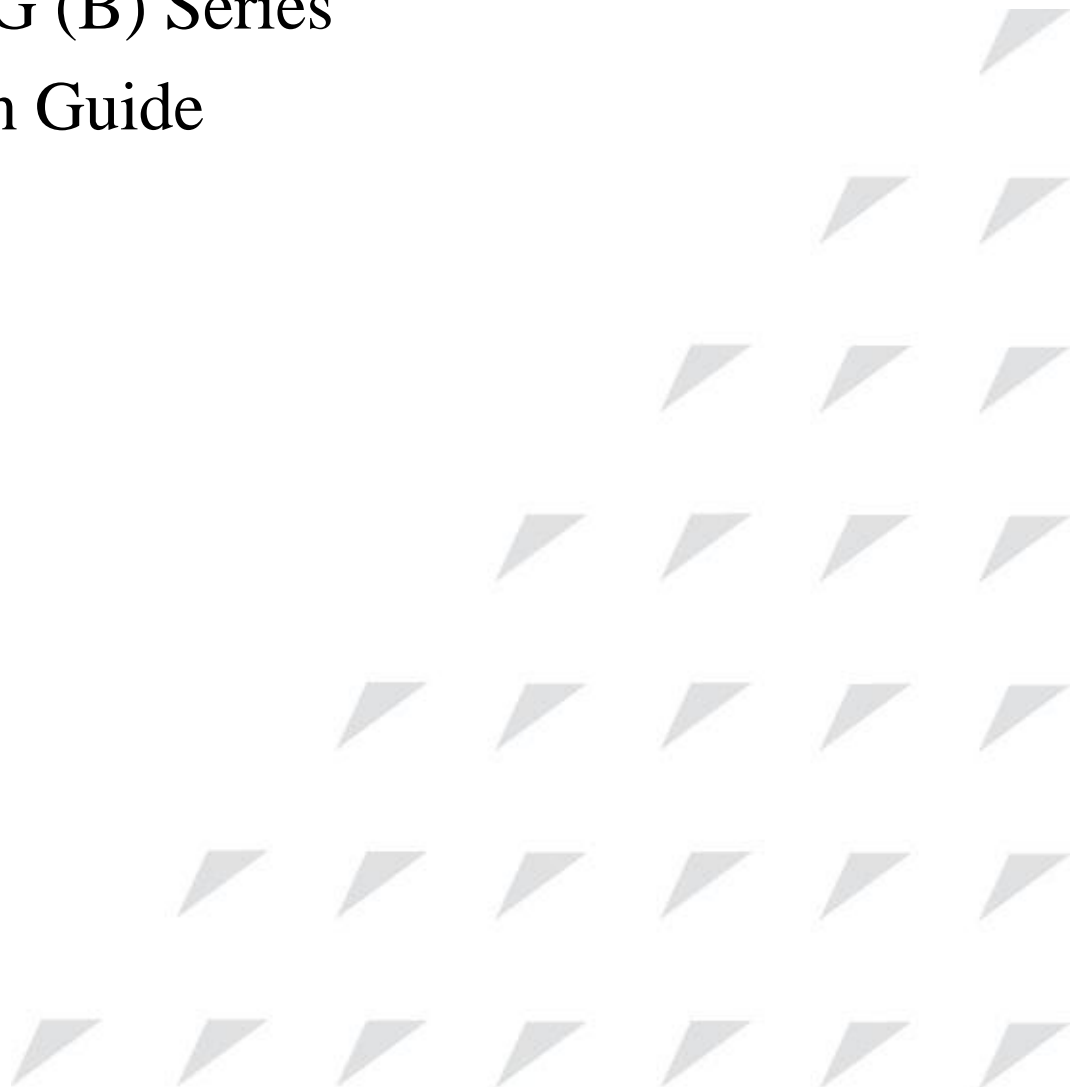


www.raisecom.com

**ISCOM3000G (B) Series
Configuration Guide
(Rel_05)**



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 ©2017

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 ISCOM3000G series switch, and related configurations, including basic configurations, basic principles and configuration procedures of Ethernet, ring network protection, IP routing, 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 ISCOM3000G series switch, and how to network with the ISCOM3000G series switch.

Versions



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



Product name	Software version	Hardware version
ISCOM3000G series switch	V3.41	B

Conventions

Symbol conventions

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

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.

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 .
<i>Italic</i>	Book titles are in <i>italics</i> .
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 .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[]	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.

Change history

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

Issue 05 (2017-08-15)

Fifth commercial release

- Added cable diagnosis, SFTP uploading and downloading, NTP encryption, and rate limiting.
- Updated commands in time management, interface management, QinQ, VLAN mapping, QoS, DHCP, multicast, storm control, TACACS+, RADIUS, and 802.1x.
- Fixed known bugs.

Issue 04 (2017-01-15)

Fourth commercial release

- Upgraded software version to V3.41.
- Added voice VLAN, ISIS, RIP, BGP, anti-ARP attack, performance statistics, mLACP, and MRSTP. Optimized ISF.
- Fixed known bugs.

Issue 03 (2016-10-14)

Third commercial release

- Fixed known bugs.

Issue 02 (2016-08-05)

Second commercial release

- Fixed known bugs.

Issue 01 (2016-04-21)

Initial commercial release

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.....	7
1.1.6 Display information	9
1.1.7 Command history	10
1.1.8 Restoring default value of command line	10
1.1.9 Logging command lines.....	11
1.2 Accessing device	11
1.2.1 Introduction.....	11
1.2.2 Accessing through Console interface	12
1.2.3 Accessing through Telnet	13
1.2.4 Accessing through SSH.....	15
1.2.5 Managing users	17
1.2.6 Checking configurations	19
1.2.7 Example for configuring user management	19
1.3 File management	21
1.3.1 Managing BootROM files.....	21
1.3.2 Managing system files	22
1.3.3 Managing configuration files	22
1.3.4 Checking configurations	23
1.3.5 Maintenance	24
1.4 Loading and upgrade.....	24
1.4.1 Introduction.....	24
1.4.2 Upgrading system software through BootROM.....	25
1.4.3 Upgrading system software through CLI	26
1.4.4 Checking configurations	27
1.5 Time management	27
1.5.1 Introduction.....	27

1.5.2	Preparing for configurations	30
1.5.3	Default configurations of time management	30
1.5.4	Configuring time and time zone.....	32
1.5.5	Configuring DST	32
1.5.6	Configuring NTP	32
1.5.7	Configuring SNTP	34
1.5.8	Checking configurations	34
1.5.9	Example for configuring NTP.....	34
1.6	Interface management	37
1.6.1	Introduction.....	37
1.6.2	Default configurations of interface management	38
1.6.3	Configuring basic attributes of interfaces	38
1.6.4	Configuring interface rate statistics	40
1.6.5	Configuring flow control on interfaces	40
1.6.6	Shutting down/Restarting interface	40
1.6.7	Configuring Console interface	41
1.6.8	Configuring sub-interface	41
1.6.9	Configuring Combo interface	41
1.6.10	Checking configurations	42
1.7	Configuring basic information	42
1.8	Task scheduling	43
1.8.1	Introduction.....	43
1.8.2	Configuring task scheduling	43
1.8.3	Checking configurations	44
1.9	Watchdog.....	44
1.9.1	Introduction.....	44
1.9.2	Preparing for configurations	45
1.9.3	Default configurations of Watchdog	45
1.9.4	Configuring Watchdog	45
1.9.5	Checking configurations	45
1.10	Configuring Banner.....	45
1.10.1	Preparing for configurations	45
1.10.2	Configuring Banner.....	46
1.10.3	Enabling Banner display	46
1.10.4	Checking configurations	47
2	ISF	48
2.1	Introduction	48
2.1.1	ISF advantages	49
2.1.2	ISF application	49
2.2	ISF concepts	49
2.2.2	Principles of ISF	52

2.2.3 ISF merge and ISF split.....	55
2.2.4 ISF management and maintenance.....	56
2.2.5 MAD	57
2.3 Establishing ISF environment	57
2.3.1 Establishment flow.....	57
2.3.2 Planning number of ISF members.....	58
2.3.3 Planning roles and IDs of ISF members.....	59
2.3.4 Planning ISF topology	59
2.3.5 Planning ISF physical interfaces	59
2.3.6 Installing ISF members	59
2.3.7 Connecting ISF cables	59
2.3.8 Configuring ISF system software.....	59
2.4 Configuring ISF	60
2.4.1 Preparing for configurations	60
2.4.2 Default configurations of ISF.....	60
2.4.3 Preconfiguration mode.....	60
2.4.4 Non-preconfiguration mode	61
2.5 Preconfiguring ISF in standalone mode	61
2.5.1 Configuring ISF interface	62
2.5.2 Configuring member priority	62
2.5.3 Configuring ISF mode	63
2.6 Configuring ISF in ISF mode.....	63
2.6.1 Configuring ISF mode	63
2.6.2 Configuring ISF domain ID	63
2.6.3 Configuring ISF interface	64
2.6.4 Configuring member ID.....	65
2.6.5 Configuring member priority	66
2.6.6 Configuring reservation time for ISF bridge MAC address	66
2.6.7 Enabling automatic device restart upon ISF merge.....	67
2.6.8 Configuring MAD.....	68
2.7 Checking configurations	73
2.8 Configuration examples	74
2.8.1 Example for configuring ISF in preconfiguration mode with BFD MAD	74
2.8.2 Example for configuring ISF in non-preconfiguration mode with BFD MAD.....	77
2.8.3 Example for switching member device from ISF mode to standalone mode	80
2.8.4 Example for configuring four devices to form ISF	82
3 Ethernet.....	88
3.1 MAC address table	88
3.1.1 Introduction.....	88
3.1.2 Preparing for configurations	90
3.1.3 Default configurations of MAC address table.....	91

3.1.4 Configuring static MAC address.....	91
3.1.5 Configuring blackhole MAC address.....	91
3.1.6 Filtering unknown multicast packets.....	92
3.1.7 Configuring MAC address learning	92
3.1.8 Configuring aging time of MAC addresses.....	92
3.1.9 Enabling suppression of MAC address flapping	92
3.1.10 Checking configurations	93
3.1.11 Maintenance	93
3.1.12 Example for configuring MAC address table.....	94
3.2 VLAN.....	95
3.2.1 Introduction.....	95
3.2.2 Preparing for configurations	98
3.2.3 Default configurations of VLAN	98
3.2.4 Configuring VLAN attributes	98
3.2.5 Configuring interface mode	99
3.2.6 Configuring VLAN on Access interface	99
3.2.7 Configuring VLAN on Trunk interface.....	100
3.2.8 Configuring VLAN based on MAC address	101
3.2.9 Configuring VLAN based on IP subnet	101
3.2.10 Checking configurations	102
3.2.11 Example for configuring VLAN	102
3.3 PVLAN	105
3.3.1 Introduction.....	105
3.3.2 Preparing for configuration.....	106
3.3.3 Default configurations of PVLAN	106
3.3.4 Configuring PVLAN type	106
3.3.5 Configuring PVLAN association	107
3.3.6 Configuring PVLAN mode on interface	107
3.3.7 Checking configuration.....	108
3.3.8 Example for configuring PVLAN.....	108
3.4 Super VLAN	112
3.4.1 Introduction.....	112
3.4.2 Preparing for configurations	113
3.4.3 Configuring super VLAN	113
3.4.4 Checking configurations	114
3.4.5 Example for configuring super VLAN.....	114
3.5 QinQ.....	117
3.5.1 Introduction.....	117
3.5.2 Preparing for configurations	118
3.5.3 Default configurations of QinQ	118
3.5.4 Configuring basic QinQ.....	118
3.5.5 Configuring selective QinQ	119

3.5.6	Configuring network-side interface to Trunk mode	120
3.5.7	Configuring TPID	120
3.5.8	Checking configurations	121
3.5.9	Example for configuring basic QinQ	121
3.5.10	Example for configuring selective QinQ	123
3.6	VLAN mapping	124
3.6.1	Introduction	124
3.6.2	Preparing for configurations	125
3.6.3	Default configurations of VLAN mapping	125
3.6.4	Configuring VLAN mapping	126
3.6.5	Checking configurations	126
3.6.6	Example for configuring VLAN mapping	127
3.7	STP/RSTP	129
3.7.1	Introduction	129
3.7.2	Preparation for configuration	132
3.7.3	Default configurations of STP	132
3.7.4	Enabling STP	133
3.7.5	Configuring STP parameters	133
3.7.6	(Optional) configuring RSTP edge interface	134
3.7.7	(Optional) configuring RSTP link type	134
3.7.8	Checking configurations	135
3.7.9	Example for configuring STP	135
3.8	MSTP	138
3.8.1	Introduction	138
3.8.2	Preparation for configuration	141
3.8.3	Default configurations of MSTP	141
3.8.4	Enabling MSTP	142
3.8.5	Configuring MST domain and its maximum number of hops	142
3.8.6	Configuring root/backup bridge	143
3.8.7	Configuring interface priority and system priority	144
3.8.8	Configuring network diameter for switch network	145
3.8.9	Configuring internal path cost of interface	145
3.8.10	Configuring external path cost of interface	146
3.8.11	Configuring maximum transmission rate on interface	146
3.8.12	Configuring MSTP timer	147
3.8.13	Configuring edge interface	147
3.8.14	Configuring BPDU filtering	148
3.8.15	Configuring BPDU Guard	148
3.8.16	Configuring STP/RSTP/MSTP mode switching	149
3.8.17	Configuring link type	149
3.8.18	Configuring root interface protection	150
3.8.19	Configuring interface loopguard	150

3.8.20	Checking configurations	151
3.8.21	Maintenance	151
3.8.22	Example for configuring MSTP	152
3.9	MRSTP.....	156
3.9.1	Introduction.....	156
3.9.2	Preparing for configurations	156
3.9.3	Default configurations of MRSTP	157
3.9.4	Enabling MRSTP	157
3.9.5	Configuring MRSTP parameters.....	157
3.9.6	Checking configurations	158
3.10	Loop detection.....	158
3.10.1	Introduction.....	158
3.10.2	Preparing for configurations	160
3.10.3	Default configurations of loop detection.....	161
3.10.4	Configuring loop detection	161
3.10.5	Checking configurations	162
3.10.6	Maintenance	162
3.10.7	Example for configuring inner loop detection	162
3.11	Interface protection.....	164
3.11.1	Introduction	164
3.11.2	Preparing for configurations.....	164
3.11.3	Default configurations of interface protection	164
3.11.4	Configuring interface protection	165
3.11.5	Configuring interface isolation.....	165
3.11.6	Checking configurations	165
3.11.7	Example for configuring interface protection	166
3.12	Port mirroring.....	167
3.12.1	Introduction.....	167
3.12.2	Preparing for configurations	168
3.12.3	Default configurations of port mirroring.....	168
3.12.4	Configuring port mirroring on local port	168
3.12.5	Checking configurations	169
3.12.6	Example for configuring port mirroring.....	169
3.13	L2CP	171
3.13.1	Introduction.....	171
3.13.2	Preparing for configurations	171
3.13.3	Default configurations of L2CP	171
3.13.4	Configuring global L2CP.....	171
3.13.5	Configuring L2CP profile	172
3.13.6	Configuring L2CP profile on interface	172
3.13.7	Checking configurations	173
3.13.8	Maintenance.....	173

3.13.9 Example for configuring L2CP	173
3.14 Voice VLAN	176
3.14.1 Introduction	176
3.14.2 Preparing for configurations	177
3.14.3 Default configurations of voice VLAN	177
3.14.4 Configuring OUI address	178
3.14.5 Enabling voice VLAN	178
3.14.6 Configuring QoS of voice VLAN	178
3.14.7 Checking configurations	179
4 Ring network protection	180
4.1 G.8032	180
4.1.1 Introduction	180
4.1.2 Preparing for configurations	180
4.1.3 Default configurations of G.8032	181
4.1.4 Creating G.8032 ring	181
4.1.5 (Optional) creating G.8032 tributary ring	183
4.1.6 (Optional) configuring G.8032 switching control	185
4.1.7 Checking configurations	186
4.1.8 Maintenance	186
5 IP services	187
5.1 IP basis	187
5.1.1 Introduction	187
5.1.2 Preparing for configurations	187
5.1.3 Default configurations of Layer 3 interface	188
5.1.4 Configuring IPv4 address of VLAN interface	188
5.1.5 Configuring IPv6 address of VLAN interface	188
5.1.6 Configuring attributes of management VLAN	189
5.1.7 Checking configurations	189
5.1.8 Example for configuring VLAN interface to interconnect with host	189
5.2 Loopback interface	191
5.2.1 Introduction	191
5.2.2 Preparing for configurations	191
5.2.3 Default configurations of loopback interface	191
5.2.4 Configuring IP address of loopback interface	191
5.2.5 Checking configurations	192
5.3 ARP	192
5.3.1 Introduction	192
5.3.2 Preparing for configurations	193
5.3.3 Default configurations of ARP	193
5.3.4 Configuring static ARP entries	193
5.3.5 Configuring dynamic ARP entries	194

5.3.6 Configuring local proxy ARP.....	194
5.3.7 Checking configurations	194
5.3.8 Maintenance	194
5.3.9 Example for configuring ARP	195
5.4 NDP.....	196
5.4.1 Introduction.....	196
5.4.2 Preparing for configurations	197
5.4.3 Default configurations of NDP	197
5.4.4 Configuring static neighbor entries	197
5.4.5 Configuring times of sending NS messages for detecting duplicated addresses.....	197
5.4.6 Configuring maximum number of NDPs allowed to be learnt on Layer 3 interface.....	198
5.4.7 Checking configurations	198
5.4.8 Maintenance	199
5.5 Route management.....	199
5.5.1 Preparing for configurations	199
5.5.2 Configuring route management.....	199
5.5.3 Checking configurations	200
5.6 Static route	201
5.6.1 Introduction.....	201
5.6.2 Preparing for configurations	201
5.6.3 Configuring static route	201
5.6.4 Checking configurations	202
5.6.5 Example for configuring static route.....	202
5.7 Routing policy.....	204
5.7.1 Configuring IP prefix list	204
5.7.2 Configuring routing table.....	205
5.7.3 Checking configurations	206
5.8 OSPFv2	207
5.8.1 Introduction.....	207
5.8.2 Configuring basic functions of OSPF	212
5.8.3 Configuring OSPF route attributes.....	213
5.8.4 Configuring load balancing	214
5.8.5 Configuring OSPF network	215
5.8.6 Optimizing OSPF network.....	216
5.8.7 Configuring OSPF authentication mode	218
5.8.8 Configuring Stub area	219
5.8.9 Controlling OSPF routing information	220
5.8.10 Configuring OSPF routing policy	222
5.8.11 Checking configurations	225
5.8.12 Maintenance	226
5.9 ISIS.....	226
5.9.1 Configuring ISIS basic functions	226

5.9.2 Configuring ISIS routing	226
5.9.3 Configuring ISIS network	228
5.9.4 Optimizing ISIS network	230
5.9.5 Configuring ISIS authentication	232
5.9.6 Controlling ISIS routing information	233
5.9.7 Configuring ISIS BFD	235
5.9.8 Configuring ISIS GR	235
5.9.9 Checking configurations	236
5.9.10 Maintenance	236
5.10 BGP	236
5.10.1 Configuring BGP basic functions	236
5.10.2 Configuring BGP redistributed routes	237
5.10.3 Configuring BGP routing	239
5.10.4 Configuring BGP network	241
5.10.5 Configuring BGP GR	244
5.10.6 Configuring BFD for BGP	245
5.10.7 Configuring BGP authentication	245
5.10.8 Checking configurations	245
5.10.9 Maintenance	246
5.11 RIP	246
5.11.1 Configuring basic functions of RIP	246
5.11.2 Configuring RIP version	247
5.11.3 Configuring redistribution of external routes	248
5.11.4 Configuring RIP timer	248
5.11.5 Configuring loop suppression	249
5.11.6 Configuring authentication	249
5.11.7 Configuring routing policy	250
5.11.8 Configuring route calculation	250
5.11.9 Checking configurations	251
5.11.10 Maintenance	251
6 PoE	252
6.1 Introduction	252
6.1.1 Principles of PoE	252
6.1.2 PoE modules	253
6.1.3 PoE advantages	253
6.1.4 PoE concepts	253
6.1.5 Smart PoE	254
6.2 Configuring PoE	254
6.2.1 Preparing for configurations	254
6.2.2 Default configurations of PoE	255
6.2.3 Enabling interface PoE	255

6.2.4	Configuring maximum output power of PoE	255
6.2.5	Configuring priority of PoE	256
6.2.6	Configuring PSE power utilization rate threshold	256
6.2.7	Configuring identification of non-standard PDs	256
6.2.8	Enabling forcible power supply on interface	256
6.2.9	Enabling overtemperature protection	257
6.2.10	Enabling global Trap	257
6.2.11	Checking configurations	257
6.3	Configuring Smart PoE	258
6.3.1	Preparing for configurations	258
6.3.2	Default configurations of PoE.....	258
6.3.3	Configuring PoE scheduling profile for interface	259
6.3.4	Configuring linktrace	259
6.3.5	Configuring PD active check	260
6.3.6	Checking configurations	260
6.4	Example for configuring PoE power supply	260
7	DHCP.....	264
7.1	DHCP Client	264
7.1.1	Introduction.....	264
7.1.2	Preparing for configurations	267
7.1.3	Default configurations of DHCP Client	267
7.1.4	Configuring DHCP Client.....	268
7.1.5	Configuring DHCPv6 Client.....	268
7.1.6	Checking configurations	269
7.1.7	Example for configuring DHCP Client	269
7.2	DHCP Snooping	271
7.2.1	Introduction.....	271
7.2.2	Preparing for configurations	272
7.2.3	Default configurations of DHCP Snooping.....	273
7.2.4	Configuring DHCP Snooping	273
7.2.5	Configure DHCP Snooping to support Option 82.....	274
7.2.6	Configuring DHCPv6 Snooping	274
7.2.7	Checking configurations	275
7.2.8	Example for configuring DHCP Snooping.....	275
7.3	DHCP Options.....	277
7.3.1	Introduction.....	277
7.3.2	Preparing for configurations	278
7.3.3	Default configurations of DHCP Option.....	279
7.3.4	Configuring DHCP Option fields.....	279
7.3.5	Configuring DHCP Option 18 over IPv6.....	280
7.3.6	Configuring DHCP Option 37 over IPv6.....	280

7.3.7 Configuring user-defined DHCP Option over IPv6	281
7.3.8 Checking configurations	281
7.4 DHCP Server.....	282
7.4.1 Introduction.....	282
7.4.2 Preparing for configurations	284
7.4.3 Creating and configuring IPv4 address pool	285
7.4.4 Enabling DHCPv4 Server on VLAN interface	285
7.4.5 Enabling DHCP Server on VLAN interface	286
7.4.6 Configuring DHCP Server to support Option 82	286
7.4.7 Checking configurations	286
7.4.8 Example for configuring DHCPv4 Server	287
7.5 DHCP Relay.....	288
7.5.1 Introduction.....	288
7.5.2 Preparing for configurations	289
7.5.3 Default configurations of DHCP Relay.....	289
7.5.4 Configuring global DHCP Relay	289
7.5.5 Configuring DHCP Relay on VLAN interface	290
7.5.6 Configuring DHCP Relay on physical interface or sub-interface	290
7.5.7 (Optional) configuring DHCP Relay to support Option 82.....	290
7.5.8 Checking configurations	291
7.5.9 Example for configuring DHCPv4 Relay	291
8 QoS.....	293
8.1 Introduction.....	293
8.1.1 Service model.....	293
8.1.2 Priority trust	294
8.1.3 Traffic classification.....	294
8.1.4 Traffic policy.....	296
8.1.5 Priority mapping	297
8.1.6 Queue scheduling.....	297
8.1.7 Congestion avoidance	299
8.1.8 Rate limiting based on interface and VLAN	300
8.1.9 Bandwidth rate limiting	300
8.2 Configuring priority	301
8.2.1 Preparing for configurations	301
8.2.2 Default configurations of basic QoS	301
8.2.3 Configuring types of priorities trusted by interface	302
8.2.4 Configuring mapping from CoS to local priority.....	302
8.2.5 Configuring mapping from DSCP to local priority and color	303
8.2.6 Configuring DSCP mutation	303
8.2.7 Configuring CoS remarking.....	304
8.2.8 Checking configurations	304

8.3 Configuring congestion management.....	305
8.3.1 Preparing for configurations	305
8.3.2 Default configurations of congestion management.....	305
8.3.3 Configuring SP queue scheduling	305
8.3.4 Configuring WRR or SP+WRR queue scheduling	305
8.3.5 Configuring DRR or SP+DRR queue scheduling	306
8.3.6 Configuring queue bandwidth guarantee	306
8.3.7 Checking configurations	306
8.4 Configuring congestion avoidance.....	307
8.4.1 Preparing for configurations	307
8.4.2 Default configurations of congestion avoidance	307
8.4.3 Configuring WRED	307
8.4.4 Checking configurations	308
8.5 Configuring traffic classification and traffic policy	308
8.5.1 Preparing for configurations	308
8.5.2 Default configurations of traffic classification and traffic policy	308
8.5.3 Creating traffic classification	309
8.5.4 Configuring traffic classification rules.....	309
8.5.5 Creating rate limit rule and shapping rule.....	310
8.5.6 Creating traffic policy	311
8.5.7 Defining traffic policy mapping	311
8.5.8 Defining traffic policy operation.....	311
8.5.9 Applying traffic policy to interfaces.....	312
8.5.10 Checking configurations	313
8.6 Configuring rate limiting.....	313
8.6.1 Preparing for configurations	313
8.6.2 Configuring rate limiting based on interface.....	314
8.6.3 Checking configurations	314
8.7 Configuring bandwidth rate limiting.....	314
8.7.1 Preparing for configurations	314
8.7.2 Default configurations of bandwidth rate limiting	315
8.7.3 Configuring bandwidth guarantee	315
8.7.4 Configuring hierarchical bandwidth guarantee	316
8.7.5 Checking configurations	318
8.8 Configuring examples	318
8.8.1 Example for configuring congestion management.....	318
8.8.2 Example for configuring rate limiting based on traffic policy	320
8.8.3 Example for configuring rate limiting based on interface	323
9 Multicast	326
9.1 Introduction.....	326
9.2 IGMP.....	331

9.2.1 Introduction.....	331
9.2.2 Preparing for configurations	333
9.2.3 Default configurations of IGMP	333
9.2.4 Enabling IGMP	334
9.2.5 Configuring static group members	334
9.2.6 Configuring interval for sending IGMP Query packets	334
9.2.7 Configuring robustness factor	335
9.2.8 Configuring query interval of last member	335
9.2.9 Configuring maximum response time for querying IGMP packets.....	335
9.2.10 Configuring immediate leave for multicast members	336
9.2.11 Configuring access control for multicast groups and multicast sources.....	336
9.2.12 Checking configurations	336
9.2.13 Maintenance	337
9.3 Basic functions of Layer 2 multicast	337
9.3.1 Introduction.....	337
9.3.2 Preparing for configurations	338
9.3.3 Default configurations of Layer 2 multicast basic functions.....	339
9.3.4 Configuring basic functions of Layer 2 multicast	339
9.3.5 Checking configurations	339
9.3.6 Maintenance	340
9.4 IGMP Snooping.....	340
9.4.1 Introduction.....	340
9.4.2 Preparing for configurations	341
9.4.3 Default configurations of IGMP Snooping	341
9.4.4 Configuring IGMP Snooping	341
9.4.5 Checking configurations	342
9.4.6 Example for applying multicast on ring network.....	343
9.5 IGMP Querier.....	345
9.5.1 Introduction.....	345
9.5.2 Preparing for configurations	346
9.5.3 Default configurations of IGMP Querier	347
9.5.4 Configuring IGMP Querier	347
9.5.5 Checking configurations	348
9.5.6 Example for configuring IGMP Snooping and IGMP Querier.....	348
9.6 IGMP MVR.....	350
9.6.1 Introduction.....	350
9.6.2 Preparing for configurations	351
9.6.3 Default configurations of IGMP MVR	352
9.6.4 Configuring IGMP MVR	352
9.6.5 Checking configurations	353
9.6.6 Example for configuring IGMP MVR	353
9.7 IGMP filtering	355

9.7.1 Introduction.....	355
9.7.2 Preparing for configurations	356
9.7.3 Default configurations of IGMP filtering.....	356
9.7.4 Enabling global IGMP filtering.....	357
9.7.5 Configuring IGMP filter profile.....	357
9.7.6 Configuring maximum number of multicast groups	358
9.7.7 Checking configurations	358
9.7.8 Example for applying IGMP filtering on interface	359
9.8 Multicast VLAN copy	361
9.8.1 Introduction.....	361
9.8.2 Preparing for configurations	363
9.8.3 Default configurations of multicast VLAN copy	363
9.8.4 Configuring multicast VLAN copy.....	364
9.8.5 Configuring static multicast members of VLAN copy.....	364
9.8.6 Configuring customer VLAN of VLAN copy.....	365
9.8.7 Checking configurations	365
9.9 MLD.....	366
9.9.1 Introduction.....	366
9.9.2 Preparing for configurations	366
9.9.3 Default configurations of MLD	366
9.9.4 Configuring basic functions of MLD.....	367
9.9.5 Configuring MLD Snooping.....	367
9.9.6 Configuring MLD Querier	368
9.9.7 Configuring MLD filtering	369
9.9.8 Checking configurations	370
9.9.9 Maintenance.....	371
9.10 PIM-SM	371
9.10.1 Introduction.....	371
9.10.2 Preparing for configurations	372
9.10.3 Default configurations of PIM-SM	373
9.10.4 Configuring dynamic RP	373
9.10.5 Configuring static RP.....	374
9.10.6 Configuring Layer 3 multicast forwarding.....	374
9.10.7 Checking configurations	374
10 Security.....	375
10.1 ACL.....	375
10.1.1 Introduction.....	375
10.1.2 Preparing for configurations	376
10.1.3 Configuring MAC ACL	376
10.1.4 Configuring filter	379
10.1.5 Configuring ACL period	379

10.1.6 Configuring IP address list for SNMP access control	380
10.1.7 Checking configurations	380
10.1.8 Maintenance	380
10.2 Port security MAC	381
10.2.1 Introduction	381
10.2.2 Preparing for configurations	382
10.2.3 Default configurations of port security MAC	382
10.2.4 Configuring basic functions of port security MAC	383
10.2.5 Configuring static secure MAC address	383
10.2.6 Configuring dynamic secure MAC address	384
10.2.7 Configuring sticky secure MAC address	384
10.2.8 Checking configurations	385
10.2.9 Maintenance	385
10.2.10 Example for configuring port security MAC	386
10.3 Dynamic ARP inspection	388
10.3.1 Introduction	388
10.3.2 Preparing for configurations	389
10.3.3 Default configurations of dynamic ARP inspection	389
10.3.4 Configuring trusted interfaces of dynamic ARP inspection	390
10.3.5 Configuring static binding of dynamic ARP inspection	390
10.3.6 Configuring dynamic binding of dynamic ARP inspection	391
10.3.7 Configuring protection VLAN of dynamic ARP inspection	391
10.3.8 Configuring auto-recovery time for rate limiting on ARP packets	391
10.3.9 Checking configurations	391
10.3.10 Example for configuring dynamic ARP inspection	392
10.4 RADIUS	394
10.4.1 Introduction	394
10.4.2 Preparing for configurations	395
10.4.3 Default configurations of RADIUS	395
10.4.4 Configuring RADIUS authentication	396
10.4.5 Configuring RADIUS accounting	396
10.4.6 Checking configurations	397
10.4.7 Example for configuring RADIUS	397
10.5 TACACS+	399
10.5.1 Introduction	399
10.5.2 Preparing for configurations	399
10.5.3 Default configurations of TACACS+	400
10.5.4 Configuring TACACS+ authentication	400
10.5.5 Configuring TACACS+ accounting	400
10.5.6 Configuring TACACS+ authorization	401
10.5.7 Checking configurations	401
10.5.8 Maintenance	401

10.5.9 Example for configuring TACACS+	402
10.6 Storm control	403
10.6.1 Introduction	403
10.6.2 Preparing for configurations	404
10.6.3 Default configurations of storm control	404
10.6.4 Configuring storm control	404
10.6.5 Configuring DLF packet forwarding	405
10.6.6 Checking configurations	406
10.6.7 Example for configuring storm control	406
10.7 802.1x	407
10.7.1 Introduction	407
10.7.2 Preparing for configurations	410
10.7.3 Default configurations of 802.1x	410
10.7.4 Configuring basic functions of 802.1x	410
10.7.5 Configuring 802.1x re-authentication	411
10.7.6 Configuring 802.1x timers	412
10.7.7 Checking configurations	412
10.7.8 Maintenance	413
10.7.9 Example for configuring 802.1x	413
10.8 IP Source Guard	415
10.8.1 Introduction	415
10.8.2 Preparing for configurations	416
10.8.3 Default configurations of IP Source Guard	416
10.8.4 Configuring interface trust status of IP Source Guard	417
10.8.5 Configuring IP Source Guide binding	417
10.8.6 Configuring priority and rate limit of IP packets	418
10.8.7 Checking configurations	418
10.8.8 Example for configuring IP Source Guard	419
10.9 PPPoE+	421
10.9.1 Introduction	421
10.9.2 Preparing for configurations	422
10.9.3 Default configurations of PPPoE+	422
10.9.4 Configuring basic functions of PPPoE+	423
10.9.5 Configuring PPPoE+ packet information	424
10.9.6 Checking configurations	426
10.9.7 Maintenance	426
10.9.8 Example for configuring PPPoE+	426
10.10 Configuring URPF	428
10.10.1 Preparing for configurations	428
10.10.2 Configuring URPF	428
10.11 Configuring CPU protection	429
10.11.1 Preparing for configurations	429

10.11.2 Configuring global CPU CAR	429
10.11.3 Checking configurations	429
10.11.4 Maintenance	429
10.12 Configuring anti-ARP attack	430
10.12.1 Preparing for configurations	430
10.12.2 Configuring ARP	430
10.12.3 Checking configurations	431
11 Reliability	432
11.1 Link aggregation.....	432
11.1.1 Introduction	432
11.1.2 Preparing for configurations.....	433
11.1.3 Configuring manual link aggregation.....	433
11.1.4 Configuring static LACP link aggregation	434
11.1.5 Configuring manual master/slave link aggregation	435
11.1.6 Checking configurations	435
11.1.7 Example for configuring static LACP link aggregation	436
11.2 Link-state tracking.....	438
11.2.1 Introduction	438
11.2.2 Preparing for configurations.....	438
11.2.3 Default configurations of link-state tracking.....	439
11.2.4 Configuring link-state tracking	439
11.2.5 Configuring action taken by link-state group.....	440
11.2.6 Checking configurations	440
11.3 Interface backup	440
11.3.1 Introduction	440
11.3.2 Preparing for configurations.....	442
11.3.3 Default configurations of interface backup	442
11.3.4 Configuring basic functions of interface backup.....	443
11.3.5 (Optional) configuring FS on interfaces.....	444
11.3.6 Checking configurations	444
11.3.7 Example for configuring interface backup	444
11.4 Configuring VRRP	447
11.4.1 Preparing for configurations.....	447
11.4.2 Configuration flow	447
11.4.3 Configuring VRRP backup group	448
11.4.4 (Optional) configuring ping function of VRRP virtual IP address	449
11.4.5 Configuring VRRP monitoring interface	449
11.4.6 Configuring BFD for VRRP	450
11.4.7 Checking configurations	450
11.5 mLACP.....	450
11.5.1 Introduction	450

11.5.2 Preparing for configurations.....	451
11.5.3 Configuring ICCP channel.....	452
11.5.4 Configuring mLACP link aggregation.....	452
11.5.5 Checking configurations.....	453
11.5.6 Maintenance.....	453
11.5.7 Example for configuring mLACP.....	454
12 OAM.....	459
12.1 Introduction.....	459
12.1.1 EFM.....	459
12.1.2 BFD.....	461
12.2 Configuring EFM.....	463
12.2.1 Preparing for configurations.....	463
12.2.2 Configuring basic functions of EFM.....	463
12.2.3 Configuring EFM active function.....	463
12.2.4 Configuring EFM passive function.....	465
12.2.5 Configuring link monitoring and fault indication.....	465
12.2.6 Checking configurations.....	467
12.3 Configuring BFD.....	467
12.3.1 Preparing for configurations.....	467
12.3.2 Configuring BFD session binding.....	468
12.3.3 Configuring BFD session parameters.....	468
12.3.4 Checking configurations.....	469
13 System management.....	470
13.1 SNMP.....	470
13.1.1 Introduction.....	470
13.1.2 Preparing for configurations.....	472
13.1.3 Default configurations of SNMP.....	472
13.1.4 Configuring basic functions of SNMPv1/SNMPv2c.....	473
13.1.5 Configuring basic functions of SNMPv3.....	474
13.1.6 Configuring IP address authentication by SNMP server.....	475
13.1.7 Configuring other information about SNMP.....	475
13.1.8 Configuring Trap.....	476
13.1.9 Checking configurations.....	476
13.1.10 Example for configuring SNMPv1/SNMPv2c and Trap.....	477
13.1.11 Example for configuring SNMPv3 and Trap.....	479
13.2 KeepAlive.....	481
13.2.1 Introduction.....	481
13.2.2 Preparing for configurations.....	482
13.2.3 Default configurations of KeepAlive.....	482
13.2.4 Configuring KeepAlive.....	482
13.2.5 Checking configurations.....	483

13.2.6 Example for configuring KeepAlive	483
13.3 RMON	484
13.3.1 Introduction	484
13.3.2 Preparing for configurations	485
13.3.3 Default configurations of RMON	485
13.3.4 Configuring RMON statistics	486
13.3.5 Configuring RMON historical statistics	486
13.3.6 Configuring RMON alarm group	486
13.3.7 Configuring RMON event group	487
13.3.8 Checking configurations	487
13.3.9 Maintenance	488
13.3.10 Example for configuring RMON alarm group	488
13.4 LLDP	489
13.4.1 Introduction	489
13.4.2 Preparing for configurations	491
13.4.3 Default configurations of LLDP	491
13.4.4 Enabling global LLDP	492
13.4.5 Enabling interface LLDP	492
13.4.6 Configuring basic functions of LLDP	493
13.4.7 Configuring LLDP alarm	493
13.4.8 Configuring TLV	493
13.4.9 Checking configurations	494
13.4.10 Maintenance	494
13.4.11 Example for configuring LLDP	495
13.5 Optical module DDM	498
13.5.1 Introduction	498
13.5.2 Preparing for configurations	498
13.5.3 Default configurations of optical module DDM	498
13.5.4 Enabling optical module DDM	499
13.5.5 Enabling optical module DDM Trap	499
13.5.6 Checking configurations	500
13.6 System log	500
13.6.1 Introduction	500
13.6.2 Preparing for configurations	501
13.6.3 Default configurations of system log	501
13.6.4 Configuring basic information of system log	502
13.6.5 Configuring system log output	503
13.6.6 Checking configurations	504
13.6.7 Maintenance	504
13.6.8 Example for configuring outputting system logs to log host	505
13.7 Alarm management	506
13.7.1 Introduction	506

13.7.2	Preparing for configurations	510
13.7.3	Configuring basic functions of alarm management	511
13.7.4	Checking configurations	512
13.8	Hardware environment monitoring	513
13.8.1	Introduction.....	513
13.8.2	Preparing for configurations	516
13.8.3	Default configurations of hardware environment monitoring	516
13.8.4	Enabling global hardware environment monitoring.....	517
13.8.5	Configuring temperature monitoring alarm	517
13.8.6	Configuring voltage monitoring alarm.....	518
13.8.7	Clearing all hardware environment monitoring alarms manually	518
13.8.8	Checking configurations	518
13.9	CPU monitoring	519
13.9.1	Introduction.....	519
13.9.2	Preparing for configurations	519
13.9.3	Default configurations of CPU monitoring	519
13.9.4	Showing CPU monitoring information	520
13.9.5	Configuring CPU monitoring alarm.....	520
13.9.6	Checking configurations	520
13.10	Cable diagnosis	521
13.10.1	Introduction.....	521
13.10.2	Preparing for configurations	521
13.10.3	Configuring cable diagnosis.....	521
13.10.4	Checking configurations	521
13.11	Memory monitoring	522
13.11.1	Preparing for configurations.....	522
13.11.2	Configuring memory monitoring	522
13.11.3	Checking configurations	522
13.12	Fan monitoring	522
13.12.1	Introduction.....	522
13.12.2	Preparing for configurations	523
13.12.3	Configuring fan monitoring	523
13.12.4	Checking configurations	523
13.13	Performance statistics.....	524
13.13.1	Introduction.....	524
13.13.2	Preparing for configurations	524
13.13.3	Default configurations of performance statistics.....	524
13.13.4	Configuring performance statistics	524
13.13.5	Checking configurations	525
13.13.6	Maintenance.....	525
13.14	Ping	525
13.14.1	Introduction.....	525

13.14.2 Configuring Ping.....	526
13.15 Traceroute.....	526
13.15.1 Introduction.....	526
13.15.2 Configuring Traceroute.....	527
14 Appendix	528
14.1 Terms.....	528
14.2 Acronyms and abbreviations	533

Figures

Figure 1-1 Accessing device through PC connected with RJ45 Console interface	12
Figure 1-2 Configuring communication parameters in Hyper Terminal	13
Figure 1-3 Networking with device as Telnet server	14
Figure 1-4 Networking with device as Telnet client.....	15
Figure 1-5 User management networking	19
Figure 1-6 Basic principles of NTP.....	29
Figure 1-7 NTP networking	35
Figure 2-1 ISF networking	49
Figure 2-2 ISF visualization.....	50
Figure 2-3 ISF merge	51
Figure 2-4 ISF split	52
Figure 2-5 Chain networking	53
Figure 2-6 Ring networking	53
Figure 2-7 ISF relay networking	54
Figure 2-8 Flow for establishing the ISF environment.....	58
Figure 2-9 Multi-ISF-domain networking.....	64
Figure 2-10 BFD MAD networking (without intermediate device).....	69
Figure 2-11 BFD MAD networking (with intermediate device).....	70
Figure 2-12 Clearing MAD fault (clearing ISF link fault)	72
Figure 2-13 Clearing MAD fault (ISF link fault and Active ISF fault).....	73
Figure 2-14 ISF networking (BFD MAD mode).....	75
Figure 2-15 ISF networking with member device changing from ISF mode to standalone mode	78
Figure 2-16 ISF networking (BFD MAD mode).....	81
Figure 2-17 Networking topology before configuring ISF	83
Figure 2-18 Networking topology after adding Switch A to ISF.....	84
Figure 3-1 Forwarding packets according to the MAC address table	89

Figure 3-2 MAC networking.....	94
Figure 3-3 VLAN partition	96
Figure 3-4 VLAN and interface protection networking	103
Figure 3-5 Networking with PVLAN.....	109
Figure 3-6 Sub-VLAN and super VLAN partition.....	113
Figure 3-7 Super VLAN networking.....	115
Figure 3-8 Principles of basic QinQ.....	117
Figure 3-9 Basic QinQ networking	122
Figure 3-10 Selective QinQ networking	123
Figure 3-11 Principles of VLAN mapping	125
Figure 3-12 VLAN mapping networking	127
Figure 3-13 Network storm due to loopback.....	130
Figure 3-14 Loop networking with STP.....	131
Figure 3-15 VLAN packet forward failure due to RSTP	132
Figure 3-16 STP networking	135
Figure 3-17 Basic concepts of the MSTI network.....	139
Figure 3-18 MSTI concepts.....	140
Figure 3-19 Networking with multiple spanning trees instances in MST domain	141
Figure 3-20 MSTP networking.....	152
Figure 3-21 Configuring MRSTP for specifying root bridge	156
Figure 3-22 Loop detection networking	159
Figure 3-23 Loop detection networking	163
Figure 3-24 Interface protection networking.....	166
Figure 3-25 Principles of port mirroring	167
Figure 3-26 Port mirroring networking	170
Figure 3-27 L2CP networking.....	174
Figure 3-28 Networking for IP phone to connect to switch	177
Figure 5-1 VLAN interface networking	189
Figure 5-2 Configuring ARP networking	195
Figure 5-3 Principles of NDP address resolution	196
Figure 5-4 Static route networking.....	203
Figure 5-5 Roles of broadcast interface.....	208
Figure 5-6 OSPF area and router type.....	211

Figure 6-1 Principles of PoE	253
Figure 6-2 PD Active check	258
Figure 6-3 PoE switch power supply networking	261
Figure 7-1 DHCP typical networking.....	265
Figure 7-2 Structure of a DHCP packet	265
Figure 7-3 DHCP Client networking.....	267
Figure 7-4 DHCP Client networking.....	270
Figure 7-5 DHCP Snooping	272
Figure 7-6 DHCP Snooping networking	276
Figure 7-7 DHCP Server and Client networking.....	283
Figure 7-8 Structure of a DHCP packet	283
Figure 7-9 DHCP Server networking	287
Figure 7-10 Typical application of DHCP Relay.....	288
Figure 7-11 DHCP Relay networking	292
Figure 8-1 Traffic classification	295
Figure 8-2 Structure of IP packet header.....	295
Figure 8-3 Structures of ToS priority and DSCP priority	295
Figure 8-4 Structure of a VLAN packet	296
Figure 8-5 Structure of CoS priority	296
Figure 8-6 SP scheduling	298
Figure 8-7 WRR scheduling.....	298
Figure 8-8 DRR scheduling.....	299
Figure 8-9 Queue scheduling networking	318
Figure 8-10 Rate limiting based on traffic policy.....	321
Figure 8-11 Rate limiting based on interface	324
Figure 9-1 Multicast transmission networking.....	327
Figure 9-2 Basic concepts in multicast.....	329
Figure 9-3 Mapping between IPv4 multicast address and multicast MAC address	330
Figure 9-4 Operating of IGMP and Layer 2 multicast features	330
Figure 9-5 Principles of IGMP	332
Figure 9-6 IGMP Snooping networking.....	341
Figure 9-7 Ring network multicast networking.....	343
Figure 9-8 IGMP Snooping networking.....	349

Figure 9-9 IGMP MVR networking	351
Figure 9-10 MVR networking	354
Figure 9-11 Applying IGMP filtering on interface	359
Figure 9-12 Data transmission of IGMP MVR	362
Figure 9-13 Data transmission of multicast VLAN copy	362
Figure 9-14 Multicast VLAN copy networking	363
Figure 9-15 PIM-SM networking	372
Figure 10-1 Port security MAC networking	386
Figure 10-2 Principles of dynamic ARP inspection	389
Figure 10-3 Configuring dynamic ARP inspection	392
Figure 10-4 RADIUS networking	398
Figure 10-5 TACACS+ networking	402
Figure 10-6 Storm control networking	406
Figure 10-7 802.1x structure	408
Figure 10-8 Dot1x networking	413
Figure 10-9 Principles of IP Source Guard	416
Figure 10-10 Configuring IP Source Guard	419
Figure 10-11 Accessing the network through PPPoE authentication	421
Figure 10-12 PPPoE+ networking	426
Figure 11-1 Static LACP mode link aggregation networking	436
Figure 11-2 Principles of interface backup	441
Figure 11-3 Networking with interface backup in different VLANs	442
Figure 11-4 Interface backup networking	445
Figure 11-5 VRRP configuration flow	448
Figure 11-6 Dual-homed application based on LACP	451
Figure 11-7 mLACP networking	454
Figure 12-1 OAM loopback	460
Figure 13-1 Principles of SNMP	471
Figure 13-2 Principles of SNMPv3 authentication	474
Figure 13-3 SNMPv1/SNMPv2c networking	477
Figure 13-4 SNMPv3 and Trap networking	479
Figure 13-5 KeepAlive networking	483
Figure 13-6 RMON networking	485

Figure 13-7 RMON networking	488
Figure 13-8 Structure of a LLDPDU	490
Figure 13-9 Structure of a TLV packet	490
Figure 13-10 LLDP networking	495
Figure 13-11 Networking of outputting system log to log host	505
Figure 13-12 Principles of Ping	526
Figure 13-13 Principles of Traceroute	527

Tables

Table 1-1 Shortcut keys for display features	9
Table 3-1 Interface mode and packet processing.....	96
Table 7-1 Fields of a DHCP packet.....	265
Table 7-2 Common DHCP options.....	277
Table 7-3 Fields of a DHCP packet.....	283
Table 8-1 Mapping between local priority and DSCP priority	297
Table 8-2 Mapping between local priority and queue	297
Table 8-3 Default mapping from CoS to local priority	301
Table 8-4 Default mapping from DSCP to local priority.....	302
Table 8-5 Default mapping from ToS to local priority and color	302
Table 13-1 TLV types	490
Table 13-2 Log levels.....	500
Table 13-3 Alarm fields	507
Table 13-4 Alarm levels.....	508
Table 13-5 Trap information	515
Table 13-6 Syslog information	515

1 Basic configurations

This chapter describes basic configurations and configuration procedures of the ISCOM3000G 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 ISCOM3000G series switch. You can configure, monitor, and manage the ISCOM3000G series switch through the CLI.

You can log in to the ISCOM3000G 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:

- Configure the ISCOM3000G series switch locally through the Console interface.
- Configure the ISCOM3000G series switch locally or remotely through Telnet/Secure Shell v2 (SSHv2).
- Commands are classified into different levels. You can execute the commands that correspond to your level only.

- The commands available to you depend on which mode you are currently in.
- Shortcut keys can be used to execute commands.
- Check or execute a history command by checking command history. The last 20 history commands can be saved on the ISCOM3000G series switch.
- Enter a question mark (?) at the system prompt to obtain online help.
- Support multiple intelligent analysis methods, such as fuzzy match and context association.

1.1.2 Privileges

The ISCOM3000G series switch uses hierarchical protection methods to divide commands into 16 privileges in an ascending order.

- Privileges 0–4: viewing privilege. Users can execute viewing commands, such as the **ping**, **clear**, and **history** commands.
- Privileges 5–10: monitoring privilege. Users can execute monitoring commands, such as the **show** command.
- Privileges 11–14: configuring privilege. Users can execute commands for configuring different services, such as Virtual Local Area Network (VLAN) and Internet Protocol (IP).
- Privilege 15: administering privilege. 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.

If the ISCOM3000G series switch is in default configuration, a "login" prompt will appear. After you enter the user name raisecom and password raisecom, it will enter user EXEC mode, and the screen will display:

```
Raisecom>
```



Users under privilege 11 do not need to enter the password when entering privileged EXEC mode.

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

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



- Command line prompt "Raisecom" is the default host name. You can use the **hostname** *string* command to modify the host name 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 previous command mode.
- You can use the **end** command to return to privileged EXEC mode from any modes except user EXEC mode and privileged EXEC mode.

The ISCOM3000G series switch supports the following command line modes:

Mode	Enter method	Description
Privileged EXEC	After login, enter the user name and password at the "login" prompt.	Raisecom#
Global configuration	In privileged EXEC mode, use the config terminal command.	Raisecom(config)#
Physical layer interface configuration	In global configuration mode, use the interface { gigaethernet tengigethernet } unit/slot/interface command.	Raisecom(config-gigaethernet1/1/interface)# Raisecom(config-tengigaethernet1/1/interface)#
Physical interface batch configuration	In global configuration mode, use the interface range { gigaethernet tengigethernet } unit/slot/interface command.	Raisecom(config-range)#
Layer 3 physical interface configuration	In global configuration mode, use the interface { tengigabitethernet fortygigabitethernet } unit/slot/interface command.	Raisecom(config-tengigabitethernet1/1/interface)# Raisecom(config-fortygigabitethernet1/1/interface)#
Sub-interface configuration	In global configuration mode, use the interface ethernet unit/slot/port.sub-interface command.	Raisecom(config-tengigabitethernet1/1/port.sub-interface)# Raisecom(config-fortygigabitethernet1/1/port.sub-interface)#
SNMP interface configuration	In global configuration mode, use the interface fastethernet 1/0/1 command.	Raisecom(config-subif)#
Tunnel interface configuration	In global configuration mode, use the interface tunnel tunnel-id command.	Raisecom(config-tunnel)#

Mode	Enter method	Description
Loopback interface configuration	In global configuration mode, use the interface loopback <i>lb-number</i> command.	Raisecom(config-loopback)#
VLAN configuration	In global configuration mode, use the vlan <i>vlan-id</i> command.	Raisecom(config-vlan)#
Aggregation group configuration	In global configuration mode, use the interface port-channel <i>channel-number</i> command.	Raisecom(config-port-channel)#
Traffic classification configuration	In global configuration mode, use the class-map <i>class-map-name</i> command.	Raisecom(config-cmap)#
Traffic policy configuration	In global configuration mode, use the policy-map <i>policy-map-name</i> command.	Raisecom(config-pmap)#
Traffic policy configuration binding with traffic classification	In floe policy configuration mode, use the class-map <i>class-map-name</i> command.	Raisecom(config-pmap-c)#
Basic IP ACL configuration	In global configuration mode, use the access-list <i>acl-number</i> command. Wherein, <i>acl-number</i> ranges from 1000 to 1999.	Raisecom(config-acl-ipv4-std)#
Extended IP ACL configuration	In global configuration mode, use the access-list <i>acl-number</i> command. Wherein, <i>acl-number</i> ranges from 2000 to 2999.	Raisecom(config-acl-ipv4-ext)#
MAC ACL configuration	In global configuration mode, use the access-list <i>acl-number</i> command. Wherein, <i>acl-number</i> ranges from 3000 to 3999.	Raisecom(config-acl-mac)#
User ACL configuration	In global configuration mode, use the access-list <i>acl-number</i> command. Wherein, <i>acl-number</i> ranges from 5000 to 5999.	Raisecom(config-acl-udf)#
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 <i>profile-number</i> command.	Raisecom(config-igmp-profile)#
cos-remark configuration	In global configuration mode, use the mls qos mapping cos-remark <i>profile-id</i> command.	Raisecom(cos-remark)#

Mode	Enter method	Description
cos-to-pri configuration	In global configuration mode, use the mls qos mapping cos-to-local-priority <i>profile-id</i> command.	Raisecom(cos-to-pri)#
dscp-mutation configuration	In global configuration mode, use the mls qos mapping dscp-mutation <i>profile-id</i> command.	Raisecom(dscp-mutation)#
dscp-to-pri configuration	In global configuration mode, use the mls qos mapping dscp-to-local-priority <i>profile-id</i> command.	Raisecom(dscp-to-pri)#
WRED profile configuration	In global configuration mode, use the mls qos wred profile <i>profile-id</i> command.	Raisecom(wred)#
CMAP configuration	In global configuration mode, enter the class-map <i>class-map-name</i> command.	Raisecom(config-cmap)#
Traffic monitoring profile configuration	In global configuration mode, enter the mls qos policer-profile <i>policer-name</i> [single] command.	Raisecom(traffic-policer)#
PMAP configuration	In global configuration mode, enter the policy-map <i>policy-map-name</i> command.	Raisecom(config-pmap)#
Traffic policy bound with traffic classification configuration	In PMAP configuration mode, enter the class-map <i>class-map-name</i> command.	Raisecom(config-pmap-c)#
Stack interface configuration	In global configuration mode, use the interface isf-port <i>interface-number</i> command.	Raisecom(config-isf-port3/1/1)
Chinese prompt	In any configuration mode, use the language chinese command.	Raisecom#
English prompt	In any configuration mode, use the language english command.	Raisecom#

1.1.4 Shortcut keys

The ISCOM3000G series switch supports the following shortcut keys.

Shortcut key	Description
Up Arrow (↑)	Show the previous command if there is any command entered earlier; the display has no change if the current command is the earliest one in history records.

Shortcut key	Description
Down Arrow (↓)	Show the next command if there is any newer command. The display does not change if the current command is the newest one in history records.
Left Arrow (←)	Move the cursor leftward by one character. The display does not change if the cursor is already at the beginning of the command.
Right Arrow (→)	Move the cursor rightward by one character. The display does not change if the cursor is already at the end of the command.
Backspace	Delete the character before the cursor. The display does not change if the cursor is already at the beginning of the command.
Tab	<p>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 entering keywords.</p> <p>Press Tab after entering an incomplete keyword, and the system automatically executes partial helps:</p> <ul style="list-style-type: none"> • 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 tracert .
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.
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).

Shortcut key	Description
Ctrl+Y	Show history commands.
Ctrl+Z	Return to privileged EXEC mode from the current mode (except user EXEC 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 view a list of commands and brief descriptions available for each command mode.

```
Raisecom>?
```

The command output is as below.

```
clear      Clear screen
enable     Turn on privileged mode command
exit       Exit current mode and down to previous mode
help       Message about help
history    Most recent history command
language   Language of help message
list       List command
quit       Exit current mode and down to previous mode
terminal   Configure terminal
```

- 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 ?
```

The command output is as below.

```
peer          Configure NTP peer
refclock-master set local clock as reference clock
```

server Configure NTP server

- 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.

```
<1-4094> vlan interface 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.

```
cache                    Cache information
class-map                Set class map
clear                    Clear screen
command-log              Log the command to the file
cpu                      Configure cpu parameters
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.

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

The command output is as below.

```
link-aggregation        Link aggregation
link-state-tracking      Link state tracking
```


- 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 ISCOM3000G 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 with "^" is invalid.
Ambiguous input in the position marked by '^'	The keyword marked with "^" 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.

Filtering displayed information

The ISCOM3000G 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 ISCOM3000G series switch supports three kinds of filter modes:

- | **begin string**: show all lines starting from the assigned string.
- | **exclude string**: show all lines mismatch with the assigned string.
- | **include string**: show all lines only match with the assigned string.

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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# terminal page-break enable	Enable 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.

Configure the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# terminal history number	(Optional) configure the number of history commands saved in the system.
2	Raisecom# terminal time-out period	(Optional) configure the Console terminal timeout period.
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 the **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 a feature while the **disable** parameter is used to disable the feature.

For example:

- In physical layer interface configuration mode, the **description** *text* command is used to modify descriptions of an interface while the **no description** command is used to delete descriptions of the interface and restore to the default values.
- In physical layer interface configuration mode, the **shutdown** command is used to shut down an interface while the **no shutdown** command is used to restart the 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.



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

1.1.9 Logging command lines

Configure the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#command-log enable</code> <code>Raisecom(config)#exit</code>	Enable command line logging.

1.2 Accessing device

1.2.1 Introduction

The ISCOM3000G series switch can be configured and managed in Command Line Interface (CLI) mode or NView NNM network management mode.

The ISCOM3000G 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 conduct remote Telnet configuration.
- SSH mode: before accessing the ISCOM3000G series switch through SSH, you need to log in to the ISCOM3000G series switch and start the SSH service through the Console interface.

When configuring the ISCOM3000G series switch in network management mode, you must first configure the IP address of the VLAN interface on CLI, and then configure the ISCOM3000G series switch through NView NNM system.

1.2.2 Accessing through Console interface

Introduction

The Console interface is an interface which is commonly used to connect the network device with a PC running the terminal emulation program. You can use this interface to configure and manage local devices. This management method can communicate directly without a network, so it is called out-of-band management. You can also configure and manage the ISCOM3000G series switch through the Console interface when the network fails.

In the following two conditions, you can only log in to the ISCOM3000G series switch and configure it through the Console interface:

- The ISCOM3000G series switch is powered on to start for the first time.
- Accessing the ISCOM3000G series switch through Telnet fails.

Accessing device from RJ45 Console interface

If you wish to access the ISCOM3000G series switch through PC through RJ45 Console interface, connect Console interface and PC RS-232 serial port, as shown in Figure 1-1; then run the terminal emulation program, such as Windows XP Hyper Terminal on a PC, to configure communication parameters as shown in Figure 1-2, and then log in to the ISCOM3000G series switch.

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

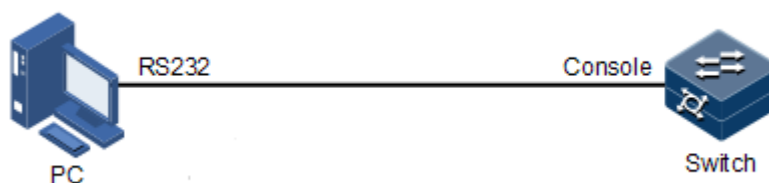
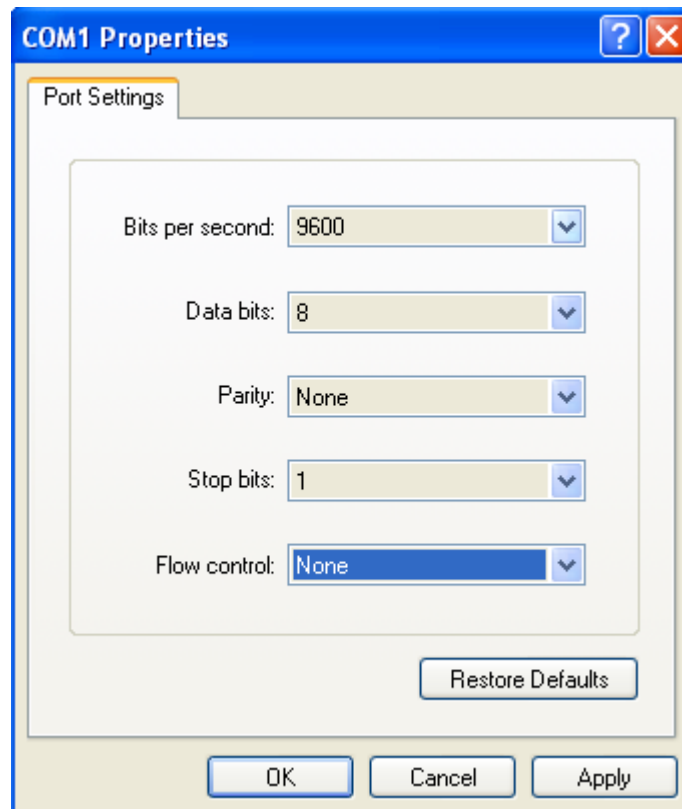


Figure 1-2 Configuring communication parameters in Hyper Terminal



 **Note**

By default, the baud rate is 9600 baud.

Configure the ISCOM3000G series switch as below.

Step	Command	Description
1	<pre>Raisecom#config Raisecom(config)#console baud-rate { 115200 19200 38400 9600 }</pre>	Modify the baud rate for login from the Console interface.

1.2.3 Accessing through Telnet

 **Note**

By default, the management IP address of the out-of-band management interface (SNMP interface: fasterethernet 1/0/1) on the ISCOM3000G series switch is 192.168.0.1, and the subnet mask is 255.255.255.0. To modify the management IP address, you can log in to the ISCOM3000G series switch from the Console interface, and configure it. Both the default user name and password for the ISCOM3000G series switch are raisecom.

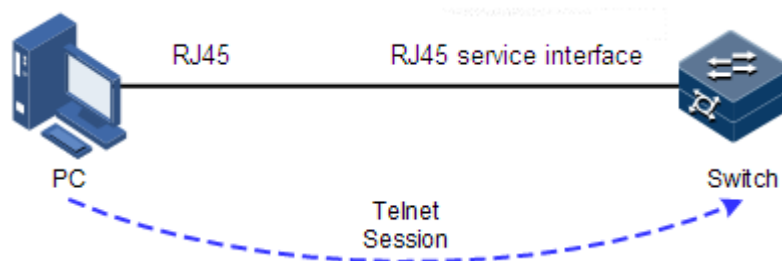
You can use a PC to log in to the ISCOM3000G series switch remotely through Telnet. You can log in to an ISCOM3000G series switch from a PC, and then Telnet another

ISCOM3000G series switch on the network. You do not need to connect a PC to each ISCOM3000G series switch.

Telnet services provided by the ISCOM3000G series switch are as below:

- Telnet Server: run the Telnet Client program on a PC to log in to the ISCOM3000G series switch, and conduct configuration and management. As shown in Figure 1-3, ISCOM3000G series switch is providing Telnet Server service at this time.

Figure 1-3 Networking with device as Telnet server



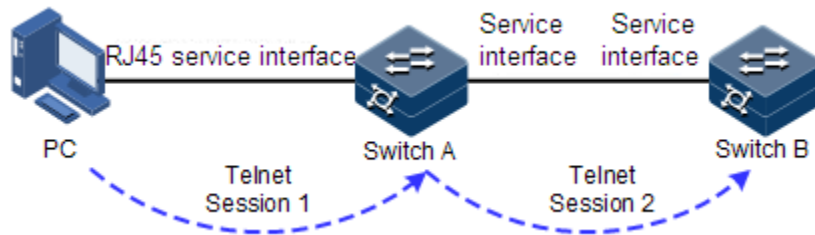
Before accessing the ISCOM3000G series switch through Telnet, you need to log in to the ISCOM3000G series switch through the Console interface and start the Telnet service. Configure the Telnet service for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface fastethernet 1/0/1</code>	Enter out-of-band network management interface configuration mode
3	<code>Raisecom(config-fastethernet 1/0/1)#ip address ip-address [ip-mask]</code> <code>Raisecom(config-fastethernet1/0/1)#exit</code>	Configure the IP address for the out-of-band network management interface. By default, it is 198.168.0.1/24. Both the default user name and password for the ISCOM3000G series switch are raisecom.
4	<code>Raisecom(config-fastethernet 1/0/1)#shutdown</code>	(Optional) shut down the out-of-band management interface.
5	<code>Raisecom(config)#telnet-server accept interface-type interface-list</code>	(Optional) configure the Telnet-supportive interface.
6	<code>Raisecom(config)#telnet-server close terminal-telnet session-number</code>	(Optional) release the specified Telnet session.
7	<code>Raisecom(config)#telnet-server max-session session-number</code>	(Optional) configure the maximum number of Telnet sessions supported by the ISCOM3000G series switch. By default, it is 10.

- Telnet Client: when you connect to the ISCOM3000G series switch through the terminal emulation program or Telnet client program on a PC, then telnet another ISCOM3000G

series switch and configure/manage them. As shown in Figure 1-4, Switch A not only works as Telnet server but also provides the Telnet Client service.

Figure 1-4 Networking with device as Telnet client



Configure Telnet Client as below.

Step	Command	Description
1	<code>Raisecom#telnet { ip-address ipv6-address } [port port-id]</code>	Log in to another device through Telnet.

1.2.4 Accessing through SSH

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

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

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

Before accessing the ISCOM3000G series switch through SSHv2, you must log in to the ISCOM3000G series switch through the Console interface and start SSH service.


Default configurations for accessing the ISCOM3000G series switch through SSHv2 are as follows.

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
Number of SSHv2 authentication failures allowed by the device	20

Function	Default value
SSH snooping port number	22
SSH session status	Disable
SSH protocol version	v2

Configure SSH service for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#generate ssh-key length</code>	Generate local SSHv2 key pair and designate its length. By default, it is 512 bits.
3	<code>Raisecom(config)#ssh2 server</code>	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	<code>Raisecom(config)#ssh2 server authentication { password rsa-key }</code>	(Optional) configure SSHv2 authentication mode. By default, it is password.
5	<code>Raisecom(config)#ssh2 server authentication public-key public key</code>	(Optional) record the public key of the client on the ISCOM3000G series switch in rsa-key authentication mode.
6	<code>Raisecom(config)#ssh2 server authentication-timeout period</code>	(Optional) configure the SSHv2 authentication timeout. The ISCOM3000G 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.
7	<code>Raisecom(config)#ssh2 server authentication-retries times</code>	(Optional) configure the allowable failure times for SSHv2 authentication. The ISCOM3000G 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.

Step	Command	Description
8	<code>Raisecom(config)#ssh2 server port <i>port-number</i></code>	(Optional) configure SSHv2 snooping port number. By default, it is 22.  Note When configuring SSHv2 snooping port number, the entered parameter cannot take effect until SSH is restarted.
9	<code>Raisecom(config)#ssh2 server max-session <i>session-number</i></code>	(Optional) configure the maximum number of SSHv2 sessions.
10	<code>Raisecom(config)#ssh2 access-list { <i>ip access-list number</i> <i>ipv6 access-list number</i> }</code>	(Optional) configure the ACL number.
11	<code>Raisecom(config)#ssh2 server rekey-interval <i>value</i></code>	(Optional) configure the SSH renegotiation period.
12	<code>Raisecom(config)#ssh2 server close session <i>session-number</i></code>	(Optional) close the specified SSHv2 session.

1.2.5 Managing users

When you start the ISCOM3000G series switch for the first time, connect the PC to the ISCOM3000G series switch through the Console interface, enter the initial user name and password in HyperTerminal to log in to and configure the ISCOM3000G series switch.



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

If there is no privilege restriction, any remote user can log in to the ISCOM3000G series switch through Telnet or access network by establishing a PPP (Point to Point Protocol) connection when service interfaces are configured with IP addresses. This is insecure to the ISCOM3000G series switch and network. Creating users for the ISCOM3000G series switch and configuring password and privilege help manage login users and ensures network and device security.

Default configurations of user management are as below.

Function	Default value
Local user information	<ul style="list-style-type: none"> • User name: raisecom • Password: raisecom • Privilege: 15
New user privilege	15
New user activation status	Activate

Function	Default value
New user service type	N/A
Enable password	raisecom
User login authentication mode	local-user
Enable login authentication mode	local-user

Configure login user management for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# user name <i>user-name</i> password [cipher simple] <i>password</i>	Create or modify the user name and password.
2	Raisecom# user name <i>user-name</i> privilege <i>privilege-level</i>	Configure the privilege of the login user.
3	Raisecom# user <i>user-name</i> { allow-exec disallow-exec } <i>first-keyword</i> [<i>second-keyword</i>]	(Optional) configure the priority rule for login user to perform the command line.
4	Raisecom# user <i>user-name</i> service-type { lan-access ssh telnet web console all }	(Optional) configure the service type supported by the user.
5	Raisecom# user login { local-radius local-user radius-local radius-user local-tacacs tacacs-local tacacs-user }	(Optional) configure authentication mode for user login.
6	Raisecom# enable password [cipher <i>password</i>]	(Optional) modify the password for entering privileged EXEC mode. Users under privilege 11 do not need to enter the password when entering privileged EXEC mode.
7	Raisecom# password check { complex simple }	(Optional) configure the strength of password check. By default, it is complex; in other words, the password must contain uppercase letters, lowercase letters, and digits.
8	Raisecom# logout	(Optional) log out.



Note

- Besides the default user raisecom, you can create up to 9 local users.
- The login password is 8–16 characters, mandatorily including digits, uppercase letter, and lowercase letters.

- A local user under level 15 is not allowed to modify the login password unless specially authorized.

1.2.6 Checking configurations

Use the following commands to check the configuration results.

No.	Command	Description
1	<code>Raisecom#show user table</code>	Show login user information.
2	<code>Raisecom#show user active</code>	Show information about users logged in to the ISCOM3000G series switch.
3	<code>Raisecom#show telnet-server</code>	Show configurations of the Telnet server.
4	<code>Raisecom#show ssh public-key [authentication]</code>	Show the public key used for SSH authentication on the ISCOM3000G series switch and client.
5	<code>Raisecom#show ssh2 { server session }</code>	Show SSHv2 server or session information.

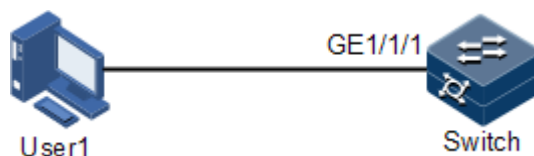
1.2.7 Example for configuring user management

Networking requirements

As shown in Figure 1-5, to prevent malicious users from logging in to the ISCOM3000G series switch and to eliminate risks on the ISCOM3000G series switch, configure user management as below:

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

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 user's service type.

```
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
User Login :local-user
Enable Login:local-user

Username:raisecom
Priority:15
Server:Local
Login :console
Status :online
Service type:console telnet ssh web lan-access
User State :active

Username:user1
Priority:10
Server:Local
Login :--
Status :offline
Service type:console telnet ssh web lan-access
User State :active
User command control config:
-----
Type:allow
First keyword :minrpor
```

Use the newly-created user name user1 and password aaAA123@ to log in to the ISCOM3000G 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.
  
```

1.3 File management

1.3.1 Managing BootROM files

When the system prompts "Press Ctrl+b or Ctrl+B to enter boot menu:", press **Ctrl+B** to enter Bootrom command mode.

In Boot mode, you can do the following operations.

Operation	Description
t	Update system software to the ISCOM3000G series switch.
m	Update the boot file to the ISCOM3000G series switch.
b	Read system software from the ISCOM3000G series switch, and load it.
s	Specify the sequence of system software to be loaded upon startup.
e	Clear environment variables.
r	Restart the ISCOM3000G series switch.
p	Configure the BootROM password.
?/h	Show information about system files and help.

Configure the ISCOM3000G series switch as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Raisecom#upload bootstrap { ftp ip-address user-name password file-name tftp ip-address file-name sftp ip-address user-name password file-name } [dir]	(Optional) download the BootROM file through FTP or TFTP from the device to a local disk.
2	Raisecom#erase [file-name]	(Optional) delete files saved in the Flash.

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 ISCOM3000G 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 ISCOM3000G series switch supports dual-system. There are 2 independent sets of system software saved at the memory. When the ISCOM3000G series switch fails to work due to upgrade failure, you can use the other set to boot the ISCOM3000G series switch.

Manage system files for the ISCOM3000G series switch as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Raisecom# download system-boot { ftp ip-address user-name password file-name tftp ip-address file-name sftp ip-address user-name password file-name } { system1.z system2.z }	(Optional) download the system boot file through FTP or TFTP.
2	Raisecom# erase [<i>file-name</i>]	(Optional) delete files saved in the Flash.
3	Raisecom# upload system-boot { ftp ip-address user-name password file-name tftp ip-address file-name sftp ip-address user-name password file-name } { system1.z system2.z }	(Optional) upload the system boot file through FTP or TFTP.

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 ISCOM3000G 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 as Mode+Command format.
- Just keep the non-default parameters to save space (see the command reference manual for default values of configuration parameters).
- 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 ISCOM3000G 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 ISCOM3000G series switch uses the default parameters for initialization.

The configuration that is currently used by the ISCOM3000G series switch is called the running configuration.

You can modify the running configuration of ISCOM3000G 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# download startup-config { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> sftp <i>ip-address user-name password file-name</i> } } [<i>dir</i>]	(Optional) download the startup configuration file through FTP or TFTP.
2	Raisecom# download backup-config { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> sftp <i>ip-address user-name password file-name</i> } } [<i>dir</i>]	(Optional) download the backup configuration file through FTP or TFTP.
3	Raisecom# erase [<i>file-name</i>]	(Optional) delete files saved in the Flash.
4	Raisecom# upload startup-config { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> sftp <i>ip-address user-name password file-name</i> } } [<i>dir</i>]	(Optional) upload the startup configuration file through FTP or TFTP.
5	Raisecom# upload backup-config { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> sftp <i>ip-address user-name password file-name</i> } } [<i>dir</i>]	(Optional) upload the backup configuration file through FTP or TFTP.
6	Raisecom# upload command-log { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> sftp <i>ip-address user-name password file-name</i> } } [<i>dir</i>]	(Optional) upload the command line logging file and system logs through FTP or TFTP.
7	Raisecom# upload logging-file { ftp <i>ip-address user-name password file-name</i> tftp <i>ip-address file-name</i> sftp <i>ip-address user-name password file-name</i> } } [<i>dir</i>]	(Optional) upload the system log file through FTP or TFTP.
8	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.

No.	Command	Description
2	Raisecom# show running-config	Show the running configurations.

1.3.5 Maintenance

Maintain the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# write [backup-config]	Write the running configuration file to the Flash, and save it as a startup configuration file which can take effect upon next startup.  Caution When you save the running configuration file as a startup configuration file in the Flash, the startup file will overwrite the original one; therefore back up the original one in advance.
2	Raisecom# dir	Show names of system files.
3	Raisecom# erase [<i>file-name</i> backup-config]	Delete a specified system file. If the file-name parameter is not configured, this configuration will delete the startup configuration file.  Caution After a file is deleted through this command, it cannot be restored. Use this command with caution.

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 ISCOM3000G 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 ISCOM3000G 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 ISCOM3000G 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 ISCOM3000G series switch confirms the name according to naming conventions and its attributes (device type, MAC address, software version, and so on).

Upgrade

The ISCOM3000G series switch needs to be upgraded if you wish to add new features, optimize functions, or fix bugs in the current software version.

The ISCOM3000G series switch supports the following two upgrade modes:

- Upgrade through BootROM
- Upgrade through CLI

1.4.2 Upgrading system software through BootROM

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

- The device is started for the first time.
- 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 ISCOM3000G 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 ISCOM3000G series switch.
- Connect the Ethernet interface on the FTP server to the SNMP interface on the ISCOM3000G series switch. The default IP address of the SNMP interface is 192.168.0.1 by default.

Upgrade system software through BootROM for the ISCOM3000G series switch as below.

Step	Operation
1	Log in to the ISCOM3000G series switch through serial interface as the administrator, enter Privileged EXEC mode, and restart the ISCOM3000G series switch with the reboot command. Ra ise com#reboot

Step	Operation
2	<p>When the system prompts "Press Ctrl+b or Ctrl+B to enter boot menu:", press Ctrl+B to enter Bootrom command mode. The command list is displayed as below:</p> <pre style="text-align: center;"> 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]: </pre>
3	<p>Type "t" to upgrade system software to the ISCOM3000G series switch.</p> <pre> [Raisecom]:t ipaddr: 192.168.5.100 serverip: 192.168.5.1 filename: uImage Current system partiton info: Partition number Name Size ----- 1 ISCOM3000_image 16320072 2 None 0 Please input system partition number for upgrading(1-2):1 </pre>
4	<p>Type "m" to upgrade the Boot software to the ISCOM3000G series switch.</p> <pre> [Raisecom]:m ipaddr: 192.168.5.100 serverip: 192.168.5.1 filename: uImage mboot.bin press y to confirm: y </pre>
5	<p>Type "r" to rapidly execute the big BootROM file. The ISCOM3000G series switch is restarted and will load the downloaded startup file.</p>

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 ISCOM3000G series switch as the client. Basic requirements are as below.

- Connect the Ethernet interface on the TFTP server to the SNMP interface on the ISCOM3000G 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 ISCOM3000G series switch so that the ISCOM3000G series switch can access the TFTP server.

Upgrade system software through CLI for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# download system-boot { ftp { <i>ipv4-address</i> / <i>ipv6-address</i> } <i>user-name password file-name</i> tftp { <i>ipv4-address</i> / <i>ipv6-address</i> } <i>file-name</i> sftp { <i>ipv4-address</i> / <i>ipv6-address</i> } <i>user-name password file-name</i> } [system1.z system2.z]	Download the system boot file through FTP, SFTP, or TFTP. Support the IPv6 address.
2	Raisecom# boot sequence	(Optional) configure the sequence for loading system software.
3	Raisecom# reboot [now]	Restart the ISCOM3000G series switch, and it will automatically load the downloaded system boot file.

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

To ensure precise system time, the ISCOM3000G 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).

The ISCOM3000G 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 ISCOM3000G series switch.

DST

DST is an 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 ISCOM3000G 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 1-6 shows basic principles of NTP. Clock synchronization works as below:

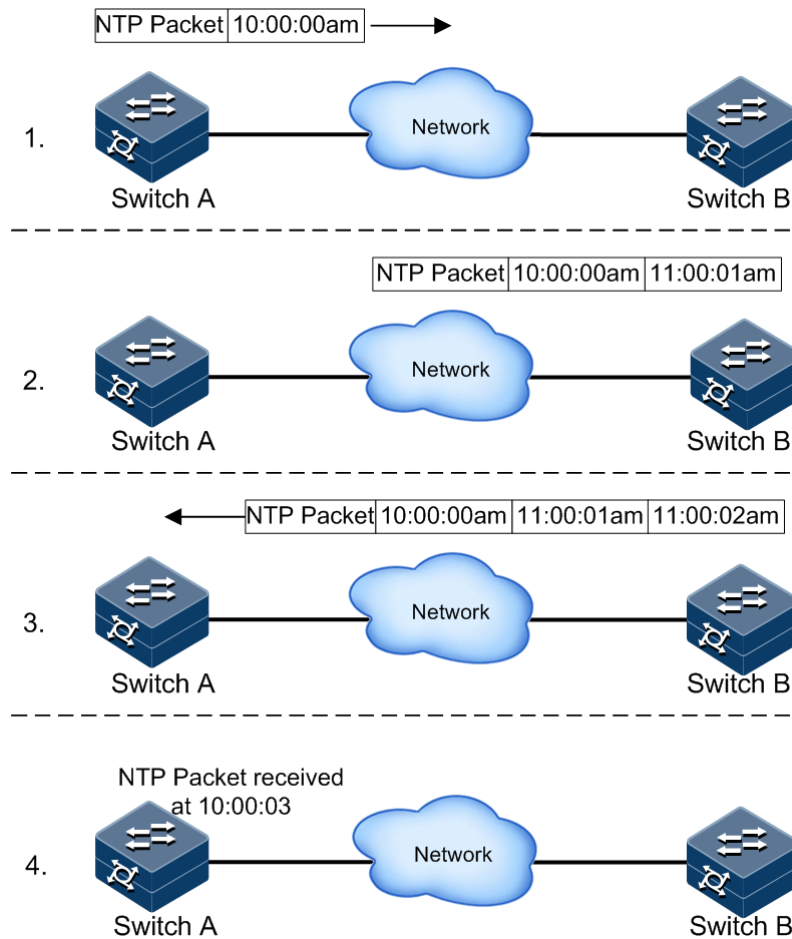
- Step 1 Switch A sends Switch B a NTP message which carries the timestamp of leaving Switch A. The timestamp is 10:00:00am and recorded as t1.
- Step 2 When the message reaches Switch B, it is added with the timestamp of reaching Switch B, which is 11:00:01am and recorded as t2.
- Step 3 When the message 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: $\text{delay} = (t4 - t1) - (t3 - t2)$
- Time offset between Switch A and Switch B: $\text{offset} = ((t2 - t1) + (t3 - t4))/2$

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

Figure 1-6 Basic principles of NTP



The ISCOM3000G series switch adopts multiple NTP working modes for time synchronization:

- Server/Client 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 ISCOM3000G series switch can work as a client or server.

- Symmetric peer mode

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

SNTP

Simple Network Time Protocol (SNTP) is used to synchronize the system time of the ISCOM3000G 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 packets from 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 packets from the broadcast server 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 ISCOM3000G 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



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 (PST): 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	N/A
Global NTP equity	N/A
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


1.5.4 Configuring time and time zone

Configure time and time zone for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# clock set <i>hour minute second year month day</i>	Configure system time.
2	Raisecom# clock timezone { + - } <i>hour minute timezone-name</i>	Configure the local time zone.
3	Raisecom# clock display { default utc }	Configure system clock display mode.

1.5.5 Configuring DST

Configure DST for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# clock summer-time enable	Enable DST.
2	Raisecom# clock summer-time recurring { <i>week</i> <i>last</i> } { <i>fri</i> <i>mon</i> <i>sat</i> <i>sun</i> <i>thu</i> <i>tue</i> <i>wed</i> } <i>month hour minute</i> { <i>week</i> <i>last</i> } { <i>fri</i> <i>mon</i> <i>sat</i> <i>sun</i> <i>thu</i> <i>tue</i> <i>wed</i> } <i>month hour minute offset-mm</i>	Configure calculation period for system DST.  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 advance the clock one hour faster 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 inexist. 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. Namely, 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 ISCOM3000G series switch as below.

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

Step	Command	Description
2	Raisecom(config)#ntp server { ipv4-address ipv6-address } [version version-number] [keyid key-id]	(Optional) configure the IP address of the NTP server for the client working in server/client mode.
3	Raisecom(config)#ntp peer { ipv4-address ipv6-address } [version version-number] [keyid key-id]	(Optional) configure the IP address of the NTP peer for the ISCOM3000G series switch working in symmetric peer mode.
4	Raisecom(config)#ntp refclock-master [ip-address] [stratum]	Configure the clock of the ISCOM3000G series switch as the NTP reference clock source for the ISCOM3000G series switch.




Note

If the ISCOM3000G 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.

Configure NTP identity authentication for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ntp authenticate enable	Enable identity authentication on the NTP server/client.
3	Raisecom(config)#ntp authentication-keyid key-id md5 password	Configure the key ID and key password for identity authentication on the NTP server/client.
4	Raisecom(config)#ntp trusted-keyid key-id	Configure the key ID for identity authentication on the NTP server/client 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config))# sntp server { <i>ipv4-address</i> <i>ipv6-address</i> }	Configure the IP address of the SNTP unicast server. After the SNTP server is configured with an IP address, the ISCOM3000G series switch tries to get the clock information from the SNTP server every 10s. In addition, the maximum timeout is 60s.

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.

