

www.raisecom.com

ISCOM S2600 Series
Configuration Guide (CLI)
(Rel_01)

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 ©2023

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 a warranty of any kind, express or implied.

Preface

Objectives

This document describes features supported by the device, and related configurations, including basic configurations, basic principles and configuration procedures of Ethernet, ring network protection, 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 device, and how to network with the device.

Versions

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

Product name	Software version	Hardware version
ISCOM S2600 series switch	V7.01	–

Conventions

Symbol conventions

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

Symbol	Description
 Warning	Indicate a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
 Caution	Indicate a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
 Note	Provide additional information to emphasize or supplement important points of the main text.

Symbol	Description
	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 paths 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 01 (2023-09-28)

Initial commercial release

Contents

1 Basic configurations	1
1.1 Time management	1
1.1.1 Introduction.....	1
1.1.2 Preparing for configurations	4
1.1.3 Configuring NTP	5
1.1.4 Configuring SNTP	6
1.1.5 Checking configurations	7
1.1.6 Example for configuring NTP.....	8
1.2 Interface management	10
1.2.1 Introduction.....	10
1.2.2 Default configurations of interface management	11
1.2.3 Configuring basic attributes of interfaces	11
1.2.4 Configuring interface rate statistics	12
1.2.5 Configuring flow control on interfaces	13
1.2.6 Shutting down/Restarting the interface	13
1.2.7 Checking configurations	13
2 Ethernet	14
2.1 MAC address table	14
2.1.1 Introduction.....	14
2.1.2 Preparing for configurations	16
2.1.3 Default configurations of MAC address table.....	17
2.1.4 Configuring the static MAC address.....	17
2.1.5 Configuring the blackhole MAC address.....	17
2.1.6 Configuring MAC address learning	17
2.1.7 Configuring the MAC address limit.....	18
2.1.8 Configuring the aging time of MAC addresses.....	18
2.1.9 MAC address flapping detection and protection	18
2.1.10 Checking configurations	19
2.1.11 Maintenance	20
2.1.12 Example for configuring the MAC address table.....	20
2.2 VLAN.....	22
2.2.1 Introduction.....	22

2.2.2	Preparing for configurations	24
2.2.3	Default configurations of VLAN	25
2.2.4	Configuring VLAN attributes	25
2.2.5	Configuring the interface mode	25
2.2.6	Configuring the VLAN on the Access interface	26
2.2.7	Configuring the VLAN on the Trunk interface	26
2.2.8	Configuring the VLAN based on the Hybrid interface	27
2.2.9	Configuring the VLAN based on MAC address	28
2.2.10	Configuring the VLAN based on IP subnet	28
2.2.11	Configuring the VLAN based on protocol	28
2.2.12	Checking configurations	29
2.2.13	Example for configuring VLANs.....	29
2.3	Voice VLAN.....	32
2.3.1	Introduction.....	32
2.3.2	Preparing for configurations	33
2.3.3	Default configurations of the voice VLAN.....	33
2.3.4	Configuring the OUI	34
2.3.5	Enabling the voice VLAN.....	34
2.3.6	Checking configurations	34
2.3.7	Example for adding interfaces to the voice VLAN	35
2.3.8	Example for configuring the IP phone to access voice VLAN packets through LLDP	36
2.4	QinQ.....	38
2.4.1	Introduction.....	38
2.4.2	Preparing for configurations	39
2.4.3	Default configurations of QinQ	40
2.4.4	Configuring basic QinQ	40
2.4.5	Configuring selective QinQ	40
2.4.6	Configuring the network-side interface to Trunk mode	41
2.4.7	Configuring the TPID	41
2.4.8	Checking configurations	41
2.4.9	Example for configuring basic QinQ	42
2.4.10	Example for configuring selective QinQ	43
2.5	VLAN mapping.....	45
2.5.1	Introduction.....	45
2.5.2	Preparing for configurations	45
2.5.3	Default configurations of VLAN mapping	46
2.5.4	Configuring VLAN mapping	46
2.5.5	Checking configurations	47
2.5.6	Example for configuring VLAN mapping	47
2.6	MRP/VRP	49
2.6.1	Introduction.....	49
2.6.2	Preparing for configurations	52

2.6.3 Default configurations.....	52
2.6.4 Configuring basic functions of MVRP.....	52
2.6.5 Checking configurations	53
2.6.6 Example for configuring MVRP	53
3 IP services	57
3.1 IP basis	57
3.1.1 Introduction.....	57
3.1.2 Preparing for configurations	57
3.1.3 Default configurations of VLAN interface	57
3.1.4 Configuring the IPv4 address of the VLAN interface.....	58
3.1.5 Configuring the IPv6 address of the interface.....	58
3.1.6 Checking configurations	59
3.1.7 Example for configuring the VLAN interface to interconnect with the host	59
3.2 Loopback interface.....	61
3.2.1 Introduction.....	61
3.2.2 Preparing for configurations	61
3.2.3 Default configurations of the Loopback interface.....	61
3.2.4 Configuring the IP address of the Loopback interface	61
3.2.5 Checking configurations	62
3.3 ARP	62
3.3.1 Introduction.....	62
3.3.2 Preparing for configurations	63
3.3.3 Default configurations of ARP	63
3.3.4 Configuring static ARP entries.....	63
3.3.5 Configuring dynamic ARP entries	63
3.3.6 Checking configurations	64
3.3.7 Maintenance.....	64
3.3.8 Example for configuring ARP.....	64
3.4 NDP.....	66
3.4.1 Introduction.....	66
3.4.2 Preparing for configurations	67
3.4.3 Default configurations of NDP	67
3.4.4 Configuring static neighbor entries.....	68
3.4.5 Configuring the aging time of dynamic NDPs.....	68
3.4.6 Checking configurations	68
3.4.7 Maintenance.....	68
3.5 Static route	69
3.5.1 Introduction.....	69
3.5.2 Preparing for configurations	69
3.5.3 Configuring the static route.....	69
3.5.4 Checking configurations	70

3.5.5 Example for configuring the static route	70
4 DHCP.....	73
4.1 ZTP.....	73
4.1.1 Introduction.....	73
4.1.2 Default configurations of ZTP	74
4.1.3 Preparing for configuration.....	74
4.1.4 Configuring ZTP	75
4.1.5 Checking configurations	75
4.2 DHCP Client	75
4.2.1 Introduction.....	75
4.2.2 Preparing for configurations	78
4.2.3 Default configurations of DHCP Client	78
4.2.4 Configuring DHCP Client	78
4.2.5 Checking configurations	79
4.2.6 Example for configuring DHCP Client	79
4.3 DHCP Server.....	81
4.3.1 Introduction.....	81
4.3.2 Preparing for configurations	83
4.3.3 Creating and configuring the IPv4 address pool	84
4.3.4 Enabling DHCP Server on the interface.....	84
4.3.5 Recycling the IP address pool	85
4.3.6 Configuring DHCPv4 Server PING	85
4.3.7 Checking configurations	85
4.3.8 Maintenance	85
4.3.9 Example for configuring DHCPv4 Server	86
4.4 DHCP Relay	87
4.4.1 Introduction.....	87
4.4.2 Preparing for configurations	88
4.4.3 Default configurations of DHCP Relay.....	88
4.4.4 Configuring interface DHCP Relay	89
4.4.5 Configuring interface DHCPv6 Relay	89
4.4.6 Configuring DHCP Relay to support Option 82	89
4.4.7 Configuring DHCP Relay to support Option 18/37	90
4.4.8 Checking configurations	91
4.4.9 Maintenance	91
4.4.10 Example for configuring DHCPv4 Relay	91
5 QoS.....	93
5.1 Introduction.....	93
5.1.1 Service models	93
5.2 Priority mapping.....	94
5.2.1 Introduction.....	94

5.2.2 Preparing for configurations	95
5.2.3 Default configurations of basic QoS	95
5.2.4 Configuring types of priorities trusted by the ingress interface	99
5.2.5 Configuring the diffserv profile	99
5.2.6 Configuring IEEE 802.1p/DSCP remarking on the egress interface	100
5.2.7 Checking configurations	101
5.3 Queue scheduling	101
5.3.1 Introduction	101
5.3.2 Preparing for configurations	102
5.3.3 Default configurations of congestion management	103
5.3.4 Configuring SP queue scheduling	103
5.3.5 Configuring WRR or SP+WRR queue scheduling	103
5.3.6 Configuring DRR or SP+DRR queue scheduling	104
5.3.7 Configuring queue bandwidth guarantee	104
5.3.8 Checking configurations	104
5.3.9 Maintenance	105
5.3.10 Example for configuring queue scheduling	105
5.4 Congestion avoidance	106
5.4.1 Introduction	106
5.4.2 Preparing for configurations	107
5.4.3 Default configurations of congestion avoidance	107
5.4.4 Configuring WRED	107
5.4.5 Checking configurations	108
5.5 Rate limiting	108
5.5.1 Introduction	108
5.5.2 Preparing for configurations	109
5.5.3 Configuring the rate limiting mode	109
5.5.4 Configuring rate limiting based on physical interface	109
5.5.5 Configuring rate limiting based on VLAN	110
5.5.6 Configuring rate limiting based on LAG	110
5.5.7 Checking configurations	110
5.5.8 Example for configuring rate limiting based on interface	111
5.6 Bandwidth rate limiting	112
5.6.1 Introduction	112
5.6.2 Preparing for configurations	113
5.6.3 Default configurations of bandwidth rate limiting	113
5.6.4 Configuring bandwidth guarantee	113
5.6.5 Checking configurations	116
6 Multicast	118
6.1 Multicast	118
6.2 IGMP Snooping	123

6.2.1 Introduction.....	123
6.2.2 Preparing for configurations	124
6.2.3 Default configurations of IGMP Snooping	124
6.2.4 Configuring basic functions of IGMP Snooping.....	125
6.2.5 Configuring IGMP Snooping Querier	125
6.2.6 Configuring IGMP Snooping packet suppression	126
6.2.7 Configuring IGMP Snooping multicast copy	126
6.2.8 Configuring the static multicast member of IGMP Snooping	127
6.2.9 Configuring IGMP Snooping Proxy.....	127
6.2.10 Configuring the limit on the number of IGMP Snooping interface multicast groups	128
6.2.11 Configuring the multicast policy of IGMP Snooping.....	128
6.2.12 Configuring IGMP Snooping SSM Mapping.....	128
6.2.13 Checking configurations	129
6.2.14 Maintenance	129
6.2.15 Example for configuring basic functions of IGMP Snooping	130
6.2.16 Example for configuring the static member of IGMP Snooping.....	131
6.2.17 Example for configuring IGMP Snooping multicast copy	134
6.2.18 Example for configuring IGMP Snooping Proxy.....	136
6.2.19 Example for configuring the multicast policy of IGMP Snooping.....	138
6.3 MLD Snooping.....	140
6.3.1 Introduction.....	140
6.3.2 Preparing for configurations	141
6.3.3 Default configurations of MLD Snooping	141
6.3.4 Configuring basic functions of MLD Snooping.....	142
6.3.5 Configuring MLD Snooping Querier.....	142
6.3.6 Configuring MLD Snooping packet suppression.....	143
6.3.7 Configuring MLD Snooping multicast copy	143
6.3.8 Configuring the static multicast member of MLD Snooping	144
6.3.9 Configuring MLD Snooping Proxy	144
6.3.10 Configuring the limit on the number of MLD Snooping interface multicast groups	144
6.3.11 Configuring the multicast policy of MLD Snooping.....	145
6.3.12 Configuring MLD Snooping SSM Mapping.....	145
6.3.13 Checking configurations	146
6.3.14 Maintenance	146
6.3.15 Example for configuring basic functions of MLD Snooping	146
6.3.16 Example for configuring the static member of MLD Snooping.....	148
6.3.17 Example for configuring MLD Snooping multicast copy	151
6.3.18 Example for configuring MLD Snooping Proxy.....	153
6.3.19 Example for configuring the multicast policy of MLD Snooping.....	155
7 OAM	158
7.1 Introduction.....	158

7.2 EFM	160
7.2.1 Introduction.....	160
7.2.2 Preparing for configurations	160
7.2.3 Default configurations of EFM	160
7.2.4 Configuring basic functions of EFM.....	161
7.2.5 Configuring CFM interface loopback	162
7.2.6 Configuring EFM link performance monitoring	163
7.2.7 Configuring EFM link fault detection.....	164
7.2.8 Checking configurations	164
7.2.9 Maintenance	165
7.3 Link-state tracking	165
7.3.1 Introduction.....	165
7.3.2 Preparing for configurations	165
7.3.3 Default configurations of link-state tracking	166
7.3.4 Configuring link-state tracking	166
7.3.5 Checking configurations	167
7.3.6 Example for configuring link-state tracking	167
7.4 VRRP	169
7.4.1 Introduction.....	169
7.4.2 Preparing for configurations	171
7.4.3 Default configurations of VRRP	172
7.4.4 Configuration flow	172
7.4.5 Configuring the VRRP backup group	172
7.4.6 Configuring the VRRP6 backup group	174
7.4.7 Configuring VRRP Trap.....	175
7.4.8 Configuring the VRRP monitoring interface	176
7.4.9 Configuring BFD for VRRP	176
7.4.10 Checking configurations	177
7.5 CFM	177
7.5.1 Introduction.....	177
7.5.2 Preparing for configurations	180
7.5.3 Default configurations of CFM	180
7.5.4 Configuring basic functions of CFM	181
7.5.5 Configuring fault detection	182
7.5.6 Configuring fault acknowledgement.....	182
7.5.7 Configuring fault location	183
7.5.8 Configuring alarm inhibition	183
7.5.9 Configuring the one-way packet loss test	184
7.5.10 Configuring the round-trip delay test	184
7.5.11 Checking configurations	185
7.5.12 Maintenance	185
7.5.13 Example for configuring CFM.....	185

8 Security	191
8.1 ACL	191
8.1.1 Introduction	191
8.1.2 Preparing for configurations	192
8.1.3 Configuring the ACL	192
8.1.4 Applying the ACL	194
8.1.5 Configuring statistics	195
8.1.6 Configuring the ACL IP list	195
8.1.7 Checking configurations	196
8.1.8 Maintenance	196
8.2 AAA	197
8.2.1 Introduction	197
8.2.2 Preparing for configurations	198
8.2.3 Default configurations of AAA	198
8.2.4 Configuring the RADIUS server	199
8.2.5 Configuring the TACACS+ server	200
8.2.6 Configuring the AAA server group	200
8.2.7 Configuring the AAA mode	201
8.2.8 Checking configurations	201
8.2.9 Example for configuring AAA	201
8.3 802.1x	204
8.3.1 Introduction	204
8.3.2 Preparing for configurations	206
8.3.3 Default configurations of 802.1x	207
8.3.4 Configuring basic functions of 802.1x	207
8.3.5 Configuring 802.1x re-authentication	208
8.3.6 Configuring 802.1x timers	209
8.3.7 Checking configurations	209
8.3.8 Example for configuring 802.1x	210
8.4 PPPoE+	212
8.4.1 Introduction	212
8.4.2 Preparing for configurations	213
8.4.3 Default configurations of PPPoE+	213
8.4.4 Configuring basic functions of PPPoE+	214
8.4.5 Configuring PPPoE+ packets	214
8.4.6 Checking configurations	216
8.4.7 Maintenance	216
8.4.8 Example for configuring PPPoE+	217
8.5 Port security MAC	219
8.5.1 Introduction	219
8.5.2 Preparing for configurations	220
8.5.3 Default configurations of port security MAC	220

8.5.4 Configuring basic functions of port security MAC	220
8.5.5 Configuring the sticky secure MAC address.....	221
8.5.6 Checking configurations	222
8.5.7 Maintenance	222
8.5.8 Example for configuring port security MAC	222
8.6 Storm suppression and storm control	224
8.6.1 Introduction.....	224
8.6.2 Preparing for configurations	225
8.6.3 Default configurations of storm suppression and storm control	226
8.6.4 Configuring storm suppression	226
8.6.5 Checking configurations	227
8.6.6 Example for configuring storm suppression	227
8.6.7 Configuring storm control.....	229
8.6.8 Checking configurations	229
8.6.9 Example for configuring storm control	230
8.7 ARP attack protection.....	231
8.7.1 Preparing for configurations	231
8.7.2 Default configurations of ARP attack protection	231
8.7.3 Configuring ARP	231
8.7.4 Checking configurations	233
8.7.5 Example for configuring ARP attack protection	233
8.8 ND Snooping.....	235
8.8.1 Introduction.....	235
8.8.2 Preparing for configurations	236
8.8.3 Default configurations of ND Snooping	236
8.8.4 Configuring ND Snooping	236
8.8.5 Checking configurations	237
8.8.6 Maintenance.....	237
8.8.7 Example for configuring ND Snooping	237
8.9 DHCP Snooping	239
8.9.1 Introduction.....	239
8.9.2 Preparing for configurations	240
8.9.3 Default configurations of DHCP Snooping.....	241
8.9.4 Configuring DHCP Snooping	241
8.9.5 Configure DHCP Snooping to support Option 82.....	242
8.9.6 Configuring DHCPv6 Snooping	242
8.9.7 Checking configurations	243
8.9.8 Maintenance	243
8.9.9 Example for configuring DHCP Snooping.....	244
8.10 IP Source Guard	245
8.10.1 Introduction.....	245
8.10.2 Preparing for configurations	247

8.10.3 Default configurations of IP Source Guard	247
8.10.4 Configuring IP Source Guard binding.....	247
8.10.5 Configuring the interface trust status of IP Source Guard.....	247
8.10.6 Checking configurations	248
8.10.7 Example for configuring IP Source Guard	248
8.11 CPU attack protection	250
8.11.1 Preparing for configurations.....	250
8.11.2 Configuring CPU attack protection.....	250
8.11.3 Checking configurations	251
8.11.4 Maintenance	251
9 Reliability	252
9.1 Link aggregation	252
9.1.1 Introduction.....	252
9.1.2 Preparing for configurations	253
9.1.3 Default configurations of link aggregation	253
9.1.4 Configuring manual link aggregation	254
9.1.5 Configuring static LACP link aggregation.....	254
9.1.6 Configuring master/slave link aggregation	255
9.1.7 Configuring the load balancing algorithm for the LAG	256
9.1.8 Checking configurations	256
9.1.9 Example for configuring static LACP link aggregation	257
9.2 G.8032.....	259
9.2.1 Introduction.....	259
9.2.2 Preparing for configurations	264
9.2.3 Default configurations of G.8032	265
9.2.4 Creating a G.8032 ring.....	265
9.2.5 Creating a G.8032 tributary ring	267
9.2.6 Configuring G.8032 switching control.....	268
9.2.7 Checking configurations	269
9.2.8 Maintenance.....	269
9.2.9 Example for configuring single ring G.8032	270
9.2.10 Example for configuring intersecting G.8032	272
9.3 STP/RSTP	276
9.3.1 Introduction.....	276
9.3.2 Preparation for configuration	278
9.3.3 Default configurations of STP	278
9.3.4 Enabling STP	279
9.3.5 Configuring STP parameters.....	279
9.3.6 Configuring the RSTP edge interface	280
9.3.7 Configuring the RSTP link type.....	280
9.3.8 Checking configurations	281

9.3.9 Example for configuring STP	281
9.4 MSTP	284
9.4.1 Introduction.....	284
9.4.2 Preparation for configuration	287
9.4.3 Default configurations of MSTP	287
9.4.4 Enabling MSTP.....	288
9.4.5 Configuring the MST region and its maximum number of hops	288
9.4.6 Configuring the root/backup bridge	289
9.4.7 Configuring the interface priority and system priority	290
9.4.8 Configuring the path cost of the interface	291
9.4.9 Configuring the maximum transmission rate on interface	291
9.4.10 Configuring the MSTP timer.....	291
9.4.11 Configuring the edge interface.....	292
9.4.12 Configuring BPDU filtering.....	293
9.4.13 Configuring BPDU Guard.....	293
9.4.14 Configuring STP/RSTP/MSTP mode switching	294
9.4.15 Configuring the link type	294
9.4.16 Configuring root interface isolation	295
9.4.17 Configuring interface loopguard	295
9.4.18 Configuring TC packet suppression	296
9.4.19 Configuring TC protection.....	296
9.4.20 Checking configurations	297
9.4.21 Maintenance	297
9.4.22 Example for configuring MSTP.....	297
9.5 Loop detection.....	301
9.5.1 Introduction.....	301
9.5.2 Preparing for configurations	303
9.5.3 Default configurations of loop detection.....	303
9.5.4 Configuring loop detection	303
9.5.5 Checking configurations	304
9.5.6 Example for configuring inner loop detection	304
9.6 Interface backup	306
9.6.1 Introduction.....	306
9.6.2 Preparing for configurations	308
9.6.3 Default configurations of interface backup	308
9.6.4 Configuring basic functions of interface backup	308
9.6.5 Configuring FS on interfaces	309
9.6.6 Checking configurations	309
9.6.7 Example for configuring interface backup.....	310
9.7 Interface isolation.....	312
9.7.1 Introduction.....	312
9.7.2 Preparing for configurations	312

9.7.3 Default configurations of interface isolation.....	312
9.7.4 Configuring interface isolation	313
9.7.5 Checking configurations	313
9.7.6 Example for configuring interface isolation.....	313
10 System management.....	316
10.1 SNMP.....	316
10.1.1 Introduction.....	316
10.1.2 Preparing for configurations	318
10.1.3 Default configurations of SNMP	318
10.1.4 Configuring basic functions of SNMPv1/SNMPv2c	319
10.1.5 Configuring basic functions of SNMPv3	319
10.1.6 Configuring other information about SNMP	321
10.1.7 Configuring Trap.....	322
10.1.8 Checking configurations	322
10.1.9 Example for configuring SNMPv1/SNMPv2c and Trap	323
10.1.10 Example for configuring SNMPv3 and Trap	325
10.2 RMON.....	327
10.2.1 Introduction.....	327
10.2.2 Preparing for configurations	328
10.2.3 Default configurations of RMON	328
10.2.4 Configuring RMON statistics	329
10.2.5 Configuring RMON history statistics	329
10.2.6 Configuring the RMON alarm group	329
10.2.7 Configuring the RMON event group	330
10.2.8 Checking configurations	330
10.2.9 Example for configuring the RMON alarm group	331
10.3 LLDP.....	333
10.3.1 Introduction.....	333
10.3.2 Preparing for configurations	335
10.3.3 Default configurations of LLDP	335
10.3.4 Enabling global LLDP	336
10.3.5 Enabling interface LLDP	336
10.3.6 Configuring basic functions of global LLDP	337
10.3.7 Configuring basic functions of interface LLDP	338
10.3.8 Configuring the LLDP alarm	338
10.3.9 Configuring TLV	338
10.3.10 Checking configurations	339
10.3.11 Maintenance	340
10.3.12 Example for configuring LLDP	340
10.4 Port mirroring.....	343
10.4.1 Introduction.....	343

10.4.2 Preparing for configurations	344
10.4.3 Default configurations of port mirroring.....	344
10.4.4 Configuring port mirroring	345
10.4.5 Default configurations of VLAN mirroring	345
10.4.6 Configuring VLAN mirroring.....	346
10.4.7 Checking configurations	346
10.4.8 Example for configuring port mirroring.....	347
10.5 Cable diagnosis	348
10.5.1 Introduction.....	348
10.5.2 Preparing for configurations	348
10.5.3 Configuring cable diagnosis.....	348
10.5.4 Checking configurations	349
10.6 UDLD.....	349
10.6.1 Introduction.....	349
10.6.2 Preparing for configurations	349
10.6.3 Default configurations of UDLD	350
10.6.4 Configuring UDLD	350
10.6.5 Checking configurations	351
10.7 Optical module DDM.....	352
10.7.1 Introduction.....	352
10.7.2 Preparing for configurations	352
10.7.3 Default configurations of optical module DDM	352
10.7.4 Enabling optical module DDM	352
10.7.5 Enabling optical module DDM Trap.....	353
10.7.6 Checking configurations	354
10.8 System log	354
10.8.1 Introduction.....	354
10.8.2 Preparing for configurations	355
10.8.3 Default configurations of system log	356
10.8.4 Configuring basic information about the system log	356
10.8.5 Configuring system log output.....	356
10.8.6 Checking configurations	357
10.8.7 Maintenance	358
10.8.8 Example for configuring outputting system logs to the log host.....	358
10.9 Alarm management	359
10.9.1 Preparing for configurations	359
10.9.2 Configuring basic functions of alarm management	360
10.9.3 Checking configurations	360
10.10 CPU monitoring	361
10.10.1 Introduction.....	361
10.10.2 Preparing for configurations	361
10.10.3 Default configurations of CPU monitoring	362

10.10.4 Configuring the CPU monitoring alarm.....	362
10.10.5 Checking configurations	362
10.11 Memory monitoring	363
10.11.1 Preparing for configurations.....	363
10.11.2 Configuring memory monitoring	363
10.11.3 Checking configurations	363
10.12 PING	364
10.12.1 Introduction.....	364
10.12.2 Configuring PING.....	364
10.13 Trace.....	365
10.13.1 Introduction.....	365
10.13.2 Configuring IPv4 Trace.....	366
10.13.3 Configuring IPv6 Trace.....	367
10.14 Hardware monitoring	367
10.14.1 Introduction.....	367
10.14.2 Configuring temperature monitoring	367
10.14.3 Configuring power supply monitoring.....	368
10.14.4 Checking configurations	368
10.15 Fan monitoring.....	369
10.15.1 Introduction.....	369
10.15.2 Preparing for configurations	369
10.15.3 Configuring fan monitoring	369
10.15.4 Checking configurations	370
11 Appendix	371
11.1 Terms.....	371
11.2 Acronyms and abbreviations	376

Figures

Figure 1-1 Basic principles of NTP.....	3
Figure 1-2 NTP networking	8
Figure 2-1 Forwarding packets according to the MAC address table	15
Figure 2-2 MAC networking.....	21
Figure 2-3 VLAN partitions	22
Figure 2-4 VLAN and interface isolation networking.....	30
Figure 2-5 Networking for IP phone to connect to switch	33
Figure 2-6 Networking with adding interface to voice VLAN and configuring it to work in manual mode	35
Figure 2-7 Configuring IP phone to access voice VLAN packets through LLDP.....	37
Figure 2-8 Principles of basic QinQ.....	38
Figure 2-9 Basic QinQ networking	42
Figure 2-10 Selective QinQ networking	44
Figure 2-11 Principles of VLAN mapping	45
Figure 2-12 VLAN mapping networking	48
Figure 2-13 Principles of MVRP	51
Figure 2-14 MVRP networking.....	54
Figure 3-1 VLAN interface networking	59
Figure 3-2 Configuring ARP networking	65
Figure 3-3 Principles of NDP address resolution	67
Figure 3-4 Configuring the static route	71
Figure 4-1 ZTP server networking	74
Figure 4-2 DHCP typical networking.....	76
Figure 4-3 Structure of a DHCP packet	76
Figure 4-4 DHCP Client networking.....	78
Figure 4-5 DHCP Client networking.....	80
Figure 4-6 DHCP Server and Client networking.....	82

Figure 4-7 Structure of a DHCP packet	82
Figure 4-8 DHCP Server networking	86
Figure 4-9 Typical application of DHCP Relay	88
Figure 4-10 DHCP Relay networking	92
Figure 5-1 SP scheduling	101
Figure 5-2 WRR scheduling.....	102
Figure 5-3 DRR scheduling.....	102
Figure 5-4 Queue scheduling networking	105
Figure 5-5 Rate limiting based on interface	111
Figure 6-1 Multicast transmission networking.....	119
Figure 6-2 Basic concepts in multicast.....	120
Figure 6-3 Mapping between IPv4 multicast address and multicast MAC address	121
Figure 6-4 Operating of IGMP and Layer 2 multicast features	122
Figure 6-5 IGMP Snooping networking.....	124
Figure 6-6 Configuring basic functions of IGMP Snooping	130
Figure 6-7 Configuring the static member of IGMP Snooping	132
Figure 6-8 Configuring IGMP Snooping multicast copy	134
Figure 6-9 Configuring IGMP Snooping Proxy	136
Figure 6-10 Configuring the multicast policy of IGMP Snooping	138
Figure 6-11 MLD Snooping networking	141
Figure 6-12 Configuring basic functions of MLD Snooping	147
Figure 6-13 Configuring the static member of MLD Snooping.....	149
Figure 6-14 Configuring MLD Snooping multicast copy	151
Figure 6-15 Configuring MLD Snooping Proxy	153
Figure 6-16 Configuring the multicast policy of MLD Snooping.....	155
Figure 7-1 OAM loopback	159
Figure 7-2 Link-state tracking networking.....	167
Figure 7-3 VRRP principles	170
Figure 7-4 Principles of VRRP load balancing	171
Figure 7-5 MDs at different levels	178
Figure 7-6 MEP and MIP	179
Figure 7-7 Typical CFM networking.....	186
Figure 8-1 Domain-based authentication application networking.....	202

Figure 8-2 802.1x structure	204
Figure 8-3 Dot1x networking.....	210
Figure 8-4 Accessing the network through PPPoE authentication	212
Figure 8-5 PPPoE+ networking.....	217
Figure 8-6 Port security MAC networking.....	223
Figure 8-7 Storm suppression networking	228
Figure 8-8 DAI networking.....	234
Figure 8-9 ND Snooping networking.....	238
Figure 8-10 DHCP Snooping	240
Figure 8-11 DHCP Snooping networking	244
Figure 8-12 Principles of IP Source Guard	246
Figure 8-13 Configuring IP Source Guard	249
Figure 9-1 Static LACP mode Link aggregation networking.....	257
Figure 9-2 G.8032 ring networking.....	260
Figure 9-3 Idle state	262
Figure 9-4 Protecting state	262
Figure 9-5 Tributary ring.....	263
Figure 9-6 Single ring G.8032 networking.....	270
Figure 9-7 Intersecting ring G.8032 networking	273
Figure 9-8 Network storm due to loopback.....	276
Figure 9-9 Loop networking with STP.....	277
Figure 9-10 Failure in forwarding VLAN packets due to RSTP	278
Figure 9-11 STP networking	281
Figure 9-12 Basic concepts of the MSTI network.....	285
Figure 9-13 MSTI concepts.....	286
Figure 9-14 Networking with multiple spanning trees instances in MST region	287
Figure 9-15 MSTP networking.....	298
Figure 9-16 Loop detection networking	302
Figure 9-17 Loop detection networking	305
Figure 9-18 Principles of interface backup	307
Figure 9-19 Networking with interface backup in different VLANs	308
Figure 9-20 Interface backup networking	310
Figure 9-21 Interface isolation networking	314

Figure 10-1 Principles of SNMP	317
Figure 10-2 SNMPv3 authentication mechanism.....	320
Figure 10-3 SNMPv1/SNMPv2c networking	323
Figure 10-4 SNMPv3 and Trap networking	325
Figure 10-5 RMON networking.....	328
Figure 10-6 RMON networking.....	331
Figure 10-7 Structure of a LLDPDU.....	333
Figure 10-8 Structure of a TLV packet.....	334
Figure 10-9 LLDP networking	341
Figure 10-10 Principles of port mirroring	344
Figure 10-11 Port mirroring networking	347
Figure 10-12 Networking of outputting system log to log host	358
Figure 10-13 Principles of PING.....	364
Figure 10-14 Principles of Trace.....	366

Tables

Table 2-1 Interface mode and packet processing.....	23
Table 4-1 Fields of a DHCP packet	76
Table 4-2 Fields of a DHCP packet	82
Table 5-1 Default mapping from the IEEE 802.1p ingress direction to local priority and color	96
Table 5-2 Default mapping from the IEEE 802.1p egress direction to local priority and color	96
Table 5-3 Default mapping from the DSCP ingress direction to local priority and color	97
Table 5-4 Default mapping from the DSCP egress direction to local priority and color	98
Table 10-1 TLV types	334
Table 10-2 IEEE 802.1 organization-defined TLVs	334
Table 10-3 IEEE 802.3 organization-defined TLVs	334
Table 10-4 Log levels	355

1 Basic configurations

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

- Time management
- Interface management

1.1 Time management

1.1.1 Introduction

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

To ensure precise system time, the device 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 device 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 device.

