authentication through RADIUS. • local-radius: when local authentication coexists with RADIUS authentication, use local authentication preferentially. • radius-local: when local authentication coexists with RADIUS authentication, use RADIUS authentication preferentially. • radius-user: use RADIUS authentication. • server-no-response: use local authentication only when the RADIUS server stops responding.
7	Raisecom#**radius nas-ip-address** *ip-address* **Example:** Raisecom#radius nas-ip-address 192.168.1.5	Configure the NAS IP address of RADIUS authentication. • ip-address: NAS IP address, in dotted decimal notation, such as 10.0.0.1
8	Raisecom#**radius response-timeout** *time* **Example:** Raisecom#radius response-timeout 10	Configure the timeout for response by the RADIUS authentication server. • time: response timeout of the authentication server, in units of second, an integer, ranging from 1 to 10
9	Raisecom#**radius authorization no-privilege** { **default** | **offline** | *priority* } **Example:** Raisecom#radius authorization no-privilege offline	Configure the processing policy for RADIUS authorization failure. • offline: forced to be offline • priority: priority of authorization failure user, an integer, ranging from 1 to 15 • default: return to the default priority after authorization failure.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

10	`Raisecom#radius [ backup ] sourceip ipv4-address`
	Example:
	`Raisecom#radius sourceip 10.0.0.1`
		Configure the source IP address of the RADIUS authentication server.
		• backup: if this parameter is selected, the IP address of the backup RADIUS authentication server will be configured. If this parameter is not selected, the IP address of the master RADIUS authentication server will be configured.
		• ipv4-address: IPv4 address, in dotted decimal notation, such as 10.10.1.1

9.4.6 Configuring RADIUS accounting

Configure RADIUS accounting for the ISCOM2600G series switch as below.

Step	Command	Description

1	`Raisecom#radius [ backup ] accounting-server ipv4-address [ acct-port port-id ]`
	Example:
	`Raisecom#radius accounting-server 10.10.10.1 acct-port 1000`
		Assign IP address and UDP port number for the RADIUS accounting server. Configure the **backup** parameter to assign the backup RADIUS accounting server.
		• backup: if this parameter is selected, the IP address of the backup RADIUS accounting server will be configured. If this parameter is not selected, the IP address of the master RADIUS accounting server will be configured.
		• accounting-server: RADIUS accounting server
		• ipv4-address: IPv4 address, in dotted decimal notation, such as 10.10.10.1
		• acct-port port-id: UDP ID of the RADIUS accounting server, an integer, ranging from 1 to 65535

2	`Raisecom#radius [ backup ] accounting-server key string`
	`Raisecom#radius [ backup ] accounting-server encrypt-key string`
	Example:
	`Raisecom#radius accounting-server key raisecom`
		Configure the shared plaintext or ciphertext key to communicate with the RADIUS accounting server. The shared key must be identical to the one configured on the RADIUS accounting server. Otherwise, accounting will fail.
		• backup: configure the shared key for communicating with the backup accounting server. If this parameter is not selected, the shared key for communicating with the RADIUS primary accounting service will be configured.
		• key string: key string, a string of 1 to 100 characters
		• encrypt-key string: key string, a string of 1 to 270 characters

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

3	`Raisecom#radius accounting nas-ip-address ip-address`
	Example:
	`Raisecom#radius accounting nas-ip-address 192.168.1.5`
		Configure the NAS IP address of the RADIUS accounting server.
		• ip-address: NAS IP address, in dotted decimal notation, such as 10.0.0.1

4	`Raisecom#radius [ backup ] accounting-server sourceip { ipv4-address | ipv6-address }`
	Example:
	`Raisecom#radius accounting-server sourceip 10.0.0.1`
		Configure the source IP address of the RADIUS accounting server.
		• backup: if this parameter is selected, the IP address of the backup RADIUS accounting server will be configured. If this parameter is not selected, the IP address of the master RADIUS accounting server will be configured.
		• ipv4-address: IPv4 address, in dotted decimal notation, such as 10.10.1.1

9.4.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show radius-server`	Show configurations of the RADIUS server.
2	`Raisecom#show aaa`	Show configurations of AAA.

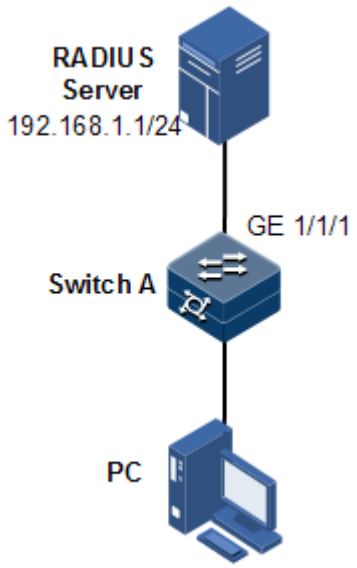
9.4.8 Example for configuring RADIUS

Networking requirements

As shown in Figure 9-4, to control a user from accessing the Switch, you need to configure RADIUS authentication and accounting on Switch A to authenticate login users on Switch A and record the operations. The period for sending Account-Update packets is 2 minutes. The user will be logged out if accounting fails.

Copyright © Raisecom Technology Co., Ltd.

Figure 9-4 RADIUS networking



Configuration steps

Step 1 Configure authentication for login user through RADIUS.

```
Raisecom#radius 192.168.1.1
Raisecom#radius-key raisecom
Raisecom#user login radius-user
```

Step 2 Configure accounting for login user through RADIUS.

```
Raisecom#aaa accounting login enable
Raisecom#radius accounting-server 192.168.1.1
Raisecom#radius accounting-server key raisecom
Raisecom#aaa accounting fail offline
Raisecom#aaa accounting update 2
```

Checking results

Use the **show radius-server** to show RADIUS configurations.

```
Raisecom#show radius-server
Server Response Timeout       :3s
Authentication server IP      :192.168.1.1
port                       :1812
Backup authentication server IP :
port                       :1812
Authentication server key     :o7MCKszV2X38
```


Copyright © Raisecom Technology Co., Ltd.

```
Backup authentication server Key:--
Accounting server IP          :192.168.1.1
port                        :1813
Backup accounting server IP    :
port                        :1813
Accounting server key         :gWOIjAJxkJKy
Backup Accounting server Key   :--
authorization fail policy      :15
NAS IP Address               :--
Accounting NAS IP Address      :--
Authentation source ip        :--
Authentation backup source ip  :--
Accounting source ip          :--
Accounting backup source ip    :--
```

Use the **show aaa** command to show RADIUS accounting.

```
Raisecom#show aaa
Accounting login      :enable
Update interval(minute):2
Accounting fail policy:offline
Command Authorization policy      :disable
Command Accounting policy      :enable
```

9.5 TACACS+

9.5.1 Introduction

Terminal Access Controller Access Control System (TACACS+) is a kind of network access authentication protocol similar to RADIUS. The differences between them are:

- TACACS+ uses TCP port 49, which has higher transmission reliability compared with UPD port used by RADIUS.
- TACACS+ encrypts the holistic of packets except the standard head of TACACS+, and there is a field to show whether the data packets are encrypted in the head of packet. Compared to RADIUS user password encryption, the TACACS+ is much safer.
- TACACS+ authentication function is separated from authorization and accounting functions; it is more flexible in deployment.

In a word, TACACS+ is safer and more reliable than RADIUS; however, as an open protocol, RADIUS is more widely used.

9.5.2 Preparing for configurations

Scenario

You can authenticate and account on users by deploying a TACACS+ server on the network to control users to access the ISCOM2600G series switch and network. TACACS+ is safer and

Copyright © Raisecom Technology Co., Ltd.

more reliable than RADIUS. The ISCOM2600G series switch can be used as an agent of the TACACS+ server, and authorize users access according to feedback result from the TACACS+ server.

Prerequisite

N/A

9.5.3 Default configurations of TACACS+

Default configurations of TACACS+ are as below.

Function	Default value
TACACS+ function	Disable
Login mode	local-user
IP address of the TACACS+ authentication server	0.0.0.0, shown as "--"
IP address of the TACACS+ accounting server	0.0.0.0, shown as "--"
Shared key for communicating with the TACACS+ accounting server	N/A
Processing policy for accounting failure	Online
Period for sending Account-Update packet	0
AAA accounting	Disable
AAA authorization through CLI	Disable
AAA accounting through CLI	Enable

9.5.4 Configuring basic functions of AAA

Configure basic functions of AAA for the ISCOM2600G series switch as below.

Step	Command	Description

1	`Raisecom#aaa command authorize { enable | disable }`
	Example:
	`Raisecom#aaa command authorize enable`
		Enable/Disable AAA authorization through CLI.
		• enable: enable AAA authorization through CLI.
		• disable: disable AAA authorization through CLI.

2	`Raisecom#aaa command accounting { enable | disable }`
	Example:
	`Raisecom#aaa command accounting enable`
		Enable/Disable AAA accounting through CLI.
		• enable: enable AAA accounting through CLI.
		• disable: disable AAA accounting through CLI.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

3	`Raisecom#aaa accounting login { enable | disable }`
	Example:
	`Raisecom#aaa accounting login enable`
		Enable/Disable RADIUS accounting.
		• enable: enable AAA accounting through CLI.
		• disable: disable AAA accounting through CLI.

4	`Raisecom#aaa accounting fail { offline | online }`
	Example:
	`Raisecom#aaa accounting fail offline`
		Configure the processing policy for accounting failure.
		• online: allow login.
		• offline: disallow login.

5	`Raisecom#aaa accounting update minute`
	Example:
	`Raisecom#aaa accounting update 10`
		Configure the period for sending Account-Update packets. If it is configured to 0, no Account-Update packet will be sent.
		• Minute: sending period, an integer, ranging from 0 to 300, in units of minute
		Note
		The accounting server can record access time and operation for each user through Account-Start packets, Account-Update packets, and Account-Stop packets.

9.5.5 Configuring TACACS+ authentication

Configure TACACS+ authentication for the ISCOM2600G series switch as below.

Step	Command	Description

1	`Raisecom#tacacs-server [ backup ] { ipv4-address | ipv6-address } [ auth-port port-id ]`
	Example:
	`Raisecom#tacacs-server backup 10.0.0.1`
		Assign the IP address and port number for the TACACS+ authentication server. Configure the **backup** parameter to assign the backup TACACS+ authentication server.
		• backup: if this parameter is selected, the IP address of the backup TACACS+ authentication server will be configured. If this parameter is not selected, the IP address of the master TACACS+ authentication server will be configured.
		• ipv4-address: IPv4 address, in dotted decimal notation, such as 10.10.10.1
		• ipv6-address: IPv6 address, in colon decimal notation, such as 2001::3
		• auth-port port-id: authentication interface ID, an integer, ranging from 1 to 65535

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom#**tacacs-server quiet** *time* **Example:** Raisecom#tacacs-server quiet 300	Configure the time for the master TACACS+ authentication server to restore to the activation status. • time: time for the authentication server to return to the activated status, in units of minutes, ranging from 5 to 300
3	Raisecom#**tacacs-server** [**backup**] **key** *string* Raisecom#**tacacs-server** [**backup**] **encrypt-key** *string* **Example:** Raisecom#tacacs-server key raisecom	Configure the shared plaintext or ciphertext key for TACACS+ authentication. Configure the **backup** parameter to assign the backup TACACS+ authentication server. • backup: if this parameter is selected, the IP address of the backup TACACS+ accounting server will be configured. If this parameter is selected, the IP address of the master TACACS+ accounting server will be configured. • key string: key string, a string of 1 to 100 characters, supporting #, @, &, and *. • encrypt-key string: key string, a string of 1 to 270 characters
4	Raisecom#**user login** { **local-tacacs** | **tacacs-local** [**server-no-response**] | **tacacs-user** } **Example:** Raisecom#user login local-tacacs	Configure the login authentication mode to TACACS+. • local-tacacs: when local authentication coexists with TACACS+ authentication, use local authentication preferentially. • tacacs-local: when local authentication coexists with TACACS+ authentication, use TACACS+ authentication preferentially. • tacacs-user: use TACACS+ authentication. • server-no-response: use local authentication only when the TACACS+ server stops responding.
5	Raisecom#**tacacs-server response-timeout** *time* **Example:** Raisecom#tacacs-server response-timeout 10	Configure the timeout of response by the TACACS+ authentication server. • time: response timeout of the authentication server, in units of second, an integer, ranging from 3 to 100

9.5.6 Configuring TACACS+ accounting

Configure TACACS+ accounting for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**tacacs** [**backup**] **accounting-server** { *ipv4-address* | *ipv6-address* } [**acct-port** *port-id*] **Example:** Raisecom#tacacs accounting-server 10.0.0.1	Assign the IP address and UDP port number for the TACACS+ accounting server. Configure the **backup** parameter to assign the backup TACACS+ accounting server. • backup: if this parameter is selected, the IP address of the backup TACACS+ accounting server will be configured. If this parameter is not selected, the IP address of the master TACACS+ accounting server will be configured. • ipv4-address: IPv4 address, in dotted decimal notation, such as 10.10.10.1 • ipv6-address: IPv6 address, in colon decimal notation, such as 2001::3 • auth-port port-id: authentication interface ID, an integer, ranging from 1 to 65535
2	Raisecom#**tacacs** [**backup**] **accounting-server key** *string* Raisecom#**tacacs** [**backup**] **accounting-server encrypt-key** *string* **Example:** Raisecom#tacacs accounting-server key raisecom	Configure the shared plaintext or ciphertext key to communicate with the TACACS+ accounting server. • key string: key string, a string of 1 to 100 characters • encrypt-key string: key string, a string of 1 to 270 characters

9.5.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show tacacs-server**	Show configurations of the TACACS+ authentication server.
2	Raisecom#**show aaa**	Show configurations of AAA.

9.5.8 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
Raisecom#**clear tacacs statistics**	Clear TACACS+ statistics.

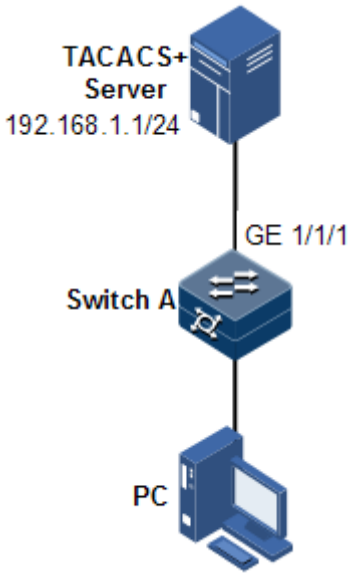
Copyright © Raisecom Technology Co., Ltd.

9.5.9 Example for configuring TACACS+

Networking requirements

As shown in Figure 9-5, configure TACACS+ authentication on Switch A to authenticate login user and control users from accessing the ISCOM2600G series switch.

Figure 9-5 TACACS+ networking



Configuration steps

Configure user login authentication through TACACS+.

```
Raisecom#tacacs-server 192.168.1.1
Raisecom#tacacs-server key raisecom
Raisecom#user login tacacs-user
```

Checking results

Use the **show tacacs-server** command to show TACACS+ configurations.

```
Raisecom#show tacacs-server
Server Address                : 192.168.1.1
Port:  49
Server Status                : Active
Backup Server Address          : --
Port:  49
Backup Server Status          : --
Server Shared Key             : YcrTxZF0aWN6
Backup Authentication server Shared Key:       --
```


Copyright © Raisecom Technology Co., Ltd.

```
Accounting server Address      : --
Port:  49
Accounting server Status      : --
Backup Accounting server Address: --
Port:  49
Backup Accounting server Status: --
Accounting server Shared Key:                --
Backup Accounting server Shared Key:          --
Total Packet Sent               : 0
Total Packet Recv               : 0
Num of Error Packets             : 0
Server Response Timeout(s):  5
Server Quiet Time(m):  30
```

9.6 Storm control

9.6.1 Introduction

The Layer 2 network is a broadcast domain. When an interface receives excessive broadcast, unknown multicast, and unknown unicast packets, broadcast storm occurs. If you do not control broadcast packets, broadcast storm may occur and occupy much network bandwidth. Broadcast storm can degrade network performance and impact forwarding of unicast packets or even lead to communication halt.

Restricting broadcast flow generated from network on Layer 2 device can suppress broadcast storm and ensure common unicast forwarding normally.

Occurrence of broadcast storm

The following flows may cause broadcast flow:

- Unknown unicast packets: unicast packets of which the destination MAC is not in the MAC address table, namely, the Destination Lookup Failure (DLF) packets. If these packets are excessive in a period, the system floods them and broadcast storm may occur.
- Unknown multicast packets: the ISCOM2600G series switch neither supports multicast nor has a multicast MAC address table, so it processes received multicast packets as unknown multicast packets.
- Broadcast packets: packets of which the destination MAC is a broadcast address. If these packets are excessive in a period, broadcast storm may occur.

Principles of storm control

Storm control allows an interface to filter broadcast packets received by the interface. After storm control is enabled, when the number of received broadcast packets reaches the pre-configured threshold, the interface will automatically discard the received packets. If storm control is disabled or if the number of received broadcast packets does not reach the pre-configured threshold, the broadcast packets are broadcasted to other interfaces of the switch properly.

Copyright © Raisecom Technology Co., Ltd.

Types of storm control

Storm controls is performed in the following forms:

- Radio (bandwidth ratio): the allowed percentage of broadcast, unknown multicast, or unknown unicast traffic to total bandwidth
- Bits Per Second (BPS): the number of bits allowed to pass per second
- Packet Per Second (PPS): the number of packets allowed to pass per second

The ISCOM2600G series switch supports BPS and PPS storm control.

9.6.2 Preparing for configurations

Scenario

Configuring storm control on Layer 2 devices can prevent broadcast storm from occurring when broadcast packets increase sharply on the network. In this case, normal packets can be properly forwarded.

Prerequisite

N/A

9.6.3 Default configurations of storm control

Default configurations of storm control are as below.

Function	Default value
Broadcast storm control	Enable
Storm control detection	Disable
Storm control mode	pps
Number of allowed storm packets per second, namely, PPS	1024
DLF packet forwarding	Enable
Action for storm control on the interface	Discarding packets
Restoration period of the interface	300s
Strom control Trap	Disable

9.6.4 Configuring storm control over interface

Caution

Storm control and VLAN-based rate limiting are exclusive. We do not recommend enabling them on the same interface concurrently.

Configure storm control for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**storm-control detection { enable | disable }** **Example:** Raisecom(config)#storm-control detection enable	Enable or disable storm control detection. • enable: enable storm control detection. • disable: disable storm control detection.
3	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1 Raisecom(config)#interface port-channel 1	Enter physical interface configuration mode, or aggregation group configuration mode. • interface-type: interface type • interface-number: interface ID
4	Raisecom(config-gigaethernet1/1/port)#**storm-control** { **broadcast** | **unknown-multicast** | **dlf** | **all** } { **bps** *value* [**burst** *value*] | **pps** *value* } Raisecom(config-port-channel*)#**storm-control** { **broadcast** | **unknown-multicast** | **dlf** | **all** } { **bps** *value* [**burst** *value*] | **pps** *value* } **Example:** Raisecom(config-gigaethernet1/1/1)#storm-control broadcast bps 1024	Enable storm control on the physical interface or LAG, and configure the storm control threshold. • broadcast: execute storm control over broadcast traffic. • unknown-multicast: execute storm control over unknown multicast traffic. • dlf: execute storm control over unknown unicast traffic. • all: control the traffic of the broadcast, the unknown multicast, and the unknown unicast. • pps value: the number of packets allowed to pass per second, an integer, ranging from 1 to 262143, in units of pcs • bps value: packet rate allowed to pass per second, an integer, ranging from 0 to 100000 in step of 64, in units of bit/s • burst value: burst packet rate, an integer, ranging from 0 to 512, in units of Kbyte/s
5	Raisecom(config-gigaethernet1/1/port)#**storm-control action** { **shutdown** | **drop** } **Example:** Raisecom(config-gigaethernet1/1/1)#storm-control action shutdown	Configure the action for storm control on the interface. • shutdown: shut down the interface. • drop: discard packets.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config-gigaethernet1/1/port)#**storm-control interval second** *interval* **Example:** Raisecom(config-gigaethernet1/1/1)#storm-control interval second 10	Configure the restoration period of the shutdown interface. • interval: restoration interval of the interface, an integer, ranging from 1 to 9000, in units of second
7	Raisecom(config-gigaethernet1/1/port)#**storm-control trap { enable | disable }** **Example:** Raisecom(config-gigaethernet1/1/1)#storm-control trap enable	Enable or disable storm control Trap. • enable: enable storm control Trap on the interface. • disable: disable storm control Trap on the interface.

Caution

- Storm control supports only one rate limiting mode at a time. When you change the rate limiting mode of one type of packets, the ISCOM2600G series switch will prompt you that the change of the rate limiting mode will cause the mode of other two types of packets to change to the same mode.
- If you configure storm control on the LAG, you cannot configure storm control on the interface; otherwise the later configuration will not take effect.

9.6.5 Configuring DLF packet forwarding

Configure DLF packet forwarding for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**dlf-forwarding { enable | disable }** **Example:** Raisecom(config)#dlf-forwarding enable	Enable or disable DLF packet forwarding on an interface. • enable: enable DLF packet forwarding. • disable: disable DLF packet forwarding.

9.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show storm-control interface** [*interface-type interface-number*]	Show configurations of storm control.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
2	`Raisecom#show dlf-forwarding`	Show DLF packet forwarding status.
3	`Raisecom#show storm-control status interface [ interface-type interface-number ]`	Show storm control status.

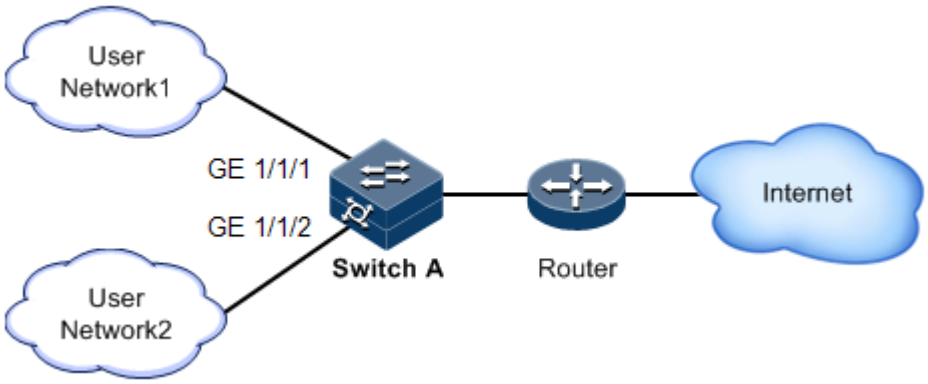
9.6.7 Example for configuring storm control

Networking requirements

As shown in Figure 9-6, when GE 1/1/1 and GE 1/1/2 on the Switch receive excessive unknown unicast packets or broadcast packets, the Switch forwards these packets to all interfaces except the Rx interface, which may cause broadcast storm and lower forwarding performance of the Switch.

To restrict impacts on Switch A caused by broadcast storm, you need to configure storm control on Switch A to control broadcast packets from user networks 1 and 2, with the threshold of 640 pps.

Figure 9-6 Storm control networking



Configuration steps

Enable storm control, and configure the threshold for storm control.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#storm-control broadcast bps 640
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#storm-control broadcast bps 640
```


Copyright © Raisecom Technology Co., Ltd.

Checking results

Use the **show storm-control** command to show configurations of storm control.

```
Raisecom#show storm-control interface
Interface     Packet-Type      Pps(pps)         Bps(Kbps)
-----------------------------------------------------------------------
GE1/1/1       Broadcast        --               640
              Multicast        --               0
              Dlf              --               0
GE1/1/2       Broadcast        --               640
              Multicast        --               0
              Dlf              --               0
```

9.7 802.1x

9.7.1 Introduction

802.1x, based on IEEE 802.1x, is a VLAN-based network access control technology. It is used to solve authentication and security problems for LAN users.

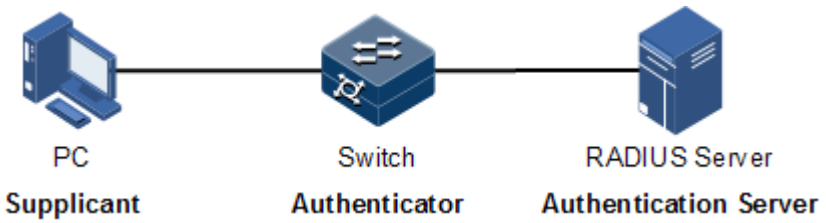
It is used to authenticate and control access devices at the physical later of the network device. It defines a point-to-point connection mode between the device interface and user devices. User devices, connected to the interface, can access resources in the LAN if they are authenticated. Otherwise, they cannot access resources in the LAN through the switch.

802.1x structure

As shown in Figure 9-7, 802.1x authentication uses Client/Server mode, including the following 3 parts:

- Supplicant: a user-side device installed with the 802.1x client software (such as Windows XP 802.1x client), such as a PC
- Authenticator: an access control device supporting 802.1x authentication, such as a switch
- Authentication Server: a device used for authenticating, authorizing, and accounting users. Generally, the RADIUS server is taken as the 802.1x authentication server.

Figure 9-7 802.1x structure



Interface access control modes

The authenticator uses the authentication server to authenticate clients that need to access the LAN and controls interface authorized/ unauthorized status through the authentication results. You can control the access status of an interface by configuring access control modes on the interface. 802.1x authentication supports the following 3 interface access control modes:

- Protocol authorized mode (auto): the protocol state machine determines the authorization and authentication results. Before clients are successfully authenticated, only EAPoL packets are allowed to be received and sent. Users are disallowed to access network resources and services provided by the switch. If clients are authorized, the interface is switched to the authorized state, allowing users to access network resources and services provided by the switch.
- Force interface authorized mode (authorized-force): the interface is in authorized state, allowing users to access network resources and services provided by the switch without being authorized and authenticated.
- Force interface unauthorized mode (unauthorized-force): the interface is in unauthorized mode. Users are disallowed to access network resources and services provided by the switch; in other words, users are disallowed to be authenticated.

802.1x authentication procedure

The 802.1x system supports the authentication process between the supplicant and the RADIUS server through EAP relay and EAP termination.

- EAP relay

The supplicant and the authentication server exchange information through the Extensible Authentication Protocol (EAP) packet while the supplicant and the authenticator exchange information through the EAP over LAN (EAPoL) packets. The EAP packet is encapsulated with authentication data. This authentication data will be encapsulated into the RADIUS packet to be transmitted to the authentication server through a complex network. This procedure is called EAP relay.

Both the authenticator and the suppliant can initiate the 802.1x authentication procedure. This document takes the suppliant for example, as shown below:

Step 1 The user enters the user name and password. The supplicant sends an EAPoL-Start packet to the authenticator to start the 802.1x authentication.

Step 2 The authenticator sends an EAP-Request/Identity to the suppliant, asking the user name of the suppliant.

Step 3 The suppliant replies an EAP-Response/Identity packet to the authenticator, which includes the user name.

Step 4 The authenticator encapsulates the EAP-Response/Identity packet to the RADIUS packet and sends the RADIUS packet to the authentication server.

Step 5 The authentication server compares the received user name with the one in the database, finds the password for the user, and encrypts the password with a randomly-generated encryption word. Meanwhile it sends the encryption word to the authenticator who then sends the encryption word to the suppliant.

Step 6 The suppliant encrypts the password with the received encryption password, and sends the encrypted password to the authentication server.

Copyright © Raisecom Technology Co., Ltd.

Step 7 The authentication server compares the received encrypted password with the one generated by itself. If identical, the authenticator modifies the interface state to authorized state, allowing users to access the network through the interface and sends an EAP-Success packet to the suppliant. Otherwise, the interface is in unauthorized state and sends an EAP-Failure packet to the suppliant.

- EAP termination

Terminate the EAP packet at the device and map it to the RADIUS packet. Use standard RADIUS protocol to finish the authorization, authentication, and accounting procedure. The device and RADIUS server adopt Password Authentication Protocol (PAP)/Challenge Handshake Authentication Protocol (CHAP) to perform authentication.

In the EAP termination mode, the random encryption character, used for encrypting the password, is generated by the device. And then the device sends the user name, random encryption character, and encrypted password to the RADIUS server for authentication.

802.1x timers

802.1x authentication involves the following 5 timers:

- Reauth-period: re-authorization t timer. After the period is exceeded, the ISCOM2600G series switch re-initiates authorization.
- Quiet-period: quiet timer. When user authorization fails, the ISCOM2600G series switch needs to keep quiet for a period. After the period is exceeded, the ISCOM2600G series switch re-initiates authorization. During the quiet time, the ISCOM2600G series switch does not process authorization packets.
- Tx-period: transmission timeout timer. When the ISCOM2600G series switch sends a Request/Identity packet to users, the ISCOM2600G series switch will initiate the timer. If users do not send an authorization response packet during the tx-period, the ISCOM2600G series switch will re-send an authorization request packet. The ISCOM2600G series switch sends this packet three times in total.
- supp-timeout: Supplicant authorization timeout timer. When the ISCOM2600G series switch sends a Request/Challenge packet to users, the ISCOM2600G series switch will initiate supp-timeout timer. If users do not send an authorization response packet during the supp-timeout, the ISCOM2600G series switch will re-send the Request/Challenge packet. The ISCOM2600G series switch sends this packet twice in total.
- Server-timeout: authentication server timeout timer. The timer defines the total timeout of sessions between the authorizer and RADIUS server. When the configured time expires, the authenticator will end the session with the RADIUS server and start a new authorization process.

9.7.2 Preparing for configruations

Scenario

To realize access authentication on LAN users and ensure access user security, you need to configure 802.1x authentication on the ISCOM2600G series switch.

If users are authenticated, they are allowed to access network resources. Otherwise, they cannot access network resources. By performing authentication control on user access interface, you can manage the users.

Copyright © Raisecom Technology Co., Ltd.

Prerequisite

If RADIUS authentication server is used, you need to perform following operations before configuring 802.1x authentication:

- Configure the IP address of the RADIUS server and the RADIUS shared key.
- The ISCOM2600G series switch can ping through the RADIUS server successfully.

9.7.3 Default configurations of 802.1x

Default configurations of 802.1x are as below.

Function	Default value
Global 802.1x	Disable
Interface 802.1x	Disable
Global authentication mode	Chap
Interface access control mode	Auto
Authentication method	Portbased
RADIUS server expiration timer	5s
Re-authentication	Disable
802.1x re-authentication timer	3600s
802.1x quiet timer	60s
Transmission timeout timer	30s
Supplicant authorization timeout timer	30s
Maximum number of users	512

9.7.4 Configuring basic functions of 802.1x

Caution

- 802.1x and STP are exclusive on the same interface. You cannot enable them concurrently.
- Only one user authentication request is processed on an interface at a time.

Configure basic functions of 802.1x for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#dot1x { enable | disable }`
	Example:
	`Raisecom(config)#dot1x enable`
		Enable or disable global 802.1x.
		• enable: enable global 802.1x.
		• disable: disable global 802.1x.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**dot1x authentication-method** { **chap** | **pap** | **eap** } **Example:** Raisecom(config)#dot1x authentication-method chap	Configure global authentication mode. • chap: three-way handshaking protocol that only transmits user name through the network. It does not transmit password during authentication and thus is more secure and reliable. • pap: two-way handshaking protocol that transmits the password in clear text • eap: the switch will directly send authorization information of 802.1x users to the RADIUS server in form of EAP packets without converting them into standard RADIUS packets. To configure this mode, the RADIUS server must support EAP.
4	Raisecom(config)#**dot1x auth-mode** { **radius** | **local** | **tacacs+** } **Example:** Raisecom(config)#dot1x auth-mode local	Configure the mode of 802.1x authentication. • radius: configure the 802.1x authentication mode to RADIUS server authentication. • local: configure the 802.1x authentication mode to local authentication. • tacacs+: configure the 802.1x authentication mode to TACACS+ server authentication.
5	Raisecom(config)#**dot1x free-ip** *ip-address* [*ip-mask* | *mask-length*] **Example:** Raisecom(config)#dot1x free-ip 10.1.1.0 24	Configure the IP address segment available for 802.1x terminal users who fail to be authenticated or exit authentication. • ip-address: IP address segment that is free of authentication, in dotted decimal notation, such as 10.10.10.0 • ip-mask: mask address, in dotted decimal notation, such as 255.255.255.0 • mask-length: mask length, an integer, ranging from 1 to 32
6	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.
7	Raisecom(config-gigaethernet1/1/port)#**dot1x** { **enable** | **disable** } **Example:** Raisecom(config-gigaethernet1/1/1)#dot1x enable	Enable or disable interface 802.1x. • enable: enable interface 802.1x. • disable: enable interface 802.1x.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
8	Raisecom(config-gigaethernet1/1/port)#**dot1x auth-control** { **auto** | **authorized-force** | **unauthorized-force** } **Example:** Raisecom(config-gigaethernet1/1/1)#dot1x auth-control authorized-force	Configure access control mode on the interface. • authorized-force: forced-authorized mode. The interface is in authorized status. Users can access the network without authentication. • unauthorized-force: forced-unauthorized mode. The interface is in unauthorized status. User authentication is not allowed. Users cannot access the network. • auto: automatic-recognition mode. User authentication is allowed. The user can access the network once being authenticated.
9	Raisecom(config-gigaethernet1/1/port)#**dot1x auth-method** { **portbased** | **macbased** } **Example:** Raisecom(config-gigaethernet1/1/1)#dot1x auth-method macbased	Configure access control mode of 802.1x authentication on the interface. • macbased: MAC-based mode. Users cannot access the network through one account on the same interface. Only the last user authenticated by the interface can access the network. • portbased: port-based mode. Users can access the network without authentication as long as the first user on the interface is successfully authenticated.
10	Raisecom(config-gigaethernet1/1/port)#**dot1x keepalive** { **enable** | **disable** } **Example:** Raisecom(config-gigaethernet1/1/1)#dot1x keepalive disable	Enable or disable 802.1x handshake on the interface. • keepalive: interface handshake • enable: enable 802.1x handshake. • disable: disable 802.1x handshake.
11	Raisecom(config-gigaethernet1/1/port)#**dot1x max-user** *user-number* **Example:** Raisecom(config-gigaethernet1/1/1)#dot1x max-user 100	Configure the maximum number of users allowed to be authenticated by the 802.1x interface. • user-number: maximum number of users, an integer, ranging from 1 to 400
12	Raisecom(config-gigaethernet1/1/port)#**dot1x guest-vlan** *vlan-id* **Example:** Raisecom(config-gigaethernet1/1/1)#dot1x guest-vlan 1	Configure the 802.1x Guest VLAN of the specified interface. • vlan-id: Guest VLAN ID, an integer, ranging from 1 to 4094

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

13	`Raisecom(config-gigaethernet1/1/port)#dot1x auth-free voice-vlan`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#dot1x auth-free voice-vlan`
		Configure authentication-free for voice terminals on the specified interface.

Note

If 802.1x is disabled in global/interface configuration mode, the interface access control mode of 802.1x is configured to force interface authorized mode.

9.7.5 Configuring 802.1x re-authentication

Caution

Re-authentication is initiated for authorized users. Before enabling re-authentication, you must ensure that global/interface 802.1x is enabled. Authorized interfaces are still in this mode during re-authentication. If re-authentication fails, the interfaces are in unauthorized state.

Configure 802.1x re-authentication for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.
3	`Raisecom(config-gigaethernet1/1/port)#dot1x reauthentication { enable | disable }` `Raisecom(config-gigaethernet1/1/1)#dot1x reauthentication enable`	Enable or disable 802.1x re-authentication. • enable: enable 802.1x re-authentication. • disable: disable 802.1x re-authentication.

9.7.6 Configuring 802.1x timers

Configure 802.1x timers for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.
3	Raisecom(config-gigaethernet1/1/port)#**dot1x timer reauth-period** *second* **Example:** Raisecom(config-gigaethernet1/1/1)#dot1x timer reauth-period 1000	Configure the time of the re-authentication timer. • second: time of the re-authentication timer, an integer, ranging from 1 to 65535, in units of second
4	Raisecom(config-gigaethernet1/1/port)#**dot1x timer quiet-period** *second* **Example:** Raisecom(config-gigaethernet1/1/1)#dot1x timer quiet-period 100	Configure the time of the quiet timer. • second: time of the quiet timer, an integer, ranging from 1 to 120, in units of second
5	Raisecom(config-gigaethernet1/1/port)#**dot1x timer supp-timeout** *second* **Example:** Raisecom(config-gigaethernet1/1/1)#dot1x timer supp-timeout 100	Configure the time of the supplicant authorization timeout timer. • second: time of the supplicant authorization timeout timer, an integer, ranging from 1 to 120, in units of second
6	Raisecom(config-gigaethernet1/1/port)#**dot1x timer tx-period** *second* **Example:** Raisecom(config-gigaethernet1/1/1)#dot1x timer tx-period 100	Configure the period for sending Request/Identity packets, namely, the packet retransmission period. • Second: timer time, an integer, ranging from 10 to 120, in units of second
7	Raisecom(config-gigaethernet1/1/port)#**dot1x timer server-timeout** *second* **Example:** Raisecom(config-gigaethernet1/1/1)#dot1x timer server-timeout 200	Configure the time of the authentication server timeout timer. • second: time of the authorization server timeout timer, an integer, ranging from 3 to 300, in units of second
8	Raisecom(config-gigaethernet1/1/port)#**dot1x timer keepalive-period** *second* **Example:** Raisecom(config-gigaethernet1/1/1)#dot1x timer keepalive-period 30	Configure the period for retransmitting KeepAlive packets by interface 802.1x. • second: period for retransmitting KeepAlive packets, an integer, ranging from 1 to 65535, in units of second

Copyright © Raisecom Technology Co., Ltd.

9.7.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show dot1x interface-type interface-number`	Show 802.1x configurations on the interface.
2	`Raisecom#show dot1x interface-type interface-number statistics`	Show 802.1x statistics on the interface.
3	`Raisecom#show dot1x interface-type interface-number user`	Show user information of 802.1x authentication on the interface.
4	`Raisecom#show dot1x free-ip`	Configure the IP address segment available for 802.1x terminal users who fail to be authenticated or exit authentication.

9.7.8 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description

`Raisecom(config)#clear dot1x interface-type interface-number statistics`
Example:
`Raisecom(config)#clear dot1x gigaethernet 1/1/1 statistics`
	Clear interface 802.1x statistics.
	• interface-type: interface type
	• interface-number: in the form of unit/slot/port. The value range depends on the interface type.

9.7.9 Example for configuring 802.1x

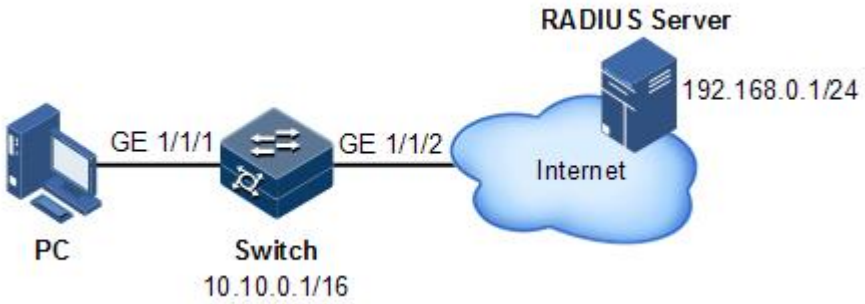
Networking requirements

As shown in Figure 9-8, the network administrator configures 802.1x to control the PC to access the Internet.

- For the switch: the IP address is 10.10.0.1, the mask is 255.255.0.0, and default gateway is 10.10.0.2.
- The RADIUS server works to authenticate and authorize PCs. Its IP address is 192.168.0.1, and the password is raisecom.
- The interface control mode is auto.
- After the PC passes authentication, the Switch will start reauthentication every 600s.

Copyright © Raisecom Technology Co., Ltd.

Figure 9-8 Dot1x networking



Configuration steps

Step 1 Configure the IP addresses of the Switch and RADIUS server.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 10.10.0.1 255.255.0.0
Raisecom(config-vlan1)#exit
Raisecom(config)#ip route 0.0.0.0 0.0.0.0 10.10.0.2
Raisecom(config)#exit
Raisecom#radius 192.168.0.1
Raisecom#radius-key raisecom
```