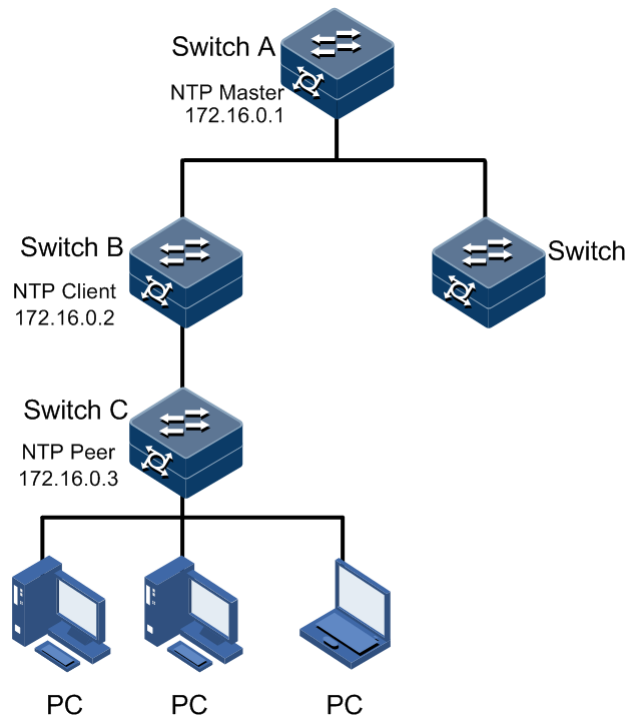
1.5.9 Example for configuring NTP

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.

Figure 1-7 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 state** command to view configurations of Switch A.

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

```

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 state** 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 state** 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 ISCOM3000G 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. When successful in negotiation, the devices at both ends of the link can work in the same duplex mode and interface rate.

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 ISCOM3000G 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	12 Kbytes
Duplex mode of interface	Auto-negotiation
Interface rate	Auto-negotiation
Interval for monitoring the interface rate	5s
Interface rate statistics status	Disable
Time interval of interface dynamic statistics	2s
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 thus 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. When 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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.

Step	Command	Description
2	<code>Raisecom(config)#interface vlan-id</code>	Enter VLAN interface configuration mode.
3	<code>Raisecom(config-vlan1)#mtu max-frame-length Raisecom(config-vlan1)#exit</code>	Configure the MTU on the interface. When the length of the IP packet to be forwarded exceeds the maximum value, the ISCOM3000G series switch will fragment the IP packet.
4	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter physical layer interface configuration mode.
5	<code>Raisecom(config- gigaethernet1/1/1)#duplex { full half }</code>	Configure the duplex mode of the interface.
6	<code>Raisecom(config- gigaethernet1/1/1)#speed { auto 10 100 1000 10000 }</code>	Configure the interface rate. It depends on specifications of the optical module for the optical interface.
7	<code>Raisecom(config- gigaethernet1/1/1)# description string</code>	(Optional) configure the description of the interface, which supports special characters, such as the space, "\", "", "<", ">", and "&".
8	<code>Raisecom(config- gigaethernet1/1/1)#jumboframe frame-size</code>	(Optional) configure the maximum framelength allowed by the interface. You can use this command to configure interfaces in batches.
9	<code>Raisecom(config- gigaethernet1/1/1)#mdi { xover auto normal }</code>	(Optional) configure the MDI/MDIX mode of the electrical interface.
10	<code>Raisecom(config- gigaethernet1/1/1)#mac mac- address</code>	(Optional) configure the MAC address of the interface.
11	<code>Raisecom(config- gigaethernet1/1/1)#portswitch</code>	(Optional) configure the interface to switching mode from routing mode. Use the no form of this command to restore the routing mode.
12	<code>Raisecom(config- tengigabitethernet1/1/1)port- type { 100base_t1 100base_t2 100base_x 100base_fx 100base_tx 10Gbase_r } Raisecom(config- tengigabitethernet1/1/1)exit</code>	(Optional) configure the connection mode of the SFP interface.

1.6.4 Configuring interface rate statistics

Configure interface rate statistics for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#dynamic statistics time <i>time</i>	(Optional) configure the period for dynamic statistics.
3	Raisecom(config)#interface <i>vlan</i> <i>vlan-id</i>	Enter VLAN interface configuration mode.
4	Raisecom(config-vlan1)#statistics enable	Enable interface rate statistics.
5	Raisecom(config-vlan1)#clear interface statistics	(Optional) 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#flowcontrol { receive send } { off on }	Enable/Disable interface flow control over 802.3x packets. By default, it is disabled.


1.6.6 Shutting down/Restarting interface

Shut down/Restart an interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#shutdown	Shut down the current interface. Use the no shutdown command to restart the shutdown interface.

1.6.7 Configuring Console interface

Configure the Console interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#console open</code>	(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 ISCOM3000G series switch to be out of control. Use it with caution.
3	<code>Raisecom(config)#login-trap enable</code>	(Optional) enable sending Trap upon user login or exit.

1.6.8 Configuring sub-interface

Configure the sub-interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface {gigaethernet tengigabitethernet }1/1/port.sub-interface</code>	Create a sub-interface, and enter Ethernet sub-interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/1.1)#encapsulation dot1Q vlan-id-1 [to vlan-id-2]</code>	(Optional) configure the VLAN ID of VLAN segment carried in the VLAN Tag of the sub-interface.

1.6.9 Configuring Combo interface

Configure the Combo interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.

Step	Command	Description
3	<code>Raisecom(config-tengigabitethernet1/1/1)#medium-priority { copper fiber }</code>	(Optional) configure the Combo interface to preferentially work as an optical interface or electrical interface.
4	<code>Raisecom(config-tengigabitethernet1/1/1)#media-type { auto fiber copper }</code>	(Optional) configure the optical/electrical selection mode of the Combo interface.



Note

This feature can be configured only on the device that provides the Combo interface.

1.6.10 Checking configurations


Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show interface [interface-type interface-number]</code>	Show interface status.
2	<code>Raisecom#show interface brief</code>	Show the brief of the interface.
3	<code>Raisecom#show interface [interface-type interface-number] description</code>	Show the description of the interface.
4	<code>Raisecom#show interface interface-type interface-number statistics [dynamic] [detail]</code>	Show interface statistics.

1.7 Configuring basic information

Configure basic information for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#host name name</code>	(Optional) configure the device name. By default, the device name is Raisecom. The system supports changing the device name to make users distinguish different devices on the network. The device name supports special characters, such as the space, "\", "'", "<", ">", and "&". When the device name changes, it can be seen in terminal prompt.
2	<code>Raisecom#language { chinese english }</code>	(Optional) configure language mode. By default, the language is English.

Step	Command	Description
3	<code>Raisecom#write</code>	<p>Save configurations.</p> <p>Save configurations to the ISCOM3000G series switch after configurations, and the new configurations will overwrite the original configurations.</p> <p>Without saving, the new configurations will be lost after restarting, and the ISCOM3000G series switch will continue working with the original configurations.</p> <p> Caution</p> <p>Use the <code>erase file-name</code> command to delete the configuration file. This operation cannot be rolled back, so use this command with caution.</p>
4	<code>Raisecom#reboot [now in time]</code>	<p>(Optional) configure restart options.</p> <p>When the ISCOM3000G series switch fails, restart it to try to solve the problem according to actual condition.</p>

 **Caution**

- Restarting the ISCOM3000G 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 ISCOM3000G series switch supports implementing task scheduling by combining the program list to 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 realize the periodic execution of command lines.

1.8.2 Configuring task scheduling

Configure task scheduling for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.

Step	Command	Description
2	<code>Raisecom(config)#schedule-list <i>list-number</i> start date-time { <i>mm-dd-yyyy hh:mm:ss</i> [every { <i>day</i> <i>week</i> } stop <i>mm-dd-yyyy hh:mm:ss</i>] every <i>days-interval</i> <i>time-interval</i> [stop <i>mm-dd-yyyy hh:mm:ss</i>] }</code>	Create a schedule list, and configure it.
	<code>Raisecom(config)#schedule-list <i>list-number</i> start date-time <i>mm-dd-yyyy hh:mm:ss</i> every <i>weekday-list</i> { <i>fri</i> <i>mon</i> <i>off-day</i> <i>sta</i> <i>sun</i> <i>thu</i> <i>tue</i> <i>wed</i> <i>working-day</i> <i>weekday-list</i> }</code>	
	<code>Raisecom(config)#schedule-list <i>list-number</i> start up-time <i>days-after-startup hh:mm:ss</i> [every <i>days-interval</i> <i>time-interval</i> [stop <i>days-after-startup hh:mm:ss</i>]]</code>	
3	<code>Raisecom(config)#<i>command-string</i> schedule-list <i>list-number</i></code>	Bind the command line which needs periodical execution and supports the schedule list to the schedule list.

1.8.3 Checking configurations

Use the following command to check configuration results.

No.	Command	Description
1	<code>Raisecom#show schedule-list [<i>list-number</i>]</code>	Show configurations of the schedule 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 state of the MCU, a program is specially used, which is commonly known as the Watchdog.

The ISCOM3000G 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 Watchdog.

1.9.4 Configuring Watchdog

Configure Watchdog for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#watchdog enable</code>	Enable Watchdog.

1.9.5 Checking configurations

Use the following command to check configuration results.

Step	Command	Description
1	<code>Raisecom#show watchdog</code>	Show Watchdog status.

1.10 Configuring Banner

1.10.1 Preparing for configurations

Scenario

Banner is a message displayed on the configuration interface when you log in to or exit the ISCOM3000G series switch, such as the precautions or disclaimer.

You can configure the Banner of the ISCOM3000G series switch as required. In addition, the ISCOM3000G series switch provides the Banner switch. After Banner display is enabled, the configured Banner information appears when you log in to or exit the ISCOM3000G series switch.


After configuring Banner, you should use the **write** command to save configurations. Otherwise, Banner information will be lost when the ISCOM3000G series switch is restarted.

Prerequisite

N/A

1.10.2 Configuring Banner

Configure the Banner for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#banner login word Press Enter. Enter text message followed by the character ' <i>word</i> ' to finish. User can stop configuration by inputting 'ctrl+c' <i>message word</i>	Configure the Banner contents. Enter the banner login and <i>word</i> , press Enter , enter the Banner contents, and then end with the <i>word</i> character.  Note The <i>word</i> parameter is a 1-byte character. It is the beginning and end marker of the Banner contents. These 2 marks must be the identical characters. We recommend selecting the specified character that will not occur at the <i>message</i> . The message parameter is the 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#banner enable	Enable Banner display. By default, Banner display is disabled. Use the banner disable command to disable Banner display.

1.10.4 Checking configurations

Use the following commands to check configurations.

No.	Command	Description
1	<code>Raisecom#show banner login</code>	Show Banner status and contents of the configured Banner.

2 ISF

This chapter describes principles and configuration procedures of Intelligent Stacking Framework (ISF), and provides related configuration examples, including the following sections:

- Introduction
- ISF concepts
- Establishing ISF environment
- Configuring ISF
- Preconfiguring ISF in standalone mode
- Configuring ISF in ISF mode
- Checking configurations
- Configuration examples

2.1 Introduction

ISF, a typical stack protocol, is a virtualization technology developed by Raisecom. It connects multiple devices and virtualizes them into one device after necessary configurations. In this case, it combines hardware and software processing capabilities of multiple devices, and implements coordinated working, uniform management, and uninterrupted maintenance of multiple devices.



- The ISF interface should be a 10 Gbit/s interface. All member switches in an ISF should be of the same model.
- An ISF consists of at most 9 member switches.
- For the ISCOM3048G series switch, interfaces 1/1/49–1/1/52 can be added to different ISF interfaces, and interfaces 1/1/49–1/1/50 or interfaces 1/1/51–1/1/52 can be added to the same ISF interface (for example, interfaces 1/1/49–1/1/50 can be added to ISF interface 1/1/1 and interfaces 1/1/51–1/1/52 can be added to ISF interface 1/1/2).
- For the ISCOM3048G series switch, interfaces 1/1/49, 1/1/50 or 1/1/51, or 1/1/52 cannot be added to the same ISF interface (for example, interfaces 1/1/49 and 1/1/51 can be added to ISF interface 1/1/1, but interface 1/1/49 can be added to ISF interface 1/1/1 while interface 1/1/51 can be added to ISF interface 1/1/2).

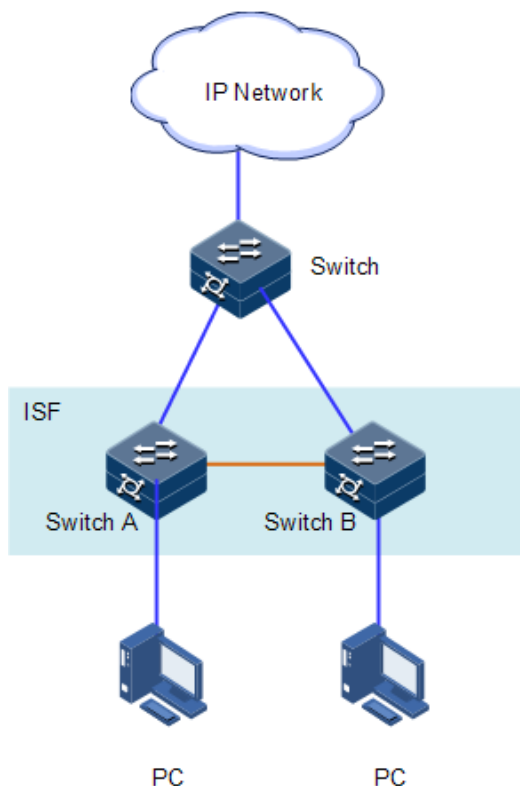
2.1.1 ISF advantages

- Simplified management: after an ISF is formed, you can log in from any interface on any member switch to manage all members in the ISF.
- Powerful network scalability: you can increase interfaces, network bandwidth, and processing capability of an ISF simply by adding member switches.
- High reliability: the ISF is reliable in many aspects. The ISF consists of multiple member switches. The master switch operates, manages, and maintains the ISF while the backup switch and slave switch work as backup and meanwhile process services. When the master switch fails, the ISF will rapidly elect a new master switch to resume services and implement 1:N device backup. ISF links between member switches support link aggregation, and the physical links between the ISF and the upstream or downstream device also support link aggregation. In this way, multiple links can back up each other and balance load, thus improving ISF reliability.

2.1.2 ISF application

As shown in Figure 2-1, the master switch and backup switch form an ISF, so they appear as only one device, for the upstream or downstream devices.

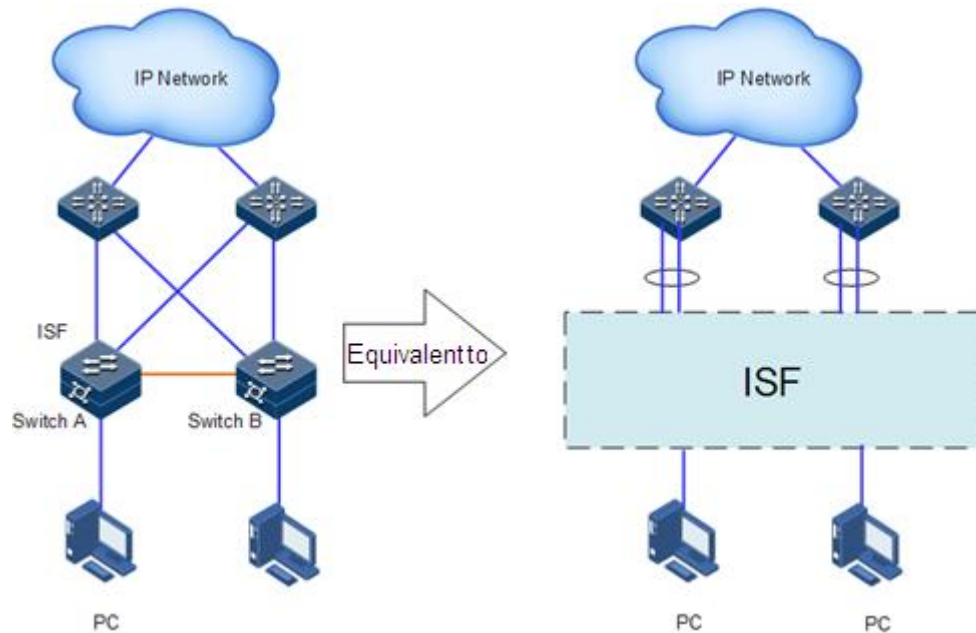
Figure 2-1 ISF networking



2.2 ISF concepts

As shown in Figure 2-2, connect Switch A with Switch B, and configure them properly to form an ISF. The ISF manages physical and software resources of Switch A and Switch B.

Figure 2-2 ISF visualization



Basic concepts of ISF are as below.

Operating modes

An ISF device supports two operating modes:

- Standalone mode: it runs independently, unable to form an ISF with other devices.
- ISF mode: it can be connected with other devices to form an ISF device.

Use commands to switch an ISF device between the previous two modes.

Roles

Each ISF device is a member of ISF. There are three roles as below:

- Master: it manages the entire ISF.
- Backup: it works as a backup for the master device. Namely, when the master device fails, it becomes the master device.
- Slave: it works as a backup for the backup device. Namely, when the master and backup device fail, the ISF will automatically elect a new master device from all slave devices to replace the original master device.

The master device, backup device, and slave device are elected as roles. An ISF contains only one master device, only one backup device, and multiple slave devices.

Member ID

An ISF uses member IDs to identify and manage member devices. Each member ID is unique in the ISF. For example, the member ID is used in the interface ID in the ISF. When a switch runs in standalone mode, the ID of an interface is `tengigabitethernet1/1/1`. When the switch joins the ISF and its member ID is 2, the interface ID will be `tengigabitethernet2/1/1`.

When a switch runs in standalone mode, its default member ID is 1. When it is to join the ISF but its member ID conflicts with that of an existing ISF member, it will fail to join the ISF. In this case, you should plan and configure member IDs uniformly to ensure uniqueness of ISF member IDs.



The member ID ranges from 1 to 9.

ISF interfaces

An ISF interface is a logical interface specially used for the ISF. If the member ID of an ISF interface is N, its interface IDs will be ISF-PortN/1/1 and ISF-PortN/1/2. The interface ID will take effect after the ISF interface is bound with a physical interface. An ISF logical interface can be bound with one or more physical interfaces to increase bandwidth and reliability of ISF links. At present, the ISCOM3000G series switch support binding an ISF interface with up to 8 physical interfaces. For a dual-chip device, physical interfaces connected to different chips cannot be bound with the same ISF interface while those connected to the same chip cannot be bound with different ISF interfaces.



In standalone mode, IDs of ISF interfaces are ISF-Port1/1/1 and ISF-Port1/1/2. In ISF mode, IDs of ISF interfaces are ISF-PortN/1/1 and ISF-PortN/2/1; wherein, N is the member ID. To be brief, this document uses ISF-Port1 and ISF-Port2 uniformly.

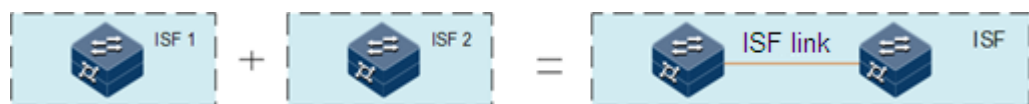
ISF physical interface

An ISF physical interface is a physical interface used for the ISF. A physical interface can be an optical interface which usually forwards service packets. When a physical interface is bound with an ISF interface, it becomes an ISF physical interface which forwards packets between member devices. These packets include negotiation packets related to the ISF and service packets forwarded between member devices.

ISF merge

As shown in Figure 2-3, two ISFs run stably. The process of physically connecting and configuring these two ISFs to form a new ISF is called ISF merge.

Figure 2-3 ISF merge



ISF split

As shown in Figure 2-4, an ISF has formed, but it has a link fault which causes two neighboring members of the ISF to be disconnected. The process of an ISF to be split into two ISFs is called ISF split.

Figure 2-4 ISF split



ISF domain

An ISF domain is a logical concept. To satisfy various networking applications, you can deploy multiple ISFs, distinguished by domain IDs and independent of each other, in a network. ISF involves the process of discovering devices, detecting device connectivity, electing the master device and backup device, generating topology based on collected information, and monitoring connectivity of member devices, thus ensuring normal operation of the virtualization system.

Member priority

Member priority determines the role of a member device in role election. The greater the priority value is, the higher the priority is and the more probably it can be elected as the master device. The default priority of a device is 1. The greater the value is, the higher the priority is. To make a device be elected as the master device, you can modify its member priority to a high value on CLI before establishing an ISF.

2.2.2 Principles of ISF

Establishing an ISF consists of the following four phases:

- Physical connection: connect member devices physically.
- Topology collection: the ISF automatically collects information to form topology.
- Role election: the ISF automatically elects roles.
- Management and maintenance

Physical connection

- Connection medium

To form an ISF, connect ISF physical interfaces of member devices. The connection medium varies with the type of ISF physical interfaces supported by the ISCOM3000G series switch. When the ISF physical interface is an optical interface, connect it with fiber. In this connection mode, you can connect distant member devices to form an ISF, thus making networking more flexible.

- Connection topology

ISF topology consists of two types: chain networking and ring networking, as shown in Figure 2-5 and Figure 2-6.

Figure 2-5 Chain networking

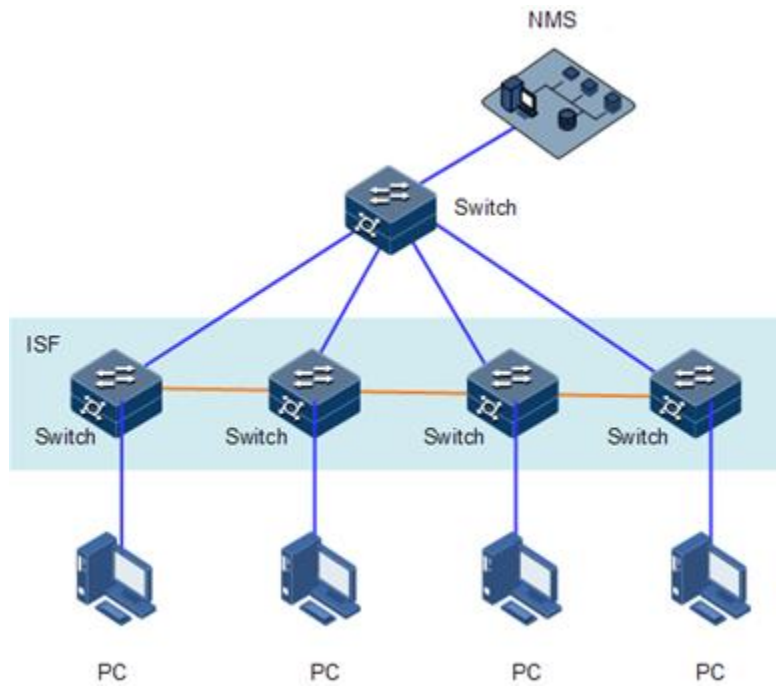
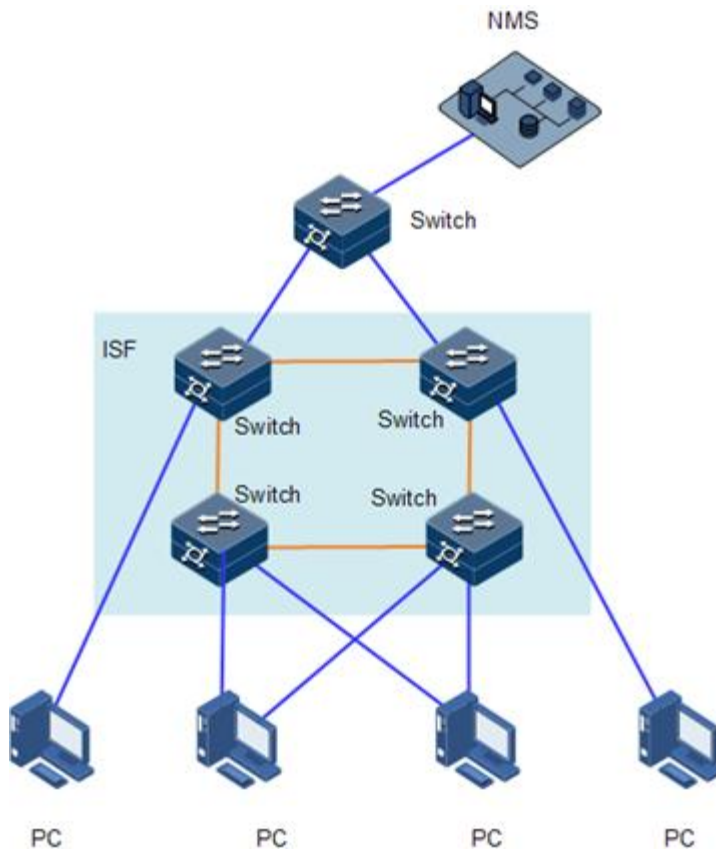


Figure 2-6 Ring networking

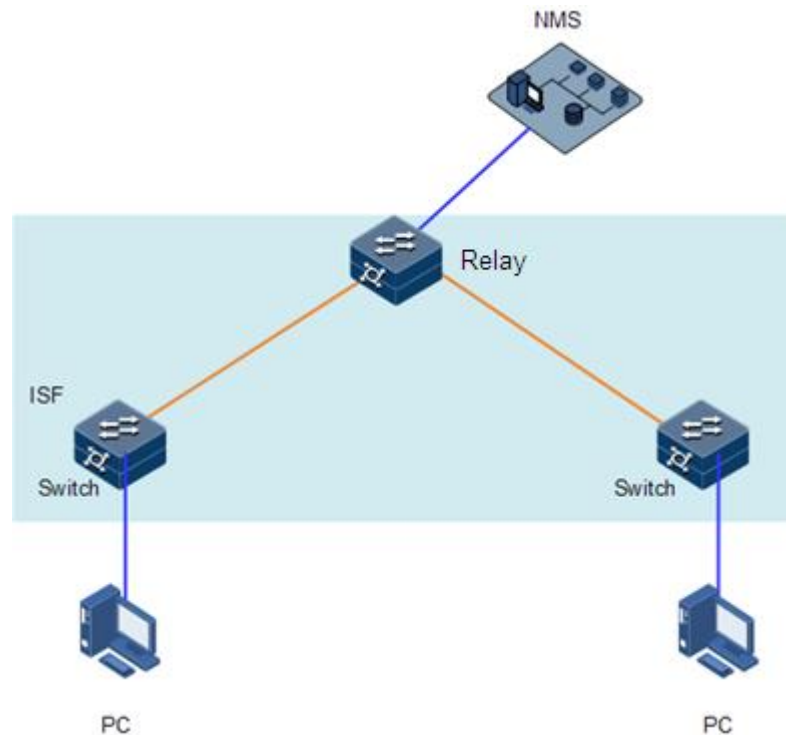


Chain networking: it has a lower physical location than the ring networking, so it is used when members are scattered.

Ring networking: it is more reliable than the chain network because a fault in chain networking disconnects the ISF while a fault in ring networking produces chain networking from the ring networking without affecting ISF services.

If two member devices are far away from each other, such as in Beijing and Hangzhou, you can use a relay device to form an ISF, as shown in Figure 2-7.

Figure 2-7 ISF relay networking



Note

If the ISCOM3000G series switch is configured with ISF enhancement, the ISF connection topology must be the ring type and exclude ISF relay networking.

Topology collection

A member device and its neighbors exchange ISF Probe packets to collect the entire ISF topology.

The ISF Route packet carries topology information, including connection relation of ISF interfaces, ID of member device, priority of member device, and bridge MAC addresses of member interfaces.

When a member switch is started, the local master MCC will perform the following operations:

- Periodically send known topology information from the Up ISF interface.
- Update topology information recorded locally after collecting topology information about neighbors.

In this way, all member devices can collect the entire ISF topology after a period (called topology convergence). Then, the ISF enters the role election phase.

Role election

The process for determining a member device as the master or backup device is called role election, which occurs when the topology changes as below:

- ISF is established.
- A device joins the ISF.
- The master device leaves or fails.
- Two ISFs are merged.

Roles are elected in the following roles in descending order:

1. The current master device, even if a new member device has a higher priority (when an ISF is established, all member devices consider themselves as the master because there is no master. Thus this rule is skipped for the next rule).
2. The device that has been running for the longest time (the up time of each device is carried by the ISF Hello packet)
3. The device with a smaller bridge MAC address

Role election follows the previous rules from the first rule. If multiple member devices are equivalently optimal according to a rule, the following rules will not stop working until a unique optimal member device is elected. Then, this optimal member device is the master, the second optimal one is the backup device, and others are slave devices.

After role election is complete, the master device sends a Config packet to check whether communication is normal. After the ISF is completely established, it enters management and maintenance phase.



Note

When two ISF merge, ISF election will occur by following rules of role election. The devices in the loser ISF join the winner ISF as the backup device or slave devices, and forming a new ISF with the master member device. The restart during ISF merge is manually operated.

No matter a device forms an ISF with other devices or joins an ISF, it will be initialized and restarted by using configurations of the master device to synchronize with the master device if it works as the slave device, regardless of what configurations it has nor whether it has saved current configurations.

2.2.3 ISF merge and ISF split

ISF merge

ISF merge occurs in the following conditions:

- A device is powered on or restarted to join the ISF. In this case, it will be elected as the backup device or slave device (depending on whether there is a slave device in the ISF because the ISF can contain only one backup device). For example, device A is elected as the master device (ISF takes effect upon power-on, so it elects itself as the master device if there is no new member); then, device B joins the ISF after being restarted, and is elected as the backup device (according to role election rule 1). The MAC address of the ISF is that of device A.
- The new device is already the master device (ISF is already effective. The device is connected with the other device). There two devices will compete to elect for the master

device. The one that fails will be restarted (automatically if enabled with restart upon ISF split and ISF merge, or manually) and then join the ISF as a backup device or slave device (due to lower priority or shorter running time). The MAC address of the ISF is that of the master device.

After ISF merge is complete, the MAC address of the ISF is that of the master device, and backup device and slave devices just forward management packets and protocol packets to the master device.

After the ISF runs stably, the master device will back up configurations in batches by issuing its configurations to the backup device and slave devices to synchronize configurations.

After batch backup is complete, realtime backup will start; namely, the master device processes services while the backup device and slave devices back up data and configurations of the master device. The ISF adopts strict synchronization to reliably issue data and configurations to the backup device and slave devices. In this way, when the master device fails, the backup device will replace it within 15s to improve system stability.

ISF split

ISF split occurs in the following conditions:

- Two neighboring devices periodically send heartbeat packets to each other. If a device fails to receive heartbeat packets from its neighbor for multiple periods (usually 16 periods), it considers that the neighbor has left the ISF. Thus new topology will form.
- If a stack interface in the ISF becomes Down, the ISF will re-elect members to form a new topology. If the master device leaves, the ISF will elect the backup device as the master device preferentially. If the backup device leaves, the ISF will elect a slave device as the backup device. If a slave device leaves, roles of other devices will remain the same.

After ISF split is complete, two connected devices will delete related physical interfaces of each other and become independent. Then, they do not need to be restarted or reconfigured.

After ISF split is complete, its MAC address will be those of each device. The original backup device and slave devices will not forward management packets and protocol packets to the original master device.

2.2.4 ISF management and maintenance

After role election is complete, an ISF has formed. All member devices form a virtual device on the network, and their resources are possessed by the virtual device and managed by the master device.

Member ID

When working, an ISF uses member IDs to identify and manage member devices. For example, the interface ID in the ISF is used in the member ID. When a switch works in standalone mode, the ID of an interface changes (such as from tengigabitethernet1/1/1 to tengigabitethernet2/1/1). Thus, you must guarantee uniqueness of all member IDs; otherwise, the ISF will fail to form.

Maintaining ISF topology

If member device A becomes Down or an ISF link becomes Down, its neighbor devices will broadcast the message that member device A leaves to other member devices in the ISF. These

member devices receiving the message, according to the local ISF topology information table, will determine whether member device A is the master or slave device.

- If member device A is the master device, its leave triggers role election and then its neighbor devices will update local ISF topology.
- If member device A is the slave device, its neighbor devices will update local ISF topology to guarantee rapid convergence of ISF topology.



Note

The status of an ISF interface depends on that of the bound ISF physical interface. When all ISF physical interfaces become Down, the ISF interface will be Down.

2.2.5 MAD

Multi-Active Detection (MAD) is a detection and processing mechanism. When an ISF link is faulty, the ISF will be split to two new ISFs which have the same IP address and thus conflict with each other and amplify the fault. Thus, a mechanism is required to improve system availability when ISF split occurs. MAD can detect whether there are multiple ISFs on the network, take actions accordingly to minimize impact of ISF split on services, and enable the ISF at the master device side to work normally. MAD has the following functions:

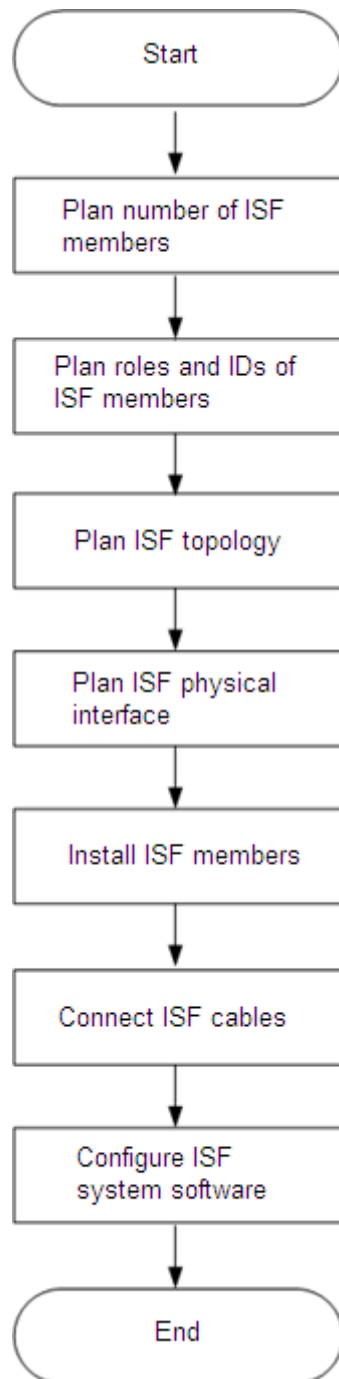
- Detect ISF split: use Bidirectional Forwarding Detection (BFD) to detect whether there are multiple ISFs on the network.
- Eliminate conflict: after ISF split occurs, the original ISF can detect other ISFs in Active status (indicating the ISF is working). This function allows the ISF with the minimum unit ID of the master device to continue to work while converting other ISFs to Recovery status (indicating the ISF is disabled) and shuts down all physical interfaces except the reserved interface in the Recovery ISFs to prevent these ISFs from forwarding packets.
- Clear MAD faults: when an ISF link is faulty, the ISF will be split to two new ISFs. In this case, you can clear the fault by resuming the faulty link to merge two conflicting ISFs to one. If a Recovery ISF becomes faulty before an existing MAD fault is cleared, you must resume the faulty ISF and faulty link to merge two conflicting ISFs to one. If the Active ISF becomes faulty before an existing MAD fault is cleared, you can use command lines to enable the Recovery ISF to replace the original ISF to minimize impact on services, and then clear the existing MAD fault.

2.3 Establishing ISF environment

2.3.1 Establishment flow

Figure 2-8 shows the flow for establishing the ISF environment. We recommend planning the ISF topology and then installing devices to facilitate physical connection of cables in the ISF.

Figure 2-8 Flow for establishing the ISF environment



2.3.2 Planning number of ISF members

After multiple member devices form an ISF, the sum of their switching capacity is the switching capacity of the ISF. Determine the number and model of ISF members according to access and uplink requirements for the network. An ISF supports up to 9 members.

2.3.3 Planning roles and IDs of ISF members

Determining master device

You can configure a device with a higher priority as required. In this way, it can be elected as the master among multiple devices when these devices form an ISF for the first time.

Determining member IDs

When working, an ISF uses member IDs to identify and manage member devices. In this case, before adding devices to the ISF, you should plan and configure member IDs uniformly to ensure uniqueness of ISF member IDs.

2.3.4 Planning ISF topology

The ISF supports chain topology and ring topology. The ring topology is more reliable than chain topology, so it is recommend.

2.3.5 Planning ISF physical interfaces

An ISF interface can be bound with 8 physical interfaces. We recommend bounding an ISF interface with at least 2 physical interfaces to increase bandwidth and reliability of the ISF interface. The two ISF interfaces that connect two neighbor devices should be bound with the same number of ISF physical interfaces so that these ISF physical interfaces can be interconnected with those on the neighbor device. For example, the number of ISF physical interfaces bound with ISF-Port2 on Device A should be equal to that of ISF physical interfaces bound with ISF-Port1 on Device B.



Note

In standalone mode, a physical interface on the device works as an ISF physical interface. When the device enters ISF mode, services configured on the physical interface will be invalid. In this case, you should plan ISF topology to prevent services from being affected.

2.3.6 Installing ISF members

After planning ISF topology, install ISF members.

2.3.7 Connecting ISF cables

When you use an Ethernet optical interface as the ISF physical interface, insert an optical module into the Ethernet optical interface, and then connect the fiber. For optical modules corresponding to Ethernet optical interfaces of different types, see *ISCOM3000G (B) Series Product Description*.

2.3.8 Configuring ISF system software

After installing ISF members, start them. Log in to them respectively to configure ISF system software as planned.

2.4 Configuring ISF

There are two modes for configuring the ISF: preconfiguration mode and non-preconfiguration mode. In preconfiguration mode, an ISF member is restarted for only one time, so this mode is recommended.

2.4.1 Preparing for configurations

Scenario

- Before establishing an ISF, ensure that multiple devices work in the same mode; otherwise, the ISF will fail to form.
- Ensure that all member IDs are different.

Prerequisite

Connect physical interfaces of member devices.

2.4.2 Default configurations of ISF

Default configurations of ISF are as below.

Function	Default value
Stacking mode	Standalone
Unit ID	1
Domain ID	0
Priority	0
Automatic upgrade	Disable
Restart upon ISF split or merge	Enable

2.4.3 Preconfiguration mode

In preconfiguration mode, you can configure a standalone device with the ISF interface ID, member ID, and member priority. These configurations do not affect the running of the standalone device, but will take effect after the standalone device enter ISF mode. Before forming an ISF, you should configure the standalone device in preconfiguration mode. You can configure the standalone device with high priority. In this way, it can be elected as the master among multiple devices when these devices form an ISF for the first time. Configure the ISF interface to switch the operating mode to ISF mode so that the device can form an ISF with other devices (only one restart is needed to form the ISF).

Task		Description
Configuring the ISF interface	Configuring the ISF interface	Required
	Configuring the member ID	Required

Task		Description
	Configuring the member priority	Optional
Configure the ISF mode		Required
Configuring the ISF in ISF mode	Configuring the reservation time for the bridge MAC address of the ISF	Optional
	Enabling restart upon ISF merge	Optional
	Enabling auto-loading of the startup file of the ISF	Optional
	Configuring MAD	Optional

2.4.4 Non-preconfiguration mode

In non-preconfiguration mode, you can configure a standalone device with the member ID, switch the device to the ISF mode, and configure ISF parameters, such as the ISF interface and member priority (multiple restarts are required during the entire process). This configuration method is used to modify current configurations. For example,

- Modify the ID of a member device to a specified value (note that after device restart the modification takes effect and the original member ID becomes invalid).
- Modify the priority of a member device to make the device be elected as the master device.
- Modify the existing binding of an ISF (deleting a binding or add a binding). The configuration of the ISF interface may affect the running of the local device (such as causing ISF split or ISF merge).

Task		Description
Configuring ISF member ID in standalone mode		Required
Configuring ISF mode		Required
Configuring the ISF in ISF mode	Configuring the reservation time for the bridge MAC address of the ISF	Optional
	Enabling restart upon ISF merge	Optional
	Enabling auto-loading of the startup file of the ISF	Optional
	Configuring MAD	Optional

2.5 Preconfiguring ISF in standalone mode

To make a device form an ISF with other devices after switching of the operating mode, you can preconfigure parameters of the device in standalone mode, such as the unit ID, member priority, member domain ID, and ISF interface. Configurations of these parameters do not take effect in standalone mode but will take effect after switching to ISF mode.

2.5.1 Configuring ISF interface

The ISF interface is a logical concept. After you create an ISF interface and bind it with a physical interface, the physical interface is an ISF physical interface which can be connected to another device through an ISF connection. An ISF interface can be bound with up to 8 physical interfaces through multiple binding commands. The ISF interface aggregated from multiple physical interfaces is called the aggregation ISF interface. In this way, up to 16 Ethernet cables or fibers can connect two devices to increase bandwidth and reliability of the ISF interface.

Configure the ISF interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface isf-port <i>interface-number</i></code>	Create an ISF interface, and enter ISF interface configuration mode.
3	<code>Raisecom(config-isf-port1/1/1)#isf port-group <i>interface-number</i></code> <code>Raisecom(config-isf-port1/1/1)#exit</code>	Bind a physical interface with the ISF interface.



Note

Save the configuration to the startup configuration file so that it can take effect when the device switches to the ISF mode and load the startup configuration file.

In standalone mode, binding an ISF interface with an ISF physical interface does not affect current services of the ISF physical interface. When the device switches to ISF mode, configurations of the ISF physical interface will be restored to the default ISF status (configurations of current services will be deleted).

When a device leaves the factory, it is in standalone mode without a member ID. You must configure a member ID and then switch the device from standalone mode to ISF mode. Use the **show isf configuration** command to show the member ID. To avoid conflicts of member IDs upon adding the member to the ISF, you should plan ISF member IDs.

2.5.2 Configuring member priority

The member priority is used in role election. A device with high priority can be elected as the master device with high probability.

Configure the member priority for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#isf priority <i>priority-number</i></code>	Configure the member priority.

2.5.3 Configuring ISF mode

Configure the ISF mode for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#isf-mode single</code> Set successfully. The device will switch to single mode,take effect after reboot	Configure the ISF mode.



Note

When the configuration command is executed, the system prompts "Set successfully. The device will switch to single mode, take effect after reboot". To prevent the device from being restarted, type "no", and press **Enter**. The device will not be restarted, so you can further configure it.

2.6 Configuring ISF in ISF mode

2.6.1 Configuring ISF mode

Configure the ISF mode for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#isf mode isf</code>	Configure the ISF mode.



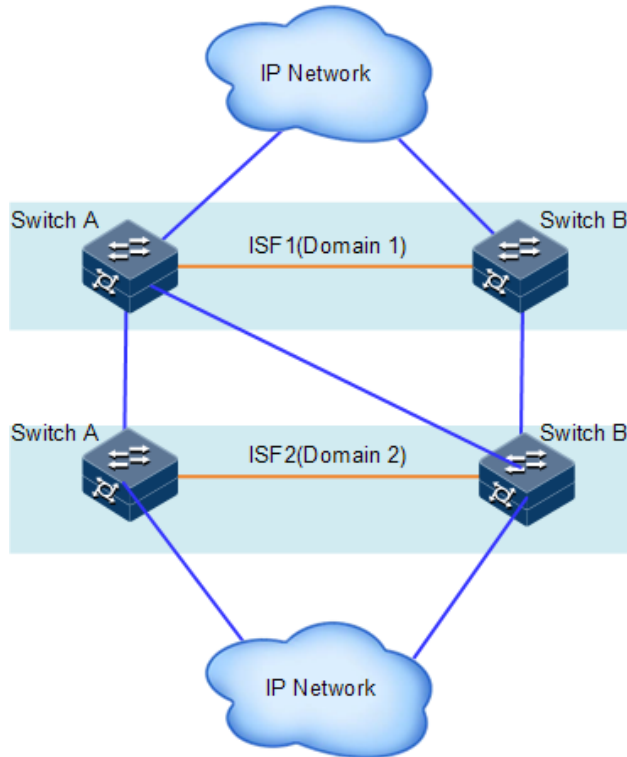
Note

When the configuration command is executed, the system prompts "Set successfully. The device will switch to isf mode, take effect after reboot". To prevent the device from being restarted, type "no", and press **Enter**. The device will not be restarted, so you can further configure it.

2.6.2 Configuring ISF domain ID

An ISF domain is a logical concept. Multiple devices form an ISF through ISF links, and the set of these devices is an ISF domain. To meet requirements for different networking applications, you can deploy multiple ISFs on a network. These ISFs are identified by ISF domain IDs. As shown in Figure 2-9, Switch A and Switch B form ISF 1 while Switch C and Switch D form ISF 2. If there is a MAD link between ISF 1 and ISF 2, these two ISFs send MAD packets to each other, thus affecting their status and operation. In this case, you can configure two different ISF domain IDs to prevent them from affecting each other.

Figure 2-9 Multi-ISF-domain networking



Configure the ISF domain ID for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#isf unit number domain domain-number</code>	Configure the domain ID.

2.6.3 Configuring ISF interface

After switching multiple devices to ISF mode, create their ISF interfaces respectively, and bind these ISF interfaces with their physical interfaces to form ISF physical interfaces. Use ISF cables to connect these ISF physical interfaces. Then, ISF on these devices will take effect. ISF-Port1 (ISF-Port2/1/1 as used in ISF mode) on one device can be connected to ISF-Port2 (ISF-Port2/1/2 as used in ISF mode) only on the other device.

An ISF interface can be bound with up to 8 physical interfaces through multiple execution of the **isf port-group interface** command. The ISF interface aggregated from multiple physical interfaces is called the aggregation ISF interface. In this way, up to 16 Ethernet cables or fibers can connect two devices to increase bandwidth and reliability of the ISF interface.

Configure the ISF interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.

Step	Command	Description
2	<code>Raisecom(config)#interface isf-port interface-number</code>	Enter ISF interface configuration mode, and create an ISF interface.
3	<code>Raisecom(config-isf-port1/1/1)#isf port-group interface-number</code>	Bind a physical interface with the ISF interface.



Note

When a physical interface is bound with an ISF interface, services configured on the physical interface will be invalid. You should plan the binding to prevent original services from being affected.

An ISF interface can be bound with multiple physical interfaces through multiple executions of the **port-group interface** command to implement backup or load balancing of ISF links and to increase bandwidth and reliability of ISF links. An ISF interface can be bound with up to 8 physical interfaces. When the number of bound physical interfaces reaches the upper limit, the execution of the **port-group interface** command will fail.

After binding or unbinding a physical interface with an ISF interface, use the **write** command to save this configuration to the startup configuration file; otherwise, this configuration will not take effect upon next device startup.

2.6.4 Configuring member ID

The ISF uses the member ID to uniquely identify member devices. Information and configurations of the device are related to the member ID, such as the interface ID (including the physical interface and logic interface), interface configurations, and member priority.

- If you modify the member ID but do not restart the device, the original member ID will still take effect and be used by physical resources. In the configuration file, all configurations, except the ISF interface ID, configurations of the ISF interface, and member priority, will remain the same.
- If you modify the member ID and restart the device, the new member ID will take effect and be used by physical resources. In the configuration file, the ISF interface ID, configurations of the ISF interface, and member priority will take effect; other configurations related to the member ID will be invalid and need reconfiguration.

Configure the member ID for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#isf unit old-number renumber new-number</code>	(Optional) modify the unit number from the original unit number to a new unit number in ISF mode.
3	<code>Raisecom(config)#isf renumber number</code>	(Optional) modify the unit number from the original unit number to a new unit number in standalone mode.



The new member ID takes effect after device restart.
The ISF uses the member ID to uniquely identify member devices. Configurations of the ISF interface and member priority are related to the member ID, so modification of the member ID may cause configurations to change or loss. Use the command with caution.

2.6.5 Configuring member priority

The member priority is used in role election. A device with higher priority can be elected as the master device with high probability.

Configure the member priority for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#isf unit number priority priority- number</code>	Configure the priority of a member device.

2.6.6 Configuring reservation time for ISF bridge MAC address

The bridge MAC address is the MAC address when a device communicates as a bridge. Some Layer 2 protocols (such as LACP) use bridge MAC addresses to identify devices, so a bridge device on the network must have a unique bridge MAC address. If there are multiple devices with the same bridge MAC address on the network, the bridge MAC address will conflict with each other and thus the network communication will fail.

An ISF communicates with the external network as a virtual device, so it should have a unique bridge MAC address, called the ISF bridge MAC address. It usually uses the bridge MAC address of the master device as the ISF bridge MAC address.

Conflict with the bridge MAC address causes communication failure, but switching of the bridge MAC address causes service interruption. In this case, you should configure the reservation time for the ISF bridge MAC address according to actual network conditions:

- When the reservation time for the ISF bridge MAC address is configured to 10min, the ISF bridge MAC address remains the same within 10min if the master device leaves the ISF. If the master device fails to return to the ISF, the bridge MAC address of the newly elected master device will be the ISF bridge MAC address. This configuration is suitable when the master device leaves the ISF for a short time and then returns (for example, the master device is restarted or a link is faulty temporarily), and can thus avoid service interruption due to switching of the bridge MAC address.
- When the reservation time for the ISF bridge MAC address is permanent, the ISF bridge MAC address remains the same regardless of whether the master leaves the ISF.
- When the ISF bridge MAC address is configured to unreserved, the bridge MAC address of the newly elected master device will be the ISF bridge MAC address when the master leaves the ISF.

Configure the reservation time for ISF bridge MAC address for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#isf mac-address persistent always	Configure the ISF bridge MAC address to be permanent when the master device leaves the ISF.
3	Raisecom(config)#isf mac-address persistent timer	Configure the reservation time for the ISF bridge MAC address to 10min when the master device leaves the ISF.
4	Raisecom(config)#no isf mac-address persistent	Configure the ISF bridge MAC address to be updated immediately when the master device leaves the ISF.



Note

The change of the bridge MAC address may interrupt services for a short time. If bridge MAC addresses of two ISFs are the same, these two ISFs cannot be merged into an ISF.

When VRRP load balancing is configured in ISF mode, you must configure the ISF bridge MAC address to be permanently reserved (also permanently reserved by default).

2.6.7 Enabling automatic device restart upon ISF merge

When multiple ISFs merge, they will elect according to role election rules. All member devices of the loser ISF have to be restarted before joining the winner ISF.

- If automatic device restart upon ISF merge is disabled, you have to restart devices as prompted by the system during ISF merge.
- If automatic device restart upon ISF merge is enabled, the system will automatically restart devices during ISF merge.

Enable automatic device restart upon ISF merge for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#isf auto-merge enable	Enable automatic device restart upon ISF merge.



Note

All member devices in the loser ISF are restarted and join the winner ISF to merge into one ISF if automatic device restart upon ISF merge is enabled in the following conditions that trigger ISF merge:

- The ISF link fault is cleared.

- Multiple physical interfaces and ISF interfaces are bound in startup configuration files of multiple ISFs, and then establishing the ISF physical connection makes the ISF interface Up.

To keep automatic device restart upon ISF merge in normal operation, enable this function on all ISFs to be merged.

By default, automatic device restart upon ISF merge is enabled.

2.6.8 Configuring MAD

Multi-Active Detection (MAD) is a detection and process mechanism. When an ISF link is faulty, the ISF splits into two new ISFs. These two ISFs have the same IP address, which causes IP address conflict and thus enlarges the fault. In this case, a mechanism is required to improve system availability and detect whether there are multiple ISFs on the network, and take actions accordingly to minimize impact of ISF split on services.

The MAD mode supported by the ISF is Bidirectional Forwarding Detection (BFD) MAD.

BFD MAD

- Principles of BFD MAD

BFD MAD works based on BFD. To make BFD MAD work properly, enable BFD MAD on the VLAN interface, and configure the MAD IP address of the VLAN interface. Different from a common IP address, a MAD IP address is bound with a member device of an ISF. MAD IP addresses must be configured on all member devices and belong to the same network segment.

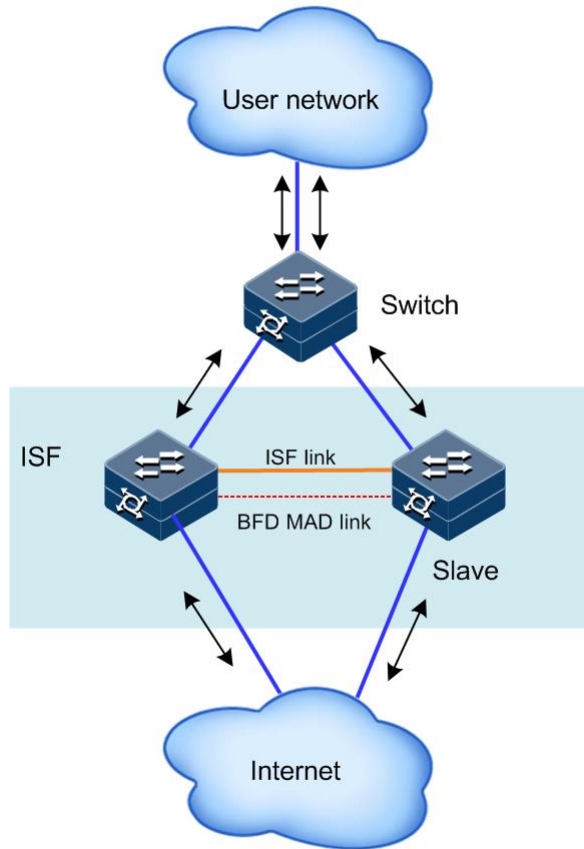
When an ISF works properly, the MAD IP address of the master device takes effect, that of the slave device does not take effect, and thus the BFD session is Down (use the **show bfd state** command to show the status of a BFD session. If the session state is Up, the session is Up. If the session state is Down, the session is Down).

When the ISF splits into multiple ISFs, MAD IP addresses of master devices in different ISFs take effect, BFD sessions become Up, and then multi-active conflict is detected.

- Networking requirements for BFD MAD

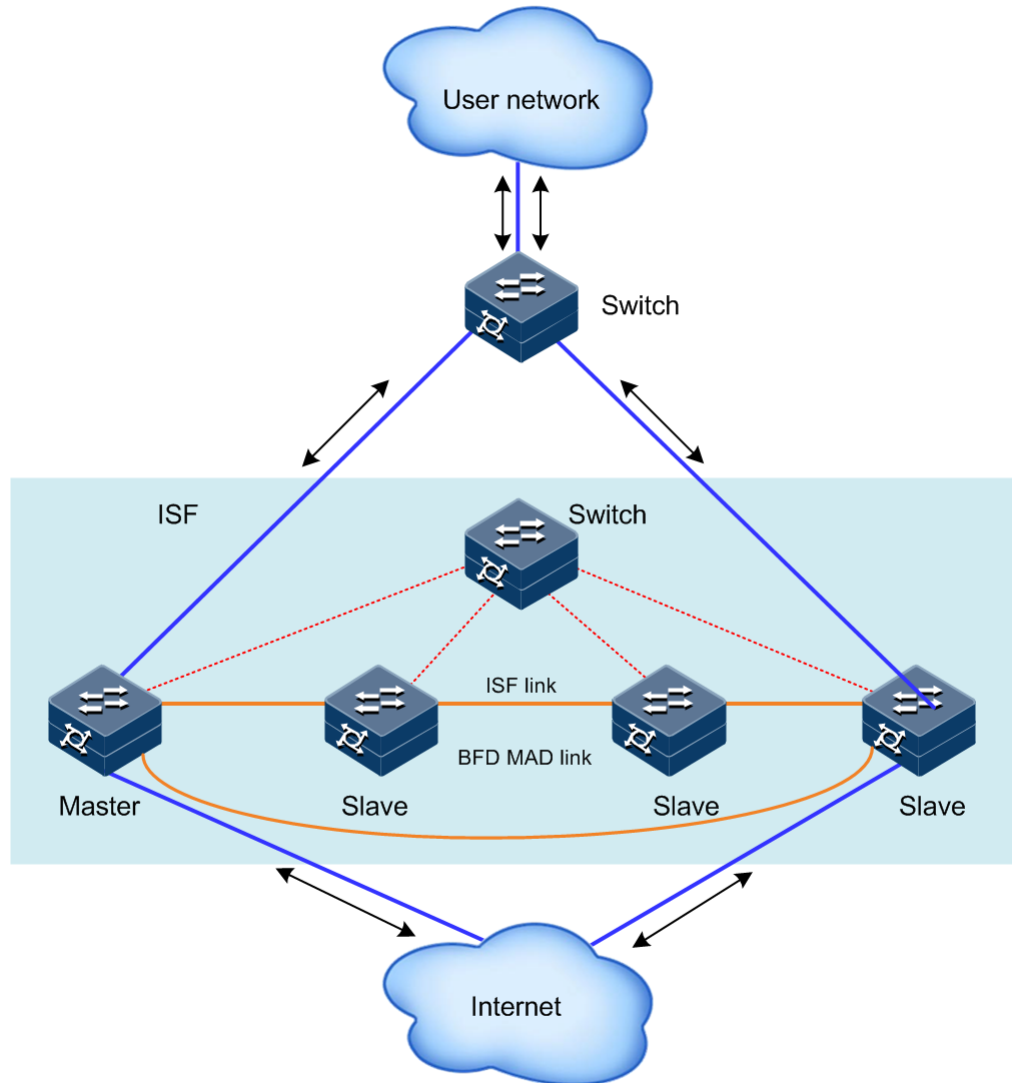
If there are only two member devices in an ISF, you can use an intermediate device or not to configure BFD MAD. As shown in Figure 2-10, there must be one BFD MAD link between any two member devices. The interfaces of these BFD MAD links must belong to the same VLAN. Configure these member devices with different IP addresses in the same network segment in VLAN interface configuration mode.

Figure 2-10 BFD MAD networking (without intermediate device)



If there are 3 or 4 member devices in an ISF, you must use an intermediate device to configure BFD MAD. As shown in Figure 2-11, there must be one BFD MAD link between any member device and the intermediate switch. The interfaces of these BFD MAD links must belong to the same VLAN. Configure these member devices with different IP addresses in the same network segment in VLAN interface configuration mode.

Figure 2-11 BFD MAD networking (with intermediate device)



Configuring BFD MAD

Configure BFD MAD as below:

- Step 1 Create a VLAN specially for BFD MAD (if an intermediate device is used for networking, you should also configure it with this step).
- Step 2 Determine physical interfaces (at least one on each member device) used for BFD MAD, and add them to the VLAN specially used for BFD MAD (if an intermediate device is used for networking, you should also configure it with this step)
- Step 3 Create a VLAN interface for the VLAN specially used for BFD MAD. Enable BFD MAD on the VLAN interface. Configure the MAD IP address.

Configure BFD MAD for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>raisecom#2#config</code>	Enter global configuration mode.

Step	Command	Description
2	Raisecom#2 (config)# interface <i>vlan</i> <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom#2 (config- vlan2)# mad bfd enable	Enable MAD BFD.
4	Raisecom#2(config-vlan2)# mad ip address <i>ip-address</i> [<i>ip-</i> <i>mask</i>] unit <i>number</i>	Configure the MAD IP address of the specified ISF among all ISFs.
5	Raisecom#2(config)# mad restore	(Optional) restore a device disabled due to MAD to normal status.



Note

- After BFD MAD is enabled, the special VLAN should be reserved for this feature only, instead of other usage.
- If the VLAN specially used for BFD MAD contains a Trunk interface which allows packets of multiple VLANs to pass, you must ensure that the default VLAN of the Trunk interface is different from the special VLAN; otherwise, other services configured on the Trunk interface will be affected.
- BFD MAD cannot be enabled on VLAN 1 interface.
- The interface used for BFD MAD must be configured with the MAD IP address through the **mad ip address** command, instead of other IP addresses (common IP address configured through the **ip address** command and VRRP IP address), to prevent from affecting MAD.
- BFD MAD and STP are mutually exclusive, so do not enable STP on the physical interface that is in the VLAN corresponding to the VLAN interface enabled with BFD MAD. Ensure that there is no physical loop.
- Plan the MAD IP address to avoid conflict with the externally learnt route.

Configuring reserved interface

When multiple ISFs conduct MAD, it will shut down all services interfaces in the Recovery ISF. If any interface (such as the Telnet login interface and interface for MAD) has to be Up due to special usage, you can configure the interface as reserved interface through commands.

Configure the reserved interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# mad exclude interface <i>interface-type interface-</i> <i>number</i>	Configure an interface as the reserved interface which will not be shut down when the device enters Recovery status.



Note

The ISF physical interface and Console interface are automatically regarded as reserved interfaces, needless of manual configuration.

To make a VLAN interface in a Recovery ISF continue to receive and send packets (such as using the VLAN interface for remote login), configure the VLAN interface and its corresponding Layer 2 Ethernet interface as reserved interfaces.

Clearing MAD fault

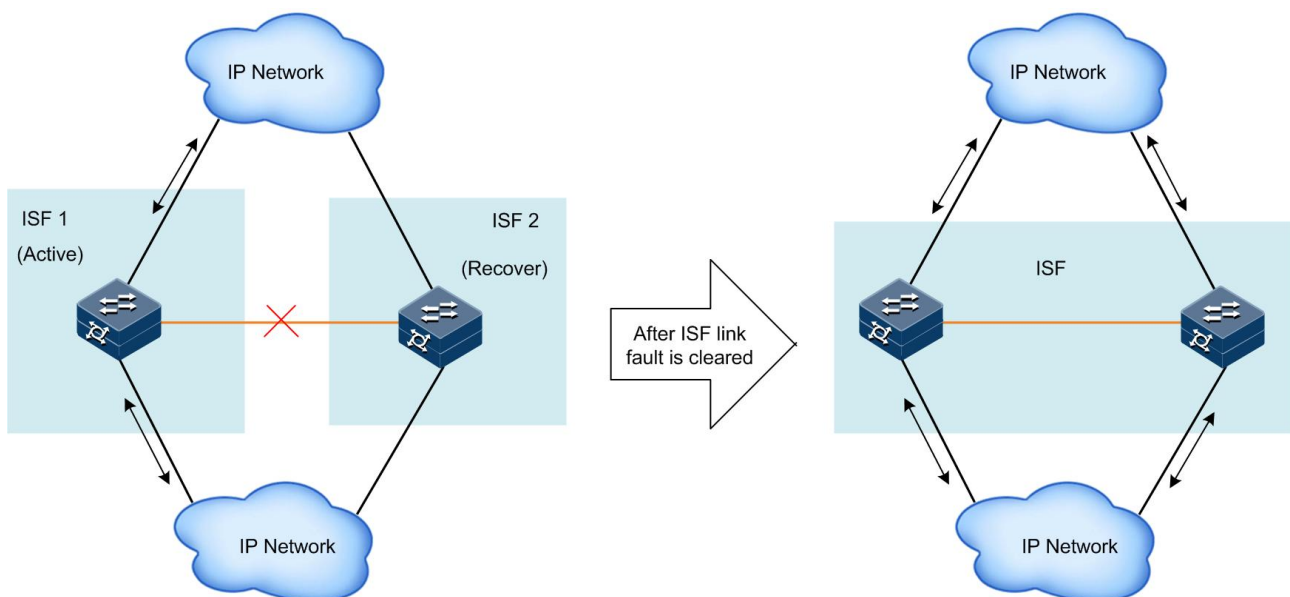
When an ISF link is faulty, the ISF splits into two ISFs, and thus multi-active conflict occurs. When the ISF system detects multi-active conflict, these two conflicting ISFs will elect as below:

1. Compare the number of member devices in these two ISFs. The ISF with more member devices will win and resume working. The loser ISF transits to Recovery status, in which it fails to forward service packets.
2. If these two ISFs have the same number of member devices, the ISF system will compare the member ID of the master device. The ISF with the master device of a greater member ID will win and resume working. The loser ISF transits to Recovery status, in which it fails to forward service packets.

In this case, you can clear the ISF link fault to resume the ISF system (devices will automatically try to clear the ISF link fault. If failed, it needs manual restoration).

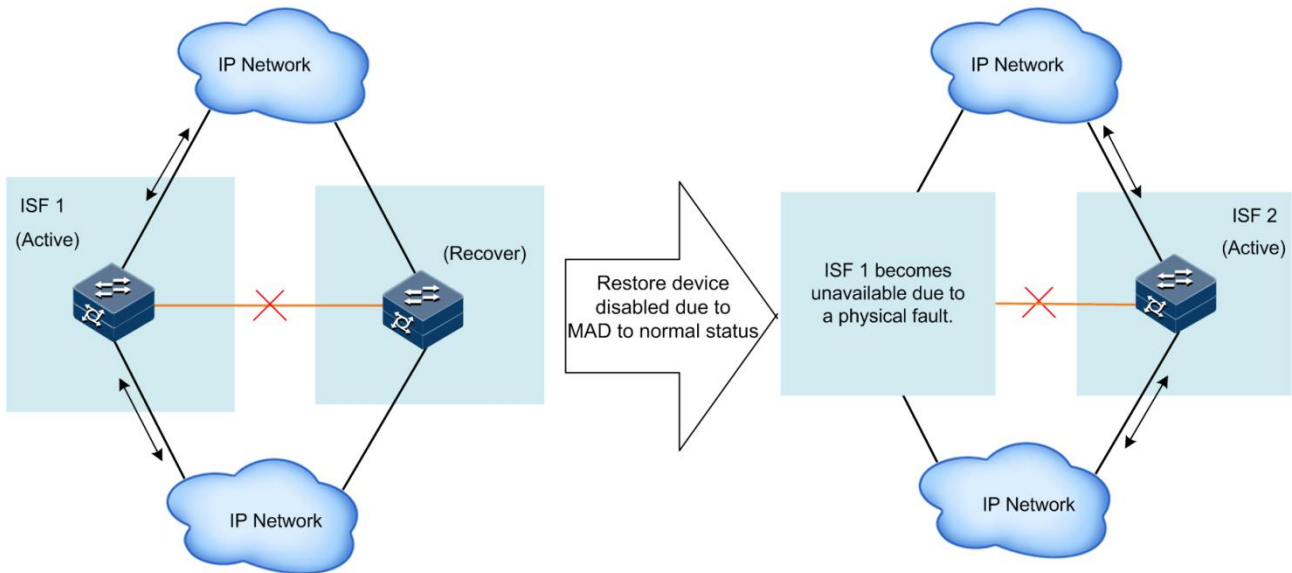
After the ISF link fault is cleared, the Active ISF and the Recovery ISF will merge into an ISF. The ISF system prompts you to restart the Recovery ISF. After the Recovery ISF is restarted, its services interfaces forcibly shut down will be restored to the actual physical status, and the ISF system will resume. As shown in Figure 2-12, if you restart the Active ISF, the two ISFs will merge into one. Then, you need to use the **mad restore** command to restore services interfaces, which are forcibly shut down, in the Recovery ISF to the actual physical status, and the ISF system will resume.

Figure 2-12 Clearing MAD fault (clearing ISF link fault)



As shown in Figure 2-13, if the Active ISF (ISF 1) becomes faulty (device fault or uplink/downlink fault) before the MAD fault is cleared, you can use the **mad restore** command on the Recovery ISF (ISF 2) to restore it and make it replace ISF 1. Then, clear the fault of the link between ISF 1 and ISF 2. Then, these two ISFs merge and the ISF system is restored.

Figure 2-13 Clearing MAD fault (ISF link fault and Active ISF fault)



Restore service interfaces shut down due to MAD to normal status for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mad restore</code>	Restore service interfaces shut down due to MAD to normal status.

2.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show isf</code>	Show all collected ISF information.
2	<code>Raisecom#show isf topology</code>	Show information about ISF topology.
3	<code>Raisecom#show isf packet</code>	Show statistics about ISF packets.
4	<code>Raisecom#show isf configuration</code>	Show ISF preconfigurations.
5	<code>Raisecom#show mad info</code>	Show configurations and status of MAD.

2.8 Configuration examples



By default, the Ethernet interface, VLAN interface, and aggregation interface are in Down status. To configure these interfaces, use the **undo shutdown** command to make them Up. The following example takes the ISCOM3024G for example.

2.8.1 Example for configuring ISF in preconfiguration mode with BFD MAD

Networking requirements

When the network grows rapidly, the central switch (Switch A) fails to meet forwarding requirements. To double forwarding capability based on protecting the existing investment with easy management and maintenance, you can configure ISF.

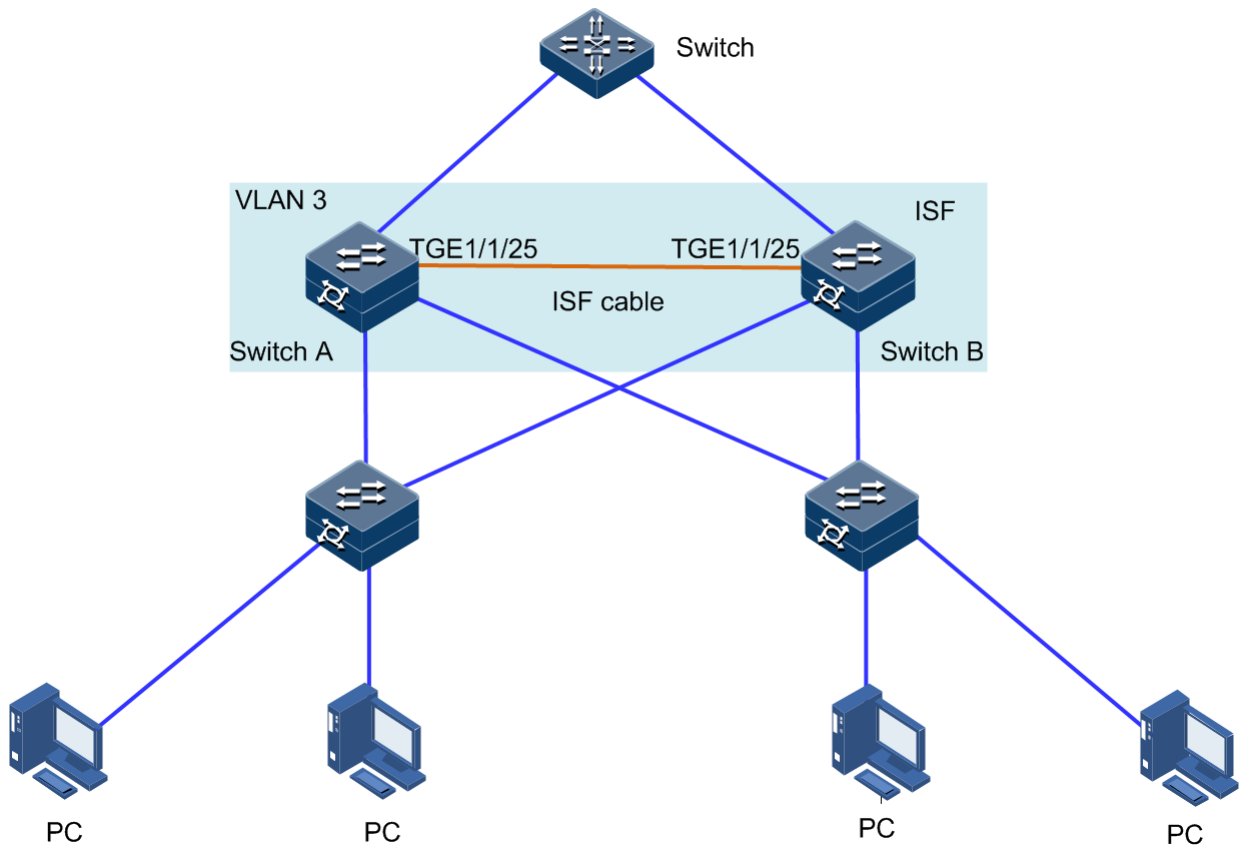
Configuration principles

To double forwarding capability of Switch A, add Switch B to the network, and then configure ISF on them.

When an ISF splits into two ISFs due to an ISF link fault, these two ISFs will conflict with each other. To prevent this, configure MAD. You can configure BFD MAD to monitor the ISF status.

Networking topology

Figure 2-14 ISF networking (BFD MAD mode)



Configuration steps

Step 1 Configure switches in standalone mode.

- Configure Switch A.

Configure the member ID to 1 and member priority to 12. Create ISF interface 2. Binding it with the physical interface Tengigabitethernet 1/1/25.

```
Raisecom#config
Raisecom(config)#isf renumber 1
Raisecom(config)#isf priority 12
Raisecom(config)#interface tengigabitethernet 1/1/25
Raisecom(config-tengigabitethernet1/1/25)#portswitch
Raisecom(config-tengigabitethernet1/1/25)#exit
Raisecom(config)#interface isf-port 1/1/1
Raisecom(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom(config-isf-port1/1/1)#exit
Raisecom(config)#exit
```

Save running configurations to the startup configuration file.

```
Raisecom#write
```

Configure Switch A to ISF mode.

```
Raisecom#config
Raisecom(config)#isf mode isf
next unit is: 9, please input 'yes':yes
This configuration will go into effect after reboot, Please input 'yes'
to reboot:yes
Will you change start-config ? please input 'yes' to change:yes

1970-01-01,08:06:46 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
Raisecom(config)#
BOOTROM starting ..
```

After Switch A is restarted, it forms an ISF that has only one member device.

- Configure Switch B.

Configure the member ID to 2 and member priority to 26. Create ISF interface 1. Bind it with physical interface tengigabitethernet 1/1/25.

```
Raisecom#config
Raisecom(config)#isf renumber 2
Member ID change will take effect after the switch reboots and work in
ISF mode
Will you change start-config ? please input 'yes' to change:no
Raisecom(config)#isf priority 26
Raisecom(config)#interface tengigabitethernet 1/1/25
Raisecom(config-tengigabitethernet1/1/25)#portswitch
Raisecom(config)#interface isf-port 1/1/1
Raisecom(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom(config)#exit
```

Save running configurations as the startup configuration file.

```
Raisecom#write
```

Configure Switch B to ISF mode.

```
Raisecom#config
Raisecom(config)#isf mode isf
```

```
next unit is: 2, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
will you change start-config ? please input 'yes' to change:yes
1970-01-01,08:10:05 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
Raisecom(config)#
BOOTROM starting ..
```

Step 2 Configure switches in ISF mode.

Configure BFD MAD.

- Configure Switch A.

Create VLAN 3. Configure the MAD IP address. Enable BFD MAD on Switch A (with the member ID as 1).

```
Raisecom#1#config
Raisecom#1(config)#create vlan 3 active
Raisecom#1(config)#interface vlan 3
Raisecom#1(config-vlan3)#mad ip address 192.168.2.1 unit 1
Raisecom#1(config-vlan3)#mad bfd enable
1970-01-01,08:17:21 BFD-5-BFD_SESSIONID_DOWN:unit1: Bfd session 65 is
down.#
```

- Configure Switch B.

Create VLAN 3. Configure the MAD IP address. Enable BFD MAD on Switch B (with the member ID as 2).

```
Raisecom#2#config
Raisecom#2(config)#create vlan 3 active
Raisecom#2(config)#interface vlan 3
Raisecom#2(config-vlan3)#mad ip address 192.168.2.2 unit 2
Raisecom#2(config-vlan3)#mad bfd enable
1970-01-01,08:17:21 BFD-5-BFD_SESSIONID_DOWN:unit1: Bfd session 65 is
down.#
```

2.8.2 Example for configuring ISF in non-preconfiguration mode with BFD MAD

Networking requirements

When the network grows rapidly, the central switch (Switch A) fails to meet forwarding requirements. To double forwarding capability based on protecting the existing investment with easy management and maintenance, you can configure ISF.

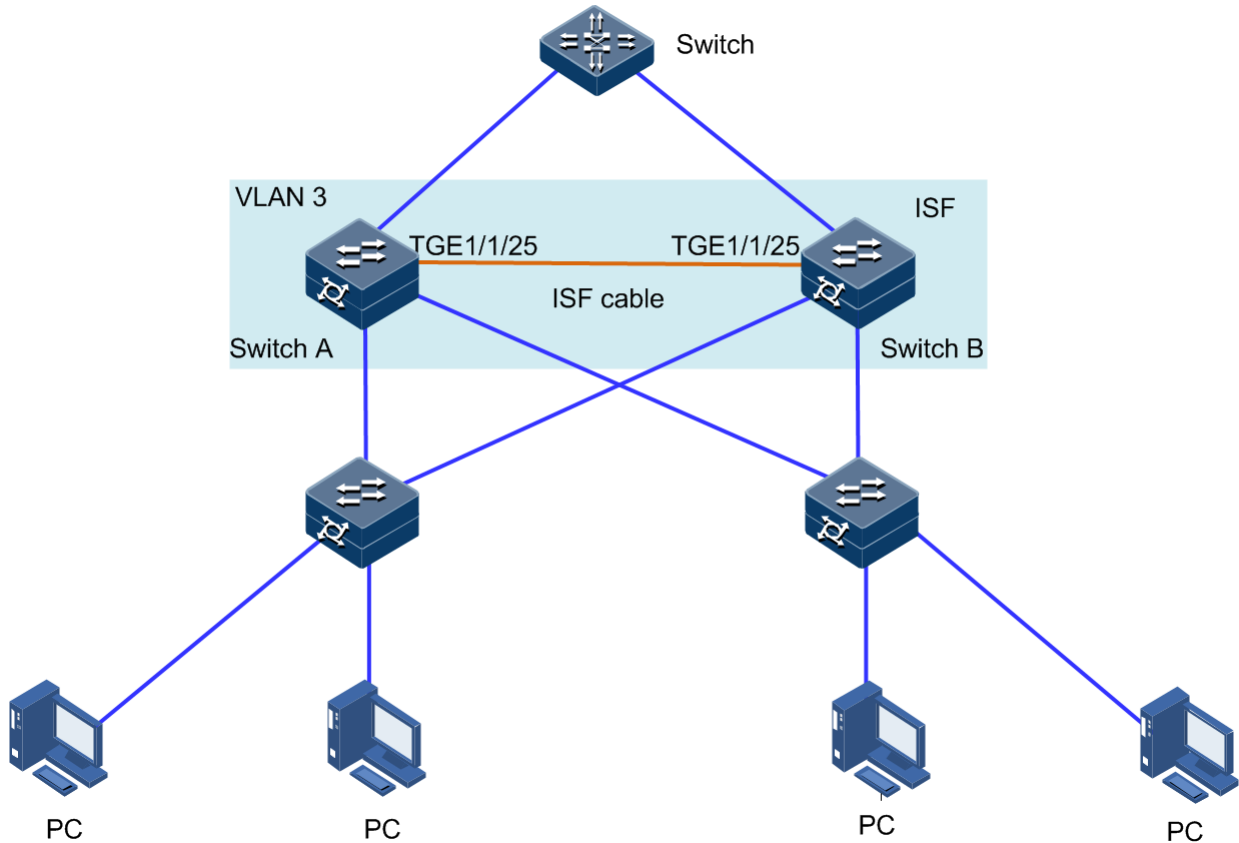
Configuration principles

Disconnect the ISF link by manually removing the ISF cable or using CLI to shut down all ISF physical interfaces on the master device. This example takes CLI for example.

After the ISF splits, switch the two member devices from ISF mode to standalone mode.

Networking topology

Figure 2-15 ISF networking with member device changing from ISF mode to standalone mode



Configuration steps

- Determine the master device.

```
Raisecom#1#show isf
Raisecom#1(config)#isf renumber 1
Raisecom#1(config)#isf mode isf
next unit is: 1, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
BOOTROM starting ..
```

Configure ISF interface 1/1/1, and bind it with physical interface tengigabitethernet 1/1/25.

```
Raisecom#1(config)#interface tengigabitethernet 1/1/25
Raisecom#1(config-tengigabitethernet1/1/25)#portswitch
Raisecom#1(config-tengigabitethernet1/1/25)#exit
Raisecom#1(config)#interface isf-port 1/1/1
Raisecom#1(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom#1(config-isf-port1/1/1)#exit
Raisecom#1(config)#isf unit 1 priority 64
Raisecom#1(config)#exit
```

Save running configurations to the startup configuration file.

```
Raisecom#1#write
```

- Configure Device B.

Configure Switch B to ISF mode.

```
Raisecom#1#config
Raisecom#1(config)#isf renumber 2
Raisecom#1(config)#isf-mode isf
next unit is: 2, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
BOOTROM starting ..
```

Configure ISF interface 1/1/1, and bind it with physical interface tengigabitethernet 1/1/25.

```
Raisecom#2(config)#interface tengigabitethernet 1/1/25
Raisecom#2(config-tengigabitethernet1/1/25)#portswitch
Raisecom#2(config-tengigabitethernet1/1/25)#exit
Raisecom#2(config)#interface isf-port 1/1/1
Raisecom#2(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom#2(config-isf-port1/1/1)#exit
Raisecom#2(config)#isf unit 1 priority 255
Raisecom#2(config)#exit
```

Save running configurations to the startup configuration file.

```
Raisecom#1#write
```

Step 1 Configure switches in ISF mode.

Configure BFD MAD detection.

- Configure Switch A.

Create VLAN 3. Configure the MAD IP address. Enable BFD MAD on Switch A (with the member ID as 1).

```
Raisecom#1#config
Raisecom#1(config)#create vlan 3 active
Raisecom#1(config)#interface vlan 3
Raisecom#1(config-vlan3)#mad ip address 192.168.2.1 unit 1
Raisecom#1(config-vlan3)#mad bfd enable
1970-01-01,08:17:21 BFD-5-BFD_SESSIONID_DOWN:unit1: Bfd session 65 is
down.#
```

- Configure Switch B.

Create VLAN 3. Configure the MAD IP address. Enable BFD MAD on Switch A (with the member ID as 2).

```
Raisecom#2#config
Raisecom#2(config)#create vlan 3 active
Raisecom#2(config)#interface vlan 3
Raisecom#2(config-vlan3)#mad ip address 192.168.2.2 unit 2
Raisecom#2(config-vlan3)#mad bfd enable
1970-01-01,08:17:21 BFD-5-BFD_SESSIONID_DOWN:unit1: Bfd session 65 is
down.#
```

If the intermediate device is an ISF, you must configure it with a domain ID that is different from the domain ID of the target ISF system.

2.8.3 Example for switching member device from ISF mode to standalone mode

Networking requirements

An ISF runs stably with two member devices: Switch A and Switch B. Due to network adjustment, you need to switch them from ISF mode to standalone mode.

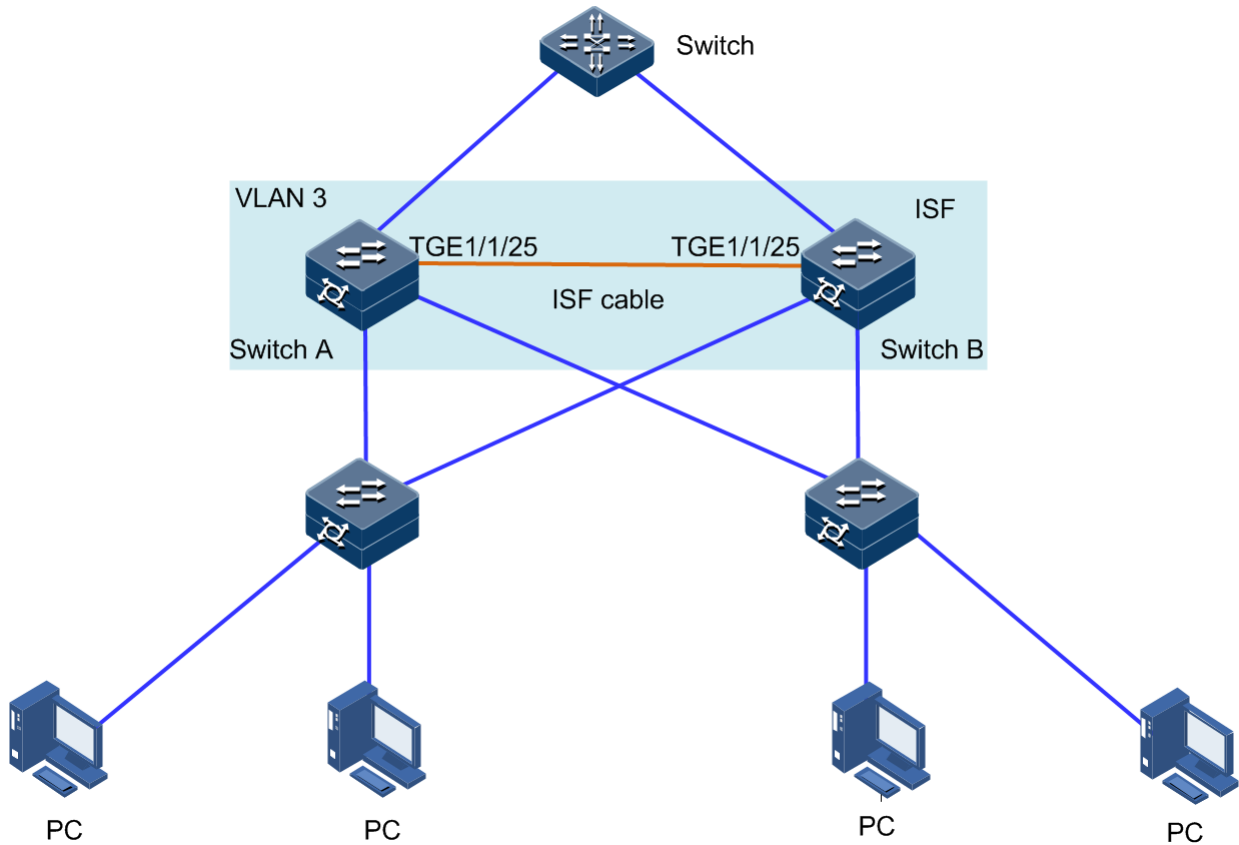
Configuration principles

To double forwarding capability of Switch A, add Switch B to the network, and then configure ISF on them.

When an ISF splits into two ISFs due to an ISF link fault, these two ISFs will conflict with each other. To prevent this, configure MAD. You can configure BFD MAD to monitor the ISF status.

Networking topology

Figure 2-16 ISF networking (BFD MAD mode)



Configuration steps

Step 1 Determine the master device. Configure Switch A as below:

```

Raisecom#1#show isf
MODE:ISF mode
ISF MAC:00:01:22:44:76:78
-----
Isf-port1/1/1
Tengigabitethernet1/1/25
Number  MAC Address      Domain  Unit  Priority  Role
stk Time  Version  Minversion
1      00:01:22:44:76:78    0       2     255     master
18          2          9
2      00:0e:5e:61:91:cf    0       1     64     backup
30          2          9
    
```

Previous information shows that Switch B is the master device.

Step 2 Disconnect the ISF link by manually shutting down ISF physical interface tengigabitethernet 1/1/25 on the master device.

Step 3 Configure Switch A to standalone mode.

Configure Switch A as below:

```
Raisecom#1#config
Raisecom#1#(config)#isf mode single
This config reboot go into effect, Please input 'yes' to reboot:yes
Will you change start-config ? please input 'yes' to change:yes
1970-01-01,08:36:35 System-4-SYSTEM_REBOOT:unit2: Change work Mode
reboot !
Operation successfully
BOOTROM starting ..
```

Step 4 Log in to Switch B. Configure it to standalone mode.