DST

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

The device 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 1-1 shows basic principles of NTP. Clock synchronization works as below:

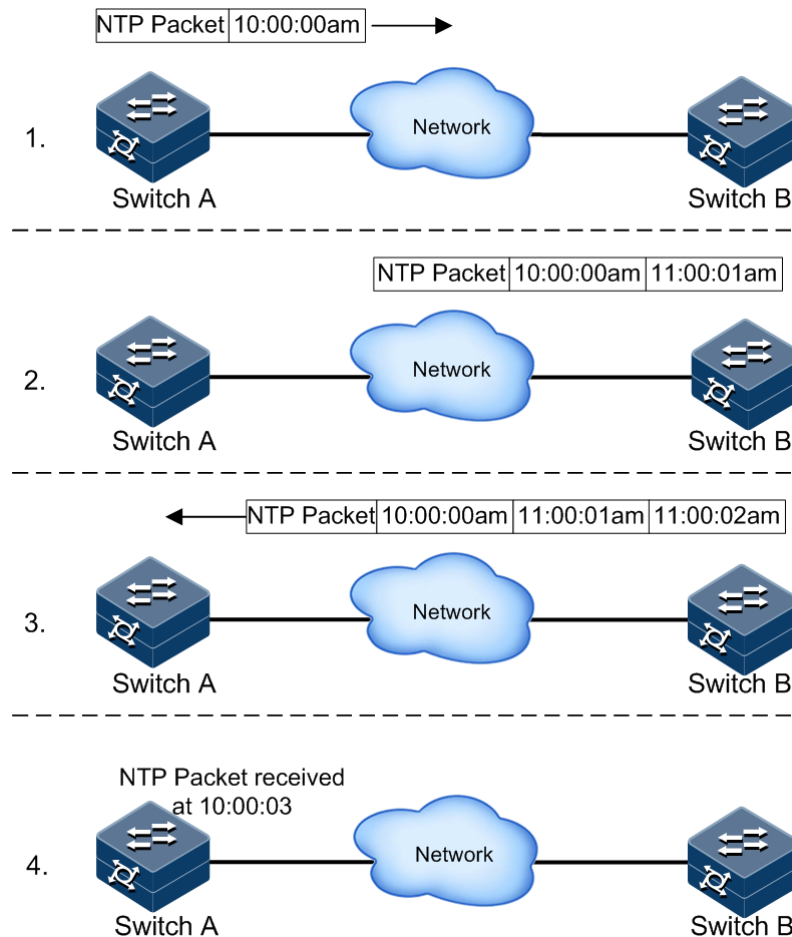
- Step 1 Switch A sends Switch B a NTP message which carries the timestamp of leaving Switch A. The timestamp is 10:00:00am and recorded as t1.
- Step 2 When the message reaches Switch B, it is added with the timestamp of reaching Switch B, which is 11:00:01am and recorded as t2.
- Step 3 When the message 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 1-1 Basic principles of NTP



The device adopts multiple NTP working modes for time synchronization:

- Client/Server mode

In this mode, the client sends clock synchronization messages to different servers. After receiving the synchronization message, the server sends the response message. 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 time only but the server cannot be synchronized to the client time. The device cannot work as both a client and a server.

- Symmetric mode

In this mode, you can configure the device to be synchronized to a higher-stratum device or server.

The device configured as the NTP server cannot be configured with the symmetric mode.

SNTP

Simple Network Time Protocol (SNTP) is used to synchronize the system time of the device 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 3s.
- Multicast or broadcast mode: SNTP client passively monitors the packet.
 - After being configured to multicast mode, the device monitors the multicast IP address of 224.0.1.1 in real time and obtain clock signals from the SNTP multicast server. The maximum timeout for obtaining clock signals from the SNTP server is 1.5 multiples of the server sending period.
 - After being configured to broadcast mode, the device monitors the broadcast IP address of 255.255.255.255 in real time and obtain clock signals from the SNTP broadcast server. The maximum timeout for obtaining clock signals from the SNTP server is 1.5 multiples of the server sending period.

1.1.2 Preparing for configurations

Scenario

Configure the system time of the device, 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.

Prerequisite

N/A

NTP

Default configurations of NTP are as below.

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

SNTP

Default configurations of SNTP are as below.

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

1.1.3 Configuring NTP

Configuring basic functions of NTP



Caution

NTP and SNTP are mutually exclusive, so they cannot be configured concurrently.

Configure NTP for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config-ntp)#client update-interval { interval default }	Configure the update interval of the NTP client. interval: update interval, ranging from 4s to 17s By default, it is 6s.
3	Raisecom(config)#server broadcast-interval { interval default }	Configure the broadcast interval of the NTP server. interval: broadcast interval, ranging from 4s to 17s By default, it is 6s.
4	Raisecom(config-ntp)#master	Configure the master clock.
5	Raisecom(config-ntp)#stratum value	Configure the stratum of the system clock. value: stratum value, ranging from 1 to 15 By default, it is 16.
6	Raisecom(config-ntp)#ntp unicast-peer peer-ipv4 { version version-id authentication-keyid key-value vpn vpn-name port port-id }	Configure the specified IPv4 peer. • peer-ipv4: peer IPv4 address • version-id: NTP version • key-value: in-used authentication index • vpn-name: VPN name • port-id: in-use UDP port number
7	Raisecom(config-ntp)#ntp unicast-server sserver-ipv4 { version version-id authentication-keyid key-value vpn vpn-name port port-id }	Configure the specified IPv4 server. • peer-ipv4: server IPv4 address • version-id: NTP version • key-value: in-used authentication index • vpn-name: VPN name • port-id: in-use UDP port number



Note

If the device is configured as the NTP reference clock source, it cannot be configured as the NTP server or NTP symmetric peer; if the device is configured as the NTP server or symmetric peer, it cannot be configured as the NTP reference clock source.

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 device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config-ntp)#authentication { enable disable }	(Optional) enable global NTP authentication. • Enable: enabled • Disable: disabled.
3	Raisecom(config-ntp)#authentication-keyid key-value md5 key { cipher plain } string	(Optional) add the NTP authentication key. • Key-value: key index • Cipher: cipher text • Plain: plaintext • string: key string
4	Raisecom(config-ntp)#trusted-keyid key-value	(Optional) specify the created key to be trustful. • Key-value: key index

1.1.4 Configuring SNTP

Configure SNTP Client for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config-sntp)#sntp client update-interval <4-17>	Configure the update interval of the SNTP client.
3	Raisecom(config-sntp)#sntp server broadcast-interval <4-17>	Configure the broadcast interval of the SNTP server.
4	Raisecom(config-sntp)#sntp authentication { enable disable }	Enable global SNTP authentication
5	Raisecom(config-sntp)#sntp authentication-keyid <1-4294967295> md5 key string	Add the SNTP authentication key.

Step	Command	Description
6	Raisecom(config-sntp)#sntp master	Configure the master clock.
7	Raisecom(config-sntp } sntp stratum <1-15>	Configure the stratum of the system clock. value: stratum value, ranging from 1 to 15 By default, it is 16.
8	Raisecom(config-sntp)#sntp trusted-keyid <1-4294967295>	Specify the created key to be trustful
9	Raisecom(config-sntp)#sntp unicast-peer { A.B.C.D } Raisecom(config-sntp)#sntp unicast-peer { A.B.C.D } version { 3 4 } Raisecom(config-sntp)#sntp unicast-peer { A.B.C.D } version { 3 4 } authentication-keyid <1-4294967295> Raisecom(config-sntp)#sntp unicast-peer { A.B.C.D } authentication-keyid <1-4294967295>	Specify the IPv4 peer for the device.
10	Raisecom(config-sntp)#sntp unicast-server { A.B.C.D } Raisecom(config-sntp)#sntp unicast-server { A.B.C.D } version { 3 4 } Raisecom(config-sntp)#sntp unicast-server { A.B.C.D } version { 3 4 } authentication-keyid <1-4294967295> Raisecom(config-sntp)#sntp unicast-server { A.B.C.D } authentication-keyid <1-4294967295>	Specify the unicast IPv4 SNTP server for the device.

1.1.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show ntp	Show global NTP configurations.
2	Raisecom#show ntp service	Show NTP service configurations.
3	Raisecom#show ntp service verbose	Show detailed NTP service configurations.
4	Raisecom#show sntp	Show global SNTP configurations.

No.	Command	Description
5	Raisecom#show sntp service	Show SNTP service configurations.
6	Raisecom#show sntp service verbose	Show detailed SNTP service configurations.

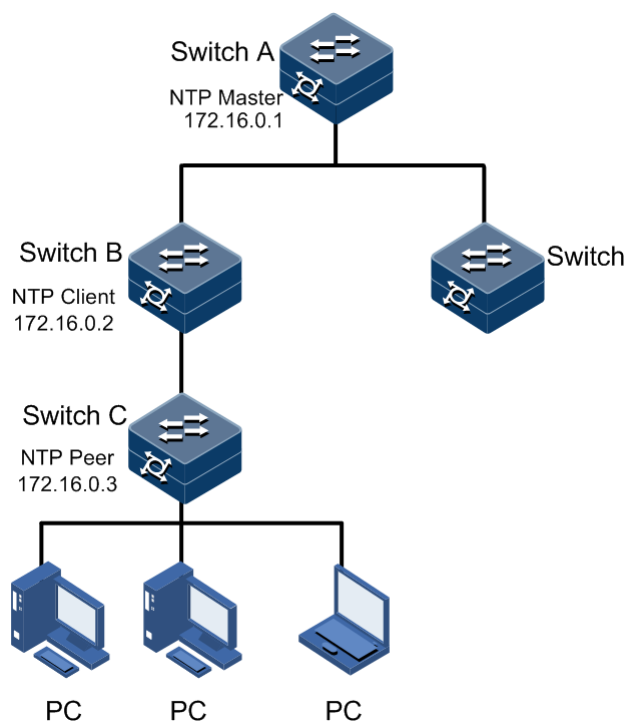
1.1.6 Example for configuring NTP

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 1-2 NTP networking



Configuration steps

Step 1 Configure Switch A.

```

Raisecom#hostname SwitchA
SwitchA#configure
  
```



```
SwitchA(config)#ntp  
SwitchA(config-ntp)#master  
SwitchA(config-ntp)#stratum 2
```

Step 2 Configure Switch B.

```
Raisecom#hostname SwitchB  
SwitchB#configure  
SwitchB(config)#ntp  
SwitchB(config-ntp)#ntp unicast-server 172.16.0.1  
SwitchB(config-ntp)#ntp unicast-peer 172.16.0.3  
SwitchB(config-ntp)#stratum 3
```

Step 3 Configure Switch C.

```
Raisecom#hostname SwitchC  
SwitchC#configure  
SwitchC(config)#ntp  
SwitchC(config-ntp)#ntp unicast-peer 172.16.0.2  
SwitchC(config-ntp)#stratum 4
```

Checking results

- Check Switch A.

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

```
SwitchA#show ntp status
```

- Check Switch B.

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

```
SwitchB#show ntp status
```

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

```
SwitchB#show ntp service
```

- Check Switch C.

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

```
Raisecom#show ntp status
```

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

```
Raisecom#show ntp associations
```

1.2 Interface management

1.2.1 Introduction

Ethernet interface

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 device supports both Ethernet electrical and optical interfaces.

- Auto-negotiation

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

- 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 device supports auto-MDI/MDIX.

VLAN interface

The VLAN interface is a logical interface and is used to implement layer 3 interconnection between VLANs. Each VLAN corresponds to a VLAN interface. After being configured with an IP address, the VLAN interface can work as the gateway of devices inside the VLAN, and forward layer 3 packets based on IP address across network segments.

Loopback interface

The Loopback interface is a logical virtual interface. Its physical layer status and link layer status are Up, so it is stable and can be configured with the IP address. It is usually used in dynamic routing protocol as the router ID of the device.

Null interface

The Null interface is a logical virtual interface, is always Up, but cannot forward packets and be configured with the IP address and link layer protocol. It can filter packets, so you can send needless network traffic to it to avoid complex operations of configuring the ACL. For example, if you specify the next hop for reaching a network segment as the Null interface in a network protocol, the Null interface will discard all data packets sent to the network segment.

1.2.2 Default configurations of interface management

Default configurations of interface management are as below.

Function	Default value
Duplex mode of interface	Auto-negotiation
Interface rate	Auto-negotiation
Interface rate statistics status	Disable
Interface flow control status	Disable
Interface status	Enable

1.2.3 Configuring basic attributes of interfaces

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

The Ethernet physical layer works in three modes as below:

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

Configure the basic attributes of interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-ge- 1/0/1)#description <i>string</i>	Configure the description of the interface.

Step	Command	Description
4	<code>Raisecom(config-ge-1/0/1)#mtu max-frame-length</code>	Configure the MTU of the interface.
5	<code>Raisecom(config-ge-1/0/1)#negotiation auto { enable disable }</code>	Enable or disable interface auto-negotiation.
6	<code>Raisecom(config-ge-1/0/1)#duplex { full half default }</code>	Configure the duplex mode of the interface.
7	<code>Raisecom(config-ge-1/0/1)#speed { 10 100 1000 default }</code>	Configure the interface rate.
8	<code>Raisecom(config-ge-1/0/1)#transceiver type { 1000BASE-T 1000BASE-X 100GBASE-COPPER 100GBASE-FIBER 10GBASE-COPPER 10GBASE-FIBER }</code>	Configure the connection mode of the SFP interface.
9	<code>Raisecom(config-ge-1/0/1)#port up-hold-time delay-time-value</code>	Configure the delayed time for processing when the interface status becomes Up.
10	<code>Raisecom(config-ge-1/0/1)#port down-hold-time delay-time-value</code>	Configure the delayed time for processing when the interface status becomes Down.

1.2.4 Configuring interface rate statistics

Configure interface rate statistics for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#flow-statistic interval time-value</code>	Configure the period for information statistics on all interfaces. This command takes effect on all interfaces. You can also configure the period for the specific interface to override the period for all interfaces.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical interface configuration mode.
4	<code>Raisecom(config-ge-1/0/1)#port flow-statistic interval time-value</code>	Configure the period for information statistics on the interface. This command can override the configuration of the period for all interfaces.
5	<code>Raisecom(config-ge-1/0/1)#reset statistics</code>	Clear interface statistics.

1.2.5 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 device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-ge-1/0/1)#flow-control { enable disable }	Configure flow control on the interface.

1.2.6 Shutting down/Restarting the interface

Shut down/Restart the interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#inte rface <i>interface-type</i> <i>interface-number</i>	Enter physical interface configuration mode, VLAN interface configuration mode, or link aggregation configuration mode.
3	Raisecom(config-ge-1/0/1)#shutdown	Shut down the current interface. Use the no shutdown command to re-enable the disabled interface.

1.2.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show interface	Show brief information about the interface list.
2	Raisecom#show interface verbose	Show detailed information about the interface list.
3	Raisecom#show interface <i>interface-type interface-number</i>	Show detailed information about the specific interface.
4	Raisecom#show interface [<i>interface-type</i> <i>interface-number</i>] config	Show configurations of the interface.

2 Ethernet

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

- MAC address table
- VLAN
- Voice VLAN
- QinQ
- VLAN mapping
- MRP

2.1 MAC address table

2.1.1 Introduction

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

The MAC address table contains the following information:

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

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

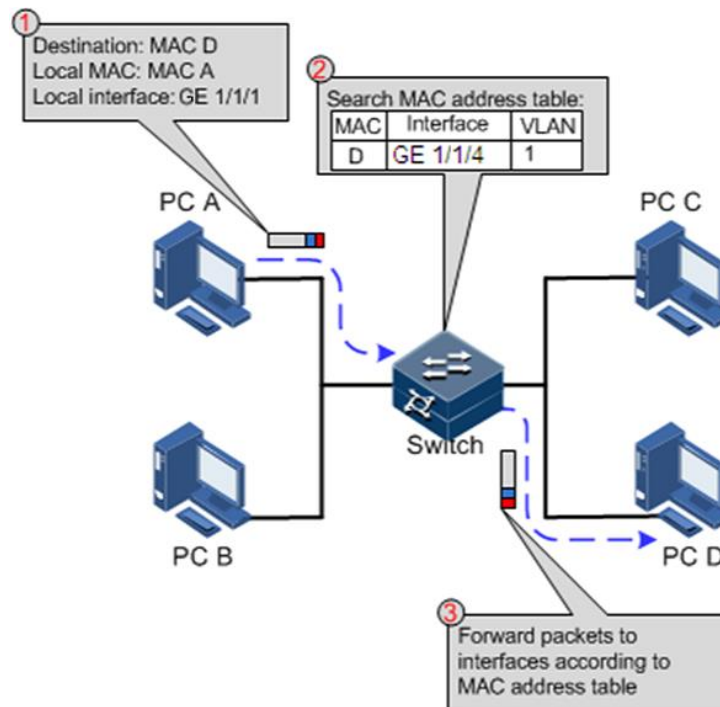
Forwarding modes of MAC addresses

When forwarding packets, based on the information about MAC addresses, the device 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 device 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 device broadcasts the packet to all interfaces except the receiving interface, as shown in Figure 2-1.

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



- Multicast: when the device 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 device receives an all-F packet, or the MAC address is not listed in the MAC address table, the device forwards the packet to all interfaces except the interface that receives this packet. Broadcast addresses are special multicast addresses.

Classification of MAC addresses

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

- Static MAC address entry: also called permanent address, added and removed by the user manually, not aged with time. For a network with small changes of devices, adding static address entry manually can reduce the network broadcast flow, improve the security of the interface, and prevent entries from being lost after the system is reset.
- Dynamic MAC address entry: the device can add dynamic MAC address entries through MAC address learning. The entries are aged according to the configured aging time, and will be empty after the system is reset.

Aging time of MAC addresses

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

The device 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 device searches the MAC address table for the interface related to the destination MAC address of packets.

- If it is successful, and the interface corresponding with the destination MAC address is different from the ingress interface, it forwards packets, records the source MAC addresses of packets, interface ID of ingress packets, and VLAN ID in the MAC address table. If packets from other interface are sent to the MAC address, the device can send them to the related interface.
- If it fails, it broadcasts packets to all interfaces except the source interface, and records the source MAC address in the MAC address table.

MAC address limit

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

The MAC address limit improves the speed of forwarding packets.

2.1.2 Preparing for configurations

Scenario

Configure the static MAC address table in the following situations:

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

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

Prerequisite

N/A

2.1.3 Default configurations of MAC address table

Default configurations of the MAC address table are as below.

Function	Default value
MAC address learning status	Enable
MAC address aging time	300s
MAC address limit	Unlimited
MAC address flapping detection	Enable
MAC address flapping protection	Disable

2.1.4 Configuring the static MAC address

Configure the static MAC address for the device as below.

Step	Command	Description
1	Raisecom# configure	Enter global configuration mode.
2	Raisecom(config)# mac-address static vlan <i>vlan-id</i> mac <i>mac-address</i> interface-type <i>interface-number</i>	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.

2.1.5 Configuring the blackhole MAC address

Configure blackhole MAC addresses for the device as below.

Step	Command	Description
1	Raisecom# configure	Enter global configuration mode.
2	Raisecom(config)# mac-address blackhole <i>mac-address</i> vlan <i>vlan-id</i>	Configure blackhole MAC addresses.

2.1.6 Configuring MAC address learning

Configure MAC address learning for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-ge-1/0/1)#mac-address learning { disable enable }	Enable or disable MAC address learning.

2.1.7 Configuring the MAC address limit

Configure the MAC address limit for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i> vlan <i>vlan-id</i>	Enter Layer 2 physical interface configuration mode or VLAN interface configuration mode. The following steps take VLAN interface configuration interface for example.
3	Raisecom(config-vlan*)#mac-address threshold <i>threshold-value</i>	Configure the interface-based MAC address limit.

2.1.8 Configuring the aging time of MAC addresses

Configure the aging time of MAC addresses for the device as below.

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

2.1.9 MAC address flapping detection and protection

Configure MAC address flapping detection and protection for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#mac-address flapping detection { enable disable }	Enable or disable MAC address flapping detection.

Step	Command	Description
3	Raisecom(config)#mac-address flapping detection exclude-vlan <i>vlan-list</i>	Configure the VLANs excluded from MAC address flapping detection.
4	Raisecom(config)#mac-address flapping detection vlan <i>vlan-list</i> security-level { high middle low }	Configure the VLANs for MAC address flapping detection, and configure the security level for triggering MAC address flapping protection. The higher the security level is, the smaller the times of MAC address flapping for triggering flapping protection is.
5	Raisecom(config)#mac-address flapping error-down recovery-interval <i>period</i>	Configure the auto-recovery interval for triggering the interface error-down by MAC address flapping.
6	Raisecom(config)#mac-address flapping quit-vlan recover-time <i>period</i>	Configure the auto-recovery interval for triggering the interface quit-vlan by MAC address flapping.
7	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
8	Raisecom(config-ge-1/0/1)#mac-address flapping action { error-down quit-vlan }	Configure the action for MAC address flapping on the interface.
9	Raisecom(config-ge-1/0/1)#mac-address flapping action priority <i>priority</i>	Configure the priority of the action for MAC address flapping on the interface. The higher the priority is, the protection action is more preferentially triggered.

2.1.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show mac-address	Show information about MAC address entries.
2	Raisecom#show mac-address vlan <i>vlan-id</i>	Show information about MAC address entries for the specified VLAN.
3	Raisecom#show mac-address interface <i>interface-type interface-number</i>	Show information about MAC address entries for the specified interface.
4	Raisecom#show mac-address { static dynamic blackhole } [vlan <i>vlan-id</i>]	Show information about the static/dynamic/blackhole MAC address entries.
5	Raisecom#show mac-address aging-time	Show the aging time of MAC addresses.

No.	Command	Description
6	Raisecom#show mac-address flapping record	Show records on MAC address flapping detection.
7	Raisecom#show mac-limit [interface <i>interface-type</i> <i>interface-number</i>]	Show the configured MAC address limit.

2.1.11 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)#no mac-address [vlan <i>vlan-id</i>] [mac <i>mac-address</i>]	Clear MAC addresses of the specified parameter.
Raisecom(config)#no mac-address <i>interface-type interface-number</i>	Clear MAC addresses of the specified interface.
Raisecom(config)#no mac-address { static dynamic blackhole } [vlan <i>vlan-id</i>] [mac <i>mac-address</i>]	Clear static/dynamic/blackhole MAC addresses of the specified parameter.
Raisecom(config)#no mac-address { static dynamic } [<i>interface-type</i> <i>interface-number</i>]	Clear static/dynamic MAC addresses of the specified interface.
Raisecom(config)#reset mac-address flapping record	Clear records on MAC address flapping detection.

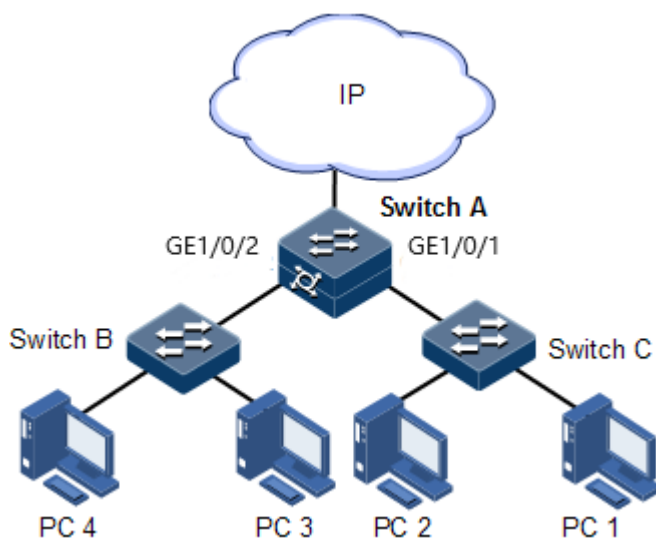
2.1.12 Example for configuring the MAC address table

Networking requirements

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

- Configure a static unicast MAC address 0001.0203.0405 on GE 1/0/2 and configure its VLAN to VLAN 10.
- Configure the aging time to 500s.

Figure 2-2 MAC networking



Configuration steps

Step 1 Create VLAN 10, and activate it, and add GE 1/0/2 to VLAN 10.

```
Raisecom#configure
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port link-type access
Raisecom(config-ge-1/0/2)#port default vlan 10
Raisecom(config-ge-1/0/2)#quit
```

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 static vlan 10 mac 00:01:02:03:04:05 ge
1/0/2
```

Checking results

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

```
Raisecom#show mac-address
```

Learned-From	Type	valid	MacAddress	VLAN/VSI/BD
0001:0203:0405	10/--/--	ge-1/0/2		static
yes				
Total:1	Static:1	Dynamic:0	Blackhole:0	
Sticky:0	Security:0	Snooping:0		

2.2 VLAN

2.2.1 Introduction

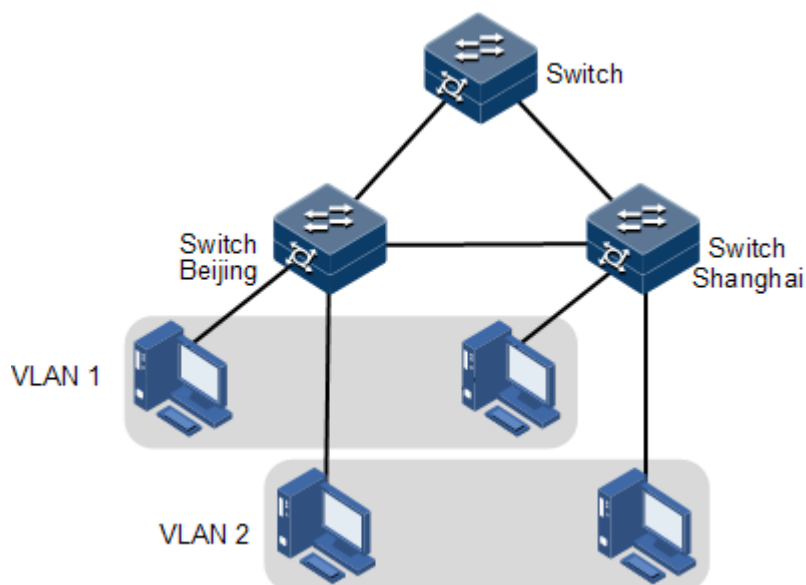
Overview

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

VLAN partitions

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

Figure 2-3 VLAN partitions



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

The device complies with IEEE 802.1Q standard VLAN and supports 4094 concurrent VLANs.

- VLAN partitions by interface

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

Table 2-1 Interface mode and packet processing

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

- VLAN partitions by MAC address

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

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

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

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

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

This refers to VLAN partitions by the protocol type carried in the packet and encapsulation format.

- After receiving an untagged packet from an interface, the device according to the protocol domain of the packet determines the VLAN to which the packet belongs, and sends the packet to the specified VLAN for later transmission.
- When receiving a tagged packet from an interface, the device receives the packet if the VLAN ID is in the list of VLANs of which packets are allowed to pass by the interface, or discards the packet if the VLAN ID is not in the list of VLANs of which packets are allowed to pass by the interface.

2.2.2 Preparing for configurations

Scenario

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

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

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

Prerequisite

N/A

2.2.3 Default configurations of VLAN

Default configurations of VLAN are as below.

Function	Default value
Create VLAN	VLAN 1
Interface mode	Hybrid
PVID	1
VLAN of Trunk interface	VLAN 1
VLAN of Access interface	VLAN 1

2.2.4 Configuring VLAN attributes

Configure VLAN attributes for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#vlan <i>vlan-list</i>	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.

2.2.5 Configuring the interface mode

Configure the interface mode for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter Layer 2 physical interface configuration mode or link aggregation configuration mode. The following steps take Layer 2 physical interface configuration mode for example.
3	Raisecom(config-ge-1/0/*)#port link-type { access default dot1q-tunnel hybrid trunk }	Configure the interface to Access, Trunk, Hybrid, or dot1q-tunnel mode.

2.2.6 Configuring the VLAN on the Access interface

Configure the VLAN on the Access interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode, or aggregation group configuration mode. Take Layer 2 physical interface configuration mode for example.
3	Raisecom(config-ge-1/0/*)#port link-type access Raisecom(config-ge-1/0/*)#port default vlan <i>vlan-id</i>	Configure the interface to Access mode, and add the Access interface to the VLAN.



Note

- The interface allows Access VLAN packets to pass regardless of configuration for VLAN allowed by the Access interface. The forwarded packets do not carry the VLAN Tag.
- Configuring the Access VLAN will fail if you have not created and activated the VLAN in advance.
- If you delete or suspend the Access VLAN manually, the system will not automatically configure the interface Access VLAN as the default VLAN.
- When you configure the interface Access VLAN as the non-default Access VLAN, the default Access VLAN 1 is the VLAN allowed by the Access the egress interface, you can delete Access VLAN 1 from the allowed VLAN list of the egress Access interface.
- If the configured Access VLAN is not the default VLAN and there is no default VLAN in the allowed VLAN list of the Access interface, the interface does not allow packets of the default VLAN to pass.

2.2.7 Configuring the VLAN on the Trunk interface

Configure the VLAN on the Trunk interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode, or aggregation group configuration mode. Take Layer 2 physical interface configuration mode for example.
3	Raisecom(config-ge-1/0/*)#port link-type trunk	Configure the interface to Trunk mode.
4	Raisecom(config-ge-1/0/*)#port trunk pvid <i>vlan-id</i>	Configure the PVID of the interface.

Step	Command	Description
5	Raisecom(config-ge-1/0/*)#port trunk allowed-pass vlan { all vlan-list }	Configure VLANs allowed to pass by the Trunk interface.



Note

- No matter how the VLAN list allowed to pass by the interface is configured, the interface allows packets of the VLAN to pass and forward packets without the corresponding PVID.
- The system will not create and activate the VLAN if no VLAN is created and activated in advance when configuring the Native VLAN.
- The system will not configure 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 configured Native VLAN is not the default VLAN, and the VLAN list allowed to pass by the Trunk interface does not include the default VLAN, the interface will disallow packets of the default VLAN to pass.
- The VLAN list allowed by the Trunk interface is only effective to static VLAN, and ineffective for cluster VLAN, MVRP dynamic VLAN.

2.2.8 Configuring the VLAN based on the Hybrid interface

Configure the VLAN based on the Hybrid interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface interface-type interface-number	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-ge-1/0/*)#port link-type hybrid	Configure the interface mode to Hybrid.
4	Raisecom(config-ge-1/0/*)#port hybrid pvid vlan-id	Configure the interface PVID.
5	Raisecom(config-ge-1/0/*)#port hybrid vlan { all vlan-list } { tagged untagged }	Configure the VLANs allowed to pass in tagged or untagged mode by the Hybrid interface.



Note

The Hybrid interface can work in different modes as configured. In untagged mode, its working mode is the same as that in the Access mode, but it can be configured with multiple allowed VLANs. In tagged mode, its working mode is the same as that in the Trunk mode.

2.2.9 Configuring the VLAN based on MAC address

Configure the VLAN based on MAC address for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#mac-vlan <i>mac-address vlan-id</i>	Associate a MAC address and mask with a VLAN
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
4	Raisecom(config-ge-1/0/*)#mac-vlan enable	Enable MAC-VLAN.



Caution

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

2.2.10 Configuring the VLAN based on IP subnet

Configure the VLAN based on IP subnet for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#ip-subnet-vlan <i>ip-address [ip-mask] vlan vlan-id</i>	Associate a MAC address with an IP subnet.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
4	Raisecom(config-ge-1/0/*)#ip-subnet-vlan enable	Enable VLAN partitions based on IP subnet.



Caution

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

2.2.11 Configuring the VLAN based on protocol

Configure the VLAN based on protocol for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#protocol-vlan <i>protocol-index { ethernet2 llc snap protocol-id }</i>	Configure the rule for associating the protocol VLAN with Ethernet packets.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
4	Raisecom(config-ge-1/0/*)#protocol-vlan <i>protocol-index vid vlan-id</i>	Configure the rule for associating the interface with the protocol VLAN.

2.2.12 Checking configurations

Use the following commands to check configuration results.

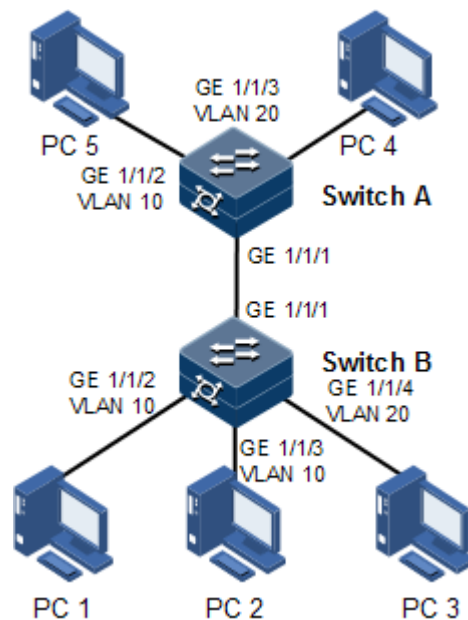
No.	Command	Description
1	Raisecom#show vlan <i>[vlan-list vlan-id]</i>	Show VLAN configurations.
2	Raisecom#show port vlan	Show configurations of the VLAN on the interface.
3	Raisecom#show mac-vlan <i>[vlan vlan-id]</i>	Show configurations of the MAC VLAN.
4	Raisecom#show ip-subnet-vlan <i>[vlan vlan-id]</i>	Show configurations of the IP subnet VLAN.
5	Raisecom#show protocol-vlan all	Show configurations of all protocol VLANs.
6	Raisecom#show protocol-vlan interface	Show configurations of the protocol VLAN on the interface.

2.2.13 Example for configuring VLANs

Networking requirements

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

Figure 2-4 VLAN and interface isolation networking



Configuration steps

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

Configure Switch A.

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

Configure Switch B.

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

Step 2 Add GE 1/0/2 and GE 1/0/3 in Access mode on Switch B to VLAN 10, add GE 1/0/4 as Access mode to VLAN 20, configure GE 1/0/1 to Trunk mode, and allow VLAN 10 to pass.