Step 2 Enable global 802.1x and interface 802.1x.

```
Raisecom#config
Raisecom(config)#dot1x enable
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#dot1x enable
```

Step 3 (Optional) configure interface authorization mode to auto. By default, authentication is required and thus does not need to be configured.

```
Raisecom(config-gigaethernet1/1/1)#dot1x auth-control auto
```

Step 4 Enable reauthentication, and configure the timer to 600s.

```
Raisecom(config-gigaethernet1/1/1)#dot1x reauthentication enable
Raisecom(config-gigaethernet1/1/1)#dot1x timer reauth-period 600
```


Copyright © Raisecom Technology Co., Ltd.

Checking results

Use the **show dot1x** command to show 802.1x configurations on the interface.

```
Raisecom#show dot1x gigaethernet 1/1/1
802.1x Global Admin State: enable
802.1x Authentication Method: chap
802.1x Authentication Mode: radius
802.1x allowed max user number: 512
-------------------------------------------------------
Port gigaethernet1/1/1
-------------------------------------------------------
802.1X Port Admin State: Enable
PAE: Authenticator
PortMethod: Portbased
PortControl: Auto
ReAuthentication: Enable
KeepAlive: Enable
QuietPeriod: 60(s)
ServerTimeout: 5(s)
SuppTimeout: 30(s)
ReAuthPeriod: 600(s)
TxPeriod: 30(s)
KeepalivePeriod: 60(s)
MaxUserNum: 512
GuestVlanID: 0
AuthFree Protocol: None
```

9.8 IP Source Guard

9.8.1 Introduction

IP Source Guard uses a binding table to defend against IP Source spoofing and solve IP address embezzlement without identity authentication. IP Source Guard can cooperate with DHCP Snooping to generate dynamic binding. In addition, you can configure static binding manually. DHCP Snooping filters untrusted DHCP packets by establishing and maintaining the DHCP binding database.

IP Source Guard binding entry

IP Source Guard is used to match packet characteristics, including source IP address, source MAC address, and VLAN tags, and can support the interface to be combined with the following characteristics (hereinafter referred to as binding entries):

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

Copyright © Raisecom Technology Co., Ltd.

According to the generation mode of binding entries, IP Source Guard can be divided into static binding and dynamic binding:

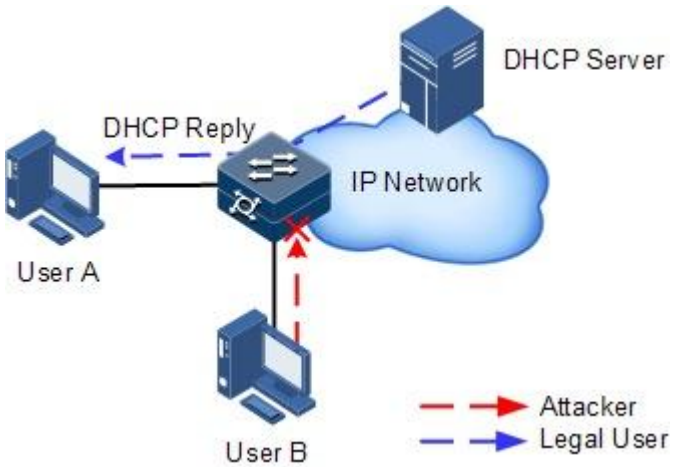
- Static binding: configure binding information manually and generate binding entry to complete the interface control, which fits for the case where the number of hosts is small or where you need to perform separate binding on a single host.
- Dynamic binding: obtain binding information automatically from DHCP Snooping to complete the interface control, which fits for the case where there are many hosts and you need to adopt DHCP to perform dynamic host configurations. Dynamic binding can effectively prevent IP address conflict and embezzlement.

Principles of IP Source Guard

Principles of IP Source Guard are to create an IP source binding table within the ISCOM2600G series switch. The IP source binding table is taken as the basis for each interface to test received data packets. Figure 9-9 shows principles of IP Source Guard.

- If the received IP packets meet the relationship of Port/IP/MAC/VLAN binding entries in IP source binding table, forward these packets.
- If the received IP packets are DHCP data packets, forward these packets.
- Otherwise, discard these packets.

Figure 9-9 Principles of IP Source Guard



Before forwarding IP packets, the ISCOM2600G series switch compares the source IP address, source MAC address, interface ID, and VLAN ID of the IP packets with the binding table. If the information matches, it indicates that the user is legal and the packets are permitted to forward normally. Otherwise, the user is an attacker and the IP packets are discarded.

9.8.2 Preparing for configurations

Scenario

There are often some IP source spoofing attacks on the network. For example, the attacker forges legal users to send IP packets to the server, or the attacker forges the source IP address of another user to communicate. This prevents legal users from accessing network services normally.

Copyright © Raisecom Technology Co., Ltd.

With IP Source Guard binding, you can filter and control packets forwarded by the interface, prevent the illegal packets from passing through the interface, thus to restrict the illegal use of network resources and improve the interface security.

Prerequisite

Enable DHCP Snooping if there are DHCP users.

9.8.3 Default configurations of IP Source Guard

Default configurations of IP Source Guard are as below.

Function	Default value
IP Source Guard static binding	Disable
IP Source Guard dynamic binding	Disable
Interface trust status	Untrusted

9.8.4 Configuring interface trust status of IP Source Guard

Configure the interface trust status of IP Source Guard for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.
3	`Raisecom(config-gigaethernet1/1/port)#ip verify source trust`	(Optional) configure the interface to a trusted interface. Use the **no ip verify source trust** command to configure the interface as an untrusted interface. In this case, all packets, except DHCP packets and IP packets that meet binding relation, are not forwarded. When the interface is in trusted status, all packets are forwarded normally.
4	`Raisecom(config-gigaethernet1/1/port)#ip v6 verify source trust`	(Optional) configure the IPv6 interface to trusted status.

Copyright © Raisecom Technology Co., Ltd.

9.8.5 Configuring IP Source Guard binding

Configuring IP Source Guard static binding

Configure IP Source Guard static binding for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip verify source`	Enable IP Source Guard static binding.
3	`Raisecom(config)#ip source binding` *`ip-address`* `[` *`ip-mask-address`* `|] [` *`mac-address`* `|] [ vlan` *`vlan-id`* `}]` *`interface-type interface-number`* **Example:** `Raisecom(config)#ip source binding 1.2.3.4 gigaethernet 1/1/1`	Configure static binding. • ip-address: IP address, in dotted decimal notation, such as 10.0.0.1 • ip-mask-address: IP address mask, in dotted decimal notation, such as 255.0.0.0 • mac-address: MAC address, in dotted hexadecimal notation, such as 000E.5E12.3456 • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • interface-type: interface type • interface-number: interface ID. The form and value range depend on the interface type.
4	`Raisecom(config)#ipv6 verify source`	Enable IPv6 static binding.
5	`Raisecom(config)#ipv6 source binding` *`ipv6-address`* `[` *`mac-address`* `|] [ vlan` *`vlan-id`* `]` *`interface-type interface-number`* `Raisecom(config)#ipv6 source binding prefix` *`ipv6-address/prefix-length`* `[` *`mac-address`* `] [ vlan` *`vlan-id`* `]` *`interface-type interface-number`* **Example:** `Raisecom(config)#ipv6 source binding 3001::1 gigaethernet 1/1/1`	Configure IPv6 static binding. • ipv6-address: IPv6 address, in colon hexadecimal notation, such as 3001::1 • mac-address: MAC address, in colon hexadecimal notation, such as 000E.5E12.3456 • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • interface-type: interface type • interface-number: interface ID. The form and value range depend on the interface type. • static-all: all existing static binding entries • prefix ipv6-address/prefix-length: IPv6 address with a prefix, such as 1:123::0:1/96

Note

- The configured static binding does not take effect when global static binding is disabled. Only when global static binding is enabled can the static binding take effect.
- For an identical IP address, the manually configured static binding will cover the dynamic binding. However, it cannot cover the existing static binding. When the

Copyright © Raisecom Technology Co., Ltd.

static binding is deleted, the system will recover the covered dynamic binding automatically.

Configuring IP Source Guard dynamic binding

Configure IP Source Guard dynamic binding for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip verify source dhcp`	Enable IP Source Guard dynamic binding.
3	`Raisecom(config)#ipv6 verify source dhcp-snooping`	Enable IPv6 Source Guard dynamic binding.

Note

- The dynamic binding learnt through DHCP Snooping does not take effect when global dynamic binding is disabled. Only when global dynamic binding is enabled can the dynamic binding take effect.
- If an IP address exists in the static binding table, the dynamic binding does not take effect. In addition, it cannot cover the existing static binding.

Configuring binding translation

Configure binding translation for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip verify source dhcp`	Enable IP Source Guard dynamic binding.
3	`Raisecom(config)#ip source binding dhcp static`	Translate the dynamic binding to the static binding.
4	`Raisecom(config)#ip source binding auto-update`	(Optional) enable auto-translation. After it is enabled, dynamic binding entries learned through DHCP Snooping are directly translated into static binding entries.

9.8.6 Configuring priority and rate limit of IP source guard

Configure the priority and rate limit of IP source guard for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#ip verify source [ ip-address ip-mask ] set-cos cos-value [ rate-limit rate-value burst-value ]`
	Example:
	`Raisecom(config)#ip verify source set-cos 1`
		Configure the priority and rate limit of IP source guard.
		• ip-address: source IP address of the data packet, in dotted decimal notation, such as 10.0.0.1
		• ip-mask: mask of the source IP address of the data packet, in dotted decimal notation, such as 255.0.0.0
		• cos-value: CoS priority, an integer, ranging from 0 to 7
		• rate-value: rate limit, an integer, ranging from 1 to 1048576, in units of Kbps
		• burst-value: burst value, an integer, ranging from 1 to 2048, in units of Kbyte

9.8.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show ip verify source`	Show global binding status and interface trusted status.
2	`Raisecom#show ip source binding [ interface-type interface-number ]`	Show configurations of IP Source Guard binding, interface trusted status, and binding table.
3	`Raisecom#show ip verify source set-cos`	Show priority configurations.
4	`Raisecom#show ipv6 source binding [ interface-type interface-number ]`	Show binding information about IPv6 Source Guard.
5	`Raisecom#show ipv6 verify source`	Show the IPv6 global binding status and interface trusted status.

9.8.8 Example for configuring IP Source Guard

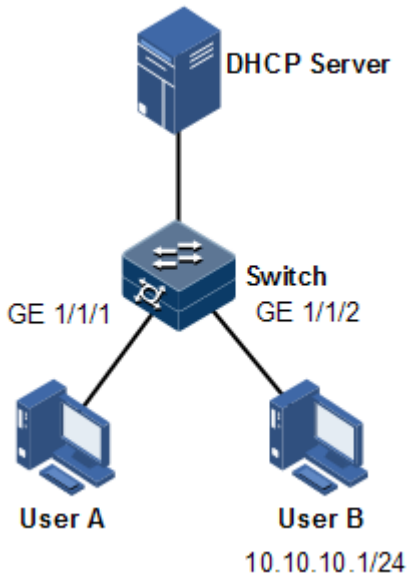
Networking requirements

As shown in Figure 9-10, to prevent IP address embezzlement, you need to configure IP Source Guard on the Switch.

- The Switch permits all IP packets on GE 1/1/1 to pass.
- GE 1/1/2 permits those IP packets to pass, of which the IP address is 10.10.10.1, the subnet mask is 255.255.255.0, and the status meets the dynamic binding learnt by DHCP Snooping.
- Other interfaces only permit the packets meeting DHCP Snooping learnt dynamic binding to pass.

Copyright © Raisecom Technology Co., Ltd.

Figure 9-10 Configuring IP Source Guard



Configuration steps

Step 1 Configure GE 1/1/1 to the trusted interface.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#ip verify source trust
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 2 Configure static binding.

```
Raisecom(config)#ip verify source
Raisecom(config)#ip source binding 10.10.10.1 gigaethernet 1/1/2
```

Step 3 Enable global dynamic IP Source Guard binding.

```
Raisecom(config)#ip verify source dhcp
```

Checking results

Use the **show ip source binding** command to show configurations of the static binding table.

```
Raisecom#show ip source binding
```

```
History Max Entry Num: 1
Current Entry Num: 1
Ip Address        Mask                Mac Address     VLAN   Port
Type           Inhw
-----------------------------------------------------------------------
---------------------------------------------
10.10.10.1        255.255.255.255       --            --
gigaethernet1/1/2         static         yes
```

Use the **show ip verify source** command to show interface trusting status and configurations of IP Source Guard static/dynamic binding.

```
Raisecom#show ip verify source
Static Bind: Enable
Dhcp Bind: Enable
Port                        Trust
---------------------------------------
gigaethernet1/1/1             yes
gigaethernet1/1/2             no
gigaethernet1/1/3             no
gigaethernet1/1/4             no
gigaethernet1/1/5             no
gigaethernet1/1/6             no
gigaethernet1/1/7             no
gigaethernet1/1/8             no
gigaethernet1/1/9             no
gigaethernet1/1/10            no
……
```

9.9 PPPoE+

9.9.1 Introduction

PPPoE Intermediate Agent (PPPoE+) is used to process authentication packets. PPPoE+ adds more information about access devices into the authentication packet to bind account and access device so that the account is not shared and stolen, and the carrier's and users' interests are protected. This provides the server with enough information to identify users, avoiding account sharing and theft and ensuring the network security.

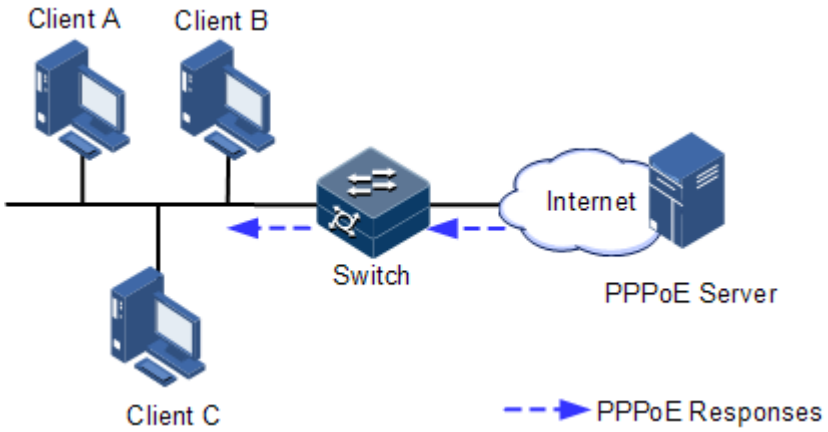
In PPPoE dial-up mode, you can access the network through various interfaces on the device as long as authentication by the authentication server is successful.

However, the server cannot accurately differentiate users just by the authentication information, which contains the user name and password. With PPPoE+, besides the user name and the password, other information, such as the interface ID, is included in the authentication packet for authentication. If the interface ID identified by the authentication server cannot match with the configured one, authentication will fail. This helps prevent illegal users from stealing accounts of other legal users for accessing the network.

Copyright © Raisecom Technology Co., Ltd.

The PPPoE protocol adopts Client/Server mode, as shown in Figure 9-11. The Switch acts as a relay agent. Users access the network through PPPoE authentication. If the PPPoE server needs to locate users, more information should be contained in the authentication packet.

Figure 9-11 Accessing the network through PPPoE authentication



To access the network through PPPoE authentication, you need to pass through the following 2 stages: discovery stage (authentication stage) and session stage. PPPoE+ is used to process packets at the discovery stage. The following steps show the whole discovery stage.

Step 1 To access the network through PPPoE authentication, the client sends a broadcast packet PPPoE Active Discovery Initiation (PADI). This packet is used to query the authentication server.

Step 2 After receiving the PADI packet, the authentication server replies a unicast packet PPPoE Active Discovery Offer (PADO).

Step 3 If multiple authentication servers reply PADO packets, the client selects one from them and then sends a unicast PPPoE Active Discovery Request (PADR) to the authentication server.

Step 4 After receiving the PADR packet, if the authentication server believes that the user is legal, it sends a unicast packet PPPoE Active Discovery Session-confirmation (PADS) to the client.

PPPoE is used to add user identification information in to PADI and PADR. Therefore, the server can identify whether the user identification information is identical to the user account for assigning resources.

9.9.2 Preparing for configurations

Scenario

To prevent illegal client access during PPPoE authentication, you need to configure PPPoE+ to add additional user identification information in PPPoE packets for network security.

Because the added user identification information is related to the specified switch and interface, the authentication server can bind the user with the switch and interface to effectively prevent account sharing and theft. In addition, this helps users enhance network security.

Prerequisite

N/A

Copyright © Raisecom Technology Co., Ltd.

9.9.3 Default configurations of PPPoE+

Default configurations of I PPPoE+ are as below.

Function	Default value
Global PPPoE	Disable
Interface PPPoE	Disable
Padding mode of Circuit ID	Switch
Circuit ID information	Interface ID/VLAN ID/attached string
Attached string of Circuit ID	hostname
Padded MAC address of Remote ID	MAC address of the switch
Padding mode of Remote ID	Binary
Interface trusted status	Untrusted
Tag overriding	Disable

Note

By default, PPPoE packets are forwarded without being attached with any information.

9.9.4 Configuring basic functions of PPPoE+

Caution

PPPoE+ is used to process PADI and PADR packets. It is designed for the PPPoE client. Generally, PPPoE+ is only enabled on interfaces that are connected to the PPPoE client. Trusted interfaces are interfaces through which the switch is connected to the PPPoE server. PPPoE+ and trusted interface are exclusive; in other words, an interface enabled with PPPoE+ cannot be configured as a trusted interface.

Enabling PPPoE+

After global PPPoE+ and interface PPPoE+ is enabled, PPPoE authentication packets sent to the interface will be attached with user information and then are forwarded to the trusted interface.

Enable PPPoE+ for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#pppoeagent { enable | disable }`
	`Example:`
	`Raisecom(config)#pppoeagent enable`
		Enable or disable global PPPoE+.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

3	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: in the form of unit/slot/port. The value range depends on the interface type.

4	`Raisecom(config-gigaethernet1/1/port)#pppoeagent { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#pppoeagent enable`
		Enable or disable interface PPPoE+.
		• enable: enable PPPoE+.
		• disable: disable PPPoE+.

Configuring PPPoE trusted interface

The PPPoE trusted interface can be used to prevent PPPoE server from being cheated and avoid security problems because PPPoE packets are forwarded to other non-service interfaces. Generally, the interface connected to the PPPoE server is configured to the trusted interface. PPPoE packets from the PPPoE client to the PPPoE server are forwarded by the trusted interface only. In addition, only PPPoE received from the trusted interface can be forwarded to the PPPoE client.

Configure the PPPoE trusted interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: in the form of unit/slot/port. The value range depends on the interface type.

3	`Raisecom(config-gigaethernet1/1/port)#pppoeagent trust`	Configure the PPPoE trusted interface.

Note

Because PPPoE+ is designed for the PPPoE client instead of the PPPoE server, downlink interfaces of the device cannot receive the PADO and PADS packets. It means that interfaces, where PPPoE+ is enabled, should not receive PADO and PADS packet. If there interfaces receive these packets, it indicates that there are error packets and the packets should be discarded. However, these interfaces can forward PADO and PADS packets of trusted packet. In addition, PADI and PADR packets are forwarded to the trusted interface only.

Copyright © Raisecom Technology Co., Ltd.

9.9.5 Configuring PPPoE+ packet information

PPPoE is used to process a specified Tag in PPPoE packets. This Tag contains Circuit ID and Remote ID.

- Circuit ID: is padded with the VLAN ID, interface ID, and host name of request packets at the RX client.
- Remote ID: is padded with the MAC address of the client or the switch.

Configuring Circuit ID

The Circuit ID has 2 padding modes: Switch mode and ONU mode. By default, Switch mode is adopted. In ONU mode, the Circuit ID has a fixed format. The following commands are used to configure the padding contents of the Circuit ID in Switch mode.

In switch mode, the Circuit ID supports 2 padding modes:

- Default mode: when customized Circuit ID is not configured, the padding content is the VLAN ID, interface ID, or the attached string. If the attached string is not defined, it is configured to hostname by default.
- Customized mode: when customized Circuit ID is configured, the padding content is the Circuit ID string.

Configure Circuit ID for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#pppoeagent circuit-id { attach-string | format | hex } string`
	Example:
	`Raisecom(config)#pppoeagent circuit-id attach-string user01`
		Configure the attached string of Circuit ID.
		• attach-string: any fixed string
		• format: variable parameters
		• hex: hexadecimal notion
		• string: attached string, with the length ranging from 1 to 55 bytes. If the string contains spacing, bracket the string in double-quotes.

3	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: in the form of unit/slot/port. The value range depends on the interface type.

4	`Raisecom(config-gigaethernet1/1/port)#pppoeagent circuit-id string`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#pppoeagent circuit-id raisecom`
		(Optional) configure the Circuit ID to the customized string.
		string: content of the circuit ID, a string 1 to 63 characters. If the circuit ID contains spacing, bracket the whole character string with quotes.

In default mode, the Circuit ID contains an attached string. By default, the attached string is configured to the hostname of the switch. You can configure it to a customized string.

Copyright © Raisecom Technology Co., Ltd.

Configure the attached string of the Circuit ID for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#pppoeagent circuit-id attach-string string`
	Example:
	`Raisecom(config)#pppoeagent circuit-id attach-string user01`
		(Optional) configure the attached string of the Circuit ID.
		If the Circuit ID is in default mode, attached string configured by this command will be added to the Circuit ID.
		• attach-string: any fixed string
		• string: attached string, with the length ranging from 1 to 55 bytes. If the string contains spacing, bracket the string in double-quotes.

Configuring Remote ID

The Remote ID is padded with a MAC address of the switch or a client. In addition, you can specify the form (binary/ASCII) of the MAC address.

Configure the Remote ID for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: in the form of unit/slot/port. The value range depends on the interface type.

3	`Raisecom(config-gigaethernet1/1/port)#pppoeagent remote-id { client-mac | switch-mac | user-define string }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#pppoeagent remote-id client-mac`
		(Optional) configure PPPoE+ Remote ID to be padded with the MAC address.
		• client-mac: pad the remote ID with the client MAC address.
		• switch-mac: pad the remote ID with the switch MAC address.
		• user-define string: string defined by the user

4	`Raisecom(config-gigaethernet1/1/port)#pppoeagent remote-id format { ascii | binary }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#pppoeagent remote-id format ascii`
		(Optional) configure the padding modes of the PPPoE+ Remote ID.
		• ascii: padding the remote ID in the ASCII format
		• binary: padding the remote ID in the binary format.

Copyright © Raisecom Technology Co., Ltd.

Configuring Tag overriding

Tags of some fields may be forged by the client because of some reasons. The client overrides the original Tags. After Tag overriding is enabled, if PPPoE packets contain Tags, these Tags are overridden. If not, add Tags to these PPPoE packets.

Configure Tag overriding for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: in the form of unit/slot/port. The value range depends on the interface type.

3	`Raisecom(config-gigaethernet1/1/1)#pppoeagent vendor-specific-tag overwrite { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#pppoeagent vendor-specific-tag overwrite enable`
		Enable or disable Tag overriding on the specified interface.
		• enable: enable Tag overriding on the specified interface.
		• disable: disable Tag overriding on the specified interface.

9.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show pppoeagent [ interface-type interface-number ]`	Show PPPoE+ configurations.
2	`Raisecom#show pppoeagent statistic [ interface-type interface-number ]`	Show PPPoE+ statistics.

9.9.7 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description

`Raisecom(config)#clear pppoeagent statistic [ interface-type interface-number ]`
Example:
`Raisecom(config)#clear pppoeagent statistic gigaethernet 1/1/1`
	Clear PPPoE+ statistics. The device supports clearing PPPoE+ statistics on the specified interface.
	• interface-type: interface type
	• interface-number: in the form of unit/slot/port. The value range depends on the interface type.

Copyright © Raisecom Technology Co., Ltd.

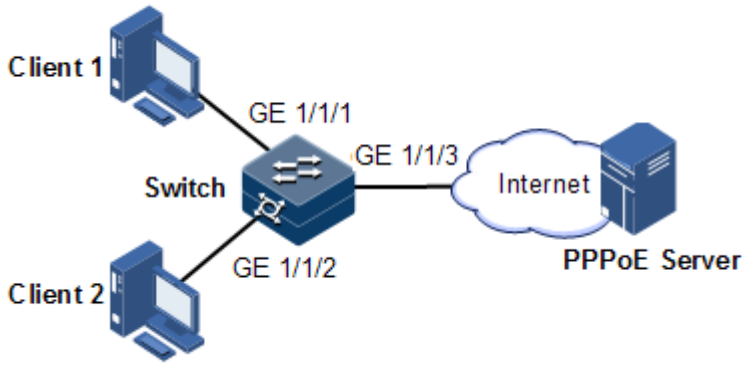
9.9.8 Example for configuring PPPoE+

Networking requirements

As shown in Figure 9-12, to prevent illegal clients from accessing and managing legal users, you can configure PPPoE+ on the Switch.