```
Raisecom#2#config
Raisecom#2(config)#isf mode single
This config reboot go into effect, Please input 'yes' to reboot:yes
Will you change start-config ? please input 'yes' to change:yes
1970-01-01,08:36:35 System-4-SYSTEM_REBOOT:unit2: Change work Mode
reboot !
Operation successfully
BOOTROM starting ..
```

2.8.4 Example for configuring four devices to form ISF

Networking requirements

When the network grows rapidly, the central switch (Switch A) fails to meet forwarding requirements. To implement easy management and maintenance, add three devices to form an ISF with Switch A, as shown in Figure 2-17.

Networking topology

Figure 2-17 Networking topology before configuring ISF

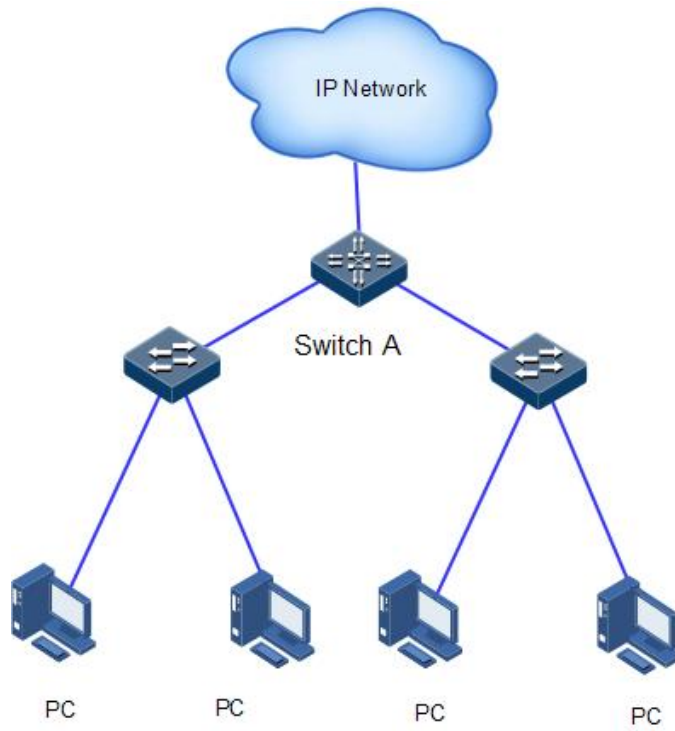
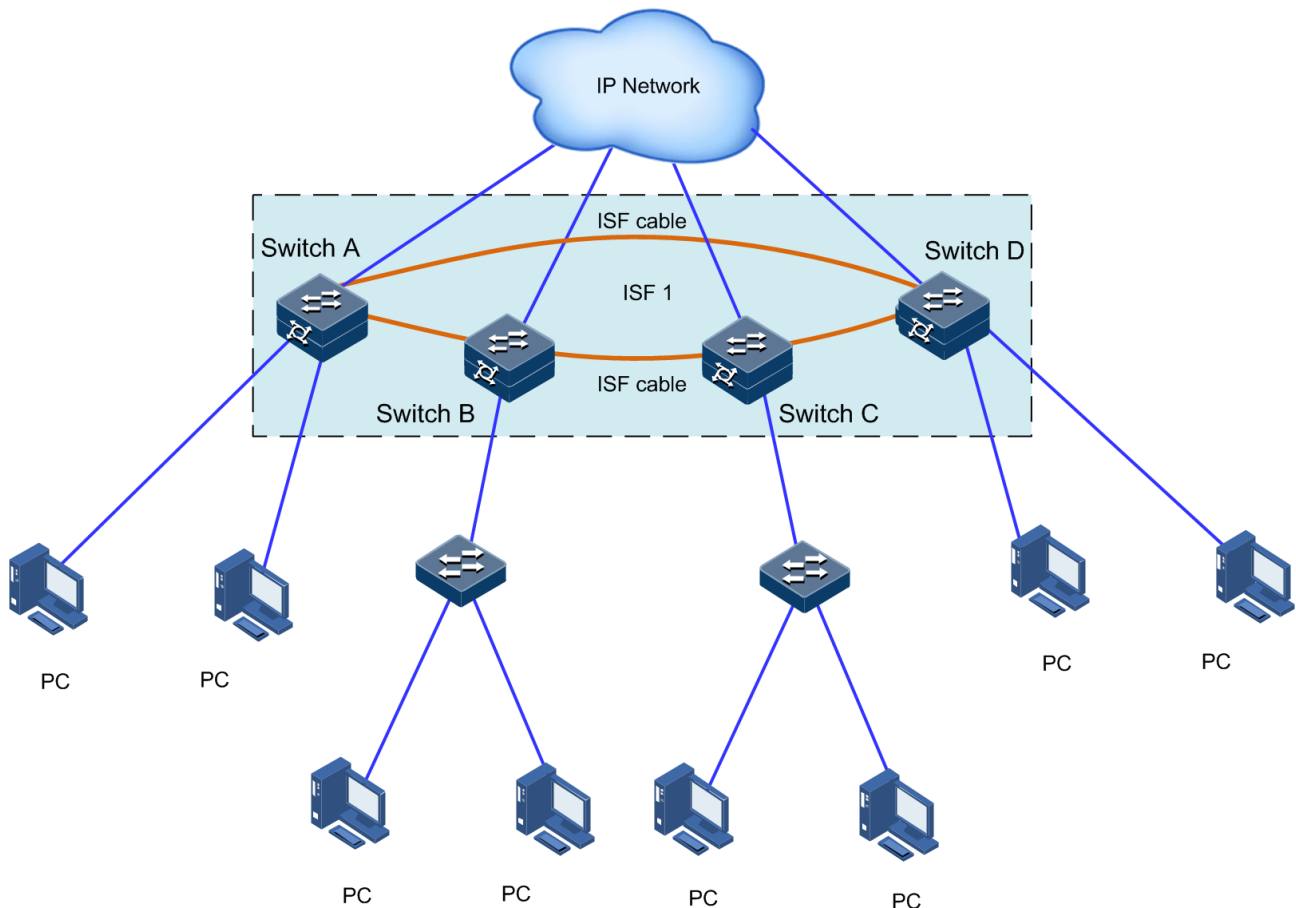


Figure 2-18 Networking topology after adding Switch A to ISF



Configuration principles

- Configure the member ID, member priority, and ISF interface of these four member devices.
- Configure ISF on them. Connect them according to the previous networking topology.
- Switch them to ISF mode.

Configuration steps

Step 1 Configure Switch A.

1. Configure the member ID of Switch A to 1 and member priority to 12.

```
Raisecom#config
Raisecom(config)#isf renumber 1
Raisecom(config)#isf priority 12
Raisecom(config)#interface tengigabitethernet 1/1/25
Raisecom(config-tengigabitethernet1/1/25)#portswitch
Raisecom(config-tengigabitethernet1/1/25)#exit
Raisecom(config)#interface tengigabitethernet 1/1/27
Raisecom(config-tengigabitethernet1/1/27)#portswitch
Raisecom(config-tengigabitethernet1/1/27)#exit
```

```
Raisecom(config)#interface isf-port 1/1/1
Raisecom(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom(config-isf-port1/1/1)#exit
Raisecom(config)#interface isf-port 1/1/2
Raisecom(config-isf-port1/1/2)#isf port-group tengigabitethernet 1/1/27
Raisecom(config-isf-port1/1/2)#exit
```

2. Save running configurations as the startup configuration file.

```
Raisecom#write
```

3. Configure Switch A to ISF mode.

```
Raisecom#config
Raisecom(config)#isf mode isf
next unit is: 1, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
BOOTROM starting ..
```

After Switch A is restarted, it forms an ISF that has only one member device.

Step 2 Configure Device B.

1. Configure the member ID of Switch B to 2 and member priority to 26.

```
Raisecom#config
Raisecom(config)#isf renumber 2
Raisecom(config)#isf priority 26
Raisecom(config)#interface tengigabitethernet 1/1/25
Raisecom(config-tengigabitethernet1/1/25)#portswitch
Raisecom(config-tengigabitethernet1/1/25)#exit
Raisecom(config)#interface tengigabitethernet 1/1/27
Raisecom(config-tengigabitethernet1/1/27)#portswitch
Raisecom(config-tengigabitethernet1/1/27)#exit
Raisecom(config)#interface isf-port 1/1/1
Raisecom(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom(config-isf-port1/1/1)#exit
Raisecom(config)#interface isf-port 1/1/2
Raisecom(config-isf-port1/1/2)#isf port-group tengigabitethernet 1/1/27
Raisecom(config-isf-port1/1/2)#exit
```

2. Save running configurations as the startup configuration file.

```
Raisecom#write
```

3. Configure Switch B to ISF mode.

```
Raisecom#config
Raisecom(config)#isf mode isf
next unit is: 9, please input 'yes':yes
This configuration will go into effect after reboot, Please input 'yes'
to reboot:yes
Will you change start-config ? please input 'yes' to change:yes

1970-01-01,08:06:46 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
Raisecom(config)#
BOOTROM starting ..
```

After Switch B is restarted, it joins the ISF with Switch A.

Step 3 Configure Switch C.

1. Configure the member ID of Switch C to 3 and member priority to 6.

```
Raisecom#config
Raisecom(config)#isf renumber 3
Raisecom(config)#isf priority 6
Raisecom(config)#interface tengigabitethernet 1/1/25
Raisecom(config-tengigabitethernet1/1/25)#portswitch
Raisecom(config-tengigabitethernet1/1/25)#exit
Raisecom(config)#interface tengigabitethernet 1/1/27
Raisecom(config-tengigabitethernet1/1/27)#portswitch
Raisecom(config-tengigabitethernet1/1/27)#exit
Raisecom(config)#interface isf-port 1/1/1
Raisecom(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom(config-isf-port1/1/1)#exit
Raisecom(config)#interface isf-port 1/1/2
Raisecom(config-isf-port1/1/2)#isf port-group tengigabitethernet 1/1/27
Raisecom(config-isf-port1/1/2)#exit
```

2. Save running configurations as the startup configuration file.

```
Raisecom#write
```

3. Configure Switch C to ISF mode.

```
Raisecom#config
Raisecom(config)#isf mode isf
next unit is: 3, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
Operation successfully
BOOTROM starting ..
```

After Switch C is restarted, it joins the ISF with Switch A and Switch B.

Step 4 Configure Switch D.

1. Configure the member ID of Switch D to 4 and member priority to 2.

```
Raisecom#config
Raisecom(config)#isf renumber 4
Raisecom(config)#isf priority 2
Raisecom(config)#interface tengigabitethernet 1/1/25
Raisecom(config-tengigabitethernet1/1/25)#portswitch
Raisecom(config-tengigabitethernet1/1/25)#exit
Raisecom(config)#interface tengigabitethernet 1/1/27
Raisecom(config-tengigabitethernet1/1/27)#portswitch
Raisecom(config-tengigabitethernet1/1/27)#exit
Raisecom(config)#interface isf-port 1/1/1
Raisecom(config-isf-port1/1/1)#isf port-group tengigabitethernet 1/1/25
Raisecom(config-isf-port1/1/1)#exit
Raisecom(config)#interface isf-port 1/1/2
Raisecom(config-isf-port1/1/2)#isf port-group tengigabitethernet 1/1/27
Raisecom(config-isf-port1/1/2)#exit
```

2. Save running configurations as the startup configuration file.

```
Raisecom#write
```

3. Configure Switch D to ISF mode.

```
Raisecom#config
Raisecom(config)#isf-mode isf
next unit is: 4, are you sure ? please input 'yes':yes
This config reboot go into effect, Please input 'yes' to reboot:yes
1970-01-01,08:07:17 System-4-SYSTEM_REBOOT:unit1: Change work Mode
reboot !
BOOTROM starting ..
```

After Switch D is restarted, it joins the ISF with Switch A, Switch B, and Switch C.

3 Ethernet

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

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

3.1 MAC address table

3.1.1 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 number
- Interface VLAN ID
- Flag bits

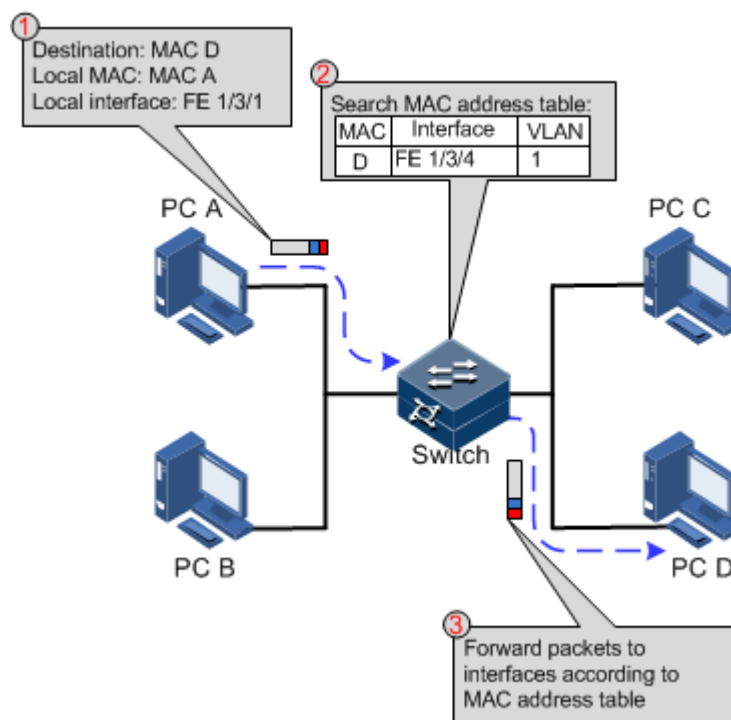
The ISCOM3000G series switch supports showing MAC address information by device, interface, or VLAN.

Forwarding modes of MAC addresses

When forwarding packets, based on the information about MAC addresses, the ISCOM3000G 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 ISCOM3000G 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 ISCOM3000G series switch broadcasts the packet to all interfaces except the receiving interface, as shown in Figure 3-1.

Figure 3-1 Forwarding packets according to the MAC address table



- **Multicast:** when the ISCOM3000G 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 ISCOM3000G series switch receives an all-F packet, or the MAC address is not listed in the MAC address table, the ISCOM3000G 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

The MAC address table contains static address entries and dynamic address entries.

- **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

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 restarted.

- Dynamic MAC address entry: the ISCOM3000G 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 cleared after the system is restarted.

The ISCOM3000G series switch supports up to 16K dynamic MAC addresses. Each interface supports 128K static MAC addresses.

Aging time of MAC addresses

There is limit on the capacity of the MAC address table on the ISCOM3000G series switch. To maximize the use of the MAC address table, the ISCOM3000G series switch uses the aging mechanism to update the MAC address table. For example, when the ISCOM3000G 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 ISCOM3000G series switch will delete the entry.

The ISCOM3000G 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 ISCOM3000G series switch searches the MAC address table for the interface related to the destination MAC address of packets.

- If it is successful and the interface corresponding to the destination MAC address is different from the interface receiving packets, it forwards packets on the related interface, records the source MAC addresses of packets, interface number of ingress packets, and VLAN ID in the MAC address table. If packets from other interfaces are sent to the MAC address, the ISCOM3000G 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

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. It is effective to manage the MAC address table.

MAC address limit improves the rate of forwarding packets.

3.1.2 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, and financial staff), and fixed and important hosts to ensure that all data forwarded to these MAC addresses is forwarded from an interface related to the static MAC address in priority.
- For the interface with fixed static MAC address, you can disable MAC address learning to prevent other hosts from accessing LAN data from the interface.

You can 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

3.1.3 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

3.1.4 Configuring static MAC address

Configure static MAC address as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mac-address static unicast mac-address vlan vlan-id interface-type interface-number</code>	Configure static unicast MAC addresses.



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.
- The maximum number of static unicast MAC addresses supported by the ISCOM3000G series switch is 1024.

3.1.5 Configuring blackhole MAC address

Configure blackhole MAC addresses as below.

Step	Command	Description
1	raisecom#config	Enter global configuration mode.
2	raisecom(config)#mac-address blackhole mac-address vlan vlan- id	Configure blackhole MAC addresses.

3.1.6 Filtering unknown multicast packets

Filter unknown multicast packets for the ISCOM3000G series switch as below.

Step	Command	Description
1	raisecom#config	Enter global configuration mode.
2	raisecom(config)#mac-address multicast drop-unknown reserved-address	(Optional) filter unknown multicast packets.

3.1.7 Configuring MAC address learning

Configure MAC address learning for the ISCOM3000G series switch as below.

Step	Command	Description
1	raisecom#config	Enter global configuration mode.
2	raisecom(config)#interface vlan vlan-id	Enter VLAN interface configuration mode.
3	raisecom(config-vlan1)#mac-address learning enable { interface-type interface-number vlanlist vlan-list }	Enable MAC address learning.

3.1.8 Configuring aging time of MAC addresses

Configure the aging time of MAC addresses for the ISCOM3000G series switch as below.

Step	Command	Description
1	raisecom#config	Enter global configuration mode.
2	raisecom(config)#mac-address aging-time { 0 period }	Configure the aging time of MAC addresses.

3.1.9 Enabling suppression of MAC address flapping

Enable suppression of MAC address flapping for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mac-address mac-move enable	Enable global suppression of MAC address flapping.
3	Raisecom(config)#mac-address mac-move trap enable	(Optional) enable MAC address flapping Trap.

3.1.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show mac-address static [<i>interface-type interface-number</i> vlan vlan-id]	Show static unicast MAC addresses.
2	Raisecom#show mac-address multicast [vlan vlan-id] [count]	Show the Layer 2 multicast addresses or number of existing multicast MAC address.
3	Raisecom#show mac-address blackhole	Show the blackhole MAC address.
4	Raisecom#show mac-address threshold [<i>interface-type interface-list</i>]	Show the dynamic MAC address limit.
5	Raisecom#show mac aging-time	Show the aging time of dynamic MAC addresses.
6	Raisecom#show mac-address learning [<i>interface-type interface-list</i>]	Show status of MAC address learning.
7	Raisecom#show mac-address count [vlan vlan-id] [<i>interface-type interface-number</i>]	Show the number of MAC address entries.
8	Raisecom#show mac-address mac-move	Show information about MAC address flapping.

3.1.11 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom(config)#clear mac-address [<i>mac-address</i>] { all blackhole dynamic static } [<i>interface-type interface-number</i> vlan vlan-id]	Clear entries in the MAC address table.

Command	Description
<pre> Raisecom(config)#search mac-address mac-address { all dynamic static } [interface-type interface-number] [vlan vlan-id] </pre>	Search for a MAC address.

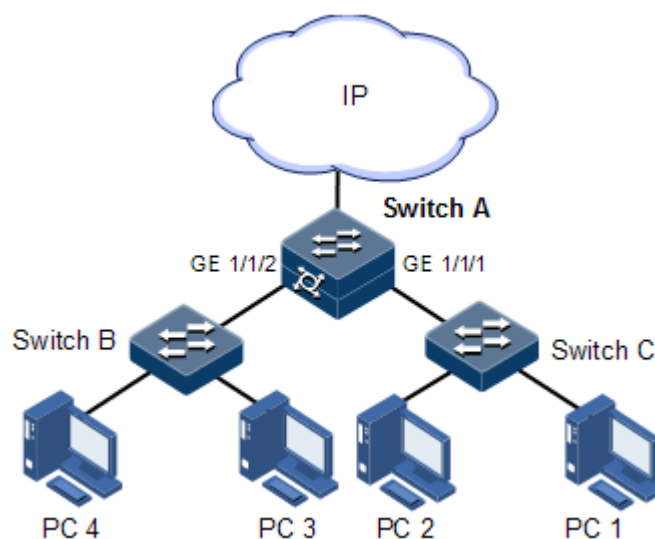
3.1.12 Example for configuring MAC address table

Networking requirements

As shown in Figure 3-2, 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.

Figure 3-2 MAC networking



Configuration steps

Step 1 Create VLAN 10, 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-port)#switchport access vlan 10
Raisecom(config-port)#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  
Aging time: 500 seconds  
Mac Address          Port                vlan    Flags  
-----  
0001.0203.0405     gigaethernet1/1/2    10     Static
```

3.2 VLAN

3.2.1 Introduction

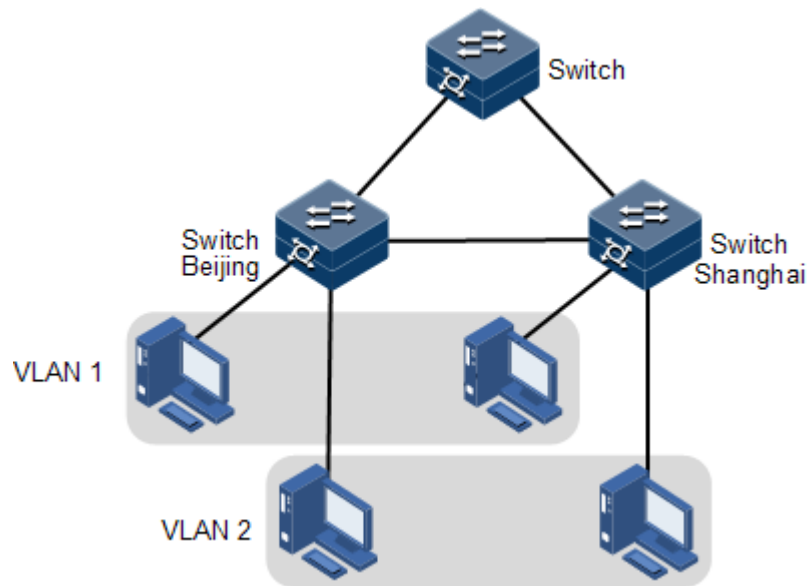
Overview

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 affecting each other. In terms of functions, VLAN has the same features as LAN, but members in one VLAN can access each other without restriction by physical location.

VLAN partition

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

Figure 3-3 VLAN partition



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

The ISCOM3000G series switch complies with IEEE 802.1Q standard VLAN and supports 4094 concurrent VLANs.

- VLAN partition by interface

The ISCOM3000G series switch supports VLAN partitioning by interface. The ISCOM3000G series switch has two interface modes: Access mode and Trunk mode. The method for processing packets for the two modes is showed as below.

Table 3-1 Interface mode and packet processing

Interface type	Processing ingress packets		Processing egress packets
	Untagged packets	Tagged packets	
Access	Add Access VLAN Tag into the packet.	<ul style="list-style-type: none"> • If VLAN ID of the packet is equal to Access VLAN ID, receive the packet. • If VLAN ID of the packet is not equal to Access VLAN ID, discard the packet. 	<ul style="list-style-type: none"> • If the VLAN ID of the packet is equal to Access VLAN ID, remove Tag and send the packet. • If the packet VLAN ID is not included in the VLAN ID list allowed to pass by the interface, discard the packet.

Interface type	Processing ingress packets		Processing egress packets
	Untagged packets	Tagged packets	
Trunk	Add Native VLAN Tag into the packet.	<ul style="list-style-type: none"> • If the packet VLAN ID is included in the VLAN ID list allowed to pass by the interface, receive the packet. • If the packet VLAN ID is not included in the VLAN ID list allowed to pass by the interface, discard the packet. 	<ul style="list-style-type: none"> • If the VLAN ID of the packet is equal to Native VLAN ID, remove Tag and send the packet. • If the VLAN ID of the packet is not equal to Native VLAN ID and the interface allows the packet to pass, keep the original Tag and send the packet.
Hybrid		<ul style="list-style-type: none"> • If the packet VLAN ID is included in the VLAN ID list allowed to pass by the interface, receive the packet. • If the packet VLAN ID is not included in the VLAN ID list allowed to pass by the interface, discard the packet. 	<ul style="list-style-type: none"> • If the packet VLAN ID is included in the VLAN ID list allowed to pass by the interface and excluded from the Untag VLAN ID list, keep the original Tag and send the packet. • If the packet VLAN ID is excluded from the Untag VLAN ID list, keep the original Tag and send the packet.

- VLAN partition by MAC address

This refers to VLAN partition 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.
- 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 partition by IP subnet

This refers to VLAN partition 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.

3.2.2 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 on 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 on 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 an enterprise that has many employees and needs a large number of hosts, in the same department but different positions. The hosts in one department can access one another so you have to partition VLANs on multiple devices. Layer 3 devices, such as routers, are required if users wish to communicate among different VLANs. The cascaded interfaces among devices are configured to 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.

Prerequisite

N/A

3.2.3 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	Suspend
Interface mode	Access
Access VLAN	VLAN 1
Native VLAN of Trunk interface	VLAN 1
Allowable VLAN in Trunk mode	All VLANs
Allowable untagged VLAN in Trunk mode	VLAN 1
VLAN mapping table ID	VLAN ID

3.2.4 Configuring VLAN attributes

Configure VLAN attributes for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#create vlan <i>vlan-list</i> active	Create a VLAN. The command can also be used to create VLANs in batches.
3	Raisecom(config)#vlan <i>vlan-id</i>	Enter VLAN configuration mode.



Note

- The VLAN created by the **vlan *vlan-id*** command is in active status.
- All configurations of VLAN do not take effect until the VLAN is activated.

3.2.5 Configuring interface mode

Configure interface mode for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#switchport mode { access trunk }	Configure the interface to Access or Trunk mode.

3.2.6 Configuring VLAN on Access interface

Configure VLAN on the Access interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#switchport mode access Raisecom(config- gigaethernet1/1/1)#switchport access vlan <i>vlan-id</i>	Configure the interface to Access mode, and add the Access interface to the VLAN.
4	Raisecom(config- gigaethernet1/1/1)#switchport access egress-allowed vlan { all [add remove] <i>vlan-list</i> }	(Optional) configure the VLAN allowed to pass by the Access interface.



Note

- The interface allows Access VLAN packets to pass regardless of configuration for VLAN permitted by the Access interface. The forwarded packets do not carry 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 or suspend the Access VLAN manually, the system will automatically configure the interface Access VLAN as the default VLAN.
- When configuring interface Access VLAN as non-default Access VLAN, default Access VLAN 1 is the VLAN allowed by the Access egress interface, you can delete Access VLAN 1 from the allowed VLAN list of Access the egress interface by deleting this VLAN.
- 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 default VLAN packets to pass.
- The allowed VLAN list of the Access interface is only effective to static VLANs, and ineffective to GVRP dynamic VLANs.

3.2.7 Configuring VLAN on Trunk interface

Configure VLAN on the Trunk interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#switchport mode trunk</code>	Configure the interface to Trunk mode.
4	<code>Raisecom(config- gigaethernet1/1/1)#switchport trunk native vlan <i>vlan-id</i></code>	Configure the Native VLAN of the interface.
5	<code>Raisecom(config- gigaethernet1/1/1)#switchport trunk allowed vlan { all [add remove] <i>vlan-list</i> }</code>	(Optional) configure VLANs allowed to pass by the Trunk interface.
6	<code>Raisecom(config- gigaethernet1/1/1)#switchport trunk untagged vlan { all [add remove] <i>vlan-list</i> }</code>	(Optional) configure VLANs from which the Trunk interface can remove Tag.



Note

- The interface allows Native VLAN packets to pass regardless of configuration in the VLAN list and untagged VLAN list allowed by the Trunk interface. The forwarded packets do not carry VLAN Tag.
- 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.
- If the configured Native VLAN is not default VLAN, and there is no default VLAN in the VLAN list allowed by the Trunk interface, the interface will not allow default VLAN packets to pass.
- 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 GVRP dynamic VLAN.

3.2.8 Configuring VLAN based on MAC address

Configure VLAN based on MAC address for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mac-vlan mac-address vlan vlan-id [priority value]</code>	Associate the MAC address with the VLAN.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
4	<code>Raisecom(config-gigaetherne1/1/1)#mac-vlan enable</code>	Enable VLAN based on MAC address.
5	<code>Raisecom(config-gigaetherne1/1/1)#vlan precedence { mac-vlan ip-subnet-vlan }</code>	(Optional) configure the priority of the VLAN based on MAC address and VLAN based on IP subnet.

Caution

- When the MAC address is the multicast MAC address, 0000-0000-0000, or FFFF-FFFF-FFFF, this configuration will fail.
- If the association between a created MAC address and the VLAN conflicts with an existing association (for example, a MAC address is associated with different VLANs), this configuration will fail.

3.2.9 Configuring VLAN based on IP subnet

Configure VLAN based on IP subnet for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip-subnet-vlan ip-address [ip-mask] vlan vlan-id [priority value]</code>	Associate the IP subnet with the VLAN.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.

Step	Command	Description
4	<code>Raisecom(config-gigaethernet1/1/1)#ip-subnet-vlan enable</code>	Enable VLAN based on IP subnet.
5	<code>Raisecom(config-gigaethernet1/1/1)#vlan precedence { mac-vlan ip-subnet-vlan }</code>	(Optional) configure the priority of the VLAN based on MAC address and VLAN based on IP subnet.

Caution

- When the IP address or subnet mask is invalid, this configuration will fail.
- If the association between a created IP subnet and the VLAN conflicts with an existing association (for example, an IP subnet is associated with different VLANs), this configuration will fail.

3.2.10 Checking configurations

Use the following commands to check configuration results.

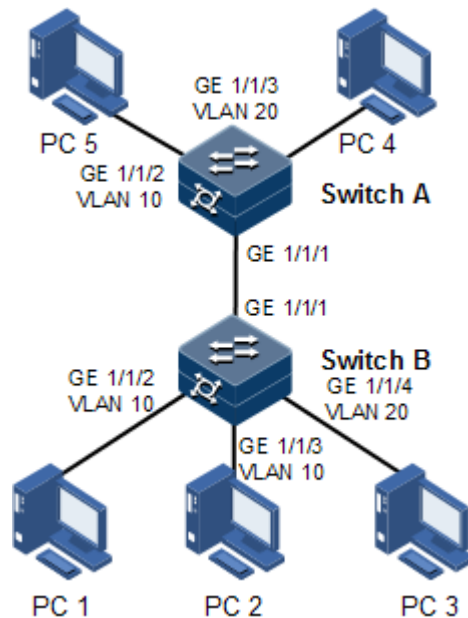
No.	Command	Description
1	<code>Raisecom#show vlan [vlan-list static dynamic] [detail]</code>	Show VLAN configurations.
2	<code>Raisecom#show switchport interface-type interface-number</code>	Show VLAN configurations on the interface.

3.2.11 Example for configuring VLAN

Networking requirements

As shown in Figure 3-4, 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 so that they cannot communicate with each other, but can respectively communicate with PC 5.

Figure 3-4 VLAN and interface protection networking



Configuration steps

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

Configure Switch A.

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

Configure Switch B.

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

Step 2 Add GE 1/1/2 and GE 1/1/3 as 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 gigaehternet1/1/2
SwitchB(config-gigaehternet1/1/2)#switchport mode access
SwitchB(config-gigaehternet1/1/2)#switchport access vlan 10
SwitchB(config-gigaehternet1/1/2)#exit
SwitchB(config)#interface gigaehternet1/1/3
SwitchB(config-gigaehternet1/1/3)#switchport mode access
SwitchB(config-gigaehternet1/1/3)#switchport access vlan 10
SwitchB(config-gigaehternet1/1/3)#exit
```

```
SwitchB(config)#interface gig Ethernet1/1/4
SwitchB(config-gig Ethernet1/1/4)#switchport mode access
SwitchB(config-gig Ethernet1/1/4)#switchport access vlan 20
SwitchB(config-gig Ethernet1/1/4)#exit
SwitchB(config)#interface gig Ethernet1/1/1
SwitchB(config-gig Ethernet1/1/1)#switchport mode trunk
SwitchB(config-gig Ethernet1/1/1)#switchport trunk allowed vlan 10
confirm
SwitchB(config-gig Ethernet1/1/1)#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 gig Ethernet1/1/2
SwitchA(config-gig Ethernet1/1/2)#switchport mode access
SwitchA(config-gig Ethernet1/1/2)#switchport access vlan 10
SwitchA(config-gig Ethernet1/1/2)#exit
SwitchA(config)#interface gig Ethernet1/1/3
SwitchA(config-gig Ethernet1/1/3)#switchport mode trunk
SwitchA(config-gig Ethernet1/1/3)#switchport trunk native vlan 20
SwitchA(config-gig Ethernet1/1/3)#exit
SwitchA(config)#interface gig Ethernet1/1/1
SwitchA(config-gig Ethernet1/1/1)#switchport mode trunk
SwitchA(config-gig Ethernet1/1/1)#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  --        P 1-6
2   VLAN0002         active  other   --        P 1-28
10  VLAN0010         active  static  --        gig Ethernet1/1/2
gig Ethernet1/1/3
20  VLAN0020         active  static  --        gig Ethernet1/1/4
```

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 gig Ethernet1/1/2
Interface: gig Ethernet1/1/2
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.

3.3 PVLAN

3.3.1 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 Promiscuous interface. The interface in the secondary VLAN is the Host interface.

- 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.

3.3.2 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.

3.3.3 Default configurations of PVLAN

Default configurations of PVLAN are as below.

Function	Default value
PVLAN mode on the interface	Access mode

3.3.4 Configuring PVLAN type

Configure the PVLAN type for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#private-vlan { primary vlan <i>vlan-id</i> isolated vlan <i>vlan-id</i> community vlan <i>vlan-list</i> }</code>	Configure the PVLAN type.



Caution

- Up to 32 primary VLANs and 2048 secondary VLANs are allowed.
- If the VLAN is associated, its PVLAN type cannot be modified nor deleted.

3.3.5 Configuring PVLAN association

Configure PVLAN association for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#private-vlan { primary vlan <i>vlan-id</i> isolated vlan <i>vlan-id</i> community vlan <i>vlan-list</i> }</code>	Configure the PVLAN type.
3	<code>Raisecom(config)#private-vlan association <i>primary-vlan-id</i> [add remove] <i>secondary-vlan-list</i></code>	Configuration association of the primary VLAN and secondary VLANs.

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 and the cluster VLAN.
- 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.

3.3.6 Configuring PVLAN mode on interface

The VLAN of the ISCOM3000G 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.
- 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 PVLAN mode on the interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-</i> <i>number</i></code>	Enter physical layer interface configuration mode.

Step	Command	Description
3	<code>Raisecom(config-gigaethernet1/1/*)#switchport mode private-vlan { host promiscuous }</code>	Configure PVLAN mode on the interface.
4	<code>Raisecom(config-gigaethernet1/1/*)#exit</code>	Return global configuration mode.
5	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
6	<code>Raisecom(config-gigaethernet1/1/*)#switchport private-vlan host-association primary-vlan-id secondary-vlan-id</code>	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.
7	<code>Raisecom(config-gigaethernet1/1/*)#switchport private-vlan mapping primary-vlan-id [add remove] secondary-vlan-list</code>	Configure 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.

3.3.7 Checking configuration

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show vlan private-vlan</code>	Show PVLAN configuration.
2	<code>Raisecom#show switchport interface interface-type interface-number</code>	Show configuration of interface VLAN attributes.
3	<code>Raisecom#show vlan [vlan-list static dynamic] [detail]</code>	Show configuration of VLAN attributes.

3.3.8 Example for configuring PVLAN

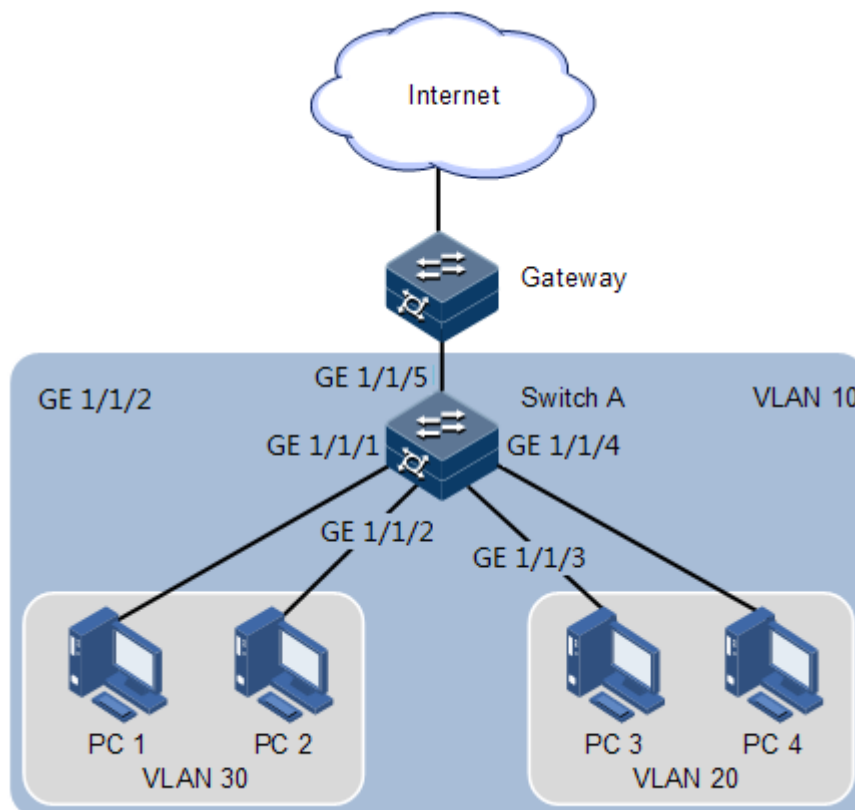
Networking requirements

To effectively distribute VLAN resources, you need to properly partition and configure VLANs. As shown in Figure 3-5, 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 Gigaethernet 1/1/1 and Gigaethernet 1/1/2 as community interfaces. Associate primary VLAN 10 with secondary VLAN 30.
- Configure Gigaethernet 1/1/3 and Gigaethernet 1/1/4 as isolated interfaces. Associate primary VLAN 10 with secondary VLAN 20.
- Configure Gigaethernet 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 Gigaethernet 1/1/1 and Gigaethernet 1/1/2 respectively, and they can communicate with these two interfaces and the promiscuous interface Gigaethernet 1/1/1.
- Connect PC 3 and PC 4 to isolated interfaces Gigaethernet 1/1/3 and Gigaethernet 1/1/4 respectively, and they can communicate with the promiscuous interface Gigaethernet 1/1/1 only.

Figure 3-5 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.

```
Raisecom(config)#interface gigabitEthernet 1/1/5
Raisecom(config-gigabitEthernet1/1/5)#switchport mode private-vlan
promiscuous
Raisecom(config-gigabitEthernet1/1/5)#switchport private-vlan mapping 10
20,30
Raisecom(config-gigabitEthernet1/1/5)#exit
```

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

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

```
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#switchport mode private-vlan host
Raisecom(config-gigabitEthernet1/1/1)#switchport private-vlan host-
association 10 30
Raisecom(config-gigabitEthernet1/1/1)#exit
Raisecom(config)#interface gigabitEthernet 1/1/3
Raisecom(config-gigabitEthernet1/1/3)#switchport mode private-vlan host
Raisecom(config-gigabitEthernet1/1/3)#switchport private-vlan host-
association 10 20
```

Checking results

Use the **show vlan private-vlan** command to show PVLAN configurations of the ISCOM3000G series switch.

```
Raisecom#show vlan private-vlan
VLAN ID: 10
Pvlan type: primary
Port-list: GE1/1/5,1/1/1-2
Associated-vlans: 20,30

VLAN ID: 20
Pvlan type: isolate
Port-list: GE1/1/5
Associated-vlans: 10

VLAN ID: 30
```

```
Pvlan type: community
Port-list: GE1/1/5,1/1/1
Associated-vlans: 10
```

Use the **show interface** *interface-type interface-number switchport* command to show configurations of VLAN attributes on promiscuous interface GigEthernet 1/1/5, community interface GigEthernet 1/1/1, and isolated interface GigEthernet 1/1/3.

```
Raisecom#show interface gigEthernet 1/1/5 switchport
Interface: gigEthernet1/1/5
Reject frame type: none
Administrative Mode: promiscuous
Operational Mode: promiscuous
Access Mode VLAN: 1
Administrative Access Egress VLANs:
Operational Access Egress VLANs: 1
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: N/A
Administrative Trunk Untagged VLANs:
Operational Trunk Untagged VLANs: N/A
Administrative private-vlan host-association: 1
Administrative private-vlan mapping: 10 20,30
Operational private-vlan: 10 20,30
```

```
Raisecom#show interface gigEthernet 1/1/1 switchport
Interface: gigEthernet1/1/1
Reject frame type: none
Administrative Mode: host
Operational Mode: host
Access Mode VLAN: 1
Administrative Access Egress VLANs:
Operational Access Egress VLANs: 1
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: N/A
Administrative Trunk Untagged VLANs:
Operational Trunk Untagged VLANs: N/A
Administrative private-vlan host-association: 10 30
Administrative private-vlan mapping: 1
Operational private-vlan: 10 30
```

```
Raisecom#show interface gigEthernet 1/1/3 switchport
Interface: gigEthernet 1/1/3
Reject frame type: none
Administrative Mode: host
Operational Mode: host
Access Mode VLAN: 1
Administrative Access Egress VLANs:
Operational Access Egress VLANs: 1
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: N/A
```

```
Administrative Trunk Untagged VLANs: N/A
Operational Trunk Untagged VLANs: N/A
Administrative private-vlan host-association: 10 20
Administrative private-vlan mapping: 1
Operational private-vlan: 10 20
```

3.4 Super VLAN

3.4.1 Introduction

The traditional ISP network assigns each customer an IP subnet. In this case, three IP addresses are used. They are the network ID, broadcasting address, and default gateway. If some unassigned IP addresses exist in the subnet of some customers, IP addresses are wasted.

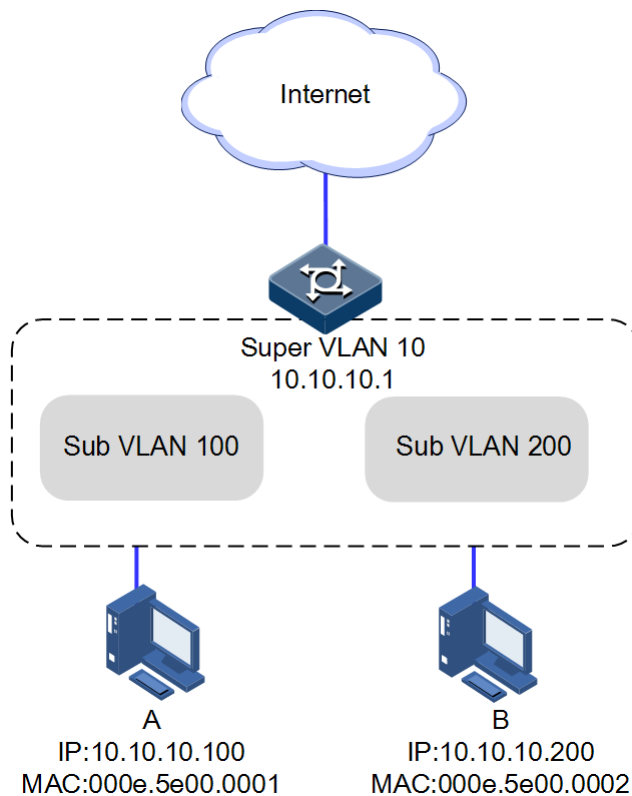
Super VLAN involves the super VLAN and sub-VLAN. A super VLAN is a set of multiple sub-VLANs. The super VLAN has the following features:

- Super VLAN: contain Layer 3 logic interfaces but physical interfaces. It is a set of multiple sub-VLANs.
- Sub-VLAN: contain physical interfaces but Layer 3 logic interfaces, use the IP address of the Layer 3 logical interface of the super VLAN as the default gateway to communicate with the external Layer 3 switch. Sub-VLANs are isolated from each other like common VLANs on the Layer 2.

ARP proxy refers to the process that a source host in a subnet of a physical network sends the ARP request to the destination host of a subnet of another physical network and the gateway connected to the source host sends ARP Reply message through the MAC address of its interface in replacement of the destination host.

As shown in Figure 3-6, a host in sub-VLAN 100 communicates with that in sub-VLAN 200. When super VLAN 10 is enabled with ARP proxy, its Layer 3 interface implements ARP learning, processing received and sent ARP packets, and ARP proxy.

Figure 3-6 Sub-VLAN and super VLAN partition



3.4.2 Preparing for configurations

Scenario

With super VLAN, hosts that are connected to the same switch but belong to different VLANs can communicate on Layer 3 by using the IP address of Layer 3 interface of the super VLAN as the default gateway.

Prerequisite

- After being configured, the super VLAN cannot contain any member interfaces. If a VLAN has member interfaces, it cannot be configured with attributes of super VLAN.
- Create a VLAN to be added to the super VLAN, and activate it. If the physical interface is taken as a Layer 3 interface by default, configure it as a Layer 2 interface.

3.4.3 Configuring super VLAN

Configure the super VLAN for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#create vlan vlan-id active</code>	Create a VLAN, and enter VLAN configuration mode.
3	<code>Raisecom(config- vlan)#supervlan</code>	Configure the VLAN as a super VLAN.

Step	Command	Description
4	Raisecom(config-vlan)# subvlan [add remove] <i>subvlan-id</i>	Configure sub-VLANs of the super VLAN.
5	Raisecom(config-vlan)# exit	Exit VLAN configuration mode.
6	Raisecom(config)# interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
7	Raisecom(config-vlan)# arp local-proxy enable	Enable local ARP proxy of the super VLAN.



Note

After the interface of the super VLAN is configured, configure its IP address. The VLAN belonging to the super VLAN is a sub-VLAN.
After being configured as a super VLAN, a VLAN cannot be configured with the VLAN interface and IP address.

3.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show supervlan [<i>vlan-id</i>]	Show configurations of super VLAN and sub-VLANs.
2	Raisecom# show ip interface brief	Show configurations of the IP address of the super VLAN.

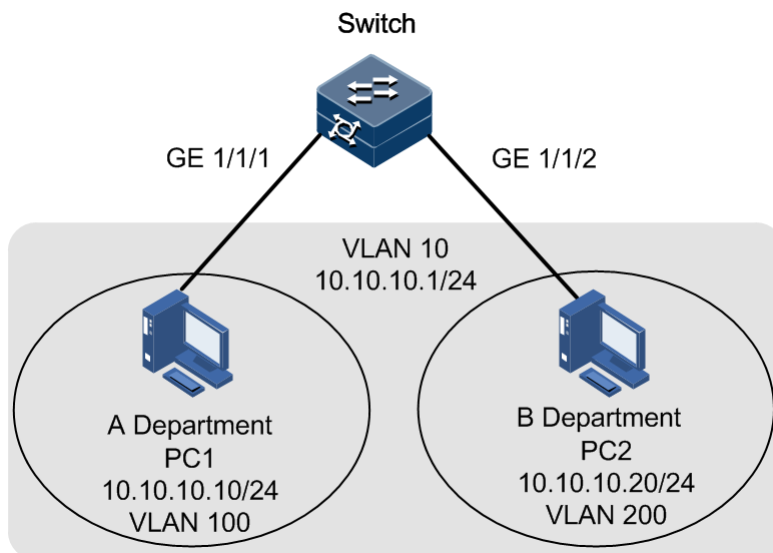
3.4.5 Example for configuring super VLAN

Networking requirements

PC 1 and PC 2 are in Department A and Department B of a company respectively. They are in different VLANs but need to communicate with each other. If you configure subnets for them respectively, excessive IP addresses will be wasted. By configuring super VLAN for Layer 3 communication, you can use less IP addresses than common VLAN mode.

As shown in Figure 3-7, PC 1 belongs to VLAN 100, and PC 2 belongs to VLAN 200. Add VLAN 100 and VLAN 200 to super VLAN 10 so that PC 1 in sub-VLAN 100 and PC 2 in sub-VLAN 200 can communicate through the gateway (10.10.10.1) of super VLAN 10.

Figure 3-7 Super VLAN networking



Configuration steps

Step 1 Create VLANs 10, 100, and 200. Add interfaces to them.

```
Raisecom#config
Raisecom(config)#create vlan 10,100,200 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport access vlan 100
Raisecom(config-gigaethernet1/1/1)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport access vlan 200
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 2 Configure VLAN 10 as a super VLAN.

```
Raisecom(config)#vlan 10
Raisecom(config-vlan)#supervlan
```

Step 3 Add sub-VLAN 100 and sub-VLAN 200 to super VLAN 10.

```
Raisecom(config-vlan)#subvlan add 100,200
Raisecom(config-vlan)#exit
```

Step 4 Configure the IP address of super VLAN 10.

```
Raisecom(config)#interface vlan 10
Raisecom(config-vlan10)#ip address 10.10.10.1 255.255.255.0
```

Step 5 Enable local ARP proxy of the super VLAN.

```
Raisecom(config-vlan10)#arp local-proxy enable
```

Checking results

Use the **show supervlan** command to show configurations of the super VLAN and sub-VLANs.

```
Raisecom#show supervlan
Supervlan ID    Subvlanlist
-----
10              100,200
```

Use the **show ip interface brief** command to show configurations of the interface of the super VLAN.

```
Raisecom#show ip interface brief
VRF              IF              Address          NetMask          Catagory
-----
Default-IP-Routing-Table  vlan10          10.10.10.1      255.255.255.0
primary
```

Configure the default gateway of PC 1 to 10.10.10.1. Use the **ping** command to check whether PC 1 can ping through PC 2.

```
C:\Users\administrator>ping 10.10.10.20
```

```
Pinging 10.10.10.20 with 32 bytes of data:
Reply from 10.10.10.20: bytes=32 time<1ms TTL=64
Reply from 10.10.10.20: bytes=32 time<1ms TTL=64
Reply from 10.10.10.20: bytes=32 time<1ms TTL=64
Reply from 10.10.10.20: bytes=32 time<1ms TTL=64
```

```
Ping statistics for 10.10.10.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3.5 QinQ

3.5.1 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 3-8 Principles of basic QinQ

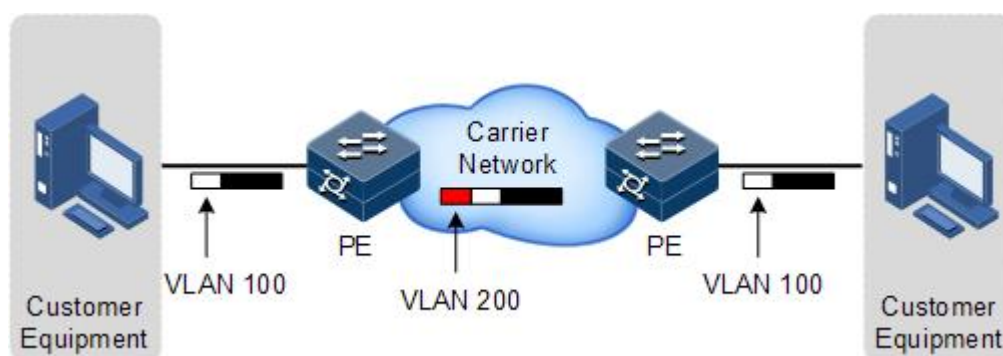


Figure 3-8 shows typical networking of basic QinQ; wherein, the ISCOM3000G series switch is the PE.

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.

Selective QinQ

Selective QinQ is an enhancement to basic QinQ, which classifies flow according to user data features, then encapsulates different types of flows 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.

3.5.2 Preparing for configurations

Scenario

Basic QinQ configuration and selective QinQ configuration for the ISCOM3000G 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 the VLAN ID on the SP 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 IDs on the user network which are divided by adding different outer VLAN Tags 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

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

3.5.3 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

3.5.4 Configuring basic QinQ

Configure basic QinQ on the ingress interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaetherne1/1/1)#dot1q-tunnel</code>	Enable basic QinQ on the interface.
4	<code>Raisecom(config-gigaetherne1/1/1)#switchport qinq default-cvlan <i>vlan-id</i></code>	Configure basic QinQ, add double Tags, and specify the PVID used by the CVLAN and SVLAN.
5	<code>Raisecom(config-gigaetherne1/1/1)#switchport reject-frame { tagged untagged }</code>	Configure the types of packets disallowed to be forwarded.



Note

- To configure basic QinQ 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.

3.5.5 Configuring selective QinQ

Configure selective QinQ on the user side interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface gigaetherne1/1/1</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaetherne1/1/1)#switchport vlan-mapping-miss discard</code>	Configure the interface to discard tagged packets that fail to match selective QinQ or VLAN mapping rules.
4	<code>Raisecom(config-gigaetherne1/1/1)#switchport vlan-mapping ethertype { arp eapol flowcontrol ip ipv6 / loopback mpls mpls-mcast pppoe pppodisc user-define <i>protocol id</i> x25 x75 }add-outer <i>outer-vlan-id</i></code>	Configure EtherType selective QinQ, and add mapping rules for Tag VLAN.

Step	Command	Description
5	<pre>Raisecom(config- gigaethernet1/1/1)#switchport vlan- mapping both priority-tagged [cos cos-value] add-outer outer-vlan-id [cos cos-value] [remove translate vlan-id] Raisecom(config- gigaethernet1/1/1)#switchport vlan- mapping both cvlan custom-vlan-list [cos cos-value] add-outer outer- vlan-id [cos cos-value] { remove translate vlan-id } Raisecom(config- gigaethernet1/1/1)#switchport vlan- mapping both { untag inner inner- vlan-id } add-outer outer-vlan-id [cos cos-value]</pre>	Configure bidirectional selective QinQ, and add outer VLAN rules.



Note

Double-tagged VLAN mapping cannot be concurrently configured with basic QinQ or tagged CVLAN/Priority-tagged VLAN mapping on the same interface. Before configuring selective QinQ and specifying CoS of the outer VLAN, configure basic QinQ.

3.5.6 Configuring network-side interface to Trunk mode

Configure the network-side interface to Trunk mode for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/1)#switchport mode trunk</code>	Configure interface trunk mode, permit double-tagged packet to pass.

3.5.7 Configuring TPID

Configure TPID on the network side interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.

Step	Command	Description
3	Raisecom(config-gigaetherne1/1/1)# tpid <i>tpid</i>	Configure the TPID of the outer VLAN Tag on the interface.

3.5.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show dot1q-tunnel	Show configurations of basic QinQ.
2	Raisecom# show vlan-mapping both interface <i>interface-number</i>	Show configurations of selective QinQ.
3	Raisecom# show vlan-mapping interface <i>interface-type interface-number</i>	Show configurations of selective QinQ of EtherType on the interface.

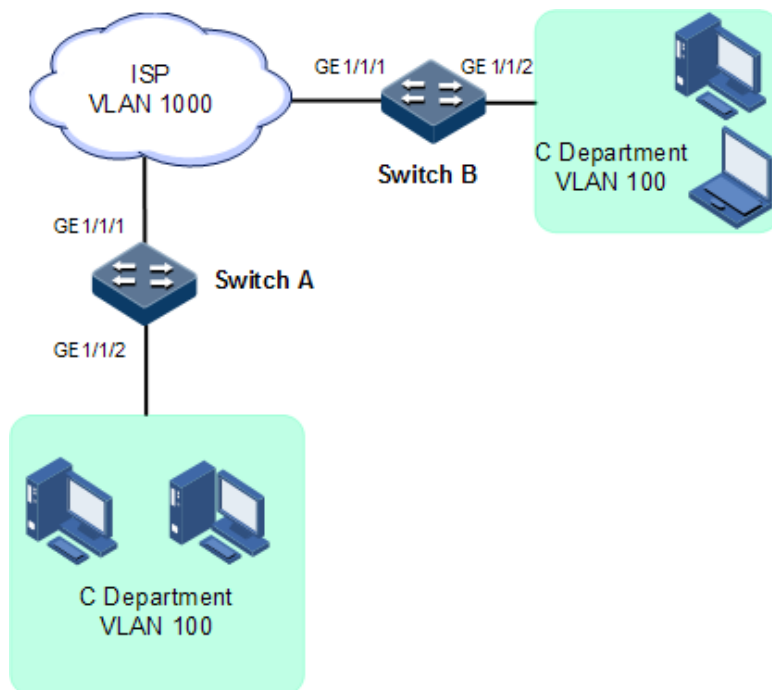
3.5.9 Example for configuring basic QinQ

Networking requirements

As shown in Figure 3-9, Switch A and Switch B are connected to two branches of Department C, which need to communicate through VLAN 1000 of the carrier network. Department C uses VLAN 100. 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 3-9 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, VLAN 200, and VLAN 1000, and activate them. TPID is 9100.

```
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-tengigabitethernet1/1/2)#switchport mode trunk
Raisecom(config-tengigabitethernet1/1/2)#switchport trunk native vlan 1000
Raisecom(config-tengigabitethernet1/1/2)#dot1q-tunnel
Raisecom(config-tengigabitethernet1/1/2)#switchport qinq default-cvlan 100
Raisecom(config-tengigabitethernet1/1/2)#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
-----
gigaethernet1/1/1  -           0x9100          -            disable
gigaethernet1/1/2  Dot1q-tunnel 0x8100          -            disable
```

3.5.10 Example for configuring selective QinQ

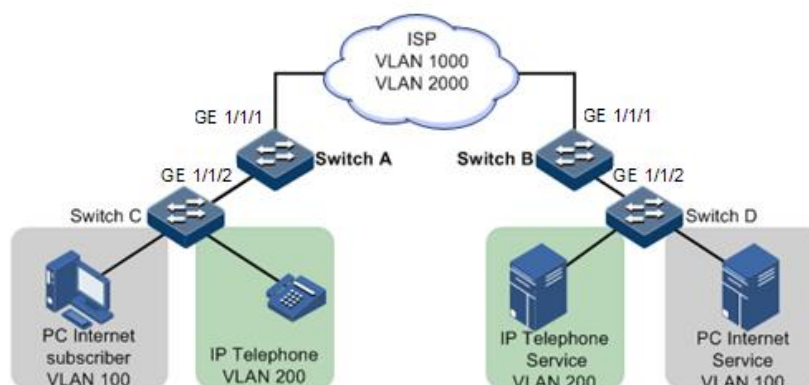
Networking requirements

As shown in Figure 3-10, 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.

Figure 3-10 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#name SwitchA
```

```
SwitchA#config
SwitchA(config)#create vlan 100,200,1000,2000 active
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/1)#switchport trunk allowed vlan 1000,2000
SwitchA(config-gigabitEthernet1/1/1)#tpid 9100
SwitchA(config-gigabitEthernet1/1/1)#exit
```

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

```
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#switchport mode trunk
Raisecom(config-gigabitEthernet1/1/2)#switchport trunk allowed vlan
100,200,1000,2000
SwitchA(config-gigabitEthernet1/1/2)#switchport vlan-mapping both
inner 100 add-outer 1000
SwitchA(config-gigabitEthernet1/1/2)#switchport vlan-mapping both
inner 200 add-outer 2000
SwitchA(config-gigabitEthernet1/1/2)#exit
```

Checking results

Use the **show switchport interface interface-type interface-number vlan-mapping add-outer** command to show configurations of selective QinQ.

Take Switch A for example.

```
SwitchA#show vlan-mapping both interface gigabitEthernet 1/1/1
Based inner VLAN flexible QinQ mapping rule:
Interface          CVLAN   Add-SVlan   Cos   CVlan-Action Translate-
CVlan Hardware
-----
gigabitEthernet1/1/1  100     1000       0     Reserve   -
Yes
gigabitEthernet1/1/2  200     2000       0     Reserve   -
Yes
```

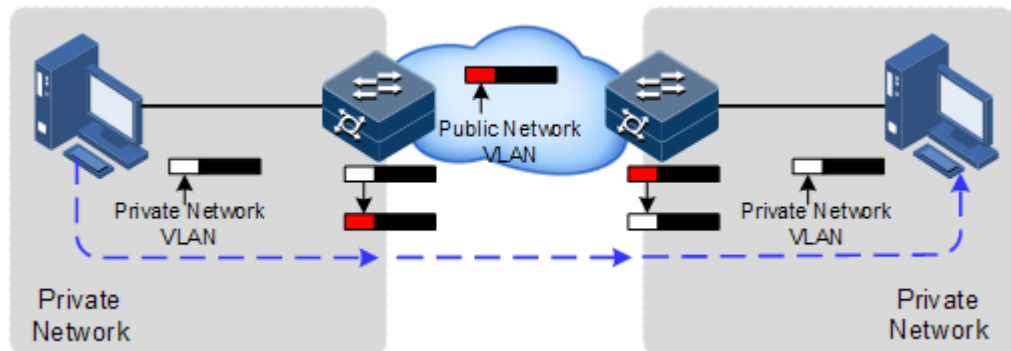
3.6 VLAN mapping

3.6.1 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 3-11 shows principles of VLAN mapping.

Figure 3-11 Principles of VLAN mapping



After receiving a user private network packet with a VLAN Tag, the ISCOM3000G 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 ISCOM3000G 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.

3.6.2 Preparing for configurations

Scenario

Different from QinQ, VLAN mapping is 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 interfaces.
- Configure its physical parameters to make it Up.
- Create VLANs.

3.6.3 Default configurations of VLAN mapping

Default configurations of VLAN mapping are as below.

Function	Default value
VLAN mapping status	Disable

3.6.4 Configuring VLAN mapping

Configure VLAN mapping for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaetherne t1/1/1)#switchport vlan-mapping both outer <i>vlan-id</i> translate outer <i>vlan-id</i> Raisecom(config-gigaetherne t1/1/1)#switchport vlan-mapping both outer <i>vlan-id</i> inner <i>inner -vlan-id</i> translate outer <i>vlan-id</i> inner <i>inner -vlan-id</i>	Configure the VLAN mapping rule based on outer and inner VLAN Tag in both the ingress and egress directions of the interface.
4	Raisecom(config-gigaetherne t1/1/1)#switchport vlan-mapping both <i>vlan-list</i> translate <i>vlan-id</i>	Configure N:1 VLAN mapping rules in both directions.



Note

- Double-tagged VLAN mapping cannot be concurrently configured with basic QinQ or tagged CVLAN/Priority-tagged VLAN mapping on the same interface.
- To concurrently configure N:1 VLAN mapping and VLAN copy, you must configure VLAN copy first and then configure N:1 VLAN mapping.
- To concurrently configure N:1 VLAN mapping and PIM, you must configure PIM first and then configure N:1 VLAN mapping.

3.6.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show vlan-mapping both interface <i>interface-type interface-number</i>	Show configurations of VLAN mapping.
2	Raisecom#show vlan-mapping interface <i>interface-type interface-number</i> both translate	Show configurations of N:1 VLAN mapping.

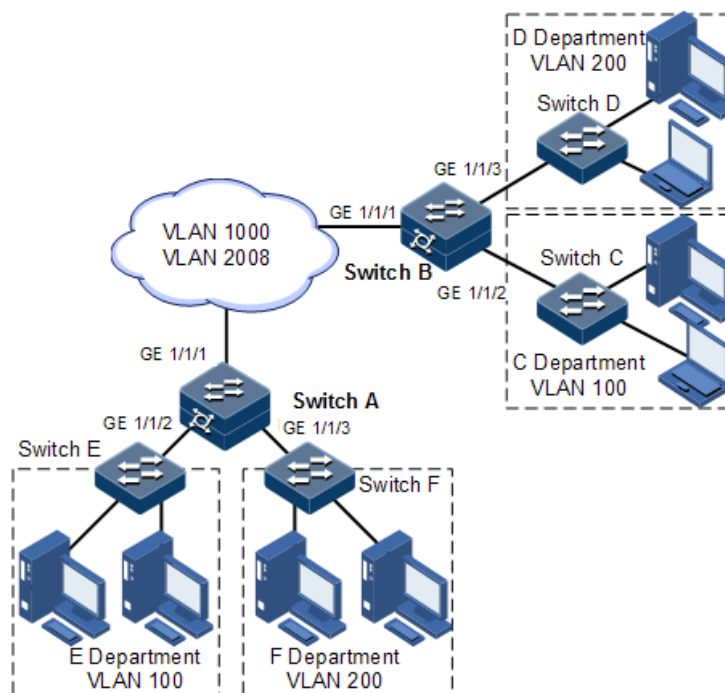
3.6.6 Example for configuring VLAN mapping

Scenario

As shown in Figure 3-12, 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 3-12 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.

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

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

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

```
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/1)#switchport trunk allowed vlan 1000,2008
confirm
SwitchA(config-gigabitEthernet1/1/1)#exit
```

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

```
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/2)#switchport trunk allowed vlan 100
confirm
SwitchA(config-gigabitEthernet1/1/2)#switchport vlan-mapping both outer 100
translate 1000
SwitchA(config-gigabitEthernet1/1/2)#exit
```

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

```
SwitchA(config)#interface gigabitEthernet 1/1/3
SwitchA(config-gigabitEthernet1/1/3)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/3)#switchport trunk allowed vlan 200
confirm
SwitchA(config-gigabitEthernet1/1/3)#switchport vlan-mapping both outer 200
translate 2008
```

Checking results

Use the **show vlan-mapping both interface gigabitEthernet 1/1/2** command to show configurations of 1:1 VLAN mapping.

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

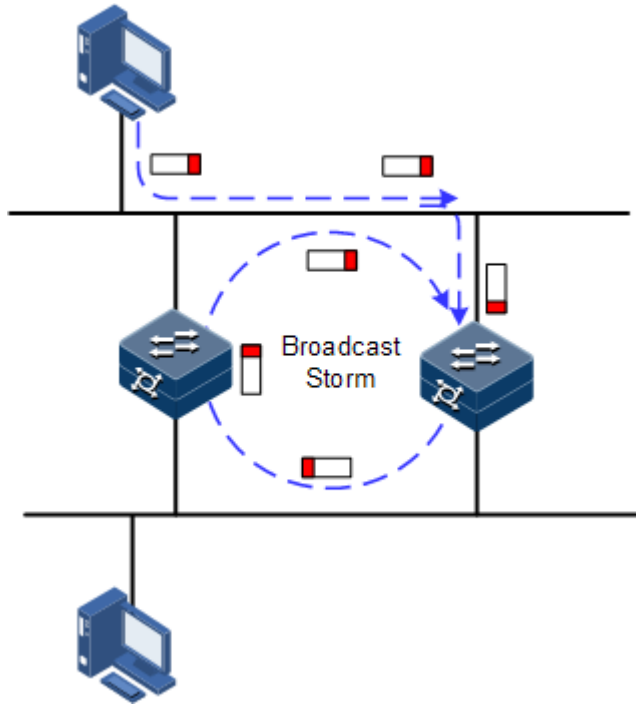
3.7 STP/RSTP

3.7.1 Introduction

STP

With the increasing complexity of network structure and growing number of switches on the network, Ethernet loops become the most prominent problem. Because of the packet broadcast mechanism, a loop causes the network to generate storms, exhausts network resources, and impacts forwarding normal data seriously. The network storm caused by the loop is shown in Figure 3-13.

Figure 3-13 Network storm due to loopback

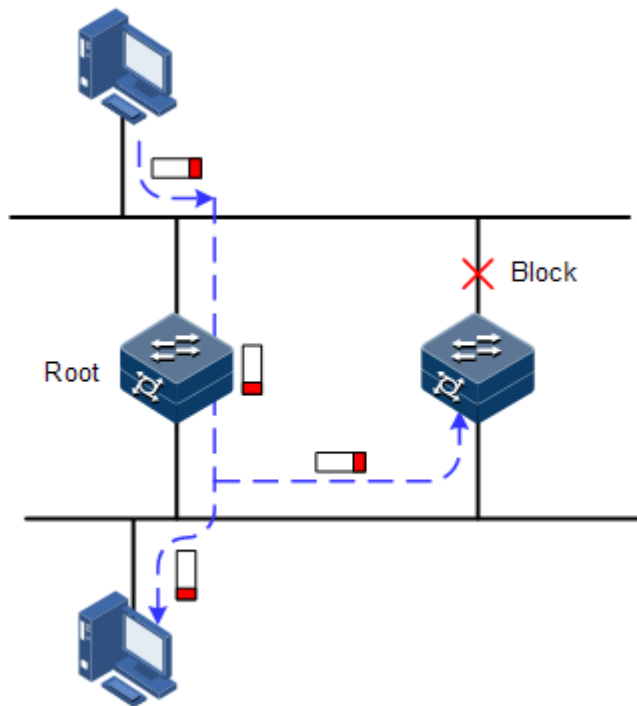


Spanning Tree Protocol (STP) is compliant to IEEE 802.1d standard and used to remove data physical loop in data link layer in the LAN.

The ISCOM3000G 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 ISCOM3000G series switch logically according to the selection results, and finally trims the loop network structure to tree network structure without loops which takes an ISCOM3000G 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 3-14 shows loop networking running STP.

Figure 3-14 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 rate.

RSTP

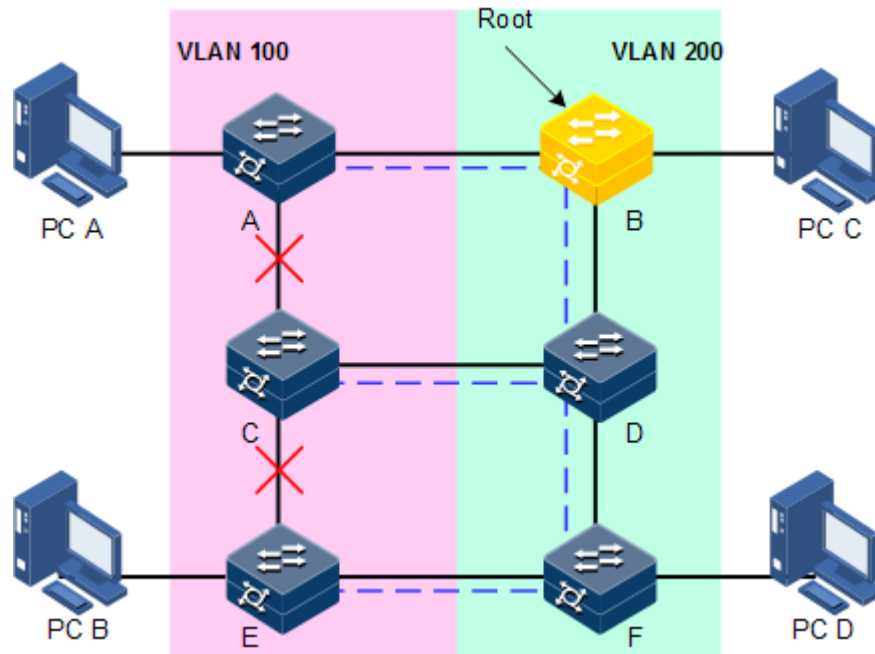
To improve the slow convergence rate of STP, IEEE 802.1w establishes Rapid Spanning Tree Protocol (RSTP), which increases the mechanism to transfer interface blocking state to forwarding state, speed up the topology convergence rate.

The purpose of STP/RSTP is to simplify a bridged LAN to a single 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 single 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 3-15, 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.

Figure 3-15 VLAN packet forward failure due to RSTP



3.7.2 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 loops, 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

3.7.3 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

Function	Default value
Forward Delay timer	15s

3.7.4 Enabling STP

Enable STP for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree enable	Enable global STP.
3	Raisecom(config)#spanning-tree mode { stp rstp }	Configure spanning tree mode.
4	Raisecom(config)#interface interface-type interface-number	Enter physical layer interface configuration mode.
5	Raisecom(config-gigaethernet1/1/1)#spanning-tree enable	Enable interface STP.

3.7.5 Configuring STP parameters

Configure STP parameters for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree priority priority-value	(Optional) configure device priorities.
3	Raisecom(config)#spanning-tree root { primary secondary }	(Optional) configure the ISCOM3000G series switch as the root or backup device.
4	Raisecom(config)#interface interface-type interface-number Raisecom(config-gigaethernet1/1/1)#spanning-tree priority priority-value	(Optional) configure interface priorities on the ISCOM3000G series switch.
5	Raisecom(config-gigaethernet1/1/1)#spanning-tree extern-path-cost cost-value Raisecom(config-gigaethernet1/1/1)#exit	(Optional) configure the path cost of interfaces on the ISCOM3000G series switch.
6	Raisecom(config)#spanning-tree hello-time value	(Optional) configure the value of Hello Time.
7	Raisecom(config)#spanning-tree transit-limit value	(Optional) configure the maximum transmission rate of the interface

Step	Command	Description
8	<code>Raisecom(config)#spanning-tree forward-delay <i>value</i></code>	(Optional) configure forward delay.
9	<code>Raisecom(config)#spanning-tree max-age <i>value</i></code>	(Optional) configure the maximum age.

3.7.6 (Optional) configuring RSTP 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 quickly transfer to the 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 ISCOM3000G series switch are configured in auto-detection attribute.

Configure the edge interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/1)#spanning-tree edged-port { auto force-true force-false }</code>	Configure attributes of the RSTP edge interface.

3.7.7 (Optional) configuring RSTP 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 link type for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#spanning-tree link-type { auto point-to-point shared }</code>	Configure link type for interface.

3.7.8 Checking configurations

Use the following commands to check configuration results.

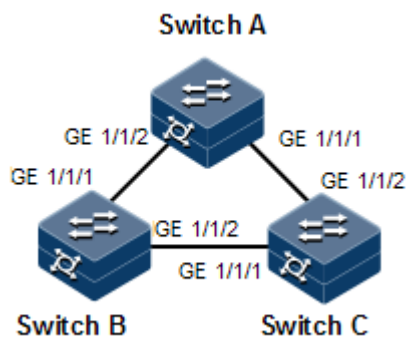
No.	Command	Description
1	<code>Raisecom#show spanning-tree</code>	Show basic configurations of STP.
2	<code>Raisecom#show spanning-tree interface-type interface-list [detail]</code>	Show STP configuration on the interface.

3.7.9 Example for configuring STP

Networking requirements

As shown in Figure 3-16, 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.

Figure 3-16 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 gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/1)#exit
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/2)#exit
```

Configure Switch B.

```
SwitchB(config)#interface gigabitEthernet 1/1/1
SwitchB(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchB(config-gigabitEthernet1/1/1)#exit
SwitchB(config)#interface gigabitEthernet 1/1/2
SwitchB(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchB(config-gigabitEthernet1/1/2)#exit
```

Configure Switch C.

```
SwitchC(config)#interface gigabitEthernet 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
Spanning-tree admin state: enable
Spanning-tree protocol mode: STP

BridgeId:    Mac 000E.5E7B.C557  Priority 0
Root:        Mac 000E.5E7B.C557  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
ExternPathCost:200000
```

```
Partner STP Mode: stp
Bpdus send: 0 (TCN<0> Config<0> RST<0> MST<0>)
Bpdus received:0 (TCN<0> Config<0> RST<0> MST<0>)
State:blocking Role:non-designated Priority:128 Cost: 200000
Root: Mac 0000.0000.0000 Priority 0 RootCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0
```

3.8 MSTP

3.8.1 Introduction

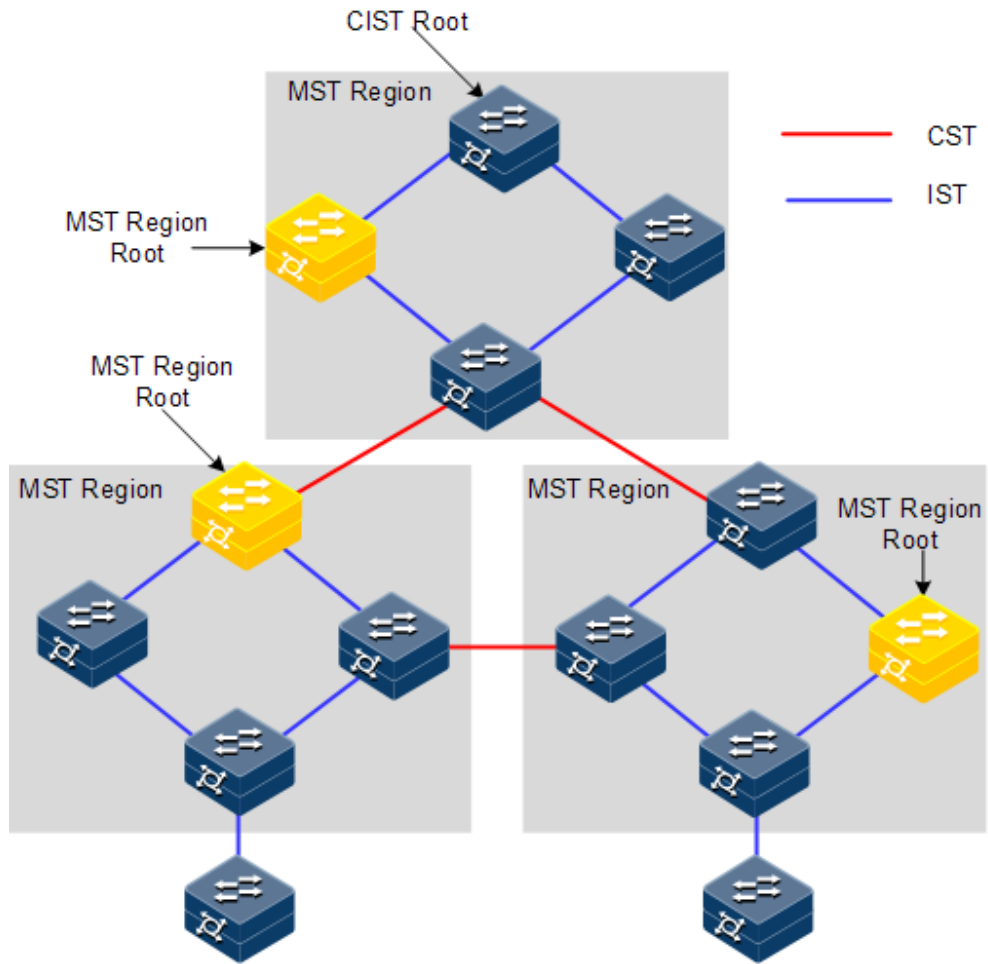
Multiple Spanning Tree Protocol (MSTP) is defined by IEEE 802.1s. Offsetting the disadvantages of STP and RSTP, the MSTP implements fast convergence and distributes different VLAN flow following its own path to provide an excellent load balancing mechanism.

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

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

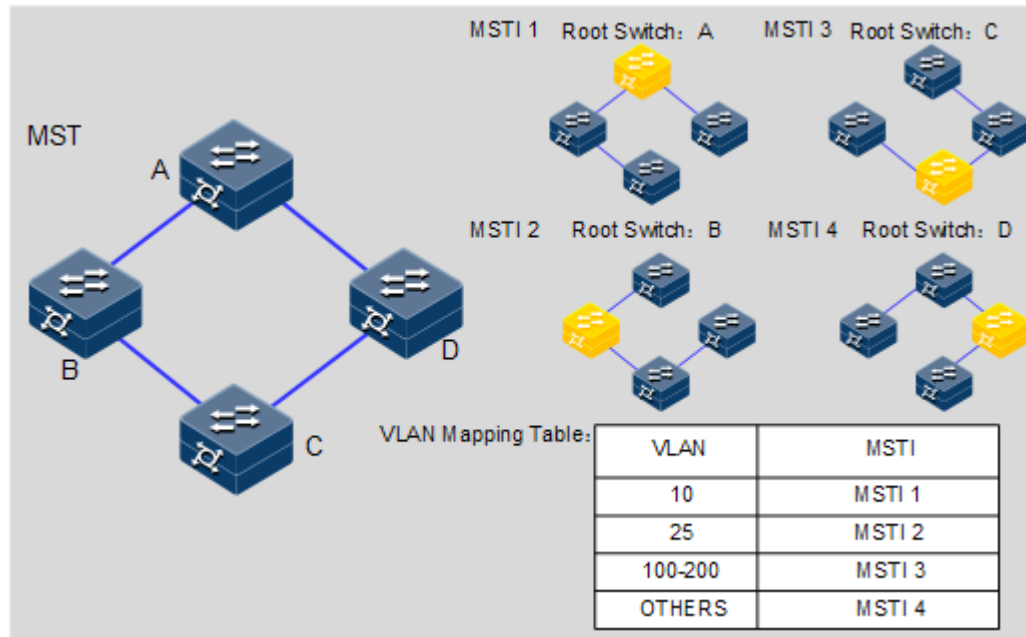
Compared with STP and RSTP, MSTP also introduces total root (CIST Root) and domain root (MST Region Root) concepts. The total root is a global concept; all switches running STP/RSTP/MSTP can have only one total root, which is the CIST Root. The domain root is a local concept, which is related to an instance in a domain. As shown in Figure 3-17, all connected devices only have one total root, and the number of domain roots contained in each domain is associated with the number of instances.

Figure 3-17 Basic concepts of the MSTI network



There can be different MST instances in each MST domain, which associates VLAN and MSTI by configuring the VLAN mapping table (relation table of VLAN and MSTI). The concept sketch map of MSTI is shown in Figure 3-18.

Figure 3-18 MSTI concepts

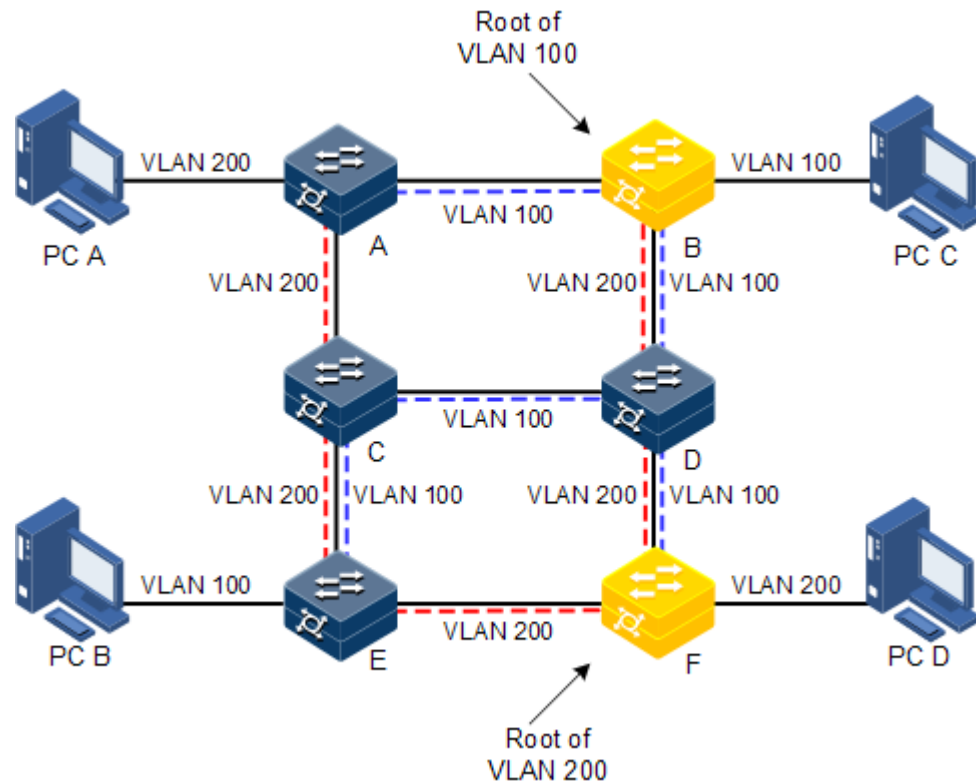


 **Note**

Each VLAN can map to one MSTI; namely, 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.

Figure 3-19 Networking with multiple spanning trees instances in MST domain



Apply MSTP to the network as shown in Figure 3-19. 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.

3.8.2 Preparation for configuration

Scenario

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

Prerequisite

N/A

3.8.3 Default configurations of MSTP

Default configurations of MSTP are as below.

Function	Default value
Global MSTP status	Disable
Interface MSTP status	Enable
Maximum numbers of hops in the MST domain	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 MST domain	0

3.8.4 Enabling MSTP

Enable MSTP for the ISCOM3000G 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	Enable global STP.
4	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	Raisecom(config- gigaethernet1/1/1)#spanning-tree enable	Enable interface STP.

3.8.5 Configuring MST domain and its maximum number of hops

You can configure domain information about the ISCOM3000G series switch when it is running in MSTP mode. The device MST domain is determined by the domain name, VLAN mapping table and configuration of MSTP revision level. You can configure current device in a specific MST domain through following configuration.

MST domain scale is restricted by the maximum number of hops. Starting from the root bridge of spanning tree in the domain, the configuration message (BPDU) reduces 1 hop count when it is forwarded passing a device; the ISCOM3000G 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 and then restrict MST domain scale.

Configure MSTP domain and its maximum number of hops for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree region-configuration	Enter MST domain configuration mode.
3	Raisecom(config-region)#name <i>name</i>	Configure MST domain name.
4	Raisecom(config-region)#revision-level <i>level-value</i>	Configure revision level for MST domain.
5	Raisecom(config-region)#instance <i>instance-id</i> vlan <i>vlan-list</i> Raisecom(config-region)#exit	Configure mapping from MST domain VLAN to instance.
6	Raisecom(config)#spanning-tree max-hops <i>hops-value</i>	Configure the maximum number of hops for MST domain.



Note

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

3.8.6 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 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, when 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 root bridge or backup bridge for the ISCOM3000G series switch as below.

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

Step	Command	Description
2	Raisecom(config)# spanning-tree [instance <i>instance-id</i>] root { primary secondary }	Configure the ISCOM3000G series switch as the root bridge or backup bridge of a STP instance.



Note

- You can confirm the effective instance of root bridge or backup bridge through the **instance** *instance-id* parameter. The current device will be assigned as 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; namely, 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.
- 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.

3.8.7 Configuring interface priority and system priority

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

The Bridge ID determines whether the ISCOM3000G series switch can be selected as the root of the spanning tree. Configuring smaller priority helps obtain smaller Bridge ID and designate the ISCOM3000G series switch as the root. If priorities of two ISCOM3000G series switch devices are identical, the ISCOM3000G series switch with lower MAC address will be selected 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 interface priority and system priority for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)# spanning-tree [instance <i>instance-id</i>] priority <i>priority-value</i> Raisecom(config- gigaethernet1/1/1)# exit	Configure interface priority for a STP instance.

Step	Command	Description
4	<code>Raisecom(config)#spanning-tree [instance <i>instance-id</i>] priority <i>priority-value</i></code>	Configure system priority for a STP instance.



Note

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

3.8.8 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 domain, it is considered as just one node. Actually, network diameter should be defined as the domain number in the path crossing the most domains. The network diameter is 1 if there is only one domain in the whole network.

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

Similar to the maximum number of hops of MST domain, only when the ISCOM3000G 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#spanning-tree bridge-diameter <i>bridge-diameter-value</i></code>	Configure the network diameter for the switching network.

3.8.9 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 the interface are mutually independent in different instances. You can configure internal path cost for instance through the **instance** *instance-id* parameter. Configure the internal path cost of the 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#spanning-tree [instance <i>instance-id</i>] inter-path-cost <i>cost-value</i>	Configure the internal path cost of the interface.

3.8.10 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 domain.

Configure the external path cost for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#spanning-tree extern-path-cost <i>cost-value</i>	Configure the external path cost of the interface.

3.8.11 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 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 maximum transmission rate on the interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree transit-limit <i>value</i>	Configure the maximum transmission rate on the interface.

3.8.12 Configuring MSTP timer

- **Hello Time:** the ISCOM3000G series switch sends the interval of bridge configurations (BPDU) regularly to check whether there is failure in detection link of the ISCOM3000G series switch. The ISCOM3000G 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; namely, 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 ISCOM3000G 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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#spanning-tree hello-time <i>value</i></code>	Configure Hello Time.
3	<code>Raisecom(config)#spanning-tree forward-delay <i>value</i></code>	Configure Forward Delay.
4	<code>Raisecom(config)#spanning-tree max-age <i>value</i></code>	Configure Max Age.

3.8.13 Configuring edge interface

The edge interface indicates the interface neither directly connected to any devices nor indirectly connected 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 ISCOM3000G series switch are configured in auto-detection attribute.

Configure the edge interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#spanning-tree edged-port { auto force-true force-false }</code>	Configure attributes of the RSTP edge interface.

3.8.14 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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#spanning-tree edged-port bpdu-filter enable interface-type interface-number</code>	Enable BPDU filtering on the edge interface.

3.8.15 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.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#spanning-tree bpduguard enable</code>	Enable BPDU Guard.

Step	Command	Description
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
4	<code>Raisecom(config- gigaethernet1/1/1)#no spanning- tree bpduguard shutdown port</code>	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.

3.8.16 Configuring STP/RSTP/MSTP mode switching

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

- STP compatible mode: the ISCOM3000G series switch does not implement expedited 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 ISCOM3000G series switch implements expedited 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 ISCOM3000G 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 domain.

Configure the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#spanning- tree mode { stp rstp mstp }</code>	Configure spanning tree mode.

3.8.17 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 link type for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#spanning-tree link-type { auto point-to-point shared }	Configure link type for interface.

3.8.18 Configuring root interface protection

The network will select a bridge again when it receives a packet with higher priority, which affects network connectivity and also consumes CPU resource. For the MSTP network, if BPDUs with higher priority are sent to attack the network, 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#spanning-tree rootguard enable	Enable/Disable root interface protection.

3.8.19 Configuring interface loopguard

The spanning tree has two functions: loopguard and link backup. Loopguard requires trimming the network topology into tree structure. There must be redundant link 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. It regards the link as faulty if it has not received packets in a period. Then it selects a new link and enables backup interface. In actual networking, the cause to failure in receiving packets may not link faults. In this case, enabling the backup interface may lead to a 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; namely, loopguard is implemented on the cost of disabling link backup.

Configure interface loop protection for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#spanning-tree loopguard enable	Configure interface loopguard attributes.

3.8.20 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show spanning-tree	Show basic configurations of STP.
2	Raisecom#show spanning-tree [instance <i>instance-id</i>] <i>interface-type interface-list</i> [detail]	Show configurations of spanning tree on the interface.
3	Raisecom#show spanning-tree region-operation	Show operation information about the MST domain.
4	Raisecom(config-region)#show spanning-tree region- configuration	Show configurations of MST domain.
5	Raisecom(config- gigaethernet1/1/1)#spanning-tree mcheck	Configure the interface to MSTP mode to check whether the peer device supports MSTP.

3.8.21 Maintenance

Maintain the ISCOM3000G series switch as below.

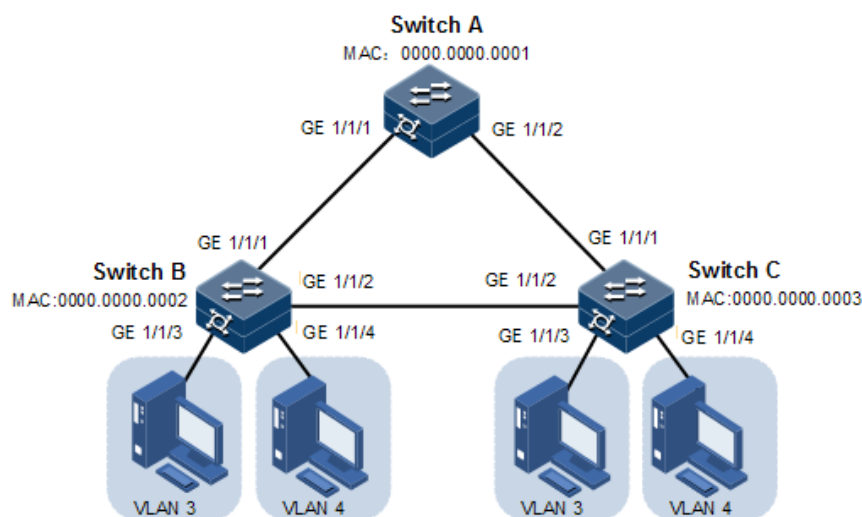
Command	Description
Raisecom(config-gigaethernet1/1/1)#spanning-tree clear statistics	Clear statistics about spanning tree on the interface.

3.8.22 Example for configuring MSTP

Networking requirements

As shown in Figure 3-20, three ISCOM3000G series switch devices are connected to form a ring network through MSTP, with the domain 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.

Figure 3-20 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#name SwitchA
SwitchA#config
SwitchA(config)#create vlan 3,4 active
```

Configure Switch B.