```
SwitchB(config)#interface ge 1/0/2
SwitchB(config-ge-1/0/2)#port link-type access
SwitchB(config-ge-1/0/2)#port default vlan 10
SwitchB(config-ge-1/0/2)#exit
SwitchB(config)#interface ge 1/0/3
SwitchB(config-ge-1/0/3)#port link-type access
SwitchB(config-ge-1/0/3)#port default vlan 10
SwitchB(config-ge-1/0/3)#exit
```

```
SwitchB(config)#interface ge 1/0/4
SwitchB(config-ge-1/0/4)#port link-type access
SwitchB(config-ge-1/0/4)#port default vlan 20
SwitchB(config-ge-1/0/4)#exit
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#port link-type trunk
SwitchB(config-ge-1/0/1)#port trunk allow-pass vlan 10
SwitchB(config-ge-1/0/1)#exit
```

- Step 3 Add GE 1/0/2 as Access mode on Switch A to VLAN 10, add GE 1/0/3 as Access mode to VLAN 20, configure GE 1/0/1 to Trunk mode, and allow VLAN 10 to pass.

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type access
SwitchA(config-ge-1/0/2)#port access vlan 10
SwitchA(config-ge-1/0/2)#exit
SwitchA(config)#interface ge 1/0/3
SwitchA(config-ge-1/0/3)#port mode trunk
SwitchA(config-ge-1/0/3)#port trunk pvid 20
SwitchA(config-ge-1/0/3)#port trunk allow-pass 20
SwitchA(config-ge-1/0/3)#exit
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allowed-pass vlan 10
```

Checking results

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

Take Switch B for example.

```
SwitchB#show vlan
normal
S: supervlan    P: pvlan    N:
vlan Type      Ports('M': member , '-': not member)
-----
1          N/static      untagged: ge-1/0/1      <->ge-
1/0/16      M---MMMM MMMMMMMMM
1/0/17<->ge-1/0/24      MMMMMMMM
10ge-1/0/25<->10ge-1/0/30  MMMMMM
10  N/static    tagged:  ge-1/0/1<->ge-1/0/16  M-----
untagged: ge-1/0/1<->ge-1/0/16  -MM-----
20          N/static      untagged: ge-1/0/1<->ge-1/0/16  ---M--
-- -----
Total: 3    Static: 3    Dynamic: 0
```

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

Take Switch B for example.

```
SwitchB#show interface ge 1/0/2 config
!
interface ge 1/0/2
    port link-type    access
                                port default vlan 10
```

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

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

2.3 Voice VLAN

2.3.1 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.

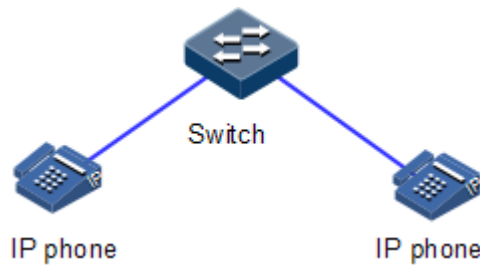
A voice VLAN is especially partitioned for voice traffic of users. By partitioning voice VLANs and add interfaces of the voice device to voice VLANs, you can configure QoS of voice traffic to increase the priority of transmitting voice traffic and guarantee call quality.

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 2-5 shows the networking mode for IP phone (with its interfaces transmitting voice traffic only) to connect to the switch. This mode enables these interfaces to transmit voice traffic only, thus minimizing the impact on voice traffic from data traffic.

Figure 2-5 Networking for IP phone to connect to switch



2.3.2 Preparing for configurations

Scenario

A specific voice VLAN can transmit voice traffic. If a voice device becomes faulty or exits the network in a period, the interface connecting the voice device will automatically exit the voice VLAN.

Prerequisite

Create a VLAN, and configure its parameters.

2.3.3 Default configurations of the 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-phone
0003.6B00.0000	FFFF.FF00.0000	Cisco-phone
0004.0D00.0000	FFFF.FF00.0000	Avaya-phone
00D0.1E00.0000	FFFF.FF00.0000	Pingtel-phone
0060.B900.0000	FFFF.FF00.0000	Philips/NEC-phone
00E0.7500.0000	FFFF.FF00.0000	Verilink-phone
00E0.BB00.0000	FFFF.FF00.0000	NBX-phone

Other default configurations of the voice VLAN are as below.

Function	Default value
Voice VLAN	Disable
Voice VLAN secure working mode	Enable
Voice VLAN common working mode	Disable
Automatic mode for the interface to join the voice VLAN	Enable

Function	Default value
Manual mode for the interface to join the voice VLAN	Disable
CoS and DSCP of Voice VLAN packets	6 and 46 respectively
QoS trust priority of Voice VLAN	N/A
Aging time of the Voice VLAN	5min

2.3.4 Configuring the OUI

Configure the OUI for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#voice-vlan oui <i>mac-address [mask-address]</i> [description word]	Configure the OUI of the voice VLAN.

2.3.5 Enabling the voice VLAN

Enable the voice VLAN for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-ge-1/1/*)#voice-vlan <i>vlan-id</i> enable	Enable the voice VLAN.
4	Raisecom(config-ge-1/1/*)#voice-vlan mode { enable disable }	Configure the working mode of the interface to join the voice VLAN.
5	Raisecom(config)#voice-vlan aging-time <i>time</i>	Configure the aging time of the interface to leave the voice VLAN in automatic mode.
6	Raisecom(config)#interface <i>interface-type interface-number</i> Raisecom(config-ge-1/1/*)#voice-vlan security enable	Configure the working mode of the voice VLAN to security.

2.3.6 Checking configurations

Use the following commands check configuration results.

No.	Command	Description
1	Raisecom#show voice-vlan oui	Show the OUI address, its mask, and description on the current device.
2	Raisecom#show voice-vlan interface	Show the status of the voice VLAN on the current device.

2.3.7 Example for adding interfaces to the voice VLAN

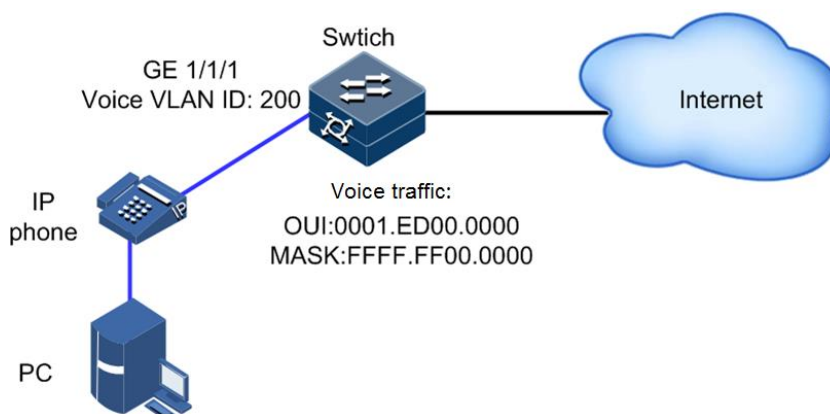
Example for adding interfaces to the voice VLAN and configuring it to work in manual mode

Networking requirements

GE 1/1/1 on the Switch connects the IP phone and PC to the Internet. It is required to concurrently forward and isolate voice traffic and data traffic.

You can configure GE 1/1/1 as a Trunk interface, making the Native VLAN forward data traffic and voice VLAN forward voice traffic. The PC sends untagged packets which are transmitted in the Native VLAN of GE 1/1/1. Configure VLAN 100 as the Native VLAN to transmit data traffic sent from the PC. The IP phone also sends untagged packets. Configure the source MAC address to the OUI address of the voice VLAN so that the device can add voice VLAN Tag when these packets pass the voice VLAN interface. Configure VLAN 200 as the voice VLAN to transmit voice traffic sent from the IP phone.

Figure 2-6 Networking with adding interface to voice VLAN and configuring it to work in manual mode



Configuration steps

- Step 1 Configure the MAC address (supporting the mask) of the IP phone as the OUI address of the voice VLAN on the switch, namely, 0001.ED00.0000. Configure the mask to FFFF.FF00.0000. For the OUI supported by the device by default, see section 2.3.3 Default configurations of the voice VLAN.

```
Raisecom(config)#voice-vlan oui 00:01:ED:00:00:00/24
```

- Step 2 Create VLAN 100 and VLAN 200, activate them, and configure VLAN 200 as the voice VLAN.

```
Raisecom(config)#vlan 100,200
Raisecom(config)#interface ge 1/1/1
Raisecom(config-ge-1/1/1)#port link-type trunk
Raisecom(config-ge-1/1/1)#port trunk allow-pass vlan 100
Raisecom(config-ge-1/1/1)#voice-vlan 200 enable
```

Checking configurations

Use the **show voice-vlan interface** command to view the current interface status of the voice VLAN.

```
Raisecom(config)#show voice-vlan interface
```

		Support max interface	:64	
Current enable interface	:1			
Interface	VID	Mode	Security	RemainTime(s)

ge-1/0/1	200	auto	enable	N/A

2.3.8 Example for configuring the IP phone to access voice VLAN packets through LLDP

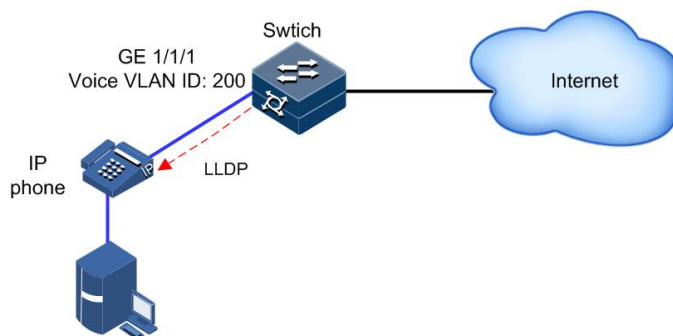
Networking requirements

As shown in Figure 2-7, when the IP phone supports LLDP, it can obtain the voice VLAN through LLDP. You can configure LLDP and voice VLAN on the switch to connect the IP phone. Configure LLDP on the switch to advertise the voice VLAN of the interface to the IP phone. To guarantee call quality, configure the voice VLAN to prioritize voice packets.

GE 1/1/1 on the Switch connects the IP phone and PC to the Internet. It is required to concurrently forward and isolate voice traffic and data traffic.

You can configure GE 1/1/1 as a Trunk interface, making the Native VLAN forward data traffic and voice VLAN forward voice traffic. The PC sends untagged packets which are transmitted in the Native VLAN of GE 1/1/1. Configure VLAN 100 as the Native VLAN to transmit data traffic sent from the PC. Configure VLAN 200 as the voice VLAN to transmit voice traffic sent from the IP phone. The IP phone obtains the voice VLAN through LLDP and sends packets with the voice VLAN Tag.

Figure 2-7 Configuring IP phone to access voice VLAN packets through LLDP



Configuration steps

- Step 1 Configure the MAC address (supporting the mask) of the IP phone as the OUI address of the voice VLAN on the switch, namely, 0001.ED00.0000. Configure the mask to FFFF.FF00.0000. For the OUI supported by the device by default, see section 2.3.3 Default configurations of the voice VLAN.

```
Raisecom(config)#voice-vlan oui 0001.ED00.0000/24
```

- Step 2 Create VLAN 100 and VLAN 200, activate them, and configure VLAN 200 as the voice VLAN.

```
Raisecom(config)#vlan 100,200
Raisecom(config)#interface ge 1/1/1
Raisecom(config-ge-1/1/1)#port link-type trunk
Raisecom(config-ge-1/1/1)#port trunk allow-pass vlan 100
Raisecom(config-ge-1/1/1)#voice-vlan 200 enable
Raisecom(config-ge-1/1/1)#exit
```

- Step 3 Enable global LLDP and interface LLDP to advertise the voice VLAN of the interface to the IP phone.

```
Raisecom(config)#lldp start
Raisecom(config)#interface ge 1/1/1
Raisecom(config-ge-1/1/1)#lldp admin-status rx-tx
```

Checking configurations

Use the **show voice-vlan interface** command to view the interface status of the voice VLAN.

```
Raisecom(config)#show voice-vlan interface
```

Support max interface	:	64			
Current enable interface	:	1			
Interface	VID	Mode	Security	RemainTime(s)	
ge-1/0/1	200	auto	enable	N/A	

2.4 QinQ

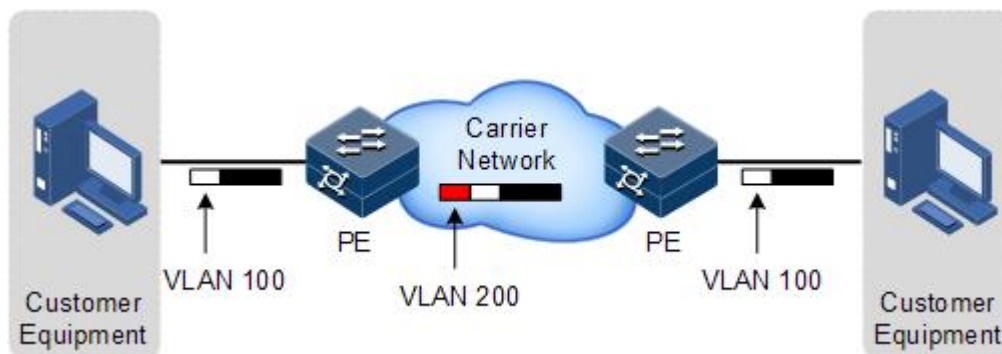
2.4.1 Introduction

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

Basic QinQ

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

Figure 2-8 Principles of basic QinQ



Typical networking of basic QinQ is shown as Figure 2-8; the device 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 flow into different outer VLAN Tags. This technique is implemented through combination of interface and VLAN. Selective QinQ can perform different actions on different VLAN Tags received by one interface and add different outer VLAN IDs for different inner VLAN IDs. According to configured mapping rules for inner and outer Tags, you can encapsulate different outer Tags for different inner tagged packets.

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

2.4.2 Preparing for configurations

Scenario

Basic QinQ configuration and selective QinQ configuration for the device are based on different service requirements.

- Basic QinQ

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

- Selective QinQ

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

Prerequisite

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



Note

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

2.4.3 Default configurations of QinQ

Default configurations of QinQ are as below.

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

2.4.4 Configuring basic QinQ

Configure basic QinQ on the ingress interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-gigaethernet1/1/*) #port link-type dot1q-tunnel	Enable basic QinQ on the interface.
4	Raisecom(config-gigaethernet1/1/*) #port hybrid pvid <i>vlan-id</i>	Configure basic QinQ, add double Tags, and specify the PVID used by the CVLAN and SVLAN.
5	Raisecom(config-gigaethernet1/1/*) #tpid tpid	Configure the TPID of the VLAN Tag on the interface. It is used identify the inner VLAN, or is used to identify the outer VLAN when QinQ is enabled. • tpid: TPID value, in dotted hexadecimal notation, an integer, being 0x8100, 0x88a8, or 0x9100
6	Raisecom(config-gigaethernet1/1/*) #inner tpid tpid	Configure the TPID of the inner VLAN Tag on the interface. It is used identify the inner VLAN, or is used to identify the outer VLAN when QinQ is enabled.



Note

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.

2.4.5 Configuring selective QinQ

Configure selective QinQ on the ingress interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-gigaetherne t1/1/port)#vlan-stacking vlan <i>vlan-id</i> stack-vlan <i>vlan-id</i> [remark-8021p <i>cos-id</i>]	Configure selective QinQ.

2.4.6 Configuring the network-side interface to Trunk mode

Configure the network-side interface to Trunk mode for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#inte rface <i>interface-type</i> <i>interface-number</i>	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config- gigaetherne t1/1/*)#sw itchport mode trunk	Configure interface trunk mode, permit double-tagged packet to pass.

2.4.7 Configuring the TPID

Configure the TPID on the network side interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#inte rface <i>interface-type</i> <i>interface-number</i>	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config- gigaetherne t1/1/*)#tp id <i>tpid</i>	Configure the TPID of the outer VLAN Tag on the interface.

2.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show vlan-stacking config	Show configurations of basic QinQ.
2	Raisecom#show vlan-stacking interface	Show QinQ configurations of the interface.
3	Raisecom#show vlan-stacking resource	Show resource information about QinQ.

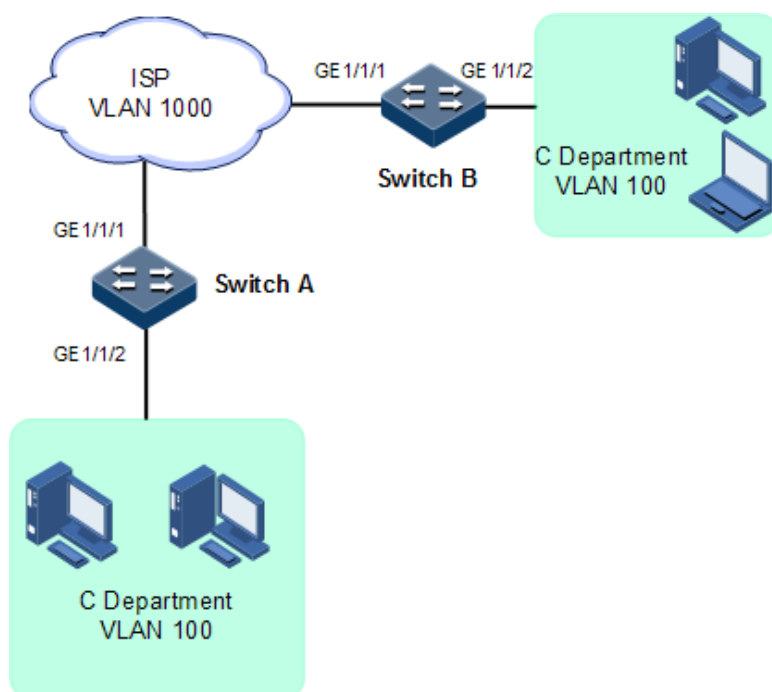
2.4.9 Example for configuring basic QinQ

Networking requirements

As shown in Figure 2-9, Switch A and Switch B are connected to two branches of Department C, which are in different locations. Department C uses VLAN 100, and needs to communicate through VLAN 1000 of the carrier network. The carrier TPID is 9100.

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

Figure 2-9 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 and VLAN 1000, and activate them. TPID is 9100.

```
Raisecom#configure
Raisecom(config)#vlan 100,1000
Raisecom(config)#interface ge 1/1/1
Raisecom(config-ge-1/1/1)#port link-type trunk
Raisecom(config-ge-1/1/1)#port trunk allow-pass vlan 1000
Raisecom(config-ge-1/1/1)#tpid 0x9100
Raisecom(config-ge-1/1/1)#exit
```

Step 2 Configure basic QinQ on the interface.

```
Raisecom(config)#interface ge 1/1/2
Raisecom(config-ge-1/1/2)#port link-type dot1q-tunnel
Raisecom(config-ge-1/1/2)#port default vlan 1000
Raisecom(config-ge-1/1/2)#exit
```

Checking results

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

```
Raisecom#show interface ge 1/1/2 config
!
interface ge 1/1/2
  port link-type dot1q-tunnel

  port default vlan 1000
```

2.4.10 Example for configuring selective QinQ

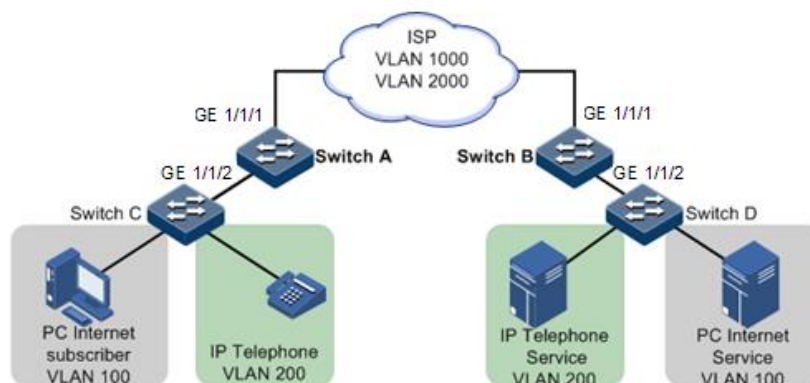
Networking requirements

As shown in Figure 2-10, 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 2-10 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#hostname SwitchA
SwitchA#configure
SwitchA(config)#vlan 100,200,1000,2000
SwitchA(config)#interface ge 1/1/1
SwitchA(config-ge-1/1/1)#port link-type trunk
SwitchA(config-ge-1/1/1)#port trunk allow-pass vlan 1000,2000
SwitchA(config-ge-1/1/1)#tpid 0x9100
SwitchA(config-ge-1/1/1)#exit
```

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

```
SwitchA(config)#interface ge 1/1/2
SwitchA(config-ge-1/1/2)#port link-type trunk
SwitchA(config-ge-1/1/2)#port trunk allow-pass vlan 100,200,1000,2000
SwitchA(config-ge-1/1/2)#vlan-stacking enable
SwitchA(config-ge-1/1/2)#vlan-stacking vlan 100 stack-vlan 1000
SwitchA(config-ge-1/1/2)#vlan-stacking vlan 200 stack-vlan 2000
SwitchA(config-ge-1/1/2)#exit
```

Checking results

Use the **show vlan-stacking interface** command to show configurations of selective QinQ.

Take Switch A for example.

```
SwitchA#show vlan-stacking interface
      Interface      MatchVlan(outer/8021p)
StackVlan(inner/outer/8021p)
-----
-----
ge-1/1/2          100/-          -/1000/-
ge-1/1/2          200/-          -/2000/-
```

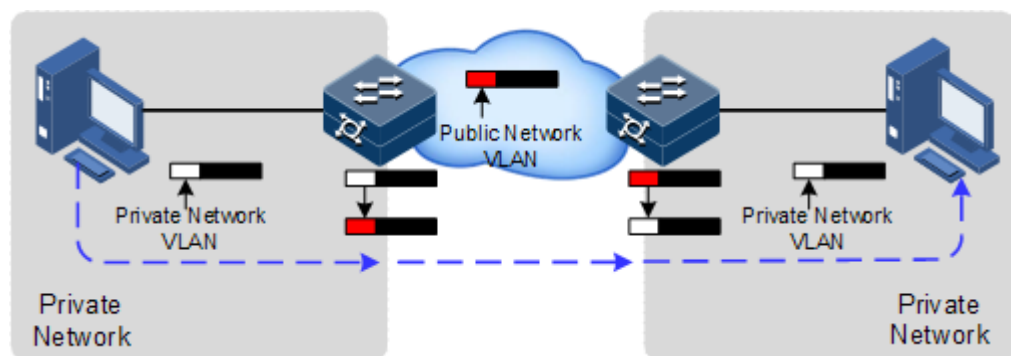
2.5 VLAN mapping

2.5.1 Introduction

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

Figure 2-11 shows principles of VLAN mapping.

Figure 2-11 Principles of VLAN mapping



After receiving a user private network packet with a VLAN Tag, the device 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 device replaces the VLAN Tag carried by a packet from a specified VLAN to the new VLAN Tag.

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

2.5.2 Preparing for configurations

Scenario

Different from QinQ, VLAN mapping is used to change the VLAN Tag without encapsulating multilayer VLAN Tag so that packets are transmitted according to the carrier's VLAN

mapping rules. VLAN mapping does not increase the frame length of the original packet. It can be used in the following scenarios:

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

Prerequisite

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

2.5.3 Default configurations of VLAN mapping

Default configurations of VLAN mapping are as below.

Function	Default value
VLAN mapping status	Disable

2.5.4 Configuring VLAN mapping

Configure VLAN mapping for the device as below.

Step	Command	Description
1	Raisecom# configure	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-ge-1/1/*)# vlan-mapping enable	Enable VLAN mapping.
4	Raisecom(config-ge-1/1/*)# vlan-mapping vlan <i>vlan-id</i> map-vlan <i>vlan-id</i> [remark-8021p <i>cos-id</i>]	Configure the single-tagged 1:1 VLAN mapping rule.
5	Raisecom(config-ge-1/1/*)# vlan-mapping vlan <i>vlan-id</i> 8021p <i>cos-id</i> map-vlan <i>vlan-id</i> [remark-8021p <i>cos-id</i>]	Configure the mapping rule for single-tagged 1:1 VLAN to match CoS.
6	Raisecom(config-ge-1/1/*)# vlan-mapping vlan <i>vlan-id</i> inner-vlan <i>vlan-id</i> map-vlan <i>vlan-id</i> map-inner-vlan <i>vlan-id</i> [remark-8021p <i>cos-id</i>]	Configure the inner and outer 2:2 VLAN mapping rule.
7	Raisecom(config-ge-1/1/*)# vlan-mapping vlan <i>vlan-id</i> inner-vlan <i>vlan-id</i> map-vlan <i>vlan-id</i> [remark-8021p <i>cos-id</i>]	Configure the inner and outer 2:1 VLAN mapping rule.
8	Raisecom(config-ge-1/1/*)# vlan-mapping 8021p <i>vlan-id</i> map-vlan <i>vlan-id</i> [remark-8021p <i>cos-id</i>]	Configure the mapping rule for matching CoS.



Note

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

2.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show vlan-mapping interface	Show configurations of VLAN mapping rules on the interface.

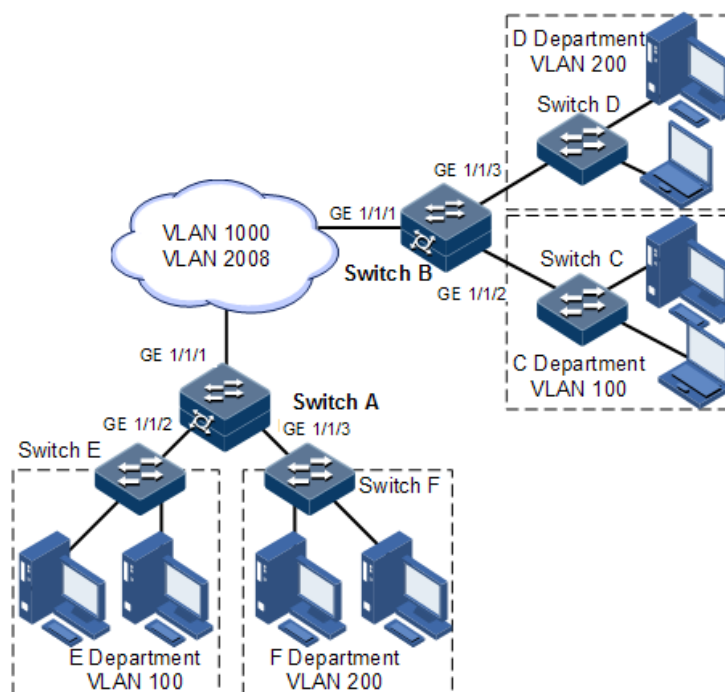
2.5.6 Example for configuring VLAN mapping

Scenario

As shown in Figure 2-12, 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 2-12 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#hostname SwitchA
SwitchA#configure
SwitchA(config)#vlan 100,200,1000,2008
```

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

```
SwitchA(config)#interface ge 1/1/1
SwitchA(config-ge-1/1/1)#port link-type trunk
SwitchA(config-ge-1/1/1)#port trunk allow-pass vlan 1000,2008
SwitchA(config-ge-1/1/1)#exit
```

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

```
SwitchA(config)#interface ge 1/1/2
SwitchA(config-ge-1/1/2)#port link-type trunk
SwitchA(config-ge-1/1/2)#port trunk allow-pass vlan 100
```



```
SwitchA(config-ge-1/1/2)#vlan-mapping vlan 100 map-vlan 1000
SwitchA(config-ge-1/1/2)#exit
```

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

```
SwitchA(config)#interface ge 1/1/3
SwitchA(config-ge-1/1/3)#port link-type trunk
SwitchA(config-ge-1/1/3)#port trunk allow-pass vlan 100
SwitchA(config-ge-1/1/3)#vlan-mapping vlan 200 map-vlan 2008
```

Checking results

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

```
SwitchA#show vlan-mapping interface
Interface          MatchVlan(vlan/8021p)      MapVlan(vlan/8021p)
-----
--
ge-1/1/2           inner: -                   inner: -/-
                   outer: 100/-              outer: 1000/-
ge-1/1/3           inner: -                   inner: -/-
                   outer: 200/-              outer: 2008/-
-----
--
```

2.6 MRP/VRP

2.6.1 Introduction

Multiple Registration Protocol (MRP) is an attribute registration protocol, which can be used to transfer attribute information. Multiple VLAN Registration Protocol (MVRP) is an application of MRP, which is used to advertise and learn VLAN configurations between devices. Through MVRP, devices in the LAN can automatically synchronize VLAN configurations, greatly reducing VLAN configuration work by the network administrator.