- GE 1/1/1 and GE 1/1/2 are connected to Client 1 and Client 2 respectively. GE 1/1/3 is connected to the PPPoE server.
- Enable global PPPoE+, and PPPoE on GE 1/1/1 and GE 1/1/2. Configure GE 1/1/3 as the trusted interface.
- Configure the attached string of Circuit ID to raisecom, padding information about Circuit ID on GE 1/1/1 to user01, padding information about Circuit ID on GE 1/1/2 to the MAC address of Client 2, in ASCII format.
- Enable Tag overwriting on GE 1/1/1 and GE 1/1/2.

Figure 9-12 PPPoE+ networking



Configuration steps

Step 1 Configure GE 1/1/3 as the trusted interface.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#pppoeagent trust
Raisecom(config-gigaethernet1/1/3)#exit
```

Step 2 Configure packet information about GE 1/1/1 and GE 1/1/2.

```
Raisecom(config)#pppoeagent circuit-id attach-string raisecom
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#pppoeagent circuit-id user01
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#pppoeagent remote-id client-mac
```


Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config-gigaethernet1/1/2)#pppoeagent remote-id format ascii
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 3 Enable Tag overwriting on GE 1/1/1 and GE 1/1/2.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#pppoeagent vendor-specific-tag
overwrite enable
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#pppoeagent vendor-specific-tag
overwrite enable
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 4 Enable global PPPoE+, and PPPoE on GE 1/1/1 and GE 1/1/2.

```
Raisecom(config)#pppoeagent enable
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#pppoeagent enable
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#pppoeagent enable
```

Checking results

Use the **show pppoeagent** command to show PPPoE+ configurations.

```
Raisecom#show pppoeagent
Global PPPoE+ status: enable
Attach-string: %default%
Circuit ID padding mode: switch

Port        :gigaethernet1/1/1
State       :enable
Overwrite    :enable
Format-rules :binary
Remote-ID    :client-mac
Circuit-ID   :(21ra

Port        :gigaethernet1/1/2
State       :disable
Overwrite    :disable
Format-rules :binary
Remote-ID    :switch-mac
Circuit-ID   :%default%

Port        :gigaethernet1/1/3
```


Copyright © Raisecom Technology Co., Ltd.

```
State       :disable
Overwrite    :disable
Format-rules :binary
```

9.10 Configuring CPU protection

9.10.1 Preparing for configurations

Scenario

When the ISCOM2600G series switch receives massive attacking packets in a short period, the CPU will run with full load and the CPU utilization rate will reach 100%. This will cause device malfunction. CPU CAR helps efficiently limit the speed of packets which enters the CPU.

Prerequisite

N/A

9.10.2 Configuring global CPU CAR

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#cpu-protect car global { pps pps-value | kbps cir cir-value cbs cbs-value }`
	Example:
	`Raisecom(config)#cpu-protect car global kbps cir 400 cbs 600`
		Configure the protocol type, CIR, and CBS of global CPU packet protection.
		• cpu-protect: CPU protection
		• car: committed access rate
		• global: global information
		• kbps: in units of kbps
		• pps pps-value: in units of pps
		• cir cir-value: CIR, an integer, ranging from 1 to 10000 kbps
		• cbs cbs-value: CBS, an integer, ranging from 1 to 10000 Kbytes

3	`Raisecom(config)#cpu-protect car queue queue-id { pps pps-value | kbps cir cir-value cbs cbs-value }`
	Example:
	`Raisecom(config)#cpu-protect car queue 1 kbps cir 400 cbs 600`
		Configure the CIR and CBS of packets in the queue.
		• cpu-protect: CPU protection
		• car: committed access rate
		• queue-id: queue ID, an integer, ranging from 0 to 7
		• kbps: in units of kbps
		• pps pps-value: in units of pps
		• cir cir-value: CIR, an integer, ranging from 1 to 10000 kbps
		• cbs cbs-value: CBS, an integer, ranging from 1 to 10000 Kbytes

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

4	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: in the form of unit/slot/port. The value range depends on the interface type.

5	`Raisecom(config-gigaethernet1/1/port)#cpu-protect car type { arp | dhcp | igmp | lacp | lldp | mld | oam | stp } queue queue-id`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#cpu-protect car type igmp queue 2`
		Configure the mapping between the protocol and queue.
		• cpu-protect: CPU protection
		• car: commited access rate
		• arp: ARP packet
		• dhcp: DHCP packet
		• igmp: IGMP packet
		• lacp: LACP packet
		• lldp: LLDP packet
		• mld: MLD packet
		• oam: OAM packet
		• stp: STP packet
		• queue-id: Queue ID, an integer, ranging from 0 to 7

Note

Configurations of CPU protection affect other protocol modules, so we do not recommend modifying them. Only professional personnel can modify them.

9.10.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show cpu-protect car statistics [ dynamic ]`	Show CPU CAR statistics.
2	`Raisecom#show cpu-protect car [ arp | dhcp | igmp | lacp | lldp | mld | oam | stp ]`	Show global mappings between protocols and queues.

9.10.4 Maintenance

Maintain the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Command	Description
Raisecom(config)#**clear cpu-protect car queue** [*queue-id*] **statistics** **Example:** Raisecom(config)#clear cpu-protect car queue 1 statistics	Clear global CPU CAR statistics. • queue-id: queue ID, an integer, ranging from 0 to 7

9.11 Configuring ARP attack protection

9.11.1 Preparing for configurations

Scenario

ARP is simple and easy to use, but vulnerable to attacks due to no security mechanism.

Attackers can forge ARP packets from users or gateways. When they send excessive IP packets, whose IP addresses cannot be resolved, to the ISCOM2600G series switch, they will cause the following harms:

- The ISCOM2600G series switch sends excessive ARP request packets to the destination network segment, so this network segment is overburdened.
- The ISCOM2600G series switch repeatedly resolve destination IP addresses, so the CPU is overburdened.

To prevent theses harms due to attacks on IP packets, the ISCOM2600G series switch supports ARP attack protection.

Prerequisite

N/A

9.11.2 Configuring ARP

Configure ARP for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface vlan** *vlan-id* **Example:** Raisecom(config)#interface vlan 1	Enter VLAN interface configuration mode. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlan*)#**arp learning strict { enable | disable }** **Example:** aisecom(config-vlan1)#arp learning strict enable	Enable or disable the device to learn ARP entries requested by itself. • enable: enable the device to learn ARP entries requested by itself. • disable: disable the device to learn ARP entries requested by itself.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-vlan*)#**arp check-destination-ip { enable | disable }** **Example:** Raisecom(config-vlan1)#arp check-destination-ip enable	Enable or disable the check of ARP destination IP address. • enable: enable the check of ARP destination IP address. • disable: disable the check of ARP destination IP address.
5	Raisecom(config-vlan*)#**arp filter** { **gratuitous | mac-illegal | tha-filled-request** } **Example:** Raisecom(config-vlan1)#arp filter gratuitous	Configure ARP filtering. • gratuitous: gratuitous ARP packets • mac-illegal: illegal MAC • tha-filled-request: ARP request packets with non-empty destination MAC
6	Raisecom(config-vlan*)#**arp anti-attack entry-check** { **fixed-all | fixed-mac | send-ack** } **Example:** Raisecom(config-vlan1)#arp anti-attack entry-check fixed-all	Configure the fixing of ARP entries. • fixed-all: fix entries. • fixed-mac: MAC will not be updated. • send-ack: send ACK for confirmation.
7	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.
8	Raisecom(config-gigaethernet1/1/port)#**ip arp-rate-limit rate** *rate-value* **Example:** Raisecom(config-gigaethernet1/1/1)#ip arp-rate-limit rate 30	Configure rate limiting of ARP. • rate-value: rate limit, an integer, ranging from 1 to 1000, in units of packet/s

9.11.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show** ip **arp-rate-limit**	Show information about rate limiting on ARP packets.
2	Raisecom#**show ip arp filter**	Show information about ARP filtering.

Copyright © Raisecom Technology Co., Ltd.

9.12 ND Snooping

9.12.1 Introduction

Neighbor Discovery (ND) is a group of messages or processes for determining relations between neighboring nodes. Its messages replace IPv4 Address Resolution Protocol (ARP), ICMP Router Discovery (RD), and ICMP Redirect messages, and it also supports the following functions:

- Detecting address conflicts
- Resolving the neighbor address
- Determining neighbor reachability
- Configuring the IP address of the host

ND Snooping is used on the ISCOM2600G to check user validity. It normally forwards ND packets of authorized users and discards those of unauthorized users, thus preventing attacks from pseudo users and gateways.

User validity check is used to determine whether a user is an authorized user of the VLAN to which the interface receiving the ND packet belongs, according to the source IPv6 address and source MAC address carried in the ND packet.

ND Snooping divides interfaces of the access device into the following two types:

- ND trusted interface: this interface does not check user validity.
- ND untrusted interface: the device takes RA packets received by the ND untrusted interface invalid and thus discards them directly.

9.12.2 Preparing for configurations

Scenarios

ND Snooping is used to prevent common ND spoofing attacks on the network, thus able to isolate ND packets from unauthorized sources. You can configure the trusted status of an interface to trust ND packets or not and configure the binding table to determine whether ND packets comply with requirements.

Prerequisite

N/A

9.12.3 Default configurations of ND Snooping

Default configurations of ND Snooping are as below.

Function	Default value
Interface trusted status of ND Snooping	Untrusted
ND Snooping status	Disable
RA Snooping status	Disable
RA Snooping interface trusted status	Not trusted

Copyright © Raisecom Technology Co., Ltd.

9.12.4 Configuring ND Snooping

Enable static binding of ND Snooping for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ipv6 nd snooping`	Enable global ND Snooping.

3	`Raisecom(config)#vlan vlan-id interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		(Optional) enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: in the form of unit/slot/port. The value range depends on the interface type.

4	`Raisecom(config)#interface interface-type interface-number-gigaethernet1/1/port)#ipv6 nd snooping`	(Optional) enable ND Snooping on the interface that is connected to the gateway.
5	`Raisecom(config-tengigabitethernet1gigaethernet1/1/port)#ipv6 nd snooping trust`	Configure the interface that is connected to the gateway as a trusted interface.

6	`Raisecom(config-tengigabitethernet1gigaethernet1/1/port)#ipv6 nd snooping trustcheck { na | ns | rs }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#ipv6 nd snooping check ns`
		(Optional) enable validity check on NS/NA/RS packets by ND Snooping.
		• na: NA packets
		• ns: NS packets
		• rs: RS packets

9.12.5 RA Snooping

Note

The Router Advertisement (RA) message carries network configurations, including the default router, network prefix list, and enabling status of the DHCP server. If the victim receives the forged RA message, network configurations will be incorrect and thus spoofing attacks are generated.

Configure RA Snooping for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ipv6 ra snooping`	Enable global RA Snooping.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	(Optional) enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
4	Raisecom(config-gigaethernet 1/1/port)#**ipv6 ra snooping trust**	Configure the interface as the trusted interface.

9.12.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show ipv6 nd snooping** [**interface** *interface-type interface-number*]	Show static binding and interface trusted status.
2	Raisecom#**show ipv6 nd snooping binding** [**interface** *interface-type interface-number*]	Show the binding relation of a specified interface or all interfaces.
3	Raisecom#**show ipv6 nd- snooping statistics** [**interface** *interface-type interface-number*]	Show statistics on ND Snooping packets.
4	Raisecom#**show ipv6 ra snooping** [*interface-type interface-number*]	Show configurations of RA Snooping.

9.12.7 Maintenance

Maintain the ISCOM2600G series switch as below.

No.	Command	Description
1	Raisecom(config)#**clear ipv6 nd snooping statistics** [**interface** *interface-type interface-number*] **Example:** Raisecom(config)#clear ipv6 nd snooping statistics	Clear statistics on ND Snooping user packets received by the device. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.
2	Raisecom(config)#**clear ipv6 nd snooping ip-address** *ipv6-address* **vlan** *vlan-id* **Example:** Raisecom(config)#clear ipv6 nd snooping ip-address 3000::1 vlan 1	Delete entries dynamically learnt by ND Snooping in a specified VLAN. • ipv6-address: IPv6 address, such as A:B::C:D • vlan-id: VLAN ID, an integer, ranging from 1 to 4094

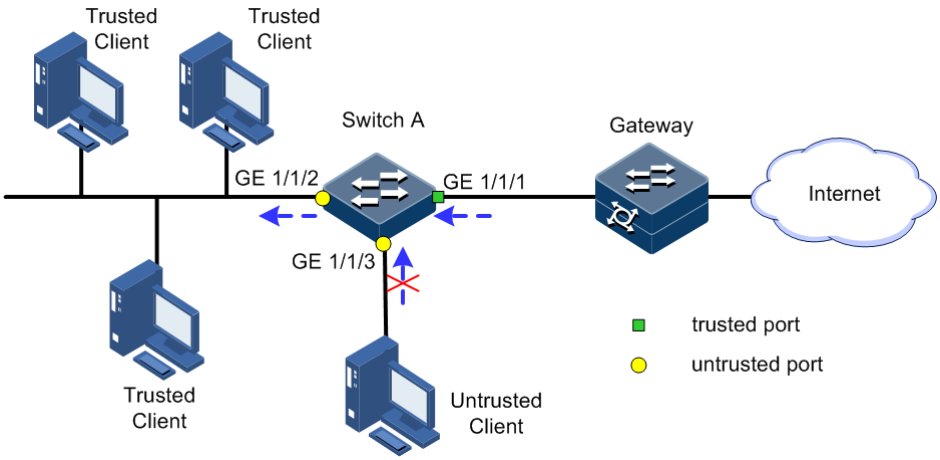
Copyright © Raisecom Technology Co., Ltd.

9.12.8 Example for configuring ND Snooping

Networking requirements

As shown in Figure 9-13, the host of a LAN user is connected to the gateway by Switch A. It has to obtain the IPv6 address through stateless automatic configuration according to the prefix assigned by the gateway to the user network because no DHCPv6 server is deployed on the network. To prevent illegal users from sending NA/NS/RS/RA packets, which causes legal hosts to fail to obtain IPv6 addresses, enable ND Snooping on Switch A to intercept illegal packets.

Figure 9-13 ND Snooping networking



Configuration steps

Step 1 Create VLAN 10 on Switch A, and activate it.

Configure Switch.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 10 active
```

Step 2 Add GE 1/1/2 on Switch A to VLAN 10 in Access mode. Configure it to Trunk mode, allowing packets of VLAN 10 to pass.

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode access
SwitchA(config-gigaethernet1/1/2)#switchport access vlan 10
SwitchA(config-gigaethernet1/1/2)#exit
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 10
confirm
SwitchB(config-gigaethernet1/1/1)#exit
```


Copyright © Raisecom Technology Co., Ltd.

Step 3 Enable global ND Snooping and enable ND Snooping in VLAN 10. Configure GE 1/1/1 as the trusted interface.

```
SwitchA(config)#ipv6 nd snooping
SwitchA(config)#vlan 10
SwitchA(config-vlan)#ipv6 nd snooping
SwitchA(config-vlan)#exit
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#ipv6 nd snooping trust
SwitchA(config-gigaethernet1/1/1)#exit
```

Step 4 Configure GE 1/1/3 as an untrusted interface. Enable validity check on ND packets.

```
SwitchA(config)#interface gigaethernet 1/1/3
SwitchA(config-gigaethernet1/1/3)#ipv6 nd snooping
SwitchA(config-gigaethernet1/1/3)#ipv6 nd snooping check ns
SwitchA(config-gigaethernet1/1/3)#ipv6 nd snooping check na
SwitchA(config-gigaethernet1/1/3)#ipv6 nd snooping check rs
SwitchA(config-gigaethernet1/1/3)#exit
```

Checking results

Use **show ipv6 nd snooping** command to check configurations of ND Snooping.

```
Raisecom#show ipv6 nd snooping
Global ND Snooping: Enable
Vlan Port                          Trust   RRRAEnable  NSEnable NAEnable
RSEnable
---------------------------------------------------------------------------
-----------
--
1   --                             --    Disable   Disable  Disable
Disable
10  gigaethernet1/1/1                            yes    Enable    Enable
Enable   Enable
```

Use the **show ipv6 nd snooping binding** command to show information about the binding table.

```
Raisecom# show ipv6 nd snooping binding
History Max Entry Num: 4
Current Entry Num: 2
IP Address                         VLAN    MAC Address       Port     sec
Type   Inhw
```


Copyright © Raisecom Technology Co., Ltd.

```
-----------------------------------------------------------------------
---------------------------------------------
FE80::C49:FE9:1CFE:437F                10      484d.7eaa.1a15
gigaethernet1/1/2             1385  nd    yes
FE80::415A:E214:F155:6163              10      509a.4c13.2020
gigaethernet1/1/2             1455  nd    yes
```


Copyright © Raisecom Technology Co., Ltd.

10 Reliability

This chapter describes basic principles and configuration procedures for reliability, and provides related configuration examples, including the following sections:

- Link aggregation
- Interface backup
- Link-state tracking
- Key-chain
- UDLD

10.1 Link aggregation

10.1.1 Introduction

Link aggregation refers to aggregating multiple physical Ethernet interfaces to a Link Aggregation Group (LAG) and taking multiple physical links in the same LAG as one logical link. Link aggregation helps share traffic among members in the LAG. Besides effectively improving reliability on links between two devices, link aggregation helps gain higher bandwidth without upgrading hardware.

Generally, the link aggregation consists of manual link aggregation, static Link Aggregation Control Protocol (LACP) link aggregation, and dynamic LACP link aggregation.

- Manual link aggregation

Manual link aggregation refers to aggregating multiple physical interfaces to one logical interface so that they can balance load.

- Static LACP link aggregation

Link Aggregation Control Protocol (LACP) is a protocol based on IEEE802.3ad. LACP communicates with the peer through the Link Aggregation Control Protocol Data Unit (LACPDU). In addition, you should manually configure the LAG. After LACP is enabled on an interface, the interface sends a LACPDU to inform the peer of its system LACP protocol priority, system MAC address, interface LACP priority, interface ID, and operation Key.

After receiving the LACPDU, the peer compares its information with the one received from other interfaces to select an interface able to be in Selected status, on which both sides can

Copyright © Raisecom Technology Co., Ltd.

agree. The operation key is a configuration combination automatically generated based on configurations of the interface, such as the speed, duplex mode, and Up/Down status. In a LAG, interfaces in the Selected status share the identical operation key.

- Dynamic LACP link aggregation

In dynamic LACP link aggregation, the system automatically creates and deletes the LAG and member interfaces through LACP. Interfaces cannot be automatically aggregated into a group unless their basic configurations, speeds, duplex modes, connected devices, and the peer interfaces are identical.

In manual aggregation mode, all member interfaces are in forwarding status, sharing loads. In static/dynamic LACP mode, there are backup links.

Link aggregation is the most widely used and simplest Ethernet reliability technology.

10.1.2 Preparing for configurations

Scenario

To provide higher bandwidth and reliability for a link between two devices, configure link aggregation.

Prerequisite

- Configure physical parameters of interfaces and make them Up.
- In the same LAG, member interfaces that share loads must be identically configured. Otherwise, data cannot be forwarded properly. These configurations include QoS, QinQ, VLAN, interface properties, and MAC address learning.
  - QoS: traffic policing, traffic shaping, congestion avoidance, rate limit, SP queue, WRR queue scheduling, interface priority and interface trust mode
  - QinQ: QinQ enabling/disabling status on the interface, added outer VLAN tag, policies for adding outer VLAN Tags for different inner VLAN IDs
  - VLAN: the allowed VLAN, default VLAN and the link type (Trunk or Access) on the interface, subnet VLAN configurations, protocol VLAN configurations, and whether VLAN packets carry Tag
  - Port properties: whether the interface is added to the isolation group, interface rate, duplex mode, and link Up/Down status
  - MAC address learning: whether MAC address learning is enabled and whether the interface is configured with MAC address limit.

10.1.3 Configuring manual link aggregation

Configure manual link aggregation for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	`Raisecom(config)#interface port-channel` *`channel-number`* **Example:** `Raisecom(config)#interface port-channel 1`	Enter aggregation group configuration mode. • channel-number: LAG interface ID, an integer, ranging from 1 to 32
3	`Raisecom(config-port-channel*)#mode manual`	Configure manual link aggregation mode.
4	`Raisecom(config-port-channel*)#{ max-active | min-active } links` *`number`* **Example:** `Raisecom(config-port-channel1)#max-active links 3`	(Optional) configure the maximum or minimum number of active links in LACP LAG. By default, the maximum number is 8 while the minimum is 1. • max-active: maximum number of active interfaces • min-active: minimum number of active interfaces • number: threshold of the active interface, an integer, ranging from 1 to 8

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

5	`Raisecom(config-port-channel1)#load-sharing mode { dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac }`
	Example:
	`Raisecom(config-port-channel1)#load-sharing mode src-ip`
		(Optional) configure a load balancing mode for link aggregation.
		By default, the load balancing algorithm is configured to sxordmac. In this mode, select a forwarding interface based on the OR result of the source and destination MAC addresses.
		• dst-ip: select the forwarding interface based on the destination IP address, ensuring packets with the same destination IP address being forwarded through the same interface.
		• dst-mac: select the forwarding interface based on the destination MAC address, ensuring packets with the same destination MAC address being forwarded through the same interface.
		• src-dst-ip: select the forwarding interface based on the result of logical XOR of source and destination IP addresses, ensuring packets with the same result being forwarded through the same interface.
		• src-dst-mac: select the forwarding interface based on the result of logical XOR of source and destination MAC addresses, ensuring packets with the same result being forwarded through the same interface.
		• src-ip: select the forwarding interface based on the source IP address, ensuring packets with the same source IP address being forwarded through the same interface.
		• src-mac: select the forwarding interface based on the source MAC address, ensuring packets with the same source MAC address being forwarded through the same interface.

6	`Raisecom(config-port-channel*)#exit`	(Optional) enter global configuration mode.
7	`Raisecom(config)#link-aggregation load-sharing mode local-first`	(Optional) enable local load balancing with a high priority in link aggregation.

10.1.4 Configuring static LACP link aggregation

Configure static LACP link aggregation for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**lacp system-priority** *system-priority* **Example:** Raisecom(config)#lacp system-priority 1	(Optional) configure the system LACP priority. The device with higher priority is the active end. LACP chooses active and backup interfaces according to configurations of the active end. The smaller the number is, the higher the priority is. The device with the smaller MAC address will be chosen as the active end if system LACP priorities of the two devices are identical. By default, the system LACP priority is 32768. • system-priority: LACP priority, an integer, ranging from 0 to 65535. The smaller the value, the higher the priority, and the more likely the device can be an active end.
3	Raisecom(config)#**lacp timeout** { **fast** | **slow** } **Example:** Raisecom(config)#lacp timeout fast	(Optional) configure LACP timeout mode. By default, it is slow. • fast: fast mode. The interval of sending packets is 1s and the period of timeout is 3s. • slow: slow mode. The interval of sending packets is 30s and the period of timeout is 90s.
4	Raisecom(config)#**interface port-channel** *channel-number* **Example:** Raisecom(config)#interface port-channel 1	Enter aggregation group configuration mode. • channel-number: LAG interface ID, an integer, ranging from 1 to 32
5	Raisecom(config-port-channel*)#**mode lacp**	Configure the working mode of the LAG to static LACP LAG.
6	Raisecom(config-port-channel*)#{ **max-active** | **min-active** } **links** *number* **Example:** Raisecom(config-port-channel1)#max-active links 3	(Optional) configure maximum or minimum number of active links in LACP LAG. By default, the maximum number is 8 while the minimum number is 1. • max-active: maximum number of active interfaces • min-active: minimum number of active interfaces • number: threshold of the active interface, an integer, ranging from 1 to 8
7	Raisecom(config-port-channel*)#**lacp priority preempt { enable | disable }** **Example:** Raisecom(config-port-channel1)#lacp priority preempt enable	Enable priority preempt on the LAG. • enable: enable priority preempt. • disable: disable priority preempt.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
8	Raisecom(config-port-channel*)#**lacp wait-timer** *time* **Example:** Raisecom(config-port-channel1)#lacp wait-timer 1	Configure the wait time on the interface. • time: WTR time on the interface, in units of millisecond, ranging from 0 to 6000
9	Raisecom(config-port-channel*)#**exit**	Return to global configuration mode.
10	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.
11	Raisecom(config-gigaethernet1/1/port)#**port-channel** *channel-number* **Example:** Raisecom(config-gigaethernet1/1/1)#port-channel 2	Add the physical interface to the LAG. • channel-number: LAG ID, an integer, ranging from 1 to 32
12	Raisecom(config-gigaethernet1/1/port)#**lacp mode** { **active** | **passive** } **Example:** Raisecom(config-gigaethernet1/1/1)#lacp mode passive	(Optional) configure the LACP mode for member interfaces. The LACP connection will fail to be established when both ends of it are in passive mode. By default, it is in active mode. • active: the interface periodically sends LACP packets to the peer for negotiation. • passive: the interface does not send any LACP packets, but receives and responds to the LACP packets sent by the peer.
13	Raisecom(config-gigaethernet1/1/port)#**lacp port-priority** *port-priority* **Example:** Raisecom(config-gigaethernet1/1/1)#lacp port-priority 1	(Optional) configure the interface LACP priority. The priority affects election for the default interface for LACP. The smaller the value is, the higher the priority is. By default, it is 32768. • port-priority: LACP priority of the interface, an integer, ranging from 0 to 65535. The smaller the value, the higher the priority, and the more likely that the interface can be an active interface.

Copyright © Raisecom Technology Co., Ltd.

Note

- In a static LACP LAG, a member interface can be an active/standby one. Both the active interface and standby interface can receive and send LACPDU. However, the standby interface cannot forward user packets.
- The system chooses default interface in the order of neighbor discovery, interface maximum speed, interface highest LACP priority, and interface minimum ID. The interface is in active status by default, the interface with identical speed, identical peer and identical device operation key is also in active status; other interfaces are in standby status.

10.1.5 Configuring manual master/slave link aggregation

Configure manual master/slave link aggregation for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port-channel` *`channel-number`* **Example:** `Raisecom(config)#interface port-channel 1`	Enter aggregation group configuration mode. • channel-number: LAG interface ID, an integer, ranging from 1 to 32
3	`Raisecom(config-port-channel*)#mode manual backup`	Configure the working mode of the LAG to manual backup LAG.
4	`Raisecom(config-port-channel*)#master-port` *`interface-type interface-number`* **Example:** `Raisecom(config-port-channel1)#master-port gigaethernet 1/1/1`	Configure the active interface of the LAG. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.

5	`Raisecom(config-port-channel*)#restore-mode { non-revertive | revertive [ restore-delay` *`second`* `] }`
	Example:
	`Raisecom(config-port-channel1)#restore-mode non-revertive`
		Configure the restoration mode and wait-to-restore time of the LAG.
		By default, the restoration mode is non-revertive.
		• non-revertive: non-revertive mode
		• revertive: revertive mode
		• restore-delay second: restore delay, an integer, ranging from 0 to 65535, in units of second

6	`Raisecom(config-port-channel*)#exit`	Return to global configuration mode.
7	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode. • interface-type: interface type • interface-number: in the form of unit/slot/port. The value range depends on the interface type.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
8	`Raisecom(config-gigaethernet1/1/port)#`**`port-channel`** *`channel-number`* **`Example:`** `Raisecom(config-gigaethernet1/1/1)#port-channel 2`	Add member interfaces to the LAG. • channel-number: LAG ID, an integer, ranging from 1 to 32
9	`Raisecom(config-gigaethernet1/1/port)#`**`exit`**	Return to global configuration mode.

Note

Before configuring the revertive mode of faults in the LAG to non-revertive, you must use the **master-port** command to configure the master interface.

10.1.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show lacp internal`**	Show local system LACP interface status, flag, interface priority, administration key, operation key, and interface status machine status.
2	`Raisecom#`**`show lacp neighbor`**	Show information about LACP neighbors, including tag, interface priority, device ID, Age, operation key value, interface ID, and interface status machine status.
3	`Raisecom#`**`show lacp statistics`**	Show statistics about interface LACP, including the total number of received/sent LACP packets, the number of received/sent Marker packets, the number of received/sent Marker Response packets, and the number of errored Marker Response packets,
4	`Raisecom#`**`show lacp sys-id`**	Show global LACP status of the local system, device ID, including system LACP priority and system MAC address.
5	`Raisecom#`**`show port-channel`** `[` *`channel-number`* `]`	Show link aggregation status of the current system, load balancing mode of link aggregation, all LAG member interfaces, and active member interfaces. **Note** The active member interface refers to the one whose interface status is Up.

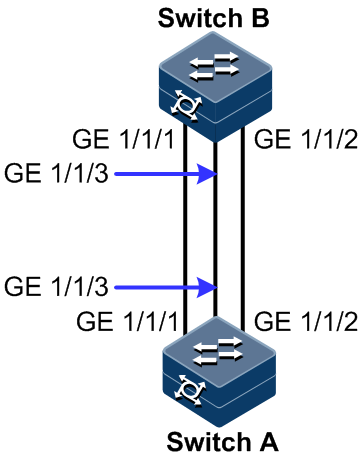
Copyright © Raisecom Technology Co., Ltd.

10.1.7 Example for configuring static LACP link aggregation

Networking requirements

As shown in Figure 10-1, to improve link reliability between Switch A and Switch B, you can configure static LACP link aggregation. That is to add GE 1/1/1, GE 1/1/2, and GE 1/1/3 to one LAG; GE 1/1/1 and GE 1/1/2 are used as the active interface while GE 1/1/3 as the standby interface.

Figure 10-1 Static LACP mode Link aggregation networking



Configuration steps

Step 1 Create static LACP link aggregation on Switch A. Configure Switch A as the active end.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#lacp system-priority 1000
SwitchA(config)#interface port-channel 1
SwitchA(config-port-channel1)#mode lacp
SwitchA(config-port-channel1)#max-active links 2
SwitchA(config-port-channel1)#exit
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#port-channel 1
SwitchA(config-gigaethernet1/1/1)#lacp port-priority 1000
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#port-channel 1
SwitchA(config-gigaethernet1/1/2)#lacp port-priority 1000
SwitchA(config-gigaethernet1/1/2)#exit
SwitchA(config)#interface gigaethernet 1/1/3
SwitchA(config-gigaethernet1/1/3)#port-channel 1
SwitchA(config-gigaethernet1/1/3)#exit
```

Step 2 Create static LACP link aggregation on Switch B.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#port-channel 1

SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#port-channel 1
SwitchB(config-gigaethernet1/1/2)#exit
SwitchB(config)#interface gigaethernet 1/1/3
SwitchB(config-gigaethernet1/1/3)#port-channel 1
SwitchB(config-gigaethernet1/1/3)#exit
```

Checking results

Use the **show port-channel** command to show global configurations of the static LACP link aggregation on Switch A.

```
SwitchA#show port-channel
Group 1 information:
Mode   :  Lacp          Load-sharing mode  : src-dst-mac
MinLinks:  1                    Max-links        : 2
UpLinks :  3                    Priority-Preemptive: Disable
Member Port  :  gigaethernet1/1/1 gigaethernet1/1/2 gigaethernet1/1/3
Efficient Port: gigaethernet1/1/1 gigaethernet1/1/2
```

Use the **show lacp internal** command to show configurations of local LACP interface status, flag, interface priority, administration key, operation key, and interface state machine on Switch A.

```
SwitchA#show lacp internal
Flags:
  S - Device is requesting Slow LACPDUs  F - Device is requesting Fast
LACPDUs
  A - Device in Active mode  P - Device in Passive mode   MP - MLACP Peer
Port
Interface               State      Flag   Port-Priority   Admin-key  Oper-
key   Port-State
-------------------------------------------------------------------------
----------------------
gigaethernet1/1/1       Active     SA     1000          1        2
0x3D
gigaethernet1/1/2       Active     SA     1000          1        2
0x3D
gigaethernet1/1/3       Standby    SA     32768         1        2
0x5
```


Copyright © Raisecom Technology Co., Ltd.

Use the **show lacp neighbor** command to show configurations of LACP interface status, flag, interface priority, administration key, operation key, and interface state machine of the peer system on Switch A.