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


Configure Switch C.

```
Raisecom#name 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 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 gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/1)#exit
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchA(config-gigabitEthernet1/1/2)#exit
```

Configure Switch B.

```
SwitchB(config)#interface gigabitEthernet 1/1/1
SwitchB(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchB(config-gigabitEthernet1/1/1)#exit
SwitchB(config)#interface gigabitEthernet 1/1/2
SwitchB(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchB(config-gigabitEthernet1/1/2)#exit
SwitchB(config)#interface gigabitEthernet 1/1/3
SwitchB(config-gigabitEthernet1/1/3)#switchport access vlan 3
SwitchB(config-gigabitEthernet1/1/3)#exit
SwitchB(config)#interface gigabitEthernet 1/1/4
SwitchB(config-gigabitEthernet1/1/4)#switchport access vlan 4
SwitchB(config-gigabitEthernet1/1/4)#exit
```

Configure Switch C.

```
SwitchC(config)#interface gigabitEthernet 1/1/1
SwitchC(config-gigabitEthernet1/1/1)#switchport mode trunk
SwitchC(config-gigabitEthernet1/1/1)#exit
SwitchC(config)#interface gigabitEthernet 1/1/2
SwitchC(config-gigabitEthernet1/1/2)#switchport mode trunk
SwitchC(config-gigabitEthernet1/1/2)#exit
SwitchC(config)#interface gigabitEthernet 1/1/3
SwitchC(config-gigabitEthernet1/1/3)#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 domain name to aaa, revised version to 0. Map instance 3 to VLAN 3, and instance 4 to VLAN 4. Exit from MST configuration mode.

Configure Switch A.

```
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 1/1/1 of spanning tree instance 3 to 500000 on Switch B.

```
SwitchB(config)#interface gigaethernet 1/1/1
```

```
SwitchB(config-gigaethernet)#spanning-tree instance 3 inter-path-cost  
500000
```

Checking results

Use the **show spanning-tree region-operation** command to show configurations of the MST domain.

Take Switch A for example.

```
SwitchA#show spanning-tree region-operation  
Operational Information:
```

```
-----  
Name: aaa  
Revision level: 0  
Instances running: 3  
Digest: 0x024E1CF7E14D5DBBD9F8E059D2C683AA  
Instance  Vlans Mapped  
-----  
0          1-2,5-4094  
3          3  
4          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
```

```
MST ID: 3
```

```
-----  
BridgeId:   Mac 000E.5E11.2233 Priority 32768  
RegionalRoot: Mac 000E.5E11.2233 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
```

```
MST ID: 4
```

```
-----  
BridgeId:   Mac 000E.5E11.2233 Priority 32768  
RegionalRoot: Mac 000E.5E11.2233 Priority 32768 InternalRootCost 0  
Port      PortState  PortRole  PathCost  PortPriority  LinkType  
-----
```

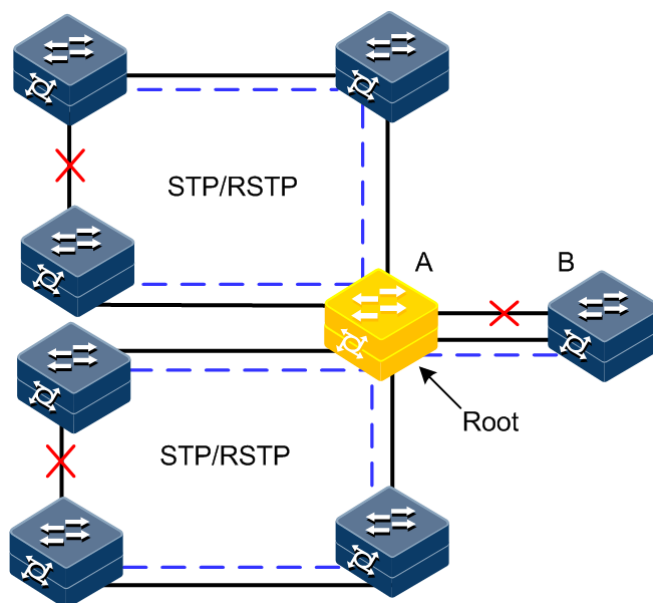
3.9 MRSTP

3.9.1 Introduction

RSTP aims to trim a bridged LAN to a logical single spanning tree. A tree network must have a root, so the concept of the root bridge is introduced. There is only one root bridge on the entire network while other devices are called leaf nodes.

As shown in Figure 3-21, when running RSTP, device B is generally elected as the root bridge. When these ring networks do not wish or fit to run MSTP, device A is specified as the root bridge of the ring network while device B is the root bridge of device A. You can create multiple MRSTP processes on device A and bind the interfaces connecting these ring networks to the specified processes. In this case, when devices on these ring networks, they will elect device A as the root bridge of each ring network while device A will elect device B as its root bridge.

Figure 3-21 Configuring MRSTP for specifying root bridge



3.9.2 Preparing for configurations

Scenarios

When device A is connected upstream to device B which has a higher priority, device B will be elected as the root bridge. Device A is concurrently connected to multiple ring networks which run STP/RSTP only, so device A is expected to be specified as the root bridge of

devices of multiple ring networks, to forward all traffic, and to choose device B as the root bridge.

Prerequisite

N/A

3.9.3 Default configurations of MRSTP

Default configurations of MRSTP are as below.

Function	Default value
MRSTP process	0
Interface MRSTP status	Enable
Device MRSTP priority	32768
Interface MRSTP priority	128
Interface path cost	0
Max Age timer	20s
Hello Time timer	2s
Forward Delay timer	15s

3.9.4 Enabling MRSTP

Enable MRSTP for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree enable	Enable STP.
3	Raisecom(config)#spanning-tree mode mrstp	Configure the mode of the spanning tree to MRSTP.
4	Raisecom(config)#spanning-tree mrstp <i>pro-id</i>	Create an MRSTP.
5	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
6	Raisecom(config-gigaethernet1/1/port)#spanning-tree mrstp <i>pro-id</i>	Bind the interface to the specified process.

3.9.5 Configuring MRSTP parameters

Configure MRSTP parameters for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree mrstp pro-id priority priority	(Optional) configure the priority of the specified process.
3	Raisecom(config)#spanning-tree root {primary secondary}	(Optional) configure the device as the root device or secondary root device.
4	Raisecom(config)#interface interface-type interface-number Raisecom(config-gigaethernet1/1/port)#spanning-tree priority priority-value	(Optional) configure the priority of the interface.
5	Raisecom(config-gigaethernet1/1/port)#spanning-tree mrstp pro-id port port-id path-cost cost Raisecom(config-gigaethernet1/1/port)#exit	(Optional) configure the path cost of the interface.
6	Raisecom(config)#spanning-tree hello-time value	(Optional) configure the Hello timer.
7	Raisecom(config)#spanning-tree transit-limit value	(Optional) configure the maximum transmission rate of the interface.
8	Raisecom(config)#spanning-tree forward-delay value	(Optional) configure the Forward Delay.
9	Raisecom(config)#spanning-tree max-age value	(Optional) configure the Max Age.

3.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show spanning-tree mrstp pro-id	Show basic configurations of MRSTP.

3.10 Loop detection

3.10.1 Introduction

Loop detection can eliminate the influence on network caused by a loop, thus 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.

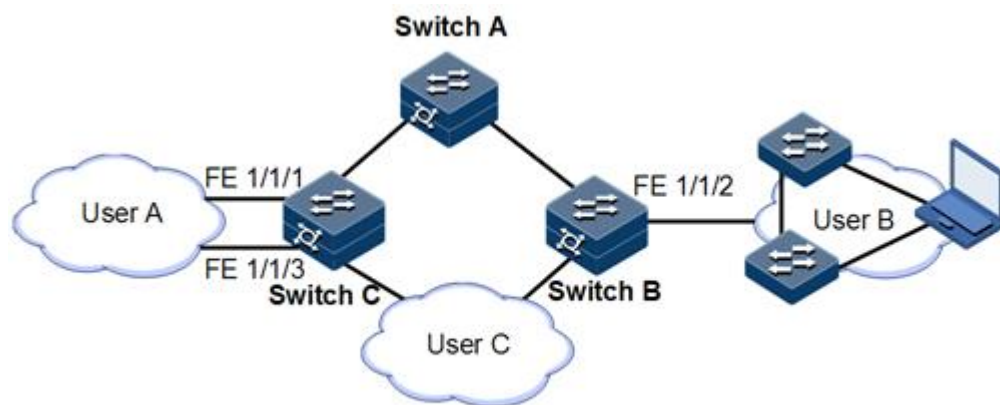
Loop types

Common loop types include self-loop, inner loop, and outer loop.

As shown in Figure 3-22, 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 is a self-loop on FE 1/1/2 on Switch B.
- Inner loop: a loop forming on different Ethernet interfaces of the same device. FE 1/1/1 and FE 1/1/3 on Switch C form an inner loop with the user network A.
-

Figure 3-22 Loop detection networking



Principles of processing loops

The ISCOM3000G series switch processes loops as below:

- If the device sending the loop detection packet is not the one receiving the packet, process the device with the larger MAC address to eliminate the loop (outer loop).
- 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 larger 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 3-22, 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:

- 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 FE 1/1/2.

- Inner loop: Switch C receives the loop detection packet 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 number, namely, FE 1/1/3.

Action for processing loops

The action for processing loops is the method for the ISCOM3000G 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 Trap.
- Trap-only: send Trap only.
- Shutdown: shut down the interface and send Trap.

Loop detection modes

The loop detection modes consist of port mode and VLAN mode:

- 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.
- VLAN mode: when a loop occurs,
 - In loopback processing mode of block, when a loop occurs on one or more of VLANs to which the interface belongs, the system blocks the VLANs with loop and leaves other VLANs to normally receive or send packets.
 - In loopback processing mode of shutdown, the system shuts down the physical interface and sends Trap information.

If the loop detection processing mode is Trap-only in the previous two modes, the ISCOM3000G series switch sends Trap 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, namely, the automatic restoration time is infinite; it will not be automatically restored.

3.10.2 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. When a loopback is detected on an interface, the interface will be blocked.

Prerequisite

Loopback interface, interface backup, STP, G.8032, and RRPS interfere with each other. We do not recommend configuring two or more of them concurrently.

3.10.3 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	VLAN

3.10.4 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode or batch interface configuration mode.

Step	Command	Description
3	<pre> Raisecom(config- gigaethernet1/1/1)loopback- detection [pkt-vlan { untag vlan- id }] [hello-time second] [restore- time second] [action { block trap- only shutdown }] [log-interval log-interval time] Raisecom(config- gigaethernet1/1/1)loopback- detection detect-vlanlist vlanlist [hello-time second] [restore-time second] [action { block trap-only shutdown }] [log-interval log- interval time] </pre>	<p>Enable loop detection on the interface.</p> <p>Configure the VLAN for sending loop detection packets.</p> <p>(Optional) configure the period for sending Hello packets.</p> <p>(Optional) configure the time for automatically restoring the blocked interface due to loop detection and the action for processing loops.</p>
4	<pre> Raisecom(config- gigaethernet1/1/1)#loopback- detection manual restore </pre>	<p>Manually restore the interface blocked due to loop detection.</p>

3.10.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<pre> Raisecom#show loopback-detection [statistics] [interface-type interface- number] [details] </pre>	<p>Show configurations and status of loop detection.</p>

3.10.6 Maintenance

Use the following commands to maintain the ISCOM3000G series switch.

Command	Description
<pre> Raisecom(config)#clear loopback-detection statistic [interface-type interface-number] </pre>	<p>Clear statistics about loop detection.</p>

3.10.7 Example for configuring inner loop detection

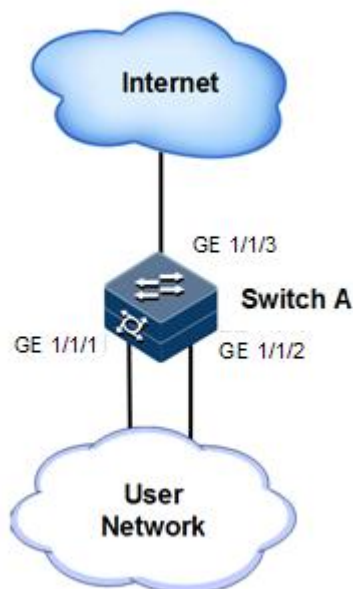
Networking requirements

As shown in Figure 3-23, 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, 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 of GE 1/1/2 to block, namely, sending Trap and blocking the interface.

Figure 3-23 Loop detection networking



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 1/1/2 is already blocked because of its greater 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      --          1          5          block      0
no      --          --          --          --          --          --
GE1/1/2  3      --          1          5          block      0
no      --          --          --          --          --          --
```

3.11 Interface protection

3.11.1 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.

3.11.2 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

3.11.3 Default configurations of interface protection

Default configurations of interface protection are as below.

Function	Default value
Interface protection status of each interface	Disable

3.11.4 Configuring interface protection



Caution

Interface protection is unrelated with the VLAN to which the interface belongs.

Configure interface protection for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#switchport protect	Enable interface protection.

3.11.5 Configuring interface isolation

Configure interface isolation for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#protect- group <i>group-id</i> vlan <i>vlan-</i> <i>id</i> <i>interface-type</i> <i>interface-number</i>	Create an interface isolation group. Configure isolation VLANs associated with the group and the list of isolated interfaces.

3.11.6 Checking configurations

Use the following commands to check configuration results.

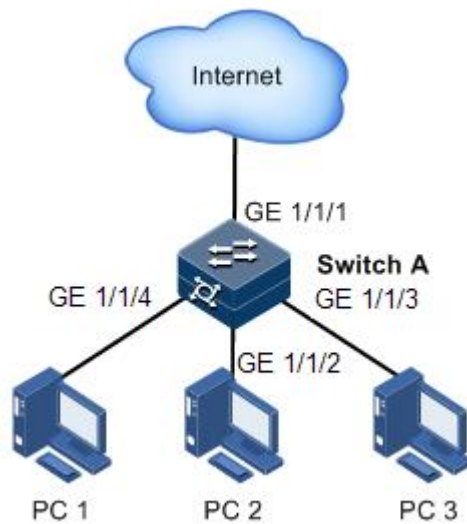
No.	Command	Description
1	Raisecom#show switchport protect	Show configurations of interface protection.
2	Raisecom#show protect- group { all <i>group-id</i> }	Show configurations of interface isolation.

3.11.7 Example for configuring interface protection

Networking requirements

As shown in Figure 3-24, 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.

Figure 3-24 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
.....
```

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.

3.12 Port mirroring

3.12.1 Introduction

Port mirroring refers to assigning some packets mirrored from the source port to the destination port, such as from the monitor port without affecting the normal packet forwarding. You can monitor sending and receiving status for packets on a port through this function and analyze the related network conditions.

Figure 3-25 Principles of port mirroring

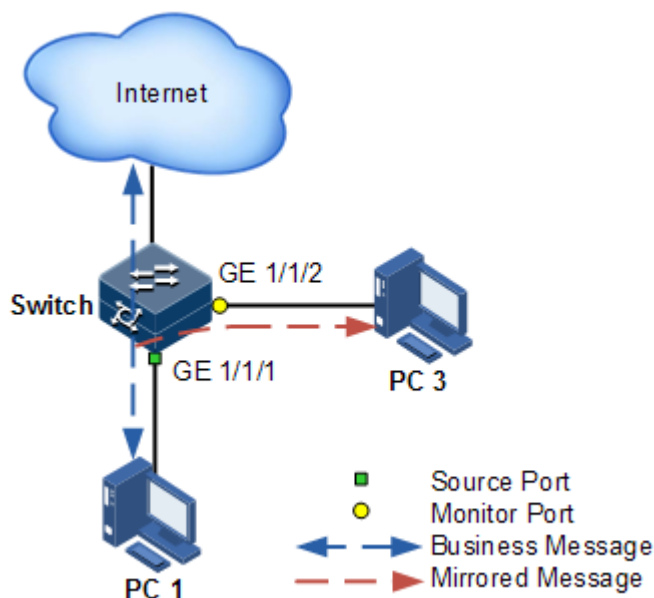


Figure 3-25 shows basic principles of port mirroring. PC 1 is connected to the external network through the GE 1/1/1. PC 3 is the monitor PC, connected to the external network through GE 1/1/2.

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 ISCOM3000G series switch, the ISCOM3000G series switch will forward and copy them to monitor port (GE 1/1/2). The monitor device connected to mirror the monitor port can receive and analyze these mirrored packets.

The ISCOM3000G series switch supports data stream mirroring on the ingress port and egress port. The packets on ingress/egress mirroring port will be copied to the monitor port after the switch is enabled with port mirroring. The monitor port and mirroring port cannot be the same one.

3.12.2 Preparing for configurations

Scenario

Port mirroring is used to monitor the type and flow of network data regularly for 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

3.12.3 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
Monitor port	gigaethernet1/1/1

3.12.4 Configuring port mirroring on local port

Configure local port mirroring for the ISCOM3000G series switch as below.

Step	Configure	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mirror-group group-id</code>	Create a port mirroring group.

Step	Configure	Description
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical interface configuration mode.
4	<code>Raisecom(config- gigaetherent1/1/1)#mirror-group group-id monitor-port</code>	Configure the monitor port for mirroring.
5	<code>Raisecom(config- gigaetherent1/1/1)#mirror-group group-id source-port { ingress egress }</code>	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.
6	<code>Raisecom(config- gigaetherent1/1/1)#exit Raisecom(config)#mirror-group group- id source-cpu [ingress egress]</code>	Configure port mirroring to mirror packets to or from the CPU.

3.12.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show mirror- group [group-id]</code>	Show configurations of port mirroring.

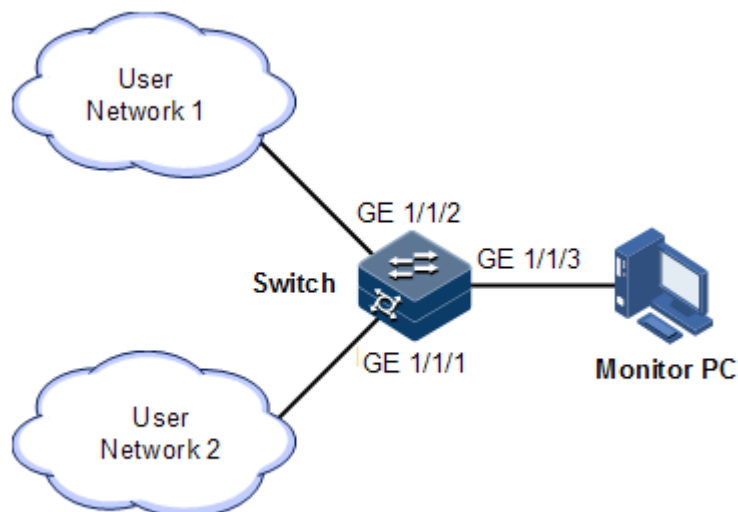
3.12.6 Example for configuring port mirroring

Networking requirements

As shown in Figure 3-26, the network administrator wishes 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 ISCOM3000G series switch is disabled with storm control and automatic packets sending. User network 1 accesses the ISCOM3000G series switch through GE 1/1/1, user network 2 accesses the ISCOM3000G series switch through GE 1/1/2, and the data monitor device is connected to GE 1/1/3.

Figure 3-26 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 1/1/2
Raisecom(config-gigaethernet1/1/2)#mirror-group source-port-list ingress
```

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
    gigaethernet1/1/2      : ingress
Remote Vlan: --
```

3.13 L2CP

3.13.1 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 ISCOM3000G 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.

3.13.2 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

3.13.3 Default configurations of L2CP

Default configurations of L2CP are as below.

Function	Default value
Global L2CP status	Disable
Applying the profile on the interface	Disable
Specified multicast destination MAC address	0x0100.0ccd.cdd0
Description of the L2CP profile	N/A

3.13.4 Configuring global L2CP

Configure global L2CP for the ISCOM3000G series switch as below.

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

Step	Command	Description
2	Raisecom(config)# l2cp-process tunnel destination-address <i>mac-address</i>	(Optional) configure the destination MAC address for transparently transmitted packets.

3.13.5 Configuring L2CP profile

Configure the L2CP profile for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# l2cp-process profile <i>profile-number</i>	Create and enter the L2CP profile.
3	Raisecom(config-l2cp-profile)# name <i>string</i>	(Optional) add profile description.
4	Raisecom(config-l2cp-profile)# l2cp-process protocol { oam stp dot1x lACP lldp cdp vtp pvst all } action { tunnel drop peer }	(Optional) configure the mode for processing L2CP packets.
5	Raisecom(config-l2cp-profile)# tunnel vlan <i>vlan-id</i>	(Optional) configure the specified VLAN for transparent transmission.
6	Raisecom(config-l2cp-profile)# tunnel interface-type <i>interface-number</i>	(Optional) configure the specified egress interface for transparent transmission.
7	Raisecom(config-l2cp-profile)# tunnel tunnel-type mac	(Optional) configure the type of the tunnel for transparent transmission.

3.13.6 Configuring L2CP profile on interface

Configure the L2CP profile on interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)# l2cp profile <i>profile-number</i>	Apply the L2CP profile on the interface.



Note

Applying a profile to an interface takes effect unless global L2CP is enabled. You can configure it but it will not take effect if global L2CP is disabled.

3.13.7 Checking configurations

Use the following commands check configuration results.

No.	Command	Description
1	Raisecom# show l2cp-process profile [<i>profile-number</i>]	Show information about the created L2CP profile.
2	Raisecom# show l2cp-process [<i>interface-type interface-number</i>]	Show configurations of L2CP on the interface.
3	Raisecom# show l2cp-process [tunnel statistics] [<i>interface-type interface-number</i>]	Show statistics about L2CP packets on the interface.

3.13.8 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom(config)# clear l2cp-process tunnel statistic [<i>interface-type interface-number</i>]	Clear statistics about L2CP packets on the interface.

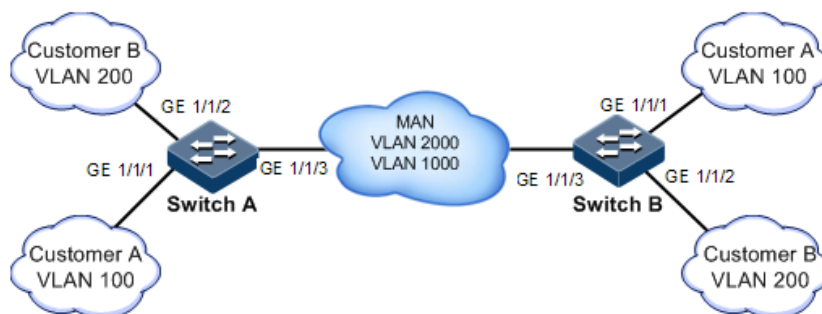
3.13.9 Example for configuring L2CP

Networking requirements

As shown in Figure 3-27, 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 3-27 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#name SwitchA
```

Step 2 Configure the specified multicast destination MAC address.

```
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 gigaethernet1/1/1
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-profile)#name CustomerB
Raisecom(config-l2cp-profile)#l2cp-process protocol all action drop
Raisecom(config-l2cp-profile)#l2cp-process protocol stp action tunnel
Raisecom(config-l2cp-profile)#l2cp-process protocol vtp action tunnel
```

```
Raisecom(config-l2cp-profile)#l2cp-process protocol elmi action peer
Raisecom(config-l2cp-profile)#exit
Raisecom(config)#interface gigaethernet1/1/2
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
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** command to show interface configurations.

```
Raisecom#show l2cp
L2CP running information
```

Port	ProfileID	BpduType	mac-address	l2cp-process
GE1/1/1	1	stp	0180.c200.0000	tunnel
		dot1x	0180.c200.0003	drop
		larp	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
		larp	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	--	--	--	--
...				

3.14 Voice VLAN

3.14.1 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.

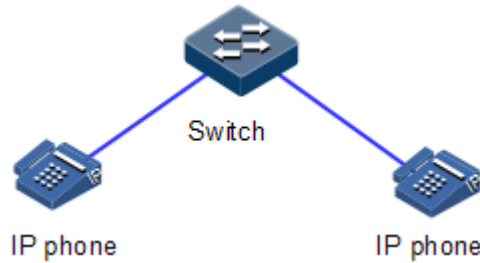
Compared with other methods for managing voice traffic, the voice VLAN has the following advantages:

- 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.

Figure 3-28 shows the networking mode for IP voice devices (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.

Figure 3-28 Networking for IP phone to connect to switch



3.14.2 Preparing for configurations

Scenario

The voice VLAN can transmit voice traffic. If the voice device is faulty or disconnected from the network, the interface connecting the voice device will automatically leave the voice VLAN.

Prerequisite

Create a VLAN, and configure its parameters.

3.14.3 Default configurations of voice VLAN

Default configurations of Organizationally Unique Identifier (OUI) of the voice VLAN are as below.

OUI-Address	Mask address	Description
0001.E300.0000	FFFF.FF00.0000	Siemens
0003.6B00.0000	FFFF.FF00.0000	Cisco
0004.0D00.0000	FFFF.FF00.0000	Avaya
00D0.1E00.0000	FFFF.FF00.0000	Pingtel
0060.B900.0000	FFFF.FF00.0000	Philips/NEC
00E0.7500.0000	FFFF.FF00.0000	Polycom
00E0.BB00.0000	FFFF.FF00.0000	3Com

Other default configurations of the voice VLAN are as below.

Function	Default value
Voice VLAN	Disable
Voice VLAN safe working mode	Enable
CoS and DSCP of Voice VLAN packets	6 and 46 respectively
QoS trust priority of Voice VLAN	N/A

3.14.4 Configuring OUI address

Configure the OUI address for the ISCOM3000G 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]	Configure the OUI of the voice VLAN.

3.14.5 Enabling voice VLAN

Enable the voice VLAN for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface interface-type interface-number	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#voice-vlan vlan-id enable	Enable the voice VLAN.

3.14.6 Configuring QoS of voice VLAN

Configure the QoS of the voice VLAN for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface interface-type interface-number	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#voice-vlan qos cos value dscp dscp value	Configure CoS and DSCP of voice VLAN packets.

Step	Command	Description
4	Raisecom(config-gigabitEthernet1/1/1)# voice-vlan qos trust	Configure QoS trust priority of the voice VLAN. Then, the interface does not modify the priority of voice VLAN packets.

3.14.7 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.

4 Ring network protection

This chapter describes principles and configuration procedures of ring network protection, including the following section:

- G.8032

4.1 G.8032

4.1.1 Introduction

G.8032 Ethernet Ring Protection Switching (ERPS) is an APS protocol based on the ITU-T G.8032 recommendation. It is a link-layer protocol specially used in Ethernet rings. Generally, ERPS can avoid broadcast storm caused by data loopback in Ethernet rings. When a link/device on the Ethernet ring fails, traffic can be quickly switched to the backup link to ensure restoring services quickly.

G.8032 uses the control VLAN on the ring network to transmit ring network control information. Meanwhile, combining with the topology feature of the ring network, it discovers network fault quickly and enable the backup link to restore service fast.

4.1.2 Preparing for configurations

Scenario

With the development of Ethernet to Telecom-grade network, voice and video multicast services bring higher requirements on Ethernet redundant protection and fault-recovery time. The fault-recovery time of current STP system is in second level that cannot meet requirements.

By defining different roles for nodes on a ring, G.8032 can block a loopback to avoid broadcast storm in normal condition. Therefore, the traffic can be quickly switched to the protection line when working lines or nodes on the ring fail. This helps eliminate the loop, perform protection switching, and automatically recover from faults. In addition, the switching time is shorter than 50ms.

The ISCOM3000G series switch supports the single ring, intersecting ring, and tangent ring.

G.8032 provides a mode for detecting faults based on physical interface status. The ISCOM3000G series switch learns link fault quickly and switches services immediately, so this mode is suitable for detecting the fault between neighboring devices.

Prerequisite

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

4.1.3 Default configurations of G.8032

Default configurations of G.8032 are as below.

Function	Default value
Protocol VLAN	1
Protection ring mode	Revertive
Ring WTR timer	5min
Ring protocol version	2
Guard timer	500ms
Ring Holdoff timer	0ms
ERPS fault reported to NMS	Disable
Tributary ring virtual channel mode in intersecting node	With
Ring Propagate switch in crossing node	Disable

4.1.4 Creating G.8032 ring


Configure G.8032 for the ISCOM3000G series switch as below.




Caution

- Only one device on the protection ring can be configured as the Ring Protection Link (RPL) Owner and only one device is configured as the RPL Neighbor. Other devices are configured as ring forwarding nodes.
- The tangent ring consists of 2 independent single rings. Configurations of the tangent ring are identical to those of the common single ring. The intersecting ring consists of a main ring and a tributary ring. Configurations of the main ring are identical to those of the common single ring. For detailed configurations of the tributary ring, see section 4.1.5 (Optional) creating G.8032 tributary ring.

Step	Command	Description
1	raisecom#config	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> east { <i>interface-type</i> <i>interface-</i> <i>number</i> port-channel <i>port-</i> <i>channel-number</i> } west { <i>interface-type</i> <i>interface-</i> <i>number</i> port-channel <i>port-</i> <i>channel-number</i> } [node-type rpl-owner rpl { east west }] [not-revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-list</i>]</pre>	<p>Create a protection ring and configure the node as the RPL Owner.</p> <p> Note The east and west interfaces cannot be the same one.</p>
	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> east { <i>interface-type</i> <i>interface-</i> <i>number</i> port-channel <i>port-</i> <i>channel-number</i> } west { <i>interface-type</i> <i>interface-</i> <i>number</i> port-channel <i>port-</i> <i>channel-number</i> } node-type rpl-neighbour rpl { east west } [not-revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-list</i>]</pre>	<p>Create a protection ring, and configure the node as the RPL Neighbour.</p>
	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> east { <i>interface-type</i> <i>interface-</i> <i>number</i> port-channel <i>port-</i> <i>channel-number</i> } west { <i>interface-type</i> <i>interface-</i> <i>number</i> port-channel <i>port-</i> <i>channel-number</i> } [not- revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-list</i>]</pre>	<p>Create a protection line, and configure the node as the protection forwarding node.</p>
3	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> name <i>string</i></pre>	<p>(Optional) configure a name for the protection ring. Up to 32 bytes are available.</p>
4	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> version { 1 2 }</pre>	<p>(Optional) configure the protocol version. The protocol version of all nodes on a protection ring should be identical.</p> <p>In protocol version 1, protection rings are distinguished based on the protocol VLAN. Therefore, you need to configure different protocol VLANs for protection rings.</p> <p>We recommend configuring different protocol VLANs for protection rings even if protocol version 2 is used.</p>

Step	Command	Description
5	<code>Raisecom(config)#ethernet ring-protection ring-id guard-time guard-time</code>	(Optional) after the ring Guard timer is configured, the failed node does not process APS packets during a period. In a bigger ring network, if the failed node recovers from a fault immediately, it may receive the fault notification sent by the neighboring node on the protection ring. Therefore, the node is in Down status again. You can configure the ring Guard timer to solve this problem.
6	<code>Raisecom(config)#ethernet ring-protection ring-id wtr-time wtr-time</code>	(Optional) configure the ring WTR timer. In revertive mode, when the working line recovers from a fault, traffic is not switched to the working line unless the WTR timer times out.
7	<code>Raisecom(config)#ethernet ring-protection ring-id holdeoff-time holdeoff-time</code>	(Optional) configure the ring Holdoff timer. After the Holdoff timer is configured, the system will delay processing the fault when the working line fails. Namely, traffic is delayed to be switched to the protection line. This helps prevent frequent switching caused by working line vibration.  Note If the ring Holdoff timer value is too great, it may influence 50ms switching performance. Therefore, we recommend configuring the ring Holdoff timer value to 0.


4.1.5 (Optional) creating G.8032 tributary ring



Caution

- Only the intersecting ring consists of a main ring and a tributary ring.
- Configurations of the main ring are identical to those of the single/tangent ring. For details, see section 4.1.4 Creating G.8032 ring.
- For the intersecting ring, configure its main ring and then the tributary ring; otherwise, the tributary ring will fail to find the interface of the main ring, thus failing to establish the virtual channel of the tributary ring.
- The ID of the tributary ring must be greater than that of the main ring.
- Configurations of non-intersecting nodes of the intersecting ring are identical to those of the single/tangent ring. For details, see section 4.1.4 Creating G.8032 ring.

Configure G.8032 intersecting rings for ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ethernet ring-protection ring-id { east west } { interface-type interface-number port- channel port-channel- number } node-type rpl- owner [not-revertive] [protocol-vlan vlan-id] [block-vlanlist vlan- list]</code>	<p>Create the tributary ring on the intersecting node and configure the intersecting node as the RPL Owner.</p> <p>The protection ring is in non-revertive mode if you configure the non-revertive parameter.</p> <ul style="list-style-type: none"> • In revertive mode, when the working line recovers from a fault, traffic is switched from the protection line to the working line. • In non-revertive mode, when the working line recovers from a fault, traffic is not switched from the protection line to the working line. <p>By default, the protection ring is in revertive mode.</p> <p> Note</p> <p>The links between 2 intersecting nodes belong to the main ring. Therefore, when you configure the tributary ring on the intersecting node, you can only configure the west or east interface.</p>
	<code>Raisecom(config)#ethernet ring-protection ring-id { east west } { interface-type interface-number port- channel port-channel- number } node-type rpl- neighbour [not- revertive] [protocol- vlan vlan-id] [block- vlanlist vlan-list]</code>	Create the tributary ring on the intersecting node, and configure the intersecting node as the RPL Neighbour.
	<code>Raisecom(config)#ethernet ring-protection ring-id { east west } { interface-type interface-number port- channel port-channel- number } [not- revertive] [protocol- vlan vlan-id] [block- vlanlist vlan-list]</code>	Create the tributary ring on the intersecting node, and configure the intersecting node as the protection forwarding node.

Step	Command	Description
3	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> raps-vc { with without }</pre>	<p>(Optional) configure the tributary ring virtual channel mode on the intersecting node. Because the intersecting node belongs to the main ring, transmission modes of protocol packets in the tributary ring are different from the ones of the main ring. In the tributary ring, transmission modes are divided into with and without modes.</p> <ul style="list-style-type: none"> • with: the main ring provides channels for APS packets of the tributary ring; the tributary ring intersecting node transmits APS packets of the tributary ring to the main ring to use the main ring to complete communications among intersecting nodes of the tributary ring. • without: APS packets of the tributary ring on intersecting nodes need to be ended and cannot be transmitted to the main ring. This mode requires the tributary ring not to block the protocol VLAN of the tributary ring (to ensure tributary ring packets to traverse Owner). <p>By default, the virtual channel of the tributary ring adopts the with mode. Transmission modes on 2 intersecting nodes must be identical.</p>
4	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> propagate enable</pre>	<p>Enable the ring Propagate switch on the intersecting node.</p> <p>Because data of the tributary ring needs to be transmitted through the main ring, there is a MAC address table of the tributary ring on the main ring. When the tributary ring fails, it needs to use the Propagate switch to inform the main ring of refreshing the MAC address table to avoid traffic loss.</p>

4.1.6 (Optional) configuring G.8032 switching control

Configure G.8032 switching control for the ISCOM3000G series switch as below.

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> force-switch { east west }</pre>	<p>Switch the traffic on the protection ring to the west/east interface forcedly.</p> <p>FS can be configured on multiple interfaces of multiple ring nodes.</p>

Step	Command	Description
3	Raisecom(config)#ethernet ring-protection ring-id manual-switch { east west }	Switch the traffic on the protection ring to the west/east interface manually. Its priority is lower than the one of FS and APS. MS can be configured on one interface of a ring node.
4	Raisecom(config)#clear ethernet ring-protection ring-id { Command statistics }	Clear switching control commands, including force-switch , manual-switch , WTR timer, and WTB timer.



Note

By default, traffic is automatically switched to the protection line when the working line fails. Therefore, you need to configure G.8032 control in some special cases.

4.1.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show ethernet ring-protection	Show configurations of the G.8032 ring.
2	Raisecom#show ethernet ring-protection status	Show G.8032 ring status.
3	Raisecom#show ethernet ring-protection statistics	Show G.8032 ring statistics.

4.1.8 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom(config)#clear ethernet ring-protection ring-id statistics	Clear statistics about the protection ring.

5 IP services

This chapter describes principles and configuration procedures of IP services, and provides related configuration examples, including the following sections:

- IP basis
- Loopback interface
- ARP
- NDP
- Route management
- Static route
- Routing policy
- OSPFv2
- ISIS
- BGP
- RIP

5.1 IP basis

5.1.1 Introduction

The IP interface is a virtual interface based on VLAN. Configuring Layer 3 interface is generally used for network management or routing link connection of multiple devices.

5.1.2 Preparing for configurations

Scenario

Configure the IP address of each VLAN interface and loopback interface.

Prerequisite

- Create VLANs.
- Activate them.

5.1.3 Default configurations of Layer 3 interface

Default configurations of the Layer 3 interface are as below.

Function	Default value
Management VLAN inner TPID	0x8100
Management VLAN inner VLAN	1
Management VLAN CoS	0

5.1.4 Configuring IPv4 address of VLAN interface

Configure the IPv4 address of the VLAN interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#ip address <i>ip-address</i> [<i>ip-mask</i>] [<i>sub</i>]	Configure the IP address of the VLAN interface. Use the no ip address <i>ip-address</i> command to delete configuration of the IP address.



Note

Up to 255 IP interfaces can be configured, and their IDs range from 0 to 254.

5.1.5 Configuring IPv6 address of VLAN interface

Configure the IPv6 address of the VLAN interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter Layer 3 interface configuration mode.
3	Raisecom(config-vlan1)#ipv6 address <i>ipv6-address</i> link-local Raisecom(config-vlan1)#ipv6 address <i>ipv6-address/prefix-length</i> [<i>eui-64</i>]	Configure the IPv6 address of the VLAN interface.

5.1.6 Configuring attributes of management VLAN

Configure attributes of the management VLAN for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan-id	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#ip management-traffic cos cos- value	Configure CoS of the management VLAN.
4	Raisecom(config-vlan1)#ip management-traffic mode double-tagging [inner-vlan vlan-id] [inner-cos cos-id]	Configure the double-tagged mode for management packets.

5.1.7 Checking configurations

Use the following commands to check configuration results.

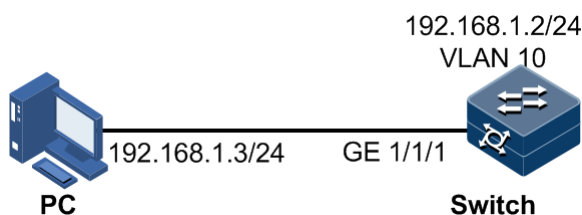
No.	Command	Description
1	Raisecom#show ip interface brief	Show configurations of the IP address of the IP interface.
2	Raisecom#show ipv6 interface brief	Show configurations of the IPv6 address of the IP interface.
3	Raisecom#show ip management- traffic	Show information about management packets on the VLAN interface.

5.1.8 Example for configuring VLAN interface to interconnect with host

Networking requirements

As shown in Figure 5-1, configure VLAN interface 10 to the switch so that the host and the ISCOM3000G series switch can ping each other.

Figure 5-1 VLAN interface networking



Configuration steps

Step 1 Create VLAN 10 and add interface GE 1/1/1 to VLAN 10.

```
Raisecom#config  
Raisecom(config)#create vlan 10 active
```

Step 2 Configure Layer 3 interface of VLAN 10 on the ISCOM3000G series switch, configure its IP address, and associate the interface with VLAN 10.

```
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  
Category  
-----  
-----  
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 ISCOM3000G 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,
Success rate is 100 percent(5/5),
round-trip (ms) min/avg/max = 0/0/0.
```

5.2 Loopback interface

5.2.1 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.

Loopback interface status is free from physical interface status (Up/Down). As long as the ISCOM3000G 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.

5.2.2 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. 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

5.2.3 Default configurations of loopback interface

N/A

5.2.4 Configuring IP address of loopback interface

Configure the IP address of the loopback interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface loopback lb-number	Enter loopback interface configuration mode.
3	Raisecom(config-loopback)#ip address ip-address [ip-mask]	Configure the IP address of the loopback interface.
4	Raisecom(config-loopback)#ipv6 address ipv6-address/prefix- length [sub]	Configure the IPv6 address of the loopback interface.

5.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show interface loopback	Show configurations of loopback interface.

5.3 ARP

5.3.1 Introduction

In a 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 a 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 mapping table contains the following two types of entries:

- Static entry: bind IP address and MAC address to avoid ARP dynamic learning cheating.
 - Static ARP address entry needs to be added/deleted manually.
 - Static ARP addresses are not aged.
- Dynamic entry: MAC address automatically learned through ARP.
 - This dynamic 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 ISCOM3000G series switch supports the following two modes of dynamically learning ARP address entries:

- Learn-all: in this mode, the ISCOM3000G 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 ISCOM3000G 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.

5.3.2 Preparing for configurations

Scenario

The mapping of IP address and MAC address is saved in the ARP address mapping table.

Generally, The ARP address mapping table is dynamically maintained by the ISCOM3000G series switch. The ISCOM3000G series switch searches for the mapping between IP address and MAC address automatically according to ARP. You just need to configure the ISCOM3000G series switch manually for preventing ARP dynamic learning from cheating and adding static ARP address entries.

Prerequisite

N/A

5.3.3 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

5.3.4 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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#arp ip-address mac-address</code>	Configure static ARP entry.

5.3.5 Configuring dynamic ARP entries

Configure dynamic ARP entries for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#arp mode { learn-all learn-reply-only }	Configure the aging time of dynamic ARP entries.
3	Raisecom(config)#arp aging-time <i>time</i>	Enter Layer 3 interface configuration mode.
4	Raisecom(config)# interface vlan 1 Raisecom(config-vlan1)#arp max- learning-num <i>number</i>	(Optional) configure the maximum number of dynamic ARP entries allowed to learn on the Layer 3 interface.
5	Raisecom(config-vlan1)#arp learning [strict] { enable disable }	Configure dynamic ARP learning.

5.3.6 Configuring local proxy ARP

Configure local proxy ARP for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan-id	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#arp local-proxy enable	Enable local proxy ARP.

5.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show arp [<i>ip-address</i> interface <i>interface-type</i> <i>interface-number</i> static]	Show information about entries in the ARP address table.
2	Raisecom#show arp local-proxy [interface vlan <i>vlan-id</i>]	Show information about local proxy ARP.

5.3.8 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
raisecom(config)#clear arp	Clear all entries in the ARP address table.

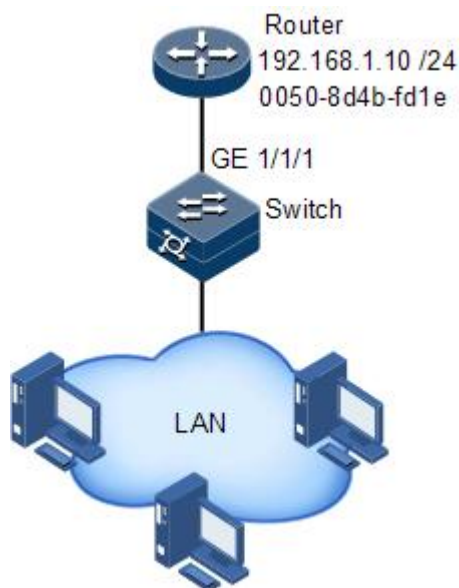
5.3.9 Example for configuring ARP

Networking requirements

As shown in Figure 5-2, the ISCOM3000G 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 is 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 ISCOM3000G series switch.

Figure 5-2 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	Type
Age(s)	status		

192.168.1.10	0050.8D4B.FD1E	0	static --
PERMANENT			

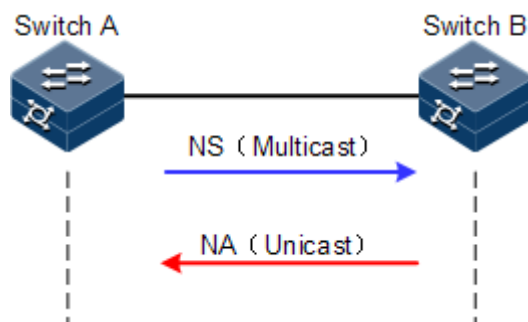
5.4 NDP

5.4.1 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 5-3 Principles of NDP address resolution



As shown in Figure 5-3, 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.

5.4.2 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.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.
- Configure the IPv6 address of the Layer 3 interface.

5.4.3 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	512

5.4.4 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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ipv6 neighbor ipv6-address mac-address</code>	configure static neighbor entries

5.4.5 Configuring times of sending NS messages for detecting duplicated addresses

Configure times of sending NS messages for detecting duplicated addresses for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface ip if-number	Enter Layer 3 interface configuration mode.
3	Raisecom(config-ip)#ipv6 nd dad attempts value	Configure times of sending NS messages for detecting duplicated addresses.



Note

When the ISCOM3000G 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.

5.4.6 Configuring maximum number of NDPs allowed to be learnt on Layer 3 interface

Configure the maximum number of NDPs allowed to be learnt on the Layer 3 interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan vlan-id	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#ipv6 neighbors max-learning-num number	Configure the maximum number of NDPs allowed to be learnt on the Layer 3 interface.

5.4.7 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 ip if-number	Show neighbor information about a specified layer 3 interface.
4	Raisecom#show ipv6 neighbors static	Show information about IPv6 static neighbor.
5	Raisecom#show ipv6 interface prefix [ip if-number]	Show prefix information about the IPv6 address.

No.	Command	Description
6	Raisecom# show ipv6 interface nd [<i>ip if-number</i>]	Show ND information configured on the interface.

5.4.8 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom(config)# clear ipv6 neighbors	Clear information about all IPv6 neighbors.

5.5 Route management

5.5.1 Preparing for configurations

Scenarios

Dynamic routing protocols require using the router ID. They will use the default router ID if no router ID is specified.

The ISCOM3000G series switch can establish and update the routing table, and forwards packets according to the routing table. By viewing the routing table, you can learn network topology and locate faults.

Prerequisite

N/A

5.5.2 Configuring route management

Configure route management for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ip route <i>ip-address</i> { <i>mask-address</i> <i>mask-length</i> } { <i>next-hop</i> [<i>interface-type interface-num</i>] NULL 0 } [distance <i>distance</i>] [description <i>text</i>] [tag <i>tag</i>]	Configure the IPv4 static route.

Step	Command	Description
	<code>Raisecom(config)#ipv6 route ipv6-address/prefix-length { ipv6-address / null 0 } [distance distance] [description text] [tag tag]</code>	Configure the IPv6 static route.
3	<code>Raisecom(config)#ip route static distance distance</code>	(Optional) configure the default administrative distance of the IPv4 static route. By default, it is 1.
	<code>Raisecom(config)#ipv6 route static distance distance</code>	(Optional) configure the default administrative distance of the IPv6 static route. By default, it is 1.

5.5.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show router id</code>	Show the router ID.
2	<code>Raisecom#show ip route protocol { static connected bgp ospf isis rip } [detail]</code> <code>Raisecom#show ipv6 route protocol { static connected bgp ospf isis rip } [detail]</code>	Show information about routing protocols in the routing table.
3	<code>Raisecom#show ip route ip-address [mask-address] [longer-prefixes] [detail]</code> <code>Raisecom#show ipv6 route { ipv6-address ipv6-address/prefix-length }</code>	Show the route to the destination address.
4	<code>Raisecom#show ip route ip-address1 [mask-address1] ip-address2 [mask- address2] [detail]</code>	Show the route between 2 IP addresses.
5	<code>Raisecom#show{ ip ipv6 } route summary</code>	Show route summary.

5.6 Static route

5.6.1 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.

The ISCOM3000G series switch supports default route and static route only but dynamic route.

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 ISCOM3000G series switch has not been configured with default route and the destination IP of the packet is not in the routing table, the ISCOM3000G 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

The static route is a route configured manually, thus bringing low requirements on the system. It is available to a simple, small, and stable network. The disadvantage is that it cannot adapt to network topology changes automatically and needs manual intervention.

5.6.2 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.

5.6.3 Configuring static route

Configure static route for the ISCOM3000G series switch as below.

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

Step	Command	Description
2	<pre>Raisecom(config)#ip route ip- address mask-address { next-hop [interface-type interface-num] NULL 0 } [distance distance] [description text] [tag tag] Raisecom(config)#ipv6 route ipv6-address/prefix-length ipv6- address [distance distance] [description text] [tag tag]</pre>	Configure the static route.
3	<pre>Raisecom(config)#ip route static distance value</pre>	(Optional) configure the default IPv4 administrative distance.

5.6.4 Checking configurations

Use the following commands to check configuration results.

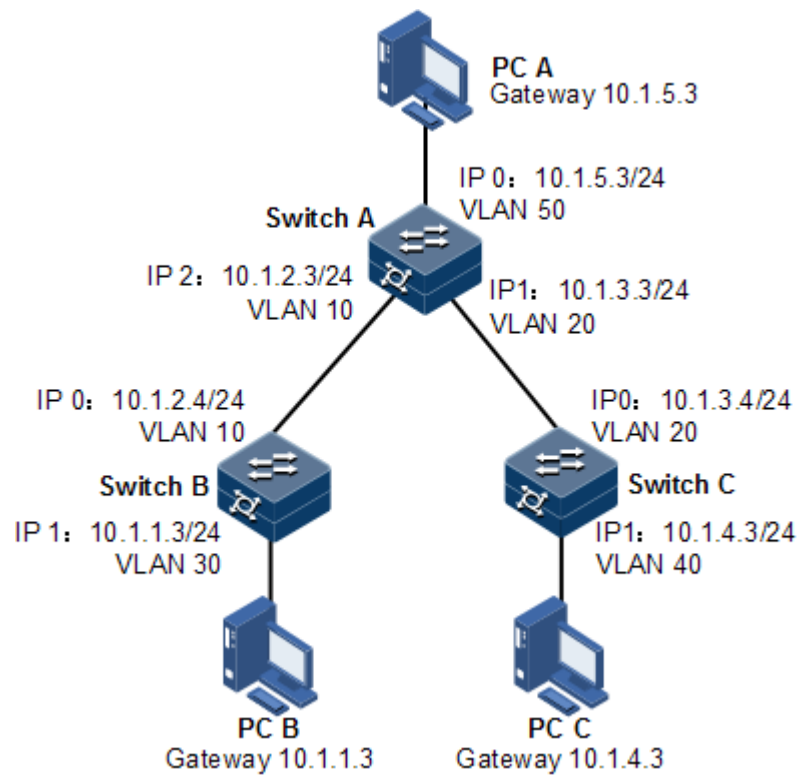
No.	Item	Description
1	<pre>Raisecom#show ip route [detail]</pre>	Show information about IPv4 routes.

5.6.5 Example for configuring static route

Networking requirements

As shown in Figure 5-4, configure a static route to make any two hosts or switches ping each other.

Figure 5-4 Static route networking



Configuration steps

- Step 1 Configure IP addresses of each device. Detailed configurations are omitted.
- Step 2 Configure a static route on Switch A.

```
Raisecom#name 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#name 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#name SwitchC
SwitchC#config
SwitchC(config)#ip route 0.0.0.0 0.0.0.0 10.1.3.3
```

- Step 5 Configure the default gateway of PC A to 10.1.5.3. Detailed configurations are omitted.
 Configure the default gateway of PC B to 10.1.1.3. Detailed configurations are omitted.
 Configure the default gateway of PC C to 10.1.4.3. Detailed configurations are omitted.