MRP messages

MRP messages include the Join message, New message, Leave message, and LeaveAll message.

- Join message: when an MRP entity is configured with certain attributes and requires the peer entity to register its attribute information, it will send a Join message to the peer entity. When the MRP peer entity receives a Join message, it registers the attributes in

the Join message and advertises the Join message to other entities of the device. After receiving the advertised Join message, other entities send a Join message to their peer entities.

- New message: the functions of a New message are similar to that of a Join message. Both messages are used to declare attributes. The difference is that the New message is used for Multiple Spanning Tree Protocol (MSTP) topology changes.
- Leave message: when an MRP entity deregisters certain attributes and needs to synchronously deregister these attributes to the peer entity, it will send a Leave message to the peer entity. When the MRP peer entity receives the Leave message from the entity, it will deregister the attributes in the Leave message and advertises the Leave message to other entities on the device. After receiving the advertised Leave message, other entities will use the attributes in the Leave message to determine their status on the device and decide whether to send the Leave message to their peer entities (for example, if the attribute in the Leave message is a VLAN, the VLAN is a dynamic VLAN, and there are no entities registered with the VLAN on this device, the peer entity deletes the VLAN on the device and sends the Leave message to the entity; if the VLAN is a static VLAN, the peer entity does not send the Leave message to the peer entity).
- LeaveAll message: each MRP entity starts its own LeaveAll timer when it starts. When the LeaveAll timer expires, the MRP entity will send a LeaveAll message to the peer entity. When an MRP entity sends or receives a LeaveAll message, it starts the Leave timer and determines whether to send a Join message based on its own attribute status and require the peer entity to re-register a certain attribute. Before the Leave timer expires, the entity re-registers the attributes in the Join message received from the peer entity. After the Leave timer expires, all unregistered attributes are deregistered, thereby periodically clearing the garbage attributes on the network.

The Leave message or LeaveAll message cooperates with the Join message to deregister or reregister attributes. Through message exchange, all attributes to be registered can be transmitted to all MRP entities in the same LAN.

MRP timers

The interval for sending the MRP message is controlled by timers. MRP defines four timers to control the interval.

- Periodic timer: each MRP entity starts its own Periodic timer when it starts to control the periodic sending of MRP messages. Before the Periodic timer expires, the MRP entity collects the MRP messages that need to be sent. After the Periodic timer expires, the MRP entity encapsulates all the MRP messages that need to be sent into as few messages as possible and sends them out, thereby reducing the number of messages sent. Then, the MRP entity restarts the Periodic timer to start a new cycle.
- Join timer: it is used to control the sending of Join messages. To ensure that Join messages can be reliably sent to the peer entity, the MRP entity starts the Join timer when sending Join messages. If the entity receives a JoinIn message from the peer entity before the timer expires, and the properties in the JoinIn message match those in the sent Join message, the entity will not resend the Join message; otherwise, after the timer expires, when the Periodic timer also expires, the entity will send the Join message once.
- Leave timer: it is used to control attribute deregistration. When an MRP entity receives a Leave message (or sends or receives a LeaveAll message) from the peer entity, it starts the Leave timer. If it receives a Join message from the peer entity before the leave timer expires, and the properties in the Join message match those in the received Leave message (or match some properties in the LeaveAll message received or sent), these properties will not be deregistered in the current entity, and other properties will be deregistered after the timer expires.

- **LeaveAll timer:** each MRP entity starts its own LeaveAll timer when it starts. When the LeaveAll timer expires, the MRP entity will send a LeaveAll message to the peer entity, and then restart the LeaveAll timer to start a new cycle. The peer entity also restarts the LeaveAll timer after receiving the LeaveAll message.

MVRP

Multiple VLAN Registration Protocol (MVRP) is an MRP application. Based on MRP working mechanism, it maintains VLAN dynamic registration information about the switch, and sends the information to other switches.

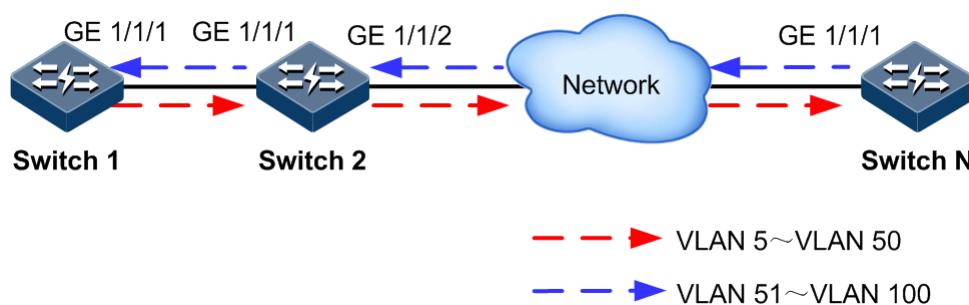
All MRP-supportive switches can receive VLAN registration information from other switches, and dynamically update local VLAN registration information. In addition, all MRP-supportive switches can send local VLAN registration information to other switches so that they have consistent VLAN registration information in the same VLAN. VLAN registration information sent by MVRP includes manually configured local static registration information and dynamic registration information from other switches.

MRP has three registration modes:

- **Normal:** in this mode, MVRP allows dynamic registration and deregistration of VLANs, and sends dynamic and static VLAN information.
- **Fixed:** in this mode, MVRP forbids dynamic registration and deregistration of VLANs, and sends static VLAN information rather than dynamic VLAN information to other MVRP members.
- **Forbidden:** in this mode, MVRP forbids dynamic registration and deregistration of VLANs, forbids creating static VLANs on the interface, deletes all VLANs except VLAN 1, allows packets of the default VLAN (VLAN 1) to pass, and transmits packets of the default VLAN to other MVRP members.

As shown in Figure 2-13, to configure VLANs on multiple devices on a network and allow packets of the specified VLAN to pass are complex. By using MVRP to dynamically register and transmit the specified VLAN, the network administrator can improve working efficiency and accuracy.

Figure 2-13 Principles of MVRP



As shown in Figure 2-13, GE 1/1/1 on Switch 1, GE 1/1/1 and GE 1/1/2 on Switch 2, and GE 1/1/1 on Switch N are Trunk interfaces. Create VLANs 5–50 on Switch 1, and then these VLANs will be dynamically registered on the Rx interface along the red direction until Switch N is registered. Create VLANs 51–100 on Switch N, and then these VLANs will be dynamically registered on the Rx interface along the blue direction so that each switch can completely process packets of VLANs 5–100.

2.6.2 Preparing for configurations

Scenario

MVRP enables configurations of a MVRP member to fast spread to all MVRP-enabled devices in the LAN.

The values of the Join timer, Leaver timer, and LeaveAll timer configured through MVRP will be applied to all MVRP applications in the LAN.

Prerequisite

N/A

2.6.3 Default configurations

Default configurations of MVRP are as below.

Function	Default value
Global MVRP status	Disable
Interface MVRP status	Disable
MVRP registration mode	Normal

2.6.4 Configuring basic functions of MVRP

Configure basic functions of MVRP for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#mvrp start	Enable global MVRP.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
4	Raisecom(config- gigaethernet1/1/*)#port link-type trunk	Configure the interface to Trunk mode.
5	Raisecom(config- gigaethernet1/1/*)#mvrp registration { fixed forbidden normal }	Configure the MVRP registration mode.
6	Raisecom(config- gigaethernet1/1/*)#mvrp enable	Enable interface MVRP.



Caution

- Interface MVRP can be enabled only after the interface is configured to Trunk mode.
- We do not recommend enabling MVRP on a LAG member interface.

2.6.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show mvrp config	Show MVRP configurations.
2	Raisecom# show mvrp	Show the interface status of MVRP.
3	Raisecom# show mvrp interface <i>interface-type interface-</i> <i>number vlan vlan-id</i>	Show configurations of the MVRP timer.

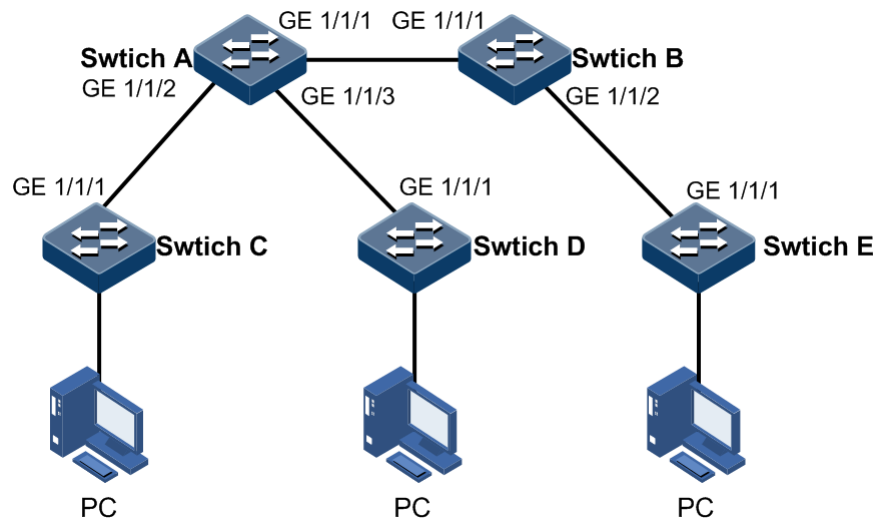
2.6.6 Example for configuring MVRP

Networking requirements

As shown in Figure 2-14, to dynamically register, deregister, and update VLAN information between switches, configure MVRP on these switches. Detailed requirements are as below:

- Configure static VLANs 5–10 on Switch A and Switch C.
- Configure static VLANs 15–20 on Switch D.
- Configure static VLANs 25–30 on Switch E.
- Configure the interfaces that are connected to other switches to Trunk mode, and enable MVRP on these interfaces.
- Configure the Join timer, Leave timer, and LeaveAll timer of MVRP on each interface to 3000, 15000, and 20000, in units of 10ms.

Figure 2-14 MVRP networking



Configuration steps

Step 1 Create VLANs and enable global MVRP.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#configure
SwitchA(config)#vlan 5-10
SwitchA(config)#mvrp start
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#configure
SwitchB(config)#mvrp start
```

Configure Switch C.

```
Raisecom#hostname SwitchC
SwitchC#configure
SwitchC(config)#vlan 5-10
SwitchC(config)#mvrp start
```

Configure Switch D.

```
Raisecom#hostname SwitchD
```

```
SwitchD#configure
SwitchD(config)#vlan 15-20
SwitchD(config)#mvrp start
```

Configure Switch E.

```
Raisecom#hostname SwitchE
SwitchE#configure
SwitchE(config)#vlan 25-30
SwitchE(config)#mvrp start
```

- Step 2 Configure GE 1/1/1, GE 1/1/2, and GE 1/1/3 on Switch A, GE 1/1/1, GE 1/1/2, and GE 1/1/3 on Switch B, GE 1/1/1 on Switch C, and GE 1/1/1 on Switch D to Trunk mode, and enable MVRP on them. Take GE 1/1/1 on Switch A for example. Configurations of other interfaces are the same.

```
SwitchA(config)#interface ge 1/1/1
SwitchA(config-ge-1/1/1)#port link-type trunk
SwitchA(config-ge-1/1/1)#port trunk allow-pass vlan all
SwitchA(config-ge-1/1/1)#mvrp enable
SwitchA(config-ge-1/1/1)#exit
```

- Step 3 Configure MVRP timers of GE 1/1/1, GE 1/1/2, and GE 1/1/3 on Switch A, GE 1/1/1, GE 1/1/2, and GE 1/1/3 on Switch B, GE 1/1/1 on Switch C, and GE 1/1/1 on Switch D, and enable MVRP on them. Take GE 1/1/1 on Switch A for example. Configurations of other interfaces are the same.

```
SwitchA(config)#interface ge 1/1/1
SwitchA(config-ge-1/1/1)#mvrp timer join 3000
SwitchA(config-ge-1/1/1)#mvrp timer leave 15000
SwitchA(config-ge-1/1/1)#mvrp timer leave-all 20000
```

Checking results

Use the **show mvrp** command to show MVRP configurations on the interface.

Take Switch A for example.

```
SwitchA#show mvrp

Version           : MVRP_V13.10.00.00
Compliance-GVRP   : disable
Interface         JoinTime(ms)  LeaveTime(ms)  LeaveAllTime(ms)
PeriodicTime(ms)  Mode      State
```

```

-----
-----
ge 1/1/1      3000      15000      20000      --
normal enable

```

Use the **show vlan** command to view information about VLANs on the device. Take Switch A for example.

SwitchA#**show vlan**

NOTE:

S: supervlan P: pvlan N: normal

```

vlan Type      Ports('M': member , '-': not member)
-----
1    N/static   untagged: ge-1/1/1<->ge-1/1/16      MMMMMMMM
MMMMMMMM
                        ge-1/1/17<->ge-1/1/32      MMMMMMMM MMMMMMMM
                        ge-1/1/33<->ge-1/1/48      MMMMMMMM MMMMMMMM
                        10ge-1/1/49<->10ge-1/1/54    MMMMMM
2    N/mvrp     tagged:  ge-1/1/1<->ge-1/1/16      M-----
3    N/mvrp     tagged:  ge-1/1/1<->ge-1/1/16      M-----
4    N/mvrp     tagged:  ge-1/1/1<->ge-1/1/16      M-----
5    N/mvrp     tagged:  ge-1/1/1<->ge-1/1/16      M-----
6    N/mvrp     tagged:  ge-1/1/1<->ge-1/1/16      M-----
7    N/mvrp     tagged:  ge-1/1/1<->ge-1/1/16      M-----
8    N/mvrp     tagged:  ge-1/1/1<->ge-1/1/16      M-----
9    N/mvrp     tagged:  ge-1/1/1<->ge-1/1/16      M-----
10   N/mvrp     tagged:  ge-1/1/1<->ge-1/1/16      M-----
20   N/mvrp     tagged:  ge-1/1/1<->ge-1/1/16      M-----
-----
Total: 11   Static: 1   Dynamic: 10

```


3 IP services

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

- IP basis
- Loopback interface
- ARP
- NDP
- Static route

3.1 IP basis

3.1.1 Introduction

The IP interface is a virtual interface based on VLAN, so it is applied when the device needs to be managed by the NMS or multiple devices needs to be routed and connected.

The device supports the double-tagged management VLAN packets, and it can send and process double-tagged packets.

3.1.2 Preparing for configurations

Scenario

Configure the IP address of each VLAN interface, SNMP interface, or loopback interface.

Prerequisite

- Create VLANs.
- Activate them.

3.1.3 Default configurations of VLAN interface

Default configurations of the VLAN interface are as below.

Function	Default value
Management VLAN inner TPID	0x8100
Management VLAN inner VLAN	1
Initial IP address of the device	192.168.0.1

3.1.4 Configuring the IPv4 address of the VLAN interface

Configure the IPv4 address of the VLAN interface for the device as below.

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

3.1.5 Configuring the IPv6 address of the interface

Configure the IPv6 address of the interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#vlan <i>vlan-id</i>	Create a VLAN.
3	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
4	Raisecom(config-vlanif-*)#ipv6 enable	Enable the IPv6 address of the VLAN interface.
5	Raisecom(config-vlanif-*)#ipv6 address <i>ipv6-address/prefix-length</i> Raisecom(config-vlanif-*)#ipv6 address <i>ipv6-address</i> link-local	Configure the IPv6 address of the VLAN interface.

3.1.6 Checking configurations

Use the following commands to check configuration results.

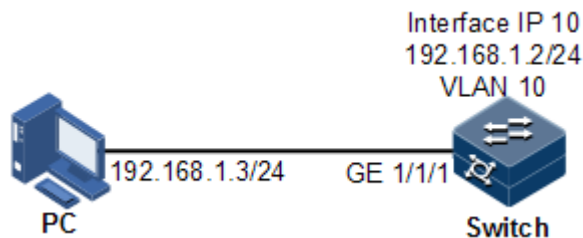
No.	Command	Description
1	Raisecom#show ip interface brief	Show configurations of the IP address of the VLAN interface.
2	Raisecom#show ipv6 interface brief	Show configurations of the IPv6 address of the VLAN interface.

3.1.7 Example for configuring the VLAN interface to interconnect with the host

Networking requirements

As shown in Figure 3-1, configure the VLAN interface to the switch so that the host and the device can ping each other.

Figure 3-1 VLAN interface networking



Configuration steps

Step 1 Create a VLAN, and add the interface to the VLAN.

```
Raisecom#configure
Raisecom(config)#vlan 10
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port hybrid pvid 10
Raisecom(config-ge-1/0/1)#port hybrid vlan 10 untagged
Raisecom(config-ge-1/0/1)#quit
```

Step 2 Create a Layer 3 interface 10 on the device, configure its IP address, and associate it with the VLAN.

```
Raisecom(config)#interface vlan 10
Raisecom(config-vlan10)#ip address 192.168.1.2 255.255.255.0
```

Checking results

Use the **show vlan** command to show mapping between the physical interface and VLAN.

Raisecom#**show vlan 10**

```

vlan-10                                information:
-----
Description                            :
Admin state                            : up
Operation state                        : down
Vlan type                              : normal
Vlan status                            : static
Unknown multicast state                 : forward
Unknown unicast state                  : forward
IPv4 address total number              : 0
IPv6 address total number              : 0

Ports :
  Interface                            Tagged
-----
  ge-1/0/1                             Untag
-----

```

Use the **show ip interface** to show configurations of the Layer 3 interface.

Raisecom#**show ip interface**

```

Total number:
2
Interface          State(a/o) Addr/Prefix      Role    Type    Vpn-
instance
-----
loopback-0         up/up      127.0.0.1/8     0.1/8   primary
auto              N/A
                  vlan-10   up/up      192.168.1.2/24
primary static    N/A
-----

```

Use the **ping** command to check whether the device and PC can ping each other.

Raisecom#**ping 192.168.1.3**

```

PING 192.168.1.3 : 64 data bytes
Reply from 192.168.1.3: bytes=64 time=0ms TTL=64 icmp_seq=1
Reply from 192.168.1.3: bytes=64 time=0ms TTL=64 icmp_seq=2
Reply from 192.168.1.3: bytes=64 time=0ms TTL=64 icmp_seq=3
Reply from 192.168.1.3: bytes=64 time=0ms TTL=64 icmp_seq=4
Reply from 192.168.1.3: bytes=64 time=0ms TTL=64 icmp_seq=5

```

```

PING Statistics for 192.168.1.3
5 packets transmitted, 5 packets received, 0% packet loss
  round-trip (ms)  min/avg/max = 0/0/0

```

3.2 Loopback interface

3.2.1 Introduction

The loopback interface is a virtual interface and can be classified into two types:

- Loopback interface automatically created by the system: the IP address is fixed to 127.0.0.1. This type of interfaces receives packets sent to the device. It does not broadcast packets through routing protocols.
- Loopback interface created by users: without affecting physical interface configurations, configure a local interface with a specified IP address, and make the interface Up permanently so that packets can be broadcasted through routing protocols.

The loopback interface status is independent from the physical interface status (Up/Down). As long as the device is working normally, the loopback interface will not become Down. Thus, it is used to identify the physical device as a management address.

3.2.2 Preparing for configurations

Scenario

Use the IP address of the loopback interface to log in through Telnet so that the Telnet operation does not become Down due to change of physical status. To enable the PC to ping through the IP address of the loopback interface, configure the corresponding static route entry on the PC. The loopback interface ID is also used as the router ID of dynamic routing protocols, such as OSPF, to uniquely identify a device.

Prerequisite

N/A

3.2.3 Default configurations of the Loopback interface

N/A

3.2.4 Configuring the IP address of the Loopback interface

Configure the IP address of the Loopback interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface loopback <i>loopback-number</i>	Enter Loopback interface configuration mode.

Step	Command	Description
3	Raisecom(config-loopback-*)#ip address <i>ip-address</i> [<i>ip-mask</i>] [<i>sub</i>]	Configure the IP address of the Loopback interface.
4	Raisecom(config-loopback-*)#ipv6 enable	Enable the IPv6 address of the Loopback interface.
4	Raisecom(config-loopback-*)#ipv6 address <i>ipv6-address/prefix-length</i> Raisecom(config-loopback-*)#ipv6 address <i>ipv6-address link-local</i>	Configure the IPv6 address of the Loopback interface.

3.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show interface loopback [<i>loopback-number</i>]	Show configurations of the Loopback interface.

3.3 ARP

3.3.1 Introduction

In TCP/IP network environment, each host is assigned with a 32-bit IP address that is a logical address used to identify hosts between networks. To transmit packets in physical link, you must know the physical address of the destination host, which requires mapping the IP address to the physical address. In Ethernet environment, the physical address is 48-bit MAC address. The system has to transfer the 32-bit IP address of the destination host to the 48-bit Ethernet address for transmitting packet to the destination host correctly. Then Address Resolution Protocol (ARP) is applied to resolve IP address to MAC address and configure mapping between IP address and MAC address.

The ARP address table contains the following two types:

- Static entry: bind the IP address and MAC address to avoid ARP dynamic learning cheating.
 - The static ARP address entry needs to be added/deleted manually.
 - The static ARP address entry is not aged.
- Dynamic entry: MAC address automatically learned through ARP.
 - This dynamic ARP address entry is automatically generated by switch. You can adjust partial parameters of it manually.
 - The dynamic ARP address entry will be aged after the aging time if not used.

3.3.2 Preparing for configurations

Scenario

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

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

Prerequisite

N/A

3.3.3 Default configurations of ARP

Default configurations of ARP are as below.

Function	Default value
Static ARP entry	N/A
Aging time of dynamic ARP entries	1200s

3.3.4 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 device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#ip arp <i>ip-address mac-address</i> { ge 10ge 25ge 40ge 100ge 400ge } <i>interface-number</i>	Configure static ARP entry.

3.3.5 Configuring dynamic ARP entries

Configure dynamic ARP entries for the device as below.

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

Step	Command	Description
2	Raisecom(config)#arp aging-time <i>time</i>	Configure the aging time of dynamic ARP entries.

3.3.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show ip arp	Show information about entries in the ARP address table.

3.3.7 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)#flush arp [all dynamic static]	Clear all entries in the ARP address table.

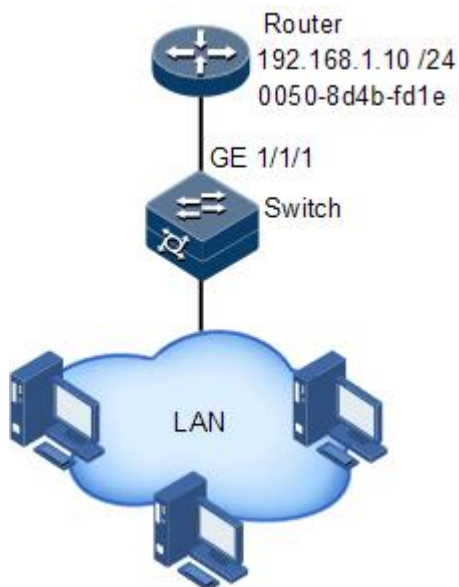
3.3.8 Example for configuring ARP

Networking requirements

As shown in Figure 3-2, the device is connected to the host, and is also connected to the upstream Router through GE 1/1/1. For the Router, the IP address and submask are 192.168.1.10/24, and the MAC address is 0050-8d4b-fd1e.

To improve communication security between the Switch and Router, you need to configure related static ARP entry on the device.

Figure 3-2 Configuring ARP networking



Configuration steps

Step 1 Create VLAN 3.

```
Raisecom#configure  
Raisecom(config)#vlan 3
```

Step 2 Add interface GE 1/0/1 to VLAN 3.

```
Raisecom(config)#inter ge 1/0/1  
Raisecom(config-ge-1/0/1)#port hybrid pvid 3  
Raisecom(config-ge-1/0/1)#port hybrid vlan 3 untagged  
Raisecom(config-ge-1/0/1)#quit
```

Step 3 Create interface VLANIF3.

```
Raisecom(config)#inter vlan 3
```

Step 4 Configure the IP address of the interface VLANIF3.

```
Raisecom(config-vlanif-3)#ip address 192.168.1.1/24  
Raisecom(config-vlanif-3)#quit
```

Step 5 Add a static ARP entry.

```
Raisecom#configure
Raisecom(config)#ip arp 192.168.1.10 00:50:8d:4b:fd:1e ge 1/0/1
```

Checking results

Use the **show ip arp** command to show configurations of the ARP address table.

```
Raisecom#show ip arp
Arp aging time: 1200 (s)
Arp entry types: D-Dynamic, S-Static, I-Invalid, DH-Dhcp, B-Bgp, INV-Invalid
Interface
IP-addr Mac-addr Type Aging Vlan(O/I) Interface Vpn-
instance
-----
192.168.1.1 0002:5600:0001 I - -/- vlan-3
N/A
192.168.1.10 0050:8d4b:fd1e S - 3/- ge-1/0
/1 N/A
-----
Total: 2 Dynamic: 0 Static: 1 Bgp: 0 Other: 1
```

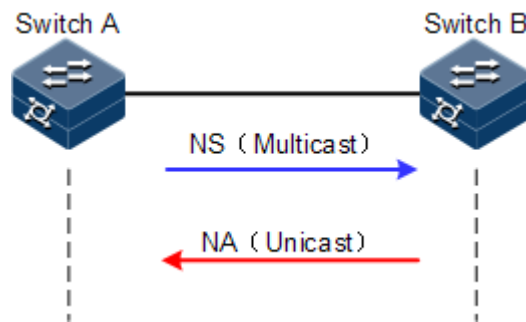
3.4 NDP

3.4.1 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 3-3 Principles of NDP address resolution



As shown in Figure 3-3, 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 the VLAN interface on Switch A, and the destination address of the NS message is the multicast address of the requested node of the Switch B. The NS message even contains the data link layer address of Switch A.
- Step 2 After receiving the NS message, Switch B judges whether the destination address of the NS message is the multicast address of the request node corresponding to the IPv6 address of Switch B. If yes, Switch B can obtain the data link layer address of Switch A, and sends a NA message which contains its data link layer address in unicast mode.
- Step 3 After receiving the NA message from Switch B, Switch A obtains the data link layer address of Switch B.

By sending ICMPv6 message, IPv6 NDP even has the following functions:

- Verify whether the neighbor is reachable.
- Detect duplicated addresses.
- Discover routers or prefix.
- Automatically configure addresses.
- Support redirection.

3.4.2 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 VLAN interface.

3.4.3 Default configurations of NDP

Default configurations of NDP are as below.

Function	Default value
Aging time of dynamic NDPs	1200s

3.4.4 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 device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config-vlanif-*)#ipv6 neighbor <i>ipv6-address mac-address { ge 10ge }</i> <i>interface-number</i>	Configure static neighbor entries.

3.4.5 Configuring the aging time of dynamic NDPs

NDP entries are not permanently valid but valid for only a period. After the period expires, a NDP entry will be deleted if it is not updated. The period is called the aging time.

Configure the aging time of dynamic NDPs for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#ipv6 nd lifetime { <i>aging-time</i> <i>default</i> }	Configure the aging time of dynamic NDPs.

3.4.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show ipv6 neighbor	Show information about all NDP neighbors.

3.4.7 Maintenance

Maintain the device as below.

Command	Description
<code>Raisecom(config)#flush ipv6 neighbor</code> <code>[all dynamic static]</code>	Clear information about all IPv6 neighbors.

3.5 Static route

3.5.1 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.

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 device has not been configured with default route and the destination IP of the packet is not in the routing table, the device will discard the packet and return an ICMP packet to the Tx end to inform that the destination address or network is unavailable.

Static route

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

3.5.2 Preparing for configurations

Scenario

Configure the static route for simple network topology manually to establish an intercommunication network.

Prerequisite

Configure the IP address of the VLAN interface correctly.

3.5.3 Configuring the static route

Configure the static route for the device as below.

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

Step	Command	Description
2	Raisecom(config)# ip route-static <i>ip-address mask-address nexthop-address</i> { preference <i>preference-value</i> }	Configure the IPv4 static route.
3	Raisecom(config)# ipv6 route-static <i>ipv6-address mask-length ipv6-nexthop-address</i> { preference <i>preference-value</i> }	Configure the IPv6 static route.

3.5.4 Checking configurations

Use the following commands to check configuration results.

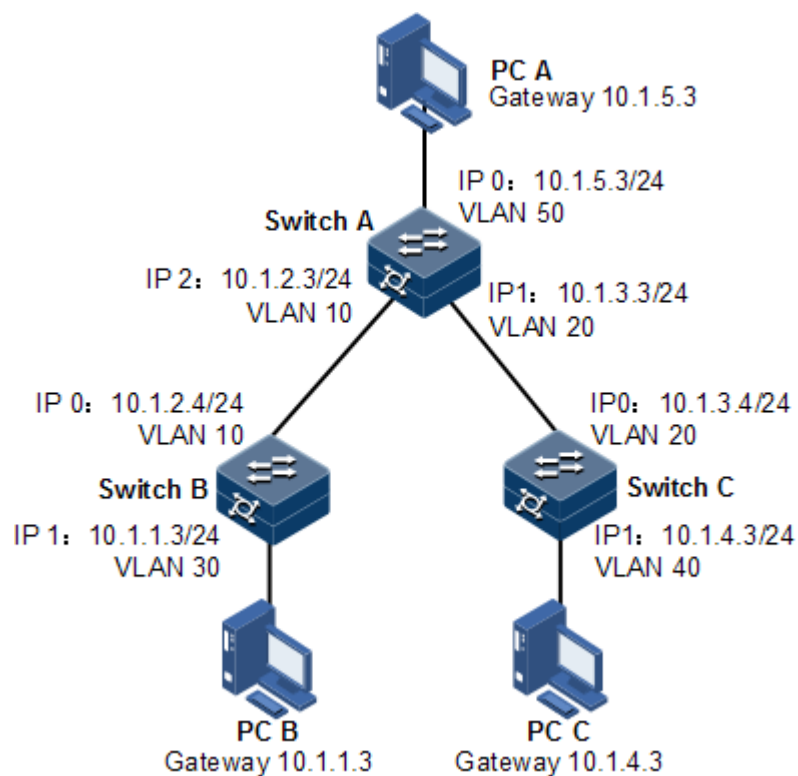
No.	Item	Description
1	Raisecom# show ip route Raisecom# show ipv6 route	Show information about the routing table.
2	Raisecom# show { ip ipv6 } route statistics	Show route statistics.

3.5.5 Example for configuring the static route

Networking requirements

Configure the static route to enable any two hosts or devices successfully to ping through each other, as shown in Figure 3-4.

Figure 3-4 Configuring the static route



Configuration steps

Step 1 Configure the IP address of each device. Detailed configurations are omitted.

Step 2 Configure the static route on Switch A.