```
Raisecom#show lacp neighbor
Flags:
  S - Device is requesting Slow LACPDUs  F - Device is requesting Fast
LACPDUs
  A - Device in Active mode  P - Device in Passive mode  MP - MLACP Peer
Port
Interface               Flag Port-Priority Age   Device-ID      Oper-key
Partner-Port Port-State
-------------------------------------------------------------------------
---------------------------
gigaethernet1/1/1       SA    32768      23s   000E.5EAB.CDEF  1       17
0x3D
gigaethernet1/1/2       SA    32768      14s   000E.5EAB.CDEF  1       18
0xD
gigaethernet1/1/3       SA    32768      10s   000E.5EAB.CDEF  1       19
0xD
```

10.2 Interface backup

10.2.1 Introduction

In dual uplink networking, Spanning Tree Protocol (STP) is used to block the redundancy link and implements backup. Though STP can meet users' backup requirements, it fails to meet switching requirements. Though Rapid Spanning Tree Protocol (RSTP) is used, the convergence is second level only. This is not a satisfying performance parameter for high-end Ethernet switch which is applied to the core of the carrier-grade network.

Interface backup, targeted for dual uplink networking, implements redundancy backup and quick switching through working and protection lines. It ensures performance and simplifies configurations.

Interface backup is another STP solution. When STP is disabled, you can realize basic link redundancy by manually configuring interfaces. If the switch is enabled with STP, you should disable interface backup because STP has provided similar functions.

When the primary link fails, traffic is switched to the backup link. In this way, not only 50ms fast switching is ensured, but also configurations are simplified.

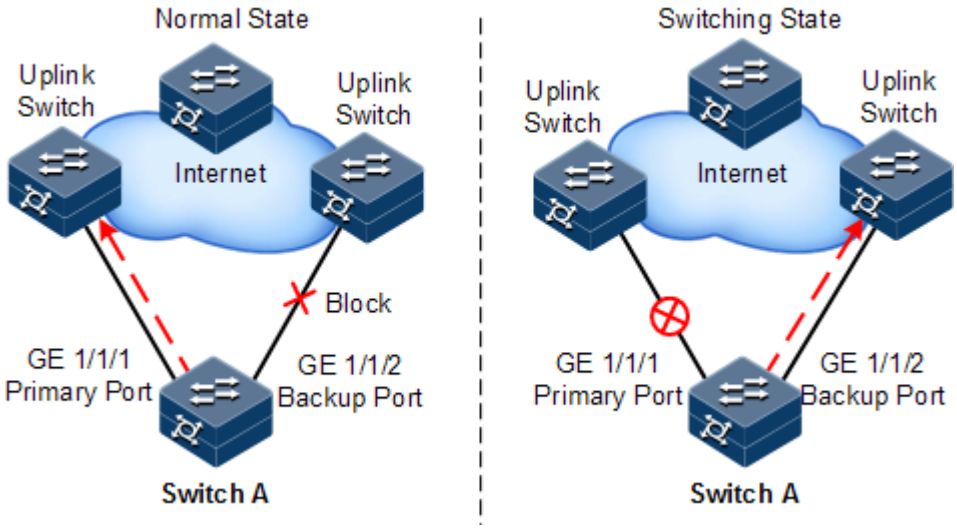
Principles of interface backup

Interface backup is implemented by configuring the interface backup group. Each interface backup group contains a primary interface and a backup interface. The link, where the primary interface is, is called a primary link while the link, where the backup interface is, is called the backup interface. Member interfaces in the interface backup group supports physical interfaces and LAGs. However, they do not support Layer 3 interfaces.

Copyright © Raisecom Technology Co., Ltd.

In the interface backup group, when an interface is in Forward status, the other interface is in Block status. At any time, only one interface is in Forward status. When the Forward interface fails, the Block interface is switched to the Forward status.

Figure 10-2 Principles of interface backup



As shown in Figure 10-2, GE 1/1/1 and GE 1/1/2 on Switch A are connected to their uplink devices respectively. The interface forwarding states are shown as below:

- Under normal conditions, GE 1/1/1 is the primary interface while GE 1/1/2 is the backup interface. GE 1/1/1 and the uplink device forward packet while GE 1/1/2 and the uplink device do not forward packets.
- When the link between GE 1/1/1 and its uplink device fails, the backup GE 1/1/2 and its uplink device forward packets.
- When GE 1/1/1 restores normally and keeps Up for a period (restore-delay), GE 1/1/1 restores to forward packets and GE 1/1/2 restores standby status.

When a switching between the primary interface and the backup interface occurs, the switch sends a Trap to the NView NNM system.

Application of interface backup in different VLANs

By applying interface backup to different VLANs, you can enable two interfaces to share service load in different VLANs, as shown in Figure 10-3.

Copyright © Raisecom Technology Co., Ltd.

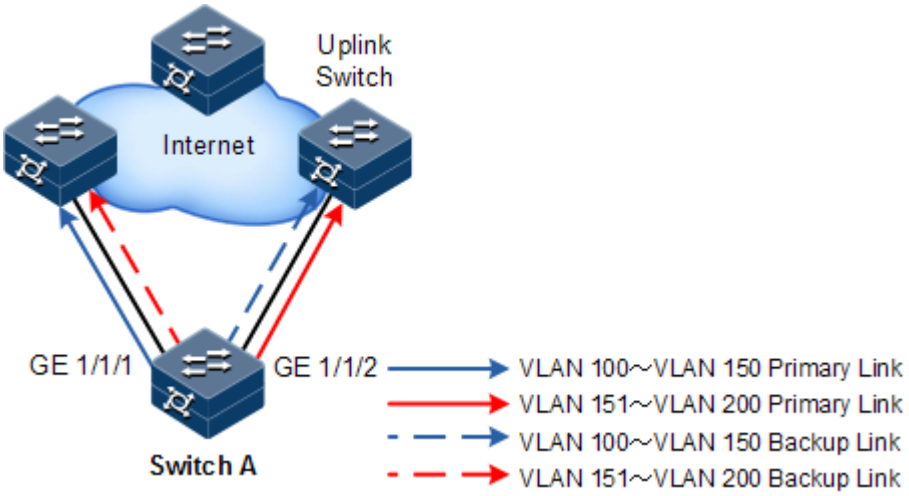


Figure 10-3 Networking with interface backup in different VLANs

In different VLANs, the forwarding status is shown as below:

- Under normal conditions, configure Switch A in VLANs 100–150.
- In VLANs 100–150, GE 1/1/1 is the primary interface and GE 1/1/2 is the backup interface.
- In VLANs 151–200, GE 1/1/2 is the primary interface and GE 1/1/1 is the backup interface.
- GE 1/1/1 forwards traffic of VLANs 100–150, and GE 1/1/2 forwards traffic of VLANs 151–200.
- When GE 1/1/1 fails, GE 1/1/2 forwards traffic of VLANs 100–200.
- When GE 1/1/1 restores normally and keeps Forward for a period (restore-delay), GE 1/1/1 forwards traffic of VLANs 100–150, and GE 1/1/2 forwards VLANs 151–200.

Interface backup is used to balance service load in different VLANs without depending on configurations of uplink switches, thus facilitating users' operation.

10.2.2 Preparing for configurations

Scenario

By configuring interface backup in a dual uplink network, you can realize redundancy backup and fast switching of the primary/backup link, and load balancing between different interfaces.

Compared with STP, interface backup not only ensures millisecond-level switching, also simplifies configurations.

Prerequisite

N/A

10.2.3 Default configurations of interface backup

Default configurations of interface backup are as below.

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
Interface backup group	N/A
Restore-delay	15s
Restoration mode	Revertive mode

10.2.4 Configuring basic functions of interface backup

Configure basic functions of interface backup for the ISCOM2600G series switch as below.

Caution

Interface backup may interfere with STP, loop detection, Ethernet ring, and G.8032. We do not recommend configuring them concurrently on the same interface.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface`** *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode or aggregation group configuration mode. • interface-type: interface type • interface-number: interface ID
3	`Raisecom(config-gigaethernet1/1/port)#`**`port backup`** *`interface-type backup-interface-number`* [**`vlanlist`** *`vlan-list`*] **Example:** `Raisecom(config-gigaethernet1/1/1)#port backup gigaethernet 1/1/2`	Configure the interface backup group. In the VLAN list, configure the interface *backup-interface-number* to the backup interface and configure the interface *primary-interface-number* to the primary interface. If no VLAN list is specified, the VLAN ranges from 1 to 4094. • interface-type: interface type • backup-interface-number: interface ID • vlan-list: VLAN list, an integer, ranging from 1 to 4094. It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3". If you do not specify the VLAN list for the interface backup group, the VLAN ID ranges from 1 to 4094 by default.
4	`Raisecom(config-gigaethernet1/1/port)#`**`port backup fault-detect lldp`**	(Optional) configure LLDP fault detection.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

5	`Raisecom(config-gigaethernet1/1/port)#port backup restore-mode { revertive [ restore-delay second ] | non-revertive }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#port backup restore-mode revertive restore-delay 600`
		(Optional) configure restoration mode.
		• non-revertive: non-revertive mode
		• revertive: revertive mode
		• restore-delay second: restore delay, an integer, ranging from 0 to 65535, in units of second

Note

- In an interface backup group, an interface is either a primary interface or a backup interface.
- In a VLAN, an interface or a LAG cannot be a member of two interface backup groups simultaneously.

10.2.5 (Optional) configuring FS on interfaces

Caution

- After FS is successfully configured, the primary/backup link will be switched; in other words, the current link is switched to the backup link (without considering Up/Down status of the primary/backup interface).
- In the FS command, the backup interface ID is optional. If different VLANs of the primary interface are configured with multiple interface backup groups, you should enter the backup interface ID.

Configure FS on interfaces for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode or aggregation group configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#port backup [ interface-type backup-interface-number ] force-switch`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#port backup gigaethernet 1/1/2 force-switch`
		Configure FS on the interface.
		Use the **no port backup** [*interface-type backup-interface-number*] **force-switch** command to cancel FS.
		• interface-type: interface type

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

	`Raisecom(config-port-channel*)#port backup [ interface-type backup-interface-number ] force-switch`
	Example:
	`Raisecom(config-port-channel1)#port backup port-channel 2 force-switch`
		interface-number: interface ID

10.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show port backup`	Show status information about interface backup.
2	`Raisecom#show port backup group`	Show configurations of interface backup.

10.2.7 Example for configuring interface backup

Networking requirements

As shown in Figure 10-4, the PC accesses the server through the Switch. To implement a reliable remote access from the PC to the server, configure an interface backup group on Switch A and specify the VLAN list so that the two interfaces concurrently forward services in different VLANs and balance load. Configure Switch A as below:

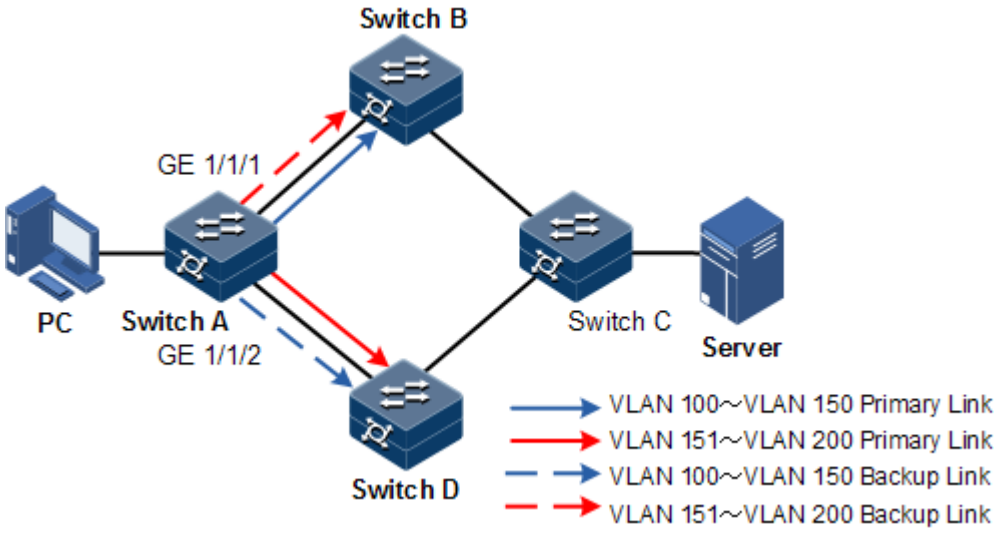
- Add GE 1/1/1 to VLANs 100–150 as the primary interface and GE 1/1/2 as the backup interface.
- Add GE 1/1/2 to VLANs 151–200 as the primary interface and GE 1/1/1 as the backup interface.

When GE 1/1/1 or its link fails, the system switches traffic to the backup interface GE 1/1/2 to resume the link.

Switch A is required to support interface backup while other switches are not.

Copyright © Raisecom Technology Co., Ltd.

Figure 10-4 Interface backup networking



Configuration steps

Step 1 Create VLANs 100–400, and add GE 1/1/1 and GE 1/1/2 to these VLANs.

```
Raisecom#config
Raisecom(config)#create vlan 100-200 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk allowed vlan 100-200
confirm
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#switchport trunk allowed vlan 100-200
confirm
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 2 Configure GE 1/1/1 as the primary interface of VLANs 100–150 and GE 1/1/2 as the backup interface.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#port backup gigaethernet 1/1/2
vlanlist 100-150
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 3 Configure GE 1/1/2 as the primary interface of VLANs 151–200 and GE 1/1/1 as the backup interface.

```
Raisecom(config)#interface gigaethernet 1/1/2
```


Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config-gigaethernet1/1/2)#port backup gigaethernet 1/1/1
vlanlist 151-200
```

Checking results

Use the **show port backup group** command to show status of interface backup under normal or faulty conditions.

When both GE 1/1/1 and GE 1/1/2 are Forward, GE 1/1/1 forwards traffic of VLANs 100–150, and GE 1/1/2 forwards traffic of VLANs 151–200.

```
Raisecom#show port backup group
Active Port(State)        Backup Port(State)      ForceSwitch  Vlanlist
-----------------------------------------------------------------------
-------------------------------------
GE1/1/1(Forward)         GE1/1/2(Block)            NO          100-150
GE1/1/2(Forward)         GE1/1/1(Block)            NO          151-200
```

Manually disconnect the link between Switch A and Switch B to emulate a fault. Then, GE 1/1/1 becomes Down, and GE 1/1/2 forwards traffic of VLANs 100–200.

```
Raisecom#show port backup group
Active Port(State)        Backup Port(State)      ForceSwitch  Vlanlist
-----------------------------------------------------------------------
-------------------------------------
GE1/1/1(Down)            GE1/1/2(Forward)       NO          100-150
GE1/1/2(Forward)         GE1/1/1(Down)          NO          151-200
```

When GE 1/1/1 resumes and keeps Forward for 15s (restore-delay), it forwards traffic of VLANs 100–150 while GE 1/1/2 forwards traffic of VLANs 151–200.

```
Raisecom#show port backup group
Active Port(State)        Backup Port(State)      ForceSwitch  Vlanlist
-----------------------------------------------------------------------
-------------------------------------
GE1/1/1(Forward)         GE1/1/2(Block)         NO          100-150
GE1/1/2(Forward)         GE1/1/1(Block)         NO          151-200
```


Copyright © Raisecom Technology Co., Ltd.

10.3 Link-state tracking

10.3.1 Introduction

Link-state tracking is used to provide interface linkage scheme for specific application and it can extend range of link backup. By monitoring uplinks and synchronizing downlinks, add uplink and downlink interfaces to a link-state group. Therefore, the fault of the upstream device can be informed to the downstream device to trigger switching. Link-state tracking can be used to prevent traffic loss due to failure in sensing the uplink fault by the downstream device.

When all uplink interfaces fail, down link interfaces are configured to Down status. When at least one uplink interface recovers, the downlink interface recovers to Up status. Therefore, the fault of the upstream device can be informed to the downlink device immediately. Uplink interfaces are not influenced when the downlink interface fail.

10.3.2 Preparing for configurations

Scenario

When uplink fails, traffic cannot be switched to the standby link if the downlink device fails to be notified in time. Then traffic will be disrupted.

Link-state tracking can be used to add downlink interfaces and uplink interfaces of the middle device to a link-state group and monitor uplink interfaces. When all uplink interfaces fails, the fault of the upstream device can be informed to the downstream device to trigger switching.

Prerequisite

N/A

10.3.3 Default configurations of link-state tracking

Default configurations of link-state tracking are as below.

Function	Default value
Link-state group	N/A
Action for processing faults on the interface	N/A
Link-state group Trap	Disable

10.3.4 Configuring link-state tracking

Note

Link-state tracking supports being configured on the physical interface and LAG interface.

Configure link-state tracking for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**link-state-tracking group** *group-number* **Example:** Raisecom(config)#link-state-tracking group 1	Create the link-state group and enable link-state tracking. • group-number: link-state group number, an integer, ranging from 1 to 100
3	Raisecom(config)#**link-state-tracking group** *group-number* **action** { **block-vlan** *vlan-id interface-type interface-number* | **delete-vlan** *vlan-id* | **flush-erps** *rind-id* | **suspend-vlan** *vlan-id* } **Example:** Raisecom(config)#link-state-tracking group 1 action delete-vlan 30	Configure the mode for processing fault on the link-state interface. • group-number: link-state group ID, an integer, ranging from 1 to 100 • interface-type: interface type • interface-number: interface ID. The form and value range depend on the interface type. • block-vlan vlan-id: block a VLAN. The vlan-id is an integer ranging from 1 to 4094. • delete-vlan vlan-id: delete a VLAN. The vlan-id is an integer ranging from 1 to 4094. • flush-erps rind-id: clear the specified G.8032 ring ID. The rind-id is an integer ranging from 1 to 255. • suspend-vlan vlan-id: suspend a VLAN. The vlan-id is an integer ranging from 1 to 4094.
4	Raisecom(config)#**link-state-tracking group** *group-number* **trap** { **enable** | **disable** } **Example:** Raisecom(config)#link-state-tracking group 1 trap enable	Configure link-state tracking group Trap. • group-number: link-state group ID, an integer, ranging from 1 to 100 • enable: enable link-state group Trap. • disable: disable link-state group Trap.
5	Raisecom(config)#**link-state-tracking group** *group-number* **upstream ma-name** *ma-name* **cfm-mepid** *cfm-mepid* **level** *level* **Example:** Raisecom(config)#link-state-tracking group 1 upstream ma-name aaa cfm-mepid 1 level 1	Configure the link-state group based on remote MEP. • group-number: link-state group number, an integer, ranging from 1 to 100 • upstream: configure the interface as an uplink interface. The uplink interface is connected with the upstream links to monitor the uplink faults. In addition, there can be multiple uplink and downlink interfaces in a link-state group. • ma-name: MA (service instance) name, a string of characters • level: MD level, an integer, ranging from 0 to 7 • cfm-mepid: remote MEP ID, an integer, ranging from 1 to 8191

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
7	Raisecom(config-gigaethernet1/1/port)#**link-state-tracking group** *group-number* { **downstream** | **upstream** } **Example:** Raisecom(config-gigaethernet1/1/1)#link-state-tracking group 1 upstream	Configure the uplink interface and downlink interface of the link-state group. • group-number: link-state group number, an integer, ranging from 1 to 100 • downstream: configure the interface as a downlink interface. The downlink interface is connected with the downstream links. If the uplink fails, all downlink interfaces will shut down informing the downlinks of service switching. • upstream: configure the interface as an uplink interface. The uplink interface is connected with the upstream links to monitor the uplink faults. In addition, there can be multiple uplink and downlink interfaces in a link-state group.
8	Raisecom(config-gigaethernet1/1/port)#**link-state-tracking group** *group-number* **action modify-pvid** *vlan-id* **Example:** Raisecom(config-gigaethernet1/1/1)#link-state-tracking group 1 action modify-pvid 30	Configure the action for the link-state group to modifying PVID. • group-number: LAG number, an integer, ranging from 1 to 100 • modify-pvid vlan-id: PVID to be modified, an integer, ranging from 1 to 4094

Note

- One link-state group can contain several uplink interfaces. Link-state tracking will not be performed when at least one uplink interface is Up. Only when all uplink interfaces are Down will link-state tracking occur.
- In global configuration mode, when you use the **no link-state-tracking group** *group-number* command to disable link-state tracking, the link-state group without interfaces will be deleted.
- In physical interface configuration mode, use the **no link-state-tracking group** *group-number* command to delete an interface. During the execution of this command, if the link-state group contains no other interfaces and is disabled, it will also be deleted.

Copyright © Raisecom Technology Co., Ltd.

10.3.5 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	`Raisecom#show link-state-tracking group [ group-number ]`	Show configurations and status of the link-state group.

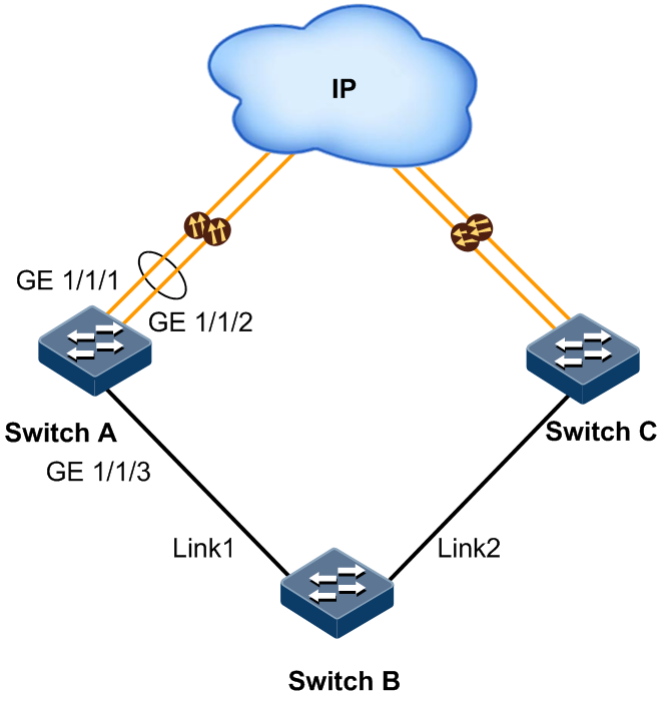
10.3.6 Example for configuring link-state tracking

Networking requirements

As shown in Figure 10-5, to improve network reliability, Link 1 and Link 2 of Switch B are connected to Switch A and Switch C respectively. Link 1 is the active link and Link 2 is the standby link. Link 2 will not be used to forward data until Link 1 is faulty.

Switch A and Switch C are connected to the uplink network in link aggregation mode. When all uplink interfaces on Switch A and Switch C fails, Switch B needs to sense the fault in time and switches traffic to the standby link. Therefore, you should deploy link-state tracking on Switch A and Switch C.

Figure 10-5 Link-state tracking networking



Configuration steps

Step 1 Configure link-state tracking on Switch A.

Create a LAG. Add uplink interfaces GE 1/1/1 and GE 1/1/2 to the LAG.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#port-channel 1
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#port-channel 1
Raisecom(config-gigaethernet1/1/2)#exit
```

Create link-state group 1. Add LAG interfaces to the link-state group.

```
Raisecom(config)#link-state-tracking group 1
Raisecom(config)#interface port-channel 1
Raisecom(config-port-channel1)#link-state-tracking group 1 upstream
Raisecom(config-port-channel1)#exit
```

Add downlink interface GE 1/1/3 to the link-state group.

```
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#link-state-tracking group 1 downstream
```

Step 2 Configure link-state tracking on Switch C.

Configurations are identical to the ones on Switch A.

Checking results

Take Switch A for example.

Use the **show link-state-tracking group** command to show configurations of the link-state group.

```
SwitchA#show link-state-tracking group 1
Link-state-tracking Group: 1
Trap State: disable
UpStream Type: port
UpStream PortList: portchannel 1
Action Mode: Shutdown-port
Action PortList: gigaethernet 1/1/3
Link-state-tracking State: normal
Fault-type: none
```

Use the **show link-state-tracking group** command to show configurations of the link-state group after all uplinks of Switch A fails. In this case, you can learn that link-state tracking is performed.

Copyright © Raisecom Technology Co., Ltd.

```
SwitchA#show link-state-tracking group 1
Link-state-tracking Group: 1
Trap State: enable
UpStream Type: port
UpStream PortList: portchannel 1
Action Mode: Shutdown-port
Action PortList: gigaethernet 1/1/3
Link-state-tracking State: failover
Fault-type: port-shutdown
```

10.4 Key-chain

10.4.1 Introduction

To implement security, the network has to keep changing authentication information at the application layer. The authentication algorithm and shared key determine whether information is altered during transmission on an insecure network. When this authentication mode is used to authenticate data, the data sender and receiver must share the security key and authentication algorithm, and cannot transmit the security key on the network.

If each application layer protocol maintains a set of authentication rules (including the authentication algorithm and key), there will be a large number of applications that use the same authentication modes. As a result, authentication information is copied and altered. Similarly, if each application adopts a fixed authentication key, it requires the network administrator to change the key every time; however, manually changing a key or authentication algorithm is complex, and modifying passwords of all routers without losing packets is difficult.

In this case, the system is required to collectively manage all authentication processings and change authentication algorithms and keys without manual intervention. To meet the requirement, Key-chain is used, which can authenticate all protocols at the application layer and dynamically change the password chain without losing packets.

10.4.2 Preparing for configurations

Scenario

In this case, the system is required to collectively manage all authentication processings and change authentication algorithms and keys without manual intervention. To meet this requirement, Key-chain is used, which can authenticate all protocols at the application layer and dynamically change the password chain without losing packets.

Prerequisite

N/A

10.4.3 Default configurations of Key-chain

N/A

Copyright © Raisecom Technology Co., Ltd.

10.4.4 Configuring Key-chain

Configure Key-chain on interfaces for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#key-chain` *`keychain-name`* **Example:** `Raisecom(config)#key-chain raisecom`	Create a key chain, and enter key-chain configuration mode. Use the **no key-chain** *keychain-name* command to delete the configuration. • keychain-name: name of the key chain, a string of 1 to 16 characters
3	`Raisecom(config-keychain)#key` *`key-id`* `key-string [ 0 | 7 ]` *`string`* **Example:** `Rasiecom(config-keychain)#key 1 key-string 0 raisecom`	Configure the key and password. • key-id: ID of key chain, an integer, ranging from 1 to 255 • 0: the password is in plaintext mode. • 7: the password is in ciphertext mode. • string: content of the password

4	`Raisecom(config-keychain)#key` *`key-id`* `accept-lifetime` *`start-time`* `{ infinite | ` *`end-time`* `| duration` *`duration-time`* `}`
	Example:
	`Rasiecom(config-keychain)#key 1 accept-lifetime 1 0 0 2011 1 1 2 0 0 2012 2 2`
		(Optional) configure the receiving time of the key.
		Use the **no key** *key-id* **accept-lifetime** command to restore the default condition.
		• key-id: ID of key chain, an integer, ranging from 1 to 255
		• start-time: start time for receiving the key, in format of hour minute second year month day
		– hour: ranging from 0 to 23
		– minute: ranging from 0 to 59
		– second: ranging from 0 to 59
		– year: ranging from 2000 to 2037
		– month: ranging from 1 to 12
		– day: ranging from 1 to 31
		• infinite: the receiving time is permanently valid.
		• end-time: end time for receiving the key, in format of hour minute second year month day
		– hour: ranging from 0 to 23
		– minute: ranging from 0 to 59
		– second: ranging from 0 to 59
		– year: ranging from 2000 to 2037
		– month: ranging from 1 to 12
		– day: ranging from 1 to 31
		• duration duration-time: duration for receiving the key, an integer, ranging from 1 to 1199224800, in units of second

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

5	`Raisecom(config-keychain)#key` *`key-id`* `send-lifetime` *`start-time`* `{ infinite | end-time | duration` *`duration-time`* `}`
	Example:
	`Rasiecom(config-keychain)#key 1 send-lifetime 1 0 0 2011 1 1 2 0 0 2012 2 2`
		(Optional) configure the sending time of the key.
		
		Use the **no key** *key-id* **send-lifetime** command to restore the default condition.
		
		• key-id: ID of key chain, an integer, ranging from 1 to 255
		• start-time: start time for receiving the key, in format of hour minute second year month day
		– hour: ranging from 0 to 23
		– minute: ranging from 0 to 59
		– second: ranging from 0 to 59
		– year: ranging from 2000 to 2037
		– month: ranging from 1 to 12
		– day: ranging from 1 to 31
		• infinite: the receiving time is permanently valid.
		• end-time: end time for receiving the key, in format of hour minute second year month day
		– hour: ranging from 0 to 23
		– minute: ranging from 0 to 59
		– second: ranging from 0 to 59
		– year: ranging from 2000 to 2037
		– month: ranging from 1 to 12
		– day: ranging from 1 to 31
		• duration duration-time: duration for receiving the key, an integer, ranging from 1 to 1199224800, in units of second

6	`Raisecom(config-keychain)#accept-tolerance { time | infinite }`
	Example:
	`Rasiecom(config-keychain)#accept-tolerance 100`
		(Optional) configure the tolerance time for receiving the key chain.
		
		Use the **no accept-tolerance** command to restore the default condition.
		
		• time: tolerance time for receiving the key, an integer, ranging from 1 to 14400, in units of minute
		• infinite: the receiving time is permanently valid.

10.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show key-chain [` *`keychain-name`* `[ key` *`key-id`* `] ]`	Show information about the key chain.

Copyright © Raisecom Technology Co., Ltd.

10.5 UDLD

10.5.1 Introduction

UniDirectional Link Detection (UDLD) is used to monitor configurations of the physical connection by the fiber or Ethernet cable. When a unidirectional link (transmitting data in only one direction) is present, UDLD can detect it, shut down the corresponding interface, and send a Trap. The unidirectional link may cause various problems, such as the spanning tree problems which may cause a loop.

10.5.2 Preparing for configurations

Scenario

When a unidirectional link (transmitting data in only one direction) is present, UDLD can detect the fault, shut down the corresponding interface, and send a Trap.

Prerequisite

Devices at both ends of the link should support UDLD.

10.5.3 Default configurations of UDLD

Default configurations of UDLD are as below.

Function	Default value
UDLD	Disable

10.5.4 Configuring UDLD

Configure UDLD for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`* **Example:** `Raisecom(config)#interface gigaethernet 1/1/1`	Enter physical interface configuration mode.

3	`Raisecom(config)#uldp { enable | disable }`
	`Raisecom(config-gigaethernet1/1/port)#uldp { enable | disable }`
	Example:
	`Raisecom(config)#uldp enable`
		Enable global UDLD or interface UDLD.
		• enable: enable UDLD.
		• disable: disable UDLD.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

4	`Raisecom(config)#uldp recovery-time time`
	Example:
	`Raisecom(config)#uldp recovery-time 20`
		(Optional) configure the recovery time for the unidirectional link.
		• time: recovery time, an integer, ranging from 15 to 86400, in units of second

10.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show uldp`	Show UDLD configurations.

Copyright © Raisecom Technology Co., Ltd.

11 System management

This chapter describes basic principles and configuration procedures for system management and maintenance, and provides related configuration examples, including the following sections:

- SNMP
- RMON
- LLDP
- Optical module DDM
- System log
- Alarm management
- Hardware environment monitoring
- CPU monitoring
- Fan monitoring
- Cable diagnosis
- Memory monitoring
- PING
- Traceroute
- Performance statistics

11.1 SNMP

11.1.1 Introduction

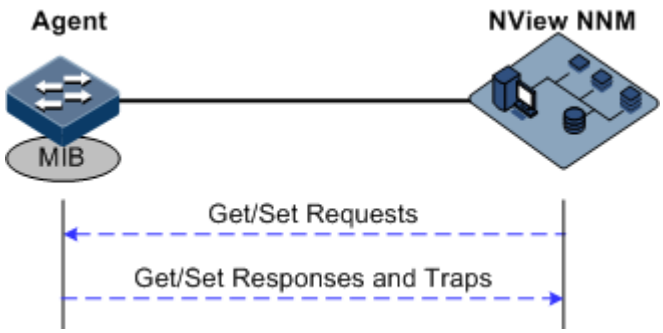
Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to resolve problems in managing network devices connected to the Internet. Through SNMP, a network management system that can manage all network devices that support SNMP, including monitoring network status, modifying configurations of a network device, and receiving network alarms. SNMP is the most widely used network management protocol in TCP/IP networks.

Copyright © Raisecom Technology Co., Ltd.

Principles

A SNMP system consists of two parts: Agent and the NView NNM system. The Agent and the NView NNM system communicate through SNMP packets sent through UDP. Figure 11-1 shows the SNMP principle.