Checking results

Use the **ping** command to check whether any two hosts or switches can ping 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.
```

5.7 Routing policy

5.7.1 Configuring IP prefix list

Configure the IP prefix list for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ip prefix-list <i>prefix-name</i> [seq seq-number] { deny permit } any	Create an IP prefix list or add a node to the IP prefix list.
	Raisecom(config)# ip prefix-list <i>prefix-name</i> [seq seq-number] { deny permit } <i>ip-</i> <i>address/mask</i> [ge min-length] [le max-length]	If no prefix list ID (<i>seq-number</i>) is configured, the system will generate a prefix list ID automatically. The generated pre-fix list ID has 5 digits.
3	Raisecom(config)# ip prefix-list <i>prefix-name</i> description string	Configure the description of the IP prefix list. If the length of descriptions exceeds 80 characters, the first 80 characters are available.



- 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.

5.7.2 Configuring routing table

Configure the routing table for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config-route-map)# description <i>string</i>	(Optional) configure the description of the routing table. If there is any space in descriptions, descriptions should be within quotes.
3	Raisecom(config-route-map)# on-match next	(Optional) configure the on-match sub-clause to continuing to match at the next node. By default, the process is finished after matching.
4	Raisecom(config-route-map)# on-match goto <i>number</i>	(Optional) configure the on-match sub-clause to continuing to match at some node. By default, the process is finished after matching.
5	Raisecom(config-route-map)# call <i>map-name</i>	(Optional) continue to match routes by scheduling other routing table after matching the route. By default, the process is finished after matching.
6	Raisecom(config-route-map)# match ip next-hop <i>acl-number</i>	(Optional) configure the match sub-clause to matching the next hop based on extended IP ACL.
7	Raisecom(config-route-map)# match ip next-hop prefix-list <i>prefix-name</i>	(Optional) configure the match sub-clause to matching the next hop based on IP prefix list.
8	Raisecom(config-route-map)# match ip address <i>acl-number</i>	(Optional) configure the match sub-clause to matching the IP address based on extended IP ACL.
9	Raisecom(config-route-map)# match ip address prefix-list <i>prefix-name</i>	(Optional) configure the match sub-clause to matching the IP address based on IP prefix list.

Step	Command	Description
10	Raisecom(config-route-map)# match interface <i>name</i>	(Optional) configure the match sub-clause to matching the interface name.
11	Raisecom(config-route-map)# match metric <i>metric</i>	(Optional) configure the match sub-clause to the matching rule that is based on route metric value.
12	Raisecom(config-route-map)# match tag <i>tag</i>	(Optional) configure the match sub-clause to the matching rule that is based on Tag field of the route tagging.
13	Raisecom(config-route-map)# match ip route-source prefix-list <i>prefix-name</i>	(Optional) configure the match sub-clause to the BGP routing information matching rule that is based on prefix list matching with source address of the route.
14	Raisecom(config-route-map)# set metric [+ -] <i>metric</i>	(Optional) configure the set sub-clause to modifying the route metric value after matching.
15	Raisecom(config-route-map)# set metric-type { <i>type-1</i> <i>type-2</i> }	(Optional) configure the set sub-clause to modifying the route metric type after matching.
16	Raisecom(config-route-map)# set src <i>ip-address</i>	(Optional) configure the set sub-clause to modifying the source IP address after matching.
17	Raisecom(config-route-map)# set ip next-hop <i>ip-address</i>	(Optional) configure the set sub-clause to modifying the next-hop IP address of the route after matching.
18	Raisecom(config-route-map)# set tag <i>tag</i>	(Optional) configure the set sub-clause to modifying the routing information Tag after matching.
19	Raisecom(config-route-map)# set as-path prepend <i>as-number</i>	(Optional) configure the set sub-clause to modifying the as-path property of the BGP routing information that matches with the routing policy.

5.7.3 Checking configurations

No.	Command	Description
1	Raisecom# show ip prefix-list [<i>prefix-name</i>] [<i>seq seq-number</i>]	Show information about the IP prefix list.
2	Raisecom# show ip prefix-list summary <i>prefix-name</i>	Show summary of the IP prefix list.
3	Raisecom# show ip prefix-list detail <i>prefix-name</i>	Show statistics about the IP prefix list.

No.	Command	Description
4	Raisecom# show route-map [<i>map-name</i>]	Show configurations of the routing table.

5.8 OSPFv2

5.8.1 Introduction

Open Shortest Path First (OSPF) is a dynamic route selection protocol based on link status. OSPF referred to in this document is OSPFv2 used for IPv4.

RIP has disadvantages of slow convergence, route loop, and weak expansibility, so it is unfit for large networks. Compared with RIP, OSPF has the following advantages:

- Wide application range: support networks of various sizes, especially large networks.
- Fast convergence: after network topology changes, OSPF immediately sends an update packet, and synchronizes the change in the Autonomous System (AS, the system composed of routing devices running the same routing protocol for exchanging information).
- No routing loop: according to collected link status, OSPF uses the shortest path tree algorithm to calculate routes, which guarantees no routing loop.
- Area division: OSPF divides the network into different areas for layering management, and routing information transmitted across areas is further abstracted, thus reducing occupied network bandwidth.
- Equivalent route: OSPF supports multiple equivalent routes to the same destination address.
- Multicast: OSPF supports sending protocol packets with a multicast address in links of certain types, thus reducing impact on other devices.

Network type of OSPF

By types of data link layer protocols, OSPF divides the network into the following types:

- Broadcast: when the data link layer protocol is Ethernet or FDDI, OSPF takes network type as broadcast by default. In such networks, OSPF sends protocol packets in multicast mode (multicast address: 224.0.0.5 and 224.0.0.6).
- Point-to-MultiPoint (P2MP): no data link layer protocol is taken as P2MP by default; instead, this type is forcibly changed from other types. A common method is to change NBMA to P2MP. In such networks, OSPF sends protocol packets in multicast mode (multicast address: 224.0.0.5) by default. You can configure OSPF to send packets in unicast mode as needed.
- Point-to-Point (P2P): when the data link layer protocol is PPP or High-Level Data Link Control (HDLC), OSPF takes network type as P2P by default. In such networks, OSPF sends protocol packets in multicast mode (multicast address: 224.0.0.5).

Router ID

To run OSPF, a router must have a router ID which is a 32-bit symbol-free integer. The router ID can uniquely identify a router in an AS.



Note

The router ID can be elected by the system or manually configured. The election rules are as below:

- If there are loopback interfaces configured with IP address, choose the maximum IP address of loopback interface as the router ID.
- If there are loopback interfaces without IP addresses, choose the maximum IP address of IP interface as the router ID.
- If the IP address is used by other OSPF process, it cannot be used by this OSPF process.
- If no IP address is configured, the route ID cannot be elected, the process cannot be created; you have to manually configure the router ID.

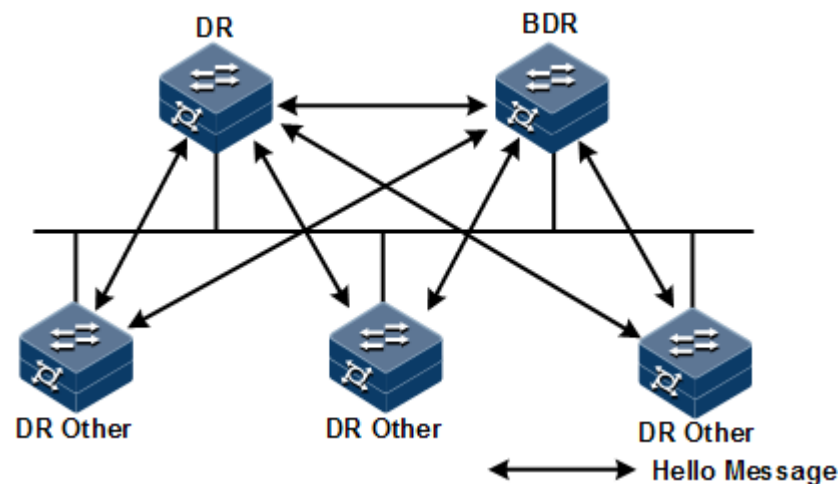
DR/BDR

In a broadcast network, any two routers need to exchange routing information. Thus route change on a router causes multiple transmissions, which wastes bandwidth resources. To solve this problem, OSPF defines the Designated Router (DR), which receives information from all routers and then advertises link status.

When the DR fails due to a fault, OSPF use a Backup Designated Router (BDR) to avoid incorrect calculation of routes in DR re-election time. Thus a BDR is elected while the corresponding DR is elected. The BDR establishes adjacency relation with all routers in the network segment and exchanges route information with them. When the DR fails, the BDR immediately becomes the DR. Then, a new BDR is elected, but this does not impact route calculation.

On a network running OSPF, a router not DR nor BDR is called DR Other. A DR Other establishes adjacency relation with DR and BDR only rather than another DR Other, as shown Figure 5-5. It reduces the number of relations between routers in the broadcast network and NBMA network, reduces network traffic, and saves bandwidth resource.

Figure 5-5 Roles of broadcast interface





- Only broadcast interfaces elect the DR. P2MP or P2P interfaces do not elect the DR.
- DR is a concept of a network segment and targeted for an interface on a router. A router may be a DR for an interface and a BDR or DR Other for another interface.
- The DR and BDR are elected by all routers in the same network segment through Hello packets according to router priority and router ID. Devices with a priority above 0 can be candidates for election. If priorities of two routers are the same, the router with the larger router ID is preferential. Devices with priority of 0 cannot be elected as the DR or BDR.
- Router priority affects DR/BDR election. When election ends, a router with higher priority may become effective for election. In this case, it does not replace the elected DR/BDR, and has to wait for next DR/BDR election.

OSPF packets

OSPF packets consist of the following types:

- Hello packet: sent periodically, used to discover and maintain OSPF neighbor relations. It carries timer values, DR, BDR, priority, and known neighbor information.
- Database Description (DD) packet: used to synchronize database between two routers. It describes abstract of each Link State Advertisement (LSA) in local LSDB, namely, LSA packet header.
- Link State Request (LSR) packet: used to request required LSA from the peer. After exchanging DD packet, two routers learn the lack LSA for local LSDB compared to the peer LSDB, and then send LSR packet to the peer to request required LSA. The content is LSA abstract.
- Link State Update (LSU) packet: used to send LSA required by the peer. The content is a set of multiple LSAs.
- Link State Acknowledgment (LSAck) packet: used to acknowledge received LSA. The content is the header of the LSA to be acknowledged. An LSAck packet can acknowledge multiple LSAs.

LSA type

OSPF describes link states, encrypts the information in LSA, and advertises LSA. There are 5 types of common LSAs:

- Router LSA (Type1): generated by each router, used to describe link status and cost, and speeded in the originating area.
- Network LSA (Type2), generated by the DR, used to describe link status of all routers in this segment, advertised in the originating area.
- Network Summary LSA (Type3), generated by the Area Border Router (ABR), used to describes routes of a network segment in the area and notify other areas.
- ASBR Summary LSA (Type4), generated by the ABR, used to describe routes to Autonomous System Boundary Router (ASBR) and notify related areas.
- AS External LSA (Type5), generated by the ASBR, used to describe routers out of AS and notify all areas except Stub area.

Neighbor and adjacency

After being started, an OSPF router sends Hello packets out through the OSPF interface. After receiving Hello packet, a device checks parameters (interval for sending Hello packets, invalidation time, and area mask information) defined in the Hello packet. If it has the same parameters, it forms a neighbor relation with the OSPF router.

A neighbor is not necessarily in an Adjacency relation, and it depends on the network type. Only when the two devices exchange DD packets and LSAs, and synchronize to the peer LSDB can they become in adjacency relation.

Calculating OSPF routes

OSPF calculates routes as below:

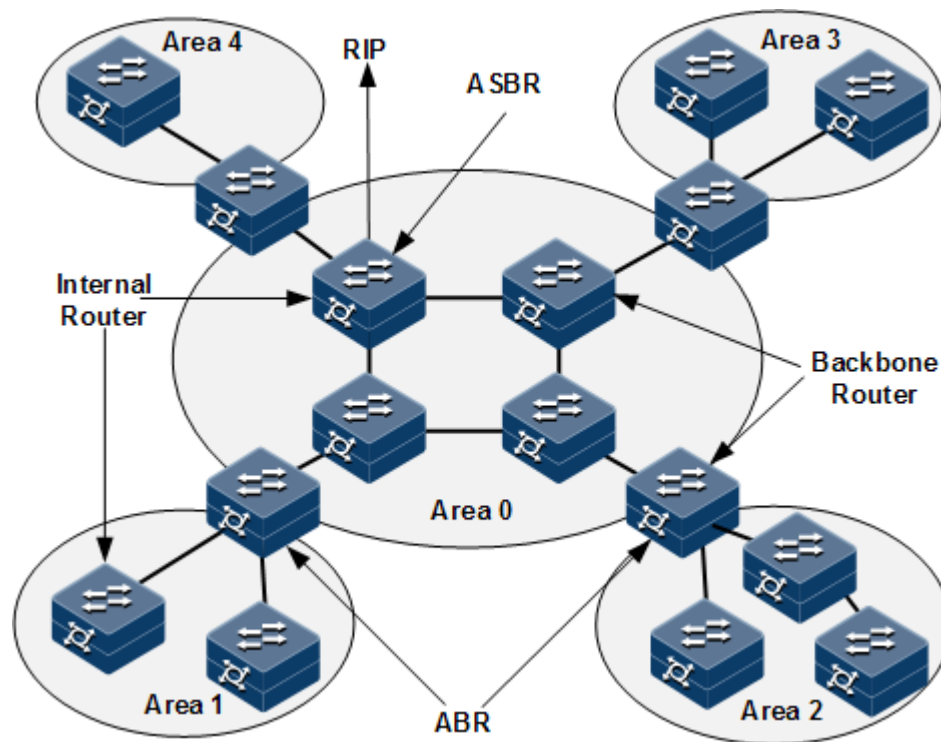
- Step 1 Each OSPF router generates LSAs according to network topology, and sends LSAs to other OSPF routers through updating packets.
- Step 2 Each OSPF router collects LSAs from other OSPF routers. All LSAs form LSDB. LSA describes network topology around the router. LSDB describes network topology of the entire AS.
- Step 3 Each OSPF router transfers LSDB to a weighted diagram, which reflects topology of the entire network. Each OSPF router obtains the same weighted diagram.
- Step 4 Each router uses the Shortest Path First (SPF) algorithm based on the weighted diagram, and then calculates a shortest path tree with itself as root. This tree provides routes to all nodes in the AS.

Area division

When routers on a large network run OSPF, increment of routers leads to a huge LSDB which occupies much storage space and causes the CPU to work in heavy burden. When the network grows larger, topology changes more frequently, the network is always in oscillation status, a large number of OSPF packets are transmitted, network bandwidth is wasted, and each change causes recalculation of routes for all routers.

OSPF divides an AS into different areas to solve the previous problem. An area logically contains some routers and is identified by the area ID. As shown in Figure 5-5, a route in an area maintains routing information of the area instead of the entire AS.

Figure 5-6 OSPF area and router type



The border of each area is a router instead of a link. A router may belong to different areas, but a network segment (link) must belong to only one area, or an interface running OSPF must belong to a specific area. After the network is divided into different areas, aggregate routes on border routers to reduce the number of LSAs advertised to other areas and minimize impact from changes of network topology.

Router types

As shown in Figure 5-6, OSPF routers can be divided into four types according to location in the AS:

- Internal router: all interfaces of an interval router belong to only one OSPF area.
- Area Border Router (ABR): this router may belong to two or more areas which must contain a backbone area. The ABR can connect a backbone area and a non-backbone area. It can be physically or logically connected to a backbone area.
- Backbone router: at least one interface of this router belongs to the backbone area, so all ABRs and internal routers in Area 0 are backbone routers.
- Autonomous System Border Router (ASBR): the router exchanges information with other AS is called the ASBR. The ASBR is not necessarily located at the border of an AS, and may be an internal router or ABR. When an OSPF router imports external routes, it becomes the ASBR.

Backbone area

After OSPF divides areas, not all areas are equal. A special area with area ID as 0 is called the backbone area. The backbone area transmits inter-area routes. Routing information from non-backbone area must be forwarded by the backbone area. The backbone area has the following information:

- All non-backbone areas must be interconnected with the backbone area.
- The backbone area must be internally interconnected.

Stub area

The border router has low performance, so its routing table must be limited. Configuring the Stub area is to prevent external LSAs from entering the area to the minimum extend.

In the Stub area, only Type1, Type2, and Type3 LSAs are advertised, and Type5 LSAs are not allowed to enter, which reduces the size of the routing table and the number of transmitted routes. In addition, you can configure the area to Totally Stub area which allows Type1 and Type2 LSAs and a default Type3 LSA. This further reduces the size and the number. In the Totally Stub area, the ABR does not transmit inter-area routes and external routes to the area.

Not each area complies with the (Totally) Stub area. Generally, the (Totally) Stub area is at the border of an AS. To make routes from other areas to the AS or external routes of the AS reachable, the ABR generates a default route, and advertises it to non-ABR routers in the area.

Route types

OSPF divides routes into four types by priority in descending order: Intra Area route, Inter Area route, Type1 External route, and Type2 External route.

The Intra Area route and Inter Area route describe network topology of the AS. External routes describe how to choose the route to a destination address out of the AS. Whether to calculate interval path cost of AS makes OSPF divide external routes into Type1 External route or Type2 External route.

- Cost of Type1 External route = cost from the local router to the corresponding ASBR + cost from the ASBR to the destination address of the route
- Cost of Type2 External route = cost from the ASBR to the destination address of the route

OSPF takes Type 1 External route with high credibility, so it chooses Type1 External route when Type 1 External route and Type2 External route for the same destination address co-exist regardless of the costs of these two routes.

5.8.2 Configuring basic functions of OSPF

Configure basic functions of OSPF for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ospf <i>process-id</i> [router-id <i>router-id</i>]</code>	Start OSPF process, and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#network <i>ip-address</i> <i>wild-card-mask</i> area <i>area-id</i></code>	Configure the network segment included by the OSPF area.



Note

- If you manually configure the *router-id* by configuring optional parameters in the **router ospf process-id [router-id router-id]** command, the OSPF process will use the *router-id* by precedence; otherwise, the process will automatically elect a *router-id*.
- If the process has configured or elected the *router-id*, and you modify the *router-id*, the modification will take effect after restart.

5.8.3 Configuring OSPF route attributes

Configuring interface cost

Configure the interface cost for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface interface-type interface-number	Enter Layer 3 interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#ip ospf cost cost	Configure the route cost of the IP interface. By default, it is not configured.

Configure the OSPF reference bandwidth for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)# router ospf process-id [router-id router-id]	Start an OSPF process, and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#reference-bandwidth bandwidth	Configure the reference bandwidth of the link. By default, it is 110 Mbit/s.



Note

- After the routing cost is manually configured through the **ip ospf cost** command, the manually-configured routing cost takes effect.
- If the routing cost is not configured manually but the link bandwidth reference value is configured, the routing cost is automatically configured based on link bandwidth reference value. The formula is: $\text{cost} = \text{link bandwidth reference value (bit/s)} / \text{link bandwidth}$. If the cost value is greater than 65535, it is configured to 65535. If no link bandwidth reference value is configured, it is configured to 100 Mbit/s by default.

Configuring OSPF administrative distance

Configure the OSPF administrative distance for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ospf process-id [router-id router-id]</code>	Enable an OSPF process and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#distance administrative-distance</code>	Configure the OSPF administrative distance. By default, it is 110.
4	<code>Raisecom(config-router-ospf)#distance ospf { intra-area inter-area external } distance</code>	Configure the administrative distance of OSPF specified route. By default, it is 0. However, it takes 110 provided by RM as the standard.

Configuring OSPF to be compatible with RFC1583

Configure OSPF to be compatible with RFC1583 for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ospf process-id [router-id router-id]</code>	Enable an OSPF process, and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#compatible rfc1583</code>	Configure OSPF to be compatible with RFC1583. By default, OSPF is compatible with RFC1583.

5.8.4 Configuring load balancing

Configure load balancing for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ospf process-id [router-id router-id]</code>	Enable an OSPF process, and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#maximum load-balancing number</code>	Configure the maximum number of paths for IP equivalent multi-path load balancing.

5.8.5 Configuring OSPF network

Configuring OSPF network type

Configure the OSPF network type for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)# ip ospf network { broadcast non- broadcast ptmp ptp }	Configuring the network type of the Layer 3 interface. By default, it is the broadcast network.

Configuring DR election priority

Configure the DR election priority for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)# ip ospf priority priority	Configure the DR election priority on the IP interface. By default, it is 1.

Configuring OSPF NBMA network neighbor

Configure the OSPF NBMA network neighbor for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interfac e interface-type <i>interface-number</i>	Enter interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)# ip ospf network non- broadcast Raisecom(config- gigaethernet1/1/1)# exit	Configure the Layer 3 interface network mode to NBMA and exit Layer 3 interface configuration mode.
4	Raisecom(config)# router ospf process-id [router- id router-id]	Enable an OSPF process and enter OSPF configuration mode.

Step	Command	Description
5	<pre>Raisecom(config-router-ospf)#neighbor ip-address [priority priority]</pre>	<p>Configure the NBMA neighbor and its priority.</p> <p>By default, no NBMA neighbor is configured and the priority is 0 when you configure the NBMA neighbor.</p>



Caution

Priorities configured by the **neighbour** and **ip ospf priority priority** commands are different:

- The priority configured by the **neighbour** command indicates that whether the neighbor has the right to vote. If you configure the priority to 0 when configuring the neighbor, the local router judges that the neighbor has no right to vote and will not sent Hello packets to the neighbor. This method helps reduce the number of Hello packets transmitted through the network during DR and BDR election processes. However, if the local router is a DR or BDR, it will send the Hello packet to the neighbor, whose priority is configured to 0, to establish the neighboring relationship.
- The priority configured by the **ip ospf priority priority** command is used for actual DR election.

5.8.6 Optimizing OSPF network

Configuring OSPF packet timer

Configure the OSPF packet timer for the ISCOM3000G series switch as below.

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#interface interface-type interface- number</pre>	Enter interface configuration mode.
3	<pre>Raisecom(config- gigaethernet1/1/1)#ip ospf dead-interval seconds</pre>	<p>Configure the OSPF neighbor dead interval.</p> <p>By default, it is 4 times of Hello packet delivery interval. If no Hello packet delivery interval is configured, it is 40s for P2P and Broadcast interfaces and 120s for P2MP and NBMA interfaces by default.</p>
4	<pre>Raisecom(config- gigaethernet1/1/1)#ip ospf hello-interval seconds</pre>	<p>Configure the ODPF Hello packet delivery interval.</p> <p>By default, it is 10s for P2P and Broadcast interfaces and 30s for P2MP and NBMA interfaces</p>
5	<pre>Raisecom(config- gigaethernet1/1/1)#ip ospf poll-interval seconds</pre>	<p>Configure the OSPF Poll timer interval.</p> <p>By default, it is 120s.</p>

Step	Command	Description
6	<code>Raisecom(config-gigaethernet1/1/1)#ip ospf retransmit-interval seconds</code>	Configure the LAS retransmission interval on the IP interface. By default, it is 5s.
7	<code>Raisecom(config-gigaethernet1/1/1)#ip ospf transmit-delay seconds</code>	Configure the LSA retransmission delay on the IP interface. By default, it is 1s.

Caution

- When the dead-interval is not manually configured, the dead-interval and poll-interval are changed to 4 times of the hello-interval after the hello-interval is configured.
- When the dead-interval is manually configured, no effect is brought to the dead-interval and poll-interval after hello-interval is configured. No matter whether you configure the poll interval or not, the poll-interval changes with the dead-interval. Therefore, we recommend configuring these 3 values in the following order: hello-interval, dead-interval, and poll-interval.

Configuring SPF calculation interval

When the OSPF Link State Database (LSDB) changes, it needs to re-calculate the shortest path. If the network changes frequently and it needs to calculate the shortest path immediately, it will occupy a great amount of system resources and affect efficiency of the router. By adjusting the SPF calculation interval, you can prevent some effects brought by frequent network changes.

Configure the SPF calculation interval for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ospf process-id [router-id router-id]</code>	Enable an OSPF process and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#timers spf delay-time hold-time</code>	Configure the calculation delay and interval of the OSPF route. By default, the calculation delay is 2s and the calculation interval is 3s.

Configuring OSPF passive interface

To prevent some OSPF routing information from being obtained by some routers on the network, you can configure the interface to an OSPF passive interface to disable the interface to send OSPF packets.

Configure the OSPF passive interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#ip ospf passive-interface enable	Enable passive interface on the OSPF interface. By default, it is disabled.

Configuring MTU ignorance

By default, the value of MTU domain in the DD packet is the MTU value of the interface, which sends the DD packet. Default MTU values may vary on devices. In addition, if the MTU value of the DD packet is greater than the one of the interface, the DD packet will be discarded. To ensure receiving the DD packet properly, enable MTU ignorance to configure the MTU value to 0. Therefore, all devices can receive the DD packet.

Configure MTU ignorance for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#ip ospf mtu-ignore enable	Enable MTU ignorance on the IP interface. By default, MTU ignorance is disabled on the IP interface to check MTU of the OSPF Hello packet.

5.8.7 Configuring OSPF authentication mode

Configuring OSPF area authentication mode

All routers in an area need to be configured with the identical area authentication mode (non-authentication, simple authentication, or MD5 authentication). The OSPF area has no authentication password but adopts the interface authentication password. If no interface authentication password is configured, the empty password will be used for authentication.

Configure the OSPF area authentication mode for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router ospf <i>process-id [router-id router-id]</i>	Enable an OSPF process and enter OSPF configuration mode.

Step	Command	Description
3	<code>Raisecom(config-router-ospf)#area <i>area-id</i> authentication { md5 simple }</code>	Configure the area authentication mode. By default, it is non-authentication.

Configuring OSPF interface authentication mode

Packet authentication prioritizes selecting the interface authentication mode. If the interface authentication mode is configured to non-authentication mode, the area authentication mode will be selected. OSPF interfaces cannot establish the neighbor relationship unless the authentication mode and authentication password are identical.

Configure the OSPF interface authentication mode for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#ip ospf authentication { md5 simple }</code>	Configure the authentication mode of the IP interface. By default, it is non-authentication. It means adopting the area authentication mode.
4	<code>Raisecom(config- gigaethernet1/1/1)#ip ospf authentication-key { simple [0 7] password md5 { [key-id [0 7] password] keychain <i>keychain-name</i> } }</code>	Configure the authentication password of the IP interface.

5.8.8 Configuring Stub area

For the non-backbone area at the edge of Autonomous System (AS), you can configure the **stub** command on all routers in the area to configure the area to a Stub area. In this case, Type5 LSA, which is used to describe external routes of the AS, cannot be flooded in the Stub area. This facilitates reducing the routing table size.

Configure the Stub area for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#rou ter ospf <i>process-id</i> [<i>router-id router- id</i>]</code>	Enable an OSPF process and enter OSPF configuration mode.

Step	Command	Description
3	Raisecom(config-router-ospf)# area area-id stub [no-summary]	Configure the area to a Stub area. The no-summary parameter is used to disable the ABR to send Summary LSA to the Stub area. It means that it is a Totally Stub area and the ABR is available for the Stub only. By default, no area is the Stub area.
4	Raisecom(config-router-ospf)# area area-id default-cost cost	Configure the default route cost of the Stub area. This command is available for the ABR in the Stub area only. By default, it is 1.
5	Raisecom(config-router-ospf)# area area-id nssa [no-summary]	(Optional) configure the area to NSSA.

Caution

- All routers in the Stub area must be configured with the Stub property through the **area area-id stub** command.
- To configure an area to a Totally Stub area, all routers in the area must be configured by the **area area-id stub** command. In addition, all ABRs in the area must be configured by the **area area-id stub no-summary** command.
- The backbone area cannot be configured to the Stub area.
- ASBR should not be in the Stub area. It means that routers besides the AS cannot be transmitted in the Stub area.

5.8.9 Controlling OSPF routing information

Configuring OSPF redistributed routes

Configure OSPF redistributed routes for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router ospf process-id [router-id router-id]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)# redistribute { static connected isis bgp } [metric metric] [metric-type { 1 2)] [tag tag-value] [route-map map-name]	Configure OSPF route redistribution polity. By default, no external route is redistributed. When an external route is redistributed: <ul style="list-style-type: none"> • When the directly-connected and static route is redistributed, the metric is 1 by default. When other routes are redistributed, take the

Step	Command	Description
	<code>Raisecom(config-router-ospf)#redistribute ospf [process-id] [metric metric] [metric-type { 1 2 } [tag tag-value] [route-map map-name]</code>	original metric of the external route as the metric of the LSA. <ul style="list-style-type: none"> • If no Metric-type is specified, the Metric-type is Type2 by default. • If no Tag is specified, take the original Tag of the external route as the Tag of the LSA.
4	<code>Raisecom(config-router-ospf)#redistribute limit limit-number</code>	Configure the threshold of redistributed OSPF external routes. By default, no threshold is configured.

Configuring inter-area route aggregation

If there are sequent network segments in the area, you can configure route aggregation on the ABR to aggregate these network segments to a network segment. When sending routing information, the ABR generates Type3 LSA in units of network segment.

Configure inter-area route aggregation for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ospf process-id [router-id router-id]</code>	Enable an OSPF process and enter OSPF configuration mode.
3	<code>Raisecom(config-router-ospf)#area area-id range ip-address ip-mask [not-advertise]</code>	Configure the inter-area route aggregation. By default, no inter-area route aggregation is configured. When you configure the aggregated route, the cost is the maximum Metric of the LSA by default. In addition, the aggregated route is redistributed.

Configuring redistributed external route aggregation

After the external route is redistributed, configure route aggregation on the ASBR. The ISCOM3000G series switch just puts the aggregated route on the ASE LSA. This helps reduce the number of LSAs in the LSDB.

Configure inter-area route aggregation for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ospf process-id [router-id router-id]</code>	Enable an OSPF process and enter OSPF configuration mode.

Step	Command	Description
3	Raisecom(config-router-ospf)# summary-address <i>ip-address ip-mask</i> [not-advertise] [metric <i>metric</i>]	Aggregate external routes. By default, external routes are not aggregated. When external aggregates are aggregated, the Metric is the maximum Metric of the LSA by default.

Configuring default route redistribution

Configure default route redistribution for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)# default-information originate [always] [metric <i>metric</i>] [type { 1 2 }]	Redistribute the default route. By default, no default route is generated. When the default LSA is generated, if the always key word is specified, the default Metric is 1. If the always key word is not specified, the Metric is 10.

5.8.10 Configuring OSPF routing policy

Configuring OSPF receiving policy

Configure the OSPF receiving policy for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ip prefix-list <i>list-name</i> { permit deny } <i>ip-address mask-length</i> [ge <i>ge-length</i>] [le <i>le-length</i>]	Configure the IP prefix list.
3	Raisecom(config)# access-list <i>acl-number</i>	Create an IP ACL, and enter ACL configuration mode. When the <i>acl-number</i> is between 1000 and 1999, this operation enters basic IP ACL configuration mode.

Step	Command	Description
	<code>Raisecom(config-ipv4-std)#rule [rule-id] { deny permit } { source-ip-address source-ip-mask any }</code>	Configure basic IP ACL rules.
4	<code>Raisecom(config)#router ospf process-id [router- id router-id]</code>	Enable an OSPF process, and enter OSPF configuration mode.
5	<code>Raisecom(config-router-ospf)#distribute-list { ip-access-list acl- number prefix-list list- name } in</code>	Configure the OSPF filtering policy for receiving the OSPF inter-area routes, intra-area routes, and AS external routes.



Note

- Before configuring OSPF receiving policy, ensure that the IP ACL used by the OSPF receiving policy has been created.
- When the ISCOM3000G series switch performs filtering based on IP ACL, all routes, which match with the ACL, can pass if the ACL mode is configured to permit. Others are filtered.
- You cannot modify the IP ACL unless it is not used by any routing policy.
- Different from IP ACL, the IP prefix-list can be modified even if it is being used.
- If the configured IP prefix list does not exist, the ISCOM3000G series switch does not filter received routes.

Configuring OSPF distributing policy

Configure the OSPF receiving policy for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip prefix- list list-name { permit deny } ip-address mask-length [ge ge-length] [le le- length]</code>	Configure the IP prefix-list. You can use the no ip prefix-list list-name [index number] command to delete the configuration.
3	<code>Raisecom(config)#access-list acl-number</code>	Configure the IP ACL rule. At present, the ISCOM3000G series switch just supports matching the address prefix information of the route by specifying the destination IP address and subnet mask.
	<code>Raisecom(config-ipv4- basic)#rule [rule-id] { deny permit } { source- ip-address source-ip-mask any }</code>	Configure basic IP ACL rules.

Step	Command	Description
4	<code>Raisecom(config)#router ospf process-id [router-id router-id]</code>	Enable an OSPF process and enter OSPF configuration mode.
5	<code>Raisecom(config-router-ospf)#distribute-list { ip- access-list acl-number prefix-list list-name } out</code>	Configure the filtering policy that the OSPF releases 5 types of LSAs to the AS.
6	<code>Raisecom(config-router-ospf)#distribute-list { ip- access-list acl-number prefix-list list-name } out [static connected isis bgp]</code>	Configure the OSPF distributing policy.
	<code>Raisecom(config-router-ospf)#distribute-list { ip- access-list acl-number prefix-list list-name } out ospf process-id</code>	



Note

- Before configuring OSPF global distributing policy, ensure that the IP ACL used by the OSPF global distributing policy has been created.
- You cannot modify the IP ACL unless it is not used by any routing policy.
- Different from IP ACL, the IP prefix-list can be modified even it is being used.
- After global distributing policy is configured, routes cannot be redistributed to the local LSDB unless it passes the global distributing policy. After protocol distributing policy is configured, the route can be redistributed through the protocol distributing policy.
- After protocol distributing policy is configured, the redistributed protocol route can be redistributed to the local LSDB through the protocol distributing policy. If global distributing policy is also configured, the route must be redistributed through the global distributing policy.

Configuring Type3 LSA filtering policy

Configure the Type3 LSA filtering policy for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip prefix- list list-name { permit deny } ip-address mask- length [ge ge-length] [le le-length]</code>	Configure the IP prefix-list. You can use the no ip prefix-list list-name [index number] command to delete the configuration.
3	<code>Raisecom(config)#router ospf process-id [router-id router-id]</code>	Enable an OSPF process and enter OSPF configuration mode.

Step	Command	Description
4	<code>Raisecom(config-router-ospf)#area area-id filter prefix-list list-name { in out }</code>	Configure Type3 LSA filtering policy in the area.



Note

If the configured filtering policy does not exist, it is believed that the command fails to configure the filtering policy and no filtering operation is performed on received routes.

5.8.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show ip ospf [process-id]</code>	Show OSPF basic information.
2	<code>Raisecom#show ip ospf [process-id] interface [interface-type interface-number]</code>	Show OSPF interface information.
3	<code>Raisecom#show ip ospf [process-id] neighbor [interface-type interface-number] [neighbor-id]</code>	Show OSPF neighbor information.
4	<code>Raisecom#show ip ospf [process-id] route</code>	Show OSPF routing information.
5	<code>Raisecom#show ip ospf [process-id] database [max-age self-originate]</code> <code>Raisecom#show ip ospf [process-id] database [router network summary asbr-summary external] [linkstate-id] [adv-router ip-address self-originate]</code> <code>Raisecom#show ip ospf [process-id] database statistics</code>	Show OSPF link status database information and statistics.
6	<code>Raisecom#show ip ospf [process-id] border-routers</code>	Show information about routers at edges of the area and AS.
7	<code>Raisecom#show ip ospf [process-id] neighbor statistics</code>	Show OSPF statistics or OSPF neighbor statistics.
8	<code>Raisecom#show ip ospf [process-id] summay-address</code>	Show OSPF ASBR external route aggregation information.

5.8.12 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom# clear ip ospf [<i>process-id</i>] process [graceful]	Restart the OSPF process.

5.9 ISIS

5.9.1 Configuring ISIS basic functions

To run ISIS normally, start ISIS process and configure the name of the network entity. You can start the ISIS process in the follow two ways:

- Use the **router isis** command.
- Use the **ip router isis** command or **ipv6 router isis** command on the interface.

Configure ISIS basic functions for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router isis [<i>area-tag</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config)# interface <i>interface-type interface-number</i>	(Optional) enter interface configuration mode.
4	Raisecom(config- tengigabitethernet1/1/1)# ip router isis [<i>area tag</i>] Raisecom(config- tengigabitethernet1/1/1)# exit Raisecom(config- tengigabitethernet1/1/1)# exit	(Optional) start an ISIS process on the interface.
5	Raisecom(config)# router isis [<i>area-tag</i>]	Enter ISIS configuration mode.
6	Raisecom(config-router-isis)# net <i>network-entity</i>	Configure the network identifier entity of ISIS routing process.

5.9.2 Configuring ISIS routing

Configuring router type

Configure the router type for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router isis [area-tag]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#is-type { level-1 level-1-2 level-2-only }	Configure the router type. By default, it is level-1-2.
4	Raisecom(config-router-isis)#hostname dynamic	(Optional) enable the switching mechanism of dynamic hostname. By default, it is disabled.

Configuring overhead

The ISIS overhead can be configured automatically or manually. After the automatic calculation of the overhead on the interface is enabled, the ISIS will automatically calculate the overhead on the interface according to the following rules:

- When the type of overhead is configured to wide, ISIS will automatically calculate the value according to the interface rate, the formula is: overhead on the interface = reference rate/interface rate × 10, and the max value obtained is 16777214.
- When the type of overhead is configured to narrow, the interface overhead is:
 - 60 for interface rate between 1 and 10 Mbit/s
 - 50 for interface rate between 1 and 100 Mbit/s
 - 40 for interface rate between 101 and 155 Mbit/s
 - 30 for interface rate between 156 and 622 Mbit/s
 - 20 for interface rate between 623 and 2500 Mbit/s
 - 10 for other conditions

Configure the overhead for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router isis [area-tag]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#metric-style { narrow transition wide } Raisecom(config-router-isis)#exit	Configure the type of ISIS overhead. By default, it is narrow.
4	Raisecom(config-router-isis)#auto-metric { enable disable }	Enable automatic calculation of overhead on the interface. By default, it is disabled.
5	Raisecom(config)#interface interface-type interface-number	Enter interface configuration mode.

Step	Command	Description
6	<code>Raisecom(config-tengigabitethernet1/1/1)#isis metric <i>metric</i> [<i>level-1</i> <i>level-2</i>]</code>	Configure the overload value on the interface. By default, it is 10.

Configuring reference bandwidth

Configure the reference bandwidth for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router isis [<i>area-tag</i>]</code>	Start an ISIS process and enter ISIS configuration mode.
3	<code>Raisecom(config-router-isis)#reference-bandwidth <i>bandwidth</i></code>	Configure reference rate referred to while calculating technical link overhead. By default, it is 100 Mbit/s.

Configuring ISIS administrative distance

Configure the ISIS administrative distance for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router isis [<i>area-tag</i>]</code>	Start an ISIS process and enter ISIS configuration mode.
3	<code>Raisecom(config-router-isis)#distance <i>distance</i> [<i>ip-address mask-address</i>]</code>	Configure the management distance of ISIS routing. By default, it is 115.

5.9.3 Configuring ISIS network

Configuring type of ISIS network

Configure the type of the ISIS network for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter interface configuration mode.

Step	Command	Description
3	<code>Raisecom(config-tengigabitethernet1/1/1)#isis network point-to-point</code>	Configure the type of interface network to P2P. By default, it is broadcast.

Adjacencies

This configuration is only applied to Level-1-2 routers.

- If the host is Level-1-2 router, it needs to establish association with peer router in certain area (Level-1 or Level-2). Configuring an area for establishing adjacency can restrain the interface from receiving and sending the Hello packet only from that certain area.
- In the point-to-point link, the interface can only receive and send one type of Hello packet. Configuring an area for establishing adjacency can reduce the processing time between routers and save bandwidth.

Configure adjacencies for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.
3	<code>Raisecom(config-tengigabitethernet1/1/1)#isis circuit-type { level-1 level-1-2 level-2-only }</code>	Configure an area for establishing interface adjacency. By default, it is Level-1-2.

Configuring DIS priority

The Designated Intermediate System (DIS) election of the ISIS is preemptive and predictable. There is not backup DIS in the ISIS. Therefore, when one DIS does not work, another DIS will be elected. The rules for electing the DIS are as below:

- The router with highest DIS election priority will be elected. If all routers have the same priority, the router with biggest MAC address will be elected.
- The DIS in Level-1 and Level-2 are elected respectively but the result may be not the same IS.
- The interval between sending Hello packet by DIS is 1/3 times of that by common routers, which can ensure that the invalid DIS be detected in no time.

Configure the DIS priority for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.

Step	Command	Description
3	<code>Raisecom(config-tengigabitethernet1/1/1)#isis priority priority [level-1 level-2]</code>	Configure the DIS priority on the interface in different areas. By default, it is 64.

5.9.4 Optimizing ISIS network

Configuring ISIS packet timer

The invalid number of Hello packet is decided by the Holddown time. If the router cannot receive Hello packet sent by the peer router within the Holddown time, the peer router can be considered invalid. The Holddown time is configured based on interface and different router in the same area can set different the Holddown time.

By changing the time interval for sending Hello packet of ISIS or the invalid number of Hello packet, you can adjust the Holddown time.

Configure the ISIS packet timer for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.
3	<code>Raisecom(config-tengigabitethernet1/1/1)#isis hello-interval seconds [level-1 level-2]</code>	Configure the interval between sending Hello packets on the interface of different areas. By default, it is 10s.
4	<code>Raisecom(config-tengigabitethernet1/1/1)#isis hello-multiplier number [level-1 level-2]</code>	Configure the number of invalid ISIS neighbor Hello packets on the interface of different areas.
5	<code>Raisecom(config-tengigabitethernet1/1/1)#isis csnp-interval seconds [level-1 level-2]</code>	Configure the interval between sending CSNP packets on the interface of different areas in the broadcast network. By default, it is 10s.

Configuring LSP

Configure LSP for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.

Step	Command	Description
2	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter interface configuration mode.
3	<code>Raisecom(config- tengigabitethernet1/1/1)#isis lsp-interval milliseconds</code>	Configure the interval between sending LSP packets. By default, it is 33ms.
4	<code>Raisecom(config- tengigabitethernet1/1/1)#isis retransmit-interval seconds Raisecom(config- tengigabitethernet1/1/1)#exit</code>	Configure retransmission interval between sending LSP packets on the point-to-point link. By default, it is 5s.
5	<code>Raisecom(config)#router isis [area-tag] Raisecom(config-router- isis)#lsp-gen-interval seconds [level-1 level-2]</code>	Configure the interval between generating LSP. By default, it is 5s.
6	<code>Raisecom(config-router- isis)#max-lsp-lifetime seconds [level-1 level-2]</code>	Configure the longest TTL of the LSP generated. By default, it is 1200s.
7	<code>Raisecom(config-router- isis)#lsp-refresh-interval seconds [level-1 level-2]</code>	Configure the refresh time of LSP. By default, it is 900s.
8	<code>Raisecom(config-router- isis)#ignore-lsp-errors</code>	Enable ignoring the checkout for LSP. By default, it is disabled.

Configuring interval for calculating SPF

Configure the interval for calculating SPF for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router isis [area-tag]</code>	Start an ISIS process and enter ISIS configuration mode
3	<code>Raisecom(config-router- isis)#spf-interval seconds [level-1 level-2]</code>	Configure the interval for calculating SPF in the ISIS. By default, it is 10s.
4	<code>Raisecom(config-router- isis)#set-overload-bit</code>	(Optional) enable overload bit. By default, it is disabled.

Configuring ISIS passive interface

If you do not wish the ISIS routing information to be obtained by the router in a network, you can configure the interface to ISIS passive interface to prevent it from sending ISIS packets.

Configure ISIS passive interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-tengigabitethernet1/1/1)#isis passive	Enable the passive function on ISIS interface. By default, it is disabled.

Configuring Hello packet padding

Hello packet padding refers to padding Hello packet with MTU field, thus notifying peer and local interface of the MTU.

Configure Hello packet padding for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router isis [<i>area-tag</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#hello padding	Enable Hello Packet padding. By default, all types of interface are padded with standard Hello packet.

5.9.5 Configuring ISIS authentication

Configure ISIS authentication for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router isis [<i>area-tag</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#area-password { <i>clear password</i> <i>md5 password</i> } [authenticate snp { send-only validate }]	Configure Level-1 area authentication.

Step	Command	Description
4	<code>Raisecom(config-router-isis)#domain-password { clear password md5 password } [authenticate snp { send-only validate }]</code>	Configure Level-2 area authentication.

Configuring ISIS interface authentication

The packet authentication gives preference to interface authentication mode. If the interface authentication mode is no authentication, the area authentication mode will be selected. Only when the authentication mode and the password are the same can the ISIS interface establish neighborhood.

Configure ISIS interface authentication for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.
3	<code>Raisecom(config-tengigabitethernet1/1/1)#isis password { clear password md5 password } [level-1 level-2]</code>	Configure the ISIS authentication mode and password on the interface.

5.9.6 Controlling ISIS routing information

Configuring ISIS redistributed routes

Configure ISIS redistributed routes for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router isis [area-tag]</code>	Start an ISIS process and enter ISIS configuration mode.
3	<code>Raisecom(config-router-isis)#redistribute { connected static rip ospf process-id isis area-tag bgp } [route-map map-name] [level-1 level-2 level-1-2] [metric metric] [metric-type { external internal }]</code>	Configure protocol route redistributed policy. By default, ISIS does not redistribute other protocol routes. If you do not specify the area when it redistributes routes, it will redistribute routes to Level-2 by default.

Step	Command	Description
4	<code>Raisecom(config-router-isis)#redistribute isis ip level-2 into level-1</code>	Configure ISIS route redistributed policy among areas. By default, the routing information in level-2 will not be distributed to Level-1.

Configuring redistribution of default route

Configure redistribution of the default route for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router isis [area-tag]</code>	Start an ISIS process and enter ISIS configuration mode.
3	<code>Raisecom(config-router-isis)#default-information originate</code>	Configure redistribution of the Level-2 default route.

Configuring ISIS route aggregation

Route aggregation can not only reduce the scale of routing table but also shrink the size of LSP packet generated by the local router and reduce the scale of LSDB.

- The aggregated route can be the route found by the ISIS and the route redistributed externally.
- The overload of aggregated route takes the minimum overload among all the routes aggregated.
- The router only aggregates the route generated in the local LSP.

Configure ISIS route aggregation for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router isis [area-tag]</code>	Start an ISIS process and enter ISIS configuration mode.
3	<code>Raisecom(config-router-isis)#summary-address ip-address mask-address [level-1 level-2 level-2-only]</code>	Configure route aggregation among areas. By default, there is no route aggregation. The overload while configuring route aggregation is the maximum Metric in the LSA. And the route aggregation will be advertised.

Configuring ISIS equal-cost multi-path load balancing

Configure ISIS equal-cost multi-path load balancing for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router isis [area-tag]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#maximum load-balancing number	Configure the maximum number of ISIS equal-cost multi-path load balancing paths.

5.9.7 Configuring ISIS BFD

Configure ISIS BFD for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router isis [area-tag]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#isis bfd enable	Enable global ISIS BFD. By default, it is disabled.
4	Raisecom(config-router-isis)#bfd all-interfaces	Enable ISIS BFD on all interfaces. By default, it is disabled.

5.9.8 Configuring ISIS GR

Configure ISIS graceful restart; namely, the switchover ensures no service interruption while the ISCOM3000G series switch is restarted.

Configuring ISIS GR for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router isis [area-tag]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#graceful-restart	Enable ISIS graceful restart. By default, it is disabled.
4	Raisecom(config-router-isis)#graceful-restart interval seconds	Enable the interval of ISIS graceful restart. By default, it is 300s.

Step	Command	Description
5	Raisecom(config-router-isis)# graceful-restart sa enable	Enable ISIS graceful restart to restrain the neighbor device from advertising routes. By default, it is enabled.

5.9.9 Checking configurations

Use the following commands to check configurations.

Step	Command	Description
1	Raisecom# show isis interface [detail]	Show ISIS interface.
2	Raisecom# show isis neighbor [<i>system-id</i> detail]	Show ISIS neighbors.
3	Raisecom# show isis hostname	Show the mapping between host name and system ID.
4	Raisecom# show isis route	Show ISIS IPv4 route.
5	Raisecom# show isis topology [level-1 level-2]	Show ISIS topology.
6	Raisecom# show isis database [<i>lsp-id</i> detail] [level-1 level-2] [local]	Show database about ISIS link status.
7	Raisecom# show isis summary	Show basic configurations about ISIS.

5.9.10 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom# clear isis process area-tag [graceful-restart]	Clear ISIS.
Raisecom# clear isis neighbor [<i>system-id</i>]	Clear ISIS neighbors.

5.10 BGP

5.10.1 Configuring BGP basic functions

Configure BGP basic functions for the ISCOM3000G series switch as below.

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

Step	Command	Description
2	<code>Raisecom(config)#router bgp as-id</code>	Enable BGP and create a BGP instance. Enter BGP configuration mode.
3	<code>Raisecom(config-router)#bgp router-id router-id</code>	Configure the BGP Router ID.

5.10.2 Configuring BGP redistributed routes

Configuring BGP neighbors

BGP uses the TCP connection. Therefore, when configuring BGP, you need to configure the IP address of the BGP neighbor. The BGP neighbor can be non-adjacent routers. You can establish a BGP neighborship. To enhance stability of the BGP connection, we recommend using the loopback interface address to establish the connection.

Specified IP addresses of BGP neighbors are divided into 2 types:

- Interface IP address of the directly-connected BGP neighbor
- Loopback interface address of the BGP neighbor, where the route can reach. In this mode, you need to configure the route update source to ensure that the BGP neighbor is established properly.

Configure BGP neighbors for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config) #router bgp as- id</code>	Enter BGP configuration mode.
3	<code>Raisecom(config- router)#neighbor ip-address remote-as as-id</code>	Create a BGP neighbor and specify the AS ID of the BGP neighbor. By default, there is no BGP neighbor.
4	<code>Raisecom(config- router)#neighbor ip-address1 update-source ip-address2 Raisecom(config- router)#neighbor ip-address1 update-source interface-type interface-number</code>	Configure to use the specified local source interface for establishing the BGP connection. The BGP connection can be established successfully when any end is configured with the update source properly. However, it may take more time to establish the connection. To ensure that the stability of the connection, we recommend configure update source addresses for both ends.
5	<code>Raisecom(config- router)#neighbor ip-address weight weight</code>	Configure the weight of the route learned from the BGP neighbor. By default, it is 0.

Step	Command	Description
6	<code>Raisecom(config-router)#neighbor ip-address activate</code>	Enable the BGP neighbor to exchange the specified address family route. By default, enable the BGP neighbor to exchange the IPv4 unicast address family route only.
7	<code>Raisecom(config-router)#neighbor ip-address default-originate</code>	Enable to send the default route to the BGP neighbor. By default, do not send the default route to the BGP neighbor.
8	<code>Raisecom(config-router)#neighbor ip-address description string</code>	Configure descriptions of the BGP neighbor. By default, there is no description of the BGP neighbor.
9	<code>Raisecom(config-router)#neighbor ip-address next-hop-self</code>	Configure the router to modify the next-hop address of the route to the IP address of the Tx end, when the router releases the route to the BGP neighbor. By default, when the router releases the route to the BGP neighbor, the next-hop address of the route is identical to the next-hop IP address of the route in the local BGP routing table.
10	<code>Raisecom(config-router)#bgp log-neighbor-changes</code>	Enable the log which is used to inform the BGP neighbor of state change. By default, it is enabled.
11	<code>Raisecom(config-router)#neighbor ip-address shutdown</code>	(Optional) disallow the ISCOM3000G series switch to establish the BGP connection with the specified BGP neighbor. By default, establishing the BGP connection with the BGP neighbor is allowed.
12	<code>Raisecom(config-router)#neighbor ip-address ebgp-multihop [ttl]</code>	(Optional) allow the ISCOM3000G series switch to establish the EBGp connection with BGP neighbors in the indirectly-connected network. In addition, specify the maximum hops allowable for the specified EBGp connection. By default, only physically directly-connected BGP neighbors can establish the EBGp connection.
13	<code>Raisecom(config-router)#bgp redistribute-internal</code>	Redistribute the routing information, learned from the IBGP neighbor, to the IGP. By default, redistributing the IBGP route to the IGP is disabled.

Configuring BGP to redistributed routes

The BGP cannot discover the route. Therefore, it needs to redistribute routes based on other protocols (such as IGP and static route) to the BGP routing table to make these routes be transmitted in or between ASs.

Configure BGP redistributed routes for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router bgp <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)# redistribute { connected static ospf isis } [metric <i>metric</i>] [route-map <i>map</i>]	Configure the BGP to redistribute routes, which based on other protocols, to the BGP routing table.

Configuring BGP to redistribute static routes

Configure BGP to redistribute static routes for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router bgp <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)# network <i>ip-address</i> [<i>mask-address</i>] [route-map <i>route-map-name</i>]	Redistribute static routes to the BGP routing table.

Configuring redistribution of default route

Configure redistribution of the default route for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router bgp <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)# default-information originate	Configure the BGP to redistribute the default route.

5.10.3 Configuring BGP routing

Configuring BGP administrative distance

Configure the BGP administrative distance for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router bgp as-id	Enter BGP configuration mode.
3	Raisecom(config-router)#distance bgp ebgp distance1 ibgp distance2 local distance3	Configure the administrative distance of the BGP route. <ul style="list-style-type: none"> • The administrative distance of external routes (routes learned through the EBGp) is 20 by default. • The administrative distance of internal routes (routes learned through the IBGP) is 200 by default. • The administrative distance of local routes (BGP routes redistributed through the aggregation command) is 200 by default.

Configuring BGP path selection policy

Configure the BGP path selection policy for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router bgp as-id	Enter BGP configuration mode.
3	Raisecom(config-router)#bgp deterministic-med	(Optional) configure the BGP not to consider the receiving sequence when selecting the route. By default, the BGP considers the receiving sequence when selecting the route.
4	Raisecom(config-router)#bgp always-compare-med	Configure the BGP to compare the MED for all paths.
5	Raisecom(config-router)#bgp bestpath compare-routerid	Configure the BGP optimum path selection policy to selecting the route with the minimum Router ID. By default, the BGP selects the BGP route which is received earliest.
6	Raisecom(config-router)#bgp bestpath as-path ignore	Configure the BGP to ignore the AS-PATH property when selecting the optimum path.

Configuring BGP and IGP route synchronization

After BGP synchronization is enabled,

- The BGP route can participate into selection if it meets the following requirements. Then, if it is selected, the RM is applied to the routing table.
 - In the RM, the BGP route learned through IBGP can exactly match the route learned through IGP.

- The administrative distance of the IGP route is shorter than the administrative distance of the BGP route.
- The BGP route status will flap and it may participate into selection or not, if it meets the following requirements:
 - The BGP route learned through IBGP can exactly match the route learned through IGP.
 - The administrative distance of the IGP route is greater than the administrative distance of the BGP route.

Configure BGP and IGP route synchronization for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router bgp as-id	Enter BGP configuration mode.
3	Raisecom(config- router)#synchronization	Enable BGP and IGP route synchronization. By default, it is disabled.

Configuring route dampening

Route flapping is one route instability form. Route flapping refers that a route appears and then disappears alternatively. Route dampening can be used to overcome route flapping.

Configure route dampening for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)# router bgp as-id	Enter BGP configuration mode.
3	Raisecom(config- router)#bgp dampening half- life reuse suppress max- suppress-time	Enable BGP route dampening or modify the BGP route dampening parameter. By default, BGP route dampening is disabled. After BGP dampening is enabled, the default values of all parameters are shown as below. <ul style="list-style-type: none"> • Half-life: 15min • Reuse value: 750 • Dampening threshold: 2000 • Maximum suppress time: 60min.

5.10.4 Configuring BGP network

Configuring RR

Prefix notification rules of the Router Reflector (RR) are shown as below:

- Rule 1: the RR just notifies or reflects the optimum path to which it returns.

- Rule 2: the RR always notifies the prefix to the BGP neighbor.
- Rule 3: when notifying the prefix, the RR client follows the common IBGP loopback prevention rule.
- Rule 4: to notify the IBGP neighbor, client, or non-client of the prefix, follow rules 5, 6, and 7.
- Rule 5: the RR will notify all its clients and non-clients of the prefix, which is learned from the external BGP neighbor.
- Rule 6: the RR will notify all its clients of the prefix, which reaches the RR through a non-client IBGP neighbor.
- Rule 7: the RR will notify other clients and non-clients of the route, if the prefix reaches the RR through a client.



In some networks, clients of the RR have established a full-connection. They can exchange routing information directly without using route reflection. In this case, you can use the **no bgp client-to-client reflection** command to disable route reflection among clients of the RR.

To enhance network reliability and prevent faults from occurring at a node, you need to configure one or more RR in a cluster. You can configure the identical cluster ID for all RRs in the cluster to identify the cluster. This helps avoid the loopback.

Configure RR for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp as-id</code>	Enter BGP configuration mode.
3	<code>Raisecom(config-router)#neighbor ip-address route-reflector-client</code>	Configure the device to the RR and set the specified neighbor as the client of the RR. By default, route reflection is disabled.
4	<code>Raisecom(config-router)#bgp client-to-client reflection</code>	Enable route reflection among clients of the RR. By default, route reflection among clients of the RR is enabled.
5	<code>Raisecom(config-router)#bgp cluster-id cluster-id</code>	Configure the cluster ID of the RR. By default, it is the Router ID.

Configuring BGP default local priority

Configure BGP default local priority for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp as-id</code>	Enter BGP configuration mode.

Step	Command	Description
3	Raisecom(config-router)# bgp default local-preference <i>priority</i>	Configure BGP default local priority. By default, it is 100.

Configuring BGP timer

Configure the BGP timer for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router bgp <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)# bgp scan-time <i>time</i>	Configure the interval for scanning the BGP routing table. By default, it is 60s.
4	Raisecom(config-router)# timers bgp <i>keep-alive-time hold-time</i>	Configure the lifetime and maintenance time of the global BGP connection. By default, the lifetime and maintenance time of the global BGP connection are configured to 60s and 180s respectively.
5	Raisecom(config-router)# neighbor ip-address timers <i>keep-alive-time hold-time</i>	Configure the lifetime and maintenance time of the neighbor. By default, the lifetime and maintenance time of the neighbor are identical to the ones of the global BGP connection.

Configuring BGP route aggregation

- At present, the ISCOM3000G series switch supports BGP manual aggregation. Manual aggregation is only valid for existing routes in the BGP local routing table. If there is no route, whose mask size is greater than 16 bytes, in the BGP routing table, the BGP will not release the aggregated route even you use the aggregate 10.1.1.1 255.255.0.0 command to aggregate the route.
- The aggregated route cannot be set to the default route (0.0.0.0/0).

Configure BGP route aggregation for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router bgp <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)# aggregate-address <i>ip-address mask-address</i>	Configure BGP route aggregation and release the aggregated route and detail route.

Step	Command	Description
4	Raisecom(config-router)# aggregate-address <i>ip-address mask-address</i> summary-only	Configure BGP route aggregation, release the aggregated route only and dampens the detail route.
5	Raisecom(config-router)# aggregate-address <i>ip-address mask-address</i> as-set	Configure BGP route aggregation and set the AS_SET option. The generated aggregated route includes all AS IDs in the AS_PATH and takes them as an AS_SET to prevent the route loop.

Configuring BGP route filtering

Configure BGP route filtering for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ip as-path access-list <i>access-list-number</i> { permint deny } <i>regexp</i>	Configure the filter of the AS_PATH list.
3	Raisecom(config)# router bgp [<i>as-id</i>]	Enter BGP configuration mode.
4	Raisecom(config-router)# neighbor <i>ip-address</i> filter-list <i>access-</i> <i>list-number</i> { in out }	Configure the BGP route filtering policy based on AS_PATH list.
5	Raisecom(config-router)# neighbor <i>ip-address</i> route-map <i>map-name</i> { in out }	Apply the routing policy to the specified neighbor to filter or release the route.
6	Raisecom(config-router)# distribute-list prefix <i>list-name</i> { in out }	Filter BGP routing information based on IP prefix-list.
7	Raisecom(config-router)# distribute-list prefix <i>list-name</i> out [connected static rip ospf isis]	Filter routes redistributed to the BGP routing table based on IP prefix-list.
8	Raisecom(config-router)# neighbor <i>ip-address</i> prefix-list <i>prefix-</i> <i>list-name</i> { in out }	Configure the specified neighbor to filter received or released routes based on IP prefix-list.

5.10.5 Configuring BGP GR

After being started, BGP Graceful Restart (GR) helps to prevent interrupting the forward process caused by protocol restart.

Configuring BGP GR for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp as-id</code>	Enter BGP configuration mode.
3	<code>Raisecom(config-router)# bgp graceful-restart all</code>	Enable BGP GR.
4	<code>Raisecom(config-router)#bgp graceful-restart restart- time seconds</code>	Configure the maximum time used for re- establishing the neighboring relationship during the GR process. By default, it is 120s.
5	<code>Raisecom(config-router)#bgp graceful-restart stalepath- time seconds</code>	Configure the maximum time for the Helper to keep the Stale route during the GR process. By default, it is 360s.

5.10.6 Configuring BFD for BGP

Configure BFD for BGP for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp as-id</code>	Enter BGP configuration mode.
3	<code>Raisecom(config-router)#neighbor ip-address fall-over bfd</code>	Enable BFD for BGP. By default, it is disabled.

5.10.7 Configuring BGP authentication

Configure BGP authentication for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#route r bgp as-id</code>	Enter BGP configuration mode.
3	<code>Raisecom(config- router)#neighbor ip- address password password</code>	Enable to perform MD5 authentication on the BGP message when the BGP neighbor establishes the TCP connection. By default, it is disabled.

5.10.8 Checking configurations

Use the following commands to check configurations.

No.	Command	Description
1	Raisecom# show ip bgp	Show contents of the local BGP routing table.
2	Raisecom# show ip bgp ip-address [ip-mask]	Show information about the specified network in the local BGP routing table.
3	Raisecom# show ip bgp dampening dampened-paths	Show dampened routing information.
4	Raisecom# show ip bgp dampening parameters	Show route dampening parameters.
5	Raisecom# show ip bgp dampening flap-statistics	Show route flapping statistics.
6	Raisecom# show ip bgp summary	Show summaries of the BGP neighbor.
7	Raisecom# show ip bgp neighbors [ip-address]	Show detailed BGP neighbor status.

5.10.9 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom# clear ip bgp dampening [network-address [network-mask]]	Clear all route dampening information.
Raisecom# clear ip bgp { all ip-address external internal } [ipv4 unicast]	Reset all or specified BGP connections of the public network.
Raisecom# clear ip bgp [ipv4 unicast] as-id	
Raisecom# clear ip bgp { all ip-address external internal } [ipv4 unicast] { in out soft }	Update all or specified BGP routes of the public network without breaking the BGP connecting.
Raisecom# clear ip bgp [ipv4 unicast] as-id { in out soft }	

5.11 RIP

5.11.1 Configuring basic functions of RIP

Configuring basic functions of RIP for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router rip	Enable RIP, and enter RIP configuration mode.

Step	Command	Description
3	Raisecom(config-rip)# network <i>ip-address</i>	Configure a directly-connected and effective network based on RIP.
4	Raisecom(config-rip)# offset-list <i>access-list-name</i> { in out } <i>offset-value</i> [<i>interface-type interface-number</i>]	Configure the additional metrics when the interface receives or sends RIP routes. By default, it is 0.
5	Raisecom(config-rip)# passive-interface { <i>interface-type interface-number</i> default }	(Optional) configure the interface to be a passive interface. By default, it is a non-passive interface.

5.11.2 Configuring RIP version

Configure the RIP version for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router rip	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)# version <i>version-id</i>	Configure global RIP version ID. By default, global RIP version is not configured. In this case, interfaces which are configured with RIP but not configured with the RIP version in the Tx direction will send V1 packets. Interfaces which are enabled with RIP but not configured with the RIP version in the Rx direction will receive packets of any version.
4	Raisecom(config-rip)# exit Raisecom(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode.
5	Raisecom(config-vlan1)# ip rip receive version { 1 2 }*	Configure the receiving RIP version. By default, the receiving RIP version is subjected to the global RIP version.
6	Raisecom(config-vlan1)# ip rip send version { 1 2 } *	Configure the sending RIP version. By default, the sending RIP version is subjected to the global RIP version.
7	Raisecom(config-vlan1)# ip rip v2-broadcast	Configure the interface which runs RIPv2 to send broadcast updates. By default, it sends multicast updates.



You can configure RIP version globally and on the interface of the ISCOM3000G series switch. If the interface is configured with RIP version, then this RIP version prevails.

5.11.3 Configuring redistribution of external routes

Configure redistribution of external routes for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router rip</code>	Enable RIP, and enter RIP configuration mode.
3	<code>Raisecom(config-rip)#host-route</code>	Enable the function of receiving host routes. By default, it is enabled.
4	<code>Raisecom(config-rip)#default-information originate</code>	Enable broadcasting the default route. By default, it is disabled.
5	<code>Raisecom(config-rip)#redistribute { static connected isis bgp ospf } [metric metric] [route-map map-name] [tag tag-value]</code>	Configure the policy for redistributing RIP routes.
6	<code>Raisecom(config-rip)#default-metric metric</code>	Configure the default metrics of redistributing external routes. By default, it is 1.
7	<code>Raisecom(config-rip)#auto-summary</code>	Enable automatic aggregation (support RIPv2 only). By default, it is enabled.
8	<code>Raisecom(config-rip)#validate-update-source</code>	Enabled the function of checking the source IP address of the received RIP packets. By default, it is enabled.

5.11.4 Configuring RIP timer

Configure the RIP timer for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router rip</code>	Enable RIP, and enter RIP configuration mode.

Step	Command	Description
3	<code>Raisecom(config-rip)#timers basic update-time invalid- time holddown-time flush- time</code>	Configure RIP timer. By default, the update interval is 30s. The invalid interval is 180s. The suppression interval is 120s. The refreshing interval is 120s.

5.11.5 Configuring loop suppression

Configure loop suppression for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter interface configuration mode.
3	<code>Raisecom(config-vlan1)#ip rip split-horizon</code>	Enable split horizon on the interface, that is, the route learned from one interface will not be broadcasted back to the interface again. By default, it is enabled.
4	<code>Raisecom(config-vlan1)#ip rip poisoned-reverse</code>	Enable poison reverse on the interface, that is, the route learned from one interface can be advertised to other interfaces through this interface. However, the metrics of those routes is configured to 16, namely, unreachable. By default, it is disabled.



Note

If poison reverse and split horizon are enabled concurrently, split horizon will be invalid.

5.11.6 Configuring authentication

Configure authentication for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.

Step	Command	Description
3	Raisecom(config-vlan1)# ip rip authentication mode { text md5 }	Configure the packet authentication mode on the interface. By default, the authentication mode of RIPv2 packets on the interface is no authentication.
4	Raisecom(config- vlan1)# ip rip authentication string <i>password-string</i>	Configure the interface-associated password.
5	Raisecom(config- vlan1)# ip rip authentication key-chain <i>key-chain-name</i>	Configure the interface-associated authentication secret string.

5.11.7 Configuring routing policy

Configure the routing policy for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router rip	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)# distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> route-map <i>rmap-name</i> } in [<i>interface-type interface-number</i>]	Configure RIP ingress routing policy.
4	Raisecom(config-rip)# distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> route-map <i>rmap-name</i> } out [<i>interface-type interface-number</i>]	Configure RIP egress routing policy.
5	Raisecom(config-rip)# distribute-list gateway <i>list-name</i> in [<i>interface-type interface-number</i>]	Execute routing policies on the source address of the received packets through RIP.

5.11.8 Configuring route calculation

Configure route calculation for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router rip	Enable RIP, and enter RIP configuration mode.

Step	Command	Description
3	Raisecom(config-rip)# distance <i>administrative-distance</i> [<i>ip-address wild-card-mask</i>]	Configure the administrative distance of RIP, namely, the protocol priority. The shorter the administrative distance is, the higher the priority will be. By default, the administrative distance is 120.
4	Raisecom(config-rip)# maximum load-balancing <i>number</i>	Configure the maximum number of IP equal-cost multi-path load balancing paths.

5.11.9 Checking configurations

Use the following commands to check configurations.

No.	Command	Description
1	Raisecom# show ip rip	Show basic information about RIP.
2	Raisecom# show ip rip database	Show information about RIP routing database.
3	Raisecom# show ip rip interface	Show configurations and status of the interface which runs RIP.

5.11.10 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom# clear rip database	Clear information about RIP routing database.
Raisecom# clear rip statistics	Clear RIP interface statistics.

6 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 supplying uninterrupted PoE during restart, but you should save configurations in advance; otherwise, configurations will be lost, PoE parameters will be restored to default values, and power supply capabilities will fail to meet actual requirements.

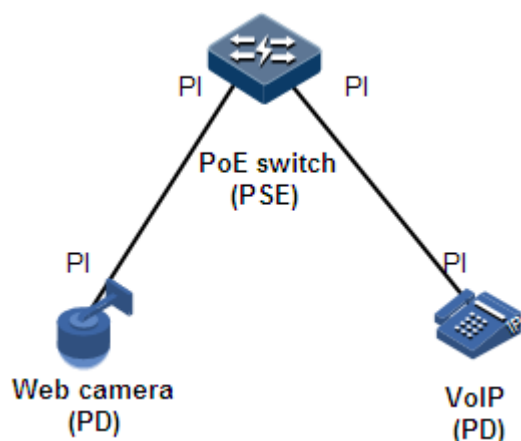
6.1 Introduction

6.1.1 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 6-1 shows principles of PoE.

Figure 6-1 Principles of PoE



6.1.2 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

6.1.3 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.

6.1.4 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

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 ISCOM3000G 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.

6.1.5 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 ISCOM3000G 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 ISCOM3000G series switch to intelligently supply power and to control when to shut down the PoE interface.

6.2 Configuring PoE

6.2.1 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.

Prerequisite

N/A

6.2.2 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%

6.2.3 Enabling interface PoE

Enable interface PoE for the ISCOM3000G series switch as below:

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#poe enable	Enable interface PoE.

6.2.4 Configuring maximum output power of PoE

Configure the maximum output power of PoE for the ISCOM3000G series switch as below:

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#poe max-power <i>max-power-value</i>	Configure the maximum output power of PoE.

6.2.5 Configuring priority of PoE

Configure priority of PoE for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#poe priority { critical high low }</code>	Configure priority of PoE.

6.2.6 Configuring PSE power utilization rate threshold

Configure the PSE power utilization rate threshold for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#poe pse power- threshold percent</code>	Configure the PSE power utilization rate threshold.

6.2.7 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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#poe legacy enable</code>	Enable the PSE to identify non-standard PDs.

6.2.8 Enabling forcible power supply on interface



Caution

When using the ISCOM3000G 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#poe force-power	Enable forcible PoE power supply on the interface.

6.2.9 Enabling overtemperature protection

Enable overtemperature protection for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#poe temperature- protection enable	Enable overtemperature protection.

6.2.10 Enabling global Trap

Enable global Trap for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#poe pse trap enable	Enable global Trap.

6.2.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show poe <i>interface-</i> <i>type interface-number</i> [detail]	Show power supply status on specified interfaces.
2	Raisecom#show poe pse [detail]	Show PSE configurations and realtime operating information.

6.3 Configuring Smart PoE

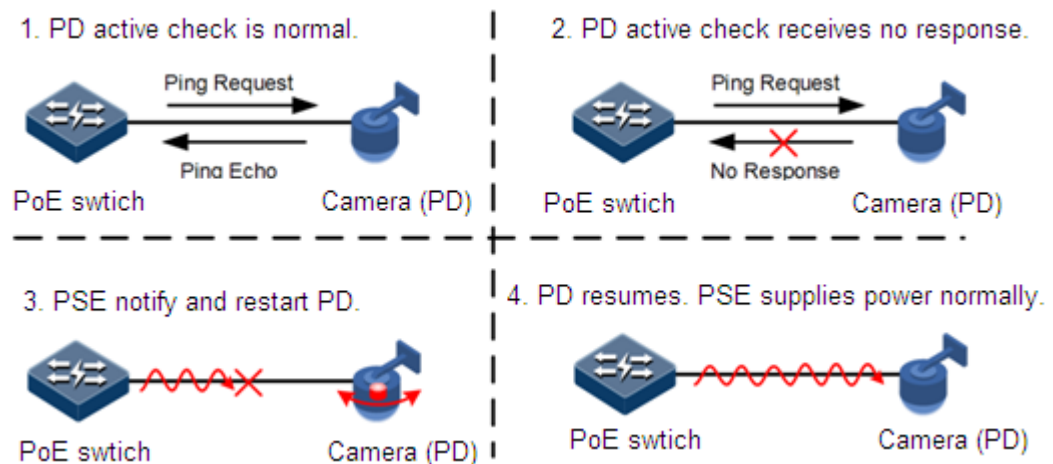
6.3.1 Preparing for configurations

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 6-2, 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 6-2 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 ISCOM3000G series switch to intelligently supply power and to control when to shut down the PoE interface.

Prerequisite

N/A

6.3.2 Default configurations of PoE

Default configurations of PoE are as below.

Function	Default value
PD Active check	Enable

Function	Default value
PD check action	N/A
Restart interval	N/A

6.3.3 Configuring PoE scheduling profile for interface

Configure the PoE scheduling profile for the interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#poe schedule profile profile Raisecom(config-profile1)#rule rule-id { reboot-time start-time end-time } week hour minute	Configure rules for the PoE scheduling profile.
3	Raisecom(config)#interface interface-type interface-number	Enter physical layer interface configuration mode.
4	Raisecom(config-gigaethernet1/1/1)#poe schedule profile profile	Configure the PoE scheduling profile for the interface.

6.3.4 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#linktrace track track-id	Configure the linktrace ID.
3	Raisecom(config-linktrace)#icmp ip-address { interface-type interface-number source ip source-ip-address }	Configure the destination IP address of linktrace, and specify the linktrace type.
4	Raisecom(config-linktrace)#icmp interval period	Configure the period for sending linktrace packets.
5	Raisecom(config-linktrace)#icmp retry count count	Configure the maximum number of retries for linktrace.

6.3.5 Configuring PD active check

Configure PD active check for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#poe alive check enable</code>	Enable PD active check.
4	<code>Raisecom(config- gigaethernet1/1/1)#poe alive action { reboot reboot-alarm alarm }</code>	Configuring the action for PD active check.
5	<code>Raisecom(config- gigaethernet1/1/1)#poe reboot interval period</code>	Configure the restart interval.
6	<code>Raisecom(config- gigaethernet1/1/1)#poe linktrace track track-id</code>	Bind a PoE interface with the specified linktrace ID.



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.

6.3.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show poe profile { all profile }</code>	Show rules of the PoE scheduling profile.
2	<code>Raisecom#show poe interface interface-type interface-number [detail]</code>	Show the power supply status of the specified PoE interface.
3	<code>Raisecom#show link-trace</code>	Show linktrace configurations.

6.4 Example for configuring PoE power supply

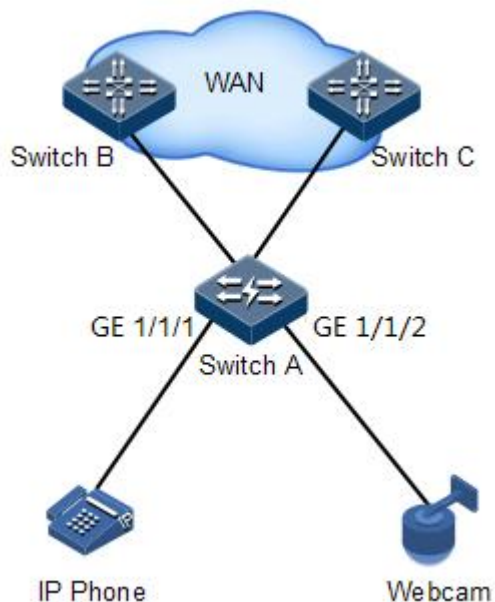
Networking requirements

As shown in Figure 6-3, 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 6-3 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.

```
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-gigaehternet1/1/2)#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 gigaethernet 1/1/1 detail** and **show poe gigaethernet 1/1/2 detail** commands to show PoE configurations on GE 1/1/2 and GE 1/1/1.

```
Raisecom#show poe 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 (V)
```

```
Raisecom#show poe 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 (V)

7 DHCP

This chapter describes basic principles and configuration procedures of DHCP, and providing related configuration examples, including the following sections:

- DHCP Client
- DHCP Snooping
- DHCP Options
- DHCP Server
- DHCP Relay

7.1 DHCP Client

7.1.1 Introduction

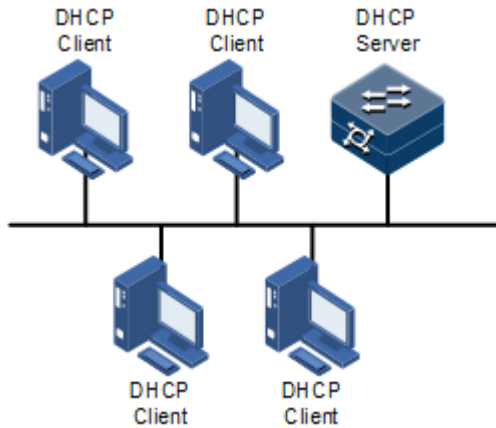
Dynamic Host Configuration Protocol (DHCP) refers to the protocol which assigns configurations, such as the IP address, to users on the TCP/IP network. Based on BOOTP (Bootstrap Protocol) protocol, it has additional features, such as automatically assigning available network addresses, reusing network 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 wide 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 configuration to the server (including IP address, subnet mask, and default gateway), and the server replies with IP address for the client and other related configurations to implement dynamic configurations of IP address.

Typical applications of DHCP usually include a set of DHCP server and multiple clients (for example PC or laptop), as shown in Figure 7-1.

Figure 7-1 DHCP typical networking



DHCP ensures rational allocation, avoids waste, and improves the utilization rate of IP addresses in the entire network.

Figure 7-2 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 7-2 Structure of a DHCP packet

0	7	15	23	31
OP	Hardware type		Hardware length	Hops
Transaction ID				
Seconds		Flags		
Client IP address				
Your(client) IP address				
Server IP address				
Relay agent IP address				
Client hardware address				
Server host name				
File				
Options				

Table 7-1 describes fields of a DHCP packet.

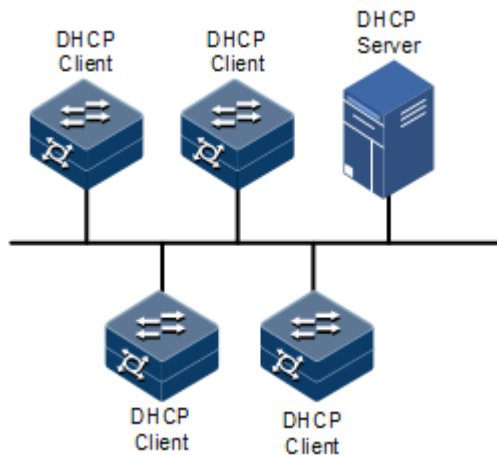
Table 7-1 Fields of a DHCP packet

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.

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. <ul style="list-style-type: none"> • 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 ISCOM3000G 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 7-3.

Figure 7-3 DHCP Client networking



7.1.2 Preparing for configurations

Scenario

As a DHCP client, the ISCOM3000G 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 withdraw 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 wish 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.
- Add the Layer 3 interface to the VLANs.
- Disable DHCP Snooping.

7.1.3 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

7.1.4 Configuring DHCP Client

Before a DHCP client applies for an IP address, you must create a VLAN, and add the interface with the IP address to the VLAN. Meanwhile you must configure the DHCP server; otherwise the interface will fail to obtain an IP address through DHCP.


For interface IP 0, the IP addresses obtained through DHCP and configured manually can overwrite each other.



Note

- By default, the ISCOM3000G series switch is enabled with DHCP Client. Use the **no ip address dhcp** command to disable DHCP Client.
- If the ISCOM3000G 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface vlan 1	Enter Layer 3 interface configuration mode.
3	Raisecom(config-vlan)# ip dhcp client { class-id class-id client-id client-id hostname hostname }	(Optional) configure DHCP client information, including the type identifier, client identifier, and host name.  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]	Configure the DHCP client to obtain IP address through DHCP.
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.
6	Raisecom(config-ip)# no ip address dhcp	(Optional) release the IP address.

7.1.5 Configuring DHCPv6 Client

Configure the DHCPv6 client for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)# interface vlan vlan-id	Enter VLAN interface configuration mode.
3	Raisecom(config- vlan1)#ipv6 address dhcp [server-ip ipv6- address]	Configure applying for IPv6 address through DHCPv6. If the ISCOM3000G 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.
4	Raisecom(config- vlan1)#ipv6 dhcp client renew	(Optional) renew the IPv6 address. If the Layer 3 interface on the ISCOM3000G series switch has obtained an IP address through DHCP, it will automatically renew the IPv6 address when the lease period expires.
5	Raisecom(config- vlan1)#ipv6 dhcp client rapid- commit	(Optional) enable DHCPv6 clients to apply for rapid interaction.

7.1.6 Checking configurations

Use the following commands to check configuration results.

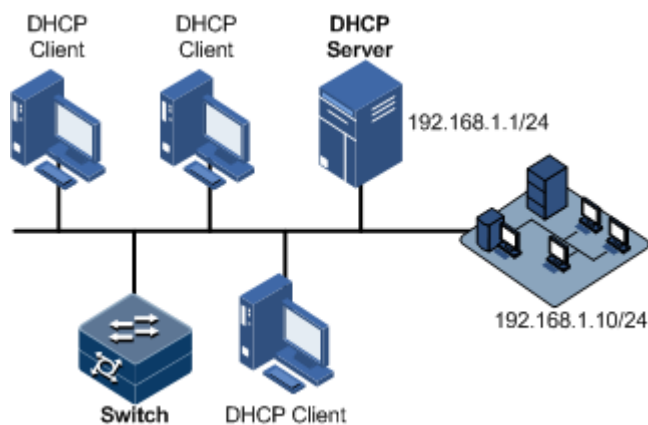
No.	Command	Description
1	Raisecom#show ip dhcp client	Show configurations of DHCP Client.
2	Raisecom#show ipv6 dhcp client	Show configurations of DHCPv6 Client.

7.1.7 Example for configuring DHCP Client

Networking requirements

As shown in Figure 7-4, 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 7-4 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.

```
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:           --
```

7.2 DHCP Snooping

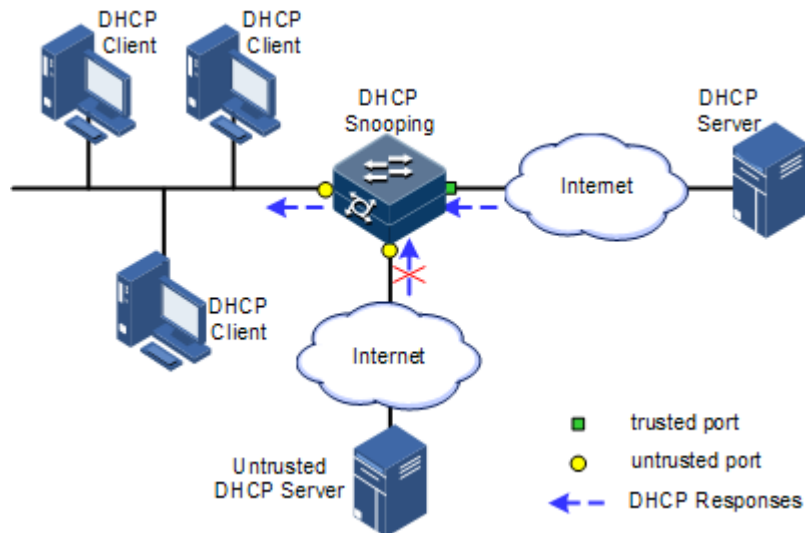
7.2.1 Introduction

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 7-5, to make DHCP client obtain the IP address from a legal DHCP server, the DHCP Snooping security system permits to configure an interface as the trusted interface or untrusted interface: the trusted interface forwards DHCP packets normally; the untrusted interface discards the reply packets from the DHCP server.

Figure 7-5 DHCP Snooping



- Record mapping between DHCP client IP address and MAC address.

DHCP Snooping records entries by monitoring 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. DHCP works based on the following 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 field to locate DHCP clients and control client security and accounting.

If the ISCOM3000G series switch is configured with DHCP Snooping to support DHCP Option:

- When the ISCOM3000G series switch receives a DHCP request packet, it processes the packet according to Option fields included or not, padding mode, and configured processing policy, then forwards the processed packet to the DHCP server.
- When the ISCOM3000G 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.

7.2.2 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

7.2.3 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

7.2.4 Configuring DHCP Snooping

Generally, you must ensure that the ISCOM3000G 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 ISCOM3000G series switch will do nothing to Option fields in packets. For packets without Option fields, the ISCOM3000G 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip dhcp snooping	Enable global DHCP Snooping.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	Raisecom(config- gigaethernet1/1/1)#ip dhcp snooping	(Optional) enable interface DHCP Snooping.
5	Raisecom(config- gigaethernet1/1/1)#ip dhcp snooping trust	Configure the trusted interface of DHCP Snooping.

Step	Command	Description
6	Raisecom(config)#ip dhcp snooping option client-id	(Optional) configure DHCP Snooping to support Option 82 field.
7	Raisecom(config)#ip dhcp snooping autosave enable	(Optional) enable auto-saving of the DHCP Snooping binding table.
8	Raisecom(config)#ip dhcp snooping autosave write-interval <i>time</i>	(Optional) configure the interval for automatically saving the DHCP Snooping binding table.

7.2.5 Configure DHCP Snooping to support Option 82

Configure DHCP Snooping to support Option 82 for the ISCOM3000G 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 <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	Raisecom(config-gigaethernet1/1/1)#ip dhcp snooping information option vlan-list <i>vlan-list</i>	(Optional) configure the lists of VLANs that support Option 82 through interface DHCP Snooping.

7.2.6 Configuring DHCPv6 Snooping

Configure DHCPv6 Snooping for the ISCOM3000G 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)#ipv6 dhcp snooping <i>interface-type interface-number</i>	(Optional) enable interface DHCPv6 Snooping.
4	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	Raisecom(config-gigaethernet1/1/1)#ipv6 dhcp snooping trust	Configure the trusted interface of DHCPv6 Snooping.

Step	Command	Description
6	<code>Raisecom(config-gigaetherne1/1/1)#exit</code> <code>Raisecom(config)#ipv6 dhcp snooping option <i>number</i></code>	(Optional) configure DHCPv6 Snooping to support customized Options.
7	<code>Raisecom(config)#ipv6 dhcp snooping option interface-id</code>	(Optional) configure DHCP Snooping to support Option 18.

7.2.7 Checking configurations

Use the following commands to check configuration results.

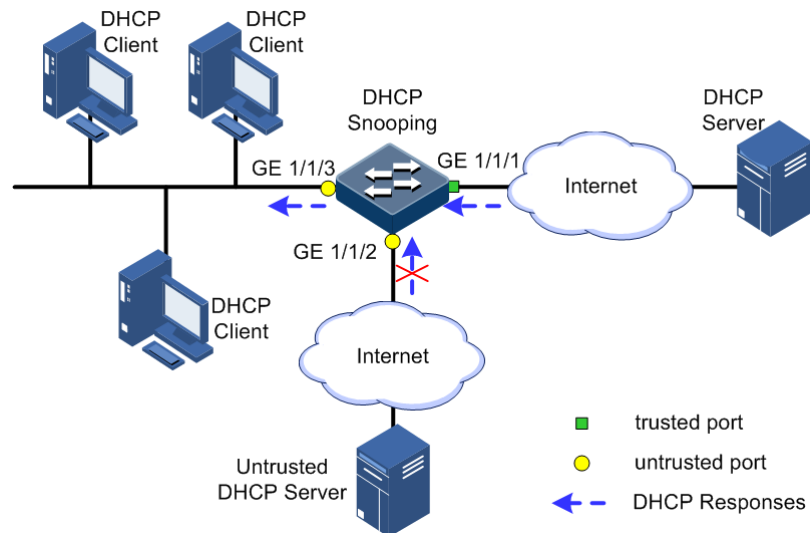
Step	Command	Description
1	<code>Raisecom#show ip dhcp snooping</code>	Show configurations of DHCP Snooping.
2	<code>Raisecom#show ip dhcp snooping binding</code>	Show configurations of the DHCP Snooping binding table.
3	<code>Raisecom#show ipv6 dhcp snooping</code>	Show configurations of DHCPv6 Snooping.
4	<code>Raisecom#show ipv6 dhcp snooping binding</code>	Show configurations of the DHCPv6 Snooping binding table.
5	<code>Raisecom#show ip dhcp snooping autosave</code>	Show auto-saving status of the DHCP Snooping binding table.

7.2.8 Example for configuring DHCP Snooping

Networking requirements

As shown in Figure 7-6, 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.

Figure 7-6 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.

```

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
.....

```

7.3 DHCP Options

7.3.1 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 7-2 lists frequently used DHCP options.

Table 7-2 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

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, customized, 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, 37, 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 ISCOM3000G 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 ISCOM3000G series switch, or user-defined string in request packets of the DHCP client.

7.3.2 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 and 37 are used to record information about IPv6 DHCP clients. Options 61 and 82 are used to record information about IPv4 DHCP clients. By cooperating with other

software, the DHCP server can implement functions, such as limit on IP address distribution and accounting, based on these Option fields.

Prerequisite

N/A

7.3.3 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

7.3.4 Configuring DHCP Option fields

Configure DHCP Option fields for the ISCOM3000G 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 <i>attach-string</i>	(Optional) configure additional information for Option 82 field.
	Raisecom(config)#interface <i>interface-type interface-number</i> Raisecom(config-gigaethernet1/1/1)#ip dhcp information option circuit-id <i>circuit-id</i> [prefix-mode]	(Optional) configure circuit ID sub-option information for Option 82 field on the interface.
	Raisecom(config-gigaethernet1/1/1)#ip dhcp option vlan <i>vlan-id description string</i> Raisecom(config-gigaethernet1/1/1)#exit	(Optional) configure the interface or VLAN description to be padded into Option 82 fields.
	Raisecom(config)#ip dhcp information option { attach-string circuit-id format circuit-id hex } <i>string</i>	(Optional) configure the attached string in Option 82 of DHCP packets.
	Raisecom(config)#ip dhcp information option circuit-id mac-format <i>string</i>	(Optional) configure the format of the MAC address in the variable of Circuit ID in Option 82 of DHCP packets.

Step	Command	Description
	<code>Raisecom(config)#ip dhcp information option remote-id { client-mac client-mac-string hostname string string switch-mac switch-mac-string }</code>	(Optional) configure remote ID sub-option information for Option 82 field.
3	<code>Raisecom(config)#ipv4 dhcp option option-id { ascii ascii-string hex hex-string ip-address ip-address }</code>	(Optional) create user-defined Option based on IPv4.
	<code>Raisecom(config)#interface gigaethernet1/1/1 Raisecom(config-gigaethernet1/1/1)#ipv4 dhcp option option-id { ascii ascii-string hex hex-string ip-address ip-address }</code>	(Optional) create user-defined Option field information on the interface.
4	<code>Raisecom(config-gigaethernet1/1/1)#exit Raisecom(config)#ipv4 dhcp option client-id { ascii ascii-string hex hex-string ip-address ip-address }</code>	(Optional) configure Option 61 field information.
	<code>Raisecom(config-gigaethernet1/1/1)#ipv4 dhcp option client-id { ascii ascii-string hex hex-string ip-address ip-address }</code>	(Optional) configure Option61 field information on the interface.

7.3.5 Configuring DHCP Option 18 over IPv6

Configure DHCP Option 18 over IPv6 for the ISCOM3000G 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ipv6 dhcp option interface-id { ascii ascii-string hex hex-string ipv6-address ipv6-address }</code>	(Optional) configure information about Option 18.
3	<code>Raisecom(config)#interface interface-type interface-number Raisecom(config-gigaethernet1/1/1)#ipv6 dhcp option interface-id { ascii ascii-string hex hex-string ipv6-address ipv6-address }</code>	(Optional) configure information about Option 18 on the interface.

7.3.6 Configuring DHCP Option 37 over IPv6

Configure DHCP Option 37 over IPv6 for the ISCOM3000G 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.
2	Raisecom(config)#ipv6 dhcp option remote-id { ascii hex } string	(Optional) configure information about Option 37.
3	Raisecom(config)#interface interface-type interface-number Raisecom(config-gigaethernet1/1/1)#ipv6 dhcp option remote-id mac-format string	(Optional) configure the format of the MAC address of the Circuit ID variable in Option 37 in DHCPv6 packets.

7.3.7 Configuring user-defined DHCP Option over IPv6

Configure user-defined DHCP Option over IPv6 for the ISCOM3000G 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.
2	Raisecom(config)#ipv6 dhcp option number { ascii ascii-string hex hex-string ipv6-address ipv6-address }	(Optional) create user-defined Option information over IPv6.
3	Raisecom(config)#interface interface-type interface-number Raisecom(config-gigaethernet1/1/1)#ipv6 dhcp option number { ascii ascii-string hex hex-string ipv6-address ipv6-address }	(Optional) create user-defined Option information over IPv6 on the interface.

7.3.8 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.

7.4 DHCP Server

7.4.1 Introduction

Dynamic Host Configuration Protocol (DHCP) refers to assigning IP address configurations dynamically for users in TCP/IP network. It is based on BOOTP (Bootstrap Protocol) protocol, and automatically adds the specified available network address, network address reuse, 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:

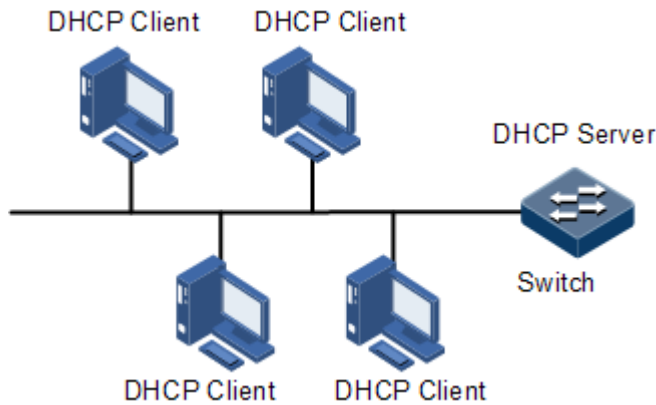
- The network scale is large. It requires much workload for manual configurations, and is difficult to manage the entire network intensively.
- The number of hosts on the network is greater than that of IP addresses, which makes it unable to assign a fixed IP address for each host and restricts the number of users connected to network simultaneously.
- Only the minority of hosts on the network requires fixed IP addresses, and most of hosts do not.

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.

The DHCP technology ensures rational allocation, avoids waste of IP addresses, and improves the utilization rate of IP addresses on the entire network.

The ISCOM3000G series switch, as the DHCP server, assigns dynamic IP addresses to clients, as shown in Figure 7-7.

Figure 7-7 DHCP Server and Client networking



DHCP packets

Figure 7-8 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 7-8 Structure of a DHCP packet

0	7	15	23	31
OP	Hardware type		Hardware length	Hops
Transaction ID				
Seconds		Flags		
Client IP address				
Your(client) IP address				
Server IP address				
Relay agent IP address				
Client hardware address				
Server host name				
File				
Options				

Table 7-3 describes fields of a DHCP packet.

Table 7-3 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.

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. <ul style="list-style-type: none"> • 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, and IP address of the WINS

7.4.2 Preparing for configurations

Scenario

When working as the DHCPv4 server, the ISCOM3000G series switch can assign IP addresses to DHCPv4 clients.

Prerequisite

- Disable DHCPv4 Client on the ISCOM3000G series switch.
- The DHCP server is a common one.

7.4.3 Creating and configuring IPv4 address pool

Configure the IPv4 address pool for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip dhcp server pool pool-name	Create an IPv4 address pool, and enter address pool configuration mode.
3	Raisecom(config-pool)#address start-ip-address end-ip-address mask { mask mask-length }	Configure the range of IP addresses in the IPv4 address pool.
4	Raisecom(config-pool)#excluded-ip-address start-ip-address [end-ip-address]	Configure the range of excluded IP addresses in the IPv4 address pool.
5	Raisecom(config-pool)#lease expired { minute infinite }	Configure the lease period for the IPv4 address pool.
6	Raisecom(config-pool)#dns-server ip-address [secondary]	Configure the DNS server address of the IPv4 address pool.
7	Raisecom(config-pool)#gateway ip-address	Configure the default gateway of the IPv4 address pool.
8	Raisecom(config-pool)#option 60 vendor-string	Configure information carried by Option 60.
9	Raisecom(config-pool)#option 43 [sub-option option-code] { ascii ascii-string hex hex-string }	Configure information carried by Option 43.
10	Raisecom(config-pool)#tftp-server ip-address	Configure the TFTP server of the IPv4 address pool.
11	Raisecom(config-pool)#trap server-ip ip-address	Configure the Trap server of the IPv4 address pool.

7.4.4 Enabling DHCPv4 Server on VLAN interface

Enable DHCPv6 Server on the VLAN interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan vlan-id	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#ip dhcp server	Enable DHCPv4 Server on the VLAN interface.

7.4.5 Enabling DHCP Server on VLAN interface

Only 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 DHCP Server on the VLAN interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan vlan-id	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#ip dhcp server	Enable DHCP Server on the VLAN interface.

7.4.6 Configuring DHCP Server to support Option 82

Configure DHCP Server to support Option 82 for the ISCOM3000G 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.

7.4.7 Checking configurations

Use the following commands to check configuration results.

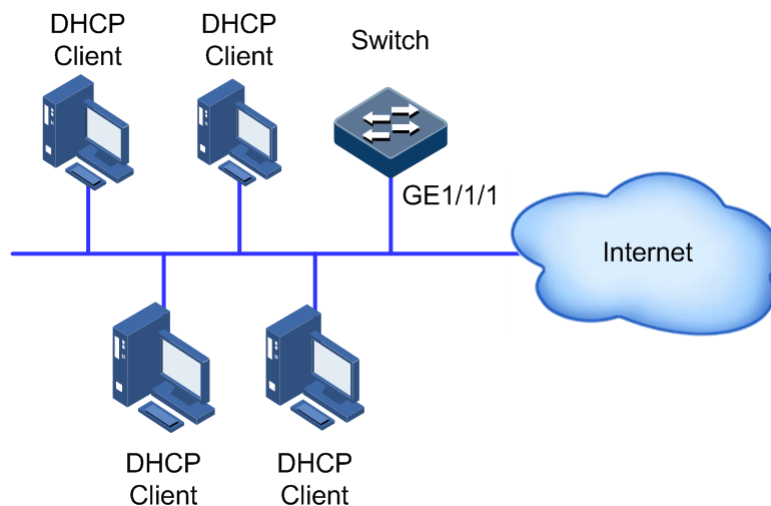
No.	Command	Description
1	Raisecom(config)#show ip dhcp server	Show configurations of DHCP Server.
2	Raisecom(config)#show ip dhcp server lease	Show assigned IPv4 addresses and clients information.
3	Raisecom(config)#show ip dhcp server statistics	Show packet statistics on the DHCPv4 Server.
4	Raisecom(config)#show ip dhcp static-bind	Show information about DHCPv4 static binding.
5	Raisecom(config)#show ip server pool	Show configurations of the address pool of DHCPv4 Server.

7.4.8 Example for configuring DHCPv4 Server

Networking requirements

As shown in Figure 7-9, 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 7-9 DHCP Server networking



Configuration steps

Step 1 Create an IP address pool, and configure it.

```
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 Configur 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 the 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      :      pool1
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      :      DHCP Relay
```

7.5 DHCP Relay

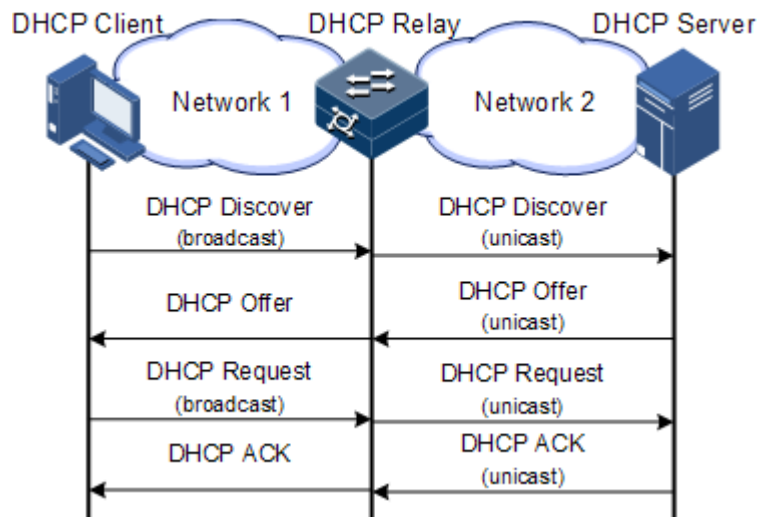
7.5.1 Introduction

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 7-10 shows typical application of DHCP Relay.

Figure 7-10 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.

7.5.2 Preparing for configurations

Scenario

When DHCP Client and DHCP Server are not in the same segment, you can use DHCP Relay to make DHCP Client and DHCP Server in different segments carry relay services, and relay DHCP packets across segments to the destination DHCP server, so that DHCP Client in different segments can share the same DHCP server.

Prerequisite

N/A

7.5.3 Default configurations of DHCP Relay

Default configurations of DHCP Relay are as below.

Function	Default value
Global DHCP Relay	Disable
Interface DHCP Relay	Disable

7.5.4 Configuring global DHCP Relay

Configure global DHCP Relay for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>raisecom#config</code>	Enter global configuration mode.

Step	Command	Description
2	<code>Raisecom(config)#ip dhcp relay</code>	Enable global DHCP Relay.

7.5.5 Configuring DHCP Relay on VLAN interface

Configure DHCP Relay on the VLAN interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface vlan <i>vlan-id</i></code>	Enter VLAN interface configuration mode.
3	<code>Raisecom(config-vlan1)#ip dhcp relay target-ip <i>ip-address</i></code>	Configure the destination IP address for forwarding packets.

7.5.6 Configuring DHCP Relay on physical interface or sub-interface

Configure DHCP Relay on physical interface or sub-interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface gigaethernet <i>1/1/port.sub</i></code>	Enter physical interface configuration mode or sub-interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/port.sub)#ip dhcp relay target-ip <i>ip-address</i></code>	Configure the destination IP address for forwarding packets.
4	<code>Raisecom(config-gigaethernet1/1/port)#ip dhcp relay relay -ip <i>ip-address</i></code>	Configure the relay IP address.

7.5.7 (Optional) configuring DHCP Relay to support Option 82

Configure DHCP Relay to support Option 82 for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip dhcp relay information option</code>	Configure DHCP Relay to support Option 82.

Step	Command	Description
3	Raisecom(config)#ip dhcp relay information policy { drop keep replace }	Configure the policy for DHCP Relay to process Option 82 request packets
4	Raisecom(config)#interface interface-type interface-number	Enter physical layer interface configuration mode.
5	Raisecom(config-gigaethernet1/1/port)#ip dhcp relay information trusted	Configure the trusted interface of DHCP Relay.
6	Raisecom(config-gigaethernet1/1/1port)#ip dhcp relay information option vlan-list vlan-list	Configure the VLAN list of DHCP Relay to support Option 82.

7.5.8 Checking configurations

Use the following commands to check configuration results.

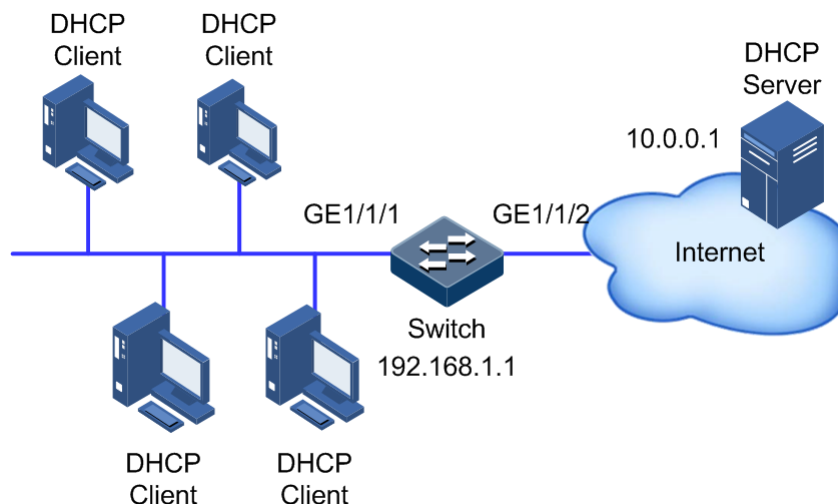
No.	Command	Description
1	Raisecom#show ip dhcp relay	Show configurations of DHCP Relay.
2	Raisecom#show ip dhcp relay information	Show information about Option 82 supported by DHCP Relay.

7.5.9 Example for configuring DHCPv4 Relay

Networking requirements

As shown in Figure 7-11, 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.

Figure 7-11 DHCP Relay networking



Configuration steps

Step 1 Enable global DHCP Relay and interface DHCP Relay.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#ip dhcp relay
Raisecom(config-gigaethernet1/1/1)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#ip dhcp relay
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 2 Configure the destination IP address of DHCP Relay.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#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
```

Interface	Status	Target Address
gigaethernet1/1/1	Enable	10.0.0.1

8 QoS

This chapter describes principles and configuration procedures of 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 rate limiting
- Configuring bandwidth rate limiting
- Configuring examples

8.1 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
- Congestion avoidance

8.1.1 Service model

QoS technical service models:

- Best-effort Service
- 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 E-mail. It is implemented by First In First Out (FIFO) queue.

DiffServ

DiffServ model is a multi-service model, which can satisfy different QoS requirements.

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.

8.1.2 Priority trust

Priority trust means that the ISCOM3000G series switch uses priority of packets for classification and performs QoS management.

The ISCOM3000G series switch supports packet priority trust based on interface, including:

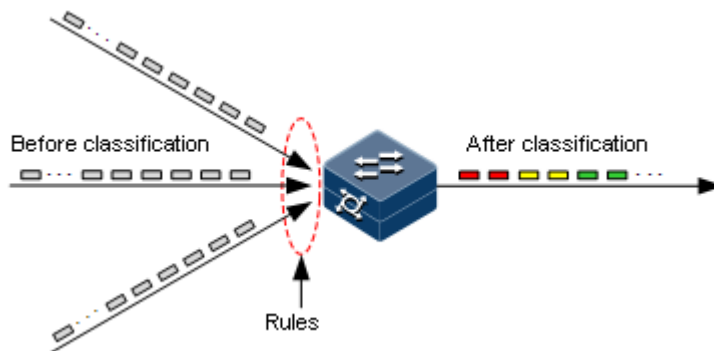
- Differentiated Services Code Point (DSCP) priority
- Class of Service (CoS) priority
- ToS priority

8.1.3 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 ISCOM3000G series switch supports traffic classification based on ToS priority, DSCP priority, CoS priority over IP packets, and based on Access Control List (ACL) rules and VLAN ID. The traffic classification procedure is shown in Figure 8-1.

Figure 8-1 Traffic classification



IP precedence and DSCP priority

Figure 8-2 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 priority with value ranging from 0 to 63, the last 2 bits (bit-6 and bit-7) are reserved. Figure 8-3 shows the structure of ToS and DSCP priorities.

Figure 8-2 Structure of IP packet header

4	8	16	32
Version	IHL	ToS	Total Length
Identification		Flags	Fragment Offset
Time-to-Live	Protocol	Header Checksum	
Source Address			
Destination Address			

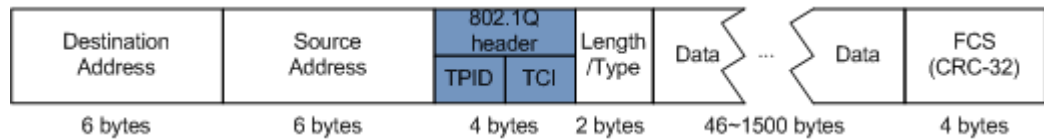
Figure 8-3 Structures of ToS priority and DSCP priority

Bits:	0	1	2	3	4	5	6	7
RFC1122:	Precedence			Type of Service			0	
RFC2474:	DSCP						Unused	

CoS priority

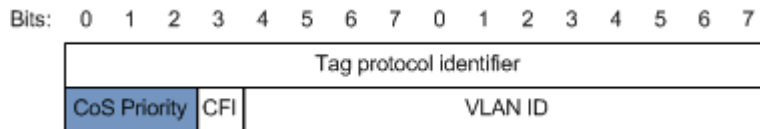
IEEE802.1Q-based VLAN packets are modifications of Ethernet packets. A 4-byte 802.1Q header is added between the source MAC address and protocol type, as shown in Figure 8-4. The 802.1Q header consists of a 2-byte Tag Protocol Identifier (TPID, valuing 0x8100) filed and a 2-byte Tag Control Information (TCI) field.

Figure 8-4 Structure of a VLAN packet



The first 3 bits of the TCI field represent the CoS priority, which ranges from 0 to 7, as shown in Figure 8-5. CoS priority is used to guarantee QoS on the Layer 2 network.

Figure 8-5 Structure of CoS priority



8.1.4 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 ISCOM3000G series switch supports rate limiting based on traffic policy in the ingress direction on the interface.

The ISCOM3000G 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 ISCOM3000G 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 services according to remarking information.

The ISCOM3000G series switch supports remarking packets by the following priority fields:

- IP precedence
- DSCP priority
- CoS priority

Traffic statistics

Traffic statistics is used to gather statistics about data packets of a specified service flow; namely, the number of packets and bytes matching traffic classification that pass the network or are discarded.