```
Raisecom#hostname SwitchA
SwitchA#configure
SwitchA(config)#ip route-static 10.1.1.0 255.255.255.0 10.1.2.4
SwitchA(config)#ip route-static 10.1.4.0 255.255.255.0 10.1.3.4
```

Step 3 Configure the default gateway on Switch B.

```
Raisecom#hostname SwitchB
SwitchB#configure
SwitchB(config)#ip route-static 0.0.0.0 0.0.0.0 10.1.2.3
```

Step 4 Configure the default gateway on Switch C.

```
Raisecom#hostname SwitchC
SwitchC#configure
SwitchC(config)#ip route-static 0.0.0.0 0.0.0.0 10.1.3.3
```

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

Checking results

Use the **ping** command to check whether any two of all devices can ping through each other.

```
SwitchA#ping 10.1.1.3
  PING 10.1.1.3 : 64 data bytes
Reply from 10.1.1.3: bytes=64 time=0ms TTL=64 icmp_seq=1
Reply from 10.1.1.3: bytes=64 time=0ms TTL=64 icmp_seq=2
Reply from 10.1.1.3: bytes=64 time=0ms TTL=64 icmp_seq=3
Reply from 10.1.1.3: bytes=64 time=0ms TTL=64 icmp_seq=4
Reply from 10.1.1.3: bytes=64 time=0ms TTL=64 icmp_seq=5
  PING Statistics for 10.1.1.3
  5 packets transmitted, 5 packets received, 0% packet loss
    round-trip (ms)  min/avg/max = 0/0/0
```


4 DHCP

This chapter describes basic principles and configurations procedures of DHCP, and providing related configuration examples, including the following sections:

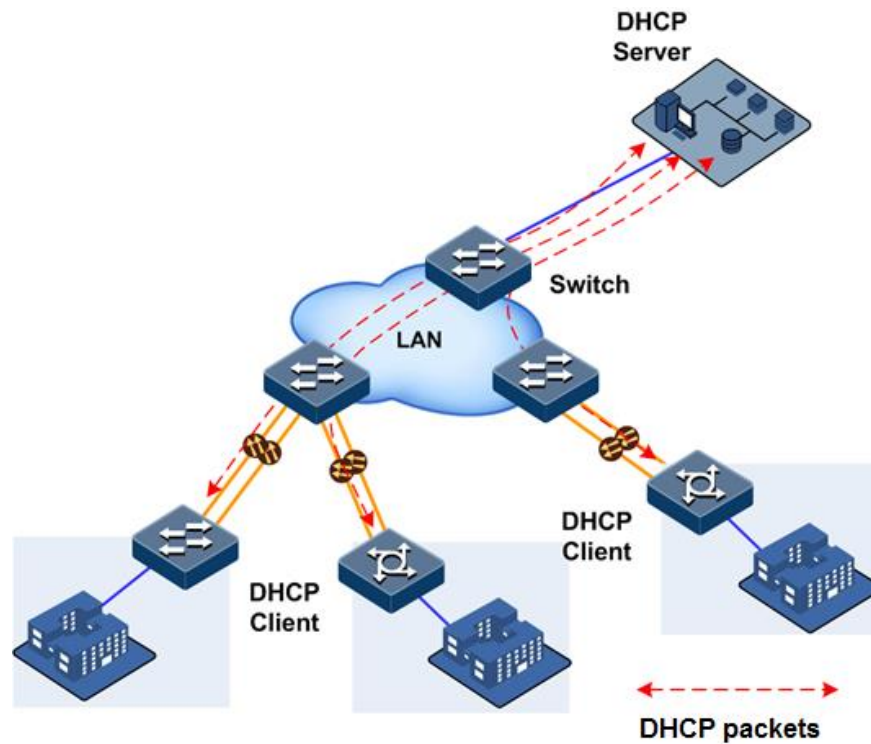
- ZTP
- DHCP Client
- DHCP Server
- DHCP Relay

4.1 ZTP

4.1.1 Introduction

Zero Touch Provisioning (ZTP) refers to that the device needs no manual configurations; it automatically sends DHCP packets for applying for an IP address to the ZTP server, and automatically downloads the configurations file from the ZTP server to update its configurations after obtaining the IP address from the ZTP server. Figure 4-1 shows ZTP server networking.

Figure 4-1 ZTP server networking



Caution

By default, ZTP is enabled on the device. To disable it, configure the device to common client mode.

4.1.2 Default configurations of ZTP

Default configurations of ZTP are as below.

Function	Default value
ZTP mode	Enable

4.1.3 Preparing for configuration

Scenario

To enable the remote device to automatically apply for the IP address after being powered on, configure ZTP. To configure ZTP parameters, see the following section.

Prerequisite

- Connect the device to the DHCP server correctly. Configure the DHCP server correctly.
- Configure the interface connected to the ZTP server to be Up.
- Configure the upstream switch to allow packets of a VLAN of the remote device to pass.
- Leave no configurations on the device.

4.1.4 Configuring ZTP

Configure ZTP for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#ztp { start stop }	Configure ZTP. By default, the DHCP client works in ZTP mode.  Caution To disable ZTP, use the command to disable ZTP.

4.1.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show dhcp client [interface-type interface-number vlan vlan-id]	Show configurations and information automatically obtained by the DHCP client.

4.2 DHCP Client

4.2.1 Introduction

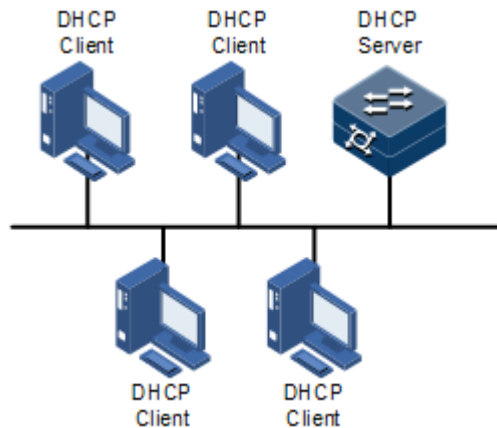
Dynamic Host Configuration Protocol (DHCP) refers to the protocol which assigns configurations, such as the IP address, to users on the TCP/IP network. Based on BOOTP (Bootstrap Protocol) protocol, it has additional features, such as automatically assigning available network addresses, reusing network addresses, and other extended configuration features.

With the enlargement of network scale and development of network complexity, the number of PCs on a network usually exceeds the maximum number of distributable IP addresses. Meanwhile, the widely use of laptops and wireless networks lead to frequent changes of locations and also related IP addresses must be updated frequently. As a result, network configurations become more and more complex. DHCP is developed to solve these problems.

DHCP adopts client/server communication mode. A client applies for configurations to the server (including the IP address, subnet mask, and default gateway), and the server replies with IP address to the client and other related configurations to implement dynamic configurations.

Typical applications of DHCP usually include a set of DHCP server and multiple clients (such as the PC or laptop), as shown in Figure 4-2.

Figure 4-2 DHCP typical networking



DHCP ensures rational allocation, avoid waste, and improve the utilization rate of IP addresses on the entire network.

Figure 4-3 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 4-3 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 4-1 describes fields of DHCP packets.

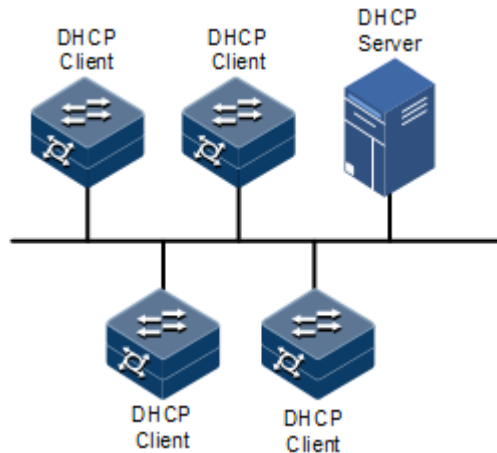
Table 4-1 Fields of a DHCP packet

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. • 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 device can be used as a DHCP client to obtain the IP address from the DHCP server for future management, as shown in Figure 4-4.

Figure 4-4 DHCP Client networking



4.2.2 Preparing for configurations

Scenario

As a DHCP client, the device obtains the IP address from the DHCP server.

The IP address assigned by the DHCP client is limited with a certain lease period when adopting dynamic assignment of IP addresses. The DHCP server will take back the IP address when it is expired. The DHCP client has to renew the IP address for continuous use. The DHCP client can release the IP address if it does not want to use the IP address before expiration.

We recommend configuring the number of DHCP relay devices smaller than 4 if the DHCP client needs to obtain IP address from the DHCP server through multiple DHCP relay devices.

Prerequisite

- Create a VLAN. Add the Layer 3 interface to the VLAN.
- DHCP Snooping is disabled.

4.2.3 Default configurations of DHCP Client

Default configurations of DHCP Client are as below.

Function	Default value
hostname	Host name of the device
class-id	Specified by the startup parameters
client-id	01 MAC

4.2.4 Configuring DHCP Client

Before a DHCP client applies for an IP address, you must create a VLAN. Meanwhile you must configure the DHCP server, otherwise the interface will fail to obtain the IP address through DHCP.

Configure DHCP Client for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter Layer 3 physical interface configuration mode or VLAN interface configuration mode. The following sections take VLAN interface configuration mode for example.
3	Raisecom(config-vlanif-*)#dhcp client { class-id <i>ascii class-id</i> client-id <i>ascii client-id</i> hostname <i>ascii host-name</i> }	Configure information about the DHCP client, 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-vlanif-*)#ip address dhcp enable	Configure the DHCP client to obtain IP address through DHCP.
5	Raisecom(config-vlan*)#ip address dhcp renew	Renew the IP address. If the VLAN 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-vlan*)#ip address dhcp release	Release the IP address.

4.2.5 Checking configurations

Use the following commands to check configuration results.

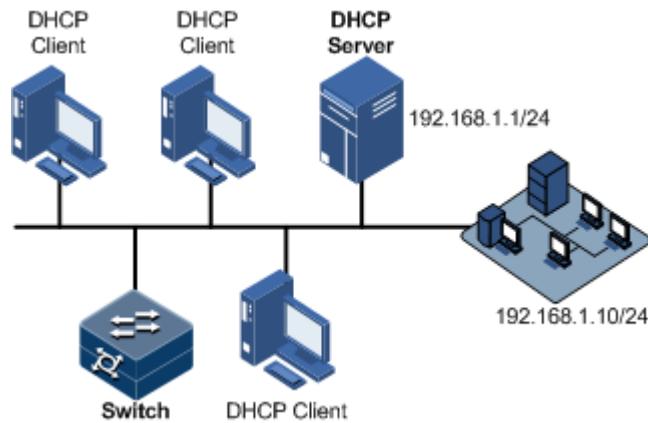
No.	Command	Description
1	Raisecom#show dhcp client [<i>interface-type interface-number</i> <i>vlan vlan-id</i>]	Show configurations of DHCP Client.

4.2.6 Example for configuring DHCP Client

Networking requirements

As shown in Figure 4-5, 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 4-5 DHCP Client networking



Configuration steps

Step 1 Configure the DHCP client.

```
Raisecom#configure
Raisecom(config)#interface vlan 1
Raisecom(config-vlanif-1)#dhcp client hostname ascii raisecom
```

Step 2 Configure the function of applying for IP addresses through DHCP.

```
Raisecom(config-vlanif-1)#ip address dhcp enable
```

Checking results

Use the **show dhcp client** command to show configurations of DHCP Client.

```
Raisecom#show dhcp client
Interface          vlan-1 dhcp client
information :

-----
Current state : Bound
Allocated IP : 192.168.1.2
Subnet Mask           : 255.255.255.0

Server IP           : 192.168.1.1

Allocated lease : 86400 seconds
Lease T1 time : 43200 seconds
Lease T2 time : 75600 seconds
Lease           obtained : 2023/07/18 Tue 18:49:37
```



```
Lease timeout : 2023/07/19 wed 18:49:37
Transaction ID : 0x5558ec
Client ID :
Class ID :
Hostname : raisecom
DNS :
Getway :
Domain :
Lease time will time out in 0 days 23 hours 59 minutes 49 seconds.
-----
```

4.3 DHCP Server

4.3.1 Introduction

Dynamic Host Configuration Protocol (DHCP) refers to assigning IP address configurations dynamically for users on the TCP/IP network. It is based on BOOTP (Bootstrap Protocol) protocol, and automatically adds the specified available network address, network address 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:

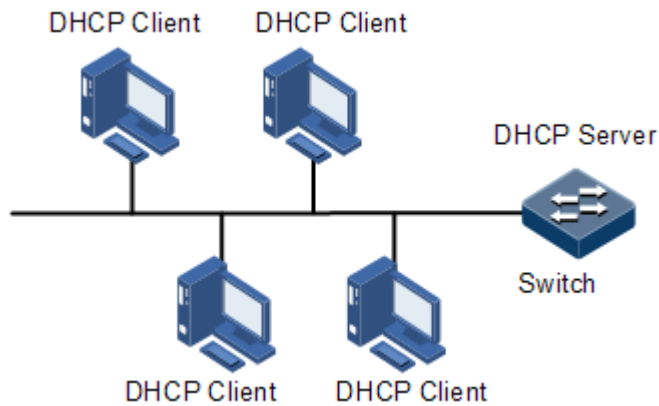
- The network scale is large. It requires much workload for manual configurations, and is difficult to manage the entire network intensively.
- The number of hosts on the network is greater than that of IP addresses, which makes it unable to assign a fixed IP address for each host and restricts the number of users connected to network simultaneously.
- Only the minority of hosts on the network need fixed IP addresses, most of hosts have no requirement for fixed IP address.

After a DHCP client obtains the IP address from the DHCP server, it cannot use the IP address permanently but in a fixed period, which is called the lease period. You can specify the duration of the lease period.

DHCP ensures rational allocation, avoids waste of IP addresses, and improves the utilization rate of IP addresses on the entire network.

The device, as the DHCP server, assigns dynamic IP addresses to clients, as shown in Figure 4-6.

Figure 4-6 DHCP Server and Client networking



DHCP packets

Figure 4-7 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 4-7 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 4-2 describes fields of a DHCP packet.

Table 4-2 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

Field	Length	Description
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.
Transaction ID	4	A random number selected by the client to initiate a request, used to identify an address request process
Seconds	2	Duration after the DHCP request for the DHCP client, fixed to 0, being idle currently
Flags	2	Bit 1 is the broadcast reply flag, used to mark that the DHCP server response packet is transmitted in unicast or broadcast mode. • 0: unicast • 1: broadcast Other bits are reserved.
Client IP address	4	IP address of the DHCP client, only filled when the client is in bound, updated or re-bound status, used to respond to ARP request
Your (client) IP address	4	IP address of the DHCP client assigned by the DHCP server
Server IP address	4	IP address of the DHCP server
Relay agent IP address	4	IP address of the first DHCP relay passing by the request packet sent by the DHCP client
Client hardware address	16	Hardware address of the DHCP client
Server host name	64	Name of the DHCP server
File	128	Startup configuration file name and path assigned by the DHCP server to the DHCP client
Options	Modifiable	A modifiable option field, including packet type, available lease period, IP address of the DNS server, IP address of the WINS

4.3.2 Preparing for configurations

Scenario

When working as the DHCPv4 server, the device can assign IP addresses to DHCPv4 clients.

Prerequisite

- Configure the IP address of the interface.

- Disable DHCP Client and DHCP Relay on the interface.

4.3.3 Creating and configuring the IPv4 address pool

Configure the IPv4 address pool for the device as below.

Step	Command	Description
1	Raisecom# configure	Enter global configuration mode.
2	Raisecom(config)# dhcp start	Enable global DHCP.
3	Raisecom(config)# dhcp pool <i>pool-name</i>	Create an IPv4 address pool, and enter address pool configuration mode.
4	Raisecom(config-dhcp-pool-*)# ip range <i>start-ip-address</i> <i>end-ip-address</i> mask <i>mask</i>	Configure the range of IP addresses in the IPv4 address pool.
5	Raisecom(config-dhcp-pool-*)# dhcp server exclude-ip <i>start-ip-address</i> [<i>end-ip-address</i>]	Configure the range of excluded IP addresses in the IPv4 address pool.
6	Raisecom(config-dhcp-pool-*)# lease-time { <i>hour</i> day <i>day</i> hour <i>hour</i> minute <i>minute</i> unlimited default }	Configure the lease period for the IPv4 address pool.
7	Raisecom(config-dhcp-pool-*)# dns <i>ip-address</i> [backup]	Configure the DNS server address of the IPv4 address pool.
8	Raisecom(config-dhcp-pool-*)# gateway <i>ip-address</i>	Configure the default gateway of the IPv4 address pool.
9	Raisecom(config-pool)# option 43 [sub-option <i>option-code</i>] { ascii <i>ascii-string</i> hex <i>hex-string</i> }	Configure information carried by the option.

4.3.4 Enabling DHCP Server on the interface

Enable DHCP Server on the interface for the device as below.

Step	Command	Description
1	Raisecom# configure	Enter global configuration mode.
2	Raisecom(config)# interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode or Layer 3 physical interface configuration mode. The following steps take VLAN interface configuration mode for example.
3	Raisecom(config-vlanif-*)# ip dhcp server	Enable DHCP Server on the interface.

4.3.5 Recycling the IP address pool

Recycle the IP address pool for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#no dhcp pool <i>pool-name</i>	Recycle the IP address pool.

4.3.6 Configuring DHCPv4 Server PING

Configure DHCPv4 Server PING for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#dhcp address-check-time { <i>period</i> default }	Configure the timeout time for waiting for checking whether the IP address assigned by the DHCP Server is occupied before assignment. The value 0 indicates that no check is conducted. By default, the timeout time is 500ms.

4.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show dhcp config	Show configurations of DHCP Server.
2	Raisecom#show dhcp information	Show detailed information about DHCP Server.
3	Raisecom#show dhcp server user-bind	Show assigned IPv4 addresses and clients information.
4	Raisecom#show dhcp server statistics	Show packet statistics on the DHCP Server.
5	Raisecom#show dhcp server pool	Show configurations of the address pool of DHCP Server.

4.3.8 Maintenance

Maintain the device as below.

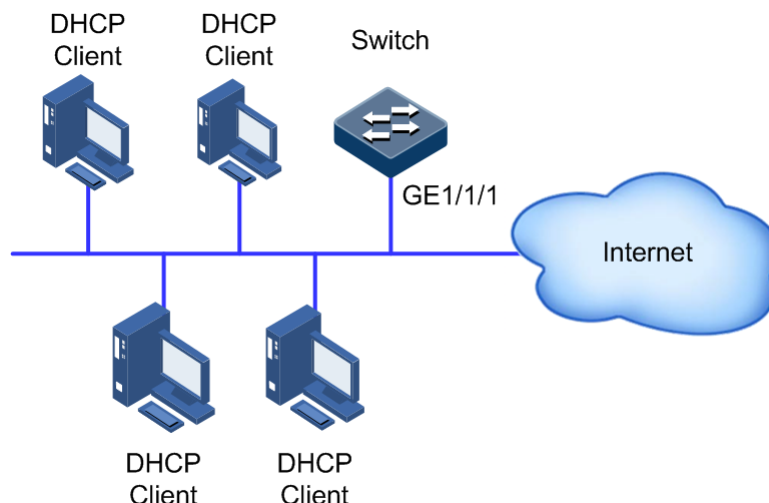
Command	Description
Raisecom(config)#reset dhcp server statistics	Clear statistics on DHCP Server.

4.3.9 Example for configuring DHCPv4 Server

Networking requirements

As shown in Figure 4-8, 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 4-8 DHCP Server networking



Configuration steps

Step 1 Create an IP address pool, and configure it.

```
Raisecom#configure
Raisecom(config)#dhcp start
Raisecom(config-dhcp-pool-1)#dhcp pool 1
Raisecom(config-dhcp-pool-1)#ip range 172.31.1.2 172.31.1.100 mask
255.255.255.0
Raisecom(config-dhcp-pool-1)#lease-time day 0 hour 8 minute 0
Raisecom(config-dhcp-pool-1)#dns 172.31.100.1
Raisecom(config-dhcp-pool-1)#exit
```

Step 2 Configure interface DHCP Server.

```
Raisecom(config)#interface vlan 1
Raisecom(config-vlanif-1)#ip address 172.31.1.1/24
Raisecom(config-vlanif-1)#ip dhcp server
```

Checking results

Use the **show dhcp config** command to show configurations of DHCP Server.

```
Raisecom#show dhcp config
!
dhcp start
dhcp pool 1
ip range 172.31.1.2 172.31.1.100 mask 255.255.255.0
dns 172.31.100.1
lease-time day 0 hour 8 minute 0
!
interface vlan 1
ip dhcp server
```

Use the **show dhcp server pool** command to show configurations of the address pool of the DHCP server.

```
Raisecom#show dhcp server pool
DHCP Pool 1 information :
-----
IP range           : 172.31.1.2 to 172.31.1.100
Mask               : 255.255.255.0
Gateway           : 0.0.0.0
DNS               : main :
172.31.100.1      , backup : 0.0 .0.0
Lease             : 0 days 8 hours 0 minutes
                  Total Number      :
99
Used Number       : 0
-----
```

4.4 DHCP Relay

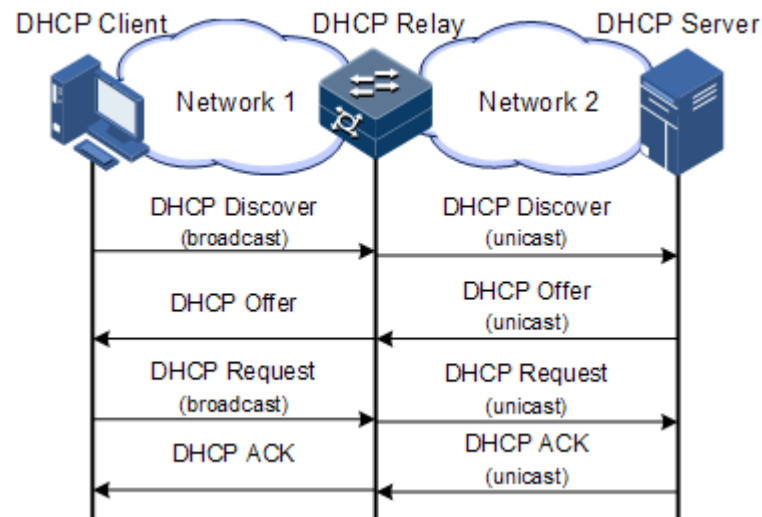
4.4.1 Introduction

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 4-9 shows typical application of DHCP Relay.

Figure 4-9 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.

4.4.2 Preparing for configurations

Scenario

When DHCP Client and DHCP Server are not in the same segment, you can use DHCP Relay function to make DHCP Client and DHCP Server in different segments carry relay service, and relay DHCP protocol packets across segment to destination DHCP server, so that DHCP Client in different segments can share the same DHCP server.

Prerequisite

N/A

4.4.3 Default configurations of DHCP Relay

Default configurations of DHCP Relay are as below.

Function	Default value
Global DHCP Relay	Disable
Interface DHCP Relay	Disable
Global DHCPv6 Relay	Disable
Interface DHCPv6 Relay	Disable

4.4.4 Configuring interface DHCP Relay

Configure interface DHCP Relay for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#dhcp start	Enable global DHCP Relay.
3	Raisecom(config)#interface vlan vlan-id	Enter VLAN interface configuration mode or Layer 3 physical interface configuration mode. The following steps take VLAN interface configuration mode for example.
4	Raisecom(config-vlanif-*)#ip dhcp relay	Enable interface DHCP Relay.
5	Raisecom(config-vlanif-*)#dhcp relay server-ip ip-address	Configure the IP address of the DHCP server.

4.4.5 Configuring interface DHCPv6 Relay

Configure interface DHCPv6 Relay for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#dhcpv6 start	Enable global DHCPv6 Relay.
3	Raisecom(config)#interface vlan vlan-id	Enter VLAN interface configuration mode or Layer 3 physical interface configuration mode. The following steps take VLAN interface configuration mode for example.
4	Raisecom(config-vlanif-*)#dhcpv6 relay	Enable interface DHCPv6 Relay.
5	Raisecom(config-vlanif-*)#dhcpv6 relay destination ipv6-address	Configure the IPv6 address of the DHCPv6 server.

4.4.6 Configuring DHCP Relay to support Option 82

Configure DHCP Relay to support Option 82 for the device as below.

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

Step	Command	Description
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode or Layer 3 physical interface configuration mode. The following steps take VLAN interface configuration mode for example.
3	Raisecom(config-vlanif-*)#dhcp relay option82 enable	Configure DHCP Relay to support Option 82.
4	Raisecom(config-vlanif-*)#dhcp relay option82 { drop keep replace }	Configure the policy for DHCP Relay to process Option 82 request packets.
5	Raisecom(config-vlanif-*)#dhcp relay option82 circuit-id { ascii <i>ascii-string</i> ip- address <i>ip-address</i> format user-defined <i>format-string</i> }	Configure contents of the Circuit ID of DHCP Relay Option 82.
6	Raisecom(config-vlanif-*)#dhcp relay option82 remote-id { ascii <i>ascii-string</i> ip- address <i>ip-address</i> format user-defined <i>format-string</i> }	Configure contents of the Remote ID of DHCP Relay Option 82.

4.4.7 Configuring DHCP Relay to support Option 18/37

Configure DHCP Relay to support Option 18/37 for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#dhcpv6 interface-id format { default user-defined <i>format-string</i> }	Configure the format of the interface-id (Option 18) in DHCPv6 packets.
3	Raisecom(config)#dhcpv6 remote-id format { default user-defined <i>format-string</i> }	Configure the format of the interface-id (Option 37) in DHCPv6 packets.
4	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode or Layer 3 physical interface configuration mode. The following steps take VLAN interface configuration mode for example.
5	Raisecom(config-vlanif- *)#dhcpv6 relay interface-id enable	Configure DHCPv6 Relay to support Option 18.
6	Raisecom(config-vlanif- *)#dhcpv6 relay remote-id enable	Configure DHCPv6 Relay to support Option 37.

4.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show dhcp config	Show configurations of DHCP Relay.
2	Raisecom#show dhcp relay user-bind	Show binding information about DHCP Relay.
3	Raisecom#show dhcp relay statistics	Show statistics on DHCP Relay packets.
4	Raisecom#show dhcpv6 config	Show configurations of DHCPv6 Relay.
5	Raisecom#show dhcpv6 statistics	Show statistics on DHCPv6 Relay packets.

4.4.9 Maintenance

Maintain the device as below.

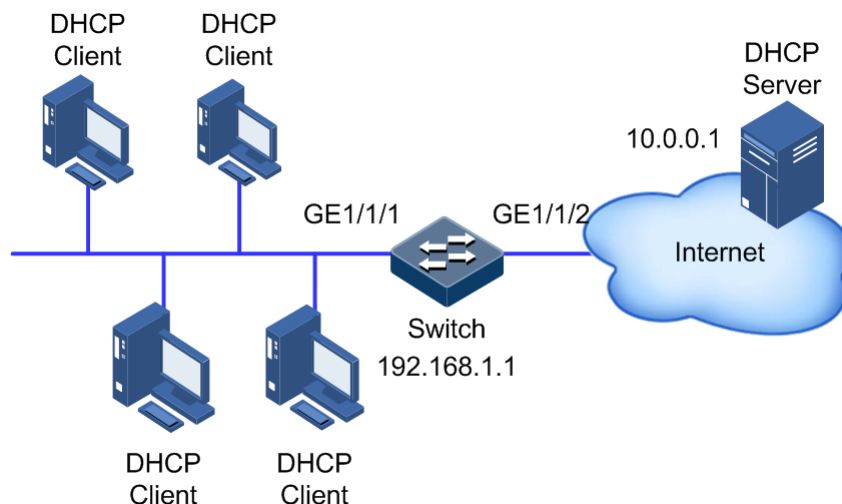
Command	Description
Raisecom(config)#reset dhcp relay statistics	Clear statistics on DHCP Relay.
Raisecom(config)#reset dhcpv6 statistics	Clear statistics on DHCPv6 Relay.

4.4.10 Example for configuring DHCPv4 Relay

Networking requirements

As shown in Figure 4-10, 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 4-10 DHCP Relay networking



Configuration steps

Step 1 Enable interface DHCP Relay.

```
Raisecom#configure
Raisecom(config)#dhcp start
Raisecom(config)#interface vlan 1
Raisecom(config-vlanif-1)#ip address 192.168.1.1/24
Raisecom(config-vlanif-1)#ip dhcp relay
Raisecom(config-vlanif-1)#dhcp relay server-ip 10.0.0.1
Raisecom(config-vlanif-1)#exit
```

Checking results

Use the **show dhcp config** command to show configurations of DHCP Relay.