Figure 11-1 Principles of SNMP



The Raisecom NView NNM system can provide friendly Human Machine Interface (HMI) to facilitate network management. The following functions can be implemented through it:

- Send request packets to the managed device.
- Receive reply packets and Trap packets from the managed device, and show result.

The Agent is a program installed on the managed device, implementing the following functions:

- Receive/Reply request packets from the NView NNM system
- To read/write packets and generate replay packets according to the packets type, then return the result to the NView NNM system
- Define trigger condition according to protocol modules, enter/exit system or restart the ISCOM2600G series switch when conditions are satisfied; replying module sends Trap packets to the NView NNM system through agent to report current status of the ISCOM2600G series switch.

Note

An Agent can be configured with several versions, and different versions communicate with different NMSs. But SNMP version of the NMS must be consistent with that of the connected agent so that they can intercommunicate properly.

Version of protocol

Till now, SNMP has three versions: v1, v2c, and v3, described as below.

- SNMPv1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a secret. The network management system can visit the agent only by specifying its community name correctly. If the community name carried in a SNMP packet is not accepted by the ISCOM2600G series switch, the packet will be discarded.
- Compatible with SNMPv1, SNMPv2c also uses community name authentication mechanism. SNMPv2c supports more operation types, data types, and errored codes, and thus better identifying errors.

Copyright © Raisecom Technology Co., Ltd.

- SNMPv3 uses User-based Security Model (USM) authentication mechanism. You can configure whether USM authentication is enabled and whether encryption is enabled to provide higher security. USM authentication mechanism allows authenticated senders and prevents unauthenticated senders. Encryption is used to encrypt packets transmitted between the network management system and agents, thus preventing interception.

The ISCOM2600G series switch supports v1, v2c, and v3 of SNMP.

MIB

Management Information Base (MIB) is the collection of all objects managed by the NMS. It defines attributes for the managed objects:

- Name
- Access right
- Data type

The device-related statistic contents can be reached by accessing data items. Each proxy has its own MIB. MIB can be taken as an interface between NMS and Agent, through which NMS can read/write every managed object in Agent to manage and monitor the ISCOM2600G series switch.

MIB stores information in a tree structure, and its root is on the top, without name. Nodes of the tree are the managed objects, which take a uniquely path starting from root (OID) for identification. SNMP packets can access network devices by checking the nodes in MIB tree directory.

The ISCOM2600G series switch supports standard MIB and Raisecom-customized MIB.

11.1.2 Preparing for configurations

Scenario

To log in to the ISCOM2600G series switch through NMS, configure SNMP basic functions for the ISCOM2600G series switch in advance.

Prerequisite

Configure the routing protocol and ensure that the route between the ISCOM2600G series switch and NMS is reachable.

11.1.3 Default configurations of SNMP

Default configurations of SNMP are as below.

Function	Default value
SNMP view	system and internet views (default)
SNMP community	public and private communities (default) Index CommunityName ViewName Permission 1 public internet ro 2 private internet rw
SNMP access group	initialnone and initial access groups (default)

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
SNMP user	none, md5nopriv, shapriv, md5priv, and shanopriv users (default)
Mapping relationship between SNMP user and access group	Index GroupName UserName SecModel ---------- 0 initialnone none usm 1 initial md5priv usm 2 initial shapriv usm 3 initial md5nopriv usm 4 initial shanopriv usm
Logo and the contact method of the administrator	support@Raisecom.com
Device physical location	world china raisecom
Trap	Enable
SNMP target host address	N/A
SNMP engine ID	800022B603000E5E000016

11.1.4 Configuring basic functions of SNMPv1/SNMPv2c

To protect itself and prevent its MIB from unauthorized access, the SNMP Agent proposes the concept of community. Management stations in the same community must use the community name in all Agent operations, or their requests will not be accepted.

The community name is used by different SNMP strings to identify different groups. Different communities can have read-only or read-write access permission. Groups with read-only permission can only query the device information, while groups with read-write access permission can configure the ISCOM2600G series switch in addition to querying the device information.

SNMPv1/SNMPv2c uses the community name authentication scheme, and the SNMP packets of which the names are inconsistent to the community name will be discarded.

Configure basic functions of SNMPv1/SNMPv2c for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#snmp-server view view-name oid-tree [ mask ] { excluded | included }`
	Example:
	`Raisecom(config)#snmp-server view mib1 1.3.6.1.2.1 1.1.1.1.0.1 included`
		(Optional) create SNMP view and configure MIB variable range.
		The default view is internet view. The MIB variable range contains all MIB variables below "1.3.6" node of MIB tree.
		• view-name: view name, up to 32 characters
		• oid-tree: MIB subtree OID corresponding to the view
		• mask: subtree OID mask. The mask is configured to 0 or 1. A maximum of 16 characters are supported, such as 1.1.1.1.0.1. If some bit configured set to 0, it indicates that the value of the MIB variable of a view may not be identical to the one of the OID. If some bit is configured to 1, it indicates that the value of the MIB variable of a view must be identical to the one of the OID. For example, the OID of a MIB subtree in a view is set to 1.3.6.1.2.1. The mask is set to 1.1.1.1.0.1. The first four bits and the last bit of the MIB variable must be identical to the ones of the subtree, that is, 1.3.6.1.x.1. The fifth x may be any number from 0 to 9. That is, the MIB variable of this view may be set to 1.3.6.1.0.1, 1.3.6.1.1.1 …1.3.6.1.9.1. If you do not select this parameter, the default mask is null.
		• included: MIB variables of the view are included in the subtree.
		• excluded: MIB variables of the view are excluded from the subtree.

3	`Raisecom(config)#snmp-server community [ encryption ] string [ view view-name ] { ro | rw }`
	Example:
	`Raisecom(config)#snmp-server community guest view mib1 ro`
		Create community name and configure the corresponding view and authority. Use default view internet if **view** *view-name* option is empty.
		• encryption: encrypt data.
		• string: community name, a string of less than or equal to 32 characters
		• view view-name: MIB view name, a string of less than or equal to 32 characters. If you do not select this parameter, the default name of an accessible view is internet.
		• ro: the community can only read data from the Agent.
		• rw: the community can read data from and write data into the Agent.

11.1.5 Configuring basic functions of SNMPv3

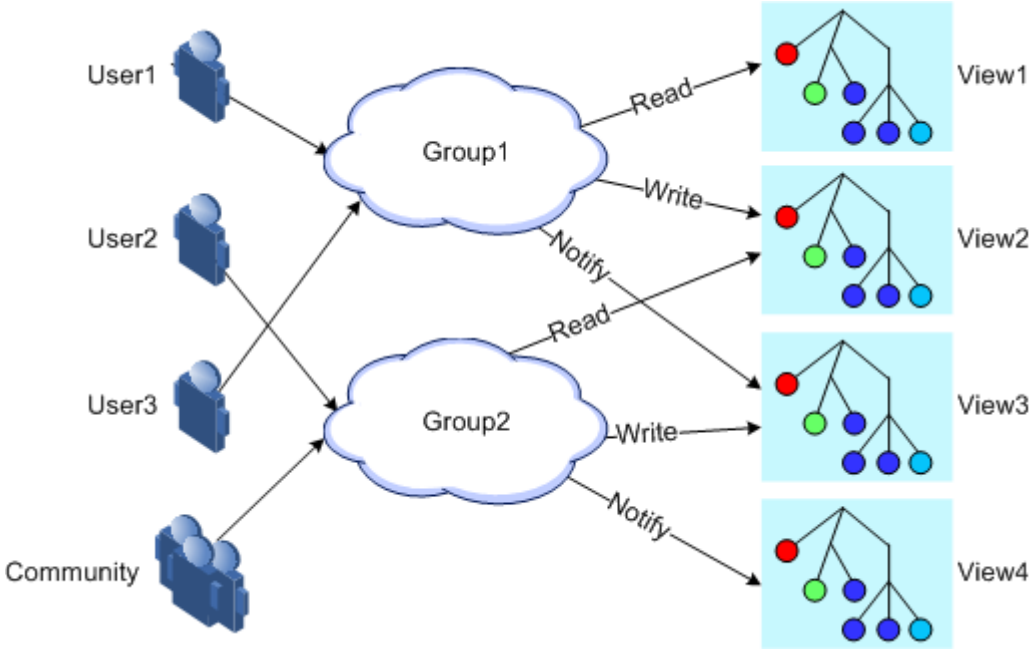
SNMPv3 uses USM over user authentication mechanism. USM comes up with the concept of access group: one or more users correspond to one access group, each access group configures the related read, write and announce view; users in access group have access permission in this view. The user access group to send Get and Set request must have permission corresponding to the request, otherwise the request will not be accepted.

As shown in Figure 11-2, the network management station uses the normal access from SNMPv3 to switch and the configuration is as below.

Copyright © Raisecom Technology Co., Ltd.

- Configure users.
- Check the access group to which the user belongs.
- Configure view permission for access groups.
- Create views.

Figure 11-2 SNMPv3 authentication mechanism



Configure basic functions of SNMPv3 for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**snmp-server view** *view-name oid-tree* [*mask*] { **excluded** | **included** } **Example:** Raisecom(config)#snmp-server view mib1 1.3.6.1.2.1 1.1.1.1.0.1 included	(Optional) create SNMP view and configure MIB variable range. The default view is internet view. The MIB variable range contains all MIB variables below "1.3.6" node of MIB tree. • view-name: view name, up to 32 characters • oid-tree: MIB subtree OID corresponding to the view • mask: subtree OID mask. The mask is configured to 0 or 1. A maximum of 16 characters are supported, such as 1.1.1.1.0.1. If some bit configured set to 0, it indicates that the value of the MIB variable of a view may not be identical to the one of the OID. If some bit is configured to 1, it indicates that the value of the MIB variable of a view must be identical to the one of the OID. For example, the OID of a MIB subtree in a view is set to 1.3.6.1.2.1. The mask is set to 1.1.1.1.0.1. The first four bits and the last bit of the MIB variable must be identical to the ones of the subtree, that is, 1.3.6.1.x.1. The fifth x may be any number from 0 to 9. That is, the MIB variable of this view may be set to 1.3.6.1.0.1, 1.3.6.1.1.1 …1.3.6.1.9.1. If you do not select this parameter, the default mask is null. • included: MIB variables of the view are included in the subtree. • excluded: MIB variables of the view are excluded from the subtree.
3	Raisecom(config)#**snmp-server user** *user-name* [**remote** *engine-id*] **authentication** { **md5** | **sha** } *authpassword* [**privacy** *privacypassword*] **Example:** Raisecom(config)#snmp-server user user1 authentication md5 raisecom	Create users and configure authentication modes. • user-name: SNMP group name, up to 32 characters • remote: ID of the specified remote SNMP engine • engine-id: SNMP engine ID related to a user name • authentication: user authentication mode • md5: configure the MD5 hash function for authentication. • sha: configure the SHA-1 hash function for authentication. • authpassword: key, generated through combination with the Hash function to implement authentication • privacy: encryption information • privacypassword: encryption password

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config)#**snmp-server user** *user-name* [**remote** *engine-id*] **authkey** { **md5** | **sha** } *authpassword* [**privkey** *privkeypassword*] **Example:** Raisecom(config)#snmp-server user user1 authkey md5 raisecom	(Optional) modify the authentication key and the encryption key. • user-name: SNMP group name, up to 32 characters • remote: ID of the specified remote SNMP engine • engine-id: SNMP engine ID related to a user name • md5: configure the MD5 hash function for authentication. • sha: configure the SHA-1 hash function for authentication. • authpassword: key, generated through combination with the Hash function to implement authentication • authkey: modify the user password. • privkey: encryption key information • privkeypassword: encryption key
5	Raisecom(config)#**snmp-server access** *group-name* [**read** *view-name*] [**write** *view-name*] [**notify** *view-name*] [**context** *context-name* { **exact** | **prefix** }] **usm** { **authnopriv** | **authpriv** | **noauthnopriv** } **Example:** Raisecom(config)#snmp-server access guestgroup read mib2 usm authnopriv	Create and configure the SNMPv3 access group. • group-name: SNMP group name, up to 32 characters • read: users in a SNMP group can only read data from the Agent. • write: users in a SNMP group can write data into the Agent. • notify: users in a SNMP group can use Trap. • view-name: view name, up to 32 characters • context context-name: specify the context name or prefix. • exact: string and the context name match each other. • prefix: string and the first characters of the context name match each other. • usm: adopt the SNMPv3 security model. • noauthnopriv: neither authenticate nor encrypt SNMP packets. It is applicable to the SNMPv3 security model. • authpriv: authenticate and encrypt SNMP packets. It is applicable to the SNMPv3 security model. • authnopriv: authenticate but not encrypt SNMP packets. It is applicable to the SNMPv3 security model.
6	Raisecom(config)#**snmp-server group** *group-name* **user** *user-name* **usm** **Example:** Raisecom(config)#snmp-server group guestgroup user guestuser1 usm	Configure the mapping between users and the access group. • group-name: SNMP group name, up to 32 characters • user-name: user name, up to 32 characters • usm: adopt SNMPv3 security model, supporting authentication and encryption.

Copyright © Raisecom Technology Co., Ltd.

11.1.6 Configuring IP address authentication by SNMP server

Configure IP address authentication by SNMP server for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#snmp-server server-auth { enable | disable }`
	Example:
	`Raisecom(config)#snmp-server server-auth enable`
		Enable or disable IP address authentication by the SNMP server.
		• enable: enable IP address authentication by the SNMP server.
		• disable: disable IP address authentication by the SNMP server.

3	`Raisecom(config)#snmp-server server-auth ip-address`
	Example:
	`Raisecom(config)#snmp-server server-auth 192.168.1.100`
		Configure the IP address of the SNMP server for authentication.
		• ip-address: IP address of the SNMP server, in dotted decimal notation

4	`Raisecom(config)#snmp-server access-list { ipv4-acl-number | ipv6-acl-number }`
	Example:
	`Raisecom(config)#snmp-server access-list 1200`
		Configure the IP ACL number for SNMP.
		• ipv4-acl-number: IPv4 ACL number, an integer, ranging from 1000 to 1999
		• ipv6-acl-number: IPv6 ACL number, an integer, ranging from 6000 to 6999

11.1.7 Configuring other information about SNMP

Other information about SNMP includes:

- Logo and contact method of the administrator: used to identify and contact the administrator
- Physical location of the device: device location

SNMPv1, SNMPv2c, and SNMPv3 support configuring this information.

Configure other information about SNMP for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#snmp-server contact string`
	Example:
	`Raisecom(config)#snmp-server contact service@raisecom.com`
		(Optional) configure the logo and contact method of the administrator.
		• string: a string, such as Email.
		Note
		For example, configure the Email to the logo and contact method of the administrator.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

3	`Raisecom(config)#snmp-server location location-string`
	Example:
	`Raisecom(config)#snmp-server location raisecom`
		(Optional) specify the physical location of the device.
		• location-string: location information

4	`Raisecom(config)#snmp-agent source ip-address`
	Example:
	`Raisecom(config)#snmp-agent source 10.3.3.3`
		(Optional) configure the source IP address of the response packets when the device walks the MIB.
		• ip-address: IP address, in dotted decimal notation, such as 10.0.0.1

11.1.8 Configuring Trap

Note

Trap configurations on SNMPv1, SNMPv2c, and SNMPv3 are identical except for Trap target host configurations. Configure Trap as required.

Trap is unrequested information sent by the ISCOM2600G series switch to the NMS automatically, which is used to report some critical events.

Before configuring Trap, you need to perform the following configurations:

- Configure basic functions of SNMP. For SNMPv1/v2c, configure the community name; for SNMPv3, configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the ISCOM2600G series switch and NMS is available.

Configure Trap of SNMP for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#snmp-server host { ip-address | ipv6-address } version 3 { authnopriv | authpriv | noauthnopriv } user-name [ udpport port-id ]`
	Example:
	`Raisecom(config)#snmp-server host 10.0.0.1 version 3 authnopriv raisecom`
		(Optional) configure the SNMPv3 Trap target host.
		• ip-address: IP address of the destination host, in dotted decimal notation
		• ipv6-address: IPv6 address of the destination host, in colon hexadecimal notation
		• 3: SNMPv3
		• udpport: UDP port number of the destination host for receiving traps. If you do not select this parameter, the default port number is configured to 162.
		• port-id: port number, an integer, ranging from 1 to 65535
		• authnopriv: authenticate but not encrypt SNMP packets.
		• authpriv: authenticate and encrypt SNMP packets, applied to the SNMPv3 security model.
		• noauthnopriv: neither authenticate nor encrypt SNMP packets
		• user-name: community name. SNMPv3 uses the user name to authenticate SNMP packets. If the user name of the NMS is inconsistent with the one on the Agent, the NMS cannot receive the trap.

3	`Raisecom(config)#snmp-server host { ip-address | ipv6-address }version { 1 | 2c } community-string [ udpport port-id ]`
	Example:
	`Raisecom(config)#snmp-server host 10.2.2.2 version 2c raisecom udpport 1`
		(Optional) configure the SNMPv1/SNMPv2c Trap target host.
		• ip-address: IP address of the destination host, in dotted decimal notation
		• ipv6-address: IPv6 address of the destination host, in colon hexadecimal notation
		• 1: SNMPv1
		• 2: SNMPv2
		• community-string: community name. SNMPv1 and SNMPv2c use the community to authenticate SNMP packets. If the community of the NMS is inconsistent with the one on the Agent, the NMS cannot receive the trap.
		• udpport: UDP port number of the destination host for receiving traps. If you do not select this parameter, the default port number is configured to 162.
		• port-id: port number, an integer, ranging from 1 to 65535

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config)#**snmp-server alarm-trap** { **enable traps**| **disable** } **Example:** Raisecom(config)#snmp-server alarm-trap enable	(Optional) enable the switch to send alarm Traps to the NMS. • enable: enable the switch to send alarm Traps to the NMS. • disable: disable the switch to send alarm Traps to the NMS.
5	Raisecom(config)#**snmp-server enable traps**	Enable Trap sending.
6	Raisecom(config)#**snmp-server trap-source** *interface-type interface-number* **Example:** Raisecom(config)#snmp-server trap-source loopback 0	Specify the source interface for the switch to send Traps. • interface-type: interface type • interface-number: interface ID
7	Raisecom(config)#**snmp-server trap-source** *ip-address* **Example:** Raisecom(config)#snmp-server trap-source 10.3.3.3	Configure the source IP address of SNMP Trap packets. • ip-address: IP address, in dotted decimal notation, such as 10.0.0.1
8	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
9	Raisecom(config-gigaethernet1/1/port)#**snmp trap link-status** { **enable** | **disable** } **Example:** Raisecom(config-gigaethernet1/1/1)#snmp trap link-status enable	Enable SNMP to generate Link Traps. Use the **disable** form of this command to disable this function. • enable: disable SNMP to generate Link Traps. • disable: disable SNMP to generate Link Traps.

11.1.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show snmp access**	Show SNMP access group configurations.
2	Raisecom#**show snmp access-list**	Show information about access and authentication of the SNMP server.
3	Raisecom#**show snmp community**	Show SNMP community configurations.
4	Raisecom#**show snmp config**	Show SNMP basic configurations, including the local SNMP engine ID, logo and contact method of the administrator, physical location of the device, and Trap status.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
5	`Raisecom#show snmp group`	Show the mapping between SNMP users and the access group.
6	`Raisecom#show snmp host`	Show Trap target host information.
7	`Raisecom#show snmp statistics`	Show SNMP statistics.
8	`Raisecom#show snmp user`	Show SNMP user information.
9	`Raisecom#show snmp view`	Show SNMP view information.
10	`Raisecom#show snmp server-auth`	Show SNMP server authentication configurations.

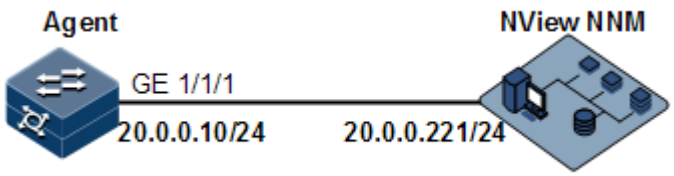
11.1.10 Example for configuring SNMPv1/SNMPv2c and Trap

Networking requirements

As shown in Figure 11-3, the route between the NView NNM system and the ISCOM2600G series switch is available. The NView NNM system can check the MIB under view corresponding to the remote Switch by SNMPv1/SNMPv2c, and the ISCOM2600G series switch can send Trap automatically to the NView NNM system in emergency.

By default, there is VLAN 1 on the ISCOM2600G series switch and all physical interfaces belong to VLAN 1.

Figure 11-3 SNMPv1/SNMPv2c networking



Configuration steps

Step 1 Configure the IP address of the ISCOM2600G series switch.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 20.0.0.10 255.255.255.0
Raisecom(config-vlan1)#exit
```

Step 2 Configure SNMPv1/SNMPv2c views.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config)#snmp-server view mib2 1.3.6.1.2.1 included
```

Step 3 Configure SNMPv1/SNMPv2c community.

```
Raisecom(config)#snmp-server community raisecom view mib2 ro
```

Step 4 Configure Trap sending.

```
Raisecom(config)#snmp-server enable traps
Raisecom(config)#snmp-server host 20.0.0.221 version 2c raisecom
```

Checking results

Use the **show ip interface brief** command to show configurations of the IP address.

```
Raisecom#show ip interface brief
VRF                  IF                        Address       NetMask
Catagory
---------------------------------------------------------------------------
-----------------------------
Default-IP-Routing-Table  fastethernet1/0/1            192.168.0.1
255.255.255.0   primary
Default-IP-Routing-Table  vlan1                      20.0.0.10
255.255.255.0   primary
```

Use the **show snmp view** command to show view configurations.

```
Raisecom#show snmp view
Index:    0
View Name: mib2
OID Tree:  1.3.6.1.2.1
Mask:     1.1.1.1.1.1.1.1
Type:     included

Index:    1
View Name: system
OID Tree:  1.2.840.10006.300.43
Mask:     --
Type:     included

Index:    2
View Name: system
OID Tree:  1.3.6.1.2.1.1
Mask:     --
```


Copyright © Raisecom Technology Co., Ltd.

```
Type:     included

Index:    3
View Name: internet
OID Tree:  1.3.6
Mask:     --
Type:     included

Index:    4
View Name: internet
OID Tree:  1.2.840.10006.300.43
Mask:     --
Type:     included
```

Use the **show snmp community** command to show community configurations.

```
Raisecom#show snmp community
Index   Community Name      View Name          Permission
-----------------------------------------------------------
1      private             internet           rw
2      public              internet           ro
3      raisecom            mib2               ro
```

Use the **show snmp host** command to show configurations of the target host.

```
Raisecom#show snmp host
Index:        0
IP family:     IPv4
IP address:    20.0.0.221
Port:         162
User Name:     raisecom
SNMP Version:   v2c
Security Level: noauthnopriv
TagList:      bridge config interface rmon snmp ospf
```

11.1.11 Example for configuring SNMPv3 and Trap

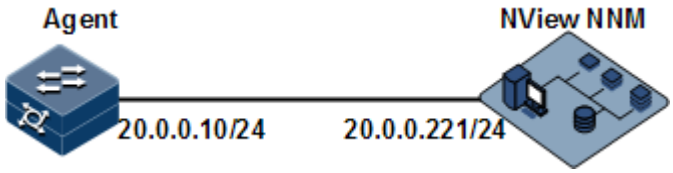
Networking requirements

As shown in Figure 11-4, the route between the NView NNM system and ISCOM2600G series switch is available, the NView NNM system monitors the Agent through SNMPv3, and the ISCOM2600G series switch can send Trap automatically to the NView NNM system when the Agent is in emergency.

By default, there is VLAN 1 on the ISCOM2600G series switch and all physical interfaces belong to VLAN 1.

Copyright © Raisecom Technology Co., Ltd.

Figure 11-4 SNMPv3 and Trap networking



Configuration steps

Step 1 Configure the IP address of the ISCOM2600G series switch.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 20.0.0.10 255.255.255.0
Raisecom(config-vlan1)#exit
```

Step 2 Configure SNMPv3 access.

Create access view mib2, including all MIB variables under 1.3.6.1.2.1.

```
Raisecom(config)#snmp-server view mib2 1.3.6.1.2.1 1.1.1.1.0.1 included
```

Create user guestuser1, and use md5 authentication algorithm. The password is raisecom.

```
Raisecom(config)#snmp-server user guestuser1 authentication md5 raisecom
```

Create a guest group access group. The security mode is usm, security level is authentication without encryption, and readable view name is mib2.

```
Raisecom(config)#snmp-server access guestgroup read mib2 usm authnopriv
```

Configure the guestuser1 user to be mapped to the access group guestgroup.

```
Raisecom(config)#snmp-server group guestgroup user guestuser1 usm
```

Step 3 Configure Trap sending.

```
Raisecom(config)#snmp-server enable traps
Raisecom(config)#snmp-server host 20.0.0.221 version 3 authnopriv
guestuser1
```


Copyright © Raisecom Technology Co., Ltd.

Checking results

Use the **show snmp access** command to show configurations of the SNMP access group.

```
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
```

Use the **show snmp group** command to show mapping between users and access groups.

```
Raisecom#show snmp group
Index   GroupName          UserName          SecModel
-----------------------------------------------------------
0       initialnone        none              usm
1       initial            md5priv           usm
2       initial            shapriv           usm
3       initial            md5nopriv         usm
4       initial            shanopriv         usm
5       guestgroup         guestuser1        usm
```

Use the **show snmp host** command to show configurations of the Trap target host.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#show snmp host
Index:        0
IP family:     IPv4
IP address:    20.0.0.221
Port:          162
User Name:     guestuser1
SNMP Version:  v3
Security Level: authnopriv
TagList:      bridge config interface rmon snmp ospf
```

11.2 RMON

11.2.1 Introduction

Remote Network Monitoring (RMON) is a standard stipulated by Internet Engineering Task Force (IETF) for network data monitoring through different network Agents and NMS.

RMON is achieved based on SNMP architecture, including the NView NNM system and the Agent running on network devices. On the foundation of SNMP, increase the subnet flow, statistics, and analysis used to achieve the monitoring to one segment and the whole network, while SNMP only can monitor the partial information about a single device and it is difficult for it to monitor one segment.

The RMON Agent is commonly referred to as the probe program. The RMON Probe can take the communication subnet statistics and performance analysis. Whenever it finds network failure, RMON Probe can report the NView NNM system, and describes the capture information under unusual circumstances so that the NView NNM system does not need to poll the device constantly. Compared with SNMP, RMON can monitor remote devices more actively and more effectively, network administrators can track the network, segment or device malfunction more quickly. This method reduces the data flows between the NView NNM system and Agent, makes it possible to manage large networks simply and powerfully, and makes up the limitations of SNMP in growing distributed Internet.

RMON Probe collects data in the following modes:

- Distributed RMON. The NMS obtains network management information and controls network resources directly from RMON Probe through dedicated RMON Probe collection data.
- Embedded RMON. Embed RMON Agent directly to network devices (such as switches) to make them with RMON Probe function. The NMS will collect network management information through the basic operation of SNMP and the exchange data information about RMON Agent.

The Raisecom ISCOM2600G series switch is embedded with RMON. As shown in Figure 11-5, the ISCOM2600G series switch implements RMON Agent function. Through this function, the management station can obtain the overall flow, error statistics and performance statistics about this segment connected to the managed network device interface so as to achieve the monitoring to one segment.

Copyright © Raisecom Technology Co., Ltd.

Figure 11-5 RMON networking

RMON MIB can be divided into nine groups according to function. Currently, there are four function groups achieved: statistics group, history group, alarm group, and event group.

- Statistic group: collect statistics on each interface, including receiving packets accounts and size distribution statistics.
- History group: similar with statistic group, it only collects statistics in an assigned detection period.
- Alarm group: monitor an assigned MIB object and configure upper threshold and lower threshold in assigned interval, trigger an event if the monitor object receives threshold value.
- Event group: cooperating with alarm group. When an alarm triggers an event, it records the event, such as sending Trap, and writes the event into log.

11.2.2 Preparing for configurations

Scenario

RMON helps monitor and account network traffics.

Compared with SNMP, RMON is a more high-efficient monitoring method. After you specifying the alarm threshold, the ISCOM2600G series switch actively sends alarms when the threshold is exceeded without obtaining variable information. This helps reduce traffic of Central Office (CO) and managed devices and facilitates network management.

Prerequisite

The route between the ISCOM2600G series switch and the NView NNM system is reachable.

11.2.3 Default configurations of RMON

Default configurations of RMON are as below.

Function	Default value
Statistics group	Enabled on all interfaces
History group	Disable
Alarm group	N/A
Event group	N/A

Copyright © Raisecom Technology Co., Ltd.

11.2.4 Configuring RMON statistics

RMON statistics is used to gather statistics on an interface, including the number of received packets, undersized/oversized packets, collision, CRC and errors, discarded packets, fragments, unicast packets, broadcast packets, multicast packets, and received packet size.

Configure RMON statistics for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#rmon statistics` *`interface-type interface-number`* `[ owner` *`owner-name`* `]`
	Example:
	`Raisecom(config)#rmon statistics gigaethernet 1/1/1 owner raisecom`
		Enable RMON statistics on an interface and configure related parameters.
		• interface-type: interface type
		• interface-number: interface ID
		• owner: description of the creator of the statistics group
		• owner-name: description string

Note

When using the **no rmon statistics** *interface-type interface-list* command to disable RMON statistics on an interface, you cannot continue to obtain the interface statistics, but the interface can still count data.

11.2.5 Configuring RMON historical statistics

Configure RMON historical statistics for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#rmon history interface-type interface-number [ shortinterval short-period ] [ longinterval long-period ] [ buckets buckets-number ] [ owner owner-name ]`
	Example:
	`Raisecom(config)#rmon history gigaethernet 1/1/1 shortinterval 60 buckets 50 owner raisecom`
		Enable RMON historical statistics on an interface and configure related parameters.
		• interface-type: interface type
		• interface-number: interface ID
		• shortinterval: short sampling interval. Collect the network status statistics every short period.
		• short-period: short period, an integer, ranging from 1 to 299, in units of second
		• longinterval: long sampling interval. Collect the network status statistics every long period.
		• long-period: long period, an integer, ranging from 300 to 3600, in units of second
		• buckets: history group data storage queue
		• buckets-number: queue size, an integer, ranging from 10 to 1000
		• owner: description of the creator of the history group
		• owner-name: description string, a string of 1 to 127 characters

Note

When you use the **no rmon history** *interface-type interface-list* command to disable RMON historical statistics on an interface, the interface will not count data and clear all historical data collected previously.

11.2.6 Configuring RMON alarm group

Configure one RMON alarm group instance (alarm-id) to monitor one MIB variable (mibvar). When the value of monitoring data exceeds the defined threshold, an alarm event will generate. Record the log to send Trap to network management station according to the definition of alarm event.

The monitored MIB variable must be real, and the data value type is correct.

- If the configured variable does not exist or value type variable is incorrect, return error.
- In the successfully configured alarm, if the variable cannot be collected later, close the alarm; reconfigure the alarm if you want to monitor the variable again.

By default, the triggered event number is 0; in other words, no event will be triggered. If the number is not zero, and there is no corresponding configuration in event group, when the control variable is abnormal, it cannot trigger the event successfully until the event is established.

An alarm will be triggered as long as matching the condition when the upper or lower limit for one of the events is configured in the event table. If there is no configuration for the upper and lower limits related alarm event (rising-event-id, falling-event-id) in the event table, no alarm will not be generated even alarm conditions are met.