Traffic statistics is not a QoS control measure, but can be used in combination with other QoS actions to improve network supervision.

8.1.5 Priority mapping

Priority mapping refers to sending packets to different queues with different local priorities according to pre-configured mapping between external priority and local priority. Therefore, packets in different queues can be scheduled on the egress interface.

The ISCOM3000G series switch supports performing priority mapping based on the DSCP priority of IP packets or the CoS priority of VLAN packets. The Traffic-Class field of IPv6 packets corresponds to the DSCP priority of IPv4 packets. The mapping from DSCP priority to local priority is applicable to IPv6 packets. Take the first 6 bits of the Traffic-Class field for use.

By default, the mapping between the local priority and DSCP, CoS priorities of the ISCOM3000G series switch is listed in Table 8-1 and Table 8-2.

Table 8-1 Mapping between local priority and DSCP priority

Local	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 ISCOM3000G series switch and is the priority corresponding to queue in QoS queue scheduling.

Local priority ranges from 0 to 7. Each interface of the ISCOM3000G 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 8-2.

Table 8-2 Mapping between local priority and queue

Local	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

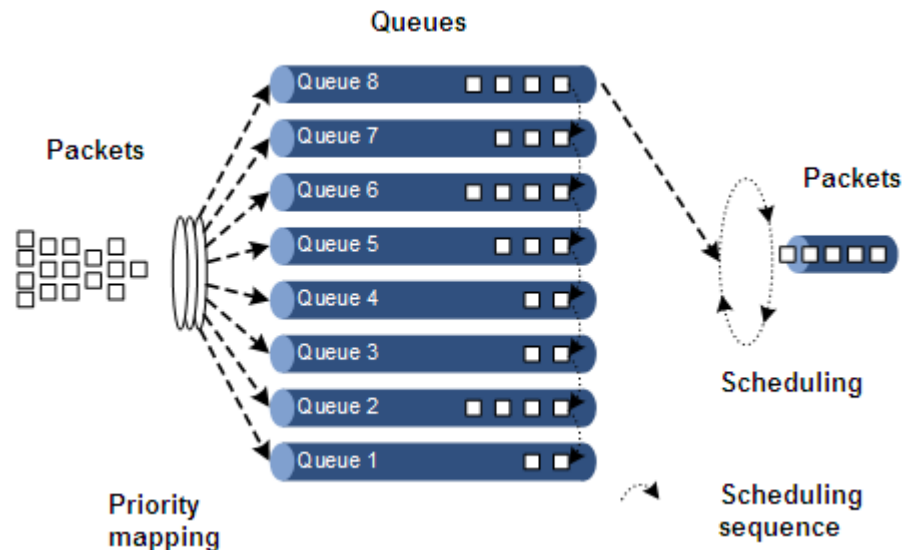
8.1.6 Queue scheduling

The ISCOM3000G series switch needs to perform queue scheduling when delay-sensitive services need better QoS services than delay-insensitive 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 ISCOM3000G 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.

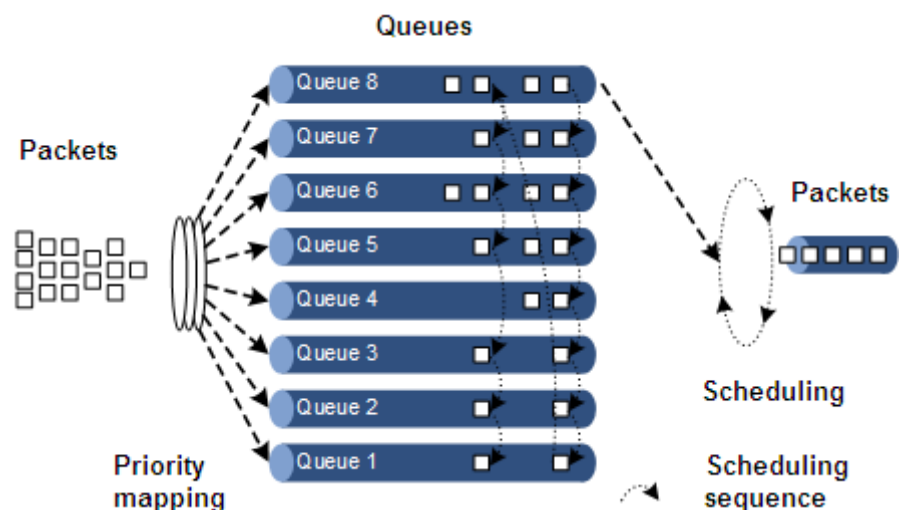
- SP: the ISCOM3000G series switch strictly schedules packets in a descending order of priority. Packets with lower priority cannot be scheduled until packets with higher priority are scheduled, as shown in Figure 8-6.

Figure 8-6 SP scheduling



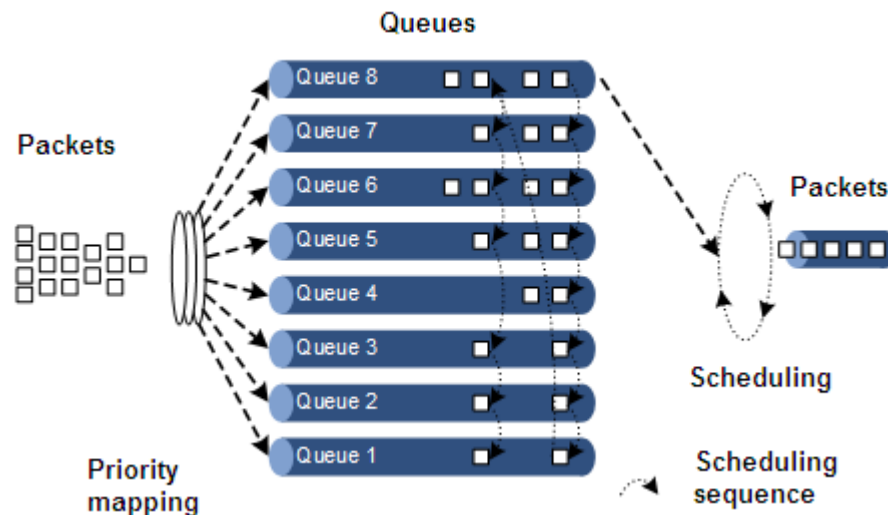
- WRR: on the basis of scheduling packets in a polling manner according to the priority, the ISCOM3000G series switch schedules packets according to the weight (based on byte) of the queue, as shown in Figure 8-7.

Figure 8-7 WRR scheduling



- DRR: similar with WRR, on the basis of scheduling packets in a polling manner according to the scheduling sequence, the ISCOM3000G series switch schedules packets according to the weight of the queue (based on packet), as shown in Figure 8-8.

Figure 8-8 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.

8.1.7 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 relieve 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 removed.

This Tail-Drop policy may cause TCP global synchronization, making network traffic change intermittently between high 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.

8.1.8 Rate limiting based on interface and VLAN

The ISCOM3000G series switch supports rate limiting based on traffic policy, interface, or VLAN, and interface+VLAN. Similar to rate limiting based on traffic policy, the ISCOM3000G series switch discards the excess traffic.

8.1.9 Bandwidth rate limiting

Bandwidth rate limiting is a subfunction of QoS and is more flexible than basic QoS. It is widely used on switches.

Bandwidth rate limiting 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.
 - Awaiting: 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. 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 ISCOM3000G 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 guaranteed bandwidth for each flow independently and even configure guaranteed bandwidth for sum of multiple flows through hierarchical bandwidth guarantee.

Color-aware and marking

If enabled with color-aware, the ISCOM3000G 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 ISCOM3000G 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.

8.2 Configuring priority

8.2.1 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 traffic classification and traffic policy. After being configured to priority trust mode, the ISCOM3000G series switch processes packets according to their priorities and provides services accordingly.

Specifying 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 ISCOM3000G series switch will conduct queue scheduling according to local priority of packets. Generally, IP packets need to be configured with mapping between IP precedence/DSCP priority and local priority; while VLAN packets need to be configured with mapping between CoS priority and local priority.

Prerequisite

N/A

8.2.2 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 priority
Mapping from CoS to local priority	See Table 8-3.
Mapping from DSCP to local priority	See Table 8-4.
Mapping from ToS to local priority and color	See Table 8-5.
Interface priority	0

Table 8-3 Default mapping from CoS to local priority

CoS	0	1	2	3	4	5	6	7
Local	0 (green)	1 (green)	2 (green)	3 (green)	4 (green)	5 (green)	6 (green)	7 (green)

Table 8-4 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	0 (green)	1 (green)	2 (green)	3 (green)	4 (green)	5 (green)	6 (green)	7 (green)

Table 8-5 Default mapping from ToS to local priority and color

ToS	0	1	2	3	4	5	6	7
Local	0 (green)	1 (green)	2 (green)	3 (green)	4 (green)	5 (green)	6 (green)	7 (green)

8.2.3 Configuring types of priorities trusted by interface

Configure types of priorities trusted by interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#mls qos trust { cos dscp port-priority }	Configure types of priorities trusted by interface.
4	Raisecom(config- gigaethernet1/1/1)#mls qos priority portpri-value	Configure the interface priority.

8.2.4 Configuring mapping from CoS to local priority

Configure mapping from CoS to local priority and color for the ISCOM3000G 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	Create a profile of mapping from CoS to local priority and color, and enter cos-to-pri configuration mode.
3	Raisecom(cos-to-pri)#cos cos-value to local-priority localpri-value [color { green red yellow }]	(Optional) modify the profile of mapping from CoS to local priority and color.

Step	Command	Description
4	<code>Raisecom(cos-to-pri)#exit</code> <code>Raisecom(config)#interface</code> <code>interface-type interface-number</code>	Enter physical layer interface configuration mode.
5	<code>Raisecom(config-gigaethernet1/1/1)#mls qos cos-to-local-priority profile-id</code>	Apply the profile of mapping from CoS to local priority and color on the interface.

8.2.5 Configuring mapping from DSCP to local priority and color

Configure mapping from DSCP to local priority and color for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mls qos mapping dscp-to-local-priority profile-id</code>	Create a profile of mapping from DSCP to local priority and color, and enter dscp-to-pri configuration mode.
3	<code>Raisecom(dscp-to-pri)#dscp dscp-value to local-priority localpri-value [color { green red yellow }]</code>	(Optional) modify the profile of mapping from DSCP to local priority and color.
4	<code>Raisecom(dscp-to-pri)#exit</code> <code>Raisecom(config)#interface</code> <code>interface-type interface-number</code>	Enter physical layer interface configuration mode.
5	<code>Raisecom(config-gigaethernet1/1/1)#mls qos dscp-to-local-priority profile-id</code>	Apply the profile of mapping from DSCP to local priority and color on the interface.

8.2.6 Configuring DSCP mutation

Configure DSCP mutation for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mls qos mapping dscp-mutation profile-id</code>	Create a DSCP mutation mapping profile, and enter dscp mutation configuration mode.
3	<code>Raisecom(dscp-mutation)#dscp dscp-value to new-dscp newdscp-value</code>	(Optional) modify the DSCP mutation profile.
4	<code>Raisecom(dscp-mutation)#exit</code> <code>Raisecom(config)#interface</code> <code>interface-type interface-number</code>	Enter physical layer interface configuration mode.

Step	Command	Description
5	Raisecom(config-gigaethernet1/1/1)# m ls q os d scp- m utation <i>profile-id</i>	Apply the DSCP mutation profile on the interface.

8.2.7 Configuring CoS remarking

Configure CoS remarking for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# m ls q os m apping cos-remark <i>profile-id</i>	Create a CoS remarking profile, and enter cos-remark configuration mode.
3	Raisecom(cos-remark)# local-priority <i>localpri-value</i> to cos <i>newcos-value</i>	Modify the CoS remarking profile.
4	Raisecom(dscp-remark)# exit Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
5	Raisecom(config-gigaethernet1/1/1)# m ls q os cos-remark <i>profile-id</i>	Apply the DSCP remarking profile on the interface.

8.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show mls qos [<i>interface-type interface-number</i>]	Show QoS priority, trust mode, and scheduling mode on the interface.
2	Raisecom# show mls qos mapping cos-to-local-priority [default <i>profile-id</i>]	Show information about mapping from CoS to local priority and color profile.
3	Raisecom# show mls qos mapping dscp-to-local-priority [default <i>profile-id</i>]	Show information about mapping from DSCP to local priority and color profile.
4	Raisecom# show mls qos mapping dscp-mutation [default <i>profile-id</i>]	Show mapping information about the DHCP mutation profile
5	Raisecom# show mls qos mapping cos-remark [default <i>profile-id</i>]	Show information about the CoS remarking profile.

8.3 Configuring congestion management

8.3.1 Preparing for configurations

Scenario

When the network is congested, you can configure queue scheduling if you wish 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.

8.3.2 Default configurations of congestion management

Default configurations of congestion management are as below.

Function	Default value
Queue scheduling mode	SP
Queue weight	<ul style="list-style-type: none"> • WRR weight for scheduling 8 queues is 1. • DRR weight for scheduling 8 queues is 81.

8.3.3 Configuring SP queue scheduling

Configure SP queue scheduling for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#m1s qos queue scheduler sp</code>	Configure queue scheduling mode as SP on the interface.

8.3.4 Configuring WRR or SP+WRR queue scheduling

Configure WRR or SP+WRR for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#m1s qos queue scheduler wrr <i>weigh1</i> <i>weight2 weight3...weight8</i>	Configure queue scheduling mode as WRR on the interface and the weight for each queue.

8.3.5 Configuring DRR or SP+DRR queue scheduling

Configure DRR or SP+DRR for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interf ace <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#m1s qos queue scheduler drr <i>weigh1 weight2</i> <i>weight3...weight8</i>	Configure queue scheduling mode as DRR, and configure weight for various queues. Conduct SP scheduling when priority of a queue is 0.

8.3.6 Configuring queue bandwidth guarantee

Configure queue bandwidth guarantee for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#m1s qos queue queue-id shaping cir <i>cir pir pir</i>	(Optional) configure queue bandwidth guarantee on the interface and configure burst size.

8.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show m1s qos queue interface <i>interface-type interface-number</i>	Show the weight of queues on the interface.

No.	Command	Description
2	Raisecom# show mls qos queue statistics interface <i>interface-type interface-number</i>	Show statistics about queues on the interface.
3	Raisecom# show mls qos queue shaping interface <i>interface-type interface-list</i>	Show queue shaping on the interface.

8.4 Configuring congestion avoidance

8.4.1 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 ISCOM3000G series switch conducts congestion avoidance based on WRED.

Prerequisite

Enable global QoS.

8.4.2 Default configurations of congestion avoidance

Default configurations of congestion avoidance are as below.

Function	Default value
Global WRED status	Enable

8.4.3 Configuring WRED

Configure WRED for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# mls qos wred profile <i>profile-id</i>	Create a SRED profile, and enter WRED configuration mode.
3	Raisecom(wred)# wred [color { green red yellow }] start-drop-threshold <i>start-drop</i> end-drop-threshold <i>end-drop</i> max-drop-probability <i>max-drop</i>	Modify the WRED profile.

Step	Command	Description
4	<code>Raisecom(wred)#exit</code> <code>Raisecom(config)#interface</code> <code>interface-type interface-number</code>	Enter physical layer interface configuration mode.
5	<code>Raisecom(config-</code> <code>gigaethernet1/1/1)#mls qos queue</code> <code>queue-id wred profile-id</code>	Apply the WRED profile to the interface.

8.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom# show mls qos wred</code> <code>profile [profile-list]</code>	Show information about the WRED profile.
2	<code>Raisecom#show mls qos queue</code> <code>wred interface interface-type</code> <code>interface-number</code>	Show WRED information about the interface.

8.5 Configuring traffic classification and traffic policy

8.5.1 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 ISCOM3000G series switch can perform corresponding operations on packets in different categories and provide corresponding services.

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 ISCOM3000G 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.

8.5.2 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

Function	Default value
Traffic policy statistics status	Disable

8.5.3 Creating traffic classification

Create traffic classification for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#class-map class-map-name [match-all match-any]</code>	Create traffic classification and enter traffic classification cmap configuration mode.
3	<code>Raisecom(config- cmap)#description string</code>	(Optional) configure the description of traffic classification.

8.5.4 Configuring traffic classification rules

Configure traffic classification rules for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#class-map class-map-name [match-all match-any]</code>	Create traffic classification and enter traffic classification cmap configuration mode.
3	<code>Raisecom(config-cmap)#match access-list { access-list name} Raisecom(config-cmap)#exit</code>	(Optional) configure traffic classification over ACL rule. The ACL rule must be defined firstly and the type must be permit .
4	<code>Raisecom(config)#policy-map policy-map-name Raisecom(config-pmap)#class- map class-map-name</code>	(Optional) configure traffic classification based on traffic classification rule. The traffic classification must have been created, and the matching type of its rule must be consistent with the
5	<code>Raisecom(config-cmap)#match cos cos-value</code>	(Optional) configure traffic classification based on CoS priority of packets.
6	<code>Raisecom(config-cmap)#match inner-vlan inner-vlan-value</code>	(Optional) configure traffic classification based on inner VLAN of packets.
7	<code>Raisecom(config-cmap)#match vlan vlan-value</code>	(Optional) configure traffic classification based on VLANs of packets.
8	<code>Raisecom(config-cmap)#match dscp dscp-value</code>	(Optional) configure traffic classification based on DSCP priority rule.




- Traffic classification rules must be created for traffic classification; namely, the **match** parameter must be configured.
- For traffic classification quoted by traffic policy, do not modify traffic classification rule; namely, do not modify the **match** parameter of traffic classification.

8.5.5 Creating rate limit rule and shapping rule

When you need to limit rate of packets based on traffic policy, create a token bucket, configure rate limit and shaping rules on the token bucket, quote these rules to traffic classification bound to the traffic policy.

Create rate limiting rules and shaping rule for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mls qos policer-profile <i>policer-name</i> [single hierarchy aggregate]</code>	Create a traffic policer profile, and enter traffic-policer configuration mode.
3	<code>Raisecom(traffic-policer)#cir <i>cir</i> cbs <i>cbs</i></code>	(Optional) configure flow mode token bucket parameters.  Flow mode token bucket is single token bucket, only supporting to configure red and green packets operation.
4	<code>Raisecom(traffic-policer)#cir <i>cir</i> cbs <i>cbs</i> ebs <i>ebs</i></code>	(Optional) configure RFC2697 mode token bucket parameters.
5	<code>Raisecom(traffic-policer)#cir <i>cir</i> cbs <i>cbs</i> pir <i>pir</i> pbs <i>pbs</i></code>	(Optional) configure RFC2698 mode token bucket parameters.
6	<code>Raisecom(traffic-policer)#cir <i>cir</i> cbs <i>cbs</i> eir <i>eir</i> ebs <i>ebs</i> [coupling]</code>	(Optional) configure RFC4115 mode or MEF token bucket parameters.
7	<code>Raisecom(traffic-policer)#drop-color { red yellow }</code>	(Optional) configure the token bucket to discard packets of a color.
8	<code>Raisecom(traffic-policer)#recolor { green-recolor { red / yellow } red-recolor { green / yellow } / yellow-recolor { green / red } }</code>	(Optional) configure packet recoloring.
9	<code>Raisecom(traffic-policer)#set-cos { green <i>cos</i> red <i>cos</i> yellow <i>cos</i> }</code>	(Optional) configure the mapping from packets color to CoS.
10	<code>Raisecom(traffic-policer)#set-dscp { green <i>green-value</i> red <i>red-value</i> yellow <i>yellow-value</i> }</code>	(Optional) configure the mapping from packets color to DSCP.

Step	Command	Description
11	Raisecom(traffic-policer)# set-pri { green <i>green-value</i> red <i>red-value</i> yellow <i>yellow-value</i> }	(Optional) configure the mapping from packets color to local priority.

8.5.6 Creating traffic policy

Create traffic policy for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# policy-map <i>policy-map-name</i>	Create traffic policy, and enter traffic policy pmap configuration mode.
3	Raisecom(config-pmap)# description <i>string</i>	(Optional) configure the description of traffic policy.

8.5.7 Defining traffic policy mapping



Note

Define one or more defined traffic classifications to one traffic policy.

Define traffic policy mapping for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# policy-map <i>policy-map-name</i>	Create traffic policy, and enter traffic policy pmap configuration mode.
3	Raisecom(config-pmap)# class-map <i>class-map-name</i>	Bind traffic classification with a traffic policy. The traffic policy is applied to the packets matching traffic classification. <div data-bbox="869 1534 965 1619" data-label="Image"> </div> <div data-bbox="954 1565 1058 1608" data-label="Section-Header"> <h3>Note</h3> </div> <p>At least one rule is required for traffic classification to bind traffic policy; otherwise the binding will fail.</p>



8.5.8 Defining traffic policy operation



Note

Define different operations to different flows in policy.

Define a traffic policy operation for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#policy-map <i>policy-map-name</i></code>	Create traffic policy, and enter traffic policy pmap configuration mode.
3	<code>Raisecom(config-pmap)#class-map <i>class-map-name</i></code>	Bind traffic classification with a traffic policy. The traffic policy is applied to the packets matching traffic classification.  Note At least one rule is necessary for traffic classification to bind traffic policy; otherwise the binding will fail.
4	<code>Raisecom(config-pmap-c)#police <i>policer-name</i></code>	(Optional) apply the token bucket on traffic policy and conduct rate limiting and shaping.  Note The token bucket needs to be created in advance and be configured with rate limiting and shaping rules; otherwise, the operation will fail.
6	<code>Raisecom(config-pmap-c)#redirect-to <i>interface-type interface-number</i></code>	(Optional) configure redirection rules under traffic classification, forwarding classified packets from assigned interface.
7	<code>Raisecom(config-pmap-c)#set { cos <i>cos-value</i> dscp <i>dscp-value</i> local-priority <i>value</i> }</code>	(Optional) configure remarking rules under traffic classification, modify packet CoS priority, local priority, inner VLAN, DSCP priority, IP precedence, and VLAN ID.
8	<code>Raisecom(config-pmap-c)#copy-to-mirror</code>	(Optional) configure traffic mirroring to the monitor interface.
9	<code>Raisecom(config-pmap-c)#statistics enable</code>	(Optional) configure traffic statistic rules under traffic classification, statistic packets for matched traffic classification.

8.5.9 Applying traffic policy to interfaces

Apply traffic policy to the interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.

Step	Command	Description
3	<code>Raisecom(config-gigaethernet1/1/1)#service-policy ingress <i>policy-map-name</i></code>	Apply the configured traffic policy to the ingress direction of the interface.

8.5.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show service-policy statistics interface <i>interface-type interface-number</i> ingress <i>policy-map policy-map-name</i> [<i>class-map class-map-name</i>]</code>	Show statistics about applied traffic policy.
2	<code>Raisecom#show service-policy interface [<i>interface-type interface-number</i>] [ingress]</code>	Show information about the applied traffic policy.
3	<code>Raisecom#show class-map [<i>class-map-name</i>]</code>	Show information about traffic classification.
4	<code>Raisecom#show policy-map [<i>policy-map-name</i>]</code>	Show information about traffic policy.
5	<code>Raisecom#show policy-map [<i>policy-map-name</i>] [<i>class class-map-name</i>]</code>	Show information about traffic classification in traffic policy.
6	<code>Raisecom#show mls qos policer [<i>policer-name</i>]</code>	Show information about the assigned token bucket (rate limiting and shaping).

8.6 Configuring rate limiting

8.6.1 Preparing for configurations

Scenario

When the network is congested, you wish 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.

Prerequisite

N/A

8.6.2 Configuring rate limiting based on interface

Configure rate limiting based on interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#rate-limit ingress cir cir-value cbs cbs-value</code>	Configure rate limiting based on interface.



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.

8.6.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show rate-limit interface</code>	Show configurations of rate limiting on interfaces.
	<code>Raisecom#show rate-limit interface interface-type interface-number</code>	

8.7 Configuring bandwidth rate limiting

8.7.1 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

8.7.2 Default configurations of bandwidth rate limiting

Default configurations of bandwidth rate limiting are as below.

Function	Default value
Color aware	Disable

8.7.3 Configuring bandwidth guarantee

Creating bandwidth guarantee profile

Create a bandwidth guarantee profile for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#bandwidth-profile <i>bwp-profile-id cir cir cbs cbs</i> [color-aware]</code> <code>Raisecom(config)#bandwidth-profile <i>bwp-profile-id cir cir cbs cbs eir</i> <i>eir ebs ebs</i> [color-aware [coupling]]</code>	Create a bandwidth guarantee profile.
3	<code>Raisecom(config)#bandwidth-profile <i>bwp-profile-id description word</i></code>	Configure the description of the bandwidth guarantee profile.
4	<code>Raisecom(config)#interface <i>interface-</i> <i>type interface-number</i></code> <code>Raisecom(config- gigaethernet1/1/*)#bandwidth ingress <i>bwp-profile-id</i></code>	Apply the bandwidth guarantee profile on the interface.

Configuring bandwidth guarantee based on interface+VLAN

Configure bandwidth guarantee based on interface+VLAN for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.

Step	Command	Description
2	<code>Raisecom(config)#bandwidth-profile bwp-profile-id cir cir cbs cbs [eir eir ebs ebs] [color-aware]</code>	Create a bandwidth guarantee profile.
3	<code>Raisecom(config)#interface interface- type interface-number Raisecom(config- gigaethernet1/1/*)#bandwidth ingress vlan vlan-id bwp-profile-id</code>	Apply the bandwidth guarantee profile on the interface+VLAN.

Configuring bandwidth guarantee based on interface+VLAN+CoS

Configure bandwidth guarantee based on interface+VLAN+CoS for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#bandwidth-profile bwp profile-id cir cir cbs cbs [eir eir ebs ebs] [color-aware]</code>	Create a bandwidth guarantee profile.
3	<code>Raisecom(config)#interface interface- type interface-number Raisecom(config- gigaethernet1/1/*)#bandwidth ingress vlan vlan-id coslist cos-value-list bwp-profile-id</code>	Apply the bandwidth guarantee profile on the interface+VLAN+CoS.



Note

If a bandwidth guarantee profile is used by other profiles or applied, it cannot be deleted.

8.7.4 Configuring hierarchical bandwidth guarantee

Creating hierarchical CoS bandwidth guarantee

Create a hierarchical CoS bandwidth guarantee for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#bandwidth-profile profile-id cir cir cbs cbs [eir eir ebs ebs] [color-aware]</code>	Create a bandwidth guarantee profile.

Step	Command	Description
3	<code>Raisecom(config)#hierarchy-cos bandwidth-profile hc-profile-id</code>	Create a hierarchical CoS profile, and enter Hcos configuration mode.
4	<code>Raisecom(config-hcos)#bandwidth coslist cos-list bwp-profile-id</code> <code>Raisecom(config-hcos)#exit</code>	Configure the hierarchical CoS profile.
5	<code>Raisecom(config)#interface interface-type interface-number</code> <code>Raisecom(config-gigaethernet1/1/*)#bandwidth ingress vlan vlan-id bwp-profile-id hierarchy-cos hc-profile-id</code>	Apply the hierarchical CoS profile on the ingress interface+VLAN.

Configuring hierarchical VLAN bandwidth guarantee

Create a hierarchical VLAN bandwidth guarantee for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#bandwidth-profile profile-id cir cir cbs cbs [eir eir ebs ebs] [color-aware]</code>	Create a bandwidth guarantee profile.
3	<code>Raisecom(config)#hierarchy-vlan bandwidth-profile hv-profile-id</code>	Create a hierarchical VLAN profile, and enter Hvlan configuration mode.
4	<code>Raisecom(config-hvlan)#bandwidth vlanlist vlan-list profile-id</code> <code>Raisecom(config-hvlan)#exit</code>	Configure the hierarchical VLAN profile.
5	<code>Raisecom(config)#interface interface-type interface-number</code> <code>Raisecom(config-gigaethernet1/1/*)#bandwidth ingress bwp-profile-id hierarchy-vlan hv-profile-id</code>	Apply the hierarchical VLAN profile on the ingress interface.



Note

If a hierarchical bandwidth guarantee profile is applied, it cannot be deleted or modified.

8.7.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show bandwidth-profile [<i>bwp-profile-id</i>]	Show information about the bandwidth guarantee profile.
2	Raisecom# show bandwidth interface <i>interface-type interface-number</i>	Show information about the bandwidth guarantee profile on the interface.
3	Raisecom# show hierarchy-cos-bandwidth profile [<i>hc-profile-id</i>]	Show information about the hierarchical CoS bandwidth guarantee profile.
4	Raisecom# show hierarchy-vlan-bandwidth profile [<i>hv-profile-id</i>]	Show information about the hierarchical VLAN bandwidth guarantee profile.

8.8 Configuring examples

8.8.1 Example for configuring congestion management

Networking requirements

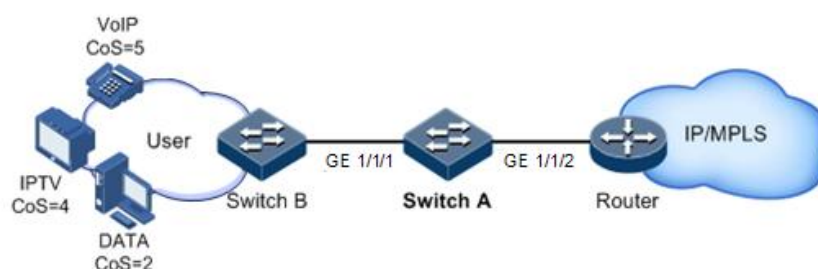
As shown in Figure 8-9, the user use voice, video and data services.

The CoS priority of voice service is 5, the CoS priority of video service is 4, and the CoS priority of data service 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 schedule to grant high priority.
- For video services, perform WRR schedule, with weight of 50.
- For data services, perform WRR schedule, with weight of 20.

Figure 8-9 Queue scheduling networking



Configuration steps

Step 1 Configure interface priority trust mode.

```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#mls qos trust cos
SwitchA(config-gigabitEthernet1/1/2)#quit
```

Step 2 Configure the profile for mapping between CoS priority and 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 between CoS priority and local priority on GE 1/1/2.

```
SwitchA(config)#interface gigabitEthernet 1/1/2
SwitchA(config-gigabitEthernet1/1/2)#mls qos cos-to-local-priority 1
SwitchA(config-gigabitEthernet1/1/2)#quit
```

Step 4 Conduct SP+WRR queue scheduling in the egress direction of GE 1/1/1.

```
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#mls qos queue scheduler wrr 1 1 20 1 1
50 0 0
SwitchA(config-gigabitEthernet1/1/1)#quit
```

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
-----
gigabitEthernet1/1/1  cos          0                   0              0              0
0
```

```

gigaethernet1/1/2    cos    0          1          0          0
0
...

```

Use the following command to show configurations of mapping between CoS priority and 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      6(G)      6(G)      7(G)      1      localpri(color) :0(G)  1(G)  2(G)  3(G)  5(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)
-----
1          1
2          1
3          20
4          1
5          1
6          50
7          0
8          0

```

8.8.2 Example for configuring rate limiting based on traffic policy

Networking requirements

As show in Figure 8-10, User A, User B, and User C respectively belong to VLAN 1, VLAN 2, and VLAN 3, and are connected to the ISCOM3000G series switch by Switch A, Switch B, and Switch C.

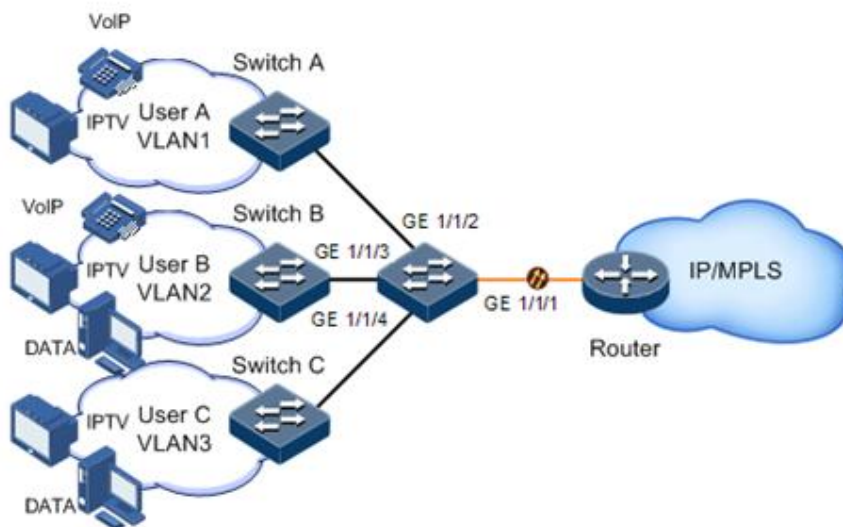
User A uses voice and video services, User B uses voice, video and data services, and User C uses video and data services.

According to service requirements, 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 8-10 Rate limiting based on traffic policy



Configuration steps

Step 1 Create and configure traffic classification, 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
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)##quit
Raisecom(config)#mls qos policer-profile userb single
Raisecom(traffic-policer)#cir 35000 cbs 100
Raisecom(traffic-policer)##quit
Raisecom(config)#mls qos policer-profile userc single
Raisecom(traffic-policer)#cir 30000 cbs 100
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 gig Ethernet 1/1/1
Raisecom(config-gig Ethernet1/1/1)#service-policy ingress usera
Raisecom(config-gig Ethernet1/1/1)#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 gig Ethernet 1/1/2
Raisecom(config-gig Ethernet1/1/2)#service-policy ingress userb
Raisecom(config-gig Ethernet1/1/1)#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 gig Ethernet 1/1/3
Raisecom(config-gig Ethernet1/1/3)#service-policy userc ingress 4
Raisecom(config-gig Ethernet1/1/1)#exit
  
```

Checking results

Use the **show class-map** command to show configurations of traffic classification.

```

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
```

8.8.3 Example for configuring rate limiting based on interface

Networking requirements

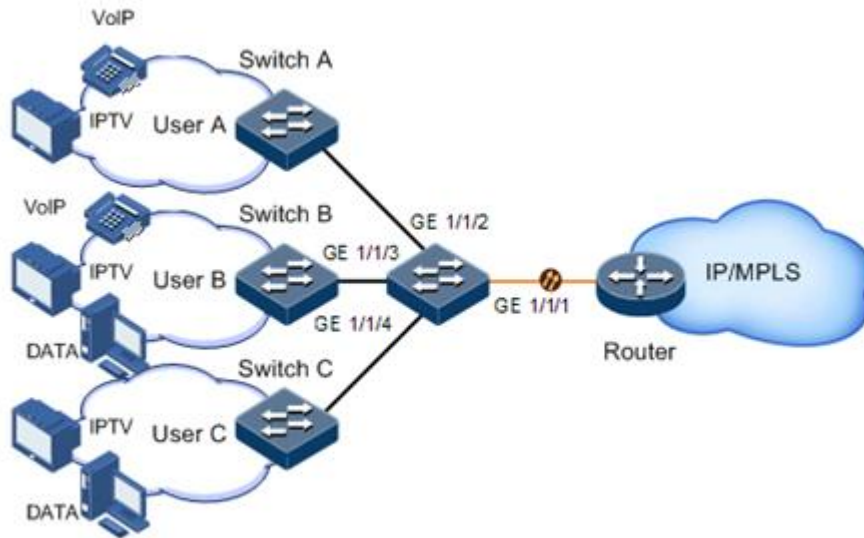
As shown in Figure 8-11, User A, User B, and User C are respectively connected to the ISCOM3000G series switch by Switch A, Switch B, and Switch C.

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.

- 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 8-11 Rate limiting based on interface



Configuration steps

Configure rate limiting based on interface.

```
Raisecom#config
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#rate-limit ingress cir 25000 cbs 100
Raisecom(config-gigabitEthernet1/1/1)#exit
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#rate-limit ingress cir 35000 cbs 100
Raisecom(config-gigabitEthernet1/1/2)#exit
Raisecom(config)#interface gigabitEthernet 1/1/3
Raisecom(config-gigabitEthernet1/1/3)#rate-limit ingress cir 30000 cbs 100
Raisecom(config-gigabitEthernet1/1/3)#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)
-----
gigabitEthernet1/1/1  ingress  25000          100          25024
101
```

gigaethernet1/1/2 101	ingress	30000	100	30016
gigaethernet1/1/3 101	ingress	30000	100	30016

9 Multicast

This chapter describes principles and configuration procedures of multicast, and provides related configuration examples, including the following sections:

- Introduction
- IGMP
- Basic functions of Layer 2 multicast
- IGMP Snooping
- IGMP Querier
- IGMP MVR
- IGMP filtering
- Multicast VLAN copy
- MLD
- PIM-SM

9.1 Introduction

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.

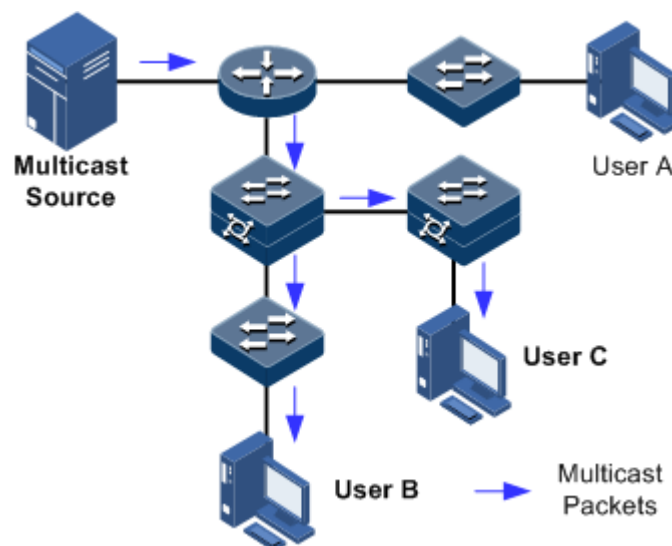
- Unicast: the system establishes a data transmission path for each user who needs the information, and sends separate copy information about them. Through unicast, the amount of information transmitted over the network is proportional to the number of

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.

- 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 on 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 9-1, 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 9-1 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 on 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
- 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

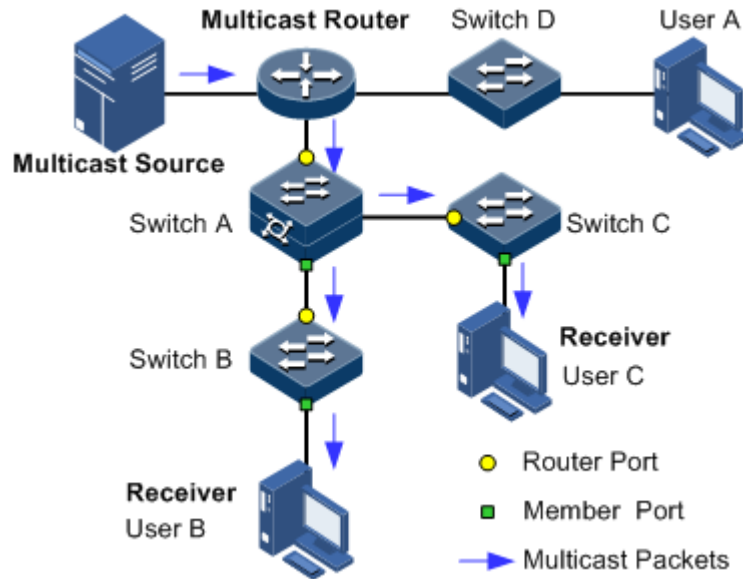
A routed interface refers to the interface towards the multicast router between a multicast router and a host. The ISCOM3000G series switch receives multicast packets from this interface.

- Member interface

Known as the Rx interface, a member interface is the interface towards the host between multicast router and the host. The ISCOM3000G series switch sends multicast packets from this interface.

Figure 9-2 shows basic concepts in multicast.

Figure 9-2 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

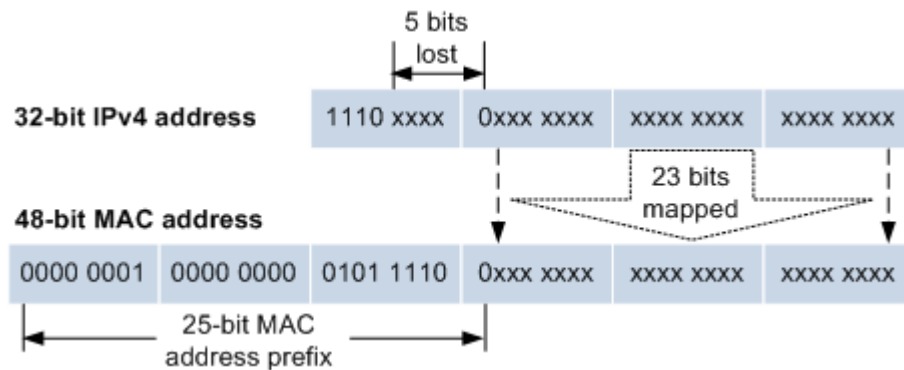
When the Ethernet transmits unicast IP packets, it uses the MAC address of the receiver as the destination MAC address. However, when multicast packets are transmitted, the destination is no longer a specific receiver, but a group with an uncertain number of members, so the Ethernet needs to use the 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 9-3 shows mapping between the IPv4 multicast address and MAC address.

Figure 9-3 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 ISCOM3000G series switch may receive excess data besides IPv4 multicast group, and these excess multicast data needs to be filtered by the upper layer on the ISCOM3000G series switch.

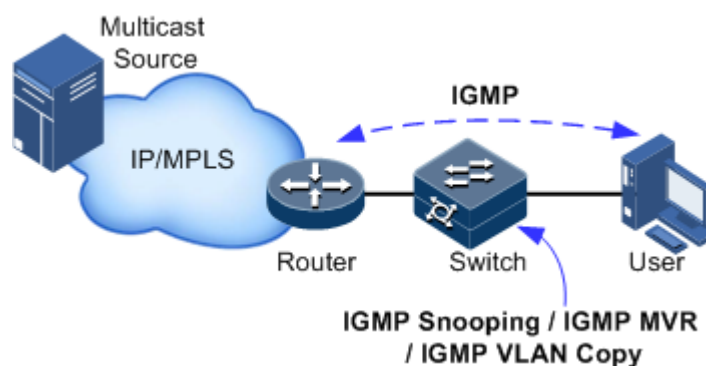
Basis of multicast protocol

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 9-4 shows operating of IGMP and Layer 2 multicast features.

Figure 9-4 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.

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 ISCOM3000G 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 ISCOM3000G series switch supports IGMPv1, IGMPv2, and IGMPv3.

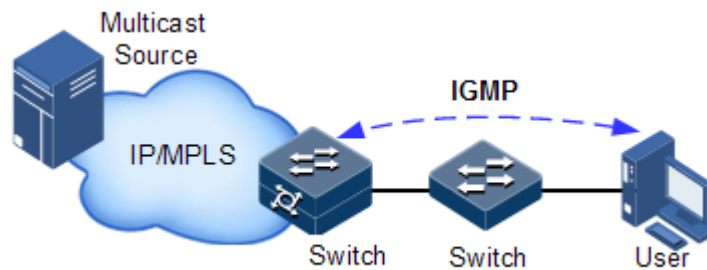
9.2 IGMP

9.2.1 Introduction

Internet Group Management Protocol (IGMP), one of the TCP/IP protocol suite, manages IPv4 multicast members. It runs between the multicast router and host. It defines the mechanism to establish and maintain multicast member relations between the multicast router and host. It does not define the mechanism to advertise and maintain group member relations between multicast routers; instead, this part is completed by multicast routing protocols.

IGMP manages multicast members by exchanging IGMP packets between the multicast router and host. IGMP runs on the network, as shown in Figure 9-5.

Figure 9-5 Principles of IGMP



IGMP packets are encapsulated in IP packets. There are three types of IGMP packets: Query packet, Report packet, and Leave packet. IGMP has the following basic functions:

- A host sends a Report packet to join a multicast group and a Leave packet to leave a multicast group. It determines multicast groups from which it receives packets.
- The multicast router periodically sends the Query packet, receives the Report packet and Leave packet sent by hosts, and thus learns multicast group members in the network segment. If there are multicast group members in the network segment, the multicast router forwards multicast packets to the network segment; otherwise, it does not forward packets.

At present, IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3. The later version is completely compatible with the former ones. IGMPv2 is most widely used. IGMPv1 does not support the Leave packet.

The ISCOM3000G series switch supports both IGMPv1 and IGMPv2.

The following part describes IGMP concepts.

Interval for sending Query packets

The querier periodically sends IGMP common group Query packets to detect whether there are multicast group members on the network. You can configure the interval for sending Query packets according to actual network conditions.

Maximum response time for Query packet

The maximum response time for Query packet determines the deadline for the host to send multicast member relation report. After receiving a Query packet, a host starts a timer for each joined multicast group. The range of the timer is configured randomly between 0 and maximum response time. When a timer expires, the host sends the Report packet to the multicast group.

Query interval of last member

The query interval of the last member is also called specific group query interval. After receiving an IGMP Leave packet sent by a host for a specified group, a switch periodically sends Query packets to the specified group.

The switch sends specific group Query packet to detect whether the multicast group has members.

- If yes, its members must send the Report packet within the maximum response time, and then the switch continues to maintain multicast forwarding entries of the multicast group upon receiving the Report packet.
- If no, the switch determines that the last member of the multicast group has left and thus the switch deletes multicast forwarding entries of the multicast group.

Robustness factor

Robustness factor is the times for the querier to send Query packets of the IGMP specific group, namely, the times for retransmitting packets to avoid possible packet loss. The greater the robustness factor is, the stronger the IGMP querier is and the longer the expiration time of the multicast group is.

Querier expiration time

The querier expiration time is the waiting time for another router to replace the former router as the new sender for Query packets after the former multicast router stops sending Query packets.

When there are multiple multicast routers in a network segment, the query router (querier) periodically sends Query packets on an interface. If another non-querier router fails to receive Query packets from the query router within querier expiration time, it determines the original query router invalid and then it becomes the querier.

9.2.2 Preparing for configurations

Scenario

IGMP is used between routers and hosts. By configuring IGMP on the interface on the multicast device connected to the user network, you can connect user hosts to the multicast network and make multicast packets reach the receiver.

The host notifies the local router through IGMP that it wishes to join a specified multicast group and receives information from the multicast group. The router uses IGMP to periodically query whether members of a known group are active. In this way, the network can collect and maintain relationship between group members on the network.

Prerequisite

- Configure network layer attributes of the interface to interconnect the network.
- Enable multicast route.

9.2.3 Default configurations of IGMP

Default configurations of IGMP are as below.

Function	Default value
IGMP status	Disable
Robustness factor	2
Expiration time for other queriers	255s
Maximum response time for Query packet	10s

Function	Default value
Interval for sending IGMP Query packets	125s
Last member query interval	1s

9.2.4 Enabling IGMP

Enable IGMP for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#ip igmp enable { 2 3 }	Configure the IGMP version.
4	Raisecom(config-vlan1)#ip igmp enable	Enable IGMP on the VLAN interface.

9.2.5 Configuring static group members

Configure static group members for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#ip igmp static group <i>group-address</i>	Configure static group members on the VLAN interface.

9.2.6 Configuring interval for sending IGMP Query packets

Configure the interval for sending IGMP Query packets for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#ip igmp query-interval <i>period</i>	Configure the interval for sending IGMP Query packets.

9.2.7 Configuring robustness factor

Configure the robustness factor for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#ip igmp robustness-variable <i>value</i>	Configure the robustness factor, namely, the times for retransmitting packets due to packet loss.

9.2.8 Configuring query interval of last member

Configure the query interval of the last member for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#ip igmp last-member-query- interval <i>interval</i>	Configure the query interval of the last member, namely, the interval for the specified group to query messages. This value can be used to adjust the leaving interval for the network.

9.2.9 Configuring maximum response time for querying IGMP packets

Configure the maximum response time for querying IGMP packets for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#int erface ip <i>if-number</i>	Enter Layer 3 interface configuration mode.
3	Raisecom(config- ip)#ip igmp query- max-response-time <i>period</i>	Configure the maximum response time for querying IGMP packets. This value is smaller than the interval for sending IGMP Query packets.

9.2.10 Configuring immediate leave for multicast members

Configure immediate leave for multicast members for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface vlan <i>vlan-id</i></code>	Enter VLAN interface configuration mode.
3	<code>Raisecom(config-vlan1)#ip igmp immediate-leave</code>	Configure immediate leave for multicast members.

9.2.11 Configuring access control for multicast groups and multicast sources

Configure access control for multicast groups and multicast sources for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip igmp ssm-mapping { <i>group-ip-address group-ip-mask</i> <i>group-ip-addresss/mask</i> } <i>source-ip-address</i></code>	Configure mapping rules for multicast groups and multicast sources.
3	<code>Raisecom(config)#interface vlan <i>vlan-id</i></code>	Enter VLAN interface configuration mode.
4	<code>Raisecom(config-vlan1)#ip igmp group-policy <i>acl-number</i></code>	(Optional) configure the range of multicast groups for the interface to join.
5	<code>Raisecom(config-vlan1)#ip igmp ssm-mapping { enable disable }</code>	(Optional) enable mapping of the specified multicast group and multicast source.

9.2.12 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show ip igmp group [<i>group-address</i> interface ip <i>if-number</i>]</code>	Show relationship between multicast group members.
2	<code>Raisecom#show ip igmp interface [ip <i>if-number</i>]</code>	Show IGMP configurations on Layer 3 interface.

No.	Command	Description
3	Raisecom# show ip igmp statistics [interface ip <i>if-number</i>]	Show statistics about IGMP packets.
4	Raisecom# show ip igmp ssm-mapping group	Show configured mapping between multicast groups and multicast sources.

9.2.13 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom(config)# clear ip igmp statistics [interface ip <i>if-number</i>]	Clear statistics about IGMP packets.
Raisecom(config)# clear ip igmp group [<i>group-address</i> <i>interface-type</i> <i>interface-number</i>]	Clear the multicast forwarding table.

9.3 Basic functions of Layer 2 multicast

9.3.1 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 ISCOM3000G series switch enabled with IGMP Snooping or IGMP MVR.



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 forwarding 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 forwarding entry when receiving IGMP Report packets. The timer of the multicast forwarding 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 forwarding entry immediately, but wait until the entry is aged after sending Leave packets. You can enable this function to delete the corresponding multicast forwarding 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.

9.3.2 Preparing for configurations

Scenario

Basic functions of Layer 2 multicast provide common features of Layer 2 multicast, and must be used on the ISCOM3000G 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.

9.3.3 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
Multicast forwarding entry aging time	300s
Interface IGMP ring network forwarding status	Disable

9.3.4 Configuring basic functions of Layer 2 multicast

Configure basic functions of Layer 2 multicast for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#igmp mrouter vlan <i>vlan-id</i> interface-type interface-number	(Optional) configure multicast route interface.
3	Raisecom(config)#igmp member- timeout { seconds infinite }	(Optional) configure immediate leave.
4	Raisecom(config)#igmp ring interface-type interface- number-list	(Optional) enable IGMP ring network forwarding on the interface.
5	Raisecom(config)#igmp report- suppression	(Optional) enable suppression.
6	Raisecom(config)#igmp version {2 3}	(Optional) configure the IGMP version.
7	Raisecom(config)#igmp snooping mrouter vlan <i>vlan-list</i> priority <i>priority-number</i>	(Optional) configure the CoS priority of the IGMP route VLAN.
8	Raisecom(config - gigaethernet1/1/1)#igmp immediate-leave vlan <i>vlan-list</i>	(Optional) configure immediate leave.

9.3.5 Checking configurations

Use the following commands to check configuration results.

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 [<i>interface-type interface- number</i>]	Show configuration of immediate leave on Layer 2 multicast.

No.	Command	Description
4	Raisecom#show igmp statistics [<i>interface-type interface-number</i>]	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.

9.3.6 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom(config)#clear igmp statistics [<i>interface-type interface-number</i>]	Clear statistics about Layer 2 multicast IGMP.
Raisecom(config)#no igmp member <i>interface-type interface-number</i>	Delete a specified multicast forwarding entry.

9.4 IGMP Snooping

9.4.1 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 ISCOM3000G series switch to monitor IGMP sessions between the host and multicast router. When monitoring a group of IGMP Report from host, the ISCOM3000G series switch will add host-related interface to the forwarding entry of this group. Similarly, when a forwarding entry reaches the aging time, the ISCOM3000G series switch will delete host-related interface from the forwarding table.

IGMP Snooping forwards multicast data through Layer 2 multicast forwarding entry. When receiving multicast data, the ISCOM3000G series switch will forward them directly according to the corresponding receiving interface of the multicast forwarding entry, instead of flooding them to all interfaces, to save bandwidth of the ISCOM3000G series switch effectively.

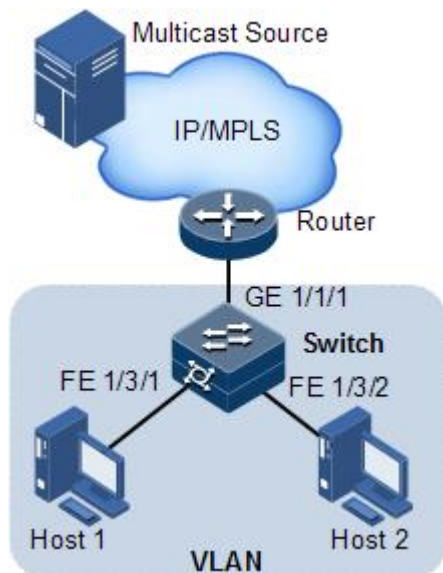
IGMP Snooping establishes a Layer 2 multicast forwarding table, of which entries can be learnt dynamically or configured manually.

9.4.2 Preparing for configurations

Scenario

As shown in Figure 9-6, 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 9-6 IGMP Snooping networking



Prerequisite

- Disable multicast VLAN copy on the ISCOM3000G series switch.
- Create VLANs.
- Add related interfaces to the VLANs.

9.4.3 Default configurations of IGMP Snooping

Default configurations of IGMP Snooping are as below.

Function	Default value
Global IGMP Snooping status	Disable
VLAN IGMP Snooping status	Disable
IGMP robustness	2

9.4.4 Configuring IGMP Snooping

Configure IGMP Snooping for the ISCOM3000G 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 time-out { seconds infinite }	(Optional) configure the aging time of IGMP members.
4	Raisecom(config)#igmp snooping vlan vlan-list	(Optional) enable IGMP Snooping on all VLANs.
5	Raisecom(config)#vlan vlan-id Raisecom(config-vlan)#igmp snooping static ip-address [interface-type interface-number]	(Optional) configure static members of IGMP Snooping in VLAN mode.
6	Raisecom(config)#igmp robust-count value	Configure IGMP robustness.



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.

9.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show igmp snooping [vlan vlan-list]	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.

9.4.6 Example for applying multicast on ring network

Networking requirements

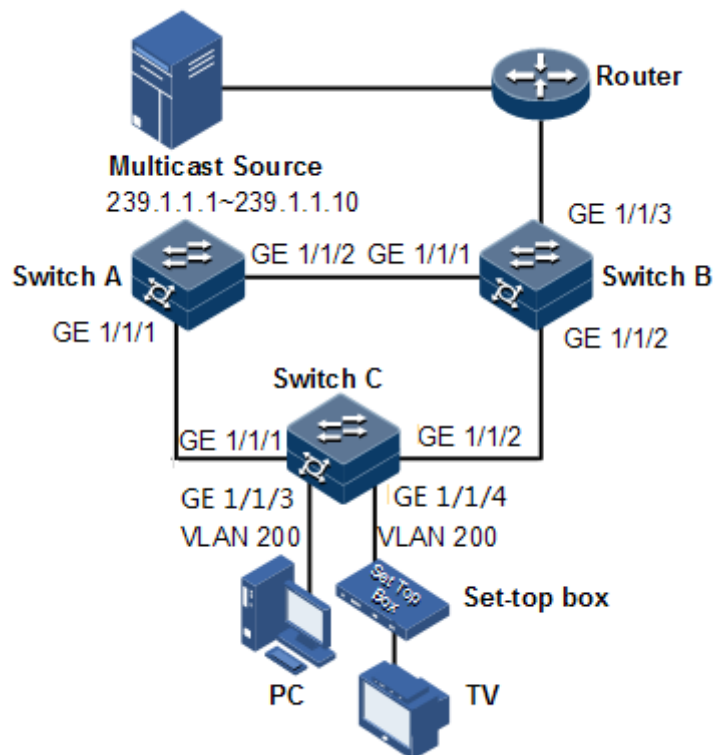
Configure IGMP ring forwarding on single Ethernet ring to make multicast service more stable and prevent multicast service from being disrupted by link failure.

As shown in Figure 9-7, 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. By doing this, it will not affect user's on-demand multicast stream whichever link fails in the Switch.

When using single Ethernet ring to provide multicast services, you can adopt IGMP MVR or IGMP Snooping to receive the multicast traffic.

The following example shows that STP provides ring network detection and IGMP Snooping provides multicast function.

Figure 9-7 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 gigaethernet1/1/1
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 gigaethernet1/1/2
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 gigaethernet1/1/1
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 gigaethernet1/1/2
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 gigaethernet1/1/1
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 gigaethernet1/1/2
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 gigaethernet1/1/1
SwitchA(config)#igmp ring gigaethernet1/1/2
SwitchA(config)#igmp snooping
SwitchA(config)#igmp snooping vlan 200
```

Configure Switch B.


```
SwitchB(config)#igmp ring gigaethernet1/1/1
SwitchB(config)#igmp ring gigaethernet1/1/2
SwitchB(config)#igmp snooping
SwitchB(config)#igmp snooping vlan 200
```

Configure Switch C.

```
SwitchC(config)#igmp ring gigaethernet1/1/1
SwitchC(config)#igmp ring gigaethernet1/1/2
SwitchC(config)#igmp snooping
```

Checking results

Disconnect any link in the ring, and check whether the multicast flow can be received normally.

9.5 IGMP Querier

9.5.1 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 proxy host function and also proxy multicast router functions for the next agent. The Layer 2 network device enabled with MVR Querier has two roles:

- On 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 user.
- On 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/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/multicast VLAN copy is enabled, IGMP Querier can be enabled or disabled respectively.

- 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.

9.5.2 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 interface to VLANs.

9.5.3 Default configurations of IGMP Querier

Default configurations of IGMP Querier area as below.

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	60s
Maximum response time to send Query packets	10s
Interval for the last member to send Query packets	1s

9.5.4 Configuring IGMP Querier

Configure IGMP Querier for the ISCOM3000G 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	(Optional) configure the source IP address for the IGMP querier to send Query packets.
4	raisecom(config)#igmp querier query-interval period	(Optional) configure the IGMP query interval.
5	raisecom(config)#igmp querier query-max-response-time period	(Optional) configure the maximum response time to send Query packets.
6	raisecom(config)#igmp querier last-member-query-interval period	(Optional) configure the interval for the last member to send Query packets.

Step	Command	Description
7	raisecom(config)# igmp proxy	Configure IGMP proxy.



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.

9.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	raisecom# show igmp querier	Show configurations of IGMP Querier.

9.5.6 Example for configuring IGMP Snooping and IGMP Querier

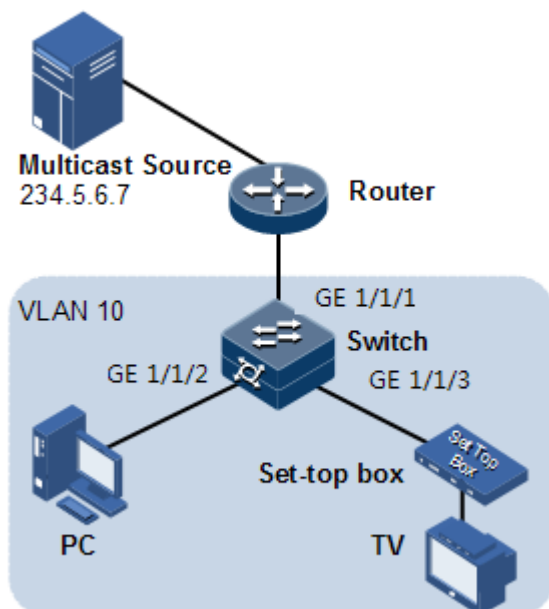
Networking requirements

As shown in Figure 9-8, 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.

Figure 9-8 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
```

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)     :300
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       --
S
```

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
Aging Time(s)           :60
Next General Query(s)    :--
```

9.6 IGMP MVR

9.6.1 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 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 achieve Layer 2 multicast, but the difference is: multicast VLAN in IGMP Snooping is the same with user VLAN, while multicast VLAN in IGMP MVR can be different with user VLAN.



Note

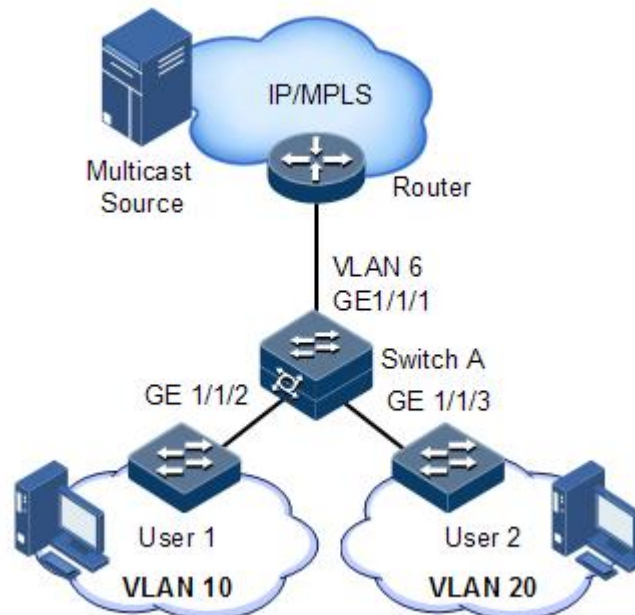
One switch can configure up to 10 multicast VLAN, at least one multicast VLAN and group addresses. The supported maximum number of multicast groups is 1024.

9.6.2 Preparing for configurations

Scenario

As shown in Figure 9-9, 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 9-9 IGMP MVR networking



Prerequisite

- Disable multicast VLAN copy.
- Create VLANs.
- Add related interfaces to the VLANs.


9.6.3 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

9.6.4 Configuring IGMP MVR

Configure IGMP MVR for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#igmp mvr</code>	Enable global IGMP MVR.
3	<code>Raisecom(config)#igmp mvr mcast-vlan vlan-id group { start-ip-address [end-ip- address] any }</code>	Configure the group address set for multicast VLAN.  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	<code>Raisecom(config)#interface gigaethernet 1/1/1</code>	Enter interface configuration mode.
5	<code>Raisecom(config- gigaethernet1/1/1)#igmp mvr mcast-vlan vlan-id static ip-address user-vlan vlan-id</code>	(Optional) configure static multicast members of MVR for a specified customer VLAN.
6	<code>Raisecom(config- gigaethernet1/1/1)#igmp mvr user-vlan vlan-id</code>	(Optional) configure the range for multicast inter-VLAN copy to take effect.
7	<code>Raisecom(config- gigaethernet1/1/1)#igmp mvr mcast-vlan vlan-id static ip-address</code>	(Optional) configure static multicast members of MVR on the Access interface.



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.

9.6.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show igmp mvr [<i>interface-type</i> <i>interface-number</i>]	Show configurations of IGMP MVR.
2	Raisecom# show igmp mvr { interface <i>interface-type</i> <i>interface-number</i> }	Show configurations of IGMP MVR on the specified interface.
3	Raisecom# show igmp mvr members [<i>interface-type</i> <i>interface-number</i> user-vlan <i>vlan-id</i>]	Show information about multicast group members of IGMP MVR.
4	Raisecom# show igmp mvr member count { <i>interface-type</i> <i>interface-number</i> user-vlan <i>vlan-id</i> }	Show the number of multicast group members of IGMP MVR.
5	Raisecom# show igmp mvr vlan-group [mcast-vlan <i>vlan-id</i>]	Show multicast VLAN and its group address set.

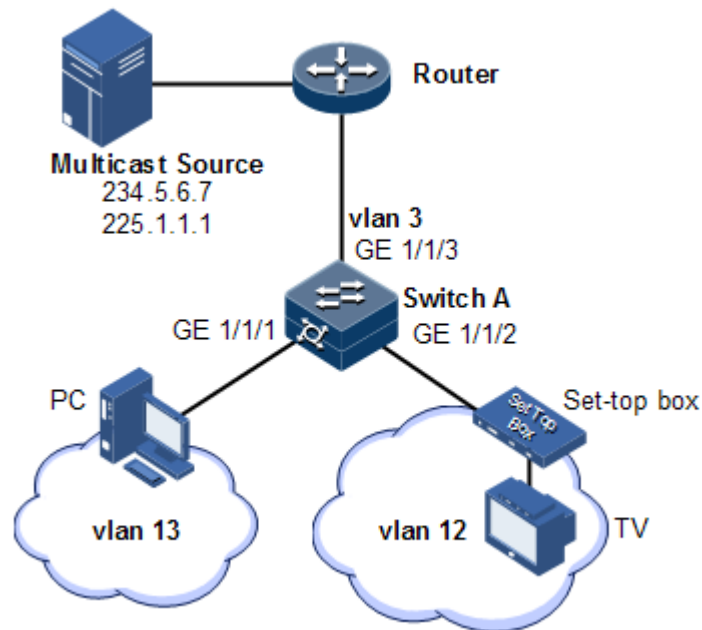
9.6.6 Example for configuring IGMP MVR

Networking requirements

As shown in Figure 9-10, 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 9-10 MVR networking



Configuration steps

Step 1 Create VLANs on Switch A and add interfaces to them.

```
Raisecom(config)#config
Raisecom(config)#creat 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 13
Raisecom(config-gigaethernet1/1/1)#switchport trunk untagged vlan 12
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet1/1/2
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 gigaethernet1/1/3
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 gigaethernet1/1/1
Raisecom(config-gigaethernet1/1/1)#igmp mvr
Raisecom(config-tengigabitethernet1/1/1)#igmp mvr user-vlan 13
```

```
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet1/1/2
Raisecom(config-gigaethernet1/1/2)#igmp mvr
Raisecom(config-tengigabitethernet1/1/2)#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)        :300
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
Mcast-vlan   Start-group   End-group
-----
3             225.1.1.1     225.1.1.1
3             234.5.6.7     234.5.6.7
```

9.7 IGMP filtering

9.7.1 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 filter 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 filter 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 filter

profile is applied to the interface, the interface will discard the IGMP report packet from this group directly when receiving it and disallow the interface to receive this group of multicast data.

IGMP filter 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.

9.7.2 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 Querier is generally used with IGMP Snooping or IGMP MVR.

Prerequisite

- Create VLANs.
- Add related interfaces to the VLANs.

9.7.3 Default configurations of IGMP filtering

Default configurations of IGMP filtering are as below.

Function	Default value
Global IGMP filtering	Disable
IGMP filter profile Profile	N/A
IGMP filter profile action	Refuse
IGMP filtering under interface	No maximum group limit, with the largest group action of drop, no application filter profile
IGMP filtering under interface+VLAN	No maximum group limit, with the largest group action of drop, no application filter profile

9.7.4 Enabling global IGMP filtering

Enable global IGMP filtering for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode
2	<code>Raisecom(config)#igmp filter</code>	Enable global IGMP filtering



Note

When configuring IGMP filter profile or the maximum group number, use the **igmp filter** command to enable global IGMP filtering.

9.7.5 Configuring IGMP filter profile

IGMP filter profile can be used to interface or interface+VLAN.

Configure IGMP filter profile for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode
2	<code>Raisecom(config)#igmp filter profile profile-number</code>	Create IGMP Profile and enter Profile configuration mode.
3	<code>Raisecom(config-igmp-profile)#{ permit deny }</code>	Configure IGMP Profile action.
4	<code>Raisecom(config-igmp-profile)#range range-id start-ip-address [end-ip-address]</code>	Configure to control IP multicast address access and range.
5	<code>Raisecom(config-igmp-profile)#exit</code> <code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode or LAG configuration mode.
6	<code>Raisecom(config-gigaethernet1/1/1)#igmp filter profile profile-number [vlan vlan-list]</code>	Configure IGMP Profile filter profile to physical interface or interface+VLAN.
	<code>Raisecom(config-aggregator)#igmp filter profile profile-number [vlan vlan-list]</code> <code>Raisecom(config-aggregator)#exit</code>	Configure IGMP Profile filter profile to LAG interface or interface+VLAN.
7	<code>Raisecom(config)# igmp drop [query report]</code>	(Optional) enable IGMP to filter query packets from the user interface or join or leave packets from the upstream interface.



Note

Perform the command of **igmp filter profile** *profile-number* 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.

9.7.6 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
3	Raisecom(config-gigaethernet1/1/1)# igmp filter max-groups <i>group-number [vlan vlan-list]</i>	Configure the maximum number of multicast groups to physical interface or interface+VLAN.
	Raisecom(config-portchannel1)# igmp filter max-groups <i>group-number [vlan vlan-list]</i>	Configure the maximum number of multicast groups to LAG interface or interface+VLAN.
4	Raisecom(config-gigaethernet1/1/1)# igmp filter max-groups action { drop replace } [vlan <i>vlan-list</i>]	(Optional) configure the action over maximum number of multicast groups in physical interface or interface+VLAN.
	Raisecom(config-portchannel1)# igmp filter max-groups action { drop replace } [vlan <i>vlan-list</i>]	(Optional) configure the action over maximum number of multicast groups in LAG interface or interface+VLAN.

9.7.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show igmp filter [interface <i>interface-type interface-number [vlan vlan-id]</i>]	Show configurations of IGMP filtering.
2	Raisecom# show igmp filter profile [<i>profile-number</i>]	Show information about the IGMP profile.

9.7.8 Example for applying IGMP filtering on interface

Networking requirements

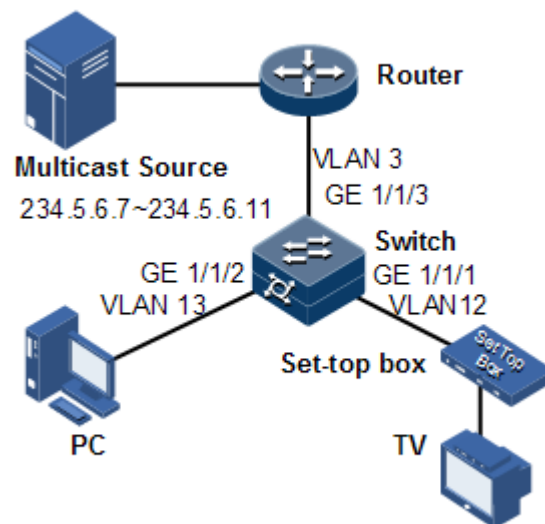
Enable IGMP filtering on the switch. Add filtering rules on the interface to filter multicast users.

As shown in Figure 9-11,

- 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 GE 1/1/2, 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 9-11 Applying IGMP filtering on interface



Configuration steps

Step 1 Create VLANs, and add interfaces to VLANs.

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

```
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 filter 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
```


Checking results

Use the following command to show configurations of IGMP filtering on the interface.