```
Raisecom#show dhcp config
!
dhcp start

interface vlan 1
ip dhcp relay
dhcp relay server-ip 10.0.0.1
```

!

5 QoS

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

- Introduction
- Priority mapping
- Queue scheduling
- Congestion avoidance
- Rate limiting
- Bandwidth rate limiting

5.1 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

5.1.1 Service models

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 Email. It is implemented by First In First Out (FIFO) queue.

DiffServ

The DiffServ model is a multi-service model, which can satisfy different QoS requirements.

The DiffServ model does not need to maintain state for each flow. It provides differentiated services according to the QoS classification of each packet. Many different methods can be used for classifying QoS packets, such as IP packet priority (IP precedence), the packet source address or destination address.

Generally, DiffServ is used to provide end-to-end QoS services for a number of important applications, which is implemented through the following techniques:

- Committed Access Rate (CAR): CAR refers to classifying the packets according to the preconfigured packet matching rules, such as IP packets priority, the packet source address or destination address. The system continues to send the packets if the flow complies with the rules of token bucket. Otherwise, it discards the packets or remarks IP precedence, DSCP, EXP CAR can not only control the flows, but also mark and remark the packets.
- Queuing technology: the queuing technologies of SP, WRR, DRR, SP+WRR, and SP+DRR cache and schedule the congestion packets to implement congestion management.

5.2 Priority mapping

5.2.1 Introduction

Priority mapping

Class of Service (CoS) refers to the quality of service of a packet within a device, which determines the type of queue that the message belongs to within the device. There are 8 values for CoS, namely, 8 Per Hop Behaviors (PHBs), with priority ranking from high to low as CS7, CS6, EF, AF4, AF3, AF2, AF1, and BE. For a detailed description of PHB behavior, refer to the PHB behavior section.

The color refers to the priority for discarding packets within the device, used to determine the order in which packets are discarded within the same queue when congestion occurs. There are three values for colors, with IEEE-defined priorities ranging from low to high being Green, Yellow, and Red. The priority of discarding actually depends on the configuration of the corresponding parameters.

The processing of packets on each DS node is called PHB. PHB describes the externally visible forwarding behavior adopted by DS nodes for packets. PHB can be defined by priority or by visible service characteristics, such as packet delay, jitter, and packet loss rate. PHB

defines some externally visible forwarding behaviors only and does not specify specific implementation methods.

RFC defines four standard PHBs: Class Selector (CS), Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). Wherein, BE is the default PHB.

In RFC 2474, CS is further divided into two levels, namely, CS6 and CS7. In RFC 2597, AF is further divided into four levels, namely, AF1 to AF4. At this point, PHB has a total of 8 sub-levels, and each PHB has a corresponding CoS within the device. Different CoSs determine the congestion management policies for different flows. At the same time, each PHB is further divided into three colors (color, also known as discarding priority), represented by Green, Yellow, and Red respectively. Different colors determine the congestion avoidance policies for different flows.

Priority trust

Priority trust means that the device uses priority of packets for classification and performs QoS management.

The device supports packet priority trust based on interface, including:

- Differentiated Services Code Point (DSCP) priority
- IEEE 802.1p inner priority
- IEEE 802.1p outer priority

5.2.2 Preparing for configurations

Scenario

You can choose to trust the priority carried by packets from an upstream device, or process packets with untrusted priority through the traffic class and traffic policy. After being configured to priority trust mode, the device processes packets according to their priorities and provides services accordingly.

To specify local priority for packets is the prerequisite for queue scheduling. For packets from the upstream device, you can not only map the external priority carried by packets to different local priorities, but also configure local priority for packets based on interface. Then the device will conduct queue scheduling according to local priority of packets. Generally, IP packets need to be configured with mapping from IP precedence/DSCP to local priority; while VLAN packets need to be configured with mapping from IEEE 802.1p inner priority to local priority.

Prerequisite

N/A

5.2.3 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 IEEE 802.1p outer priority.

Function	Default value
Remarking egress interface priority	Disable

Table 5-1 Default mapping from the IEEE 802.1p ingress direction to local priority and color

IEEE 802.1p priority	PHB	Color
0	BE	green
1	AF1	green
2	AF2	green
3	AF3	green
4	AF4	green
5	EF	green
6	CS6	green
7	CS7	green

Table 5-2 Default mapping from the IEEE 802.1p egress direction to local priority and color

PHB	Color	IEEE 802.1p priority
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4
AF4	red	4

PHB	Color	IEEE 802.1p priority
EF	green	5
EF	yellow	5
EF	red	5
CS6	green	6
CS6	yellow	6
CS6	red	6
CS7	green	7
CS7	yellow	7
CS7	red	7

Table 5-3 Default mapping from the DSCP ingress direction to local priority and color

DHCP	PHB	Color	DHCP	PHB	Color
0	BE	green	32	AF4	green
1	BE	green	33	BE	green
2	BE	green	34	AF4	green
3	BE	green	35	BE	green
4	BE	green	36	AF4	yellow
5	BE	green	37	BE	green
6	BE	green	38	AF4	red
7	BE	green	39	BE	green
8	AF1	green	40	EF	green
9	BE	green	41	BE	green
10	AF1	green	42	BE	green
11	BE	green	43	BE	green
12	AF1	yellow	44	BE	green
13	BE	green	45	BE	green
14	AF1	red	46	EF	green
15	BE	green	47	BE	green
16	AF2	green	48	CS6	green
17	BE	green	49	BE	green
18	AF2	green	50	BE	green

DHCP	PHB	Color	DHCP	PHB	Color
19	BE	green	51	BE	green
20	AF2	yellow	52	BE	green
21	BE	green	53	BE	green
22	AF2	red	54	BE	green
23	BE	green	55	BE	green
24	AF3	green	56	CS7	green
25	BE	green	57	BE	green
26	AF3	green	58	BE	green
27	BE	green	59	BE	green
28	AF3	yellow	60	BE	green
29	BE	green	61	BE	green
30	AF3	red	62	BE	green
31	BE	green	63	BE	green

Table 5-4 Default mapping from the DSCP egress direction to local priority and color

PHB	Color	DSCP
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	10
AF1	yellow	12
AF1	red	14
AF2	green	18
AF2	yellow	20
AF2	red	22
AF3	green	26
AF3	yellow	28
AF3	red	30
AF4	green	34
AF4	yellow	36
AF4	red	38

PHB	Color	DSCP
EF	green	46
EF	yellow	46
EF	red	46
CS6	green	48
CS6	yellow	48
CS6	red	48
CS7	green	56
CS7	yellow	56
CS7	red	56

5.2.4 Configuring types of priorities trusted by the ingress interface

Configure types of priorities trusted by the ingress interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-gigaetherne t1/1/*)# trust [dot1p { inner outer } dscp]	Configure types of priorities trusted by the interface. • dot1p inner: inner priority of packets • dot1p outer: outer priority of packets • dscp: priority of IP packets

5.2.5 Configuring the diffserv profile

Configure the diffserv profile for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#diffserv domain { default ds-domain-name }	Create a diffserv domain profile, or enter the default profile. • default: default profile • ds-domain-name: profile to be created

Step	Command	Description
3	<code>Raisecom(config-dsdomain-ds1)#8021p-inbound 8021p-value phb { BE AF1 AF2 AF3 AF4 EF CS6 CS7 } [green yellow red]</code>	Configure the IEEE 802.1p priority of ingress VLAN packets to be mapped into PHB. • BE AF1 AF2 AF3 AF4 EF CS6 CS7: queue • 8021p-value: IEEE 802.1p priority • green yellow red: color
4	<code>Raisecom(config-dsdomain-ds1)#8021p-outbound { BE AF1 AF2 AF3 AF4 EF CS6 CS7 } [green yellow red] map 8021p-value</code>	Configure the egress PHB and color to be mapped into IEEE 802.1p priority of VLAN packets. • BE AF1 AF2 AF3 AF4 EF CS6 CS7: queue • 8021p-value: IEEE 802.1p priority • green yellow red: color
5	<code>Raisecom(config-dsdomain-ds1)#ip-dscp-inbound dscp-value phb { BE AF1 AF2 AF3 AF4 EF CS6 CS7 } [green yellow red]</code>	Configure the DSCP priority of ingress IP packets to be mapped into PHB. • BE AF1 AF2 AF3 AF4 EF CS6 CS7: queue • dscp-value: DSCP priority • green yellow red: color
6	<code>Raisecom(config-dsdomain-ds1)#ip-dscp-outbound { BE AF1 AF2 AF3 AF4 EF CS6 CS7 } [green yellow red] map dscp-value</code>	Configure the egress PHB and color to be mapped into DSCP priority of IP packets. • BE AF1 AF2 AF3 AF4 EF CS6 CS7: queue • dscp-value: DSCP priority • green yellow red: color

5.2.6 Configuring IEEE 802.1p/DSCP remarking on the egress interface

Configure CoS remarking for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter Layer 2 physical interface configuration mode, or aggregation group configuration mode. Take Layer 2 physical interface configuration mode for example.
3	<code>Raisecom(config-gigaethernet1/1/*)#qos phb marking { 8021p dscp } { enable disable }</code>	Enable/Disable the remarking from the inner priority to outer priority on the egress interface. • 8021p: remark the IEEE 802.1p priority. • dscp: remark the DSCP priority.

5.2.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show differv domain [ds-domain-name]</code>	Show configurations of the diffserv domain profile.

5.3 Queue scheduling

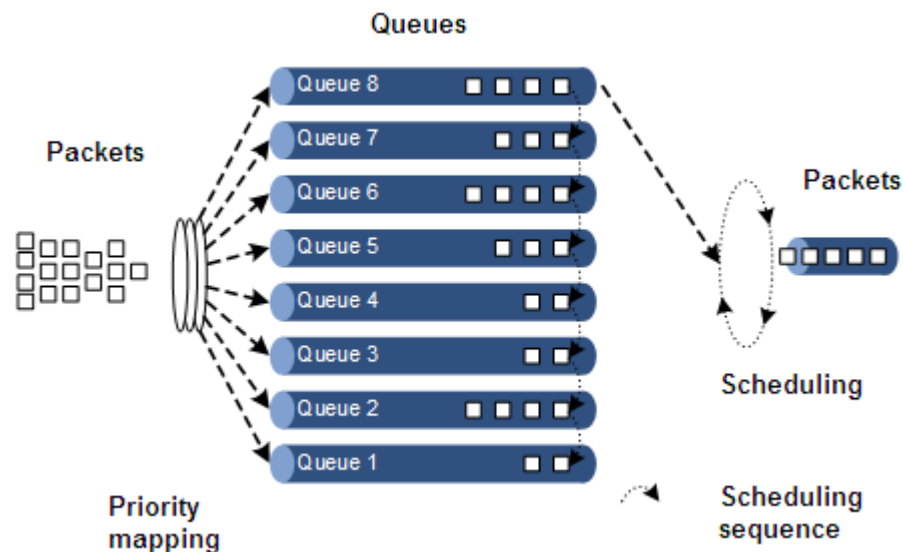
5.3.1 Introduction

The device needs to perform queue scheduling when delay-sensitive services need better QoS services than non-delay-sensitive services and when the network is congested once in a while.

Queue scheduling adopts different scheduling algorithms to send packets in a queue. Scheduling algorithms supported by the device include Strict-Priority (SP), Weight Round Robin (WRR), Weighted Fair Queueing (WRQ), SP+WRR, and SP+WFQ. All scheduling algorithms are designed for addressing specified traffic problems. And they have different effects on bandwidth distribution, delay, and jitter.

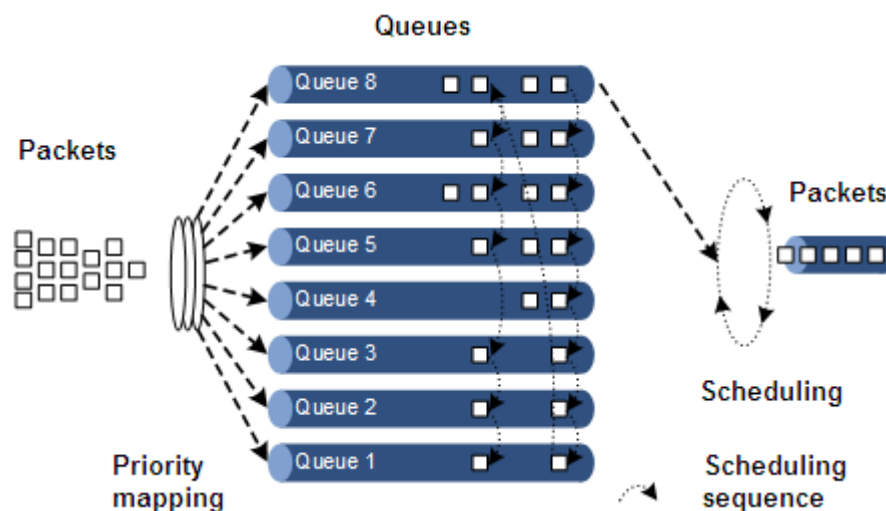
- SP: the device strictly schedules packets in a descending order of priority. Packets with lower priority cannot be scheduled until packets with higher priority are scheduled, as shown in Figure 5-1.

Figure 5-1 SP scheduling



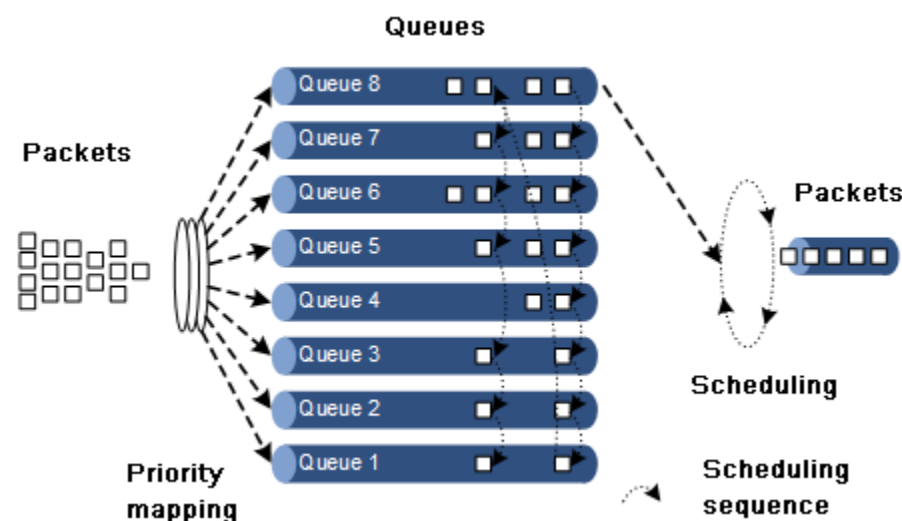
- WRR: on the basis of scheduling packets cyclically according to the priority, the device schedules packets by the weight of each queue in units of bit, as shown in Figure 5-2.

Figure 5-2 WRR scheduling



- WFQ: similar with WRR, on the basis of scheduling packets in a polling manner according to the scheduling sequence, the device schedules packets according to the weight of the queue (based on packet), as shown in DRR scheduling

Figure 5-3 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 some queues with SP scheduling and others with WRR scheduling.
- SP+WFQ: a scheduling mode combining the SP scheduling and WFQ scheduling. In this mode, queues on an interface are divided into 2 groups. You can specify some queues with SP scheduling and others with WFQ scheduling.

5.3.2 Preparing for configurations

Scenario

When the network is congested, you can configure queue scheduling if you want to:

- Balance delay and delay jitter of various packets, preferentially process packets of key services (such as video and voice).
- Fairly process packets of secondary services (such as Email) with identical priority.
- Process packets of different priorities according to respective weight values.

The scheduling algorithm to be chosen depends on the current service condition and customer requirements.

Prerequisite

Enable global QoS.

5.3.3 Default configurations of congestion management

Default configurations of congestion management are as below.

Function	Default value
Queue scheduling mode	SP
Queue weight	• WRR weight for scheduling 8 queues is 1. • WFQ weight for scheduling 8 queues is 81.

5.3.4 Configuring SP queue scheduling

Configure SP queue scheduling for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode, or aggregation group configuration mode. Take Layer 2 physical interface configuration mode for example.
3	Raisecom(config-ge- 1/1/*)#queue scheduling sp	Configure the queue scheduling mode to SP on the interface.

5.3.5 Configuring WRR or SP+WRR queue scheduling

Configure WRR or SP+WRR for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode, or aggregation group configuration mode. Take Layer 2 physical interface configuration mode for example.

Step	Command	Description
3	<code>Raisecom(config-ge-1/1/*)#queue scheduling wrr</code>	Configure the queue scheduling mode to WRR on the interface.
4	<code>Raisecom(config-ge-1/1/*)#queue queue-id weight weight-value</code>	Configure the weight of each queue.

5.3.6 Configuring DRR or SP+DRR queue scheduling

Configure DRR or SP+DRR for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter Layer 2 physical interface configuration mode, or aggregation group configuration mode. Take Layer 2 physical interface configuration mode for example.
3	<code>Raisecom(config-ge-1/1/*)#queue scheduling wfq</code>	Configure the queue scheduling mode to WFQ on the interface.
4	<code>Raisecom(config-ge-1/1/*)#queue queue-id weight weight-value</code>	Configure the weight for each queue.

5.3.7 Configuring queue bandwidth guarantee

Configure queue bandwidth guarantee for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter Layer 2 physical interface configuration mode, or aggregation group configuration mode. Take Layer 2 physical interface configuration mode for example.
3	<code>Raisecom(config-gigaethernet1/1/*)#queue queue-id min-bandwidth { kbps mbps gbps } bandwidth</code>	Configure queue bandwidth guarantee on the interface.

5.3.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show queue interface	Show the queue on the interface
2	Raisecom#show queue statistics interface <i>interface-type interface-number</i>	Show statistics about queues on the interface.

5.3.9 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)#reset queue statistics interface <i>interface-type interface-number</i>	Clear statistics on packets on the interface.

5.3.10 Example for configuring queue scheduling

Networking requirements

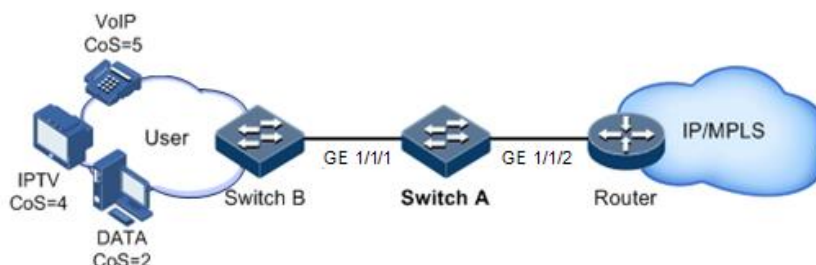
As shown in Figure 5-4, the user uses voice, video and data services.

The CoS of voice services is 5, the CoS of video services is 4, and the CoS of data services is 2.

Congestion can easily occur on Switch A. To reduce network congestion, make the following rules according to different services types:

- For voice services, perform SP scheduling to assign voice services with a high priority.
- For video services, perform WRR scheduling, with weight of 50.
- For data services, perform WRR scheduling, with weight of 20.

Figure 5-4 Queue scheduling networking



Configuration steps

Step 1 Configure interface packets to be mapped into inner priority according to IEEE 802.1p.

```
SwitchA(config)#interface ge 1/1/2
```

```
SwitchA(config-ge-1/1/2)#trust 8021p outer
```

Step 2 Conduct SP+WRR queue scheduling in the egress direction of GE 1/1/2.

```
SwitchA(config)#interface ge 1/1/2
SwitchA(config-ge-1/1/2)#queue scheduling sp+wrr queue 5
SwitchA(config-ge-1/1/2)#queue 4 weight 50
SwitchA(config-ge-1/1/2)#queue 2 weight 20
SwitchA(config-ge-1/1/2)#quit
```

Checking results

Use the following command to show the priority trust mode on the interface.

```
Raisecom#show queue interface ge 1/1/2
Current scheduling algorithm is 'sp+wrr',queue list 5
'Max-BW' means 'Max Bandwidth'
'Min-BW' means 'Min Bandwidth'
```

Interface	Queue	Max-BW	Min-BW	weight
ge-1/1/2	0	0M	0M	1
ge-1/1/2	1	0M	0M	1
ge-1/1/2	2	0M	0M	20
ge-1/1/2	3	0M	0M	1
ge-1/1/2	4	0M	0M	50
ge-1/1/2	5	0M	0M	--
ge-1/1/2	6	0M	0M	1
ge-1/1/2	7	0M	0M	1

5.4 Congestion avoidance

5.4.1 Introduction

By monitoring utilization of network resources (queues/memory buffer), congestion avoidance can discard packets actively when congestion occurs or network traffic increases. It is a traffic control mechanism that is used to resolve network overload by adjusting network traffic.

The traditional packet loss policy uses the Tail-Drop mode to process all packets equally without differentiating class of services. When congestion occurs, packets at the end of a queue are discarded until congestion is resolved.

This Tail-Drop policy may cause TCP global synchronization, making network traffic change between heavy and low and affecting link utilization.

RED

Random Early Detection (RED) discards packets randomly and prevents multiple TCP connection from reducing transmission rate simultaneously to avoid TCP global synchronization.

The RED algorithm configures a minimum threshold and maximum threshold for length of each queue. In addition:

- Packets are not discarded when the queue length is smaller than the minimum threshold.
- All received packets are discarded when the queue length is greater than the maximum threshold.
- Packets to be received are discarded randomly when the queue length is between the minimum and maximum thresholds. The greater the queue size is, the higher the packet drop probability is.

WRED

Weighted Random Early Detection (WRED) also avoids TCP global synchronization by randomly discarding packets. However, the random discarding parameters generated by this technology are based on the priority of the queue, which can distinguish discarding strategies based on the different colors of packets, prioritising high-priority packets and making their discarding probability small.

5.4.2 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.

Prerequisite

N/A

5.4.3 Default configurations of congestion avoidance

Default configurations of congestion avoidance are as below.

Function	Default value
Interface WRED status	Disable

5.4.4 Configuring WRED

Configure WRED for the device as below.

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

Step	Command	Description
2	<code>Raisecom(config)#drop-profile drop-profile-name</code>	Create a WRED profile, and enter WRED configuration mode.
3	<code>Raisecom(config-drop-profile)#color { green non-tcp red yellow } low-limit low-limit-percentage high-limit high-limit-percentage discard-percentage discard-percentage</code>	• { green non-tcp red yellow } : configure the WRED parameters of the green/non-TCP/red/yellow packets. • low-limit-percentage: discarding percentage of WRED, namely, percentage of low-threshold packets discarded by WRED to the queue length • discard-percentage: maximum discarding probability of WRED By default, the discarding percentage of WRED is 100, and the maximum discarding probability is 100.
4	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter Layer 2 physical interface configuration mode, or aggregation group configuration mode. Take Layer 2 physical interface configuration mode for example.
5	<code>Raisecom(config-gigaethernet1/1/*)#qos wred drop-profile-name</code>	Apply the WRED profile to the interface.
6	<code>Raisecom(config-gigaethernet1/1/*)#qos queue queue-index wred drop-profile-name</code>	Apply the discarding profile to the interface queue. • queue-index: interface queue indexes 0–7 correspond with BE, AF1, AF2, AF3, AF4, EF, CS6, and CS7. • drop-profile-name: name of the discarding profile to be applied

5.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show drop-profile</code>	Show information about WRED profiles.

5.5 Rate limiting

5.5.1 Introduction

The device supports rate limiting both based on traffic policy, interface, or VLAN ID. Similar to rate limiting based on traffic policy, the device discards the excess traffic.

5.5.2 Preparing for configurations

Scenario

When the network is congested, you want to restrict burst flow on an interface or VLAN to make packets transmitted at a well-proportioned rate to remove network congestion. In this case, you need to configure rate limiting.

Prerequisite

N/A

5.5.3 Configuring the rate limiting mode

Configure the rate limiting mode for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#rate-limit mode { 11 12 }	Configure the rate limiting mode of traffic.

5.5.4 Configuring rate limiting based on physical interface

Configure rate limiting based on physical interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-gigaetherne1/1/*)#rate-limit { ingress egress } cir <i>cir-value</i>	Configure rate limiting based on interface in the ingress or egress direction.
	Raisecom(config-gigaetherne1/1/*)#rate-limit { ingress egress } cir <i>cir-value</i> cbs <i>cbs-value</i>	Configure rate limiting based on interface in the ingress or egress direction.



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.
- The number of packets discarded due to rate limiting on the egress interface is added to the statistics on discarded packets on the ingress interface.
- The aggregation group interface mode does not support rate limiting in the egress direction.

5.5.5 Configuring rate limiting based on VLAN

Configure rate limiting based on VLAN for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan*)#rate-limit ingress cir <i>cir-value</i>	Configure rate limiting based on VLAN in the ingress direction.
	Raisecom(config-vlan*)#rate-limit ingress cir <i>cir-value</i> cbs <i>cbs-value</i>	Configure rate limiting based on VLAN in the ingress direction.

5.5.6 Configuring rate limiting based on LAG

Configure rate limiting based on LAG for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface port-channel <i>port-channel-id</i>	Enter aggregation group interface configuration mode.
3	Raisecom(config-port-channel*)#rate-limit ingress cir <i>cir-value</i>	Configure rate limiting based on LAG interface in the ingress direction.
	Raisecom(config-port-channel*)#rate-limit ingress cir <i>cir-value</i> cbs <i>cbs-value</i>	Configure rate limiting based on LAG interface in the ingress direction.

5.5.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show rate-limit interface [{ <i>interface-type interface-number</i> <i>vlan vlan-id</i> } [<i>ingress</i> <i>egress</i>]]	Show configurations of rate limiting based on interface.

No.	Command	Description
2	Raisecom#show rate-limit mode	Show the rate limiting mode on the interface.

5.5.8 Example for configuring rate limiting based on interface

Networking requirements

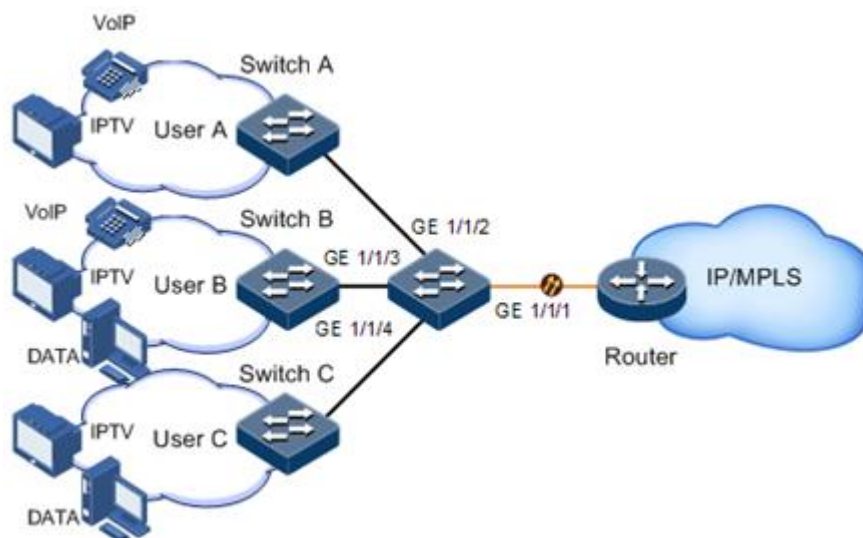
As shown in Figure 5-5, User A, User B, and User C are respectively connected to the device by Switch A, Switch B, and Switch C.

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 5-5 Rate limiting based on interface



Configuration steps

Configure rate limiting based on interface.

```
Raisecom#configure
Raisecom(config)#interface gigabitEthernet 1/1/1
Raisecom(config-gigabitEthernet1/1/1)#rate-limit ingress cir 25000 cbs 100
```

```
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#rate-limit ingress cir 35000 cbs 100
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#rate-limit ingress cir 30000 cbs 100
Raisecom(config-gigaethernet1/1/3)#exit
```

Checking results

Use the **show rate-limit interface** command to show configurations of rate limiting based on interface.