Configure the RMON alarm group for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#rmon alarm` *`alarm-id mibvar`* `[ interval` *`period`* `] { absolute | delta } rising-threshold` *`rising-num`* `[` *`rising-event`* `] falling-threshold` *`falling-num`* `[` *`falling-event`* `] [ owner` *`owner-name`* `]`
	Example:
	`Raisecom(config)#rmon alarm 1 1.3.6.1.2.1.2.2.1.20.1 interval 20 absolute rising-threshold 100001 falling-threshold 500 2 owner raisecom`
		Add alarm instances to the RMON alarm group and configure related parameters.
		• alarm-id: alarm index, an integer, ranging from 1 to 65535
		• mibvar: MIB variables (MIB OIDs) that need to be remotely monitored.
		• interval: sampling interval of MIB variables. It is used to monitor MIB changes periodically. If you do not select this parameter, the default interval 2s will be used.
		• period: interval, an integer, ranging from 2 to 3600, in units of second
		• absolute: show the absolute change of MIB variables. It is a method for generating alarms. Compare the changed MIB variable value to the configured threshold, if the value is smaller than the minimum value or greater than the maximum value, an alarm will be generated.
		• delta: show the relative change of MIB variables. It is a method for generating alarms. If the delta increases, compare the delta to the maximum value, if the delta is greater than the maximum value, an alarm will be generated. If the delta decreases, compare the delta to the minimum value, if the delta is greater than the minimum value, an alarm will be generated.
		• rising-threshold: maximum threshold
		• falling-threshold: minimum threshold
		• rising-numMaximum value, an integer, ranging from 0 to 2147483647
		• falling-num: minimum value, an integer, ranging from 0 to 2147483647
		• falling-event: number of the event triggered when the value exceeds the minimum value, an integer, ranging from 1 to 65535
		• owner: description of the creator of the RMON alarm
		• owner-name: description string

11.2.7 Configuring RMON event group

Configure the RMON event group for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**rmon event** *event-id* [**log**] [**trap**] [**description** *string*] [**owner** *owner-name*] **Example:** Raisecom(config)#rmon event 1 trap owner raisecom	Add events to the RMON event group and configure processing modes of events. • event-id: event number, an integer, ranging from 1 to 65535 • log: write the event to the system log. • trap: send a trap to the NView NNM. • description: event descriptions • string: description, a string of 1 to 127 characters • owner: description of the event creator. If you do not select this parameter, the descriptions will be configured to monitor Event by default. • owner-name: description string, a string of 1 to 127 characters

11.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show rmon**	Show RMON configurations.
2	Raisecom#**show rmon alarms**	Show information about the RMON alarm group.
3	Raisecom#**show rmon events**	Show information about the RMON event group.
4	Raisecom#**show rmon statistics** [*interface-type interface-list*]	Show information about the RMON statistics group.
5	Raisecom#**show rmon latest statistics** [**long** | **short**] **portlist** *interface-type interface-number*	Show RMON statistics in the last 5s or 5min.
6	Raisecom#**show rmon history** *interface-type interface-list*	Show information about the RMON history group.

11.2.9 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
Raisecom(config)#**clear rmon**	Clear all RMON configurations.

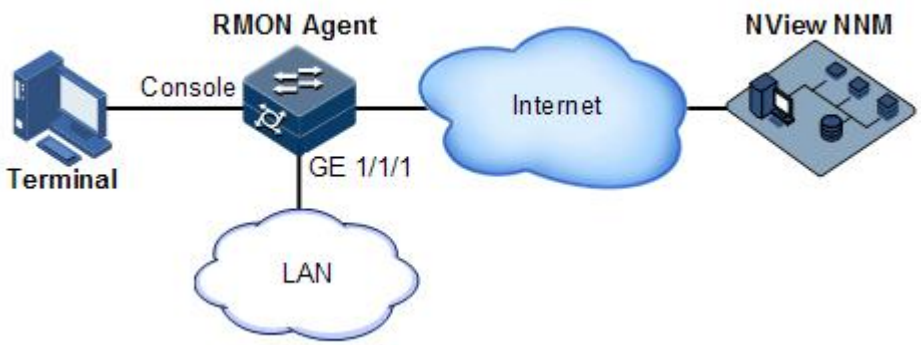
Copyright © Raisecom Technology Co., Ltd.

11.2.10 Example for configuring RMON alarm group

Networking requirements

As shown in Figure 11-6, the ISCOM2600G series switch is the Agent, connected to terminal through the Console interface, connected to remote NView NNM system through Internet. Enable RMON statistics and gather performance statistic on GE 1/1/1. When packets received on GE 1/1/1 exceeds the threshold in a period, logs are recorded and Trap is sent.

Figure 11-6 RMON networking



Configuration steps

Step 1 Create an event with index ID 1, used to record and send logs with description string High-ifOutErrors. The owner of logs is system.

```
Raisecom#config
Raisecom(config)#rmon statistics gigaethernet 1/1/1
Raisecom(config)#rmon event 1 log description High-ifOutErrors owner
system
```

Step 2 Create an alarm item with index ID 10, used to monitor MIB variables 1.3.6.1.2.1.2.2.1.20.1 every 20s. If the variable increases by more than 15, the Trap alarm will be triggered. The owner of alarm message is also 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
```

Checking results

Use the **show rmon alarms** command to check whether there is information about event group events on the ISCOM2600G series switch.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#show rmon alarms
Alarm group information:
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
```

Use the **show rmon event**s command to check whether there is information about alarm group on the ISCOM2600G series switch.

```
Raisecom#show rmon events
Event group information:
Event 1 is active, owned by system
Event description:  High-ifOutErrors
Event generated at 0:0:0
Register log information when event is fired.
```

When an alarm event is triggered, you can also check related information in the alarm management part of the NView NNM system.

11.3 LLDP

11.3.1 Introduction

With the enlargement of network scale and increase of network devices, the network topology becomes more and more complex and network management becomes more important. A lot of network management software adopts auto-detection function to trace changes of network topology, but most of the software can only analyze the Layer 3 network and cannot ensure the interfaces to be connected to other devices.

Link Layer Discovery Protocol (LLDP) is based on IEEE 802.1ab standard. The NMS can fast grip the Layer 2 network topology and changes.

LLDP organizes the local device information in different Type Length Value (TLV) and encapsulates in Link Layer Discovery Protocol Data Unit (LLDPDU) to transmit to straight-connected neighbour. It also saves the information from neighbour as standard Management Information Base (MIB) for the NMS querying and judging link communication.

LLDP packet

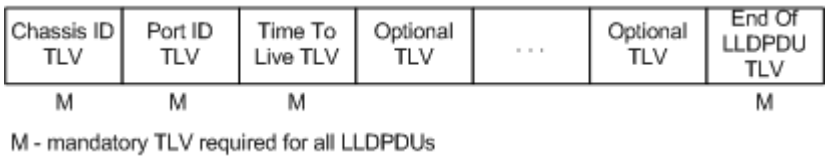
The LLDP packet is used to encapsulate LLDPDU Ethernet packet in data unit and transmitted by multicast.

LLDPDU is the data unit of LLDP. The device encapsulates local information in TLV before forming LLDPDU, then several TLV fit together in one LLDPDU and encapsulated in Ethernet data for transmission.

Copyright © Raisecom Technology Co., Ltd.

As shown in Figure 11-7, LLDPDU is made by several TLV, including 4 mandatory TLV and several optional TLV.

Figure 11-7 Structure of a LLDPDU



As shown in Figure 11-8, each TLV denotes a piece of information at local. For example, the device ID and interface ID correspond with the Chassis ID TLV and Port ID TLV respectively, which are fixed TLVs.

Figure 11-8 Structure of a TLV packet

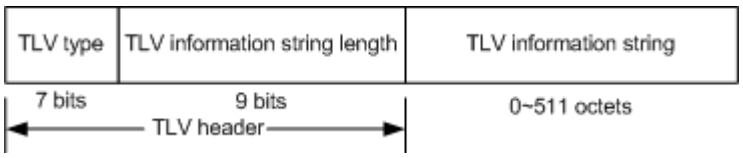


Table 11-1 lists TLV types. At present only types 0–8 are used.

Table 11-1 TLV types

TLV type	Description	Optional/Required
0	End Of LLDPDU	Required
1	Chassis ID	Required
2	Interface number	Required
3	Time To Live	Required
4	Interface description	Optional
5	System name	Optional
6	System description	Optional
7	System capabilities	Optional
8	Management address	Optional

Organization-defined TLVs are optional TLVs and are advertised in the LLDPDU as required. Table 11-2 and Table 11-3 list common organization-defined TLVs.

Table 11-2 IEEE 802.1 organization-defined TLVs

Type	Description
Port VLAN ID TLV	VLAN ID on the interface
Port And Protocol VLAN ID TLV	Protocol VLAN ID on the interface

Copyright © Raisecom Technology Co., Ltd.

Type	Description
VLAN Name TLV	VLAN name on the interface
Protocol Identity TLV	Type of the protocol supported by the interface

Table 11-3 IEEE 802.3 organization-defined TLVs

Type	Description
MAC/PHY Configuration//Status TLV	Rate and duplex mode of the interface, whether auto-negotiation is supported or enabled
Power Via MDI TLV	Power supply capability on the interface
Link Aggregation TLV	Link aggregation capability on the interface and current link aggregation status
Maximum Frame Size TLV	Size of the maximum frame able to be transmitted by the interface

Principles

LLDP is a kind of point-to-point one-way issuance protocol, which notifies local device link status to peer end by sending LLDPDU (or sending LLDPDU when link status changes) periodically from the local end to the peer end.

The procedure of packet exchange:

- When the local device transmits packet, it gets system information required by TLV from NView NNM (Network Node Management) and gets configurations from LLDP MIB to generate TLV and form LLDPDU to transmit to peer.
- The peer receives LLDPDU and analyzes TLV information. If there is any change, the information will be updated in neighbor MIB table of LLDP and notifies the NView NNM system.

When the device status is changed, the ISCOM2600G series switch sends a LLDP packet to the peer. To avoid sending LLDP packet continuously because of frequency change of device status, you can configure a delay timer for sending the LLDP packet.

The aging time of Time To Live (TTL) in local device information about the neighbour node can be adjusted by modifying the parameter values of aging coefficient, sends LLDP packets to neighbour node, after receiving LLDP packets, neighbour node will adjust the aging time of its neighbour nodes (sending side) information. Aging time formula, TTL = Min {65535, (interval ×hold-multiplier)}:

- Interval indicates the time period to send LLDP packets from neighbor node.
- Hold-multiplier refers to the aging coefficient of device information in neighbor node.

Copyright © Raisecom Technology Co., Ltd.

11.3.2 Preparing for configurations

Scenario

When you obtain connection information between devices through NView NNM system for topology discovery, the ISCOM2600G series switch needs to enable LLDP, notify their information to the neighbours mutually, and store neighbour information to facilitate the NView NNM system queries.

Prerequisite

N/A

11.3.3 Default configurations of LLDP

Default configurations of LLDP are as below.

Function	Default value
Global LLDP	Disable
LLDP interface status	Enable
Delay timer	2s
Period timer	30s
Aging coefficient	4
Restart timer	2s
Alarm function	Enable
Alarm notification timer	5s
Destination MAC address of LLDP packets	0180.c200.000e

11.3.4 Enabling global LLDP

Caution

After global LLDP is disabled, you cannot re-enable it immediately. Global LLDP cannot be enabled unless the restart timer times out.

When you obtain connection information between devices through the NView NNM system for topology discovery, the ISCOM2600G series switch needs to enable LLDP, sends their information to the neighbours mutually, and stores neighbour information to facilitate query by the NView NNM system.

Enable global LLDP for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#lldp { enable | disable }`
	Example:
	`Raisecom(config)#lldp enable`
		Enable or disable global LLDP.
		• enable: enable global LLDP.
		• disable: disable global LLDP.

11.3.5 Enabling interface LLDP

Enable interface LLDP for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
		• interface-type: interface type
		• interface-number: interface ID

3	`Raisecom(config-gigaethernet1/1/port)#lldp { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#lldp enable`
		Enable interface LLDP.
		• enable: enable interface LLDP.
		• disable: disable interface LLDP.

11.3.6 Configuring basic functions of LLDP

Caution

When configuring the delay timer and period timer, the value of the delay timer should be smaller than or equal to a quarter of the period timer value.

Configure basic functions of LLDP for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#lldp message-transmission interval second`
	Example:
	`Raisecom(config)#lldp message-transmission interval 50`
		(Optional) configure the period timer of the LLDP packet.
		• second: interval for sending LLDP packets, an integer, ranging from 5 to 32768, in units of second

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**lldp message-transmission delay** *second* **Example:** Raisecom(config)#lldp message-transmission delay 5	(Optional) configure the delay timer of the LLDP packet. • second: delay time, an integer, ranging from 1 to 8192, in units of second
4	Raisecom(config)#**lldp message-transmission hold-multiplier** *coefficient* **Example:** Raisecom(config)#lldp message-transmission hold-multiplier 10	(Optional) configure the aging coefficient of the LLDP packet. • coefficient: neighbor aging coefficient, an integer, ranging from 2 to 10
5	Raisecom(config)#**lldp restart-delay** *second* **Example:** Raisecom(config)#lldp restart-delay 10	(Optional) restart the timer. When configuring the delay timer and period timer, the value of the delay timer should be smaller than or equal to a quarter of the period timer value. • second: restart delay time, an integer, ranging from 1 to 10, in units of second

11.3.7 Configuring LLDP alarm

When the network changes, you need to enable LLDP alarm notification function to send topology update alarm to the NView NNM system immediately.

Configure the LLDP alarm for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lldp trap-interval** *second* **Example:** Raisecom(config)#lldp trap-interval 10	(Optional) configure the period of the timer for sending LLDP alarm Traps. • second: LLDP trap interval, an integer, ranging from 5 to 3600, in units of second

11.3.8 Configuring TLV

Configure TLV for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config-gigaethernet1/1/port)#**lldp tlv-select basic-tlv** { **all** | **port-description** | **system-capability** | **system-name** | **system-description** } **Example:** Raisecom(config-gigaethernet1/1/1)#lldp tlv-select basic-tlv system-description	Configure the basic TLV allowed to issue. • all: all basic TLV • port-description: interface description TLV • system-capability: system TLV • system-name: device name TLV • system-description: System description TLV
4	Raisecom(config-gigaethernet1/1/port)#**lldp tlv-select med-tlv** { **all** | **capability**| **inventory** | **network-policy**| **location-id** } { **civic-address** *device-type country-code civic-address-type ca-value* | **elin-address** *tel-number* } **Example:** Raisecom(config-gigaethernet1/1/1)#lldp tlv-select med-tlv all	Configure the MED TLV allowed to issue. • all: all MED TLV, excluding location TLV • capability: LLDP-MED TLV • inventory: inventory TLV • network-policy: network policy TLV • location-id: location ID TLV • civic-address: the location ID format is an address. • device-type: device type, an integer, ranging from 0 to 2. The value 0 indicates the DHCP server, the value 1 indicates the switch, and the value 2 indicates the MED terminal. • country-code: country code, a string of 2 characters • civic-address-type: address type, an integer, ranging from 0 to 255 • ca-value: address value, a string of 1 to 250 characters • elin-address: the position ID format is an emergency telephone number. • tel-number: emergency telephone number, 10–25 digits

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config-gigaethernet1/1/port)#**lldp tlv-select dot1-tlv** { **all** | **port-vlan-id** | **vlan-name** [*vlan-id*] } **Example:** Raisecom(config-gigaethernet1/1/1)#lldp tlv-select dot1-tlv port-vlan-id	Enable 802.1 TLV type allowed to issue. • all: all 802.1 TLV • port-vlan-id: interface VLAN ID TLV • vlan-name: VLAN name TLV • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
6	Raisecom(config-gigaethernet1/1/port)#**lldp tlv-select dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } **Example:** Raisecom(config-gigaethernet1/1/1)#lldp tlv-select dot3-tlv link-aggregation	Enable 802.3 TLV type allowed to be issued. • all: all TLV defined by the IEEE 802.3 • link-aggregation: advertise Link Aggregation TLV. • mac-physic: advertise MAC/PHY Configuration/Status TLV. • max-frame-size: advertise Maximum Frame Size TLV. • power: advertise Power Via MDI TLV.

11.3.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show lldp local config**	Show LLDP local configurations.
2	Raisecom#**show lldp local system-data** [*interface-type interface-number*]	Show information about the LLDP local system.
3	Raisecom#**show lldp remote** [*interface-type interface-number*] [**detail**]	Show information about the LLDP neighbor.
4	Raisecom#**show lldp statistic** [*interface-type interface-number*]	Show statistics about LLDP packets.
5	Raisecom#**show lldp tlv-select** [*interface-type interface-number*]	Show information about the optional TLV sent by the interface.

11.3.10 Maintenance

Maintain the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

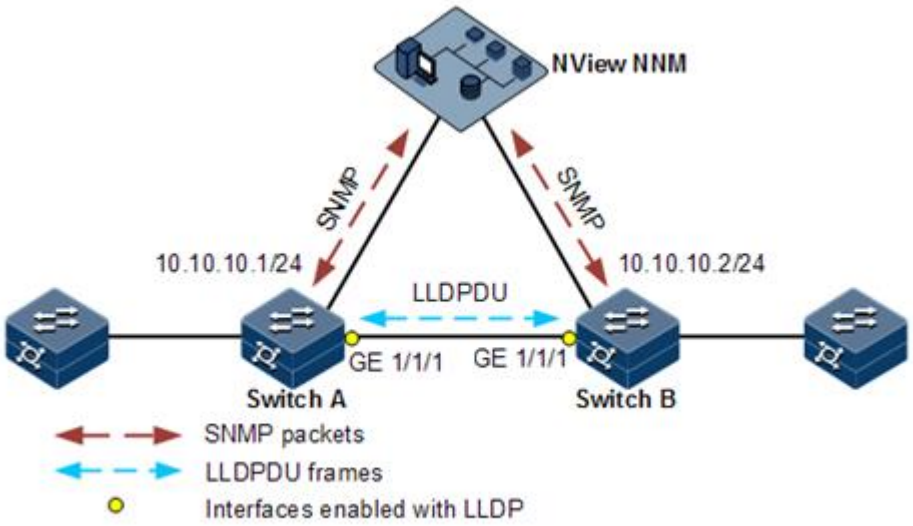
Command	Description
Raisecom(config)#**clear lldp statistic** *interface-type interface-number* **Example:** Raisecom(config)#clear lldp statistic gigaethernet 1/1/1	Clear LLDP statistics. • interface-type: interface type • interface-number: interface ID
Raisecom(config)#**clear lldp remote-table** [*interface-type interface-number*] **Example:** Raisecom(config)#clear lldp remote-table gigaethernet 1/1/1	Clear LLDP neighbor information. • interface-type: interface type • interface-number: interface ID
Raisecom(config)#**clear lldp global statistic**	Clear global LLDP statistics.

11.3.11 Example for configuring LLDP

Networking requirements

As shown in Figure 11-9, the Switch is connected to the NView NNM system; enable LLDP between Switch A and Switch B, query Layer 2 link change through the NView NNM system. The neighbor aging, new neighbor and neighbor information changes will be reported as LLDP alarms to the NView NNM system.

Figure 11-9 LLDP networking



Configuration steps

Step 1 Enable global LLDP and LLDP alarm.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#lldp enable
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#lldp enable
```

Step 2 Configure the management IP address.

Configure Switch A.

```
SwitchA(config)#create vlan 1024 active
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport access vlan 1024
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface vlan 1024
SwitchA(config-vlan1024)#ip address 10.10.10.1 255.255.255.0
SwitchA(config-vlan1024)#exit
```

Configure Switch B.

```
SwitchB(config)#create vlan 1024 active
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport access vlan 1024
SwitchB(config)#interface vlan 1024
SwitchB(config-vlan1024)#ip address 10.10.10.2 255.255.255.0
SwitchB(config-vlan1024)#exit
```

Step 3 Configure LLDP attributes.

Configure Switch A.

```
SwitchA(config)#lldp message-transmission interval 60
SwitchA(config)#lldp message-transmission delay 9
SwitchA(config)#lldp trap-interval 10
```

Configure Switch B.

```
SwitchB(config)#lldp message-transmission interval 60
SwitchB(config)#lldp message-transmission delay 9
```


Copyright © Raisecom Technology Co., Ltd.

```
SwitchB(config)#lldp trap-interval 10
```

Checking results

Use the **show lldp local config** command to show local configurations.

```
SwitchA#show lldp local config
System configuration:
-----------------------------------------------------------------
LLDP enable status:              enable (default is disabled)
LldpMsgTxInterval:               60     (default is 30s)
LldpMsgTxHoldMultiplier:          4      (default is 4)
LldpReinitDelay:                 2      (default is 2s)
LldpTxDelay:                    9      (default is 2s)
LldpNotificationInterval:         10     (default is 5s)
LldpNotificationEnable:           enable (default is enabled)
-----------------------------------------------------------------
Port            Status       Packet destination-mac
-------------------------------------------------------
GE1/1/1         enable       0180.C200.010e
GE1/1/2         enable       0180.C200.010e
GE1/1/3         enable       0180.C200.010e
GE1/1/4         enable       0180.C200.010e
GE1/1/5         enable       0180.C200.010e
GE1/1/6         enable       0180.C200.010e
……
SwitchB#show lldp local config
System configuration:
-----------------------------------------------------------------
LLDP enable status:              enable (default is disabled)
LldpMsgTxInterval:               60     (default is 30s)
LldpMsgTxHoldMultiplier:          4      (default is 4)
LldpReinitDelay:                 2      (default is 2s)
LldpTxDelay:                    9      (default is 2s)
LldpNotificationInterval:         10     (default is 5s)
LldpNotificationEnable:           enable (default is enabled)
-----------------------------------------------------------------
Port            Status       Packet destination-mac
-------------------------------------------------------
GE1/1/1         enable       0180.C200.000E
GE1/1/2         enable       0180.C200.000E
GE1/1/3         enable       0180.C200.000E
GE1/1/4         enable       0180.C200.000E
GE1/1/5         enable       0180.C200.000E
GE1/1/6         enable       0180.C200.000E
……
```

Use the **show lldp remote** command to show neighbor information.

```
SwitchA#show lldp remote
```


Copyright © Raisecom Technology Co., Ltd.

```
Port   ChassisId          PortId       SysName   MgtAddress    ExpiredTime
---------------------------------------------------------------------------
gigaethernet1/1/1  000E.5E02.B010    gigaethernet1/1/1        SwitchB
10.10.10.2    106
……
SwitchB#show lldp remote
Port           ChassisId    PortId   SysName   MgtAddress    ExpiredTime
---------------------------------------------------------------------------
gigaethernet1/1/1  000E.5E12.F120 gigaethernet1/1/1   SwitchA
 10.10.10.1 106
……
```

11.4 Optical module DDM

11.4.1 Introduction

Optical module Digital Diagnostics Monitoring (DDM) on the ISCOM2600G series switch supports Small Form-factor Pluggable (SFP) and 10GE SFP+ diagnosis.

The fault diagnostics function of SFP provides the system a performance monitor method. The network administrator analysis the monitor data provided by SFP to predict the age of transceiver, isolate system fault and authenticate modules compatibility during installation.

The performance parameters of optical module which are monitored by optical module DDM are as below:

- Modular temperature
- Inner power voltage
- Tx offset current
- Tx optical power
- Rx optical power

When the performance parameters reach alarm threshold or status information changes, the corresponding Trap alarm will be generated.

11.4.2 Preparing for configurations

Scenario

Fault diagnostics f optical modules provide a method for detecting SFP performance parameters. You can predict the service life of optical module, isolate system fault and check its compatibility during installation through analyzing monitoring data.

Prerequisite

The optical module used on the ISCOM2600G series switch should be a Raisecom-certified one. If you use an optical module of other vendors, problems of unstable services, failure in supporting DDM, or incorrect DDM information will happen.

Copyright © Raisecom Technology Co., Ltd.

11.4.3 Default configurations of optical module DDM

Default configurations of optical module DDM are as below.

Function	Default value
Global optical module DDM	Disable
Interface optical module DDM	Disable
Global optical DDM Trap	Disable
Interface optical DDM Trap	Disable

11.4.4 Enabling optical module DDM

Enable optical module DDM for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#transceiver ddm { enable | disable }`
	Example:
	`Raisecom(config)#transceiver ddm enable`
		Enable or disable optical module DDM.
		• enable: enable optical module DDM.
		• disable: disable optical module DDM.

3	`Raisecom(config)#transceiver ddm poll-interval interval` `Raisecom(config)#transceiver ddm poll-interval 30`	Configure the polling interval for optical module DDM. • interval: polling interval, an integer, ranging from 5 to 300, in units of second

3	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enter physical interface configuration mode.
		• interface-type: interface type
		• interface-number: interface ID

4	`Raisecom(config-gigaethernet1/1/port)#transceiver ddm { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#transceiver ddm enable`
		Enable interface optical module DDM.
		Only when global optical DDM is enabled, the optical module, where interface optical module DDM is enabled, can the ISCOM2600G series switch perform DDM.
		• enable: enable optical module DDM.
		• disable: disable optical module DDM.

11.4.5 Enabling optical module DDM Trap

Enable optical module DDM Trap for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server trap transceiver { enable | disable }** **Example:** Raisecom(config)#snmp-server trap transceiver disable	Enable global optical module DDM Trap. • enable: enable global optical module DDM trap. When the system detects abnormal parameters, it generates a trap. • disable: disable global optical module DDM trap.
3	Raisecom(config)#**interface** *interface-type interface-number* **Example:** Raisecom(config)#interface gigaethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
4	Raisecom(config-gigaethernet1/1/port)#**transceiver trap { enable | disable }** **Example:** Raisecom(config-gigaethernet1/1/1)#transceiver trap enable	Enable interface optical module DDM Trap. Only when global optical DDM Trap is enabled, the optical module, where interface optical module DDM Trap is enabled, can the ISCOM2600G series switch send Traps. • enable: enable interface optical module DDM trap. When the system detects abnormal parameters, it generates a trap. • disable: disable interface optical module DDM trap.

11.4.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show transceiver**	Show global optical module DDM and interface optical module DDM configurations.
2	Raisecom#**show transceiver ddm** *interface-type interface-list* [**detail**]	Show optical module DDM performance parameters.
3	Raisecom#**show transceiver** *interface-type interface-list* **history** [**15m** | **24h**]	Show historical information about optical module DDM.
4	Raisecom#**show transceiver information** *interface-type interface-list*	Show basic information about the optical module.
5	Raisecom#**show transceiver threshold-violations** *interface-type interface-list*	Show the information when the optical module parameters exceed the thresholds.
6	Raisecom#**show transceiver ddm brief**	Show brief information about optical module DDM.

Copyright © Raisecom Technology Co., Ltd.

11.5 System log

11.5.1 Introduction

The system log refers that the ISCOM2600G series switch records the system information and debugging information in a log and sends the log to the specified destination. When the ISCOM2600G series switch fails to work, you can check and locate the fault easily.

The system information and some scheduling output will be sent to the system log to deal with. According to the configuration, the system will send the log to various destinations. The destinations that receive the system log are divided into:

- Console: send the log message to the local console through Console interface.
- Host: send the log message to the host.
- Monitor: send the log message to the monitor, such as Telnet terminal.
- File: send the log message to the Flash of the device.
- Buffer: send the log message to the buffer.
- SNMP server: convert logs to Trap and then outputs Trap to the SNMP server.

According to the severity level, the log is identified by 8 severity levels, as listed in Table 11-4.

Table 11-4 Log levels

Severity	Level	Description
Emergency	0	The system cannot be used.
Alert	1	Need to deal immediately.
Critical	2	Serious status
Error	3	Errored status
Warning	4	Warning status
Notice	5	Normal but important status
Informational	6	Informational event
Debug	7	Debugging information

Note

The severity of output information can be manually configured. When you send information according to the configured severity, you can just send the information whose severity is less than or equal to that of the configured information. For example, when the information is configured with the level 3 (or the severity is errors), the information whose level ranges from 0 to 3, in other words, the severity ranges from emergencies to errors, can be sent.

Copyright © Raisecom Technology Co., Ltd.

11.5.2 Preparing for configurations

Scenario

The ISCOM2600G series switch generates the login successes or failures, key information, debugging information, and error information to system log, outputs them as log files, and sends them to the logging host, Console interface, or control console to facilitate checking and locating faults.

Prerequisite

N/A

11.5.3 Default configurations of system log

Default configurations of system log are as below.

Function	Default value
System log	Enable
Output log information to Console	Enable, the default level is information (6).
Output log information to host	N/A, the default level is information (6).
Output log information to file	Enable, the default level is debugging (7).
Output log information to monitor	Disable, the default level is information (6).
Output log information to buffer	Disable, the default level is information (6).
Log Debug level	Low
Output log information to history list	Disable
Log history list size	1
Transfer log to Trap	Disable. The default level is warning (4).
Log buffer size	4 Kbytes
Transmitting rate of system log	No limit
Timestamp of system log information	• Debug: no timestamp to debug level (7) Syslog information. • Log: The timestamp to 0–6 levels Syslog information is absolute time.

11.5.4 Configuring basic information of system log

Configure basic information of system log for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	`Raisecom(config)#logging on`	(Optional) enable system log.

3	`Raisecom(config)#logging time-stamp { debug | log } { datetime | none | uptime }`
	Example:
	`Raisecom(config)#logging time-stamp log uptime`
		(Optional) configure timestamp for system log.
		• debug: configure the timestamp for level 7 logs.
		• log: configure the timestamp for level 0–6 logs.
		• datetime: the timestamp is an absolute time, a time point, namely, the system time.
		• uptime: the timestamp is a relative time, a period, name, the period after the device is started.
		• none: there is no timestamp.

4	`Raisecom(config)#logging rate-limit log-num`
	Example:
	`Raisecom(config)#logging rate-limit 100`
		(Optional) configure transmitting rate of system log.
		• log-num: number of logs processed per second, an integer, ranging from 1 to 10000

5	`Raisecom(config)#logging sequence-number`	(Optional) configure sequence of system log. The sequence number only applies to the console, monitor, log file, and log buffer, but not log host and history list.

6	`Raisecom(config)#logging discriminator discriminator-number { facility | mnemonics | msg-body } { { drops | includes } key | none }`
	Example:
	`Raisecom(config)#logging discriminator 1 mnemonics drops test`
		(Optional) create and configure system log filter.
		The filter can filter output log from the console, monitor, log file and log buffer.
		• distriminator-number: discriminator number, an integer, ranging from 1 to 5
		• facility: filter a log based on its module name.
		• mnemonics: filter a log based on its name.
		• msg-body: filter a log based on its body text.
		• drops: discard logs that contain keywords and allow logs that do not contain keywords.
		• includes: drop logs that do not contain keywords and allow logs that contain keywords.
		• none: do not filter selected fields.
		• key: keyword, a string of characters
		– facility: the length of the key ranges from 1 to 20 characters.
		– mnemonics: the length of the key ranges from 1 to 30 characters.
		– msg-body: the length of the key ranges from 1 to 64 characters.
		– Logs that contain these keywords will be selected as filtering objects.

7	`Raisecom(config)#logging buginf [ high | normal | low | none ]`
	Example:
	`Raisecom(config)#logging buginf high`
		(Optional) configure sending Debug-level logs.
		• high: send debugging information of the highest level only.
		• normal: send debugging information of normal and higher levels.
		• low: send all debugging information.
		• none: do not send debugging information.

Copyright © Raisecom Technology Co., Ltd.

11.5.5 Configuring system log output

Configure system log output for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#logging console [ log-level | alerts | critical | debugging | emergencies | errors | informational | notifications | warnings | discriminator discriminator-number ]`
	Example:
	`Raisecom(config)#logging console errors`
		(Optional) output system logs to the console.
		• log-level: severity level of logs, an integer ranging from 0 to 7. It has the same function with the following 8 parameters. The difference is that severity level is shown in number, but the following 8 parameters are shown in characters.
		• emergencies: level 0, emergency. The system cannot be used and need to be restarted.
		• alerts: level 1, alert. Must take actions immediately.
		• critical: level 2, critical. Must take actions or analyze reasons.
		• errors: level 3, error. Do not affect serviced but need attention.
		• warnings: level 4, warning. May cause service fault and need attention.
		• notifications: level 5, normal. Provide key operation information when the device works properly.
		• informational: level 6, notification event. Provide general operation information when the device works properly.
		• debugging: level 7, debugging information. Provide general operation information when the device works properly. Need no attention.
		• distriminator: establish a connection with the discriminator. Output discriminated logs to the log history table.
		• distriminator-number: discriminator number, an integer, ranging from 1 to 5

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

3	`Raisecom(config)#logging host { ip-address | ipv6-address } [ log-level | alerts | critical | debugging | emergencies | errors | informational | notifications | warnings | discriminator discriminator-number ]`
	Example:
	`Raisecom(config)#logging host 10.0.0.1 alerts`
		(Optional) output system logs to the log host.
		Up to 10 log hosts are supported.
		• ip-address: IP address of the log host, in dotted decimal notation
		• ipv6-address: IPv6 address of the log host, in colon hexadecimal notation
		• log-level: severity level of logs, an integer ranging from 0 to 7. It has the same function with the following 8 parameters. The difference is that severity level is shown in number, but the following 8 parameters are shown in characters.
		• emergencies: level 0, emergency. The system cannot be used and need to be restarted.
		• alerts: level 1, alert. Must take actions immediately.
		• critical: level 2, critical. Must take actions or analyze reasons.
		• errors: level 3, error. Do not affect serviced but need attention.
		• warnings: level 4, warning. May cause service fault and need attention.
		• notifications: level 5, normal. Provide key operation information when the device works properly.
		• informational: level 6, notification event. Provide general operation information when the device works properly.
		• debugging: level 7, debugging information. Provide general operation information when the device works properly. Need no attention.
		• distriminator: establish a connection with the discriminator. Output discriminated logs to the log history table.
		• distriminator-number: discriminator number, an integer, ranging from 1 to 5

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config)#**logging** [**host** { *ip-address* | *ipv6-address* }] **facility** { **alert** | **audit** | **auth** | **clock** | **cron** | **daemon** | **ftp** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **ntp** | **security** | **syslog** | **user** | **uucp** } **Example:** Raisecom(config)#logging facility auth	Configure the facility field of the log to be sent to the log host. Configuration may fail if you do not create the log host. This configuration is available for all log hosts configured on the ISCOM2600G series switch. • host ip-address: IP address of the host, in dotted decimal notion • ipv6-address: IPv6 address of the log host, in colon hexadecimal notation • alert: logs generated by system alarms • audit: logs generated when audited • auth: logs generated when authenticated • clock: information about clock management process • cron: cron/at tool information • daemon: information about system guard process • ftp: information about FTP process • kern: logs generated by kernel • local0-7: locally-generated logs • lpr: logs generated by Line Printer system • mail: logs generated by mail system • news: logs generated by USENET network news system • ntp: logs generated by network time sub-system • security: logs generated when authorized • syslog: logs generated by system log • user: logs generated by user process • uucp: UUCP system information

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config)#**logging monitor** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **discriminator** *discriminator-number*] **Example:** Raisecom(config)#logging monitor warnings	(Optional) output system logs to the monitor. • log-level: severity level of logs, an integer ranging from 0 to 7. It has the same function with the following 8 parameters. The difference is that severity level is shown in number, but the following 8 parameters are shown in characters. • emergencies: level 0, emergency. The system cannot be used and need to be restarted. • alerts: level 1, alert. Must take actions immediately. • critical: level 2, critical. Must take actions or analyze reasons. • errors: level 3, error. Do not affect serviced but need attention. • warnings: level 4, warning. May cause service fault and need attention. • notifications: level 5, normal. Provide key operation information when the device works properly. • informational: level 6, notification event. Provide general operation information when the device works properly. • debugging: level 7, debugging information. Provide general operation information when the device works properly. Need no attention. • distriminator: establish a connection with the discriminator. Output discriminated logs to the log history table. • distriminator-number: discriminator number, an integer, ranging from 1 to 5
5	Raisecom(config)#**logging file** [**discriminator** *discriminator-number*] **Example:** Raisecom(config)#logging file	(Optional) output system logs to the Flash of the ISCOM2600G series switch. Only warning-level logs are available. • distriminator: establish a connection with the discriminator. Output discriminated logs to the log history table. • distriminator-number: discriminator number, an integer, ranging from 1 to 5

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config)#**logging buffered** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **discriminator** *discriminator-number*] **Example:** Raisecom(config)#logging buffered errors	(Optional) output system logs to the buffer. • log-level: severity level of logs, an integer ranging from 0 to 7. It has the same function with the following 8 parameters. The difference is that severity level is shown in number, but the following 8 parameters are shown in characters. • emergencies: level 0, emergency. The system cannot be used and need to be restarted. • alerts: level 1, alert. Must take actions immediately. • critical: level 2, critical. Must take actions or analyze reasons. • errors: level 3, error. Do not affect serviced but need attention. • warnings: level 4, warning. May cause service fault and need attention. • notifications: level 5, normal. Provide key operation information when the device works properly. • informational: level 6, notification event. Provide general operation information when the device works properly. • debugging: level 7, debugging information. Provide general operation information when the device works properly. Need no attention. • distriminator: establish a connection with the discriminator. Output discriminated logs to the log history table. • distriminator-number: discriminator number, an integer, ranging from 1 to 5
	Raisecom(config)#**logging buffered size** *size* **Example:** Raisecom(config)#logging buffered size 10	(Optional) configure the system log buffer size. • size: buffer size, an integer, ranging from 4 to 256, in units of Kbyte
7	Raisecom(config)#**logging history**	(Optional) output system logs to the log history list. The level of the output logs is the one of the translated Trap.
	Raisecom(config)#**logging history size** *size* **Example:** Raisecom(config)#logging history size 100	(Optional) configure the log history list size. • size: log history size, an integer, ranging from 1 to 500

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

	`Raisecom(config)#logging trap [ log-level | alerts | critical | debugging | emergencies | errors | informational | notifications | warnings | distriminator distriminator-number ]`
	Example:
	`Raisecom(config)#logging trap errors`
		(Optional) enable translating specified logs in the history list to Traps.
		Configurations may fail if the system logs are not output to the log history list.
		• log-level: severity level of logs, an integer ranging from 0 to 7. It has the same function with the following 8 parameters. The difference is that severity level is shown in number, but the following 8 parameters are shown in characters.
		• emergencies: level 0, emergency. The system cannot be used and need to be restarted.
		• alerts: level 1, alert. Must take actions immediately.
		• critical: level 2, critical. Must take actions or analyze reasons.
		• errors: level 3, error. Do not affect serviced but need attention.
		• warnings: level 4, warning. May cause service fault and need attention.
		• notifications: level 5, normal. Provide key operation information when the device works properly.
		• informational: level 6, notification event. Provide general operation information when the device works properly.
		• debugging: level 7, debugging information. Provide general operation information when the device works properly. Need no attention.
		• distriminator: establish a connection with the discriminator. Output discriminated logs to the log history table.
		• distriminator-number: discriminator number, an integer, ranging from 1 to 5

11.5.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show logging`	Show configurations of system log.
2	`Raisecom#show logging buffer`	Show information about the system log buffer.
3	`Raisecom#show logging discriminator`	Show filter information.
4	`Raisecom#show logging file`	Show contents of system log. The device supports this configuration at millisecond level.
5	`Raisecom#show logging history`	Show information about the system log history list.

Copyright © Raisecom Technology Co., Ltd.

11.5.7 Maintenance

Maintain the ISCOM2600G series switch as below.

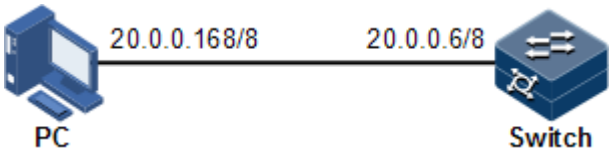
Command	Description
`Raisecom(config)#clear logging buffer`	Clear log information in the buffer.
`Raisecom(config)#clear logging statistics`	Clear log statistics.

11.5.8 Example for configuring outputting system logs to log host

Networking requirements

As shown in Figure 11-10, configure system log, and output device log information to log host for user to check.

Figure 11-10 Networking of outputting system log to log host



Configuration steps

Step 1 Configure the IP address of the ISCOM2600G series switch.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 20.0.0.6 255.0.0.0
Raisecom(config-vlan1)#exit
```