```
Raisecom#show igmp filter gigaethernet 1/1/1
igmp profile: 1
max group: 1
current group: 0
action: replace
```

9.8 Multicast VLAN copy

9.8.1 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 to copy multicast data to each user VLAN.

IGMP MVR transmits data in a way as shown in Figure 9-12 while multicast VLAN copy transmits data in a way as shown in Figure 9-13.

Figure 9-12 Data transmission of IGMP MVR

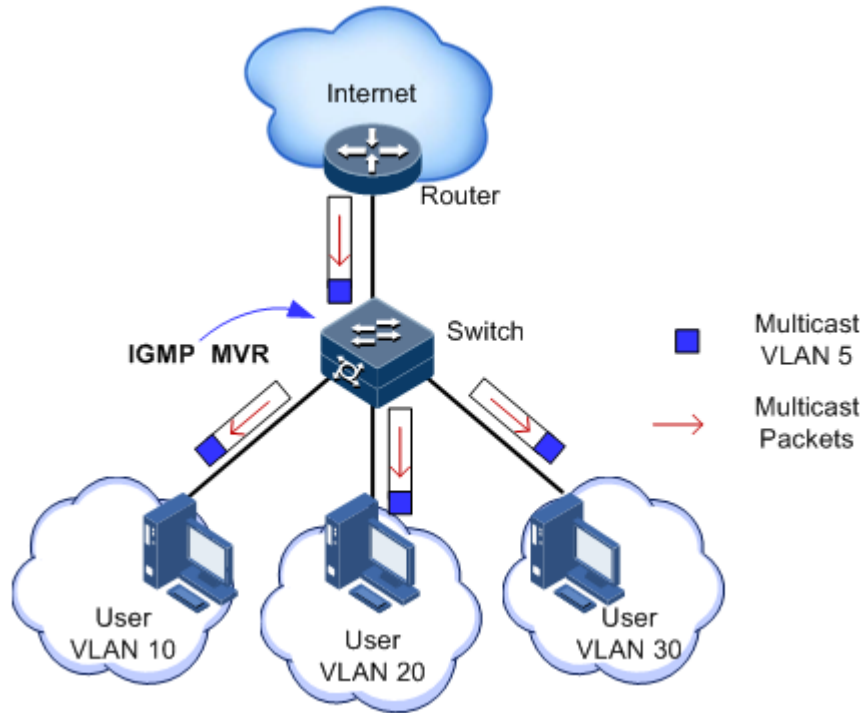
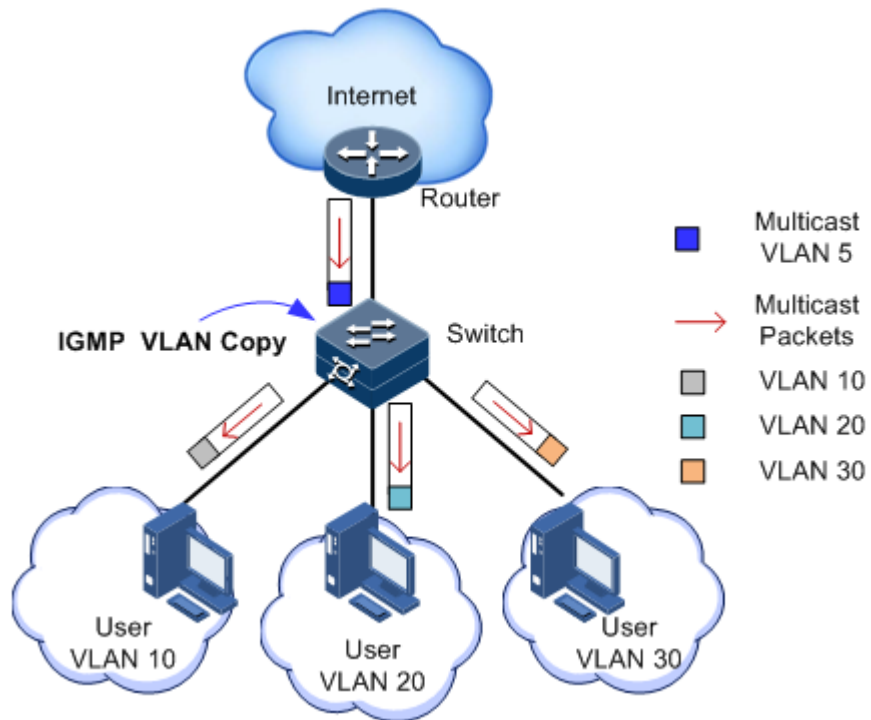


Figure 9-13 Data transmission of multicast VLAN copy





Note

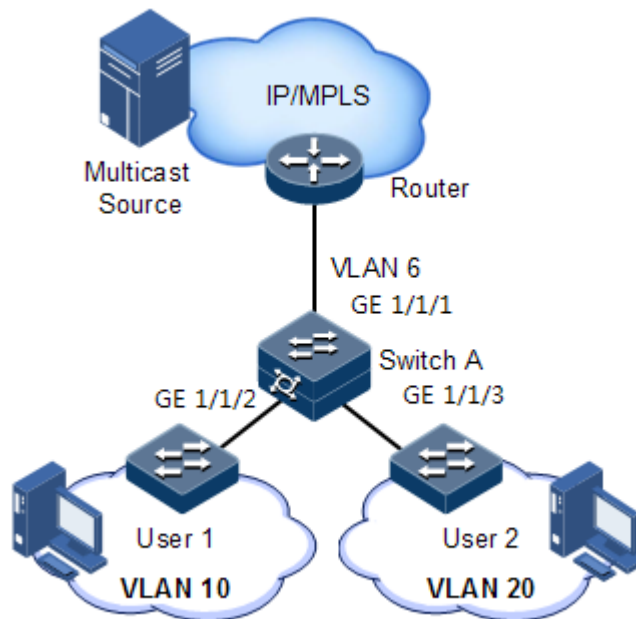
The ISCOM3000G series switch can be configured with 1–10 multicast VLANs and at least one multicast VLAN and corresponding group address set. It supports up to 1024 multicast groups.

9.8.2 Preparing for configurations

Scenario

As shown in Figure 9-14, 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 9-14 Multicast VLAN copy networking



Prerequisite

Create VLANs, and add related interfaces to VLANs.

9.8.3 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

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 first and then configure N:1 VLAN mapping.
- To concurrently configure N:1 VLAN mapping and PIM, you must configure PIM first and then configure N:1 VLAN mapping.

9.8.4 Configuring multicast VLAN copy

Configure multicast VLAN copy for the ISCOM3000G 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 }	Configure the group address set of the multicast VLAN.  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.

9.8.5 Configuring static multicast members of VLAN copy

Configure static multicast members of VLAN copy for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface interface-type interface-number	Enter physical layer interface configuration mode.
4	Raisecom(config- gigaethernet1/1/1)#igmp vlan-copy mcast-vlan vlan-id static ip- address user-vlan vlan-id	Configure static multicast members of VLAN copy.



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.

9.8.6 Configuring customer VLAN of VLAN copy

Configure the customer VLAN of VLAN copy for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#igmp vlan-copy user-vlan vlan-id</code>	Configure the customer VLAN of multicast VLAN copy.

9.8.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show igmp vlan- copy</code>	Show configurations of multicast VLAN copy.
2	<code>Raisecom#show igmp vlan- copy interface-type interface-number</code>	Show configurations of multicast VLAN copy on the specified interface.
3	<code>Raisecom#show igmp vlan- copy member</code>	Show information about multicast group members of multicast VLAN copy.
4	<code>Raisecom#show igmp vlan- copy member interface- type interface-number</code>	Show information about multicast group members of multicast VLAN copy on the specified interface.
5	<code>Raisecom#show igmp vlan- copy member user-vlan vlan-id</code>	Show information about multicast group members of multicast VLAN copy in the specified user VLAN.
6	<code>Raisecom#show igmp vlan- copy vlan-group [mcast- vlan vlan-id]</code>	Show the multicast VLAN and bound group address set of multicast VLAN copy.
7	<code>Raisecom#show igmp vlan- copy-table [vlan vlan- id] [count]</code>	Show the multicast VLAN copy table.

9.9 MLD

9.9.1 Introduction

MLD is a network protocol used in multicast technologies. Through MLD, a router can snoop whether there is a snooper of the IPv6 multicast group in the directly-connected network segment, and then record the result in the database. The router also maintains timer information about these IPv6 multicast addresses. Through MLD, the user host and the expected directly-connected multicast router establish and maintain multicast membership.

A MLD router uses the local address of IPv6 unicast link as the source address to send MLD packets, and uses ICMPv6 packets. All MLD packets are limited to local links, with hops of 1.

The ISCOM2600 supports two MLD versions:

- MLDv1: defined by RFC2710, derived from IGMPv2
- MLDv2: defined by RFC3810, derived from IGMPv3

MLDv1 is used to manage IPv6 multicast group members through the querying and response mechanism. Based on MLDv1, MLDv2:

- Additionally support filtering IPv6 multicast sources. When a host joins an IPv6 multicast group, it can request to receive or deny messages from a specified IPv6 multicast source.
- Additionally support configuring the maximum response time. Thus, MLDv2 is applicable to larger networks.
- It does not support response suppression; namely, the host does not need to process packets from other hosts, thus simplifying hosts operations.
- Add an S flag bit in the querying packet to enhance robustness of the system.
- Add the retransmission mechanism to the querying and response packets.

9.9.2 Preparing for configurations

Scenarios

Multicast arising in the IPv4 era solves the problem of single-point sending and multi-point receiving, and transmits data efficiently point to multiple points on the network, thus saving network bandwidth and lowering network load. It is enhanced on the IPv4 network. By listening MLD messages and thus creating a forwarding table for multicast packets, the ISCOM3000G series switch can manage and control the forwarding of multicast packets, and forward multicast packets to the target host.

Prerequisite

Configure the IPv6 address of the interface.

9.9.3 Default configurations of MLD

Default configurations of MLD are as below.

Function	Default value
MLD ring network forwarding on the interface	Disable

Function	Default value
MLD Snooping	Disable
MLD version	1
Aging time of MLD members	260s
MLD robustness	2

9.9.4 Configuring basic functions of MLD

Configure basic functions of MLD for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mld mrouter vlan <i>vlan-id</i> interface-type interface- number	Create a multicast router interface on the specified VLAN.
3	Raisecom(config)#mld ring interface-type interface- number	Enable MLD ring network forwarding on the interface.
4	Raisecom(config)#interface interface-type interface- number Raisecom(config- gigaethernet1/1/*)#mld immediate-leave [vlan vlan-list]	(Optional) enable immediate leave of MLD on the interface or interface+VLAN.
5	Raisecom(config)#mld report-suppression	(Optional) enable Report suppression. When receiving multiple Report packets from the same group in a specified period, the ISCOM3000G series switch forwards only one Report packet to the router interface while it suppresses others.
6	Raisecom(config)#mld member-timeout { <i>second</i> infinite }	(Optional) configure the aging time of MLD members.
7	Raisecom(config)#mld version { 1 2 }	Configure the MLD version.

9.9.5 Configuring MLD Snooping

Configure MLD Snooping for the ISCOM3000G series switch as below.

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

Step	Command	Description
2	Raisecom(config)#mld snooping	Enable global MLD Snooping.
4	Raisecom(config)#mld snooping vlan <i>vlan-list</i>	(Optional) enable MLD Snooping in all VLANs.
5	Raisecom(config)#vlan <i>vlan-id</i> Raisecom(config-vlan)#mld snooping static <i>ip-address</i> [<i>interface-type interface-number</i>]	(Optional) configure the static member of MLD Snooping in VLAN mode.

9.9.6 Configuring MLD Querier

Configure MLD Querier for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mld querier	Enable MLD querier.
3	Raisecom(config)#mld source-ip <i>ip-address</i>	(Optional) configure the source IP address for MLD Querier to send Query packets.
4	Raisecom(config)#mld query-interval <i>period</i>	(Optional) configure the MLD query interval.
5	Raisecom(config)#mld query-max-response-time <i>period</i>	(Optional) configure the maximum response time of Query packets.
6	Raisecom(config)#mld last-member-query-interval <i>period</i>	(Optional) configure the interval for the last member to send Query packets.
7	Raisecom(config)#mld robust-count <i>value</i>	Configure the robustness factor of MLD.
8	Raisecom(config)#mld proxy	Enable MLD Proxy.



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.
- MLD proxy and MLD Querier are mutually exclusive. MLD proxy and MLD report-suppression are mutually exclusive.

9.9.7 Configuring MLD filtering

Enable global MLD filtering

Enable global MLD filtering for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mld filter</code>	Enable global MLD filtering.



Note

Before applying the MLD filtering profile or configuring the maximum number of groups, use the **mld filter** command to enable global MLD filtering.

Configuring MLD filtering profile

The MLD filtering profile can be used on the interface or interface+VLAN.

Configure the MLD filtering profile for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mld filter profile profile-number</code>	Create a MLD profile, and enter profile configuration mode.
3	<code>Raisecom(config-mld-profile)#{ permit deny }</code>	Configure the action of the MLD profile.
4	<code>Raisecom(config-mld-profile)#range range-id start-ip-address [end-ip-address]</code>	Configure the IPv6 multicast address or range for access control.
5	<code>Raisecom(config-mld-profile)#exit</code> <code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode or LAG configuration mode.
6	<code>Raisecom(config-gigaethernet1/1/1)#mld filter profile profile-number [vlan vlan-list]</code>	Apply the MLD filtering profile to the physical interface or interface+VLAN.
	<code>Raisecom(config-aggregator)#mld filter profile profile-number [vlan vlan-list]</code> <code>Raisecom(config-aggregator)#exit</code>	Apply the MLD filtering profile to the LAG interface or interface+VLAN.



Note

By using the **mld filter profile** *profile-number* command in interface configuration mode, you can apply a created MLD profile to the specified interface. A MLD profile can be applied to multiple interfaces, but only one MLD profile can be applied to each interface.

Configuring maximum number of groups

The maximum number of groups for the user to join can be applied to the interface or interface+VLAN.

Configure maximum number of groups for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#mld filter max-groups <i>group-number [vlan vlan-list]</i>	Apply the maximum number of groups to the physical interface or interface+VLAN.
	Raisecom(config-aggregator)#mld filter max-groups <i>group-number [vlan vlan-list]</i>	Apply the maximum number of groups to the LAG interface or interface+VLAN.
4	Raisecom(config-gigaethernet1/1/1)#mld filter max-groups action { drop replace } [<i>vlan vlan-list</i>]	(Optional) configure the action to be taken when the number of groups for the physical interface or interface+VLAN to join exceeds the maximum number of groups.
	Raisecom(config-aggregator)#mld filter max-groups action { drop replace } [<i>vlan vlan-list</i>]	(Optional) configure the action to be taken when the number of groups for the LAG interface or interface+VLAN to join exceeds the maximum number of groups.

9.9.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show mld immediate-leave [<i>interface-type interface-number</i> port-channel <i>port-channel-id</i>]	Show configurations of immediate leave of MLD.

No.	Command	Description
2	Raisecom# show mld mrouter	Show information about the multicast router interface of MLD.
3	Raisecom# show mld snooping [<i>vlan vlan-id</i>]	Show configurations of MLD Snooping.
4	Raisecom# show mld snooping member [<i>interface-type interface-number</i> <i>vlan vlan-id</i>]	Show information about multicast group members of MLD Snooping.
5	Raisecom# show mld snooping member count [<i>interface-type interface-number</i> <i>vlan vlan-id</i>]	Show the number of multicast group members of MLD Snooping.
6	Raisecom# show mld statistics [<i>interface-type interface-number</i>]	Show statistics of MLD statistics.
7	Raisecom# show mld filter [<i>interface</i> <i>gigahernet interface-number</i> [<i>vlan vlan-id</i>]]	Show configuration of MLD filtering.
8	Raisecom# show mld filter profile [<i>profile-number</i>]	Show configurations of the MLD filtering profile.
9	Raisecom# show mld configuration	Show basic configurations of MLD.

9.9.9 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom# clear mld statistics [<i>interface-type interface-number</i>]	Clear MLD statistics.

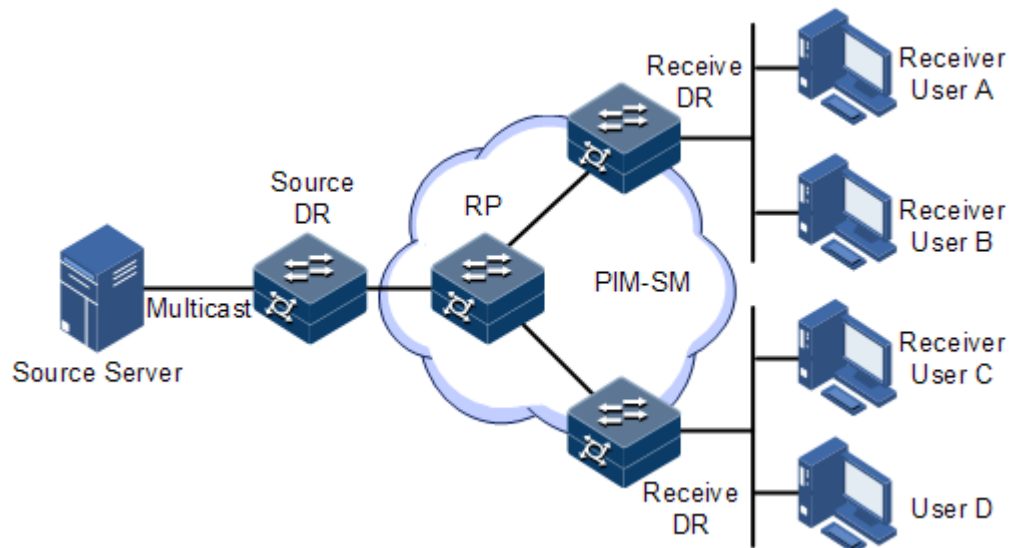
9.10 PIM-SM

9.10.1 Introduction

Protocol Independent Multicast-Dense Mode (PIM-DM) is a dense-mode multicast routing protocol and fits for a network with a wide distribution of group members, wide range, and large scale. PIM-SM is independent of any unicast routing protocol, so it is called the protocol independent multicast routing protocol.

Figure 9-15 shows the function and location of PIM-SM in the multicast network.

Figure 9-15 PIM-SM networking



PIM-SM devices discover neighbors by sending Hello packets. When a PIM-SM device is started, it periodically sends Hello packets on the PIM-SM interface. The neighbor discovery mechanism defines the neighbor holding time of Hello packets, namely, the maximum time for a neighbor to wait for the next Hello packet. If the neighbor receives the next Hello packet within the time, it deletes the device from its neighbor list.

PIM-SM uses joining and pruning to establish multicast distribution trees. The receiver sends the Report message to the receiver DR, which then sends the (*,G) joining packet towards the RP direction to establish the shared tree. The multicast source sends data and DR sends an application to be registered by the RP.

- If the RP has a receiver, it sends the (S,G) joining packet in the multicast source direction to establish the source tree. The multicast source packets in the PIM-SM network reach the RP along the shared tree to the receiver. When the receiver leaves, it sends the Leave packet to the receiver DR, which then sends the (*,G) pruning packets to prune the shared tree.
- If the RP has no receiver, it sends the (S,G) pruning packets to the multicast source direction to prune the source tree.

PIM-SM uses SPT switching to relieve the load of the shared tree. The receiving DR chooses a proper switching policy to switch (S,G) data to the SPT tree to relieve the load of the RPT tree. When the receiving DR meets the switching policy, the receiving DR sends the (S,G) joining packet to the multicast source direction to establish the SPT tree from the multicast source to the receiving DR, and sends the (S,G,rpt) pruning packet in the RP direction to prune multicast traffic of (S,G) on the RPT tree, thus relieving the load of the shared tree.

9.10.2 Preparing for configurations

Scenario

By configuring PIM-SM, you can implement multicast route and data forwarding.

Prerequisite

N/A

9.10.3 Default configurations of PIM-SM

Default configurations of PIM-SM are as below.

Function	Default value
Interface PIM-SM status	Disable
DR priority	1
Multicast source KeepAlive time	210s
Interval for checking whether the rate of multicast data exceeds the threshold before RPT switches to SPT	15s



Note

- To concurrently configure N:1 VLAN mapping and VLAN copy, you must configure VLAN copy first and then configure N:1 VLAN mapping.
- To concurrently configure N:1 VLAN mapping and PIM, you must configure PIM first and then configure N:1 VLAN mapping.

9.10.4 Configuring dynamic RP

Configure the dynamic RP for the ISCOM2924GF-4C as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router pim</code>	Enter PIM mode.
3	<code>Raisecom(config-router-pim)#bsr-candidate { interface-type interface-number vlan vlan-id loopback interface-number } [hash-mask-length mask-length] [priority priority]</code>	Configure the candidate BSR.
4	<code>Raisecom(config-router-pim)#rp-candidate { interface-type interface-number vlan vlan-id loopback interface-number } [group ip-addresss/mask]</code> <code>Raisecom(config-router-pim)#rp-candidate priority priority</code>	Configure the candidate RP and its priority.
5	<code>Raisecom(config-router-pim)#spt-threshold { rate infinity } [group-policy acl-number]</code>	Configure SPT switching control parameters.
6	<code>Raisecom(config-router-pim)#source-lifetime interval</code>	Configure the aging time of multicast routing entries.

Step	Command	Description
7	Raisecom(config-router-pim)#timer spt-switch interval	Configure the interval for checking whether the rate of multicast data exceeds the threshold before RPT switches to SPT

9.10.5 Configuring static RP

Configure the static RP for the ISCOM2924GF-4C as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router pim	Enter PIM mode.
3	Raisecom(config-router-pim)rp-address ip-address [group ip-addresss/mask]	Configure the IP address of static RP.

9.10.6 Configuring Layer 3 multicast forwarding

Configure Layer 3 multicast forwarding for the ISCOM2924GF-4C as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)ip multicast routing	Enable Layer 3 multicast forwarding.

9.10.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show ip pim neighbor	Show information about PIM neighbors.
2	Raisecom#show ip pim interface	Show information about PIM interfaces.
3	Raisecom#show ip pim bsr-router	Show BSR information.
4	Raisecom#show ip pim rp-candidate	Show information about candidate RPs.
5	Raisecom#show ip pim rp	Show RP information.
6	Raisecom#show ip pim route	Show information about the PIM multicast routing table.

10 Security

This chapter describes principles and configuration procedures of 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 URPF
- Configuring CPU protection
- Configuring anti-ARP attack

10.1 ACL

10.1.1 Introduction

Access Control List (ACL) is a set of ordered rules, which can control the ISCOM3000G 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 ID of data packets. The ISCOM3000G series switch judges receiving or rejecting packets according to the rules.

10.1.2 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:

- **IP ACL:** define classification rules according to attributes carried in the header of IP packets, such as the source IP address, destination IP address, TCP or UDP port ID (being 0 by default).
- **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.
- **MAP ACL:** MAP ACL can define more protocols and more detailed protocol fields than IP ACL and MAC ACL, can also match any bytes from byte 0 to byte 127 of Layer 2 data frame according to user's definition (the offset starts from 0).

There are 4 ACL modes according to different application environments:

- ACL based on device
- ACL based on interface
- ACL based on flow from ingress interface to egress interface
- ACL based on VLAN

Prerequisite

N/A

10.1.3 Configuring MAC ACL

Configure MAC ACL for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#access-list <i>acl-number</i> [name <i>acl-name</i>]</pre>	<p>Create an ACL, and enter ACL configuration mode.</p> <ul style="list-style-type: none"> • When the ACL number is between 1000 and 1999, this configuration enters basic IP ACL configuration mode. • When the ACL number is between 2000 and 2999, this configuration enters extended IP ACL configuration mode. • When the ACL number is between 3000 and 3999, this configuration enters MAC ACL configuration mode. • When the ACL number is between 5000 and 5999, this configuration enters User ACL configuration mode. • When the ACL number is between 6000 and 6999, this configuration enters IPv6 ACL configuration mode. • When the ACL number is between 7000 and 7999, this configuration enters advanced ACL configuration mode.
3	<pre>Raisecom(config-acl-ip-std)#rule [<i>rule-id</i>] { deny permit } { <i>source-ip-address</i> <i>source-ip-mask</i> any }</pre>	<p>(Optional) configure the matching rule for basic IP ACL.</p>
4	<pre>Raisecom(config-acl-ipv4-ext)#rule [<i>rule-id</i>] { deny permit } { <i>protocol-id</i> icmp igmp ip } { <i>source-ip-address</i> <i>source-ip-mask</i> any } { <i>destination-ip-address</i> <i>destination-ip-mask</i> any } [dscp <i>dscp-value</i>] [ttl <i>ttl-value</i>] [fragment] [icmp-type <i>icmp-type-value</i>] [precedence <i>precedence-value</i>] [tos <i>tos-value</i>]</pre>	<p>(Optional) configure the matching rule for extended IP ACL.</p>

Step	Command	Description
	<pre>Raisecom(config-acl-ipv4-advanced)#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-value] [range minimum source port maximum source port] [rst rst-value] [syn syn-value] [tos tos-value] [urg urg-value] [ttl ttl-value]</pre>	
5	<pre>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] [cos cos-value] [cvlan cvlanid] [inner-cos inner-cos]</pre>	(Optional) configure the matching rule for MAC ACL.
6	<pre>Raisecom(config-acl-udf)#rule [rule-id] { deny permit } { ipv4 layer2 } rule-string rule-mask offset</pre>	(Optional) configure the matching rule for User ACL.
7	<pre>Raisecom(config-acl-ipv6)#rule [rule-id] { deny permit } { protocol-id ipv6 icmpv6 } { source-ipv6-address/prefix any } { destination- ipv6-address/prefix any } [dscp dscp-value] [fragment] [flow-label flow label-value] Raisecom(config-acl-ipv6)#rule [rule-id] { deny permit } { tcp udp } { source-ipv6-address/prefix source-ip-mask any } { 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]</pre>	(Optional) configure the matching rule for MAP ACL.

Step	Command	Description
8	<pre> 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] [cos cos-value] [cvlan cvlanid] [inner-cos inner-cos] { 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] </pre>	(Optional) configure the matching rule for advanced ACL.

10.1.4 Configuring filter

Configure the filter for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#filter ingress access-list acl-number [statistics]</code>	Apply ACL on the interface.

10.1.5 Configuring ACL period

Configure the ACL period for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface- numbertime-range time-range-name hour minute seconds to hour minute seconds { weekday-list sun mon tue wed thu fri sat off-day working-day daily } [from hour minute seconds month- day-year] [to hour minute seconds month-day-year] to hour minute seconds month-day-year</code>	Create a period for applying ACL rules.

10.1.6 Configuring IP address list for SNMP access control

Configure the IP address list for SNMP access control for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#local-access access-list <i>acl-number</i>	Configure the IP address list for SNMP access control.

10.1.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show access-list [<i>acl-number</i>]	Show ACL configurations.
2	Raisecom#show acl resource { egress ingress } <i>interface-type interface-number</i>	Show resources used by ACL.
3	Raisecom#show filter interface	Show filter configurations.
	Raisecom#show filter interface <i>interface-type interface-number</i> [ingress]	
	Raisecom#show filter interface <i>interface-type interface-number</i> [ingress egress]	
4	Raisecom#show local-access access-list	Show SNMP information about server authentication.

10.1.8 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom(config)#clear filter statistics interface { <i>interface-type interface-number</i> vlan <i>vlan-id</i> } ingress [access-list <i>acl-number</i>]	Clear statistics on ACL filter configurations.

10.2 Port security MAC

10.2.1 Introduction

Port security MAC is used for the switching device at the user side on the edge of the network. 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

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 into 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 into sticky secure MAC addresses.
- When sticky learning is disabled, all sticky secure MAC addresses on an interface will be converted into dynamic secure MAC addresses.

Processing mode for violating secure MAC address

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, namely, 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.

10.2.2 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 secure MAC address, you can configure permitting specified users to access the interface, or permitting specified number of users to access from this interface only. However, when the number of users exceeds the limit, the accessed packets will be processed in accordance with secure MAC address violation policies.

Prerequisite

N/A

10.2.3 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	1

10.2.4 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 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 the port security MAC for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#switchport port-security</code>	Enable port security MAC.
4	<code>Raisecom(config- gigaethernet1/1/1)#switchport port-security maximum maximum</code>	(Optional) configure the maximum number of secure MAC addresses.
5	<code>Raisecom(config- gigaethernet1/1/1)#switchport port-security violation { protect restrict shutdown }</code>	(Optional) configure secure MAC violation mode.
6	<code>Raisecom(config- gigaethernet1/1/1)#no port- security shutdown Raisecom(config- gigaethernet1/1/1)#exit</code>	(Optional) restart the interface which is shut down due to violating the secure MAC address.
7	<code>Raisecom(config)#port-security recovery-time second</code>	(Optional) configure the restoration time of port security MAC.



Note

When secure MAC violation policy is in Shutdown mode, you can use this command to restart this interface which is shut down due to violating secure MAC address. When the interface is Up, the configured secure MAC violation mode will continue to be valid.

10.2.5 Configuring static secure MAC address

Configure the static secure MAC address for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#switchport port-security	Enable port security MAC.
4	Raisecom(config-gigaethernet1/1/1)#switchport port-security mac-address <i>mac-address vlan vlan-id</i>	Configure the static secure MAC address.

10.2.6 Configuring dynamic secure MAC address

Configure dynamic secure MAC address for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#port-security aging-time <i>period</i>	(Optional) configure the aging time of dynamic secure MAC address.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	Raisecom(config-gigaethernet1/1/1)#switchport port-security aging-type { absolute inactivity }	(Optional) configure the aging type of port security MAC addresses.
5	Raisecom(config-gigaethernet1/1/1)#switchport port-security	(Optional) enable port dynamic security MAC learning.
6	Raisecom(config-gigaethernet1/1/1)#switchport port-security trap enable	(Optional) enable port security MAC Trap.



Note

Use the **switchport port-security** command to enable port security MAC and dynamic secure MAC learning concurrently.

10.2.7 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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- portgigaethernet1/1/1)#switchport port-security</code>	Enable port security MAC.
4	<code>Raisecom(config- gigaethernet1/1/1)#switchport port- security mac-address sticky</code>	Enable sticky secure MAC learning.
5	<code>Raisecom(config- gigaethernet1/1/1)#switchport port- security mac-address sticky mac- <i>address vlan vlan-id</i></code>	(Optional) manually configure sticky secure MAC addresses.



Note

After sticky secure MAC address learning is enabled, the dynamic secure MAC address will be converted into the sticky secure MAC address; the manually configured sticky secure MAC address will take effect.

10.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show port-security [<i>interface-type interface-</i> <i>list</i>]</code>	Show configurations of port security MAC.
2	<code>Raisecom#show port-security mac-address [<i>interface-type</i> <i>interface-list</i>]</code>	Show configurations of port security MAC and secure MAC address learning.

10.2.9 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
<code>Raisecom(config- gigaethernet1/1/1)#clear port-security { all configured dynamic sticky }</code>	Clear a specified secure MAC address type on a specified interface.

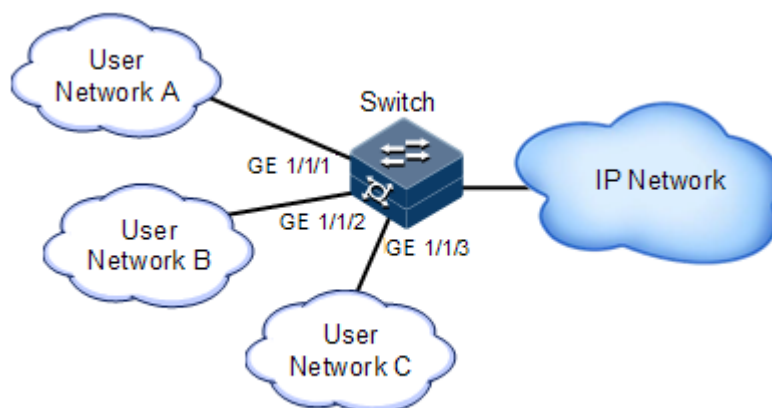
10.2.10 Example for configuring port security MAC

Networking requirements

As shown in Figure 10-1, 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 when 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; when 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 10-1 Port security MAC networking



Configuration steps

Step 1 Configure secure MAC address of 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)#exit
Raisecom(config)#port-security aging-time 10
```

Step 2 Configure the secure MAC address of GE 1/1/2.

```
Raisecom(config)#interface gig Ethernet 1/1/2
Raisecom(config-gig Ethernet1/1/2)#switchport port-security
Raisecom(config-gig Ethernet1/1/2)#switchport port-security maximum 2
Raisecom(config-gig Ethernet1/1/2)#switchport port-security mac-address
sticky
Raisecom(config-gig Ethernet1/1/2)#switchport port-security violation
restrict
Raisecom(config-gig Ethernet1/1/2)#exit
```

Step 3 Configure the secure MAC address of GE 1/1/3.

```
Raisecom(config)#interface gig Ethernet 1/1/3
Raisecom(config-gig Ethernet1/1/3)#switchport port-security
Raisecom(config-gig Ethernet1/1/3)#switchport port-security maximum 1
Raisecom(config-gig Ethernet1/1/3)#switchport port-security mac-address
sticky 0000.0000.0002 vlan 1
Raisecom(config-gig Ethernet1/1/3)#switchport port-security mac-address
sticky
Raisecom(config-gig Ethernet1/1/3)#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
-----
gig Ethernet1/1/1      Enable      3         1         1             0
protect      Enable      Absolute
gig Ethernet1/1/2      Enable      2         0         0             0
restrict     Disable     Absolute
gig Ethernet1/1/3      Enable      1         1         1             0
shutdown     Disable     Absolute
gig Ethernet1/1/4      Disable    1024      0         0             0
protect      Disable     Absolute
gig Ethernet1/1/5      Disable    1024      0         0             0
...
```

Use the **show port-security mac-address** command to show configurations and learning of secure MAC address.

```

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 --
  
```

10.3 Dynamic ARP inspection

10.3.1 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.

Figure 10-2 Principles of dynamic ARP inspection

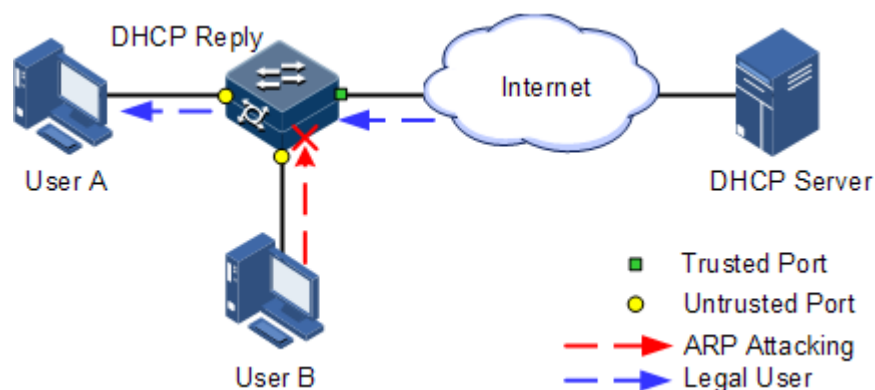


Figure 10-2 shows principles of dynamic ARP inspection. When the ISCOM3000G series switch receives an ARP packet, it compares the source IP address, source MAC address, interface number, and VLAN information of the ARP packet with the DHCP Snooping entry information. If matched, it indicates that it 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 ISCOM3000G series switch by sending a large number of ARP packets to the ISCOM3000G 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.

10.3.2 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.

10.3.3 Default configurations of dynamic ARP inspection

Default configurations of dynamic ARP inspection are as below.

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	Disable
Interface rate limiting on ARP packets	60 pps
Auto-recovery rate limiting on ARP packets	Disable
Auto-recovery time for rate limiting on ARP packets	30s

10.3.4 Configuring trusted interfaces of dynamic ARP inspection

Configure trusted interfaces of dynamic ARP inspection for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaehternet1/1/1)#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, namely, the interface does not trust the ARP packet.

10.3.5 Configuring static binding of dynamic ARP inspection

Configure static binding of dynamic ARP inspection for the ISCOM3000G 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.
3	Raisecom(config)#ip arp-inspection binding <i>ip-address</i> [<i>mac-address</i>] [<i>vlan vlan-id</i>] <i>interface-type interface-number</i>	Configure the static binding.

10.3.6 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 ISCOM3000G 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.

10.3.7 Configuring protection VLAN of dynamic ARP inspection

Configure protection VLAN of dynamic ARP inspection for the ISCOM3000G 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.
3	Raisecom(config)#ip arp-inspection vlan <i>vlan-list</i>	Configure protection VLAN of dynamic ARP inspection.

10.3.8 Configuring auto-recovery time for rate limiting on ARP packets

Configure the auto-recovery time for rate limiting on ARP packets for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip arp-rate-limit recover enable	Enable auto-recovery for rate limiting on ARP packets.
3	Raisecom(config)#ip arp-rate-limit recover time <i>time</i>	Configure the auto-recovery time for rate limiting on ARP packets.

10.3.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show ip arp-inspection</code>	Show configurations of dynamic ARP inspection.
2	<code>Raisecom#show ip arp-inspection binding [interface-type interface-number]</code>	Show information about the dynamic ARP inspection binding table.

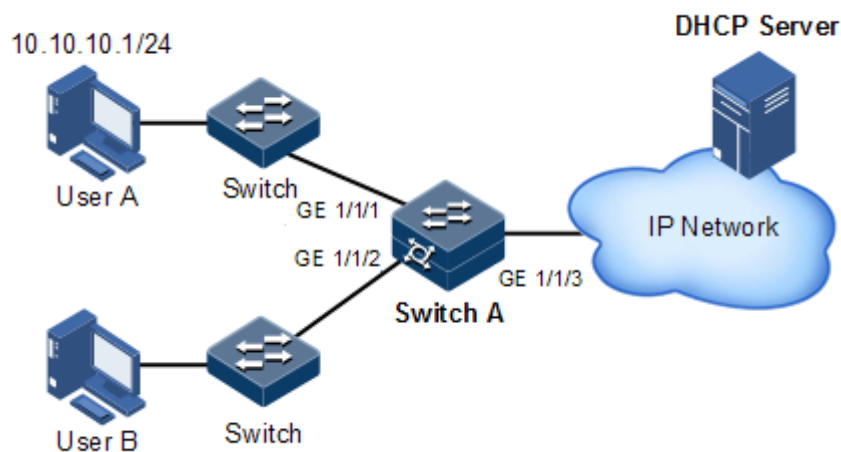
10.3.10 Example for configuring dynamic ARP inspection

Networking requirements

To prevent ARP attacks, configure dynamic ARP inspection on Switch A, as shown in Figure 10-3.

- 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 limit is configured to 20 pps and recovery time for rate limiting is configured to 15s.

Figure 10-3 Configuring dynamic ARP inspection



Configuration steps

Step 1 Configure GE 1/1/3 to the trusted interface.

```
Raisecom#config
Raisecom(config)#interface gigabitEthernet 1/1/3
Raisecom(config-gigabitEthernet1/1/3)#ip arp-inspection trust
Raisecom(config-gigabitEthernet1/1/3)#exit
```


Step 2 Configure static binding.

```
Raisecom(config)#ip arp-inspection static-config  
Raisecom(config)#ip arp-inspection binding 10.10.10.1 gig Ethernet 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 gig Ethernet 1/1/2  
Raisecom(config-gig Ethernet1/1/2)#ip arp-rate-limit rate 20  
Raisecom(config-gig Ethernet1/1/2)#ip arp-rate-limit enable  
Raisecom(config-gig Ethernet1/1/2)#exit
```

Step 5 Configure auto-recovery for rate limiting on ARP packets.

```
Raisecom(config)#ip arp-rate-limit recover time 15  
Raisecom(config)#ip arp-rate-limit recover enable
```

Checking results

Use the **show ip arp-inspection** command to show configurations of interface trust status static/dynamic ARP binding.

```
Raisecom#show ip arp-inspection  
Static Config ARP Inspection: Enable  
Static Config ARP Inspection: Enable  
DHCP Snooping ARP Inspection: Disable  
ARP Inspection Protect Vlan : 1-4094  
Bind Rule Num : 1  
Vlan Rule Num : 0  
Bind Acl Num : 1  
Vlan Acl Num : 0  
Remained Acl Num : 511  
  
Port Trust  
-----  
gig Ethernet1/1/1 no  
gig Ethernet1/1/2 no  
gig Ethernet1/1/3 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
Ip Address      Mac Address      VLAN   Port              Type
Inhw
-----
10.10.10.1      --              --     gigaethernet1/1/1  static
yes
Current Rules Num      : 1
History Max Rules Num : 1

```

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
arp rate limit auto recover      : enable
arp rate limit auto recover time : 15 second
Port                             Enable-Status   Rate(Num/Sec)   Overload
-----
--
gigaethernet1/1/1                Disabled        100              No
gigaethernet1/1/2                Enabled         20               No
gigaethernet1/1/3                Disabled        100              No
gigaethernet1/1/4                Disabled        100              No
gigaethernet1/1/5                Disabled        100              No
gigaethernet1/1/6                Disabled        100              No

```

10.4 RADIUS

10.4.1 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 Accounting-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.

10.4.2 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 ISCOM3000G series switch and network. The ISCOM3000G series switch can be used as agent of the RADIUS server, which authorizes user to access according to feedback from RADIUS.

Prerequisite

N/A

10.4.3 Default configurations of RADIUS

Default configurations of RADIUS are as below.

Function	Default value
RADIUS accounting	Disable
IP address of RADIUS server	0.0.0.0
Timeout of RADIUS server	3s
IP address of RADIUS accounting server	0.0.0.0
Port ID of RADIUS authentication server	1812
Port ID of RADIUS accounting server	1813
Shared key used for communication with RADIUS accounting server	N/A
Accounting failure processing policy	Online

Function	Default value
Period for sending update packet	0

10.4.4 Configuring RADIUS authentication


Configure RADIUS authentication for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#radius [backup] { ipv4-address ipv6-address } [auth-port port-id]	Assign the IP address and port ID for RADIUS authentication server. Configure the backup parameter to assign the backup RADIUS authentication server.
2	Raisecom#radius-key string Raisecom#radius-encrypt-key string	Configure the shared plaintext or ciphertext key for RADIUS authentication.
3	Raisecom#user login { local-radius local-user radius-local [server-no-response] radius-user local-tacacs tacacs-local [server-no-response] tacacs-user }	Configure users to perform login authentication through RADIUS.
4	Raisecom#radius nas-ip-address ip-address	Configure the NAS IP address of RADIUS authentication.
5	Raisecom#radius response-timeout time	Configure the timeout for response by the RADIUS authentication server.

10.4.5 Configuring RADIUS accounting

Configure RADIUS accounting for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#aaa accounting login enable	Enable RADIUS accounting.
2	Raisecom#radius [backup] accounting-server ip-address [account-port] [sourceip ip-address]	Assign IP address and UDP port ID for RADIUS accounting server. Configure the backup parameter to assign the backup RADIUS accounting server.
3	Raisecom#radius accounting-server key string Raisecom#radius accounting-server encrypt-key string	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.

Step	Command	Description
4	<code>Raisecom#radius accounting nas-ip-address ip-address</code>	Configure the NAS IP address of the RADIUS accounting server.
5	<code>Raisecom#aaa accounting fail { offline online }</code>	Configure the processing policy for accounting failure.
6	<code>Raisecom#aaa accounting update minute</code>	Configure the period for sending accounting update packets. If it is configured to 0, no Account-Update packet will be sent.  Note The RADIUS accounting server can record access time and operation for each user through Accounting-Start packets, Accounting-Update packets, and Accounting-End packets.

10.4.6 Checking configurations

Use the following commands to check configuration results.

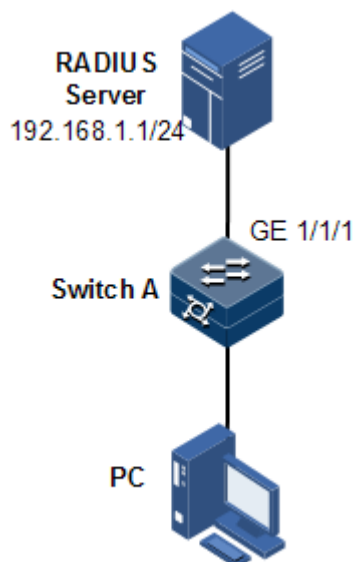
No.	Command	Description
1	<code>Raisecom#show radius-server</code>	Show configurations of the RADIUS server.
2	<code>Raisecom#show aaa</code>	Show configurations of RADIUS accounting.

10.4.7 Example for configuring RADIUS

Networking requirements

As shown in Figure 10-4, 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 update packets is 2 minutes. The user will be logged out if accounting fails.

Figure 10-4 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
Radius timeout          :3s
Authentication server IP:    192.168.1.1 port:1812
Backup authentication server IP: port:1812
Authentication server key:   I+NNa9u1uaix
Backup authentication server Key:  --
Accounting server IP:      192.168.1.1 port:1813
```

```
Backup accounting server IP:    port:1813
Accounting server key:         orMCKszv2X38
Backup Accounting server Key:   --

Accounting fail policy:        offline

Accounting
NAS IP address:
```

Use the **show aaa** command to show RADIUS accounting.

```
Raisecom#show aaa
Accounting login:              enable
Update interval(minute):      2
Accounting fail policy:        offline
```

10.5 TACACS+

10.5.1 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.

10.5.2 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 ISCOM3000G series switch and network. TACACS+ is safer and more reliable than RADIUS. The ISCOM3000G 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

10.5.3 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
Accounting failure processing policy	Online
Period for sending update packet	0

10.5.4 Configuring TACACS+ authentication

Configure TACACS+ authentication for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# tacacs-server [backup] <i>ip-address</i>	Assign the IP address and port ID for the TACACS+ authentication server. Configure the backup parameter to assign the backup TACACS+ authentication server.
2	Raisecom# tacacs-server [backup] <i>key string</i> Raisecom# tacacs-server [backup] encrypt-key <i>string</i>	Configure the shared plaintext or ciphertext key for TACACS+ authentication. Configure the backup parameter to assign the backup TACACS+ authentication server.
3	Raisecom# user login { local-tacacs tacacs- local [server-no- response] tacacs-user }	Configure users to perform login authentication through TACACS+.
4	Raisecom# enable login { local-tacacs tacacs- local [server-no- response] tacacs-user }	Configure the authentication mode for a user to enter privileged EXEC mode to TACACS+.

10.5.5 Configuring TACACS+ accounting

Configure TACACS+ accounting for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# aaa accounting login enable	Enable TACACS+ accounting.

Step	Command	Description
2	<code>Raisecom#tacacs [backup] accounting-server { ipv4- address ipv6-address }</code>	Assign the IP address and UDP port ID for the TACACS+ accounting server. Configure the backup parameter to assign the backup TACACS+ accounting server.
3	<code>Raisecom#tacacs-server key string Raisecom#tacacs [backup] accounting-server encrypt- key string</code>	Configure the shared plaintext or ciphertext key to communicate with the TACACS+ accounting server.
4	<code>Raisecom#aaa accounting fail { offline online }</code>	Configure the processing policy for accounting failure.
5	<code>Raisecom#aaa accounting update period</code>	Configure the period for sending accounting update packets. If it is configured to 0, no Account-Update packet will be sent.

10.5.6 Configuring TACACS+ authorization

Configure TACACS+ authorization for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#aaa command authorize{ enable disable }</code>	Enable/Disable TACACS+ command authorization.

10.5.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show tacacs-server</code>	Show configurations of the TACACS+ authentication server.
2	<code>Raisecom#show aaa</code>	Show configurations of TACACS+ accounting.

10.5.8 Maintenance

Maintain the ISCOM3000G series switch as below.

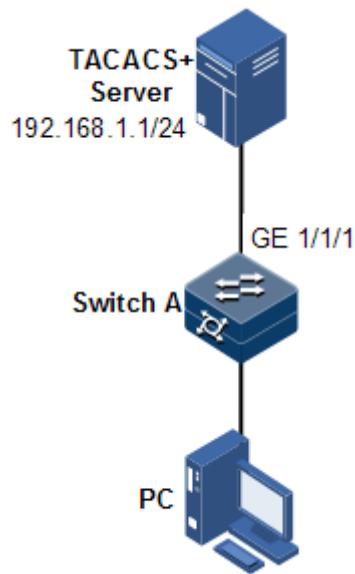
Command	Description
<code>Raisecom#clear tacacs statistics</code>	Clear TACACS+ statistics.

10.5.9 Example for configuring TACACS+

Networking requirements

As shown in Figure 10-5, configure TACACS+ authentication on Switch A to authenticate login user and control users from accessing the ISCOM3000G series switch.

Figure 10-5 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
Raisecom#enable login local-tacacs
```

Checking results

Use the **show tacacs-server** command to show TACACS+ configurations.

```
Raisecom#show tacacs-server
Server Address           : 192.168.1.1
Port: --
Backup Server Address    : --
Port: --
Server Shared Key        : oLMCKszV2X38
Backup Authentication server Shared Key: --
Accounting server Address : --
```

```
port: --
Backup Accounting server Address: --
Port: --
Accounting server Shared Key:      --
Backup Accounting server Shared Key:  --
Total Packet Sent                  : 0
Total Packet Recv                   : 0
Num of Error Packets                : 0
```

10.6 Storm control

10.6.1 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 ISCOM3000G 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.

Types of storm control

Storm controls is performed in the following forms:

- Ratio (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 ISCOM3000G series switch supports BPS and PPS storm control.

10.6.2 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

10.6.3 Default configurations of storm control

Default configurations of storm control are as below.

Function	Default value
Broadcast storm control	Enable
Storm control enhancement	Disable
Multicast and unknown unicast storm control	Disable
Bytes of frame gap and preamble	20 bytes
Storm control mode	pps
Number of allowed storm packets per second	1024 pps
DLF packet forwarding	Enable
Action for storm control on the interface	Discarding packets
Restoration period of the interface	5min
Storm control Trap	Disable

10.6.4 Configuring storm control



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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#storm-control detection enable</code>	Enable storm control enhancement.
3	<code>Raisecom(config)#interface interface- type interface-number Raisecom(config)#vlan vlan-id</code>	Enter physical layer interface configuration mode or VLAN configuration mode.
4	<code>Raisecom(config- gigaethernet1/1/1)#storm-control { broadcast unknown-multicast dlf all } { bps value [burst value] pps value } Raisecom(config-vlan)#storm-control { broadcast unknown-multicast dlf all } { bps value [burst value] pps value }</code>	Enable storm control on the interface or VLAN, and configure the storm control threshold.
5	<code>Raisecom(config- gigaethernet1/1/1)#storm-control action { shutdown drop }</code>	Configure the action for storm control on the interface.
6	<code>Raisecom(config- gigaethernet1/1/1)#storm-control interval interval</code>	Configure the restoration period of the shutdown interface.
7	<code>Raisecom(config- gigaethernet1/1/1)#storm-control trap enable</code>	Enable storm control Trap.

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 ISCOM3000G 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.
- To configure storm control in the VLAN, you must disable storm control on the interface; otherwise, the configuration will not take effect.
- To configure storm control on the interface, you must disable storm control in the VLAN; otherwise, the configuration will not take effect.

10.6.5 Configuring DLF packet forwarding

Configure DLF packet forwarding for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#dlf- forwarding enable</code>	Enable DLF packet forwarding on an interface.

10.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show storm-control interface [<i>interface-type interface-number</i>]	Show configurations of storm control.
2	Raisecom# show dlf-forwarding	Show DLF packet forwarding status.
3	Raisecom# show storm-control status	Show storm control status.
4	Raisecom# show storm-control vlan <i>vlan-list</i>	Show storm control status in the VLAN.

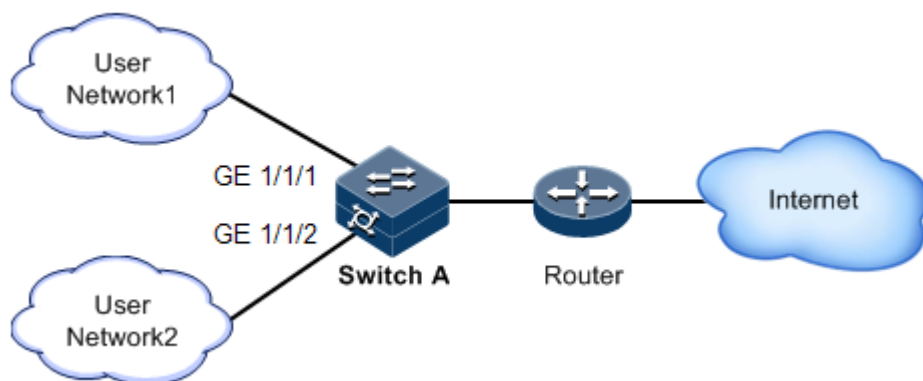
10.6.7 Example for configuring storm control

Networking requirements

As shown in Figure 10-6, 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 10-6 Storm control networking



Configuration steps

Enable storm control, and configure the threshold for storm control.

```
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#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
```

Checking results

Use the **show storm-control** command to show configurations of storm control.

```
Raisecom#show storm-control interface gigaethernet 1/1/1
Threshold: 0 kbps
Interface      Packet-Type      Pps(pps)          Bps(kbps)          Cbs(kByte)
-----
GE1/1/1       Broadcast         --                640                4
              Multicast         --                0                  0
              Dlf              --                0                  0
```

10.7 802.1x

10.7.1 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.

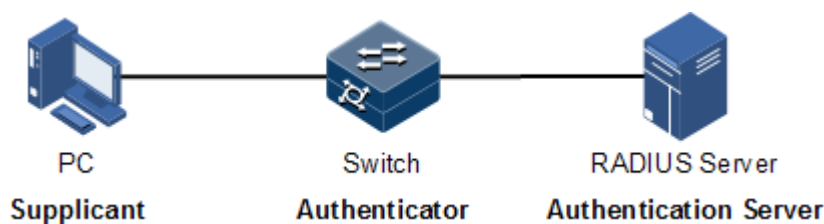
It is used to authenticate and control access devices at the physical layer of the network device. It defines a point-to-point connection mode between the device interface and user devices. User devices, connected to the interface, can access resources in the LAN if they are authenticated. Otherwise, they cannot access resources in the LAN through the switch.

802.1x structure

As shown in Figure 10-7, 802.1x authentication uses C/S 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 10-7 802.1x 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, namely, users are disallowed to be authenticated.

802.1x authentication procedure

The 802.1x system supports finishing authentication procedure between 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 protocol packet to be transmitted to the authentication server through a complex network. This procedure is call EAP relay.

Both the authenticator and the suppliant can initiate the 802.1x authentication procedure. This guide takes the suppliant for an 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 supplicant, asking the user name of the supplicant.
- 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 protocol packet and sends the RADIUS protocol 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.
- Step 7 The authentication server compares with 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

During 802.1x authentication, the following 5 timers are involved:

- Reauth-period: re-authorization timer. After the period is exceeded, the ISCOM3000G series switch re-initiates authorization.
- Quiet-period: quiet timer. When user authorization fails, the ISCOM3000G series switch needs to keep quiet for a period. After the period is exceeded, the ISCOM3000G series switch re-initiates authorization. During the quiet time, the ISCOM3000G series switch does not process authorization packets.
- Tx-period: transmission timeout timer. When the ISCOM3000G series switch sends a Request/Identity packet to users, the ISCOM3000G series switch will initiate the timer. If users do not send an authorization response packet during the tx-period, the ISCOM3000G series switch will re-send an authorization request packet. The ISCOM3000G series switch sends this packet three times in total.
- Supp-timeout: Supplicant authorization timeout timer. When the ISCOM3000G series switch sends a Request/Challenge packet to users, the ISCOM3000G series switch will initiate supp-timeout timer. If users do not send an authorization response packet during the supp-timeout, the ISCOM3000G series switch will re-send the Request/Challenge packet. The ISCOM3000G series switch sends this packet twice in total.
- Server-timeout: Authentication server timeout timer. The timer defines the total timeout period of sessions between authorizer and the RADIUS server. When the configured time is exceeded, the authenticator will end the session with the RADIUS server and start a new authorization process.

10.7.2 Preparing for configurations

Scenario

To realize access authentication on LAN users and ensure access user security, you need to configure 802.1x authentication on the ISCOM3000G 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.

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 ISCOM3000G series switch can ping through the RADIUS server successfully.

10.7.3 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
Re-authentication	Disable
802.1x re-authentication timer	3600s
802.1x quiet timer	60s
transmission timeout timer	30s
Supplicant authorization timeout timer	30s

10.7.4 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#dot1x enable	Enable global 802.1x.
3	Raisecom(config)#dot1x authentication-method { chap pap eap }	Configure global authentication mode.
4	Raisecom(config)#dot1x auth-mode { radius local tacacs+ }	Configure the mode of 802.1x authentication.
5	Raisecom(config)#dot1x free-ip ip-address [ip-mask mask-length]	Configure the IP address segment available for 802.1x terminal users who fail to be authenticated or exit authentication.
6	Raisecom(config)#interface interface-type interface-number	Enter physical layer interface configuration mode.
7	Raisecom(config-gigaethernet1/1/1)#dot1x enable	Enable interface 802.1x.
8	Raisecom(config-gigaethernet1/1/1)#dot1x auth-control { auto authorized-force unauthorized-force }	Configure access control mode on the interface.
9	Raisecom(config-gigaethernet1/1/1)#dot1x auth-method { portbased macbased }	Configure access control mode of 802.1x authentication on the interface.
10	Raisecom(config-gigaethernet1/1/1)#dot1x keepalive { enable disable }	Enable or disable 802.1x handshake on the interface.
11	Raisecom(config-gigaethernet1/1/1)#dot1x max-user user-number	Configure the maximum number of users allowed to be authenticated by the 802.1x 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.

10.7.5 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#dot1x reauthentication enable	Enable 802.1x re-authentication.

10.7.6 Configuring 802.1x timers

Configure 802.1x timers for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#dot1x timer reauth-period <i>reauth-period</i>	Configure the time of the re-authentication timer.
4	Raisecom(config-gigaethernet1/1/1)#dot1x timer quiet-period <i>second</i>	Configure the time of the quiet timer.
5	Raisecom(config-gigaethernet1/1/1)#dot1x timer supp-timeout <i>supp-timeout</i>	Configure the time of the supplicant authorization timeout timer.
6	Raisecom(config-gigaethernet1/1/1)#dot1x timer server-timeout <i>server-timeout</i>	Configure the time of the authentication server timeout timer.
7	Raisecom(config-gigaethernet1/1/1)#dot1x timer keepalive-period <i>second</i>	Configure the period for retransmitting KeepAlive packets by interface 802.1x.
8	Raisecom(config-gigaethernet1/1/1)#dot1x timer tx-period <i>second</i>	Configure the timeout timer of the Request/Identity request packet.

10.7.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show dot1x <i>interface-type interface-list</i>	Show 802.1x configurations on the interface.
2	Raisecom#show dot1x <i>interface-type interface-list statistics</i>	Show 802.1x statistics on the interface.

No.	Command	Description
3	Raisecom# show dot1x interface-type interface-list 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.

10.7.8 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom(config)# clear dot1x interface-type interface-list statistics	Clear interface 802.1x statistics.

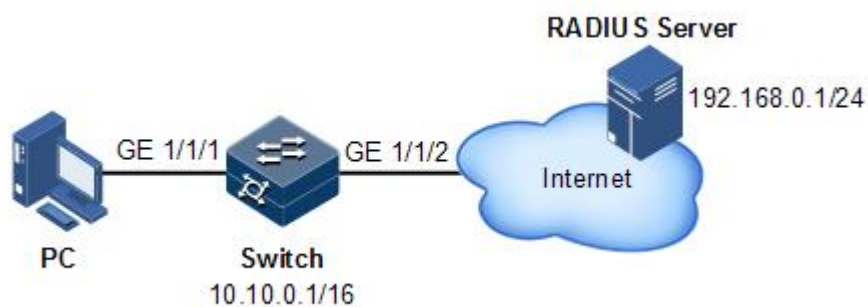
10.7.9 Example for configuring 802.1x

Networking requirements

As shown in Figure 10-8, 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.

Figure 10-8 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
```

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
Port gigaethernet1/1/1
-----
802.1X Port Admin State: enable
PAE: Authenticator
PortMethod: Portbased
```

```
PortControl: Auto
ReAuthentication: enable
KeepAlive: enable
QuietPeriod: 60(s)
ServerTimeout: 100(s)
SuppTimeout: 30(s)
ReAuthPeriod: 600(s)
TxPeriod: 30(s)
KeepalivePeriod: 60(s)
```

10.8 IP Source Guard

10.8.1 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

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.

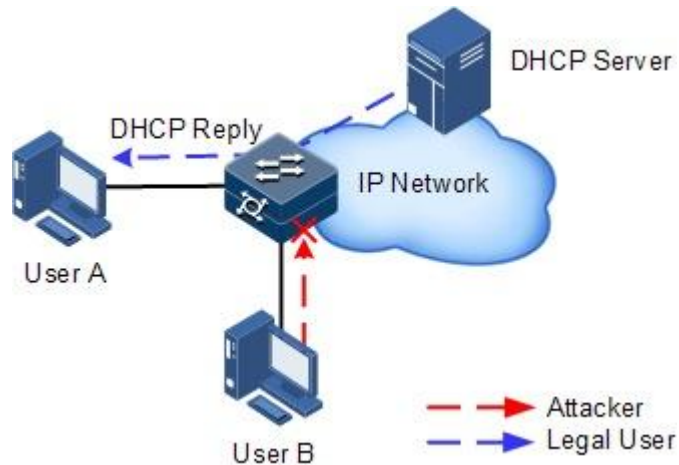
Principles of IP Source Guard

Principles of IP Source Guard are to create an IP source binding table within the ISCOM3000G series switch. The IP source binding table is taken as the basis for each interface to test received data packets. Figure 10-9 shows principles of IP Source Guard.

- If the received IP packets meet the relation 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 10-9 Principles of IP Source Guard



Before forwarding IP packets, the ISCOM3000G 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.

10.8.2 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.

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.

10.8.3 Default configurations of IP Source Guard

Default configurations of IP Source Guard are as below.

Function	Default value
IP Source Guide static binding	Disable
IP Source Guide dynamic binding	Disable
Interface trust status	Untrusted

10.8.4 Configuring interface trust status of IP Source Guard

Configure interface trust status of IP Source Guard for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)# interface interface-type interface-number	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#ip verify source trust	(Optional) configure the interface to a trusted interface. Use the no ip verify source trust command to configure the interface to 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.

10.8.5 Configuring IP Source Guide binding

Configuring IP Source Guide static binding

Configure IP Source Guide static binding for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip verify source	Enable IP Source Guide static binding.
3	Raisecom(config)#ip source binding ip-address [mac- address] [vlan vlan-id] interface-type interface-number	Configure static binding.



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 static binding is deleted, the system will recover the covered dynamic binding automatically.

Configuring IP Source Guide dynamic binding

Configure IP Source Guide dynamic binding for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip verify source dhcp-snooping</code>	Enable IP Source Guide dynamic binding.



- 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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip verify source dhcp-snooping</code>	Enable IP Source Guide dynamic binding.
3	<code>Raisecom(config)#ip source binding dhcp-snooping static</code>	Translate the dynamic binding to the static binding.
4	<code>Raisecom(config)#ip source binding auto-update</code>	(Optional) enable auto-translation. After it is enabled, dynamic binding entries learned through DHCP Snooping are directly translated into static binding entries.

10.8.6 Configuring priority and rate limit of IP packets

Configure the priority and rate limit of IP packets for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip verify source [ip-address ip-mask]set-cos cos-value [rate-limit rate-value]</code>	Configure the priority and rate limit of IP packets.

10.8.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show ip verify source</code>	Show global binding status and interface trusted status.
2	<code>Raisecom#show ip source binding [interface-type interface-number]</code>	Show configurations of IP Source Guard binding, interface trusted status, and binding table.
3	<code>Raisecom#show ip verify source set-cos</code>	Show priority configurations.

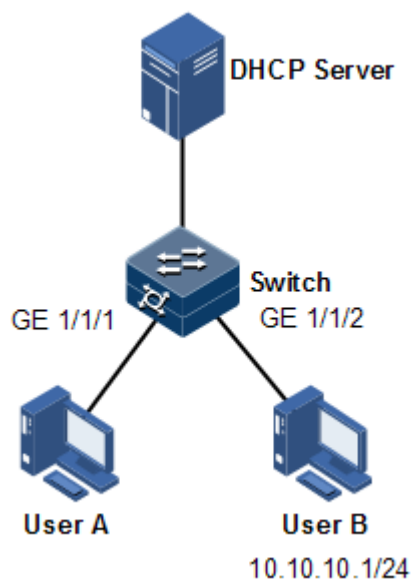
10.8.8 Example for configuring IP Source Guard

Networking requirements

As shown in Figure 10-10, to prevent IP address embezzlement, 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.

Figure 10-10 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-snooping
```

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                               Mac Address      VLAN   Port
Type          Inhw
-----
10.10.10.1    --              --       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-Snooping 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
.....
```

10.9 PPPoE+

10.9.1 Introduction

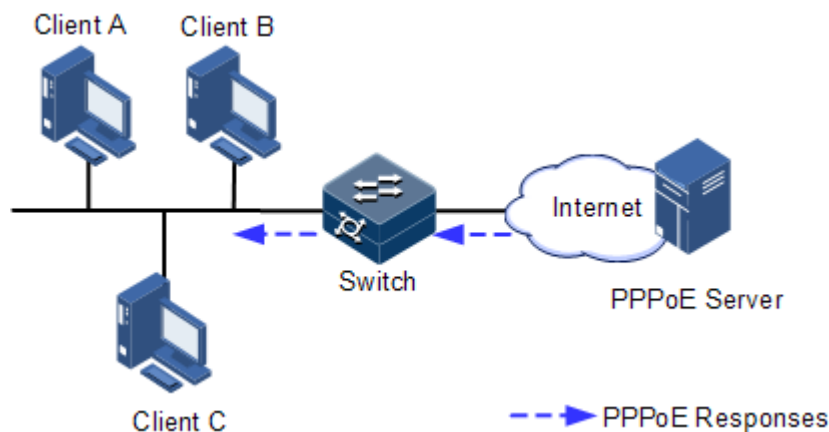
PPPoE Intermediate Agent (PPPoE+) is used to process authentication packets. PPPoE+ adds more information about access devices into the authentication packet to bind account and access device so that the account is not shared and stolen, and the carrier's and users' interests are protected. This provides 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.

The PPPoE protocol adopts C/S mode, as shown in Figure 10-11. 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 10-11 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 judges 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.

10.9.2 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

10.9.3 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.

10.9.4 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; namely, 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#pppoeagent enable	Enable global PPPoE+.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
4	Raisecom(config- gigaethernet1/1/1)#pppoeagent enable	Enable interface 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#pppoeagent trust	Configure the PPPoE trusted interface.



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.

10.9.5 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 number, 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 number, 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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#pppoeagent circuit-id mode { onu switch }</code>	Configure the padding mode of the Circuit ID.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
4	<code>Raisecom(config- gigaethernet1/1/1)#pppoeagent circuit-id string</code>	(Optional) configure the Circuit ID to the customized string.

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.

Configure the attached string of the Circuit ID for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#pppoeagent circuit-id attach-string string	(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.

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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface interface-type interface- number	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#pppoeagent remote-id { client-mac switch-mac }	(Optional) configure PPPoE+ Remote ID to be padded with the MAC address.
4	Raisecom(config- gigaethernet1/1/1)#pppoeagent remote-id format { ascii binary }	(Optional) configure the padding modes of the PPPoE+ Remote ID.

Configuring Tag overriding

Tags of some fields may be forged by the client due to some reasons, so the original Tags need to be overridden. After Tag overriding is enabled, these Tags will be overridden if the PPPoE packets contain Tags of these fields; if not, Tags will be added to these PPPoE packets.

Configure Tag overriding for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface interface-type interface-number	Enter physical layer interface configuration mode.
3	Raisecom(config- gigaethernet1/1/1)#pppoeagent vendor-specific-tag overwrite enable	Enable Tag overriding.

10.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show pppoeagent	Show PPPoE+ configurations.
2	Raisecom# show pppoeagent statistic	Show PPPoE+ statistics.

10.9.7 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom(config)# clear pppoeagent statistic	Clear PPPoE+ statistics.

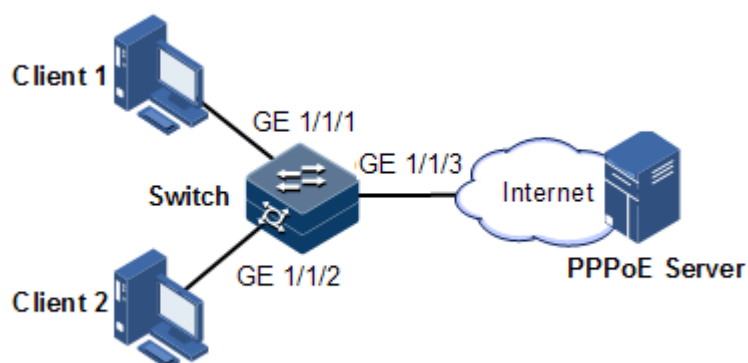
10.9.8 Example for configuring PPPoE+

Networking requirements

As shown in Figure 10-12, 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 10-12 PPPoE+ networking



Configuration steps

Step 1 Configure GE 1/1/3 as the trusted interface.

```
Raisecom#config  
Raisecom(config)#interface gigabitEthernet 1/1/3  
Raisecom(config-gigabitEthernet1/1/1)#pppoeagent trust  
Raisecom(config-gigabitEthernet1/1/1)#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 gigabitEthernet 1/1/1  
Raisecom(config-gigabitEthernet1/1/1)#pppoeagent circuit-id user01  
Raisecom(config-gigabitEthernet1/1/1)#exit  
Raisecom(config)#interface gigabitEthernet1/1/2  
Raisecom(config-gigabitEthernet1/1/2)#pppoeagent remote-id client-mac  
Raisecom(config-gigabitEthernet1/1/2)#pppoeagent remote-id format ascii  
Raisecom(config-gigabitEthernet1/1/2)#exit
```

Step 3 Enable Tag overwriting on GE 1/1/1 and GE 1/1/2.

```
Raisecom(config)#interface gigabitEthernet 1/1/1  
Raisecom(config-gigabitEthernet1/1/1)#pppoeagent vendor-specific-tag  
overwrite enable  
Raisecom(config-gigabitEthernet1/1/1)#exit  
Raisecom(config)#interface gigabitEthernet1/1/2  
Raisecom(config-gigabitEthernet1/1/2)#pppoeagent vendor-specific-tag  
overwrite enable  
Raisecom(config-gigabitEthernet1/1/2)#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 gigabitEthernet 1/1/1  
Raisecom(config-gigabitEthernet1/1/1)#pppoeagent enable  
Raisecom(config-gigabitEthernet1/1/1)#exit  
Raisecom(config)#interface gigabitEthernet 1/1/2  
Raisecom(config-gigabitEthernet1/1/2)#pppoeagent enable
```

Checking results

Use the **show pppoeagent** command to show PPPoE+ configurations.

```

Raisecom#show pppoeagent
Mac-format: hhhhhhhhhhhh
Global PPPoE+ status: enable
Attach-string: raisecom
Circuit ID padding mode: switch
      Port          State  Overwrite  Remote-ID  Format-rules
Circuit-ID
-----
-----
gigaethernet1/1/1      enable  enable    switch-mac  binary
user01
gigaethernet1/1/2      enable  enable    client-mac
ASCII %default%
gigaethernet1/1/3      trust   disable   switch-mac
binary %default%
gigaethernet1/1/4      disable disable   switch-mac
binary %default%
gigaethernet1/1/5      disable disable   switch-mac
binary %default%
gigaethernet1/1/6      disable disable   switch-mac
binary %default%
  
```

10.10 Configuring URPF

10.10.1 Preparing for configurations

Scenario

You can enable Unicast Reverse Path Forwarding (URPF) on the routing interface to avoid network attacks based on source address spoofing. After it is enabled, the interface will check legality of the source address of the packet upon receiving the packet. If the packet passes the legality check, the interface will match it with the forwarding table and then forward it, otherwise, the interface will discard it.

Prerequisite

N/A

10.10.2 Configuring URPF

Configure URPF for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode.

Step	Command	Description
3	<code>Raisecom(config-gigaethernet1/1/1)#ip urpf { loose strict } [allow-default-route]</code>	Enable URPF on the interface. By default, it is disabled.

10.11 Configuring CPU protection

10.11.1 Preparing for configurations

Scenario

When the ISCOM3000G 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 rate of packets which enters the CPU.

Prerequisite

N/A

10.11.2 Configuring global CPU CAR

Configure global CPU CAR for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#cpu-protect car { arp dhcp global icmp igmp bpdu } kbps cir cir cbs cbs</code>	Configure the protocol type, CIR, and CBS of global CPU packet protection.

10.11.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show cpu-protect car statistics</code>	Show CPU CAR statistics.

10.11.4 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
<code>Raisecom(config)# clear cpu-protect car { arp dhcp global icmp igmp } statistics</code>	Show CPU CAR statistics.

10.12 Configuring anti-ARP attack

10.12.1 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 ISCOM3000G series switch, they will cause the following harms:

- The ISCOM3000G series switch sends excessive ARP request packets to the destination network segment, so this network segment is overburdened.
- The ISCOM3000G series switch repeatedly resolve destination IP addresses, so the CPU is overburdened.

To prevent these harms due to attacks on IP packets, the ISCOM3000G series switch supports anti-ARP attack.

Prerequisite

N/A

10.12.2 Configuring ARP

Configure ARP for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface vlan <i>vlan-id</i></code>	Enter VLAN interface configuration mode.
3	<code>Raisecom(config-vlan1)#arp learning strict enable</code>	Enable the device to learn ARP entries requested by itself.
4	<code>Raisecom(config-vlan1)#arp check-destination-ip enable</code>	Enable the check of ARP destination IP address.
5	<code>Raisecom(config-vlan1)#arp filter { gratuitous mac-illegal thafilled-request }</code>	Configure ARP filtering.
6	<code>Raisecom(config-vlan1)#arp anti-attack entry-check { fixed-all fixed-mac send-ack }</code>	Configure the fixing of ARP entries.

Step	Command	Description
7	Raisecom(config-vlan1)# ip arp-rate-limit rate rate value	Configure rate limiting of ARP.

10.12.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show arp	Show ARP information.
2	Raisecom# show ip arp filter	Show information about ARP filtering.

11 Reliability

This chapter describes principles and configuration procedures of reliability, and provides related configuration examples, including the following sections:

- Link aggregation
- Link-state tracking
- Interface backup
- Configuring VRRP
- mLACP

11.1 Link aggregation

11.1.1 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 the link between two devices, link aggregation helps gain higher bandwidth without upgrading hardware.

The ISCOM3000G series switch supports the following two link aggregation modes:

- 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 number, 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 agree. The operation key is a configuration combination automatically generated based on

configurations of the interface, such as the rate, duplex mode, and Up/Down status. In a LAG, interfaces in the Selected state share the identical operation key.

11.1.2 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.

11.1.3 Configuring manual link aggregation

Configure manual link aggregation for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface port-channel channel-number</code>	Enter LAG configuration mode.
3	<code>Raisecom(config-port-channel1)#mode manual</code>	Configure manual link aggregation mode.
4	<code>Raisecom(config-port-channel1){ max-active min-active } links value threshold</code>	(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.

Step	Command	Description
5	<code>Raisecom(config-port-channel)#load-sharing mode { dst-ip dst-mac src-dst-ip src-dst-mac src-ip src-mac }</code>	(Optional) configure a load balancing mode for link aggregation. By default, the load balancing algorithm is configured to <code>sxordmac</code> . In this mode, select a forwarding interface based on the OR result of the source and destination MAC addresses.
6	<code>Raisecom(config-port-channel)#exit</code>	Return to global configuration mode.

11.1.4 Configuring static LACP link aggregation

Configure static LACP link aggregation for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#lacc system-priority system-priority</code>	(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.
3	<code>Raisecom(config)#lacc timeout { fast slow }</code>	(Optional) configure LACP timeout mode. By default, it is slow.
4	<code>Raisecom(config)#interface port-channel channel-number</code>	Enter LAG configuration mode.
5	<code>Raisecom(config-port-channel)#mode lacp</code>	Configure the working mode of the LAG to static LACP LAG.
6	<code>Raisecom(config-port-channel)#{ max-active min-active } links value threshold</code>	(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.
7	<code>Raisecom(config-port-channel)#exit</code>	Return to global configuration mode.
8	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter Layer 2 or Layer 3 physical interface configuration mode.
9	<code>Raisecom(config-gigaethernet1/1/1)#port-channel channel-number</code>	Add the Layer 2 interface to the LAG.

Step	Command	Description
10	<code>Raisecom(config-port-channel)#exit</code>	Return to global configuration mode.



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 rate, interface highest LACP priority, and interface minimum ID. The interface is in active status by default, the interface with identical rate, identical peer and identical device operation key is also in active status; other interfaces are in standby status.


11.1.5 Configuring manual master/slave link aggregation

Configure manual master/slave link aggregation for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface port-channel channel-number</code>	Enter LAG configuration mode.
3	<code>Raisecom(config-port-channel)#mode manual backup</code>	Configure the working mode of the LAG to manual backup LAG.
4	<code>Raisecom(config-port-channel)#master-port interface-type interface-number</code>	Configure the active interface of the LAG.
5	<code>Raisecom(config-port-channel)#restore-mode { non-revertive revertive [restore-delay second] }</code>	Configure the restoration mode and wait-to-restore time of the LAG. By default, the restoration mode is non-revertive.
6	<code>Raisecom(config-port-channel)#exit</code>	Return to global configuration mode.
7	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
8	<code>Raisecom(config-gigaethernet1/1/1)#port-channel channel-number</code>	Add member interfaces to the LAG.
9	<code>Raisecom(config-gigaethernet1/1/1)#exit</code>	Return to global configuration mode.

11.1.6 Checking configurations

Use the following commands to check configuration results.

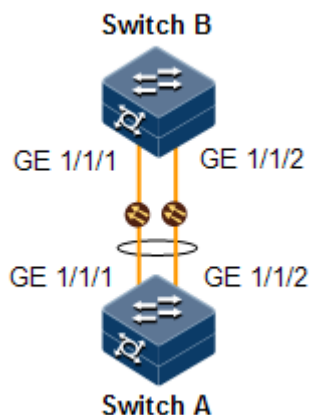
No.	Command	Description
1	<code>Raisecom#show lacp internal</code>	Show local system LACP interface status, flag, interface priority, administration key, operation key, and interface status machine status.
2	<code>Raisecom#show lacp neighbor</code>	Show information about LACP neighbors, including Tag, interface priority, device ID, Age, operation key value, interface ID, and interface status machine status.
3	<code>Raisecom#show lacp statistics</code>	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	<code>Raisecom#show lacp sys-id</code>	Show global LACP status of the local system, device ID, including system LACP priority and system MAC address.
5	<code>Raisecom#show port-channel</code>	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.

11.1.7 Example for configuring static LACP link aggregation

Networking requirements

As shown in Figure 11-1, 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 and GE 1/1/2 into one LAG; wherein GE 1/1/1 is used as the active interface and GE 1/1/2 as the standby interface.

Figure 11-1 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#name SwitchA
SwitchA#config
SwitchA(config)#larp system-priority 1000
SwitchA(config)#interface port-channel 1
SwitchA(config-port-channel1)#mode lacp
SwitchA(config-port-channel1)#max-active links 1
SwitchA(config-port-channel1)#exit
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigabitethernet1/1/1)#portswitch
SwitchA(config-gigaethernet1/1/1)#port-channel 1
SwitchA(config-gigaethernet1/1/1)#larp port-priority 1000
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigabitethernet1/1/2)#portswitch
SwitchA(config-gigaethernet1/1/2)#port-channel 1
SwitchA(config-gigaethernet1/1/2)#exit
```

Step 2 Create static LACP link aggregation on Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#interface port-channel 1
SwitchB(config-portchannel1)#mode lacp-static
SwitchB(config-portchannel1)#exit
SwitchB(config)#interface gigaethernet 1/1/1
SwitchA(config-gigabitethernet1/1/1)#portswitch
SwitchB(config-gigaethernet1/1/1)#port-channel 1
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet 1/1/2
SwitchA(config-gigabitethernet1/1/2)#portswitch
SwitchB(config-gigaethernet1/1/2)#port-channel 1
SwitchB(config-gigaethernet1/1/2)#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         : 1
UpLinks   : 0                    Priority-Preemptive: Disable
Member Port: gigaethernet1/1/1 gigaethernet1/1/2
```

Efficient Port:

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  Down      SA     1000           1          1
0x45
gigaethernet1/1/2  Down      SA     32768          1          1
0x45
```

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.

11.2 Link-state tracking

11.2.1 Introduction

Link-state tracking is used to provide port 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, faults of uplink devices can be informed to the downlink devices to trigger switching. Link-state tracking can be used to prevent traffic loss when the uplink fault fails to be sensed by the downstream device.

When all uplink interfaces fail, down link interfaces are configured to Down status. When at least one uplink interface recovers, downlink interfaces will recover to Up status. Therefore, faults of uplink devices can be informed to the downstream devices immediately. Uplink interfaces are not influenced when downlink interfaces fail.

11.2.2 Preparing for configurations

Scenario

When the uplink of an intermediate device fails, traffic will fail to be switched to the standby link and traffic will be interrupted if the uplink fails to notify the downstream device in time.

Link-state tracking can be used to add downlink interfaces and uplink interfaces of the intermediate device to a link-state group and monitor uplink interfaces. When all uplink

interfaces fails, faults of uplink devices can be sent to the downstream devices to trigger switching.

Prerequisite

N/A

11.2.3 Default configurations of link-state tracking

Default configurations of link-state tracking are as below.

Function	Default value
Link-state group	N/A

11.2.4 Configuring link-state tracking



Note

Link-state tracking supports the physical interface or LAG interface.

Configure link-state tracking for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#link-state-tracking group group-number</code>	Create a link-state group, and enable link-state tracking.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
4	<code>Raisecom(config-gigaethernet1/1/1)#link-state-tracking group group-number { downstream upstream }</code>	Configure the link-state group of the interface and interface type. One interface can belong to only one link-state group and be configured as an either uplink or downlink interface.



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 { downstream | upstream }** command to disable link-state tracking, the link-state group without interfaces will be deleted.
- In physical layer interface configuration mode, use the **no link-state-tracking group group-number { downstream | upstream }** command to delete an interface.

11.2.5 Configuring action taken by link-state group

Configure the action taken by the link-state group for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#link-state-tracking group group-number action { block-vlan vlan-id delete-vlan vlan-id flush-erps rind-id modify-pvid vlan-id suspend-vlan vlan-id }</code>	Configure the action taken by the link-state group for the fault.

11.2.6 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	<code>Raisecom#show link-state-tracking group group-number</code>	Show configurations and status of the link-state group.

11.3 Interface backup

11.3.1 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 links. 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.

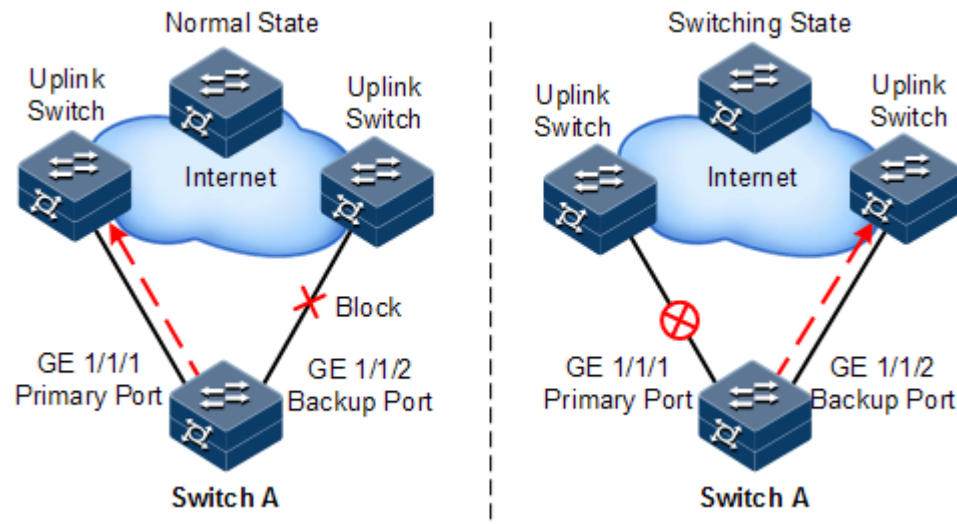
Principles of interface backup

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.

In the interface backup group, when an interface is in Up status, the other interface is in Standby status. At any time, only one interface is in Up status. When the Up interface fails, the Standby interface is switched to the Up status.

Figure 11-2 Principles of interface backup



As shown in Figure 11-2, 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:

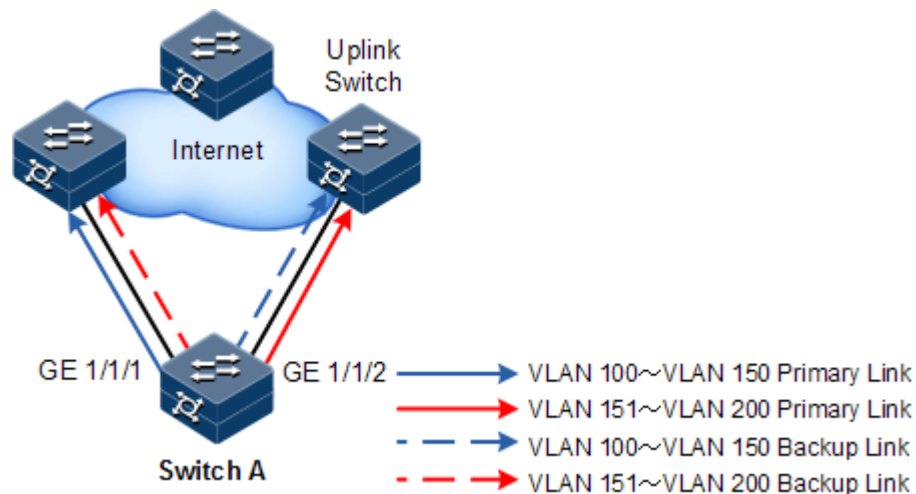
- Under normal conditions, GE 1/1/1 is the primary interface while GE 1/1/2 is the backup interface. GE 1/1/1 and the uplink device forward packet while GE 1/1/2 and the uplink device do not forward packets.
- When the link between GE 1/1/1 and its uplink device fails, the backup GE 1/1/2 and its uplink 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 11-3.

Figure 11-3 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 Up 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 share service load in different VLANs without depending on configurations of uplink switches, thus facilitating users' operation.

11.3.2 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

11.3.3 Default configurations of interface backup

Default configurations of interface backup are as below.

Function	Default value
Interface backup group	N/A
Restore-delay	15s
Restoration mode	Revertive mode

11.3.4 Configuring basic functions of interface backup

Configure basic functions of interface backup for the ISCOM3000G 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 <i>interface-type primary-interface-number</i>	Enter physical layer interface configuration mode or LAG configuration mode.
3	Raisecom(config-tengigabitethernet1/1/1)#port backup <i>interface-type backup-interface-number vlanlist vlan-list</i> Raisecom(config-tengigabitethernet1/1/1)#port backup <i>interface-type backup-interface-number [vlanlist vlan-list]</i>	Configure the interface backup group. In the VLAN list, configure the interface <i>backup-interface-number</i> to the backup interface and configure the interface <i>primary-interface-number</i> to the primary interface. If no VLAN list is specified, the VLAN ranges from 1 to 4094.
4	Raisecom(config-tengigabitethernet1/1/1)#port backup fault-detect lldp	(Optional) configure LLDP fault detection.
5	Raisecom(config-tengigabitethernet1/1/1)#port backup restore-mode { revertive non-revertive }	(Optional) configure restoration mode.



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.

11.3.5 (Optional) configuring FS on interfaces



Caution

- After FS is successfully configured, the primary/backup link will be switched; namely, 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 number 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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter physical layer interface configuration mode or LAG configuration mode.
3	<code>Raisecom(config- tengigabitethernet1/1/1)#port backup [interface-type backup-interface-number] force-switch</code> <code>Raisecom(config- tengigabitethernet1/1/1)#port backup [interface-type backup-interface-number] force-switch</code>	Configure FS on the interface. Use the no port backup [<i>interface-type backup-interface-number</i>] force-switch command to cancel FS. Then, the principles of selecting the current link according to link status are as below: <ul style="list-style-type: none"> • If the Up/Down statuses of the two interfaces are the same, the primary interface is of high priority. • If the Up/Down statuses of the two interfaces are different, the Up interface is of high priority.

11.3.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show switchport backup</code>	Show status information about interface backup.
2	<code>Raisecom#show port backup group</code>	Show configurations of interface backup.

11.3.7 Example for configuring interface backup

Networking requirements

As shown in Figure 11-4, 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

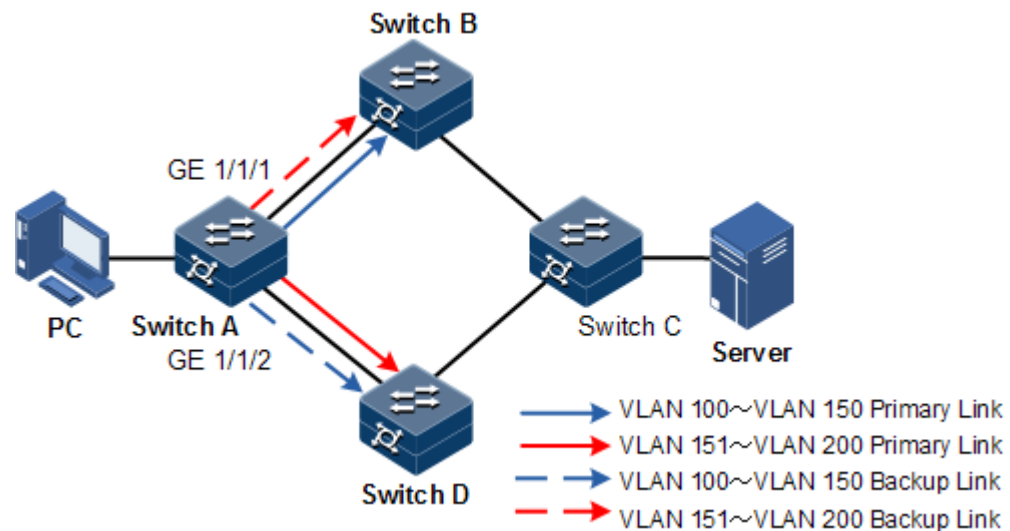
Switch A and specify the VLAN list so that the two interfaces concurrently forward services in different VLANs and balance load. Configure Switch A as below:

- 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.

Figure 11-4 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 tengigabitethernet 1/1/1
Raisecom(config-gigabitethernet1/1/1)#portswitch
Raisecom(config-gigabitethernet1/1/1)#switchport mode trunk
Raisecom(config-gigabitethernet1/1/1)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-gigabitethernet1/1/1)#exit
Raisecom(config)#interface gigabitethernet 1/1/2
Raisecom(config-gigabitethernet1/1/2)#portswitch
Raisecom(config-gigabitethernet1/1/2)#switchport mode trunk
Raisecom(config-gigabitethernet1/1/2)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-gigabitethernet1/1/2)#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 gigabitethernet 1/1/1
Raisecom(config-gigabitethernet1/1/1)#port backup gigaethernet 1/1/2
vlanlist 100-150
Raisecom(config-gigabitethernet1/1/1)#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 gigabitethernet 1/1/2
Raisecom(config-gigabitethernet1/1/2)#port backup gigaethernet 1/1/1
vlanlist 151-200
```

Checking results

Use the **show port backup** command to show status of interface backup under normal or faulty conditions.

When both GE 1/1/1 and GE 1/1/2 are Up, 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
Active Port(State)    Backup Port(State)    ForceSwitch    Vlanlist
-----
GE1/1/1(Up)  GE1/1/2(Standby)    NO    100-150
GE1/1/2(Up)  GE1/1/1(Standby)    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
Active Port(State)    Backup Port(State)    Vlanlist
-----
GE1/1/1(Down)  GE1/1/2(Up)          100-150
GE1/1/2(Up)    GE1/1/1(Down)        151-200
```

When GE 1/1/1 resumes and keeps Up for 15s (restore-delay), it forwards traffic of VLANs 100–150 while GE 1/1/2 forwards traffic of VLANs 151–200.

11.4 Configuring VRRP

11.4.1 Preparing for configurations

Scenario

Generally, a default route to the breakout gateway is configured for all devices in a LAN, so these devices can communicate with the external network. If the gateway fails, the connection will fail.

VRRP combines multiple routers to form a backup group. By configuring a virtual IP address for the backup group, you can configure the default gateway to the virtual IP address of the backup group to make devices in the LAN communicate with the external network.

VRRP helps improve network reliability by preventing network interruption caused by failure of a single link and prevents changing routing configurations due to link failure.

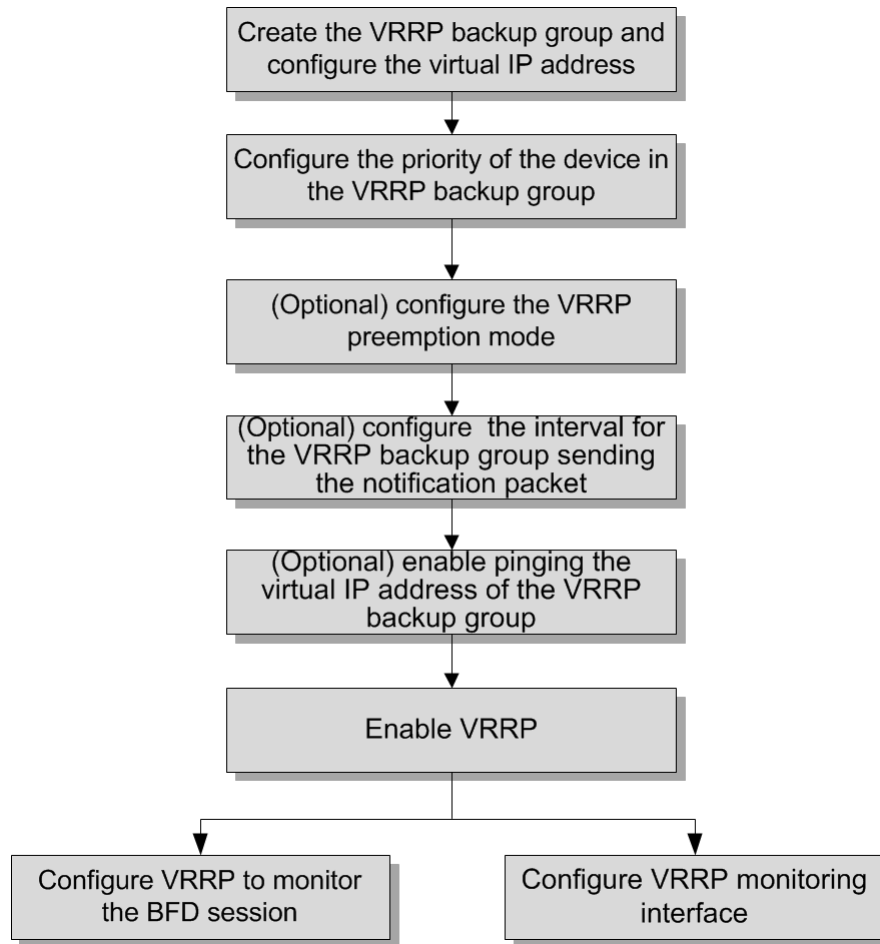
Prerequisite

N/A

11.4.2 Configuration flow

Figure 11-5 shows the VRRP configuration flow.

Figure 11-5 VRRP configuration flow



11.4.3 Configuring VRRP backup group

Configure the VRRP backup group for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter Layer 3 physical interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/1)#vrrp <i>group-id ip ip-address</i></code>	Create a VRRP backup group and configure a virtual IP address for the VRRP backup group. The virtual IP address must be in the same network segment as the interface IP address.
4	<code>Raisecom(config-gigaethernet1/1/1)#vrrp <i>group-id description description</i></code>	(Optional) configure the description of the VRRP backup group.

Step	Command	Description
5	<code>Raisecom(config-gigaethernet1/1/1)#vrrp group-id preempt [delay-time second]</code>	(Optional) enable the preemption mode of the VRRP backup group. By default, the newly-created VRRP backup group is in preemption mode. The preemption delay is 0s.
6	<code>Raisecom(config-gigaethernet1/1/1)#vrrp group-id priority priority</code>	Configure the priority of the device in the VRRP backup group. By default, the priority of the newly-created VRRP backup group is 100.
7	<code>Raisecom(config-gigaethernet1/1/1)#vrrp group-id timers advertise-interval seconds</code>	(Optional) configure the interval for the VRRP backup group to send the notification packet. By default, it is 1s.
8	<code>Raisecom(config-gigaethernet1/1/1)#vrrp group-id enable</code>	Enable VRRP. By default, it is enabled.

11.4.4 (Optional) configuring ping function of VRRP virtual IP address

Configure the ping function of VRRP virtual IP address for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#vrrp ping</code>	Enable the ping function of the virtual IP address of the VRRP backup group. By default, it is enabled.

11.4.5 Configuring VRRP monitoring interface

Configure the VRRP monitoring interface for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter Layer 3 physical interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/1)#vrrp group-id track interface-type interface-number [reduce priority]</code>	Configure the monitoring interface of VRRP.

11.4.6 Configuring BFD for VRRP

Configure BFD for VRRP for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-</i> <i>number</i></code>	Enter Layer 3 physical interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#vrrp group- <i>id track bfd-session session-</i> <i>id [increased priority </i> <i>reduce priority]</i></code>	Configure the VRRP backup group to monitor the BFD session to implement expedited switching.

11.4.7 Checking configurations

Use the following commands to check configuration results.