```
Raisecom(config)#show rate-limit interface
```

Interface	Direction	Cir(kbps)	Cbs(kb)	CiOper(kbps)	CbsOper(kb)
gigaethernet1/1/1	ingress	25000	100	25024	101
gigaethernet1/1/2	ingress	35000	100	30016	101
gigaethernet1/1/3	ingress	30000	100	30016	101

5.6 Bandwidth rate limiting

5.6.1 Introduction

Bandwidth rate limiting is a subfunction of QoS and is more flexible than basic QoS.

Bandwidth rate limiting has the following functions:

- Ingress interface
 - Bandwidth guarantee: bandwidth rate limiting implements the bandwidth service based on interface or flow. It also supports hierarchical bandwidth guarantee and refining bandwidth of different service flows.
 - 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. Bandwidth rate limiting 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 device takes different actions over flows of different colors: forward green flows, schedule yellow flows, and discard red flows.

Hierarchical bandwidth guarantee

Hierarchical bandwidth guarantee is more flexible. You can configure the token bucket action or aggregation token bucket for each flow independently and then configure hierarchical token buckets to limit the sum of multiple flows.

Color-aware and marking

If enabled with color-aware, the device is in color-aware status, in which it can identify whether the ingress flow is marked with color. If disabled with color-aware, the device 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.

5.6.2 Preparing for configurations

Scenario

Bandwidth rate limiting is used to guarantee service bandwidth for users and protect network resources and carriers' profits.

Prerequisite

N/A

5.6.3 Default configurations of bandwidth rate limiting

Default configurations of bandwidth rate limiting are as below.

Function	Default value
Color awaring	Disable

5.6.4 Configuring bandwidth guarantee

Creating a bandwidth guarantee profile

Create a bandwidth guarantee profile for the device as below.

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

Step	Command	Description
2	Raisecom(config)#bandwidth-profile <i>bw-profile-id</i> cir <i>cir</i> cbs <i>cbs</i> [color-aware]	Create a bandwidth guarantee profile.
3	Raisecom(config)#bandwidth-profile <i>bw-profile-id</i> description <i>word</i>	Configure the description of the bandwidth guarantee profile.
4	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter Layer 2 physical interface configuration mode.
5	Raisecom(config-gigaetherne1/1/*)#bandwidth ingress <i>bw-profile-id</i>	Apply the bandwidth guarantee profile in the ingress direction of the Layer 2 interface.
	Raisecom(config-gigaetherne1/1/*)#bandwidth egress <i>bw-profile-id</i>	Apply the bandwidth guarantee profile in the egress direction of the Layer 2 interface.
6	Raisecom(config-gigaetherne1/1/*)#bandwidth color-aware { enable disable }	Enable color-aware on packets in the ingress direction of the bandwidth guarantee interface. Use the disable form of this command to disable this function.
7	Raisecom(config-gigaetherne1/1/*)#exit Raisecom(config)#interface <i>vlan</i> <i>vlan-id</i>	Enter VLAN interface configuration mode.
8	Raisecom(config-vlan*)#bandwidth ingress <i>bw-profile-id</i>	Apply the bandwidth guarantee profile in the ingress direction of the VLAN interface.
	Raisecom(config-vlan*)#bandwidth egress <i>bw-profile-id</i>	Apply the bandwidth guarantee profile in the egress direction of the VLAN interface.
9	Raisecom(config-vlan*)#exit Raisecom(config)#interface port-channel <i>port-channel-id</i>	Enter aggregation group interface configuration mode.
10	Raisecom(config-port-channel*)#bandwidth ingress <i>bw-profile-id</i>	Apply the bandwidth guarantee profile in the ingress direction of the LAG interface.

Configuring bandwidth guarantee based on interface+VLAN

Configure bandwidth guarantee based on interface+VLAN for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#bandwidth-profile <i>bw-profile-id</i> cir <i>cir</i> cbs <i>cbs</i> [color-aware]	Create a bandwidth guarantee profile.

Step	Command	Description
3	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
4	Raisecom(config-gigaetherne ^t 1/1/*)# bandwidth ingress vlan <i>vlan-id bwp-profile-id</i>	Apply the bandwidth guarantee profile in the ingress direction of the interface+VLAN.
	Raisecom(config-gigaetherne ^t 1/1/*)# bandwidth egress vlan <i>vlan-id bwp-profile-id</i>	Apply the bandwidth guarantee profile in the egress direction of the interface+VLAN.
5	Raisecom(config-gigaetherne ^t 1/1/*)# exit Raisecom(config)# interface <i>port-channel-id</i>	Enter aggregation group configuration mode.
6	Raisecom(config-port-channel*)# bandwidth ingress vlan <i>vlan-id bwp-profile-id</i>	Apply the bandwidth guarantee profile in the ingress direction of the interface+VLAN.

Configuring bandwidth guarantee based on interface+CoS

Configure bandwidth guarantee based on interface+CoS for the device as below.

Step	Command	Description
1	Raisecom# configure	Enter global configuration mode.
2	Raisecom(config)# bandwidth-profile <i>bwp-profile-id cir cir cbs cbs [color-aware]</i>	Create a bandwidth guarantee profile.
3	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
4	Raisecom(config-gigaetherne ^t 1/1/*)# bandwidth ingress coslist <i>cos-value-list bwp-profile-id</i>	Apply the bandwidth guarantee profile in the ingress direction of the interface+CoS.
	Raisecom(config-gigaetherne ^t 1/1/*)# bandwidth egress coslist <i>cos-value-list bwp-profile-id</i>	Apply the bandwidth guarantee profile in the egress direction of the interface+CoS.
5	Raisecom(config-gigaetherne ^t 1/1/*)# exit Raisecom(config)# interface <i>port-channel port-channel-id</i>	Enter aggregation group configuration mode.
6	Raisecom(config-port-channel*)# bandwidth ingress coslist <i>cos-value-list bwp-profile-id</i>	Apply the bandwidth guarantee profile in the ingress direction of the interface+CoS.
7	Raisecom(config-port-channel*)# exit Raisecom(config)# interface <i>vlan vlan-id</i>	Enter VLAN interface configuration mode.

Step	Command	Description
8	Raisecom(config-vlan*)#bandwidth ingress coslist <i>cos-value-list bwp-profile-id</i>	Apply the bandwidth guarantee profile in the ingress direction of the interface+CoS.
	Raisecom(config-vlan*)#bandwidth egress coslist <i>cos-value-list bwp-profile-id</i>	Apply the bandwidth guarantee profile in the egress direction of the interface+CoS.



Note

If a bandwidth guarantee profile is used by other profiles or applied, it cannot be deleted.

Configuring bandwidth guarantee based on interface+VLAN+CoS

Configure bandwidth guarantee based on interface+VLAN+CoS for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#bandwidth-profile <i>bwp-profile-id cir cir cbs cbs [color-aware]</i>	Create a bandwidth guarantee profile.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
4	Raisecom(config-gigaetherne1/1/*)#bandwidth ingress vlan <i>vlan-id coslist cos-value-list bwp-profile-id</i>	Apply the bandwidth guarantee profile in the ingress direction of the interface+VLAN+CoS.
	Raisecom(config-gigaetherne1/1/*)#bandwidth egress vlan <i>vlan-id coslist cos-value-list bwp-profile-id</i>	Apply the bandwidth guarantee profile in the egress direction of the interface+VLAN+CoS.
5	Raisecom(config-gigaetherne1/1/*)#exit Raisecom(config)#interface port-channel <i>port-channel-id</i>	Enter aggregation group configuration mode.
6	Raisecom(config-port-channel*)#bandwidth ingress vlan <i>vlan-id coslist cos-value-list bwp-profile-id</i>	Apply the bandwidth guarantee profile in the ingress direction of the interface+VLAN+CoS.

5.6.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show bandwidth-profile [<i>bwprofile-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.

6 Multicast

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

- Multicast
- IGMP Snooping
- MLD Snooping

6.1 Multicast

With the continuous development of Internet, more and more interactive data, voice, and video of various types emerge on the network. On the other hand, the emerging e-commerce, online meetings, online auctions, video on demand, remote learning, and other services also rise gradually. These services bring higher requirements on network bandwidth, information security, and paid feature. Traditional unicast and broadcast cannot meet these requirements well, while multicast has met them timely.

Multicast is a point-to-multipoint data transmission method. The method can effectively solve the single point sending and multipoint receiving problems. During transmission of packets on the network, multicast can save network resources and improve information security.

Comparison among unicast, broadcast, and multicast

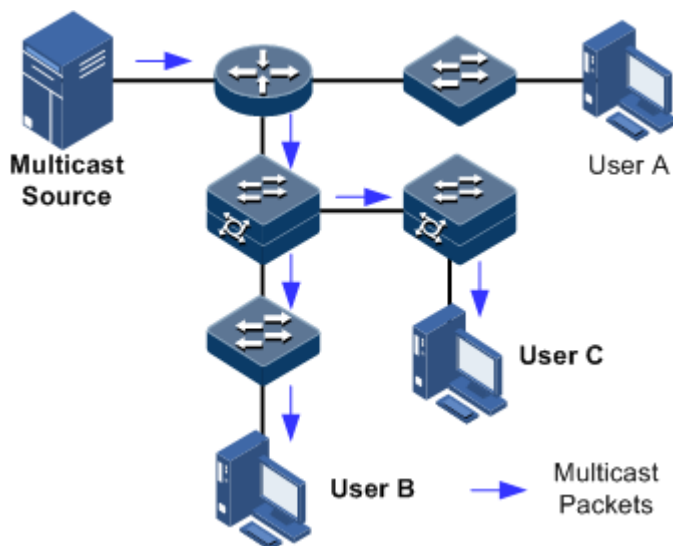
Multicast is a kind of packets transmission method which is parallel with unicast and broadcast.

- Unicast: the system establishes a data transmission path for each user who needs the information, and sends separate copy information about them. Through unicast, the amount of information transmitted over the network is proportional to the number of users, so when the number of users becomes huge, there will be more identical information on the network. In this case, bandwidth will become a bottleneck, and unicast will not be conducive to transmission of large-scale information.
- Broadcast: the system sends information to all users regardless of whether they need or not, so any user will receive it. Through broadcast, the information source delivers information to all users in the segment, which fails to guarantee information security and paid service. In addition, when the number of users who require this kind of information decreases, the utilization of network resources will be very low, and the bandwidth will be wasted seriously.

- Multicast: when some users in the network need specific information, the sender only sends one piece of information, then the transmitted information can be reproduced and distributed in fork junction as far as possible.

As shown in Figure 6-1, 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 6-1 Multicast transmission networking



In summary, the unicast is for a network with sparse users and broadcast is for a network with dense users. When the number of users in the network is uncertain, unicast and broadcast will present low efficiency. When the number of users are doubled and redoubled, the multicast mode does not need to increase backbone bandwidth, but sends information to the user in need. These advantages of multicast make itself become a hotspot in study of the current network technology.

Advantages and application of multicast

Compared with unicast and broadcast, multicast has the following advantages:

- Improve efficiency: reduce network traffic, relieve server and CPU load.
- Optimize performance: reduce redundant traffic and guarantee information security.
- Support distributed applications: solve the problem of point-point data transmission.

The multicast technology is used in the following aspects:

- Multimedia and streaming media, such as, network television, network radio, and realtime video/audio conferencing
- 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

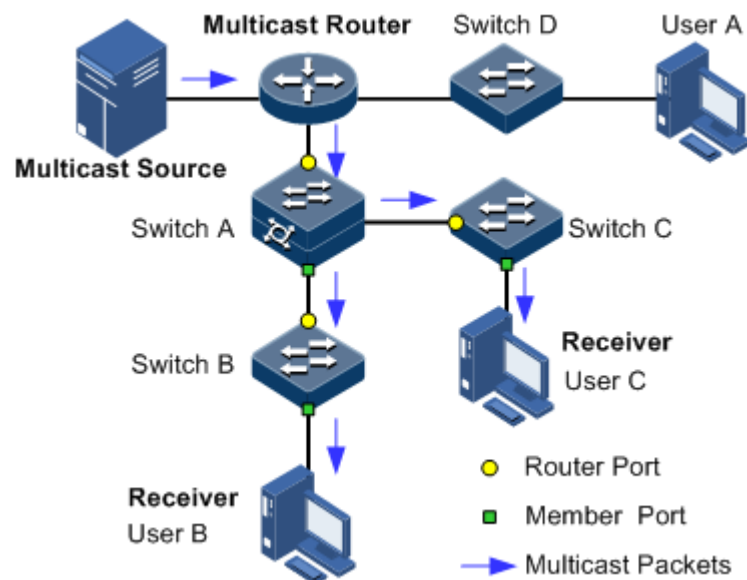
A routed interface refers to the interface towards the multicast router between a multicast router and a host. The device receives multicast packets from this interface.

- Member interface

Known as the Rx interface, a member interface is the interface towards the host between multicast router and the host. The device sends multicast packets from this interface.

Figure 6-2 shows basic concepts in multicast.

Figure 6-2 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

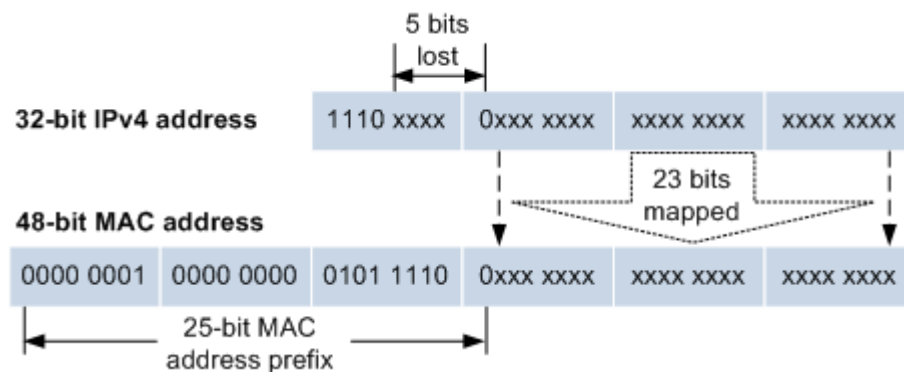
When the Ethernet transmits unicast IP packets, it uses the MAC address of the receiver as the destination MAC address. However, when multicast packets are transmitted, the destination is no longer a specific receiver, but a group with an uncertain number of members, so the Ethernet needs to use the 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 6-3 shows mapping between the IPv4 multicast address and MAC address.

Figure 6-3 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 device may receive extra data besides IPv4 multicast group, and these extra multicast data needs to be filtered by the upper layer on the device.

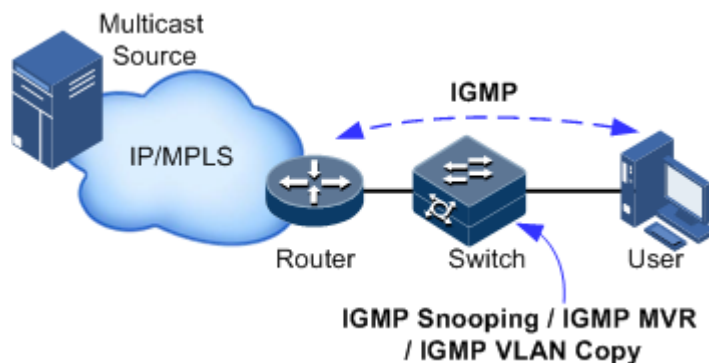
Basis of multicast protocol

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 6-4 shows operating of IGMP and Layer 2 multicast features.

Figure 6-4 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.

Basic functions of Layer 2 multicast

Basic functions of Layer 2 multicast are as below:

- Assign the multicast router interface.
- Enable immediate leave.
- Configure multicast forwarding entries and the aging time of router interfaces.

Basic functions of Layer 2 multicast provide Layer 2 multicast common features, which must be used on the device 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 entry starts a timer, namely, the aging time of a multicast member. The expiration time is IGMP Snooping aging time. The multicast member will be deleted if no IGMP Report packets are received in the aging time. Update timeout for multicast entry when receiving IGMP Report packets. The timer of the multicast entry will be updated when an IGMP Report packet is received.

Immediate leave

On Layer 2 switch running multicast function, the system will not delete the corresponding multicast entry immediately, but wait until the entry is aged after sending Leave packets. You can enable this function to delete the corresponding multicast entry quickly when there are a large number of downstream users and adding or leaving is more frequently required.

6.2 IGMP Snooping

6.2.1 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 device to monitor IGMP sessions between the host and multicast router. When monitoring the IGMP Report packet from the host to a group, the device will add host-related interface to the forwarding entry of this group. Similarly, when a forwarding entry reaches the aging time, the device will delete host-related interface from the forwarding table.

IGMP Snooping forwards multicast data through Layer 2 multicast entries. When receiving multicast data, the device will forward them directly according to the corresponding receiving interface of the multicast entry, instead of flooding them to all interfaces, to save bandwidth of the device effectively.

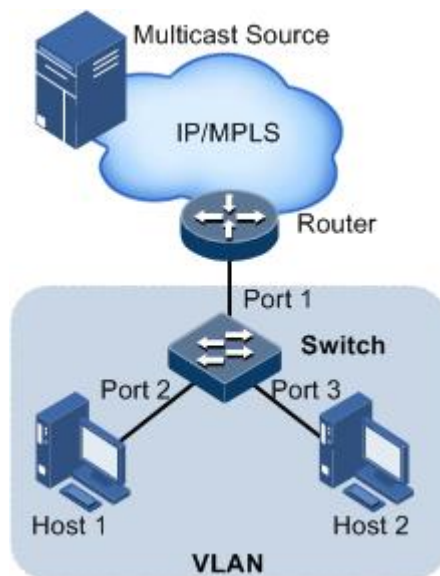
IGMP Snooping establishes a Layer 2 multicast forwarding table, of which entries can be learnt dynamically or configured manually.

6.2.2 Preparing for configurations

Scenario

As shown in Figure 6-5, multiple hosts belonging to a VLAN receive data from the multicast source. You can enable IGMP Snooping on the Switch that connects the multicast router and hosts. By listening IGMP packets transmitted between the multicast router and hosts, creating and maintaining the multicast forwarding table, you can implement Layer 2 multicast.

Figure 6-5 IGMP Snooping networking



Prerequisite

- Create VLANs.
- Add related interfaces to the VLANs.

6.2.3 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
Interface IGMP Snooping status	Disable

Function	Default value
IGMP Snooping version	V2
IGMP query interval	60s
Maximum response time	10s
Aging time of the router interface	180s
Limitation on the maximum number of multicast groups on the interface	No limit

6.2.4 Configuring basic functions of IGMP Snooping

Configure basic functions of IGMP Snooping for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#igmp-snooping start	Enable global IGMP Snooping.
3	Raisecom(config)#igmp-snooping router-aging-time <i>aging-time</i>	(Optional) configure the aging time of the router interface.
4	Raisecom(config)#vlan <i>vlan-id</i>	Enter VLAN configuration mode.
5	Raisecom(config-vlan-10)#igmp-snooping enable	Enable IGMP Snooping on all VLANs.
6	Raisecom(config-vlan-10)#igmp-snooping version { v1 v2 v3 }	(Optional) configure the protocol version.
7	Raisecom(config-vlan-10)#igmp-snooping forwarding-mode { ip mac }	(Optional) configure the forwarding mode of multicast entries to IP or MAC.
8	Raisecom(config-vlan-10)#igmp-snooping require-router-alert enable	(Optional) configure the router alert check.
9	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
10	Raisecom(config-ge-1/0/1)#igmp-snooping enable	Enable interface IGMP Snooping.

6.2.5 Configuring IGMP Snooping Querier

Configure IGMP Snooping Querier for the device as below.

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

2	Raisecom(config)#igmp-snooping query-interval <i>interval</i>	(Optional) configure the common query interval.
3	Raisecom(config)#igmp-snooping robust-count <i>count</i>	(Optional) configure the robustness.
4	Raisecom(config)#vlan <i>vlan-id</i>	Enter VLAN configuration mode.
5	Raisecom(config-vlan-10)#igmp-snooping querier enable	Enable IGMP Snooping Querier. After IGMP Snooping Querier is enabled, the device can send the common query packets and specific group query packets.
6	Raisecom(config-vlan-10)#igmp-snooping send-query source-address <i>ip-address</i>	(Optional) configure the source IP address of query packets sent by the device.
7	Raisecom(config-vlan-10)#igmp-snooping max-response-time <i>response-time</i>	(Optional) configure the maximum response time for query packets.
8	Raisecom(config-vlan-10)#igmp-snooping lastmember-queryinterval <i>interval</i>	(Optional) configure the interval for sending specific group query packets.
9	Raisecom(config-vlan-10)#igmp-snooping lastmember-querynumber <i>number</i>	(Optional) configure the number of specific group query packets to be sent.

6.2.6 Configuring IGMP Snooping packet suppression

Configure IGMP Snooping packet suppression for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
4	Raisecom(config)#vlan <i>vlan-id</i>	Enter VLAN configuration mode.
8	Raisecom(config-vlan-10)#igmp-snooping report-suppress enable	Configure suppression of Report and Leave packets.

6.2.7 Configuring IGMP Snooping multicast copy

Configure IGMP Snooping multicast copy for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#vlan <i>vlan-id</i>	Enter VLAN configuration mode.

3	Raisecom(config-vlan-10)#igmp-snooping forwarding-mode ip	Configure the forwarding mode to IP.
4	Raisecom(config-vlan-10)#igmp-snooping multicast-duplicate enable	Enable multicast copy.
5	Raisecom(config-vlan-10)#igmp-snooping multicast user-vlan vlan-list	Configure the user VLAN associated with multicast copy.

6.2.8 Configuring the static multicast member of IGMP Snooping

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface interface-type interface-number	Enter physical interface configuration mode.
3	Raisecom(config-ge-1/0/1)#igmp-snooping static-group group-address group-address [source-address source-address] vlan vlan-id [user-vlan vlan-list]	Configure the interface as a static multicast member.



Note

- To configure the static multicast member of the source address, you need to configure the protocol version to v3.
- To configure the user VLAN, you need to configure multicast copy.

6.2.9 Configuring IGMP Snooping Proxy

Configure IGMP Snooping Proxy for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#vlan vlan-id	Enter VLAN configuration mode.
3	Raisecom(config-vlan-10)#igmp-snooping workmode igmp-proxy	Configure the working mode to Proxy.
4	Raisecom(config-vlan-10)#igmp-snooping querier enable	Enable IGMP Snooping Querier. The IGMP Snooping Querier must be enabled in Proxy mode; otherwise, multicast entries may be aged.
5	Raisecom(config-vlan-10)#igmp-snooping proxy-ip ip-address	(Optional) configure the IP address of the Proxy in Proxy mode.

6.2.10 Configuring the limit on the number of IGMP Snooping interface multicast groups

Configure the limit on the number of IGMP Snooping interface multicast groups for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-ge-1/0/1)#igmp-snooping group-limit <i>number</i> [action { delay replace }]	Configure the limit on the number of IGMP Snooping interface multicast groups.

6.2.11 Configuring the multicast policy of IGMP Snooping

Configure the multicast policy of IGMP Snooping for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#acl-ipv4 <i>list-id</i>	Create an ACL policy profile, and configure it. The policy takes effect on the permit and deny actions only of the destination IP address.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
4	Raisecom(config-ge-1/0/1)#igmp-snooping group-policy acl-ipv4 <i>list-id</i>	Bind the interface multicast policy with the ACL profile.
5	Raisecom(config)#vlan <i>vlan-id</i>	Enter VLAN configuration mode.
6	Raisecom(config-vlan-10)#igmp-snooping group-policy acl-ipv4 <i>list-id</i>	Bind the VLAN multicast policy with the ACL profile.



Note

If a VLAN multicast policy and an interface multicast policy are concurrently configured, and the VLAN multicast policy is deny, the policy of the interface will not be checked.

6.2.12 Configuring IGMP Snooping SSM Mapping

Configure IGMP Snooping SSM Mapping for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#acl- ipv4 list-id	Create an ACL policy profile, and configure it. The policy takes effect on the permit and deny actions only of the destination IP address.
3	Raisecom(config)#vlan vlan-id	Enter physical interface configuration mode.
4	Raisecom(config-vlan- 10)#igmp-snooping forwarding-mode ip	Configure the forwarding mode to IP.
5	Raisecom(config-vlan- 10)#igmp-snooping version v3	Configure the protocol version to v3.
6	Raisecom(config-vlan- 10)#igmp-snooping ssm- mapping enable	Enable SSM Mapping.
7	Raisecom(config-vlan- 10)#igmp-snooping ssm- mapping acl-ipv4 list-id source-address ip-address	Map the multicast address into the source address. The command takes effect on the group address of which the ACL action is permit.

6.2.13 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show igmp- snooping config	Show configurations of IGMP Snooping.
2	Raisecom#show igmp- snooping interface	Show information about IGMP Snooping interfaces.
3	Raisecom#show igmp- snooping vlan	Show information about IGMP Snooping multicast VLANs.
4	Raisecom#show igmp- snooping forwarding-table	Show multicast entries of IGMP Snooping.

6.2.14 Maintenance

Maintain the device as below.

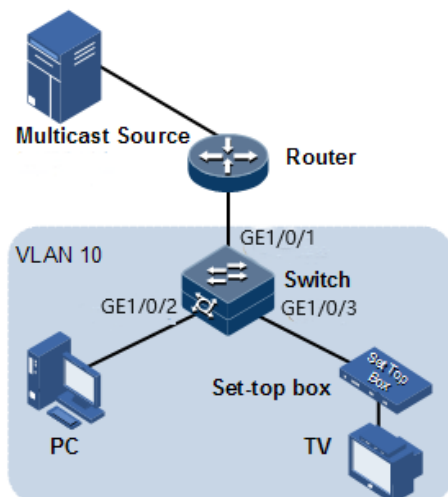
Command	Description
Raisecom(config)#reset igmp- snooping forwarding-table	Clear dynamically learnt multicast entries.
Raisecom(config)#reset igmp- snooping statistics	Clear statistics on IGMP Snooping packets.

6.2.15 Example for configuring basic functions of IGMP Snooping

Networking requirements

As shown below, switch interface gigaehternet 1/0/1 is connected to the multicast router. Switch interfaces Gigaethernet 1/0/2 and Gigaethernet 1/0/3 are connected to user devices, which are in VLAN 10. Configure the switch with IGMP Snooping.

Figure 6-6 Configuring basic functions of IGMP Snooping



Configuration steps

Step 1 Create a VLAN. Add interfaces to it.

```
Raisecom#configure
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port link-type trunk
Raisecom(config-ge-1/0/1)#port trunk allow-pass vlan 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port link-type access
Raisecom(config-ge-1/0/2)#port default vlan 10
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port link-type access
Raisecom(config-ge-1/0/3)#port default vlan 10
Raisecom(config-ge-1/0/3)#quit
```

Step 2 Enable IGMP Snooping.

```
Raisecom(config)#igmp-snooping start
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#igmp-snooping enable
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#igmp-snooping enable
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#igmp-snooping enable
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#igmp-snooping enable
Raisecom(config-ge-1/0/3)#quit
```

Checking results

Use the following command to show configurations of the IGMP Snooping.

```
Raisecom#show igmp-snooping config
!
igmp-snooping start
!
vlan 10
  igmp-snooping enable
!
interface ge 1/0/1
  igmp-snooping enable
!
interface ge 1/0/2
  igmp-snooping enable
!
interface ge 1/0/3
  igmp-snooping enable
```

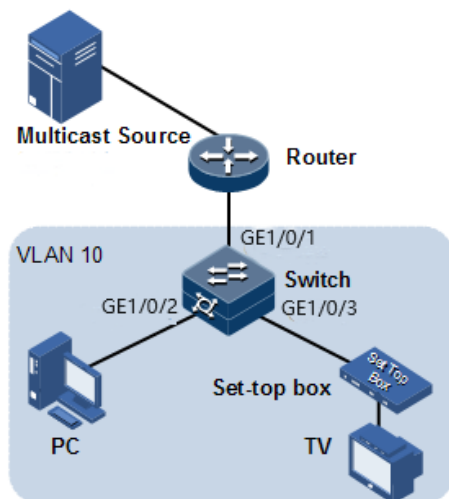
6.2.16 Example for configuring the static member of IGMP Snooping

Networking requirements

As shown below, switch interface gigabitEthernet 1/0/1 is connected to the multicast router. Switch interfaces GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 are connected to user devices, which are in VLAN 10. Configure the switch with IGMP Snooping.

The user under interface gigabitEthernet 1/0/2 wants to permanently receive multicast data from 225.1.1.1 to 225.1.1.3 stably.

Figure 6-7 Configuring the static member of IGMP Snooping



Configuration steps

Step 1 Create a VLAN. Add interfaces to it.

```
Raisecom#configure
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port link-type trunk
Raisecom(config-ge-1/0/1)#port trunk allow-pass vlan 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port link-type access
Raisecom(config-ge-1/0/2)#port default vlan 10
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port link-type access
Raisecom(config-ge-1/0/3)#port default vlan 10
Raisecom(config-ge-1/0/3)#quit
```

Step 2 Enable IGMP Snooping.

```
Raisecom(config)#igmp-snooping start
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#igmp-snooping enable
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#igmp-snooping enable
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#igmp-snooping enable
Raisecom(config-ge-1/0/2)#quit
```

```
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#igmp-snooping enable
Raisecom(config-ge-1/0/3)#quit
```

Step 3 Configure the static multicast member of IGMP Snooping.

```
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/1)#igmp-snooping static-group group-address
225.1.1.1 vlan 10
Raisecom(config-ge-1/0/1)#igmp-snooping static-group group-address
225.1.1.2 vlan 10
Raisecom(config-ge-1/0/1)#igmp-snooping static-group group-address
225.1.1.3 vlan 10
```

Checking results

Use the following command to show configurations of IGMP Snooping.

```
Raisecom#show igmp-snooping config
!
igmp-snooping start
!
vlan 10
  igmp-snooping enable
!
interface ge 1/0/1
  igmp-snooping enable
!
interface ge 1/0/2
  igmp-snooping enable
  igmp-snooping static-group group-address 225.1.1.1 vlan 10
  igmp-snooping static-group group-address 225.1.1.2 vlan 10
  igmp-snooping static-group group-address 225.1.1.3 vlan 10
!
interface ge 1/0/3
  igmp-snooping enable
```

Use the following command to show configurations of static entries of IGMP Snooping.

```
Raisecom#show igmp-snooping forwarding-table
S:Static, D:dynamic, E:Exclude, I:Include
Vlan      (Source,Group)      Port      OutVlan      Flag
Expires
10        (*,225.1.1.1)            ge-1/0/2  10           S/E      --
10        (*,225.1.1.2)            ge-1/0/2  10           S/E      --
10        (*,225.1.1.3)            ge-1/0/2  10           S/E      --
Total Group Number: 3
```

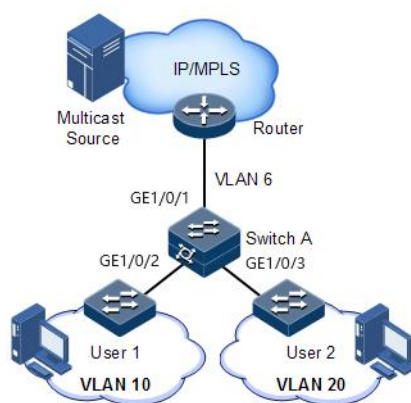
6.2.17 Example for configuring IGMP Snooping multicast copy

Networking requirements

As shown below, switch interface gigaehternet 1/0/1 is connected to the multicast router. Switch interfaces Gigaethernet 1/0/2 and Gigaethernet 1/0/3 are connected to user devices, which are in VLAN 10. The multicast VLAN is different from the user VLAN. Configure IGMP Snooping multicast copy.

Add interface gigaehternet 1/0/1 to VLAN 6. Add user 1 to VLAN 10. Add user 2 to VLAN 20.

Figure 6-8 Configuring IGMP Snooping multicast copy



Configuration steps

Step 1 Create a VLAN. Add interfaces to it.

```
Raisecom#configure
Raisecom(config)#vlan 6,10,20
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port link-type trunk
Raisecom(config-ge-1/0/1)#port trunk allow-pass vlan 6
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port link-type access
Raisecom(config-ge-1/0/2)#port default vlan 10
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port link-type access
Raisecom(config-ge-1/0/3)#port default vlan 20
Raisecom(config-ge-1/0/3)#quit
```

Step 2 Enable IGMP Snooping.

```
Raisecom(config)#igmp-snooping start
Raisecom(config)#vlan 6
Raisecom(config-vlan-6)#igmp-snooping enable
Raisecom(config-vlan-6)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#igmp-snooping enable
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#igmp-snooping enable
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#igmp-snooping enable
Raisecom(config-ge-1/0/3)#quit
```

Step 3 Enable IGMP Snooping multicast copy.

```
Raisecom(config)#vlan 6
Raisecom(config-vlan-6)#igmp-snooping forwarding-mode ip
Raisecom(config-vlan-6)#igmp-snooping multicast-duplicate enable
Raisecom(config-vlan-6)#igmp-snooping multicast user-vlan 10,20
Raisecom(config-vlan-6)#quit
```

Checking results

Use the following command to show configurations of IGMP Snooping.