Step 2 Configure the system log to be output to the log host.

```
Raisecom(config)#logging on
Raisecom(config)#logging time-stamp log datetime
Raisecom(config)#logging rate-limit 2
Raisecom(config)#logging host 20.0.0.168 warnings
```

Checking results

Use the **show logging** command to show configurations of system log.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#show logging
Syslog logging:         enable
Dropped Log messages:    0
Dropped debug messages:   0
Rate-limited:          2 messages per second
Squence number display:  disable
Debug level time stamp:  none
Log level time stamp:    datetime
Log buffer size:        4kB
Debug level:           low
Syslog history logging:  disable
Syslog history table size:1
Dest     Status   Level          LoggedMsgs  DroppedMsgs  Discriminator
-----------------------------------------------------------------------
---
buffer   enable   informational(6)  10        0          0
console  enable   informational(6)  10        0          0
trap     disable  warnings(4)      0         0          0
file     enable   debugging(7)     17        0          0
Log host information:
Max number of log server:    10
Current log server number:   1
Target Address     Level          Facility      Sent     Drop
Discriminator
-----------------------------------------------------------------------
--------------
20.0.0.168        warnings(4)      local7       0        0        0
```

11.6 Alarm management

11.6.1 Introduction

Alarm means when a fault is generated on the ISCOM2600G series switch or some working condition changes, the system will generate alarm according to different faults.

Alarm information is used to report some urgent and important events and notify them to the network administrator promptly, which provides strong support for monitoring device operation and diagnosing faults.

Alarm information is stored in the alarm buffer. Meanwhile, the alarm is generated to log information. If a Network Management System (NMS), the alarm will be sent to the NMS through SNMP. The information sent to the NMS is called Trap information.

Alarm classification

Alarms can be divided into three types according to properties:

- Fault alarm: refer to alarms for some hardware fault or some abnormal important functions, such as port Down alarm;
- Recovery alarm: refer to alarms that are generated when device failure or abnormal function returns to normal, such as port Up alarm;

Copyright © Raisecom Technology Co., Ltd.

- Event alarm: refer to prompted alarms or alarms that are generated because of failure in relating the fault to the recovery, such as alarms generated by failing to ping.

Alarms can be divided into five types according to functions:

- Communication alarm: refer to alarms related to the processing of information transmission, including alarms that are generated by communication fault between Network Elements (NE), NEs and NMS, or NMS and NMS.
- Service quality alarm: refer to alarms caused by service quality degradation, including congestion, performance decline, high resource utilization rate, and the bandwidth reducing.
- Processing errored alarm: refer to alarms caused by software or processing errors, including software errors, memory overflow, version mismatching, and the abnormal program aborts.
- Environmental alarm: refer to alarms caused by equipment location-related problems, including the environment temperature, humidity, ventilation and other abnormal working conditions.
- Device alarm: refer to alarms caused by failure of physical resources, including power, fan, processor, clock, Rx/Tx interfaces, and other hardware.

Alarm output

There are three alarm output modes:

- Alarm buffer: alarm is recorded in tabular form, including the current alarm table and history alarm table.
  - Current alarm table, recording alarm which is not cleared, acknowledged or restored.
  - History alarm table, consisting of acknowledged and restored alarm, recording the cleared, auto-restored or manually acknowledged alarm.
- Log: alarm is generated to system log when recorded in the alarm buffer, and stored in the alarm log buffer.
- Trap information: alarm sent to NMS when the NMS is configured.

Alarm will be broadcasted according to various terminals configured by the ISCOM2600G series switch, including CLI terminal and NMS.

Log output of alarm starts with the symbol "#", and the output format is as below:

```
#Index TimeStamp HostName ModuleName/Severity/name:Arise From Description.
```

Table 11-5 describes alarm fields.

Table 11-5 Alarm fields

Field	Description
TimeStamp	Time when an alarm is generated
ModuleName	Name for a module where alarms are generated
Severity	Alarm level

Copyright © Raisecom Technology Co., Ltd.

Field	Description
Arise From Description	Descriptions about an alarm

Alarm levels

The alarm level is used to identify the severity degree of an alarm. The level is defined in Table 11-6.

Table 11-6 Alarm levels

Level	Description	Syslog
Critical (3)	This alarm has affected system services and requires immediate troubleshooting. Restore the device or source immediately if they are completely unavailable, even it is not during working time.	1 (Alert)
Major (4)	This alarm has affected the service quality and requires immediate troubleshooting. Restore the device or source service quality if they decline; or take measures immediately during working hours to restore all performances.	2 (Critical)
Minor (5)	This alarm has not influenced the existing service yet, which needs further observation and take measures at appropriate time to avoid more serious fault.	3 (Error)
Warning (6)	This alarm will not affect the current service, but maybe the potential error will affect the service, so it can be considered as needing to take measures.	4 (Warning)
Indeterminate (2)	Uncertain alarm level, usually the event alarm.	5 (Notice)
Cleared (1)	This alarm shows to clear one or more reported alarms.	5 (Notice)

Related concepts

Related concepts about alarm management are displayed as below:

- Alarm suppression

The ISCOM2600G series switch only records root-cause alarms but incidental alarms when enabling alarm suppression. For example, the generation of alarm A will inevitably produce alarm B which is in the inhibition list of alarm A, then alarm B is inhibited and does not appear in alarm buffer and record the log information when enabling alarm suppression. By enabling alarm suppression, the ISCOM2600G series switch can effectively reduce the number of alarms.

Copyright © Raisecom Technology Co., Ltd.

Alarm A and alarm B will be recorded on the ISCOM2600G series switch and reported to the NMS when alarm suppression is disabled.

- Alarm auto-report

Auto-report refers that an alarm will be reported to NMS automatically with its generation and you do not need to initiate inquiries or synchronization.

You can configure auto-report to some alarm, some alarm source, or the specified alarm from specified alarm source.

Note

The alarm source refers to an entity that generates related alarms, such as ports, devices, and cards.

- Alarm monitoring

Alarm monitoring is used to process alarms generated by modules:

  - When the alarm monitoring is enabled, the alarm module will receive alarms generated by modules, and process them according to the configurations of the alarm module, such as recording alarm in alarm buffer, or recording system logs.
  - When the alarm monitoring is disabled, the alarm module will discard alarms generated by modules without follow-up treatment. In addition, alarms will not be recorded on the ISCOM2600G series switch.

You can perform the alarm monitoring on some alarm, alarm source or specified alarm on from specified alarm source.

- Alarm reverse mode

Alarm reverse refers to the device will report the information opposite to actual status when recording alarm, or report the alarm when there is no alarm. Alarms are not reported if there are alarms.

Currently, the device is only in support of reverse mode configuration of the interface. There are three reverse modes to be configure; the specific definitions are as below:

  - Non-reverse mode

The device alarm is reported normally.

  - Manual reverse mode

Configure the alarm reverse mode of an interface as manual reverse mode. In this mode, no matter what the current alarm status is, the reported alarm status of the interface will be changed opposite to the actual alarm status immediately; in other words, alarms are not reported when there are alarms, and alarms are reported when there are no alarms actually. The interface will maintain the opposite alarm status regardless of the alarm status changes before the alarm reverse status being restored to non-reverse mode.

  - Auto-reverse mode

Configure the alarm reverse mode as auto-reverse mode. If no reversible alarm is on the interface, this configuration will be prompted as failure. If reversible alarms are on the interface, this configuration will succeed and enter reverse mode; in other words, the reported alarm status of the interface will be changed opposite to the actual alarm status immediately. After the alarm is finished, the enabling state of interface alarm reverse will end automatically

Copyright © Raisecom Technology Co., Ltd.

and changes to non-reverse alarm mode so that the alarm status can be reported normally in the next alarm.

- Alarm delay

Alarm delay refers that the ISCOM2600G series switch will record alarms and report them to NMS after a delay but not immediately when alarms generate. Delay for recording and reporting alarms are identical.

By default, the device alarm is reported once generating (0s), which is instant reporting; clear alarm once it ends (0s), which is instant clearing.

- Alarm storage mode

Alarm storage mode refers to how to record new generated alarms when the alarm buffer is full. There are two ways:

  - stop: stop mode, when the alarm buffer is full, new generated alarms will be discarded without recording.
  - loop: wrapping mode, when the alarm buffer is full, the new generated alarms will replace old alarm and take rolling records.

Use configured storage mode to deal with new generated alarm when the alarm in device alarm table is full.

- Clearing alarms

Clear the current alarm, which means deleting current alarms from the current alarm table. The cleared alarms will be saved to the history alarm table.

- Viewing alarms

The administrator can check alarms and monitor alarm directly on the ISCOM2600G series switch. If the ISCOM2600G series switch is configured with NView NNM system, the administrator can monitor alarms on the NView NNM system.

11.6.2 Preparing for configurations

Scenario

When the device fails, alarm management module will collect fault information and output alarm occurrence time, alarm name and description information in log format to help users locate problem quickly.

If the device is configured with the NMS, alarm can be reported directly to the NMS, providing possible alarm causes and treatment recommendations to help users deal with fault.

If the device is configured with hardware monitoring, it will record the hardware monitoring alarm table, generated Syslog, and sent Trap when the operation environment of the device becomes abnormal, and notify the user of taking actions accordingly and prevent faults.

Alarm management facilitates alarm suppression, alarm auto-reporting, alarm monitoring, alarm reverse, alarm delay, alarm memory mode, alarm clear and alarm view directly on the device.

Prerequisite

Hardware environment monitoring alarm output:

Copyright © Raisecom Technology Co., Ltd.

- In Syslog output mode: alarms will be generated into system logs. To send alarm to the system log host, configure the IP address of the system log host for the device.
- In Trap output mode: configure the IP address of the NMS for the device.

11.6.3 Configuring basic functions of alarm management

Configure basic information of alarm management for the ISCOM2600G series switch as below.

All following steps are optional and no sequence between them.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#alarm inhibit { enable | disable }`
	Example:
	`Raisecom(config)#alarm inhibit enable`
		Enable or disable alarm suppression.
		By default, it is enabled.
		• enable: enable alarm suppression.
		• disable: disable alarm suppression.

3	`Raisecom(config)#alarm auto-report all { enable | disable }`
	Example:
	`Raisecom(config)#alarm auto-report all enable`
		Enable alarm auto-reporting.
		• all: all alarms
		• enable: enable alarm auto-report.
		• disable: disable alarm auto-report.

	`Raisecom(config)#alarm auto-report alarm-restype alarm-restype-value { enable | disable }`
	Example:
	`Raisecom(config)#alarm auto-report gigaethernet 1/1/1 enable`
		Enable or disable alarm auto-reporting of a specified alarm source.
		• alarm-restype: alarm source type, a string. The value is the name of an alarm source type, such as port-channel.
		• alarm-restype-value: alarm source value, an integer, related to the alarm source type
		• enable: enable alarm auto-report.
		• disable: disable alarm auto-report.

	`Raisecom(config)#alarm auto-report type alarm-type { enable | disable }`
	Example:
	`Raisecom(config)#alarm auto-report type system_authfailure disable`
		Enable alarm auto-reporting of a specified alarm type.
		• type alarm-type: alarm type, a string. The value is an alarm name, such as aiblightparameterhigh.
		• enable: enable alarm auto-report.
		• disable: disable alarm auto-report.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config)#**alarm auto-report type** *alarm-type alarm-restype alarm-restype-value* { **enable** | **disable** } **Example:** Raisecom(config)#alarm auto-report type erroredframeevent gigaethernet 1/1/1 enable	Enable alarm auto-reporting of a specified alarm source and type. • type alarm-type: alarm type, a string. The value is an alarm name, such as aiblightparameterhigh. • alarm-restype: alarm source type, a string. The value is the name of an alarm source type, such as port-channel. • alarm-restype-value: alarm source value, an integer, related to the alarm source type • enable: enable alarm auto-report. • disable: disable alarm auto-report.
4	Raisecom(config)#**alarm monitor all** { **enable** | **disable** } **Example:** Raisecom(config)#alarm monitor all enable	Enable alarm monitoring. • all: all alarms • enable: enable alarm monitoring. • disable: disable alarm monitoring.
	Raisecom(config)#**alarm monitor** *alarm-restype alarm-restype-value* { **enable** | **disable** } **Example:** Raisecom(config)#alarm monitor gigaethernet 1/1/1 enable	Enable alarm monitoring of a specified alarm source. • alarm-restype: alarm source type, a string. The value is the name of an alarm source type, such as port-channel. • alarm-restype-value: alarm source value, an integer, related to the alarm source type • enable: enable alarm monitoring. • disable: disable alarm monitoring.
	Raisecom(config)#**alarm monitor type** *alarm-type* { **enable** | **disable** } **Example:** Raisecom(config)#alarm monitor type erroredframeevent enable	Enable alarm monitoring of a specified alarm type. • type alarm-type: alarm type, a string. The value is an alarm name, such as blightparameterhigh. • enable: enable alarm monitoring. • disable: disable alarm monitoring.
	Raisecom(config)#**alarm monitor type** *alarm-type alarm-restype alarm-restype-value* { **enable** | **disable** } **Example:** Raisecom(config)#alarm monitor type erroredframeevent gigaethernet 1/1/1 enable	Enable alarm monitoring of a specified alarm source and type. • type alarm-type: alarm type, a string. The value is an alarm name, such as blightparameterhigh. • alarm-restype: alarm source type, a string. The value is the name of an alarm source type, such as port-channel. • alarm-restype-value: alarm source value, an integer, related to the alarm source type • enable: enable alarm monitoring. • disable: disable alarm monitoring.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config)#**alarm monitor-level** { **critical** | **major** | **minor** | **warning** } **Example:** Raisecom(config)#alarm monitor-level minor	(Optional) configure the level of alarm monitoring. • critical: monitoring level 1, critical alarm • major: monitoring level 2, major alarm • minor: monitoring level 3, minor alarm • warning: monitoring level 4, warning alarm
6	Raisecom(config)#**alarm inverse** *interface-type interface-number* { **none** | **auto** | **manual** } **Example:** Raisecom(config)#alarm inverse gigaethernet 1/1/1 auto	Configure alarm reverse modes. By default, it is none; in other words, alarm reverse is disabled. • interface-type: interface type • interface-number: interface ID. The form and value range depend on the interface type. • auto: automatic inverse mode • manual: manual inverse mode • none: non-inverse mode
7	Raisecom(config)#**alarm** { **active** | **clear** } **delay** *second* **Example:** Raisecom(config)#alarm active delay 200	Configure alarm delay. By default, it is 0s. • delay second: alarm delay time, an integer, ranging from 0 to 600, in units of second
8	Raisecom(config)#**alarm active storage-mode** { **loop** | **stop** } **Example:** Raisecom(config)#alarm active storage-mode loop	Configure alarm storage modes. By default, it is stop. • loop: specify the alarm storage mode to loop. • stop: specify the alarm storage mode to stop.
9	Raisecom(config)#**alarm clear all**	(Optional) clear all current alarms.
	Raisecom(config)#**alarm clear index** *index-value* **Example:** Raisecom(config)#alarm clear index 2	(Optional) clear current alarms of the specified alarm index. • index index-value: index of the specified alarm, an integer, ranging from 1 to 4294967295
	Raisecom(config)#**alarm clear** *alarm-restype alarm-restype-value* **Example:** Raisecom(config)#alarm clear gigaethernet 1/1/1	(Optional) clear current alarms of the specified alarm source. • alarm-restype: alarm source type, a string. The value is the name of an alarm source type, such as cpuindex and port-channel. • alarm-restype-value: alarm source value, an integer, related to the alarm source type
	Raisecom(config)#**alarm clear type** *alarm-type* **Example:** Raisecom(config)#alarm clear type erroredframeevent	(Optional) clear current alarms of the specified alarm type. • type alarm-type: alarm type, a string. The value is an alarm name, such as blightparameterhigh and criticalevent.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

	`Raisecom(config)#alarm clear type alarm-type alarm-restype alarm-restype-value`
	Example:
	`Raisecom(config)#alarm clear type erroredframeevent gigaethernet 1/1/1`
		(Optional) clear current alarms of the specified alarm source and type.
		• type alarm-type: alarm type, a string. The value is an alarm name, such as ais, blightparameterhigh, and criticalevent.
		• alarm-restype: alarm source type, a string. The value is the name of an alarm source type, such as boardindex, fanindex, and port-channel.
		• alarm-restype-value: alarm source value, an integer, related to the alarm source type

9	`Raisecom(config)#alarm syslog { enable | disable }`
	Example:
	`Raisecom(config)#alarm syslog enable`
		(Optional) enable or disable alarms to be output to system logs.
		By default, it is disabled.
		• enable: enable alarms to be output to system logs.
		• disable: disable alarms to be output to system logs.

10	`Raisecom(config)#alarm correlation-Inhibit { enable | disable }`
	Example:
	`Raisecom(config)#alarm correlation-Inhibit enable`
		(Optional) enable relevant alarm inhibition.
		Use the **disable** form of this command to disable this function.
		• enable: enable relevant alarm inhibition.
		• disable: disable relevant alarm inhibition.

Note

You can enable/disable alarm monitoring, alarm auto-reporting, and alarm clearing on modules that support alarm management.

11.6.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show alarm management [ alarm_type ]`	Show parameters of current alarms, including status of alarm suppression, alarm reverse mode, alarm delay, and alarm storage mode, maximum alarm buffer size, and alarm log size.
2	`Raisecom#show alarm log`	Show alarm statistics in the system log.
3	`Raisecom#show alarm management statistics`	Show statistics about alarm management module.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
4	Raisecom#**show alarm active** [*module_name* **alarm_manage** | **aps** | **bfd** | **cfm** | **cpcar** | **digitaldiagnotic** | **fanmonitor** | **hw_monitor** | **lbd** | **oam** | **ospf** | **portbackup** | **portlib** | **powermonitor** | **system** | **severity** *severity*]	Show information about current alarms.
5	Raisecom#**show alarm cleared** [*module_name***alarm_manage** | **aps** | **bfd** | **cfm** | **cpcar** | **digitaldiagnotic** | **fanmonitor** | **hw_monitor** | **lbd** | **oam** | **ospf** | **portbackup** | **portlib** | **powermonitor** | **system** | **severity** *severity*]	Show information about history alarms.

11.7 Hardware environment monitoring

Note

Some models of the ISCOM2600G series switch do not support abnormal temperature alarms. For details, see their descriptions.

11.7.1 Introduction

Hardware environment monitoring mainly refers to monitor the running environment of the ISCOM2600G series switch. The monitoring alarm events include:

- Power supply state alarm
- Temperature beyond threshold alarm
- Flash monitoring alarm

There are several ways to notify users when an alarm is generated. The alarm event output methods are as below:

- Save to the device hardware environment monitoring alarm buffer.
- Output Syslog system log.
- Send Trap to the NMS.

You can take appropriate measures to prevent failure when alarm events happen.

Alarm events

- Power supply monitoring alarms
- Power supply state change alarms

Power supply state change refers that unplugged power supply is plugged into the device and vice versa. The ISCOM2600G series switch supports dual power supplies. Therefore, power

Copyright © Raisecom Technology Co., Ltd.

supply state change alarms are divided into the single power supply state change alarm and device dying gasp alarm.

- Dual power supply state change alarm: notify uses that power supply 1/power supply 2 changes. The ISCOM2600G series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.
- Device dying gasp alarm: dual power modules are unplugged, in other words, two power modules are out of position. The ISCOM2600G series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.

- Temperature beyond threshold alarm

The device supports temperature beyond threshold alarm event, when the current temperature is lower than low temperature threshold, the low temperature alarm event will generate. The ISCOM2600G series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.

When the device current temperature is higher than high temperature threshold, the high temperature alarm event will generate. The ISCOM2600G series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.

Alarm output modes

Hardware environment monitoring alarm output modes are as below.

- Hardware environment monitoring alarm buffer output, which is recorded to the hardware environment monitoring alarm table
  - The hardware environment monitoring current alarm table, recording current alarm which has not been cleared and restored.
  - The hardware environment monitoring history alarm table, recording current, restored, and manually cleared alarms.

Hardware environmental monitoring alarm can be recorded in the current hardware environment monitoring alarm table and hardware environment monitoring history alarm table automatically without configuring manually.

- Trap output

Alarms are output to the NMS in Trap mode.

Trap output has global switch and all monitored alarm events still have their own Trap alarm output switches. When enabling the global switch and monitored alarm events switches simultaneously, the alarm will generate Trap output.

Table 11-7 describes Trap information.

Table 11-7 Trap information

Field	Description
Alarm status	• asserted (current alarm) • cleared (alarm recovery) • clearall (clear all alarm)

Copyright © Raisecom Technology Co., Ltd.

Field	Description
Alarm source	• device (global alarm) • Interface number (interface status alarm)
Timestamp	Alarm time, in the form of absolute time
Alarm event type	• dev-power-down (power-down alarm) • power-abnormal (power-abnormal alarm, one of two powers is power down.) • high-temperature (high-temperature alarm) • low-temperature (low-temperature alarm) • all-alarm (clear all alarms)

- Syslog output

Record alarms to Syslog.

Syslog output has global switch and all monitored alarm events still have their own Syslog alarm output switches. When the global switch and monitored alarm events switches are concurrently enabled, the alarm will generate Syslog output.

Table 11-8 describes Syslog information.

Table 11-8 Syslog information

Field	Description
Facility	The module name generating alarm, the hardware environment monitoring module is fixed as alarm.
Severity	Level, the same as defined in system logs. For details, see Table 11-4.
Mnemonics	Alarm event type. For details, see Table 11-7.
Msg-body	Main body, describing alarm event contents.

11.7.2 Preparing for configurations

Scenario

Hardware environment monitoring provides environment monitoring for the devices, through which you can monitor the fault. When device operation environment is abnormal, this function will record hardware environment monitoring alarm list, generate system log, or send Trap and other alarms to notify taking corresponding measures and preventing fault.

Prerequisite

Hardware environment monitoring alarm output:

- In Syslog output mode: alarms will be generated into system logs. To send alarm to the system log host, configure system log host IP address for the device.
- In Trap output mode: configure the management IP address of the device.

Copyright © Raisecom Technology Co., Ltd.

11.7.3 Default configurations of hardware environment monitoring

Default configurations of hardware environment monitoring are as below.

Function	Default value
Global hardware environment monitoring alarm Syslog output	Disable
Global hardware environment monitoring alarm Trap output	Enable
Power down event alarm	• Enable Trap output. • Enable Syslog system log output.
Temperature alarm output	
High temperature alarm threshold	90 ℃
Low temperature alarm threshold	-10 ℃

11.7.4 Enabling global hardware environment monitoring

Enable global hardware environment monitoring for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#logging alarm`	(Optional) enable global hardware environment monitoring alarm Syslog output.

3	`Raisecom(config)#snmp-server alarm-trap { enable | disable }`
	Example:
	`Raisecom(config)#snmp-server alarm-trap enable`
		(Optional) enable or disable global hardware environment monitoring alarm Trap.
		• enable: enable global hardware environment monitoring alarm Trap.
		• disable: disable global hardware environment monitoring alarm Trap.

Note

- When enabling global hardware environment monitoring alarm Syslog output, alarm event can generate Syslog only when Syslog output under alarm event is also enabled.
- When enabling global hardware environment monitoring alarm sending Trap, alarm event can send Trap only when Trap output under alarm event is also enabled.

11.7.5 Configuring temperature monitoring alarm

Configure temperature monitoring alarm for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom(config)#` **`alarm temperature`** `{` **`high`** *`high-value`* `|` **`low`** *`low-value`* `|` **`notifies`** `|` **`syslog`** `}`
	`Example:`
	`Raisecom(config)# alarm temperature low 10`
		Enable temperature monitoring alarm output and configure temperature monitoring alarm output modes.
		• high-value: high temperature threshold, an integer, ranging from 10 to 70 ℃
		• low-value: low temperature threshold, an integer, ranging from 10 to 90 ℃
		• notifies: output temperature alarms in form of Trap.
		• syslog: output temperature alarms in form of Syslog.

11.7.6 Configuring power supply alarm

Configure voltage monitoring alarm for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.

2	`Raisecom(config)#`**`alarm power-supply`** `{` **`notifies`** `|` **`syslog`** `}`
	`Example:`
	`Raisecom(config)#alarm power-supply notifies`
		Enable power supply alarm and configure alarm output mode.
		• notifies: output temperature alarms in form of Trap.
		• syslog: output temperature alarms in form of Syslog.

11.7.7 Clearing all hardware environment monitoring alarms manually

Clear all hardware environment monitoring alarms manually for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`clear alarm`**	Clear alarms manually. **Note** Use this command to clear all alarms in current alarm list and generate an all-alarm alarm in history alarm list. If enabling global sending Trap, the all-alarm alarm will be output in Trap mode; if enabling global Syslog, the all-alarm alarm will be output in Syslog mode.

Copyright © Raisecom Technology Co., Ltd.

11.7.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show alarm`	Show global hardware environment monitoring alarm configurations.
2	`Raisecom#show alarm current`	Show current alarms of hardware environment monitoring.
3	`Raisecom#show alarm history`	Show history alarms of hardware environment monitoring.
4	`Raisecom#show environment { temperature | power }`	Show information about the current environment, such as power supply, temperature, and alarms.

11.8 CPU monitoring

11.8.1 Introduction

The ISCOM2600G series switch supports CPU monitoring. It can monitor state, CPU utilization rate, and application of stacking of each task in real time in the system. It helps locate faults.

CPU monitoring can provide the following functions:

- Viewing CPU utilization rate

It can be used to view unitization of CPU in each period (5s, 1minute, 10minutes, 2hours). Total unitization of CPU in each period can be shown dynamically or statically.

It can be used to view the operational status of all tasks and the detailed running status information about assigned tasks.

It can be used to view history utilization of CPU in each period.

It can be used to view information about dead tasks.

- Threshold alarm of CPU unitization

If CPU utilization of the system is more than configured upper threshold or less than preconfigured lower threshold in specified sampling period, Trap will be sent, and Trap will provide serial number of 5 tasks whose unitization rate of CPU is the highest in the latest period (5s, 1minute, 10minutes) and their CPU utilization rate.

Copyright © Raisecom Technology Co., Ltd.

11.8.2 Preparing for configurations

Scenario

CPU monitoring can provide realtime monitoring to the task status, CPU utilization rate and stack usage in the system, provide CPU utilization rate threshold alarm, detect and eliminate hidden dangers, or help administrator for fault location.

Prerequisite

When the CPU monitoring alarm needs to be output in Trap mode, configure Trap output target host address, which is IP address of NView NNM system.

11.8.3 Default configurations of CPU monitoring

Default configurations of CPU monitoring are as below.

Function	Default value
CPU utilization rate alarm Trap output	Enable
Upper threshold of CPU utilization alarm	99%
Lower threshold of CPU utilization alarm	79%
Sampling period of CPU utilization	60s

11.8.4 Configuring CPU monitoring alarm

Configure CPU monitoring alarm for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#cpu threshold recovering recovering-threshold-value rising rising-threshold-value`
	Example:
	`Raisecom(config)#cpu threshold recovering 20 rising 80`
		(Optional) configure the recovering threshold and rising threshold for CPU alarms.
		• recovering-threshold-value: recovering threshold, an integer, ranging from 1 to 98, indicating 1% to 98%
		• rising-threshold-value: rising threshold, an integer, ranging from 2 to 99, indicating 2% to 99%

3	`Raisecom(config)#cpu interval interval-value`
	Example:
	`Raisecom(config)#cpu interval 60`
		(Optional) configure the interval for sampling CPU alarms.
		• interval-value: sample collection interval, an integer, ranging from 5 to 36000, in units of second

Copyright © Raisecom Technology Co., Ltd.

11.8.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show cpu-utilization [ dynamic | history { 10min | 1min | 2hour | 5sec } ]`	Show CPU utilization.
2	`Raisecom#show process [ sorted { priority | name } | taskname ]`	Show states of all tasks.
3	`Raisecom#show process cpu [ sorted [ 10mins | 1min | 5secs | invoked ] ]`	Show CPU utilization of all tasks.
4	`Raisecom#show process dead`	Show information about dead tasks.
5	`Raisecom#show process pid range`	Show information about the specified task.

11.9 Fan monitoring

11.9.1 Introduction

The ISCOM2600G series switch supports monitoring the fan, including the rotational speed and temperature. It sends Trap when the rotational speed or temperature is abnormal.

The ISCOM2600G series switch monitors the fan in two modes:

- Forcible monitoring: forcibly configure the rotational speed of the fan.
- Automatic monitoring: the fan adjusts its rotational speed by temperature.

In automatic monitoring mode, the rotational speed of the fan has four levels, each of which corresponds to a temperature range. The fan adjusts its rotational speed by temperature.

11.9.2 Preparing for configurations

Scenario

In hot environment, too high temperature affects heat dissipation of the ISCOM2600G series switch. Thus fan monitoring must be configured so that the rotational speed is automatically adjusted according to environment temperature and the ISCOM2600G series switch runs properly.

Precondition

N/A

Copyright © Raisecom Technology Co., Ltd.

11.9.3 Configuring fan monitoring

Configure fan monitoring for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#fan-monitor mode { auto | enforce }`
	Example:
	`Raisecom(config)#fan-monitor mode auto`
		Configure the monitoring mode for the rotational speed.
		By default, it is auto.
		• auto: configure fan monitor mode to auto.
		• enforce: configure fan monitor mode to enforce.

3	`Raisecom(config)#fan-monitor enforce level level`
	Example:
	`Raisecom(config)#fan-monitor enforce level 3`
		(Optional) configure the rotational speed in enforced mode.
		• level: rotational speed level, an integer, ranging from 1 to 4, corresponding to 0 r/s, 7880 r/s, 11300 r/s, and 11500 r/s respectively

4	`Raisecom(config)#fan-monitor trap send { enable | disable }`
	Example:
	`Raisecom(config)#fan-monitor trap send enable`
		(Optional) enable or disable Trap sending for fan monitoring.
		• enable: enable Trap sending for fan monitoring.
		• disable: disable Trap sending for fan monitoring.

11.9.4 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	`Raisecom#show fan-monitor information`	Show configurations of fan monitoring.
2	`Raisecom#show fan-monitor status`	Show fan monitoring status.

11.10 Cable diagnosis

11.10.1 Introduction

The ISCOM2600G series switch supports cable diagnosis, which helps you detect lines.

Cable diagnosis contains the following results:

- Detection result of the Tx cable
- Errored location of the Tx cable

Copyright © Raisecom Technology Co., Ltd.

- Detection result of the Rx cable
- Errored location of the Rx cable

11.10.2 Preparing for configurations

Scenario

After cable diagnosis is enabled, you can learn the running status of cables, locate and clear faults, if any, in time.

Prerequisite

N/A

11.10.3 Configuring cable diagnosis

Configure cable diagnosis for the ISCOM2600G series switch as below.

Step	Command	Description

1	`Raisecom(config)#test cable-diagnostics noshutdown { enable | disable } [ confirm ]`
	Example:
	`Raisecom(config)#test cable-diagnostics noshutdown enable`
		Enable or disable the function of not restarting the interface upon cable diagnosis.
		• enable: enable the function of not restarting the interface upon cable diagnosis.
		• disable: disable the function of not restarting the interface upon cable diagnosis.
		• confirm: confirm.

2	`Raisecom#test cable-diagnostics interface-type interface-number`
	Example:
	`Raisecom#test cable-diagnostics gigaethernet 1/1/1`
		Enable cable diagnosis. The device supports this configuration on multiple interfaces.
		• interface-type: interface type
		• interface-number: interface ID. The form and value range depend on the interface type.

Note

When you enable the function of not restarting the interface upon cable diagnosis, the interface that is in Up status will be restarted once and then obtain cable diagnosis data. Then, when cable diagnosis is ongoing, the interface that is in Up status will not be restarted but directly read cable diagnosis data saved in the buffer, and the interface that is in Down status will obtain the length to the faulty point during cable diagnosis. The newly inserted interface will automatically execute cable diagnosis and save results in the buffer.

11.10.4 Checking configurations

Use the following commands to check configuration results.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
1	`Raisecom#show cable-diagnostics [ interface-type interface-number ]`	Show results of cable diagnosis.

11.11 Memory monitoring

11.11.1 Preparing for configurations

Scenario

Memory monitoring enables you to learn the memory utilization in real time, and provides memory utilization threshold alarms, thus facilitating you to locate and clear potential risks and help network administrator to locate faults.

Prerequisite

To output memory utilization threshold alarms as Trap, configure the IP address of the target host, namely, the IP address of the NMS server.

11.11.2 Configuring memory monitoring

Configure memory monitoring for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#memory threshold recovering recovering-threshold-value rising rising-threshold-value`
	Example:
	`Raisecom(config)#memory threshold recovering 10 rising 90`
		Configure the rising threshold and recovering threshold for memory utilization alarms.
		• recovering-threshold-value: recovering threshold of memory, an integer, ranging from 1 to 98, indicating 1% to 98%
		• rising-threshold-value: rising threshold of memory, an integer, ranging from 2 to 99, indicating 2% to 99%
		• threshold: configure the threshold of memory utilization rate.

3	`Raisecom(config)#memory interval observation-interval-value`
	Example:
	`Raisecom(config)#memory interval 60`
		Configure the interval for sampling memory alarms.
		• interval: configure sample collection time.
		• observation-interval-value: sampling interval, an integer, ranging from 5 to 36000, in units of second

Copyright © Raisecom Technology Co., Ltd.

11.11.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show memory [ module { value | bufferpool | diff }`	Show information about the system memory, including the alarm enabling status, rising threshold, recovering threshold, sampling interval, total memory, used memory, idle memory, memory utilization, and memory used by each module, and memory change.

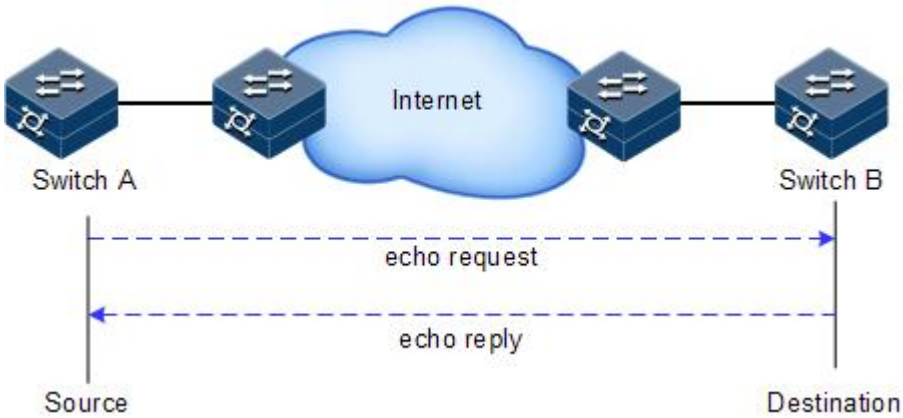
11.12 PING

11.12.1 Introduction

Packet Internet Groper (PING) derives from the sonar location operation, which is used to detect whether the network is normally connected. PING is achieved with ICMP echo packets. If an Echo Reply packet is sent back to the source address during a valid period after the Echo Request packet is sent to the destination address, it indicates that the route between source and destination address is reachable. If no Echo Reply packet is received during a valid period and timeout information is displayed on the sender, it indicates that the route between source and destination addresses is unreachable.

Figure 11-11 shows principles of PING.

Figure 11-11 Principles of PING



11.12.2 Configuring PING

Configure PING for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**ping** [**vrf** *name*]*ip-address* [**count** *countvalue*] [**size** *sizevalue*] [**waittime** *period*] [**source** *ip-address*] **Example:** Raisecom#ping 10.0.0.1	(Optional) test the connectivity of the IPv4 network by the **ping** command. • vrfname: VPN router name, a string of 1 to 31 characters • ip-address: destination IP address • count: specify the numbers of detection packets sent for exiting the PING program. • countvalue: number of detection packets, an integer, ranging from 1 to 65535 • size: specify the size of the detection packet. • sizevalue: size of the detection packet, an integer, ranging from 0 to 12242, in units of Byte • waittime: specify the wait time for PING program. If no response is received when the wait time expires, it is believed the destination is unreachable. • period: timeout time, an integer, ranging from 1 to 60, in units of second • source ip-address: source IP address.
2	Raisecom#**ping ipv6** *ipv6-address* [**count** *countvalue*] [**size** *sizevalue*] [**waittime** *period*] **Example:** Raisecom#**ping ipv6 3001::1**	(Optional) test the connectivity of the IPv6 network by the **ping** command. • ipv6-address: destination IPv6 address • count: specify the numbers of detection packets sent for exiting the PING program. • countvalue: number of detection packets, an integer, ranging from 1 to 65535 • size: specify the size of the detection packet. • sizevalue: size of the detection packet, an integer, ranging from 0 to 12242, in units of Byte • waittime: specify the wait time for PING program. If no response is received when the wait time expires, it is believed the destination is unreachable. • period: timeout time, an integer, ranging from 1 to 60, in units of second

Note

The ISCOM2600G series switch cannot perform other operations in the process of PING. It can perform other operations only when PING is finished or break off PING by pressing **Ctrl**+**C**.

Copyright © Raisecom Technology Co., Ltd.

11.13 Traceroute

11.13.1 Introduction

Similar with PING, Traceroute is a commonly-used maintenance method in network management. Traceroute is often used to test the network nodes of packets from sender to destination, detect whether the network connection is reachable, and analyze network fault

Traceroute works as below:

Step 1 Send a piece of TTL1 sniffer packet (where the UDP port number of the packet is unavailable to any application programs in destination side).

Step 2 TTL deducts 1 when reaching the first hop. Because the TTL value is 0, in the first hop the device returns an ICMP timeout packet, indicating that this packet cannot be sent.

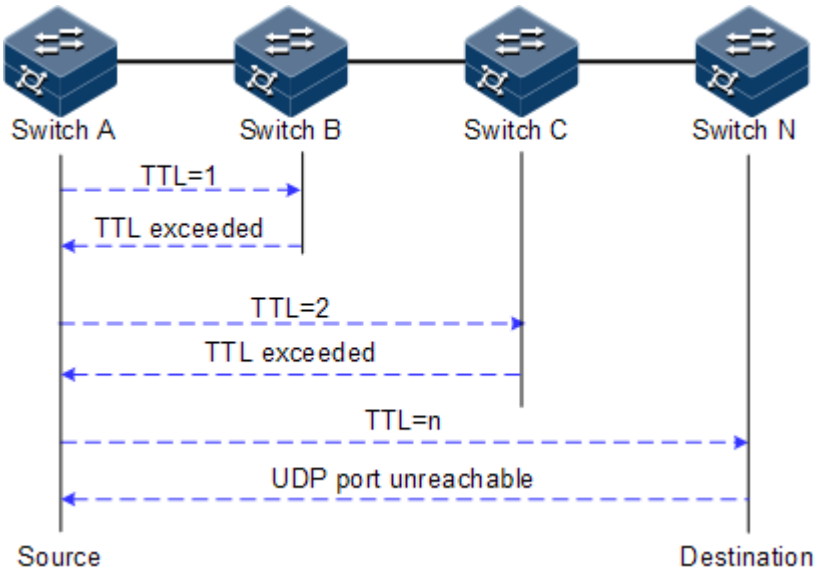
Step 3 The sending host adds 1 to TTL and resends this packet.

Step 4 Because the TTL value is reduced to 0 in the second hop, the device will return an ICMP timeout packet, indicating that this packet cannot be sent.

The previous steps continue until the packet reaches the destination host, which will not return ICMP timeout packets. Because the port number of destination host is not be used, the destination host will send the port unreachable packet and finish the test. Thus, the sending host can record the source address of each ICMP TTL timeout packet and analyze the path to the destination according to the response packet.

Figure 11-12 shows principles of traceroute.

Figure 11-12 Principles of Traceroute



11.13.2 Configuring Traceroute

Before using Traceroute, you should configure the IP address and default gateway of the ISCOM2600G series switch.

Configure Traceroute for the ISCOM2600G series switch as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

1	`Raisecom#`**`traceroute`** `[` **`vrf`** *`name`* `]` *`ip-address`* `[` **`firstttl`** *`first-ttl`* `]` `[` **`maxttl`** *`max-ttl`* `]` `[` **`port`** *`port-number`* `]` `[` **`waittime`** *`period`* `]` `[` **`count`** *`times`* `]` `[` **`size`** *`sizevalue`* `]`
	Example:
	`Raisecom#traceroute 10.0.0.1`
		(Optional) test the connectivity of the IPv4 network and view nodes passed by the packet by the **traceroute** command.
		• vrf name: VPN router name, a string of 1 to 31 characters
		• ip-address: IP address of the destination host/network
		• firstttl: first TTL
		• first-ttl: value of the first TTL, an integer, ranging from 1 to 255
		• maxttl: maximum TTL. When this value is exceeded, the destination is unreachable.
		• max-ttl: value of the maximum TTL, an integer, ranging from 1 to 255
		• port: port number of the UDP packet
		• port-number: interface ID, an integer, ranging from 1 to 65535
		• waittime: specify the timeout for Traceroute program. If no response is received when the timeout expires, the destination is unreachable.
		• period: timeout, an integer, ranging from 1 to 60, in units of second
		• count: configure the number of detection packets sent at the same hop.
		• times: number of detection packets, an integer, ranging from 1 to 10
		• size: specify the size of detection packets.
		• sizevalue: size of detection packets, an integer, ranging from 0 to 4096, in units of Byte

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description

2	`Raisecom#trace route ipv6 ipv6-address [ firstttl fitst-ttl ] [ maxttl max-ttl ] [ port port-number] [ waittime period ] [ count times ] [ size sizevalue ]`
	Example:
	`Raisecom#trace route 3000::1`
		(Optional) test the connectivity of the IPv6 network and view nodes passed by the packet by the **traceroute** command.
		• ipv6-address: IPv6 address, in colon hexadecimal notation, such as 3001::1
		• firstttl: first TTL
		• first-ttl: value of the first TTL, an integer, ranging from 1 to 255
		• maxttl: maximum TTL. When this value is exceeded, the destination is unreachable.
		• max-ttl: value of the maximum TTL, an integer, ranging from 1 to 255
		• port: port number of the UDP packet
		• port-number: interface ID, an integer, ranging from 1 to 65535
		• waittime: specify the timeout for Traceroute program. If no response is received when the timeout expires, the destination is unreachable.
		• period: timeout, an integer, ranging from 1 to 60, in units of second
		• count: configure the number of detection packets sent at the same hop.
		• times: number of detection packets, an integer, ranging from 1 to 10
		• size: specify the size of detection packets.
		• sizevalue: size of detection packets, an integer, ranging from 0 to 4096, in units of Byte

11.14 Performance statistics

11.14.1 Introduction

Performance statistics is used to gather statistics about service packets on the interface of a monitoring device and enable you to learn network performance. It can be based on interface or service flow in a short or long period. The short period is 15 minutes while the long period is 24 hours. Data in a statistical period is written as data block to the Flash for your review.

11.14.2 Preparing for configurations

Scenario

To learn performance of the ISCOM2600G series switch, you can use performance statistics to gather current or historical statistics about packets based on interface or service flow.

Prerequisite

N/A

Copyright © Raisecom Technology Co., Ltd.

11.14.3 Default configurations of performance statistics

Default configurations of performance statistics are as below.

Function	Default value
Performance statistics	Enable
Number of data blocks saved in period statistics mode	16

11.14.4 Configuring performance statistics

Configure performance statistics for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

2	`Raisecom(config)#performance statistics interval buckets buckets-number`
	Example:
	`Raisecom(config)#performance statistics interval buckets 10`
		Configure the number of data blocks saved in the Flash for performance statistics in different statistics period mode.
		• buckets-number: bucket value, an integer, ranging from 10 to 64, in units of pcs

3	`Raisecom(config)#interface interface-type interface-number`
	Example:
	`Raisecom(config)#interface gigaethernet 1/1/1`
		Enable cable diagnosis. The device supports this configuration on multiple interfaces.
		• interface-type: interface type
		• interface-number: interface ID. The form and value range depend on the interface type.

4	`Raisecom(config-gigaethernet1/1/port)#performance statistics [ vlan vlan-id [ cos statistics-cos ] ] { enable | disable }`
	Example:
	`Raisecom(config-gigaethernet1/1/1)#performance statistics enable`
		Enable performance statistics in the VLAN or CoS list.
		Use the **disable** form of this command to disable this function.
		• vlan-id: VLAN ID, an integer, ranging from 1 to 4094
		• statistics-cos: CoS, an integer, ranging from 0 to 7
		• enable: enable performance statistics in the VLAN or CoS list.
		• disable: disable performance statistics in the VLAN or CoS list.

Note

The time for gathering statistics is not related to the time for configuring the command, but related to the system time. Performance statistics take 15min as a period to complete a round of statistics. For example, if the first round of performance statistics

Copyright © Raisecom Technology Co., Ltd.

is enabled at the 5th minute, the first round actually starts at the 15th minute and ends at 30th minute.

11.14.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show performance statistics interface** *interface-type interface-number* { **current**|**history** } Raisecom#**show performance statistics interval buckets** Raisecom#**show interface** *interface-type interface-number* **vlan** *vlan-id* [**cos** *cos-value*] { **current** | **history** }	Show performance statistics.

11.14.6 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
Raisecom(config)#**clear performance statistics history**	Clear performance statistics.

Copyright © Raisecom Technology Co., Ltd.

12 Appendix

This chapter list terms, acronyms, and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

12.1 Terms

A

Access Control List (ACL)	A series of ordered rules composed of permit | deny sentences. These rules are based on the source MAC address, destination MAC address, source IP address, destination IP address, and interface ID. The device determines to receive or refuse the packets based on these rules.
Automatic Laser Shutdown (ALS)	The technology that is used for automatically shutting down the laser to avoid the maintenance and operation risks when the fiber is pulled out or the output power is too great.
Auto-negotiation	The interface automatically chooses the rate and duplex mode according to the result of negotiation. The auto-negotiation process is: the interface adapts its rate and duplex mode to the highest performance according to the peer interface; in other words, both ends of the link adopt the highest rate and duplex mode they both support after auto-negotiation.
Automatic Protection Switching (APS)	APS is used to monitor transport lines in real time and automatically analyze alarms to discover faults. When a critical fault occurs, through APS, services on the working line can be automatically switched to the protection line, thus the communication is recovered in a short period.

B

Bracket	Small parts at both sides of the chassis, used to install the chassis into the cabinet

Copyright © Raisecom Technology Co., Ltd.

C

Challenge Handshake Authentication Protocol (CHAP)	CHAP is a widely supported authentication method in which a representation of the user's password, rather than the password itself, is sent during the authentication process. With CHAP, the remote access server sends a challenge to the remote access client. The remote access client uses a hash algorithm (also known as a hash function) to compute a Message Digest-5 (MD5) hash result based on the challenge and a hash result computed from the user's password. The remote access client sends the MD5 hash result to the remote access server. The remote access server, which also has access to the hash result of the user's password, performs the same calculation using the hash algorithm and compares the result to the one sent by the client. If the results match, the credentials of the remote access client are considered authentic. A hash algorithm provides one-way encryption, which means that calculating the hash result for a data block is easy, but determining the original data block from the hash result is mathematically infeasible.

D

Dynamic ARP Inspection (DAI)	A security feature that can be used to verify the ARP data packets in the network. With DAI, the administrator can intercept, record, and discard ARP packets with invalid MAC address/IP address to prevent common ARP attacks.
Dynamic Host Configuration Protocol (DHCP)	A technology used for assigning IP address dynamically. It can automatically assign IP addresses for all clients in the network to reduce workload of the administrator. In addition, it can implement centralized management of IP addresses.

E

Ethernet in the First Mile (EFM)	Complying with IEEE 802.3ah protocol, EFM is a link-level Ethernet OAM technology. It provides the link connectivity detection, link fault monitoring, and remote fault notification for a link between two directly-connected devices. EFM is mainly used for the Ethernet link on edges of the network accessed by users.
Ethernet Ring Protection Switching (ERPS)	It is an APS protocol based on ITU-T G.8032 standard, which is a link-layer protocol specially used for the Ethernet ring. In normal conditions, it can avoid broadcast storm caused by the data loop on the Ethernet ring. When the link or device on the Ethernet ring fails, services can be quickly switched to the backup line to enable services to be recovered in time.

F

Full duplex	In a communication link, both parties can receive and send data concurrently.

G

Copyright © Raisecom Technology Co., Ltd.

GFP encapsulation	Generic Framing Procedure (GFP) is a generic mapping technology. It can group variable-length or fixed-length data for unified adaption, making data services transmitted through multiple high-speed physical transmission channels.
Ground cable	The cable to connect the device to ground, usually a yellow/green coaxial cable. Connecting the ground cable properly is an important guarantee to lightning protection, anti-electric shock, and anti-interference.

H

Half duplex	In a communication link, both parties can receive or send data at a time.

I

Institute of Electrical and Electronics Engineers (IEEE)	A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.
Internet Assigned Numbers Authority (IANA)	The organization operated under the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the NIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP suite, including autonomous system numbers.
Internet Engineering Task Force (IETF)	A worldwide organization of individuals interested in networking and the Internet. Managed by the Internet Engineering Steering Group (IESG), the IETF is charged with studying technical problems facing the Internet and proposing solutions to the Internet Architecture Board (IAB). The work of the IETF is carried out by various working groups that concentrate on specific topics, such as routing and security. The IETF is the publisher of the specifications that led to the TCP/IP protocol standard.

L

Label	Symbols for cable, chassis, and warnings
Link Aggregation	With link aggregation, multiple physical Ethernet interfaces are combined to form a logical aggregation group. Multiple physical links in one aggregation group are taken as a logical link. Link aggregation helps share traffic among member interfaces in an aggregation group. In addition to effectively improving the reliability on links between devices, link aggregation can help gain greater bandwidth without upgrading hardware.

Copyright © Raisecom Technology Co., Ltd.

Link Aggregation Control Protocol (LACP)	A protocol used for realizing link dynamic aggregation. The LACPDU is used to exchange information with the peer device.
Link-state tracking	Link-state tracking provides an interface linkage scheme, extending the range of link backup. Through monitoring upstream links and synchronizing downstream links, faults of the upstream device can be transferred quickly to the downstream device, and primary/backup switching is triggered. In this way, it avoids traffic loss because the downstream device does not sense faults of the upstream link.

M

Multi-Mode Fiber (MMF)	In this fiber, multi-mode optical signals are transmitted.

N

Network Time Protocol (NTP)	A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed time server and clients. NTP is used to perform clock synchronization on all devices that have clocks in the network. Therefore, the devices can provide different applications based on a unified time. In addition, NTP can ensure a very high accuracy with an error of 10ms or so.

O

Open Shortest Path First (OSPF)	An internal gateway dynamic routing protocol, which is used to determine the route in an Autonomous System (AS)
Optical Distribution Frame (ODF)	A distribution connection device between the fiber and a communication device. It is an important part of the optical transmission system. It is mainly used for fiber splicing, optical connector installation, fiber adjustment, additional pigtail storage, and fiber protection.

P

Password Authentication Protocol (PAP)	PAP is an authentication protocol that uses a password in Point-to-Point Protocol (PPP). It is a twice handshake protocol and transmits unencrypted user names and passwords over the network. Therefore, it is considered unsecure.
Point-to-point Protocol over Ethernet (PPPoE)	PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames. With PPPoE, the remote access device can control and account each access user.

Copyright © Raisecom Technology Co., Ltd.

Private VLAN (PVLAN)	PVLAN adopts Layer 2 isolation technology. Only the upper VLAN is visible globally. The lower VLANs are isolated from each other. If you partition each interface of the switch or IP DSLAM device into a lower VLAN, all interfaces are isolated from each other.

Q

QinQ	QinQ is (also called Stacked VLAN or Double VLAN) extended from 802.1Q, defined by IEEE 802.1ad recommendation. Basic QinQ is a simple Layer 2 VPN tunnel technology, encapsulating outer VLAN Tag for client private packets at carrier access end, the packets take double VLAN Tag passing through trunk network (public network). In public network, packets only transmit according to outer VLAN Tag, the private VLAN Tag are transmitted as data in packets.
Quality of Service (QoS)	A network security mechanism, used to solve problems of network delay and congestion. When the network is overloaded or congested, QoS can ensure that packets of important services are not delayed or discarded and the network runs high efficiently. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio.

R

Rapid Spanning Tree Protocol (RSTP)	Evolution of the Spanning Tree Protocol (STP), which provides improvements in the speed of convergence for bridged networks
Remote Authentication Dial In User Service (RADIUS)	RADIUS refers to a protocol used to authenticate and account users in the network. RADIUS works in client/server mode. The RADIUS server is responsible for receiving users' connection requests, authenticating users, and replying configurations required by all clients to provide services for users.

S

Simple Network Management Protocol (SNMP)	A network management protocol defined by Internet Engineering Task Force (IETF) used to manage devices in the Internet. SNMP can make the network management system to remotely manage all network devices that support SNMP, including monitoring network status, modifying network device configurations, and receiving network event alarms. At present, SNMP is the most widely-used network management protocol in the TCP/IP network.
Simple Network Time Protocol (SNTP)	SNTP is mainly used for synchronizing time of devices in the network.
Single-Mode Fiber (SMF)	In this fiber, single-mode optical signals are transmitted.

Copyright © Raisecom Technology Co., Ltd.

Spanning Tree Protocol (STP)	STP can be used to eliminate network loops and back up link data. It blocks loops in logic to prevent broadcast storms. When the unblocked link fails, the blocked link is re-activated to act as the backup link.

V

Virtual Local Area Network (VLAN)	VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segments logically rather than physically, thus implementing multiple virtual work groups which are based on Layer 2 isolation and do not affect each other.
VLAN mapping	VLAN mapping is mainly used to replace the private VLAN Tag of the Ethernet service packet with the ISP's VLAN Tag, making the packet transmitted according to ISP's VLAN forwarding rules. When the packet is sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Thus, the packet is sent to the destination correctly.

12.2 Acronyms and abbreviations

A

AAA	Authentication, Authorization and Accounting
ABR	Area Border Router
AC	Alternating Current
ACL	Access Control List
ANSI	American National Standards Institute
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
AS	Autonomous System
ASCII	American Standard Code for Information Interchange
ASE	Autonomous System External
ATM	Asynchronous Transfer Mode
AWG	American Wire Gauge

B

BC	Boundary Clock
BDR	Backup Designated Router

Copyright © Raisecom Technology Co., Ltd.

BITS	Building Integrated Timing Supply System
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BTS	Base Transceiver Station

C

CAR	Committed Access Rate
CAS	Channel Associated Signaling
CBS	Committed Burst Size
CE	Customer Edge
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CST	Common Spanning Tree

D

DAI	Dynamic ARP Inspection
DBA	Dynamic Bandwidth Allocation
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Service
DNS	Domain Name System
DRR	Deficit Round Robin
DS	Differentiated Services
DSL	Digital Subscriber Line

E

Copyright © Raisecom Technology Co., Ltd.

EAP	Extensible Authentication Protocol
EAPoL	EAP over LAN
EFM	Ethernet in the First Mile
EMC	Electro Magnetic Compatibility
EMI	Electro Magnetic Interference
EMS	Electro Magnetic Susceptibility
ERPS	Ethernet Ring Protection Switching
ESD	Electro Static Discharge
EVC	Ethernet Virtual Connection

F

FCS	Frame Check Sequence
FE	Fast Ethernet
FIFO	First Input First Output
FTP	File Transfer Protocol

G

GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GMRP	GARP Multicast Registration Protocol
GPS	Global Positioning System
GVRP	Generic VLAN Registration Protocol

H

HDLC	High-level Data Link Control
HTTP	Hyper Text Transfer Protocol

I

IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IE	Internet Explorer
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronics Engineers

Copyright © Raisecom Technology Co., Ltd.

IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System Routing Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector

L

LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LAN	Local Area Network
LCAS	Link Capacity Adjustment Scheme
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit

M

MAC	Medium Access Control
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface cross-over
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Between Failure
MTU	Maximum Transmission Unit
MVR	Multicast VLAN Registration

N

NMS	Network Management System
NNM	Network Node Management
NTP	Network Time Protocol
NView NNM	NView Network Node Management

Copyright © Raisecom Technology Co., Ltd.

O

OAM	Operation, Administration and Management
OC	Ordinary Clock
ODF	Optical Distribution Frame
OID	Object Identifiers
Option 82	DHCP Relay Agent Information Option
OSPF	Open Shortest Path First

P

P2MP	Point to Multipoint
P2P	Point-to-Point
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADS	PPPoE Active Discovery Session-confirmation
PAP	Password Authentication Protocol
PDU	Protocol Data Unit
PE	Provider Edge
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PING	Packet Internet Grope
PPP	Point to Point Protocol
PPPoE	PPP over Ethernet
PTP	Precision Time Protocol

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial In User Service
RCMP	Raisecom Cluster Management Protocol
RED	Random Early Detection
RH	Relative Humidity
RIP	Routing Information Protocol

Copyright © Raisecom Technology Co., Ltd.

RMON	Remote Network Monitoring
RNDP	Raisecom Neighbor Discover Protocol
ROS	Raisecom Operating System
RPL	Ring Protection Link
RRPS	Raisecom Ring Protection Switching
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource Reservation Protocol
RTDP	Raisecom Topology Discover Protocol

S

SCADA	Supervisory Control And Data Acquisition
SF	Signal Fail
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SPF	Shortest Path First
SSHv2	Secure Shell v2
STP	Spanning Tree Protocol

T

TACACS+	Terminal Access Controller Access Control System
TC	Transparent Clock
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service
TPID	Tag Protocol Identifier
TTL	Time To Live

U

Copyright © Raisecom Technology Co., Ltd.

UDP	User Datagram Protocol
UNI	User Network Interface
USM	User-Based Security Model

V

VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol

W

WAN	Wide Area Network
WRR	Weight Round Robin

Copyright © Raisecom Technology Co., Ltd.

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

Address: Raisecom Building, No. 11, East Area, No. 10 Block, East Xibeiwang Road, Haidian District, Beijing, P.R.China Postal code: 100094 Tel: +86-10-82883305
Fax: 8610-82883056 http://www.raisecom.com Email: export@raisecom.com