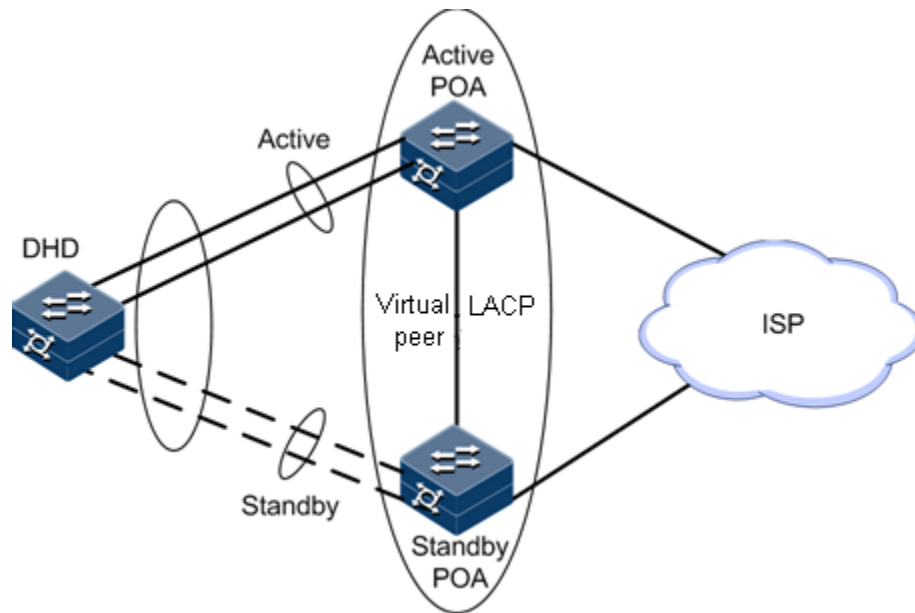
No.	Command	Description
1	<code>Raisecom#show vrrp group-id</code>	Show configurations of the VRRP backup group.
2	<code>Raisecom#show vrrp interface <i>interface-type interface-</i> <i>number [group-id]</i></code>	Show configurations of the VRRP backup group on the interface.
3	<code>Raisecom#show vrrp interface <i>interface-type interface-</i> <i>number [group-id] statistics</i></code>	Show statistics about the VRRP backup group on the interface.
4	<code>Raisecom#show vrrp [group- <i>id] track</i></code>	Show monitoring information about the VRRP backup group.

11.5 mLACP

11.5.1 Introduction

A loop may occur when a device has two uplink Points of Access (PoAs), which means that the device is a Dual Home Device (DHD). Sometimes, the DHD is incapable of running any loop detection protocols. In this case, you can use the Multi-Chassis Link Aggregation Control Protocol (mLACP), which offers you another choice, to select paths for the DHD.

Figure 11-6 Dual-homed application based on LACP



As shown in Figure 11-6, two PoAs exchange configuration information through InterChassis Communication Protocol (ICCP), synchronizing the state of each other (each PoA receives and saves information about the other PoA). The two PoAs form a virtual LACP peer and appear as a single device to the DHD.

Links that connect the DHD are configured to the same Link Aggregation Group (LAG). Interface selection and link aggregation are implemented through LACP. In this case, the two PoAs in the same LAG appear to be in one Inter-Chassis Group (ICG).

The whole system, according to the configured priority, will select a PoA from the ICG to be the active one by using LACP. The active PoA will communicate with DHD. In one ICG, only one PoA can be active and the other standby.

When the number of Up links between the active PoA and the DHD is smaller than the configured number of LAG links, the system will perform fault switching, making the other PoA active and the local PoA standby. When faults at the local PoA are cleared, the system will perform fault recovery, reselecting the local PoA as the active one.

11.5.2 Preparing for configurations

Scenario

Create an ICCP channel on the PoA. Make the two independent PoAs form a virtual redundant ICG which can implement mLACP.



Prerequisite

The special VLAN for the ICCP channel has been established. The special Layer 3 interface IP address for the special VLAN of the 2 PoAs is configured differently and in the same network segment. The LAG in each device has been established. The interfaces which are to be added to the LAG have been switched to Layer 2 interfaces and are added to the LAG without any configurations. Interfaces on the DHD which are to be added to the LAG should

be the ones connecting all links to the 2 PoAs. However, interfaces on the 2 PoAs which are to be added to the LAG contain the local interfaces which connect the DHD only.

11.5.3 Configuring ICCP channel



Configure the ICCP channel for the ISCOM3000G series switch as below.

Step	Configuration	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#iccp local-ip ip-address</code>	Configure the IP address of the local interface in the ICCP channel.  Caution The configured IP address must be the IP address of the local Layer 3 interface. When modifying the IP address of the local Layer 3 interface, you have to reconfigure the IP address of the local ICCP.
3	<code>Raisecom(config)#iccp-channel channel-id</code>	Create a communication channel and enter ICCP configuration mode.
4	<code>Raisecom(config-iccp)#member-ip ip-address</code>	Configure the IP address of the peer ICCP.  Caution The configured IP address must be the IP address of the peer Layer 3 interface. When modifying the IP address of the peer Layer 3 interface, you have to reconfigure the IP address of the ICCP peer.
5	<code>Raisecom(config-iccp)#iccp enable</code>	Enable ICCP. By default, it is disabled.

11.5.4 Configuring mLACP link aggregation

Configure mLACP link aggregation for the ISCOM3000G series switch as below.

Step	Configuration	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mlacp-group icg-id</code>	Create an ICG and enter ICG configuration mode.
3	<code>Raisecom(config-ic-group)#iccp-channel channel-id</code>	Bind the ICG with an ICCP channel.
4	<code>Raisecom(config-ic-group)#mlacp { master slave }</code>	Configure the mLACP role for the local device in the ICG.

Step	Configuration	Description
5	<code>Raisecom(config-ic-group)#port-channel group-id</code>	Bind the ICG with a LAG.  Caution The LAG ID to be bound must be the already established LAG ID. Otherwise, it will be unavailable for use. For how to create a LAG, see descriptions about the port-channel command.
6	<code>Raisecom(config-ic-group)#restore-mode { non-revertive revertive [restore- delay second] }</code>	Configure the LAG fault restore mode and restore-delay time on the ICG.
7	<code>Raisecom(config-ic-group)#mlacp system- priority system- priority</code>	Configure the system priority of the local device in the ICG. By default, the mLACP system priority of the device is 32768.  Caution The priority of the device in the ICG should be higher than that of the DHD. The smaller the value is, the higher the priority will be.

11.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show iccp channel [channel-id] statistics</code>	Check statistics on packets received by or sent from the ICCP channel.
2	<code>Raisecom#show iccp channel channel-id</code>	Check the configurations and running status of the ICCP channel.
3	<code>Raisecom#show mlacp- group [group-id]</code>	Check the mLACP configurations and running status.

11.5.6 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
<code>Raisecom(config)#clear iccp channel <i>chanel-id</i> statistics</code>	Clear statistics on packets received by or sent from the ICCP channel.
<code>Raisecom(config)#clear mlacp mlacp-group [<i>group-id</i>] statistics</code>	Clear statistics on packets received by or sent from the ICG.

11.5.7 Example for configuring mLACP

Networking requirements

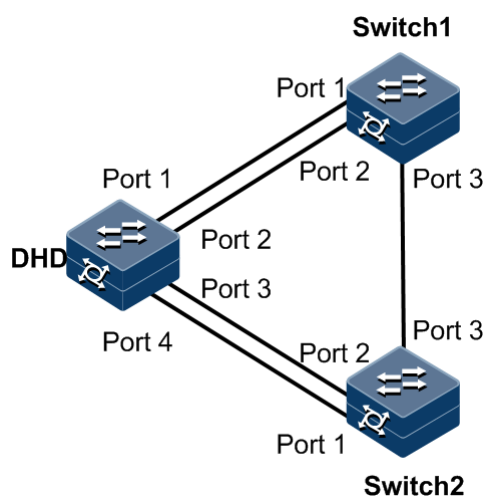
Prepare two mLACP devices: Switch1 and Switch2. The two devices exchange configuration information through ICCP. Switch1 and switch2 appear as a virtual LACP peer to the DHD.

The DHD exchanges LACPDU with the virtual LACP peer to aggregate links. At the same time, the link between the DHD and one switch is active and that between the DHD with the other switch is standby.

As shown in Figure 5-2, Port 1, Port 2, Port 3, and Port 4 on the DHD are in the same LAG. Port 1 and Port 2 on Switch 1 and Switch 2 are in the same LAG. Configure the maximum active links and minimum active links to 2 respectively. Configure the priority of Switch 1/Switch 2 higher than that of the DHD. For example, if you configure the system priority of Switch1 higher than that of the DHD, Switch1 will be the active link and Switch 2 will be the standby link when priority pre-emption is enabled.

When the number of active links between the DHD and Switch 1 is smaller than 2, link switching will occur. Traffic will be switched to the link between the DHD and Switch 2. When the number of active links between the DHD and Switch 1 is 2, the link will recover. Traffic will be switched back to the link between the DHD and Switch 1.

Figure 11-7 mLACP networking



Configuration steps

- Step 1 Configure a LAG. Add Port 1, Port 2, Port 3, and Port 4 on the DHD to the LAG and enable priority pre-emption of the LAG.

```
DHD#config
DHD(config)#interface port-channel 1
DHD(config-port-channel1)#mode lacp
DHD(config-port-channel1)#max-active links 2
DHD(config-port-channel1)#min-active links 2
DHD(config-port-channel1)#lacp priority preempt enable
DHD(config-port-channel1)#interface tengigabitethernet 1/1/1
DHD(config-gigaethernet1/1/1)#portswitch
DHD(config-gigaethernet1/1/1)#port-channel 1
DHD(config-gigaethernet1/1/1)#interface gigaehternet 1/1/2
DHD(config-gigaethernet1/1/2)#portswitch
DHD(config-gigaethernet1/1/2)#port-channel 1
DHD(config-gigaethernet1/1/2)#interface gigaehternet 1/1/4
DHD(config-gigaethernet1/1/4)#portswitch
DHD(config-gigaethernet1/1/4)#port-channel 1
DHD(config-gigaethernet1/1/4)#interface gigaehternet 1/1/3
DHD(config-gigaethernet1/1/3)#portswitch
DHD(config-gigaethernet1/1/3)#port-channel 1
```

Configure a LAG for Switch1. Add Port 1 and Port 2 on Switch 1 to the LAG and enable priority pre-emption of the LAG.

```
Switch1#config
Switch1(config)#interface port-channel 1
Switch1(config-port-channel1)#mode lacp
Switch1(config-port-channel1)#max-active links 2
Switch1(config-port-channel1)#min-active links 2
Switch1(config-port-channel1)#lacp priority preempt enable
Switch1(config-port-channel1)#interface gigaehternet 1/1/1
Switch1(config-gigaethernet1/1/1)#portswitch
Switch1(config-gigaethernet1/1/1)#port-channel 1
Switch1(config-gigaethernet1/1/1)#interface gigaehternet 1/1/2
Switch1(config-gigaethernet1/1/2)#portswitch
Switch1(config-gigaethernet1/1/2)#port-channel 1
```

Configure a LAG for Switch 2. Add Port 1 and Port 2 on Switch 2 to the LAG and enable priority pre-emption of the LAG.

```
Switch2#config
Switch2(config)#interface port-channel 1
Switch2(config-port-channel1)#mode lacp
Switch2(config-port-channel1)#max-active links 2
Switch2(config-port-channel1)#min-active links 2
Switch2(config-port-channel1)#lacp priority preempt enable
Switch2(config-port-channel1)#interface gigaehternet 1/1/1
Switch2(config-gigaethernet1/1/1)#portswitch
Switch2(config-gigaethernet1/1/1)#port-channel 1
Switch2(config-gigaethernet1/1/1)#interface gigaehternet 1/1/2
Switch2(config-gigaethernet1/1/2)#portswitch
Switch2(config-gigaethernet1/1/2)#port-channel 1
```

Step 2 Configure an ICCP channel and bind it with the ICG. Apply the ICCP channel to the LAG.

Configure Switch1 as below:

```
Switch1#config
Switch1(config)#create vlan 6 active
Switch1(config)#interface tengigabitethernet 1/1/3
Switch1(config-tengigabitethernet1/1/3)#portswitch
Switch1(config-tengigabitethernet1/1/3)#switchport access vlan 6
Switch1(config-tengigabitethernet1/1/3)#interface vlan 6
Switch1(config-vlan6)#ip address 10.110.3.1 255.255.255.0
Switch1(config-vlan6)#exit
Switch1(config)#iccp local-ip 10.110.3.1
Switch1(config)#iccp channel 1
Switch1(config-iccp)#member-ip 10.110.3.2
Switch1(config-iccp)#iccp enable
Switch1(config-iccp)#exit
Switch1(config)#mlacp-group 1
Switch1(config-ic-group)#iccp-channel 1
Switch1(config-ic-group)#mlacp master
Switch1(config-ic-group)#mlacp system-priority 20000
Switch1(config-ic-group)#port-channel 1
Switch1(config-ic-group)#restore-mode revertive restore-delay 20
Switch1(config-ic-group)#exit
```

Configure Switch 2 as below:

```
Switch2#config
Switch2(config)#create vlan 6 active
Switch2(config)#interface tengigabitethernet 1/1/3
Switch2(config-tengigabitethernet1/1/3)#portswitch
Switch2(config-tengigabitethernet1/1/3)#switchport access vlan 6
Switch2(config-tengigabitethernet1/1/3)#interface vlan 6
Switch2(config-vlan6)#ip address 10.110.3.2 255.255.255.0
Switch2(config-vlan6)#exit
Switch2(config)#iccp local-ip 10.110.3.2
Switch2(config)#iccp channel 1
Switch2(config-iccp)#member-ip 10.110.3.1
Switch2(config-iccp)#iccp enable
Switch2(config-iccp)#exit
Switch2(config)#mlacp-group 1
Switch2(config-ic-group)#iccp-channel 1
Switch2(config-ic-group)#port-channel 1
Switch2(config-ic-group)#mlacp slave
Switch2(config-ic-group)#restore-mode revertive restore-delay 20
Switch2(config-ic-group)#exit
```

Checking results

Check LACP configurations of the DHD.


```
DHD#show port-channel 1
Group 1 information:
Mode      : LACP                      Load-sharing mode : src-dst-mac
MinLinks: 2                          Max-links         : 2
UpLinks  : 4                          Priority-Preemptive: Enable
Member Port : gigaethernet1/1/1 gigaethernet1/1/2 gigaethernet1/1/4
gigaethernet1/1/3
Efficient Port: gigaethernet1/1/1 gigaethernet1/1/2
```

Check mLACP configurations of S witch1.

```
Switch1#show mlacp-group 1
mlacp group      : 1
```

```
System information:
MAC address running      : 000E.5E11.2233
System priority running  : 20000
```

```
Configuration information:
                Local information      Peer information
system mac:      000E.5E55.0001        000E.5E11.2233
System priority: 20000                 32768
Port-channel:    1                     N/A
Type:            master                 slave
Iccp-channel:    1                     N/A
Iccp-State:      connect                N/A
Track PwId:      0                     N/A
Pw Ip:           0.0.0.0                N/A
Pw state:        N/A                   N/A
State:           Active                 Standby
Restore Type:    revertive              N/A
Restore Time(s): 20                    N/A
```

Check mLACP configurations of Switch 2.

```
Switch2#show mlacp-group 1
mlacp group      : 1
```

```
System information:
MAC address running      : 000E.5E11.2233
System priority running  : 20000
```

```
Configuration information:
                Local information      Peer information
system mac:      000E.5E11.2233        000E.5E55.0001
System priority: 32768                 20000
Port-channel:    1                     N/A
Type:            slave                 master
Iccp-channel:    1                     N/A
Iccp-State:      connect                N/A
```

Track PwId:	0	N/A
Pw Ip:	0.0.0.0	N/A
Pw state:	N/A	N/A
State:	Standby	Active
Restore Type:	revertive	N/A
Restore Time(s):	20	N/A

12 OAM

This chapter describes principles and configuration procedures of OAM and provide related configuration examples, including following sections:

- Introduction
- Configuring EFM
- Configuring BFD

12.1 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.

12.1.1 EFM

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.

OAM mode and 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.

In the discovery phase, a connected Ethernet OAM entity (interface enabled with OAM) informs others of its Ethernet OAM configurations and Ethernet OAM capabilities supported by the local node by exchanging information OAM PDU. After the OAM entity receives

parameters of the peer, it determines whether to establish OAM connection. If both ends agree on establishment of the OAM connection, Ethernet OAM protocol will work on the link layer.

The ISCOM3000G series switch can choose one of the following 2 modes to establish Ethernet OAM connection:

- Active mode
- Passive mode

Only the OAM entity in active mode can initiate OAM connection while the OAM entity in passive mode just waits for connection request of the active OAM entity.

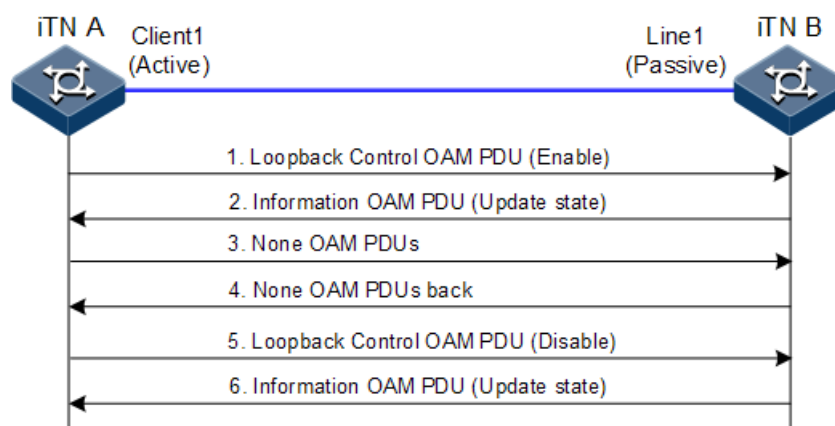
After the OAM connection is established, both ends keep connected by exchanging information OAM PDU. If an OAM entity does not receive information OAM PDU within 5s, it judges that connection expires and reconnection is required.

OAM loopback

OAM loopback occurs only after the Ethernet OAM connection is established. When connected, the active OAM entity initiates OAM loopback command, and the peer OAM entity responds to the command.

When the remote OAM entity is in loopback mode, all packets but OAM PDU packets are sent back. By observing the returned PAMPDU packets, the network administrator can judge the link performance (including packet loss rate, delay, and jitter).

Figure 12-1 OAM loopback



As shown in Figure 12-1, Port 1 on iTN A works in active mode. After the 802.3ah OAM connection between iTN A and iTN B is established, enable remote loopback on Client 1.

Start OAM loopback as below:

- Step 1 iTN A sends a Loopback Control OAM PDU packet with the Enable information to iTN B, and waits for response.
- Step 2 After receiving the Loopback Control OAM PDU packet with the Enable information, iTN B replies the Information OAM PDU packet to iTN A, and enters the loopback state.
- Step 3 After receiving the response, iTN A sends a non-OAM PDU test packet to iTN B.
- Step 4 After receiving a non-OAM PDU test packet, iTN B sends it back to iTN A.

Stop OAM loopback as below:

- Step 1 To stop remote loopback, iTN A sends a Loopback Control OAM PDU packet with the Disable information to iTN B.
- Step 2 After receiving the Loopback Control OAM PDU packet with the Disable information, iTN B exits loopback state and sends an Information OAM PDU packet to iTN A.

You can troubleshoot the fault through loop detection in different phases.

OAM events

Detecting Ethernet faults is difficult, especially when the physical communication works properly while the network performance deteriorates slowly. 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.
- Dying gasp: an unpredictable event occurs, such as power failure.
- Critical event: an uncertain critical event occurs.

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. 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.



Note

If an errored frame occurs in a second, the second is called the errored frame second.

Acquiring OAM MIB

The ISCOM3000G series switch learns the status and parameters of the peer link by acquiring link configurations/statistics about the peer through OAM.

12.1.2 BFD

Bidirectional Forwarding Detection (BFD) is used to detect connectivity of data protocol between systems or in the same path. The path is the physical link, logical link, or channel. When finding a communication fault between systems, BFD notifies applications at the upper layer.

Detection mechanism

BFD establishes a session between two endpoints in the communication system, and periodically sends BFD control packets in the detection path. If one endpoint fails to receive BFD control packets within the required time, BFD considers that fault occurs in the path.

BFD control packets are encapsulated in the UDP packets and then are transmitted. At the initial stage of the session, both systems negotiate through parameters carried on the control packets (such as session identifiers of two endpoints, the minimum interval for receiving and sending packets, BFD session status of the local endpoint). When the negotiation is successful, both systems send BFD control packets according to negotiated time of receiving and sending packets.

Modes for establishing BFD sessions

There are two modes for establishing BFD sessions: statically establishing BFD sessions and dynamically establishing BFD sessions. BFD distinguishes these two session modes through identifiers of the local endpoint and remote endpoint in the control packet.

- Statically establishing BFD session: configure BFD session parameters manually, including identifiers of local and remote endpoints.
- Dynamically establishing BFD session: the system automatically assigns values within dynamic session identifier area to be those of the local BFD session, and the local and remote endpoints will negotiate. After receiving negotiated packets, the remote endpoint determines whether identifiers match the local BFD session. If yes, the remote endpoint automatically learns identifiers of the remote session.

The ISCOM3000G series switch supports statically establishing BFD sessions.

Application types of BFD

The ISCOM3000G series switch supports the following BFD applications:

- BFD based on IP link: establish a BFD session on the IP link and use BFD detection mechanism to detect faults rapidly. The ISCOM3000G series switch supports single-hop IP detection or multi-hop IP detection on the IP link.
 - Single-hop IP detection: BFD rapidly detects communication faults between systems and supports IP connectivity detection between directly-connected devices.
 - Multi-hop IP detection: BFD rapidly detects communication faults between systems and supports IP connectivity detection between indirectly-connected devices.
- BFD based on ISIS
- BFD based on OSPF

SLA is a telecommunication service evaluation standard negotiated by the ISP and users. It is an agreement reached by both sides in service quality, priority, responsibility.

In technology, SLA is realtime network performance detection and statistics for responding time, network jitter, delay, packet loss rate.

12.2 Configuring EFM

12.2.1 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.

12.2.2 Configuring basic functions of EFM

Configure basic functions of EFM for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface gig Ethernet <i>interface-number</i>	Enter Layer 2 or Layer 3 interface configuration mode.
3	Raisecom(config-gig Ethernet1/1/1)#oam { active passive }	Configure a working mode of EFM. By default, the ISCOM3000G series switch is in passive mode.
4	Raisecom(config-gig Ethernet1/1/1)#oam send-period <i>period-number</i> timeout <i>time</i>	(Optional) configure the period for sending OAM PDUs and the OAM link timeout. By default, the period is configured to 1s (namely, <i>period-number</i> is 10, $10 \times 100\text{ms} = 1\text{s}$), and timeout is 5s.
5	Raisecom(config-gig Ethernet1/1/1)#oam enable	Enable interface OAM. By default, OAM is disabled on the interface.

12.2.3 Configuring EFM active function



Note

The EFM active function can be configured only when the ISCOM3000G series switch is in active mode.

(Optional) enabling EFM remote loop



Note

- Perform loopback detection periodically can discover network fault in time. Loopback detection in network sections can locate exact fault area and help users clear fault.
- In link loopback status, the ISCOM3000G series switch sends back all packets except OAM packets received by the link to the peer device. Disable this function in time if no loopback detection is needed.

Enable EFM remote loop for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#oam remote-loopback	Configure the interface to start EFM remote loopback.
4	Raisecom(config-gigaethernet1/1/1)#oam loopback timeout <i>time</i>	(Optional) Configure the timeout for remote loopback on the physical interface. By default, it is 3s.
5	Raisecom(config-gigaethernet1/1/1)#oam loopback retry <i>times</i>	(Optional) Configure the retries for remote loopback on the physical interface. By default, it is 3.

(Optional) showing current variable information about peer device



Note

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 packet 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 requesting object, and the branch and leaf are followed by variable to denote object responds variable request.

The ISCOM3000G series switch supports obtaining OAM information and interface statistics.

Peer variable cannot be obtained until EFM is connected.

Show current variable information about the peer device for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#show oam peer oam-info [<i>interface-type interface-number</i>]	Obtain basic OAM

Step	Command	Description
	<code>Raisecom#show oam peer [interface-type interface-number]</code>	information about the peer device.

12.2.4 Configuring EFM passive function



Note

The EFM passive function can be configured regardless the ISCOM3000G series switch is in active or passive mode.

(Optional) configuring device to respond with EFM remote loop

Configure the ISCOM3000G series switch to respond with EFM remote loop as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface tengigabitethernet interface-number</code>	Enter Layer 2 or Layer 3 interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/1)#oam loopback { ignore process }</code>	Configure the Layer 2 physical interface to ignore or process EFM remote loopback. By default, the Layer 2 physical interface responds to EFM remote loopback.

12.2.5 Configuring link monitoring and fault indication

(Optional) configuring OAM link monitoring



Note

OAM link monitor is used to detect and report link errors in different conditions. When the detection link has a fault, the ISCOM3000G 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 to the NView NNM system center through SNMP Trap.

By default, the system has default values for error generated time, window and threshold.

Configure OAM link monitoring for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.

Step	Command	Description
2	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter Layer 2 physical interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#oam errored-frame window framewindow threshold framethreshold</code>	Configure errored frame monitor window and threshold. By default, the monitor window is 1s, and the threshold is 1 errored frame.
4	<code>Raisecom(config- gigaethernet1/1/1)#oam errored-frame-period window frameperiodwindow threshold frameperiodthreshold</code>	Configure errored frame period event monitor window and threshold. By default, the monitor window is 1000ms, and the threshold is 1 errored frame.
5	<code>Raisecom(config- gigaethernet1/1/1)#oam errored-frame-seconds window framesecwindow threshold framesecsthreshold</code>	Configure link errored frame second window and threshold. By default, the monitor window is 60s, and the threshold is 1s.
6	<code>Raisecom(config- gigaethernet1/1/1)#oam errored-symbol-period window symperiodwindow threshold symperiodthreshold</code>	Configure errored code window and threshold. By default, the monitor window is 1s, and the threshold is 1s.

(Optional) configuring OAM fault indication

Configure OAM fault indication for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interfac e interface-type interface-number</code>	Enter Layer 2 physical interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#oam notify { critical-event dying-gasp errored- frame errored-frame- period errored-frame- seconds errored-symbol- period } enable</code>	Configure the OAM link event notification. By default, OAM link event notification is enabled.
4	<code>Raisecom(config- gigaethernet1/1/1)#oam event trap enable</code>	Enable local OAM event Trap to report link monitoring events to the NView NNM system immediately. By default, local OAM event Trap is disabled.

Step	Command	Description
5	<pre>Raisecom(config- gigaethernet1/1/1)#oam peer event trap { enable disable }</pre>	<p>Enable peer OAM event Trap to report link monitoring events to the NView NNM system immediately.</p> <p>By default, peer OAM event Trap is disabled.</p>

12.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<pre>Raisecom#show oam [interface-type interface-number]</pre>	Show basic configurations of EFM.
2	<pre>Raisecom#show oam event [interface- type interface-number] [critical]</pre>	Show local OAM link events.
3	<pre>Raisecom#show oam loopback [interface-type interface-number]</pre>	Show configurations of OAM remote loopback.
4	<pre>Raisecom#show oam notify [interface- type interface-number]</pre>	Show configurations of OAM event notification.
5	<pre>Raisecom#show oam peer event [interface-type interface-number] [critical]</pre>	Show configurations of OAM peer events.
6	<pre>Raisecom#show oam peer link- statistic [interface-type interface- number]</pre>	Show statistics about peer OAM links.
7	<pre>Raisecom#show oam statistics [interface-type interface-number]</pre>	Show OAM statistics.
8	<pre>Raisecom#show oam trap [interface- type interface-number]</pre>	Show OAM Trap.

12.3 Configuring BFD

12.3.1 Preparing for configurations

Scenario

To reduce effect of faults on services and improve network availability, the ISCOM3000G series switch needs to detect communication faults between it and adjacent devices. Therefore, it can take actions immediately to ensure normal transmission of services.

Prerequisite

N/A



12.3.2 Configuring BFD session binding


Configure BFD session binding for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#bfd <i>session-id</i> bind peer-ip <i>ip-address</i> [source-ip]	Create a BFD session detection multi-hop IP path, and enter BFD session configuration mode.
	Raisecom(config)#bfd <i>session-id</i> bind { peer-ip <i>ip-address</i> } interface <i>interface-type</i> <i>interface-number</i>	Create a static BFD session detection single-hop IP path, and enter BFD session mode.
3	Raisecom(config)#bfd trap enable	(Optional) enable BFD Trap. By default, it is disabled.

12.3.3 Configuring BFD session parameters

Configure BFD session parameters for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#bfd <i>session-id</i>	Enter BFD session mode.  Note You cannot use this command to enter BFD session mode unless you create the BFD and bind the related path.
3	Raisecom(config-bfd-session)# description <i>description</i>	Configure descriptions of the BFD session.
4	Raisecom(config-bfd-session)# local discriminator <i>value</i>	Configure the local identifier of the BFD session. By default, the local identifier is displayed as 0, which indicates that no local identifier is configured.  Note It is automatically generated by the system if not configured.
5	Raisecom(config-bfd-session)# min send-interval <i>interval</i>	Configure the minimum sending interval of the BFD session. By default, it is 10ms.

Step	Command	Description
6	Raisecom(config-bfd-session)# min receive-interval interval	Configure the minimum receiving interval of the BFD session. By default, it is 10ms.
7	Raisecom(config-bfd-session)# detect-multiplier multiplier	Configure the local detection times of the BFD session. By default, it is 3.
8	Raisecom(config-bfd-session)# remote discriminator value	Configure the remote identifier of the BFD session. By default, the remote identifier is displayed as 0, which indicates that no remote identifier is configured.  Note It is automatically generated by the system if not configured.
9	Raisecom(config-bfd-session)# session enable	Enable BFD session. By default, it is disabled.

12.3.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show bfd	Show BFD global configurations.
2	Raisecom# show bfd session-id config	Show configurations about the specified BFD session.
3	Raisecom# show bfd session-id state	Show status of the specified BFD session.
4	Raisecom# show bfd session-id statistics	Show statistics on the specified BFD session.
5	Raisecom# show bfd diagnostic-code	Show the diagnostic code.

13 System management

This chapter describes principles and configuration procedures of system management and maintenance, and provides related configuration examples, including the following sections:

- SNMP
- KeepAlive
- RMON
- LLDP
- Optical module DDM
- System log
- Alarm management
- Hardware environment monitoring
- CPU monitoring
- Cable diagnosis
- Memory monitoring
- Fan monitoring
- Performance statistics
- Ping
- Traceroute

13.1 SNMP

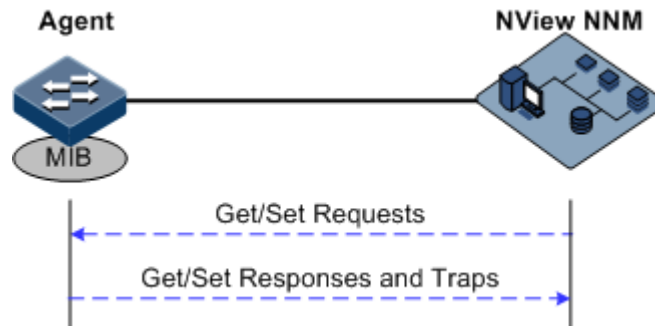
13.1.1 Introduction

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.

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 13-1 shows the SNMP principle.

Figure 13-1 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 ISCOM3000G series switch when conditions are satisfied; replying module sends Trap packets to the NView NNM system through agent to report current status of the ISCOM3000G 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 ISCOM3000G 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.

- 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 to encrypt packets transmitted between the network management system and agents, thus preventing interception.

The ISCOM3000G 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 ISCOM3000G 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 protocol packets can access network devices by checking the nodes in MIB tree directory.

The ISCOM3000G series switch supports standard MIB and Raisecom-customized MIB.

13.1.2 Preparing for configurations

Scenario

To log in to the ISCOM3000G series switch through NMS, configure SNMP basic functions for the ISCOM3000G series switch in advance.

Prerequisite

Configure the routing protocol and ensure that the route between the ISCOM3000G series switch and NMS is reachable.

13.1.3 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

Function	Default value																								
SNMP access group	initialnone and initial access groups (default)																								
SNMP user	none, md5nopriv, shapriv, md5priv, and shanopriv users (default)																								
Mapping between SNMP user and access group	<table border="1"> <thead> <tr> <th>Index</th> <th>GroupName</th> <th>UserName</th> <th>SecModel</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>initialnone</td> <td>none</td> <td>usm</td> </tr> <tr> <td>1</td> <td>initial</td> <td>md5priv</td> <td>usm</td> </tr> <tr> <td>2</td> <td>initial</td> <td>shapriv</td> <td>usm</td> </tr> <tr> <td>3</td> <td>initial</td> <td>md5nopriv</td> <td>usm</td> </tr> <tr> <td>4</td> <td>initial</td> <td>shanopriv</td> <td>usm</td> </tr> </tbody> </table>	Index	GroupName	UserName	SecModel	0	initialnone	none	usm	1	initial	md5priv	usm	2	initial	shapriv	usm	3	initial	md5nopriv	usm	4	initial	shanopriv	usm
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 administrator	support@Raisecom.com																								
Device physical location	world china raisecom																								
Trap	Enable																								
SNMP target host address	N/A																								
SNMP engine ID	800022B603000E5E000016																								

13.1.4 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 ISCOM3000G 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#snmp-server view <i>view-name</i> <i>oid-tree</i> [<i>mask</i>] { excluded 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.

Step	Command	Description
3	<code>Raisecom(config)#snmp-server community <i>com-name</i> [view <i>view-name</i>] { ro rw }</code>	Create community name and configure the corresponding view and authority. Use default view internet if view <i>view-name</i> option is empty.

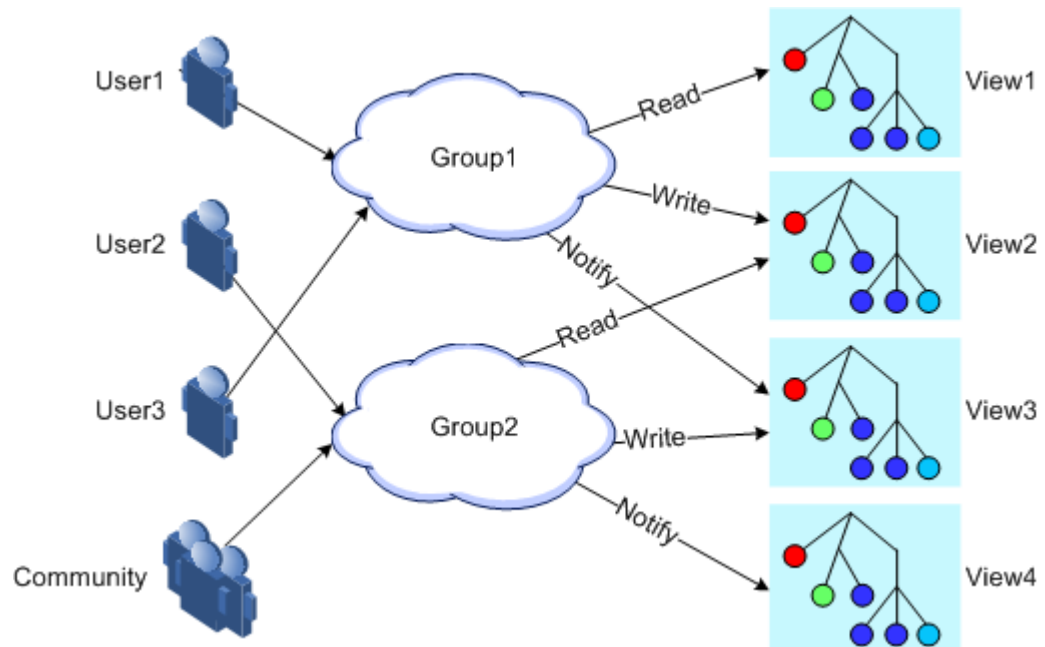
13.1.5 Configuring basic functions of SNMPv3

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 13-2, the network management station uses the normal access from SNMPv3 to switch and the configuration is as below.

- Configure users.
- Check the access group to which the user belongs.
- Configure view permission for access groups.
- Create views.

Figure 13-2 Principles of SNMPv3 authentication



Configure basic functions of SNMPv3 for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.

Step	Command	Description
2	<code>Raisecom(config)#snmp-server view view-name oid-tree [mask] { excluded included }</code>	(Optional) create SNMP view and configure MIB variable range.
3	<code>Raisecom(config)#snmp-server user user-name [remote engine-id] authentication { md5 sha } authpassword [privkey privkeypassword]</code>	Create users and configure authentication modes.
4	<code>Raisecom(config)#snmp-server user user-name [remote engine-id] authkey { md5 sha } keyword [privkey privkeypassword]</code>	(Optional) modify the authentication key and the encryption key.
5	<code>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 }</code>	Create and configure the SNMPv3 access group.
6	<code>Raisecom(config)#snmp-server group group-name user user-name usm</code>	Configure the mapping between users and the access group.

13.1.6 Configuring IP address authentication by SNMP server

Configure IP address authentication by SNMP server for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#snmp- server server-auth enable</code>	Enable IP address authentication by the SNMP server.
3	<code>Raisecom(config)#snmp- server server-auth ip- address</code>	Configure the IP address of the SNMP server for authentication.


13.1.7 Configuring other information about SNMP

Other information about SNMP includes:

- Logo and contact method of the administrator, which is used to identify and contact the administrator
- Physical location of the device: describes where the device is located

SNMPv1, SNMPv2c, and SNMPv3 support configuring this information.

Configure other information about SNMP for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#snmp-server contact <i>contact</i>	(Optional) configure the logo and contact method of the administrator.  Note For example, configure the E-mail to the logo and contact method of the administrator.
3	Raisecom(config)#snmp-server location <i>location</i>	(Optional) specify the physical location of the device.

13.1.8 Configuring Trap



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 ISCOM3000G 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. SNMPv1 and v2c need to configure the community name; SNMPv3 needs to configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the ISCOM3000G series switch and NMS is reachable.

Configure SNMP Trap for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#snmp-server host <i>ip-address version 3 { authnpriv authpriv noauthnpriv } username [udpport udpport]</i>	(Optional) configure the SNMPv3 Trap target host.
3	Raisecom(config)#snmp-server host <i>ip-address version { 1 2c } community-name [udpport udpport]</i>	(Optional) configure the SNMPv1/SNMPv2c Trap target host.
4	Raisecom(config)#snmp-server enable traps	Enable Trap.

13.1.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show snmp access</code>	Show SNMP access group configurations.
2	<code>Raisecom#show snmp community</code>	Show SNMP community configurations.
3	<code>Raisecom#show snmp config</code>	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.
4	<code>Raisecom#show snmp group</code>	Show the mapping between SNMP users and the access group.
5	<code>Raisecom#show snmp host</code>	Show Trap target host information.
6	<code>Raisecom#show snmp statistics</code>	Show SNMP statistics.
7	<code>Raisecom#show snmp user</code>	Show SNMP user information.
8	<code>Raisecom#show snmp view</code>	Show SNMP view information.
9	<code>Raisecom#show snmp server-auth</code>	Show SNMP server authentication configurations.

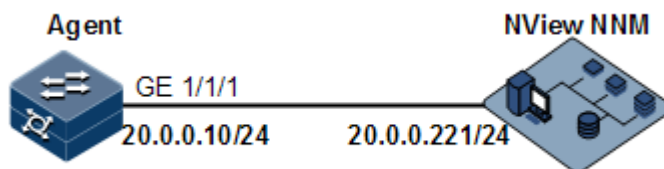
13.1.10 Example for configuring SNMPv1/SNMPv2c and Trap

Networking requirements

As shown in Figure 13-3, the route between the NView NNM system and the ISCOM3000G series switch is available. The NView NNM system can check the MIB under view corresponding to the remote Switch by SNMPv1/SNMPv2c, and the ISCOM3000G series switch can send Trap automatically to the NView NNM system in emergency.

By default, there is VLAN 1 on the ISCOM3000G series switch and all physical interfaces belong to VLAN 1.

Figure 13-3 SNMPv1/SNMPv2c networking



Configuration steps

Step 1 Configure the IP address of the ISCOM3000G 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.

```
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
Category
-----
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:       --
Type:       include
...
```

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
```

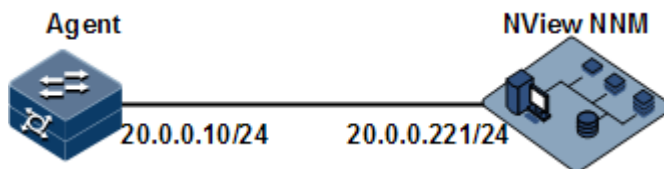
13.1.11 Example for configuring SNMPv3 and Trap

Networking requirements

As shown in Figure 13-4, the route between the NView NNM system and ISCOM3000G series switch is available, the NView NNM system monitors the Agent through SNMPv3, and the ISCOM3000G 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 ISCOM3000G series switch and all physical interfaces belong to VLAN 1.

Figure 13-4 SNMPv3 and Trap networking



Configuration steps

Step 1 Configure the IP address of the ISCOM3000G 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.x.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
```

Checking results

Use the **show snmp access** command to show configurations of the SNMP access group.

```
Raisecom#show snmp access
```

...

```
Index:          1
Group:          guestgroup
Security Model: usm
Security Level: authnopriv
Context Prefix: --
```



```
Context Match: exact
Read View:     mib2
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.

```
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
```

13.2 KeepAlive

13.2.1 Introduction

The KeepAlive packet is a kind of KeepAlive mechanism running in High-level Data Link Control (HDLC) link layer protocol. The ISCOM3000G series switch will send a KeepAlive packet to confirm whether the peer is online periodically to implement the neighbor detection mechanism.

Trap is the unrequested information sent by the ISCOM3000G series switch actively to the NView NNM system, used to report some urgent and important events.

The Switch sends KeepAlive Trap actively which includes the basic information about RC551E (device name, device OID, MAC address and IP address) to the NView NNM system. Network management synchronizes device information by IP to make the NView NNM system discover fault in a short time, improve working efficiency and reduce working load of administrators.

13.2.2 Preparing for configurations

Scenario

The ISCOM3000G series switch sends KeepAlive packet to make network management discover segment in a short time, improve working efficiency, and reduce the working load of administrators. You can configure the switch to enable or disable the KeepAlive transmission and its period. When enabled with KeepAlive Trap switch, configure with snmp enable traps and Layer 3 IP address, the Switch will send a KeepAlive Trap alarm message to all target hosts with Bridge Trap every KeepAlive Trap Interval.

Prerequisite

- Configure basic functions of SNMP. SNMPv1 and v2c need to configure the community name; SNMPv3 needs to configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the ISCOM3000G series switch and NMS is reachable.

13.2.3 Default configurations of KeepAlive

Default configurations of KeepAlive are as below.

Function	Default value
KeepAlive Trap	Disable
KeepAlive Trap period	300s

13.2.4 Configuring KeepAlive

Configure KeepAlive for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#snmp-server keepalive-trap enable</code>	Enable KeepAlive Trap.
3	<code>Raisecom(config)#snmp-server keepalive-trap interval <i>period</i></code>	(Optional) configure the period for sending KeepAlive Trap.



Caution

To avoid multiple devices sending KeepAlive Trap at the same time according to the same period and causing heavy network management load, configure the real transmission period for sending KeepAlive Trap in random transmission of $period+5s$ period.

13.2.5 Checking configurations

Use the following commands to check configuration results.

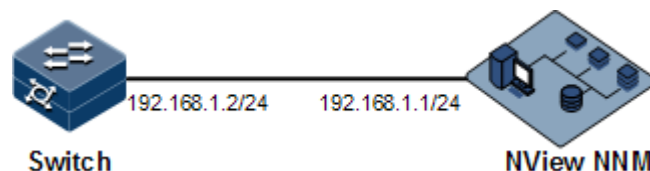
No.	Command	Description
1	<code>Raisecom#show keepalive</code>	Show KeepAlive configurations.

13.2.6 Example for configuring KeepAlive

Networking requirements

As shown in Figure 13-5, the IP address of the Switch is 192.168.1.2, the IP address of the SNMPv2c Trap target host is 192.168.1.1, the name of the read-write community is public, and the SNMP version is v2c. Configure the interval for sending KeepAlive Trap from the Switch to SNMP network management station as 120s, and enable sending KeepAlive Trap.

Figure 13-5 KeepAlive networking



Configuration steps

Step 1 Configure the IP address of the Switch.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 192.168.1.2 255.255.255.0
Raisecom(config-vlan1)#exit
```

Step 2 Configure the IP address of the Trap target host for SNMP.

```
Raisecom(config)#snmp-server host 192.168.1.1 version 2c public
```

Step 3 Configure sending KeepAlive Trap.

```
Raisecom(config)#snmp-server keepalive-trap enable
Raisecom(config)#snmp-server keepalive-trap interval 120
```

Checking results

Use the **show keepalive** command to show KeepAlive configurations.

```
Raisecom#show keepalive
Keepalive Admin State:Enable
keepalive trap interval:120s
keepalive trap count:2
```

13.3 RMON

13.3.1 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 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.

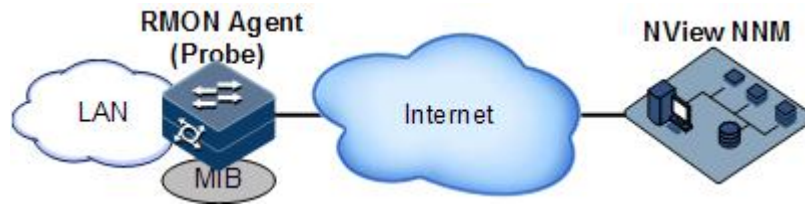
The RMON Agent is commonly referred to as the probe program. The RMON Probe can take the communication subnet statistics and performance analysis. Whenever it finds network failure, RMON Probe can report the NView NNM system, and describes the capture information under unusual circumstances so that the 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. Network management center 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. Network management center will collect network management information through the basic operation of SNMP and the exchange data information about RMON Agent.

The Raisecom ISCOM3000G series switch is embedded with RMON. As shown in Figure 13-6, the ISCOM3000G 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.

Figure 13-6 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:** gather statistics on each interface, including receiving packets accounts and size distribution statistics.
- **History group:** similar with statistic group, it only gather statistics in an assigned detection period.
- **Alarm group:** monitor an assigned MIB object, configure upper threshold and lower threshold in assigned time interval, and trigger an event if the monitor object receives threshold value.
- **Event group:** cooperating with the alarm group. When an alarm triggers an event, it records the event, such as sending Trap, and writes the event into log.

13.3.2 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 ISCOM3000G series switch actively sends alarms when the threshold is exceeded without obtaining variable information. This helps reduce traffic of the Central Office (CO) and managed devices and facilitates network management.

Prerequisite

The route between the ISCOM3000G series switch and the NView NNM system is reachable.

13.3.3 Default configurations of RMON

Default configurations of RMON are as below.

Function	Default value
Statistics group	Enable on all interfaces
History group	Disable
Alarm group	N/A
Event group	N/A

13.3.4 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 ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# rmon statistics interface-type interface-list [owner owner-name]	Enable RMON statistics on an interface and configure related parameters.



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.

13.3.5 Configuring RMON historical statistics

Configure RMON historical statistics for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# rmon history interface-type interface-list [shortinterval short-period] [longinterval long-period] [buckets buckets-number] [owner owner-name]	Enable RMON historical statistics on an interface and configure related parameters.



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.

13.3.6 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 wish to monitor the variable again.

By default, the triggered event number is 0; namely, 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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#rmon alarm alarm-id mibvar [interval period] { absolute delta } rising-threshold rising-value [rising-event-id] falling-threshold falling-value [falling-event-id] [owner owner-name]</code>	Add alarm instances to the RMON alarm group and configure related parameters.

13.3.7 Configuring RMON event group

Configure the RMON event group for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#rmon event event-id [log] [trap] [description string] [owner owner-name]</code>	Add events to the RMON event group and configure processing modes of events.

13.3.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show rmon</code>	Show RMON configurations.
2	<code>Raisecom#show rmon alarms</code>	Show information about the RMON alarm group.
3	<code>Raisecom#show rmon events</code>	Show information about the RMON event group.

No.	Command	Description
4	Raisecom# show rmon statistics [<i>interface-type interface-list</i>]	Show information about the RMON statistics group.
5	Raisecom# show rmon history <i>interface-type interface-list</i>	Show information about the RMON history group.

13.3.9 Maintenance

Maintain the ISCOM3000G series switch as below.

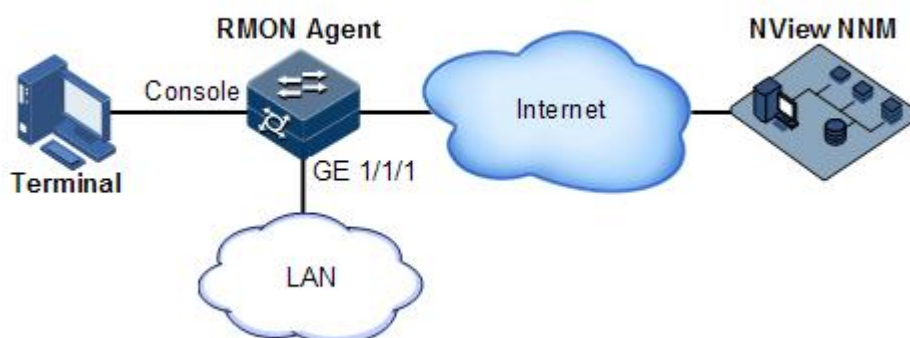
Command	Description
Raisecom(config)# clear rmon	Clear all RMON configurations.

13.3.10 Example for configuring RMON alarm group

Networking requirements

As shown in Figure 13-7, the ISCOM3000G 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 Port 3 exceeds the threshold in a period, logs are recorded and Trap is sent.

Figure 13-7 RMON networking



Configuration steps

- Step 1 Create an event with index ID 1, used to record and send logs with description string HighIfOutErrors. The owner of logs is system.

```
Raisecom#config
```



```
Raisecom(config)#rmon event 1 log description High-ifOutErrors owner system
```

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 ISCOM3000G series switch.

```
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 events** command to check whether there is information about alarm group on the ISCOM3000G series switch.

```
Raisecom#show rmon events
Event group information:
Event 1 is active, owned by system
Event description: high.
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.

13.4 LLDP

13.4.1 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. Network management system 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 network management system querying and judging link communication.

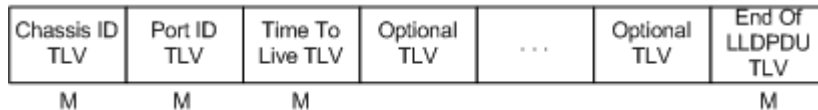
LLDP packet

The LLDP packet is 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.

As shown in Figure 13-8, LLDPDU is made by several TLV, including 4 mandatory TLV and several optional TLV.

Figure 13-8 Structure of a LLDPDU



M - mandatory TLV required for all LLDPDUs

As shown in Figure 13-9, each TLV denotes a piece of information at local. For example the device ID and interface number correspond with the Chassis ID TLV and Port ID TLV.

Figure 13-9 Structure of a TLV packet

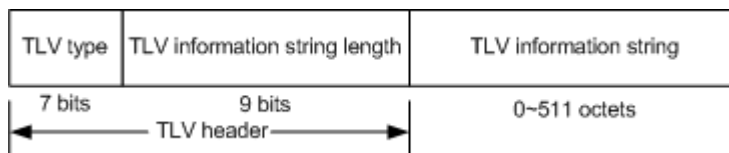


Table 13-1 lists TLV types. At present only types 0-8 are used.

Table 13-1 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

TLV type	Description	Optional/Required
5	System name	Optional
6	System description	Optional
7	System capabilities	Optional
8	Management address	Optional

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 ISCOM3000G series switch sends a LLDP packet to the peer. To avoid sending LLDP packet continuously because of device status changes frequently, you can configure a delay timer for sending the LLDP packet.

The aging time of Time To Live (TTL) of local device information in the neighboring node can be adjusted by modifying the parameter values of aging coefficient, sends LLDP packets to neighboring node, after receiving LLDP packets, neighboring node will adjust the aging time of its neighboring nodes (sending side) information. Aging time formula, $TTL = \text{Min} \{65535, (\text{interval} \times \text{hold-multiplier})\}$:

- Interval indicates the time period to send LLDP packets from neighboring node.
- Hold-multiplier refers to the aging coefficient of device information in neighboring node.

13.4.2 Preparing for configurations

Scenario

When you obtain connection information between devices through NView NNM system for topology discovery, the ISCOM3000G 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

13.4.3 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 packet	0180.c200.000e

13.4.4 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 ISCOM3000G 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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#lldp enable</code>	Enable global LLDP.

13.4.5 Enabling interface LLDP

Enable interface LLDP for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-gigaethernet1/1/1)#lldp enable</code>	Enable LLDP on an interface.

13.4.6 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 ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#lldp message-transmission interval <i>period</i></code>	(Optional) configure the period timer of the LLDP packet.
3	<code>Raisecom(config)#lldp message-transmission delay <i>period</i></code>	(Optional) configure the delay timer of the LLDP packet.
4	<code>Raisecom(config)#lldp message-transmission hold-multiplier <i>hold-multiplier</i></code>	(Optional) configure the aging coefficient of the LLDP packet.
5	<code>Raisecom(config)#lldp restart-delay <i>period</i></code>	(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.

13.4.7 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 LLDP alarm for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#lldp trap-interval <i>period</i></code>	(Optional) configure the period of the timer for sending LLDP alarm Traps.

13.4.8 Configuring TLV

Configure TLV for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.

Step	Command	Description
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config- gigaethernet1/1/1)#lldp tlv- select basic-tlv {all port- description system-capability system-name system- description }</code>	Configure the basic TLV allowed to issue.
4	<code>Raisecom(config- gigaethernet1/1/1)#lldp tlv- select med-tlv {all capability inventory network- policy location-id }</code>	Configure the MED TLV allowed to issue.
5	<code>Raisecom(config- gigaethernet1/1/1)#lldp tlv- select dot1-tlv {all port- vlan-id vlan-name }</code>	Enable 802.1 TLV type allowed to issue.
6	<code>Raisecom(config- gigaethernet1/1/1)#lldp tlv- select dot3-tlv { all link- aggregation mac-physic max- frame-size power }</code>	Enable 802.3 TLV type allowed to issue.

13.4.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show lldp local config</code>	Show LLDP local configurations.
2	<code>Raisecom#show lldp local system-data [interface-type interface-number]</code>	Show information about the LLDP local system.
3	<code>Raisecom#show lldp remote [interface-type interface- number] [detail]</code>	Show information about the LLDP neighbor.
4	<code>Raisecom#show lldp statistic [interface-type interface- number]</code>	Show statistics about LLDP packets.
5	<code>Raisecom#show lldp tlv-select [interface-type interface- number]</code>	Show information about the optional TLV sent by the interface.

13.4.10 Maintenance

Maintain the ISCOM3000G series switch as below.

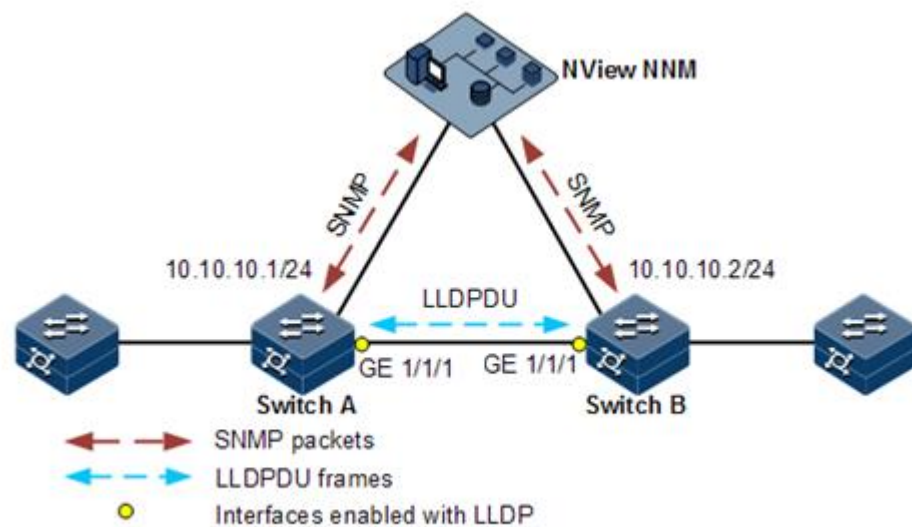
Command	Description
Raisecom(config)# clear lldp statistic <i>interface-type interface-number</i>	Clear LLDP statistics.
Raisecom(config)# clear lldp remote-table [<i>interface-type interface-number</i>]	Clear LLDP neighbor information.
Raisecom(config)# clear lldp global statistic	Clear global LLDP statistics.

13.4.11 Example for configuring LLDP

Networking requirements

As shown in Figure 13-10, 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 13-10 LLDP networking



Configuration steps

Step 1 Enable global LLDP and LLDP alarm.

Configure Switch A.

```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#lldp enable
```

Configure Switch B.

```
Raisecom#name 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 1
SwitchA(config-vlan1)#ip address 10.10.10.1 255.255.255.0
SwitchA(config-vlan1)#exit
```

Configure Switch B.

```
SwitchB(config)#create vlan 1024 active
SwitchB(config)#interface gigaethernet1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport access vlan 1024
SwitchB(config)#interface vlan 1
SwitchB(config-vlan1)#ip address 10.10.10.2 255.255.255.0
SwitchB(config-vlan1)#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
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.C200.000E
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

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

.....

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

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**

Port	ChassisId	PortId	SysName	MgtAddress	ExpiredTime
------	-----------	--------	---------	------------	-------------

```

gigaehternet1/1/1 000E.5E02.B010    gigaehternet1/1/1    SwitchB
10.10.10.2    106
.....
SwitchB#show tldp remote
Port          ChassisId    PortId    SysName    MgtAddress    ExpiredTime
-----
gigaehternet1/1/1 000E.5E12.F120 gigaehternet1/1/1    SwitchA
10.10.10.1 106
.....

```

13.5 Optical module DDM

13.5.1 Introduction

Optical module Digital Diagnostics Monitoring (DDM) on the ISCOM3000G 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 analyzes 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.

13.5.2 Preparing for configurations

Scenario

Fault diagnostics f optical modules provide a detection method to 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

N/A

13.5.3 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	Enable
Global optical DDM Trap	Disable
Interface optical DDM Trap	Disable
Interface optical DDM password check	Disable

13.5.4 Enabling optical module DDM

Enable optical module DDM for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#transceiver ddm enable	Enable SFP DDM globally.
3	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
4	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 ISCOM3000G series switch perform DDM.

13.5.5 Enabling optical module DDM Trap

Enable optical module DDM Trap for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#snmp-server trap transceiver enable	Enable optical module DDM Trap globally.
3	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
4	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 ISCOM3000G series switch send Traps.

13.5.6 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.

13.6 System log

13.6.1 Introduction

The system log refers that the ISCOM3000G series switch records the system information and debugging information in a log and sends the log to the specified destination. When the ISCOM3000G 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 13-2.

Table 13-2 Log levels

Severity	Level	Description
Emergency	0	The system cannot be used.

Severity	Level	Description
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, namely, the severity ranges from emergencies to errors, can be sent.

13.6.2 Preparing for configurations

Scenario

The ISCOM3000G series switch generates the 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

13.6.3 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	Disable. The fixed 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).

Function	Default value
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	<ul style="list-style-type: none"> • Debug: no timestamp to debug level (7) Syslog information. • Log: The timestamp to 0–6 levels Syslog information is absolute time.

13.6.4 Configuring basic information of system log

Configure basic information of system log for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#logging on</code>	(Optional) enable system log.
3	<code>Raisecom(config)#logging time-stamp { debug log } { datetime none uptime }</code>	<p>(Optional) configure timestamp for system log.</p> <p>The optional parameter debug is used to assign debug level (7) system log timestamp; by default, this system log does not have timestamp</p> <p>The optional parameter log is used to assign debug level 0–6 system log timestamp; by default, this system log adopts date-time as timestamp.</p>
4	<code>Raisecom(config)#logging rate-limit log-num</code>	(Optional) configure transmitting rate of system log.
5	<code>Raisecom(config)#logging sequence-number</code>	<p>(Optional) configure sequence of system log.</p> <p>The sequence number only applies to the console, monitor, log file, and log buffer, but not log host and history list.</p>
6	<code>Raisecom(config)#logging discriminator discriminator-number { facility mnemonics msg-body } { { drops includes } key none }</code>	<p>(Optional) create and configure system log filter.</p> <p>The filter can filter output log from the console, monitor, log file and log buffer.</p>

Step	Command	Description
7	Raisecom(config)# logging buginf [high normal low none]	(Optional) configure sending Debug-level logs.

13.6.5 Configuring system log output

Configure system log output for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# logging console [<i>log-level</i> alerts critical debugging emergencies errors informational notifications warnings distriminator <i>distriminator-number</i>]	(Optional) output system logs to the console.
3	Raisecom(config)# logging host ip-address [<i>log-level</i> alerts critical debugging emergencies errors informational notifications warnings distriminator <i>distriminator-number</i>]	(Optional) output system logs to the log host. Up to 10 log hosts are supported.
	Raisecom(config)# logging [<i>host ip-address</i>] facility { alert audit auth clock cron daemon ftp kern local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news ntp sercurity syslog user uucp }	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 ISCOM3000G series switch.
4	Raisecom(config)# logging monitor [<i>log-level</i> alerts critical debugging emergencies errors informational notifications warnings distriminator <i>distriminator-number</i>]	(Optional) output system logs to the monitor.
5	Raisecom(config)# logging file [discriminator <i>discriminateor-number</i>]	(Optional) output system logs to the Flash of the ISCOM3000G series switch. Only warning-level logs are available.

Step	Command	Description
6	Raisecom(config)#logging buffered [<i>log-level</i> alerts critical debugging emergencies errors informational notifications warnings distriminator <i>distriminator-number</i>]	(Optional) output system logs to the buffer.
	Raisecom(config)#logging buffered size <i>size</i>	(Optional) configure the system log buffer size.
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 <i>size</i>	(Optional) configure the log history list size.
	Raisecom(config)#logging trap [<i>log-level</i> alerts critical debugging emergencies errors informational notifications warnings distriminator <i>distriminator-number</i>]	(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.

13.6.6 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.
5	Raisecom#show logging history	Show information about the system log history list.

13.6.7 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom(config)#clear logging buffer	Clear log information in the buffer.

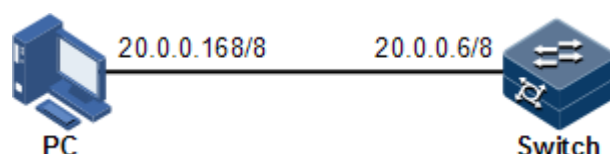
Command	Description
<code>Raisecom(config)#clear logging statistics</code>	Clear log statistics.

13.6.8 Example for configuring outputting system logs to log host

Networking requirements

As shown in Figure 13-11, configure system log, and output device log information to log host for user to check.

Figure 13-11 Networking of outputting system log to log host



Configuration steps

Step 1 Configure the IP address of the ISCOM3000G 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.

```

Raisecom#show logging
Syslog logging:          enable
Dropped Log messages:   0
Dropped debug messages: 0
Rate-limited:           2 messages per second
Sequence 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
  
```

13.7 Alarm management

13.7.1 Introduction

Alarm means when a fault is generated on the ISCOM3000G series switch or some working condition changes, the system will generate alarm information 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 information is generated to log information. If a Network Management System (NMS), the alarm information will be sent to network management system through SNMP. The information sent to the NMS is called Trap information.

Alarm classification

There are three kinds of alarm information according to properties of an alarm:

- 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.
- 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.

The alarm information 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 information output modes:

- Alarm buffer: alarm information is recorded in tabular form, including the current alarm table and history alarm table.
 - Current alarm table, recording alarm information which is not cleared, acknowledged or restored.
 - History alarm table, consisting of acknowledged and restored alarm information, recording the cleared, auto-restored or manually acknowledged alarm information.
- Log: alarm information is generated to system log when recorded in the alarm buffer, and stored in the alarm log buffer.
- Trap information: alarm information sent to NMS when the NMS is configured.

Alarm will be broadcasted according to various terminals configured by the ISCOM3000G series switch, including CLI terminal and NMS.

Log output of alarm information starts with the symbol "#", and the output format is as below:

```
#Index TimeStamp HostName ModuleName/Severity/name:Arise From Description.
```

Table 13-3 lists alarm fields.

Table 13-3 Alarm fields

Field	Description
TimeStamp	Time when an alarm is generated
ModuleName	Name for a module where alarms are generated
Severity	Alarm level
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 13-4.

Table 13-4 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 ISCOM3000G 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 ISCOM3000G series switch can effectively reduce the number of alarms.

Alarm A and alarm B will be recorded on the ISCOM3000G 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 ISCOM3000G 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 information, or report the alarm when there is no alarm information. 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 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; namely, 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 and changes to non-reverse alarm mode so that the alarm status can be reported normally in the next alarm.

- Auto-reverse mode

Configure the alarm reverse mode as auto-reverse mode. If the interface has not actual reverse alarm currently, the configuration will return fail; if the interface has actual reverse alarm, the configuration is success and enter reverse mode, i.e. the interface reported alarm status is changed opposite to the actual alarm status immediately. After the alarm is finished, the enabling state of interface alarm reverse will ends automatically and changes to non-reverse alarm mode so that the alarm state can be reported normally in next alarm.

- Alarm delay

Alarm delay refers that the ISCOM3000G 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 when 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 information and take rolling records.

Use configured storage mode to deal with new generated alarm information when the alarm information 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 information directly on the ISCOM3000G series switch. If the ISCOM3000G series switch is configured with NView NNM system, the administrator can monitor alarms on the NView NNM system.

13.7.2 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 information 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:

- In Syslog output mode: alarms will be generated into system logs. When you need to send alarm information 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.

13.7.3 Configuring basic functions of alarm management

Configure basic information of alarm management for the ISCOM3000G series switch as below.

All following steps are optional and in any sequence.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#alarm auto-report all enable	Enable alarm auto-reporting.
	Raisecom(config)#alarm auto-report alarm-restore alarm-restore-value enable	Enable alarm auto-reporting of a specified alarm source.
	Raisecom(config)#alarm auto-report type alarm-type enable	Enable alarm auto-reporting of a specified alarm type.
	Raisecom(config)#alarm auto-report type alarm-type alarm-restore alarm-restore-value enable	Enable alarm auto-reporting of a specified alarm source and type.
3	Raisecom(config)#alarm monitor all enable	Enable alarm monitoring.
	Raisecom(config)#alarm monitor alarm-restore alarm-restore-value enable	Enable alarm monitoring of a specified alarm source.
	Raisecom(config)#alarm monitor type alarm-type enable	Enable alarm monitoring of a specified alarm type.
	Raisecom(config)#alarm monitor type alarm-type alarm-restore alarm-restore-value enable	Enable alarm monitoring of a specified alarm source and type.
4	Raisecom(config)#alarm inverse interface-type interface-number { none auto manual }	Configure alarm reverse modes. By default, it is none; namely, alarm reverse is disabled.
5	Raisecom(config)#alarm { active cleared } delay second	Configure alarm delay. By default, it is 0s.
6	Raisecom(config)#alarm active storage-mode { loop stop }	Configure alarm storage modes. By default, it is stop.
7	Raisecom(config)#alarm clear all	(Optional) clear all current alarms.
	Raisecom(config)#alarm clear index index	(Optional) clear current alarms of the specified alarm index.

Step	Command	Description
	<code>Raisecom(config)#alarm clear <i>alarm-restype alarm-restype-value</i></code>	(Optional) clear current alarms of the specified alarm source.
	<code>Raisecom(config)#alarm clear type <i>alarm-type</i></code>	(Optional) clear current alarms of the specified alarm type.
	<code>Raisecom(config)#alarm clear type <i>alarm-type alarm-restype alarm-restype-value</i></code>	(Optional) clear current alarms of the specified alarm source and type.
8	<code>Raisecom(config)#alarm syslog enable</code>	(Optional) enable alarms to be output to system logs. By default, it is disabled.
9	<code>Raisecom(config)#exit</code> <code>Raisecom#show alarm active</code> <code>[<i>module_name</i> severity <i>severity</i>]</code>	(Optional) show information about current alarms.
	<code>Raisecom#show alarm cleared</code> <code>[<i>module_name</i> severity <i>severity</i>]</code>	(Optional) show information about historical alarms.



Note

You can enable/disable alarm monitoring, alarm auto-reporting, and alarm clearing on modules that support alarm management.

13.7.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show alarm management</code> <code>[<i>alarm_type</i>]</code>	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	<code>Raisecom#show alarm log</code>	Show alarm statistics in the system log.
3	<code>Raisecom#show alarm management statistics</code>	Show statistics about alarm management module.
4	<code>Raisecom#show alarm active</code>	Show information about current alarms.

13.8 Hardware environment monitoring

13.8.1 Introduction

Hardware environment monitoring mainly refers to monitor the running environment of the ISCOM3000G series switch. The monitoring alarm events include:

- Power supply state alarm
- Temperature beyond threshold alarm
- Voltage beyond threshold alarms
- Abnormal interface status 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 network management center.
- Output to the relay fault indication LED.

You can take appropriate measures to prevent failure when alarm events happen.

Alarm events

- Power supply monitoring alarms

Power supply state alarms include 2 types.

- Power supply voltage anomaly alarm

An alarm is generated when the power supply voltage is 20% greater than the pre-configured voltage (12 V) or is 20% smaller than the pre-configured voltage (12 V). In addition, an alarm is generated when the voltage value returns to normal state. The ISCOM3000G 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.

- Power supply state change alarms

Power supply state change refers that unplugged power supply is plugged into the device and vice versa. The ISCOM3000G series switch supports dual power supplies. Therefore, power 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 users that power supply 1/power supply 2 changes. The ISCOM3000G 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, namely, two power modules are out of position. The ISCOM3000G 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 ISCOM3000G 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 ISCOM3000G 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.

- Voltage beyond threshold alarm

The device supports voltage beyond threshold alarm event, when the current voltage is lower than low voltage threshold, the low voltage alarm event will generate. The ISCOM3000G 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 current voltage value of the monitored voltage is greater than the threshold, a high voltage alarm is generated. The ISCOM3000G 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.



Note

The ISCOM3000G series switch monitors 3.3V master chip voltage only.

- Interface status alarm

Each interface has two alarm events:

- Interface link-fault alarm: link failure alarm refers to the peer link signal loss. The alarm event only aims at optical port, but not power port.
- Interface link-down alarm: interface status Down alarm.

The ISCOM3000G series switch supports saving these two types of alarm events 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 information 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 information 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 network management center 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 13-5 describes Trap information.

Table 13-5 Trap information

Field	Description
Alarm status	<ul style="list-style-type: none"> • asserted (current alarm) • cleared (alarm recovery) • clearall (clear all alarm information)
Alarm source	<ul style="list-style-type: none"> • device (global alarm) • Interface number (interface status alarm)
Timestamp	Alarm time, in the form of absolute time
Alarm event type	<ul style="list-style-type: none"> • 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) • high-volt (high-voltage alarm) • low-volt (low-voltage alarm) • link-down (interface LinkDown alarm) • link-falut (interface LinkFault alarm) • all-alarm (clear all alarm information)

- Syslog output

Record alarm information to Syslog.

Syslog output has global switch and all monitored alarm events still have their own Syslog alarm output switches. When enabling the global switch and monitored alarm events switches simultaneously, the alarm will generate Syslog output.

Table 13-6 describes Syslog information.

Table 13-6 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 13-2.
Mnemonics	Alarm event type. For details, see Table 13-5.
Msg-body	Main body, describing alarm event contents.

- Relay output

"Outputting to relay" or "Outputting from relay" indicates outputting alarms to the relay and fault indication LED simultaneously. The relay and fault indication LED are bound together.

Relay output and fault indicate LED output are controlled by the relay alarm output switch. As a public fault output mode for all alarms, the relation among all alarms is logical "OR".

If any alarm is generated on the ISCOM3000G series switch, the device outputs the alarm from the relay. The relay cannot work properly unless all alarms are cleared.

Relay output cannot be enabled globally. Relay output is enabled for every monitored alarm.

13.8.2 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. When you need to send alarm information to the system log host, please configure system log host IP address for the device.
- In Trap output mode: please configure network management center IP address for the device.
- In relay output mode: relay alarm output switch is enabled for every alarm.

13.8.3 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	Disable
Power down event alarm	<ul style="list-style-type: none"> • Enable Trap output. • Enable Syslog system log output. • Enable relay output.
Temperature alarm output	
Voltage alarm output	
Interface link-down event alarm output	<ul style="list-style-type: none"> • Enable Trap output. • Enable Syslog system log output. • Disable relay output.
Interface link-fault event alarm output	<ul style="list-style-type: none"> • Disable Trap output. • Disable Syslog system log output. • Disable relay output.
High temperature alarm threshold	102 ℃
Low temperature alarm threshold	-40 ℃

Function	Default value
High voltage threshold	3450 mV
Low voltage threshold	3150 mV

13.8.4 Enabling global hardware environment monitoring

Enable global hardware environment monitoring for the ISCOM3000G 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	(Optional) enable 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.
- When enabling global hardware environment monitoring alarm Relay output, alarm event can generate Relay only when Relay output under alarm event is also enabled.


13.8.5 Configuring temperature monitoring alarm

Configure temperature monitoring alarm for the ISCOM3000G series switch as below.

Step	Command	Description
1	raisecom#config	Enter global configuration mode.
2	raisecom(config)#alarm temperature { high <i>high-value</i> low <i>low-value</i> notifies syslog }	Enable temperature monitoring alarm output and configure temperature monitoring alarm output modes. <ul style="list-style-type: none"> • The high temperature threshold (high-value) must be greater than the low temperature threshold (low-value). • The low temperature threshold (low-value) must be smaller than the high temperature threshold (high-value).


13.8.6 Configuring voltage monitoring alarm

Configure voltage monitoring alarm for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)# alarm voltage { high <i>high-value</i> low <i>low-value</i> notifies syslog }</code>	Enable voltage alarm output and configure voltage alarm output modes or voltage alarm threshold.  Note The ISCOM3000G series switch monitors 3.3V master chip voltage only.

13.8.7 Clearing all hardware environment monitoring alarms manually

Clear all hardware environment monitoring alarms manually for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#conf ig</code>	Enter global configuration mode.
2	<code>Raisecom(conf ig)#clear alarm</code>	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.

13.8.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show alarm</code>	Show global hardware environment monitoring alarm configurations.
2	<code>Raisecom#show alarm current</code>	Show current alarms of hardware environment monitoring.
3	<code>Raisecom#show alarm history</code>	Show historic alarms of hardware environment monitoring.

No.	Command	Description
4	<code>Raisecom#show environment [temperature voltage]</code>	Show current power supply, temperature, voltage alarms, and current environment information.

13.9 CPU monitoring

13.9.1 Introduction

The ISCOM3000G 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.

13.9.2 Preparing for configurations

Scenario

CPU monitoring can give realtime monitoring to task state, CPU utilization rate and stack usage in the system, provide CPU utilization rate threshold alarm, detect and eliminate hidden dangers, or help the administrator for locating faults.

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.

13.9.3 Default configurations of CPU monitoring

Default configurations of CPU monitoring are as below.

Function	Default value
CPU utilization rate alarm Trap output	Enable
Rising threshold of CPU utilization alarm	99%
Restoration threshold of CPU utilization alarm	79%
Sampling period of CPU utilization	60s

13.9.4 Showing CPU monitoring information

Show CPU monitoring information for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#show cpu-utilization [dynamic history { 10min 1min 2hour 5sec }]</code>	Show CPU utilization.
2	<code>Raisecom#show process [cpu sorted { priority name } taskname]</code>	Show statuses of all tasks.
3	<code>Raisecom#show process cpu [sorted [10min 1min 5sec invoked]]</code>	Show CPU utilization of all tasks.
4	<code>Raisecom#show process dead</code>	Show information about dead tasks.
5	<code>Raisecom#show process pid range</code>	Show information about the specified task.

13.9.5 Configuring CPU monitoring alarm

Configure CPU monitoring alarm for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#cpu threshold falling falling-threshold-value rising rising-threshold-value</code>	(Optional) configure the recovering threshold and rising threshold for CPU alarms.
3	<code>Raisecom(config)#cpu interval interval-value</code>	(Optional) configure the interval for sampling CPU alarms.

13.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show cpu-utilization</code>	Show CPU utilization and related configurations.

13.10 Cable diagnosis

13.10.1 Introduction

The ISCOM3000G series switch supports cable diagnosis, which helps you detect lines.

Cable diagnosis contains the following results:

- Time for last cable diagnosis
- Detection result of the Tx cable
- Errored location of the Tx cable
- Detection result of the Rx cable
- Errored location of the Rx cable

13.10.2 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

13.10.3 Configuring cable diagnosis

Configure cable diagnosis for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#test cable-diagnostics interface-type interface-number</code>	Enable cable diagnosis.

13.10.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show cable-diagnostics [interface-type interface-number]</code>	Show results of cable diagnosis.

13.11 Memory monitoring

13.11.1 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.

13.11.2 Configuring memory monitoring

Configure memory monitoring for the ISCOM3000G series switch as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#memory threshold recovering recovering-threshold-value rising rising-threshold-value</code>	(Optional) configure the recovering threshold and rising threshold for memory utilization alarms.
3	<code>Raisecom(config)#memory interval observation- interval-value</code>	(Optional) configure the interval for sampling memory alarms.

13.11.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show memory</code>	Show memory information.

13.12 Fan monitoring

13.12.1 Introduction

The ISCOM3000G series switch supports monitoring the fan, including the rotational speed and temperature. It sends Trap when the rotational speed or temperature is abnormal.

The ISCOM3000G 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.

13.12.2 Preparing for configurations

Scenario

In hot environment, too high temperature affects heat dissipation of the ISCOM3000G series switch. Thus fan monitoring must be configured so that the rotational speed is automatically adjusted according to environment temperature and the ISCOM3000G series switch runs properly.

Precondition

N/A

13.12.3 Configuring fan monitoring

Configure fan monitoring for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#fan-monitor mode { auto enforce }	Configure the monitoring mode for the rotational speed. By default, it is auto.
3	Raisecom(config)#fan-monitor enforce level <i>level</i>	(Optional) configure the rotational speed in enforced mode.
4	Raisecom(config)#fan-monitor temperature-scale <i>temperature1 temperature2 temperature3</i>	(Optional) configure the temperature range for different rotational speeds in automatic monitoring mode.
5	Raisecom(config)#fan-monitor trap send enable	(Optional) enable Trap sending for fan monitoring.

13.12.4 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.

13.13 Performance statistics

13.13.1 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.

- Performance based on interface:
 - Short/Long period performance statistics on the interface: the interfaces include service interfaces and management interfaces.
 - Data saving for short/long period performance statistics on the interface: the interfaces include service interfaces and management interfaces. Data is saved in the Flash in a configured period.
- Performance based on service flow:
 - Short/Long period performance statistics about a service flow: the statistics can be based on the service VLAN or priority.
 - Data saving for short/long period performance statistics about a service flow: the statistics can be based on the service VLAN or priority. Data is saved in the Flash in a configured period.

13.13.2 Preparing for configurations

Scenario

To learn performance of the ISCOM3000G series switch, you can use performance statistics to gather current or historical statistics about packets based on interface or service flow.

Prerequisite

N/A

13.13.3 Default configurations of performance statistics

Default configurations of performance statistics are as below.

Function	Default value
Performance statistics	Enable
Number of saved data blocks	16

13.13.4 Configuring performance statistics

Configure performance statistics for the ISCOM3000G series switch as below.

Step	Command	Description
1	raisecom#config	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#performance statistics interval buckets <i>buckets-number</i>	Configure the number of data blocks saved in the Flash.

13.13.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show performance statistics interval buckets Raisecom#show performance statistics interface <i>interface-type interface-number</i> { current history }	Show performance statistics.

13.13.6 Maintenance

Maintain the ISCOM3000G series switch as below.

Command	Description
Raisecom(config)#clear performance statistics history	Clear performance statistics.

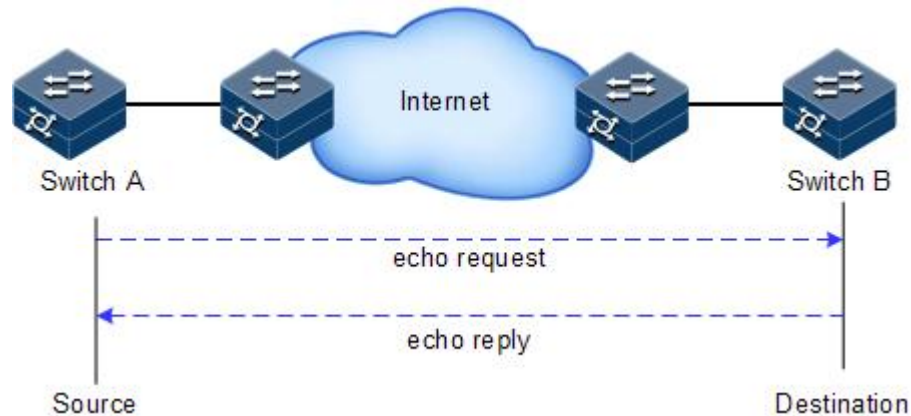
13.14 Ping

13.14.1 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 13-12 shows principles of Ping.

Figure 13-12 Principles of Ping



13.14.2 Configuring Ping

Configure Ping for the ISCOM3000G series switch as below.

Step	Command	Description
1	Raisecom# ping <i>ip-address</i> [count <i>count</i>] [size <i>size</i>] [waittime <i>period</i>] [source <i>ip-address</i>]	(Optional) test the connectivity of the IPv4 network by the ping command.
2	Raisecom# ping ipv6 <i>ipv6-address</i> [count <i>count</i>] [size <i>size</i>] [waittime <i>period</i>]	(Optional) test the connectivity of the IPv6 network by the ping command.



Note

The ISCOM3000G 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**.

13.15 Traceroute

13.15.1 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

The following shows how Traceroute works:

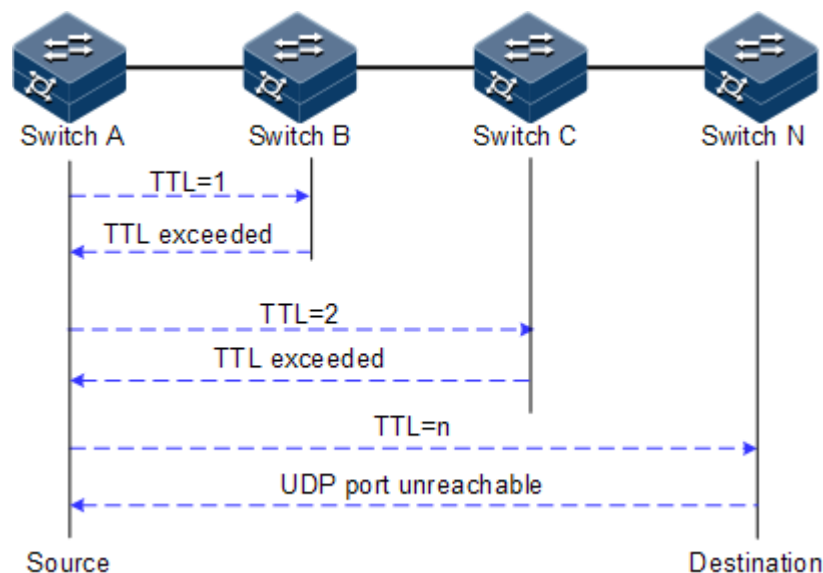
- First, send a piece of TTL1 sniffer packet (where the UDP port ID of the packet is unavailable to any application programs in destination side).
- TTL deducts 1 when reaching the first hop. Because the TTL value is 0, in the first hop the device returns an ICMP timeout packet, indicating that this packet cannot be sent.
- The sending host adds 1 to TTL and resends this packet.

- 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 ID of destination host is not 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 13-13 shows principles of Traceroute.

Figure 13-13 Principles of Traceroute



13.15.2 Configuring Traceroute

Before using Traceroute, you should configure the IP address and default gateway of the ISCOM3000G series switch.

Configure Traceroute for the ISCOM3000G series switch as below.

Step	Command	Description
1	<pre>Raisecom#tracertoute ip-address [firstttl first-ttl] [maxttl max-ttl] [port port-number] [waittime period] [count times] [size size]</pre>	(Optional) test the connectivity of the IPv4 network and view nodes passed by the packet by the tracertoute command.
2	<pre>Raisecom#tracertoute ipv6 ipv6- address [firstttl first-ttl] [maxttl max-ttl] [port port- id] [waittime second] [count times] [size size]</pre>	(Optional) test the connectivity of the IPv6 network and view nodes passed by the packet by the tracertoute command.

14 Appendix

This chapter lists terms, acronyms, and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

14.1 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, 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, namely, 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
---------	----------------------------------------------------------------------------------------

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 on 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 on 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

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.

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 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.
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 on 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 insecure.
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.

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 rate, bit error rate, and signal-to-noise ratio.

R

Rapid Spanning Tree Protocol (RSTP) Evolution of the Spanning Tree Protocol (STP), which provides improvements in the rate of convergence for bridged networks

Remote Authentication Dial In User Service (RADIUS) RADIUS refers to a protocol used to authenticate and account users on 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 on the network.

Single-Mode Fiber (SMF) In this fiber, single-mode optical signals are transmitted.

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.

14.2 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

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	

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

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

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
RED	Random Early Detection
RH	Relative Humidity
RIP	Routing Information Protocol
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	
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