```
Raisecom#show igmp-snooping config
!
igmp-snooping start
!
vlan 6
  igmp-snooping enable
  igmp-snooping forwarding-mode ip
  igmp-snooping multicast-duplicate enable
  igmp-snooping multicast user-vlan 10,20
!
interface ge 1/0/1
  igmp-snooping enable
!
interface ge 1/0/2
  igmp-snooping enable
!
interface ge 1/0/3
  igmp-snooping enable
```

6.2.18 Example for configuring IGMP Snooping Proxy

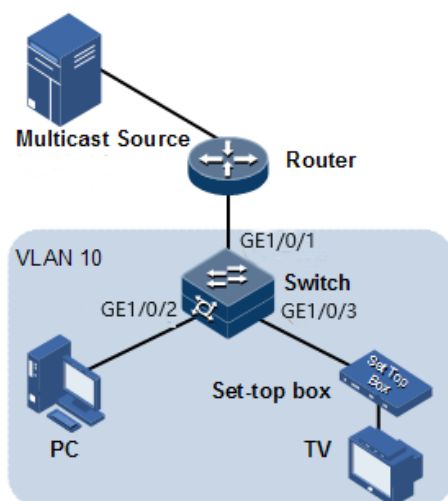
Networking requirements

As shown below, switch interface gigaehternet 1/0/1 is connected to the multicast router. Switch interfaces Gigaethernet 1/0/2 and Gigaethernet 1/0/3 are connected to user devices, which are in VLAN 10. Configure IGMP Snooping.

Enable IGMP Proxy on the switch to reduce the communication between the host and multicast router, without affecting implementation of multicast functions.

When the PC and STB are added to the same multicast group, the switch receives two copies of IGMP Report packets, and sends one copy of IGMP Report packets to the multicast router. The IGMP Query packet sent by the multicast router is not forwarded downstream, but is periodically sent by the switch.

Figure 6-9 Configuring IGMP Snooping Proxy



Configuration steps

Step 1 Create a VLAN. Add interfaces to it.

```
Raisecom#configure
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port link-type trunk
Raisecom(config-ge-1/0/1)#port trunk allow-pass vlan 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port link-type access
Raisecom(config-ge-1/0/2)#port default vlan 10
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port link-type access
Raisecom(config-ge-1/0/3)#port default vlan 10
```



```
Raisecom(config-ge-1/0/3)#quit
```

Step 2 Enable IGMP Snooping.

```
Raisecom(config)#igmp-snooping start
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#igmp-snooping enable
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#igmp-snooping enable
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#igmp-snooping enable
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#igmp-snooping enable
Raisecom(config-ge-1/0/3)#quit
```

Step 3 Enable IGMP Proxy.

```
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#igmp-snooping workmode igmp-proxy
Raisecom(config-vlan-10)#igmp-snooping querier enable
Raisecom(config-vlan-10)#quit
```

Checking results

Use the following command to show configurations of IGMP Snooping.

```
Raisecom#show igmp-snooping config
!
igmp-snooping start
!
vlan 10
  igmp-snooping enable
  igmp-snooping workmode igmp-proxy
  igmp-snooping querier enable
!
interface ge 1/0/1
  igmp-snooping enable
!
interface ge 1/0/2
  igmp-snooping enable
!
interface ge 1/0/3
  igmp-snooping enable
```

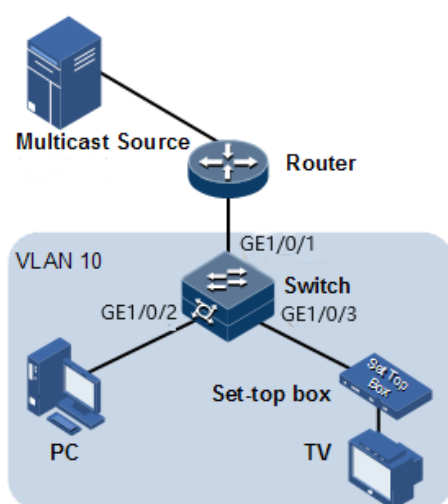
6.2.19 Example for configuring the multicast policy of IGMP Snooping

Networking requirements

As shown below, switch interface gigaehternet 1/0/1 is connected to the multicast router. Switch interfaces Gigaethernet 1/0/2 and Gigaethernet 1/0/3 are connected to user devices, which are in VLAN 10. Configure IGMP Snooping.

Enable the multicast policy on the switch to allow the user under interface Gigaethernet 1/0/2 to join 225.1.1.1 to 225.1.1.3 and the user under interface Gigaethernet 1/0/3 to join 225.1.1.4 to 225.1.1.6.

Figure 6-10 Configuring the multicast policy of IGMP Snooping



Configuration steps

Step 1 Create a VLAN. Add interfaces to it.

```
Raisecom#configure
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port link-type trunk
Raisecom(config-ge-1/0/1)#port trunk allow-pass vlan 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port link-type access
Raisecom(config-ge-1/0/2)#port default vlan 10
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port link-type access
Raisecom(config-ge-1/0/3)#port default vlan 10
Raisecom(config-ge-1/0/3)#quit
```

Step 2 Enable IGMP Snooping.

```
Raisecom(config)#igmp-snooping start
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#igmp-snooping enable
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#igmp-snooping enable
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#igmp-snooping enable
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#igmp-snooping enable
Raisecom(config-ge-1/0/3)#quit
```

Step 3 Configure the ACL profile of the GE 1/0/2 user.

```
Raisecom(config)#acl-ipv4 1001
Raisecom(configure-acl-ipv4-1001)#rule 1 src-ip any dst-ip 225.1.1.1/32
Raisecom(configure-acl-ipv4-1001)#rule 1 action permit
Raisecom(configure-acl-ipv4-1001)#rule 2 src-ip any dst-ip 225.1.1.2/32
Raisecom(configure-acl-ipv4-1001)#rule 2 action permit
Raisecom(configure-acl-ipv4-1001)#rule 3 src-ip any dst-ip 225.1.1.3/32
Raisecom(configure-acl-ipv4-1001)#rule 3 action permit
Raisecom(configure-acl-ipv4-1001)#quit
```

Step 4 Configure the ACL profile of the GE 1/0/3 user.

```
Raisecom(config)#acl-ipv4 1002
Raisecom(configure-acl-ipv4-1002)#rule 1 src-ip any dst-ip 225.1.1.4/32
Raisecom(configure-acl-ipv4-1002)#rule 1 action permit
Raisecom(configure-acl-ipv4-1002)#rule 2 src-ip any dst-ip 225.1.1.5/32
Raisecom(configure-acl-ipv4-1002)#rule 2 action permit
Raisecom(configure-acl-ipv4-1002)#rule 3 src-ip any dst-ip 225.1.1.6/32
Raisecom(configure-acl-ipv4-1002)#rule 3 action permit
Raisecom(configure-acl-ipv4-1002)#quit
```

Step 5 Bind the interface with the multicast policy ACL profile.

```
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#igmp-snooping group-policy acl-ipv4 1001
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#igmp-snooping group-policy acl-ipv4 1002
Raisecom(config-ge-1/0/2)#quit
```

Checking results

Use the following command to show configurations of IGMP Snooping.

```
Raisecom#show igmp-snooping config
!
igmp-snooping start
!
vlan 10
  igmp-snooping enable
!
interface ge 1/0/1
  igmp-snooping enable
  igmp-snooping group-policy acl-ipv4 1001 version 1-3
!
interface ge 1/0/2
  igmp-snooping enable
  igmp-snooping group-policy acl-ipv4 1002 version 1-3
!
interface ge 1/0/3
  igmp-snooping enable
```

Use the following command to show configurations of the ACL profile.

```
Raisecom#show acl config
!
acl-ipv4 1001
  rule 1 src-ip any dst-ip 225.1.1.1/32
  rule 1 action permit
  rule 2 src-ip any dst-ip 225.1.1.2/32
  rule 2 action permit
  rule 3 src-ip any dst-ip 225.1.1.3/32
  rule 3 action permit
acl-ipv4 1002
  rule 1 src-ip any dst-ip 225.1.1.4/32
  rule 1 action permit
  rule 2 src-ip any dst-ip 225.1.1.5/32
  rule 2 action permit
  rule 3 src-ip any dst-ip 225.1.1.6/32
  rule 3 action permit
```

6.3 MLD Snooping

6.3.1 Introduction

MLD Snooping is an IPv6 Layer 2 multicast protocol, which listens to multicast protocol packets sent between Layer 3 multicast devices and user hosts, maintains the information

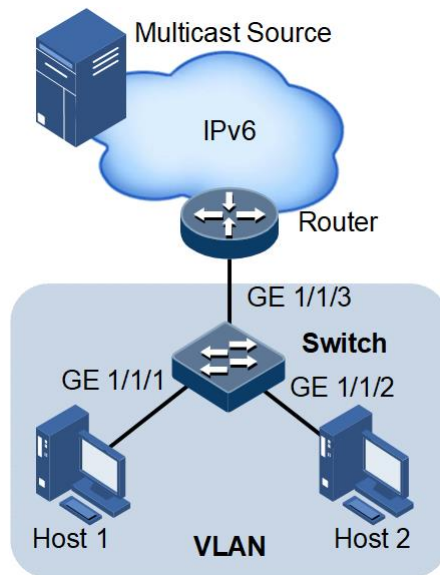
about the egress interface of the group broadcast packet, and then manage and control the forwarding of multicast data packets.

6.3.2 Preparing for configurations

Scenario

As shown in Figure 6-11, multiple hosts receive data from multicast sources and belong to the same VLAN. You can run MLD Snooping on the switch connecting the multicast router and the host. By listening to the MLD packets between the multicast router and the host, you can establish and maintain the multicast forwarding table, and implement Layer 2 multicast.

Figure 6-11 MLD Snooping networking



Prerequisite

- Create VLANs.
- Add related interfaces to the VLANs.

6.3.3 Default configurations of MLD Snooping

Default configurations of MLD Snooping are as below.

Function	Default value
Global MLD Snooping status	Disable
VLAN MLD Snooping status	Disable
Interface MLD Snooping status	Disable
MLD Snooping version	V1
MLD query interval	60s
MLD robustness factor	2

Function	Default value
Maximum response time for sending Query packets	10s
Aging time of the router interface	180s
Limitation on the maximum number of multicast groups on the interface	No limit

6.3.4 Configuring basic functions of MLD Snooping

Configure basic functions of MLD Snooping for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#mld-snooping start	Enable global MLD Snooping.
3	Raisecom(config)#mld-snooping router-aging-time <i>aging-time</i>	(Optional) configure the aging time of the router interface.
4	Raisecom(config)#vlan <i>vlan-id</i>	Enter VLAN configuration mode.
5	Raisecom(config-vlan-10)#mld-snooping enable	Enable MLD Snooping on all VLANs.
6	Raisecom(config-vlan-10)#mld-snooping version { v1 v2 }	(Optional) configure the protocol version.
7	Raisecom(config-vlan-10)#mld-snooping forwarding-mode { ip mac }	(Optional) configure the forwarding mode of multicast entries to IP or MAC.
8	Raisecom(config-vlan-10)#mld-snooping require-router-alert enable	(Optional) configure the router alert check.
9	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
10	Raisecom(config-ge-1/0/1)#mld-snooping enable	Enable interface MLD Snooping.

6.3.5 Configuring MLD Snooping Querier

Configure MLD Snooping Querier for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#mld-snooping query-interval <i>interval</i>	(Optional) configure the common query interval.

3	Raisecom(config)#mld-snooping robust-count <i>count</i>	(Optional) configure the robustness.
4	Raisecom(config)#vlan <i>vlan-id</i>	Enter VLAN configuration mode.
5	Raisecom(config-vlan-10)#mld-snooping querier enable	Enable MLD Snooping Querier. After MLD Snooping Querier is enabled, the device can send the common query packets and specific group query packets.
6	Raisecom(config-vlan-10)#mld-snooping send-query source-address <i>ipv6-address</i>	(Optional) configure the source IP address of query packets sent by the device.
7	Raisecom(config-vlan-10)#mld-snooping max-response-time <i>response-time</i>	(Optional) configure the maximum response time for query packets.
8	Raisecom(config-vlan-10)#mld-snooping lastmember-queryinterval <i>interval</i>	(Optional) configure the interval for sending specific group query packets.
9	Raisecom(config-vlan-10)#mld-snooping lastmember-querynumber <i>number</i>	(Optional) configure the number of specific group query packets to be sent.

6.3.6 Configuring MLD Snooping packet suppression

Configure MLD Snooping packet suppression for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#vlan <i>vlan-id</i>	Enter VLAN configuration mode.
3	Raisecom(config-vlan-10)#mld-snooping report-suppres enable	Configure suppression of Report and Leave packets.

6.3.7 Configuring MLD Snooping multicast copy

Configure MLD Snooping multicast copy for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#vlan <i>vlan-id</i>	Enter VLAN configuration mode.
3	Raisecom(config-vlan-10)#mld-snooping forwarding-mode ip	Configure the forwarding mode to IP.
4	Raisecom(config-vlan-10)#mld-snooping multicast-duplicate enable	Enable multicast copy.

5	Raisecom(config-vlan-10)#mld-snooping multicast user-vlan <i>vlan-list</i>	Configure the user VLAN associated with multicast copy.
---	---	---

6.3.8 Configuring the static multicast member of MLD Snooping

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-ge-1/0/1)#mld-snooping static-group group-address <i>group-address</i> vlan <i>vlan-id</i> [user-vlan <i>vlan-list</i>]	Configure the interface as a static multicast member.



Note

To configure the user VLAN, you need to configure multicast copy.

6.3.9 Configuring MLD Snooping Proxy

Configure MLD Snooping Proxy for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#vlan <i>vlan-id</i>	Enter VLAN configuration mode.
3	Raisecom(config-vlan-10)#mld-snooping workmode mld-proxy	Configure the working mode to Proxy.
4	Raisecom(config-vlan-10)#mld-snooping querier enable	Enable MLD Snooping Querier. The MLD Snooping Querier must be enabled in Proxy mode; otherwise, multicast entries may be aged.
5	Raisecom(config-vlan-10)#mld-snooping proxy-ip <i>ipv6-address</i>	(Optional) configure the IP address of the Proxy in Proxy mode.

6.3.10 Configuring the limit on the number of MLD Snooping interface multicast groups

Configure the limit on the number of MLD Snooping interface multicast groups for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-ge-1/0/1)#mld-snooping group-limit <i>number</i> [action { delay replace }]	Configure the limit on the number of MLD Snooping interface multicast groups.

6.3.11 Configuring the multicast policy of MLD Snooping

Configure the multicast policy of MLD Snooping for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#acl-ipv6 <i>list-id</i>	Create an ACL policy profile, and configure it. The policy takes effect on the permit and deny actions only of the destination IP address.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
4	Raisecom(config-ge-1/0/1)#mld-snooping group-policy acl-ipv6 <i>list-id</i>	Bind the interface multicast policy with the ACL profile.
5	Raisecom(config)#vlan <i>vlan-id</i>	Enter VLAN configuration mode.
6	Raisecom(config-vlan-10)#mld-snooping group-policy acl-ipv6 <i>list-id</i>	Bind the VLAN multicast policy with the ACL profile.



Note

If a VLAN multicast policy and an interface multicast policy are concurrently configured, and the VLAN multicast policy is deny, the policy of the interface will not be checked.

6.3.12 Configuring MLD Snooping SSM Mapping

Configure MLD Snooping SSM Mapping for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#acl-ipv6 <i>list-id</i>	Create an ACL policy profile, and configure it. The policy takes effect on the permit and deny actions only of the destination IP address.

3	Raisecom(config)#vlan vlan-id	Enter physical interface configuration mode.
4	Raisecom(config-vlan- 10)#mld-snooping forwarding-mode ip	Configure the forwarding mode to IP.
5	Raisecom(config-vlan- 10)#mld-snooping version v2	Configure the protocol version to v3.
6	Raisecom(config-vlan- 10)#mld-snooping ssm- mapping enable	Enable SSM Mapping.
7	Raisecom(config-vlan- 10)#mld-snooping ssm- mapping acl-ipv6 list- id source-address ipv6-address	Map the multicast address into the source address. The command takes effect on the group address of which the ACL action is permit.

6.3.13 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show mld- snooping config	Show configurations of MLD Snooping.
2	Raisecom#show mld- snooping interface	Show information about MLD Snooping interfaces.
3	Raisecom#show mld- snooping vlan	Show information about MLD Snooping multicast VLANs.
4	Raisecom#show mld- snooping forwarding-table	Show multicast entries of MLD Snooping.

6.3.14 Maintenance

Maintain the device as below.

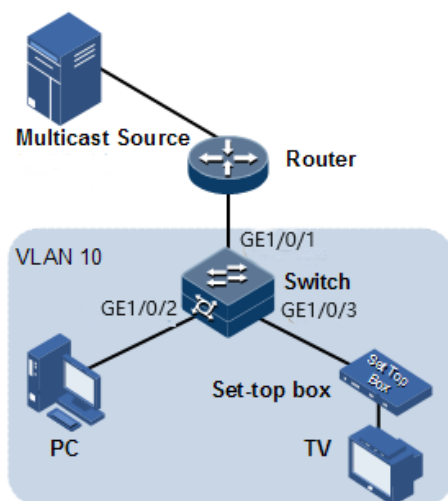
Command	Description
Raisecom(config)#reset mld-snooping forwarding-table	Clear dynamically learnt multicast entries.

6.3.15 Example for configuring basic functions of MLD Snooping

Networking requirements

As shown below, switch interface gigasethernet 1/0/1 is connected to the multicast router. Switch interfaces Gigasethernet 1/0/2 and Gigasethernet 1/0/3 are connected to user devices, which are in VLAN 10. Configure the switch with MLD Snooping.

Figure 6-12 Configuring basic functions of MLD Snooping



Configuration steps

Step 1 Create a VLAN. Add interfaces to it.

```
Raisecom#configure
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port link-type trunk
Raisecom(config-ge-1/0/1)#port trunk allow-pass vlan 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port link-type access
Raisecom(config-ge-1/0/2)#port default vlan 10
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port link-type access
Raisecom(config-ge-1/0/3)#port default vlan 10
Raisecom(config-ge-1/0/3)#quit
```

Step 2 Enable MLD Snooping.

```
Raisecom(config)#mld-snooping start
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#mld-snooping enable
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#mld-snooping enable
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#mld-snooping enable
Raisecom(config-ge-1/0/2)#quit
```

```
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#mld-snooping enable
Raisecom(config-ge-1/0/3)#quit
```

Checking results

Use the following command to show configurations of the MLD Snooping.

```
Raisecom#show mld-snooping config
!
mld-snooping start
!
vlan 10
  mld-snooping enable
!
interface ge 1/0/1
  mld-snooping enable
!
interface ge 1/0/2
  mld-snooping enable
!
interface ge 1/0/3
  mld-snooping enable
```

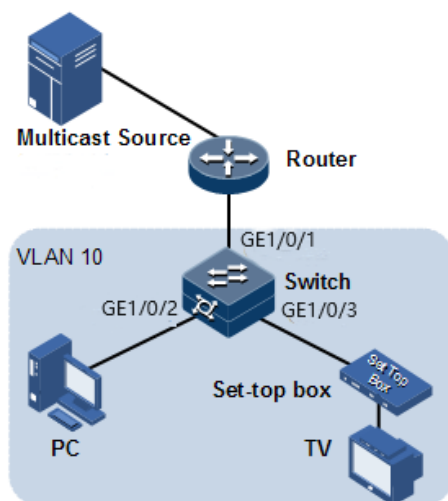
6.3.16 Example for configuring the static member of MLD Snooping

Networking requirements

As shown below, switch interface gigabitEthernet 1/0/1 is connected to the multicast router. Switch interfaces GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 are connected to user devices, which are in VLAN 10. Configure the switch with MLD Snooping.

The user under interface gigabitEthernet 1/0/2 wants to permanently receive multicast data from ff1e::1 to ff1e::3 stably.

Figure 6-13 Configuring the static member of MLD Snooping



Configuration steps

Step 1 Create a VLAN. Add interfaces to it.

```
Raisecom#configure
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port link-type trunk
Raisecom(config-ge-1/0/1)#port trunk allow-pass vlan 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port link-type access
Raisecom(config-ge-1/0/2)#port default vlan 10
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port link-type access
Raisecom(config-ge-1/0/3)#port default vlan 10
Raisecom(config-ge-1/0/3)#quit
```

Step 2 Enable MLD Snooping.

```
Raisecom(config)#mld-snooping start
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#mld-snooping enable
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#mld-snooping enable
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#mld-snooping enable
Raisecom(config-ge-1/0/2)#quit
```

```
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#mld-snooping enable
Raisecom(config-ge-1/0/3)#quit
```

Step 3 Configure the static multicast member of MLD Snooping.

```
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/1)#mld-snooping static-group group-address ff1e::1
vlan 10
Raisecom(config-ge-1/0/1)#mld-snooping static-group group-address ff1e::2
vlan 10
Raisecom(config-ge-1/0/1)#mld-snooping static-group group-address ff1e::3
vlan 10
```

Checking results

Use the following command to show configurations of MLD Snooping.

```
Raisecom#show mld-snooping config
!
mld-snooping start
!
vlan 10
    mld-snooping enable
!
interface ge 1/0/1
    mld-snooping enable
    mld-snooping static-group group-address ff1e::1 vlan 10
    mld-snooping static-group group-address ff1e::2 vlan 10
    mld-snooping static-group group-address ff1e::3 vlan 10
!
interface ge 1/0/2
    mld-snooping enable
!
interface ge 1/0/3
    mld-snooping enable
```

Use the following command to show configurations of static entries of MLD Snooping.

```
Raisecom#show mld-snooping forwarding-table
S:Static, D:dynamic, E:Exclude, I:Include
Vlan      (Source,Group)      Port      OutVlan      Flag
Expires
-----
10         (*,ff1e::1)                ge-1/0/1   10           S/E      --
```

10	(*, ff1e::2)	ge-1/0/1	10	
S/E	--			
10	(*, ff1e::3)	ge-1/0/1	10	S/E --

Total Group Number: 3

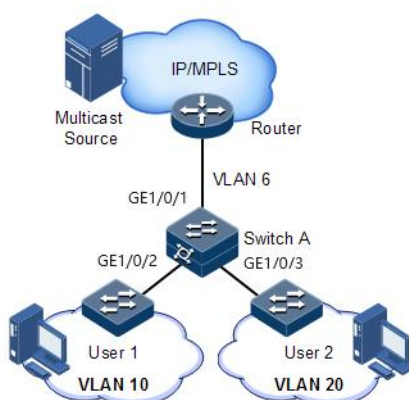
6.3.17 Example for configuring MLD Snooping multicast copy

Networking requirements

As shown below, switch interface gigabitEthernet 1/0/1 is connected to the multicast router. Switch interfaces GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 are connected to user devices, which are in VLAN 10. The multicast VLAN is different from the user VLAN. Configure MLD Snooping multicast copy.

Add interface gigabitEthernet 1/0/1 to VLAN 6. Add user 1 to VLAN 10. Add user 2 to VLAN 20.

Figure 6-14 Configuring MLD Snooping multicast copy



Configuration steps

Step 1 Create a VLAN. Add interfaces to it.

```

Raisecom#configure
Raisecom(config)#vlan 6,10,20
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port link-type trunk
Raisecom(config-ge-1/0/1)#port trunk allow-pass vlan 6
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port link-type access
Raisecom(config-ge-1/0/2)#port default vlan 10
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port link-type access

```

```
Raisecom(config-ge-1/0/3)#port default vlan 20
Raisecom(config-ge-1/0/3)#quit
```

Step 2 Enable MLD Snooping.

```
Raisecom(config)#mld-snooping start
Raisecom(config)#vlan 6
Raisecom(config-vlan-6)#mld-snooping enable
Raisecom(config-vlan-6)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#mld-snooping enable
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#mld-snooping enable
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#mld-snooping enable
Raisecom(config-ge-1/0/3)#quit
```

Step 3 Enable MLD Snooping multicast copy.

```
Raisecom(config)#vlan 6
Raisecom(config-vlan-6)#mld-snooping forwarding-mode ip
Raisecom(config-vlan-6)#mld-snooping multicast-duplicate enable
Raisecom(config-vlan-6)#mld-snooping multicast user-vlan 10,20
Raisecom(config-vlan-6)#quit
```

Checking results

Use the following command to show configurations of MLD Snooping.

```
Raisecom#show mld-snooping config
!
mld-snooping start
!
vlan 10
  mld-snooping enable
  mld-snooping forwarding-mode ip
  mld-snooping multicast-duplicate enable
  mld-snooping multicast user-vlan 10,20
!
interface ge 1/0/1
  mld-snooping enable
!
interface ge 1/0/2
  mld-snooping enable
!
```



```
interface ge 1/0/3
 mld-snooping enable
```

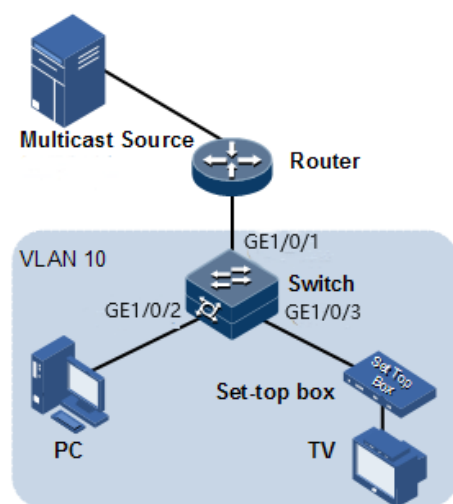
6.3.18 Example for configuring MLD Snooping Proxy

Networking requirements

As shown below, switch interface gigabernet 1/0/1 is connected to the multicast router. Switch interfaces Gigaetherent 1/0/2 and Gigaetherent 1/0/3 are connected to user devices, which are in VLAN 10. Configure MLD Snooping.

Enable MLD Proxy on the switch to reduce the communication between the host and multicast router, without affecting implementation of multicast functions.

Figure 6-15 Configuring MLD Snooping Proxy



Configuration steps

Step 1 Create a VLAN. Add interfaces to it.

```
Raisecom#configure
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port link-type trunk
Raisecom(config-ge-1/0/1)#port trunk allow-pass vlan 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port link-type access
Raisecom(config-ge-1/0/2)#port default vlan 10
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port link-type access
Raisecom(config-ge-1/0/3)#port default vlan 10
```

```
Raisecom(config-ge-1/0/3)#quit
```

Step 2 Enable MLD Snooping.

```
Raisecom(config)#mld-snooping start
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#mld-snooping enable
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#mld-snooping enable
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#mld-snooping enable
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#mld-snooping enable
Raisecom(config-ge-1/0/3)#quit
```

Step 3 Enable MLD Proxy.

```
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#mld-snooping workmode mld-proxy
Raisecom(config-vlan-10)#mld-snooping querier enable
Raisecom(config-vlan-10)#quit
```

Checking results

Use the following command to show configurations of MLD Snooping.

```
Raisecom#show mld-snooping config
!
mld-snooping start
!
vlan 10
  mld-snooping enable
  mld-snooping workmode mld-proxy
  mld-snooping querier enable
!
interface ge 1/0/1
  mld-snooping enable
!
interface ge 1/0/2
  mld-snooping enable
!
interface ge 1/0/3
  mld-snooping enable
```

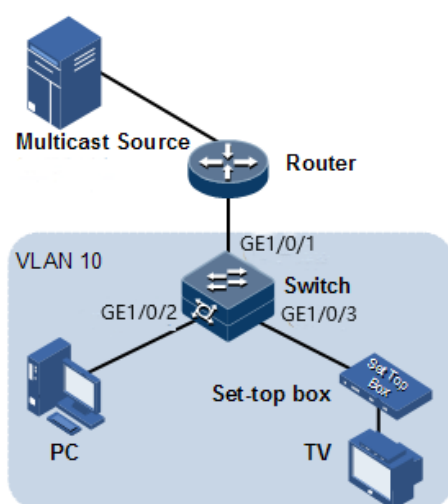
6.3.19 Example for configuring the multicast policy of MLD Snooping

Networking requirements

As shown below, switch interface gigaehternet 1/0/1 is connected to the multicast router. Switch interfaces Gigaethernet 1/0/2 and Gigaethernet 1/0/3 are connected to user devices, which are in VLAN 10. Configure MLD Snooping.

Enable the multicast policy on the switch to allow the user under interface Gigaethernet 1/0/2 to join ff1e::1 to ff1e::3 and the user under interface Gigaethernet 1/0/3 to join ff1e::4 to ff1e::6.

Figure 6-16 Configuring the multicast policy of MLD Snooping



Configuration steps

Step 1 Create a VLAN. Add interfaces to it.

```
Raisecom#configure
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port link-type trunk
Raisecom(config-ge-1/0/1)#port trunk allow-pass vlan 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port link-type access
Raisecom(config-ge-1/0/2)#port default vlan 10
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port link-type access
Raisecom(config-ge-1/0/3)#port default vlan 10
Raisecom(config-ge-1/0/3)#quit
```

Step 2 Enable MLD Snooping.

```
Raisecom(config)#mld-snooping start
Raisecom(config)#vlan 10
Raisecom(config-vlan-10)#mld-snooping enable
Raisecom(config-vlan-10)#quit
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#mld-snooping enable
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#mld-snooping enable
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#mld-snooping enable
Raisecom(config-ge-1/0/3)#quit
```

Step 3 Configure the ACL profile of the GE 1/0/2 user.

```
Raisecom(config)#acl-ipv6 3001
Raisecom(configure-acl-ipv6-3001)#rule 1 src-ip any dst-ip ff1e::1/128
Raisecom(configure-acl-ipv6-3001)#rule 1 action permit
Raisecom(configure-acl-ipv6-3001)#rule 2 src-ip any dst-ip ff1e::2/128
Raisecom(configure-acl-ipv6-3001)#rule 2 action permit
Raisecom(configure-acl-ipv6-3001)#rule 3 src-ip any dst-ip ff1e::3/128
Raisecom(configure-acl-ipv6-3001)#rule 3 action permit
Raisecom(configure-acl-ipv6-3001)#quit
```

Step 4 Configure the ACL profile of the GE 1/0/3 user.

```
Raisecom(config)#acl-ipv6 3002
Raisecom(configure-acl-ipv6-3002)#rule 1 src-ip any dst-ip ff1e::4/128
Raisecom(configure-acl-ipv6-3002)#rule 1 action permit
Raisecom(configure-acl-ipv6-3002)#rule 2 src-ip any dst-ip ff1e::5/128
Raisecom(configure-acl-ipv6-3002)#rule 2 action permit
Raisecom(configure-acl-ipv6-3002)#rule 3 src-ip any dst-ip ff1e::6/128
Raisecom(configure-acl-ipv6-3002)#rule 3 action permit
Raisecom(configure-acl-ipv6-3002)#quit
```

Step 5 Bind the interface with the multicast policy ACL profile.

```
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#mld-snooping group-policy acl-ipv6 3001
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#mld-snooping group-policy acl-ipv6 3002
Raisecom(config-ge-1/0/2)#quit
```

Checking results

Use the following command to show configurations of MLD Snooping.

```
Raisecom#show mld-snooping config
!
mld-snooping start
!
vlan 10
  mld-snooping enable
!
interface ge 1/0/1
  mld-snooping enable
  mld-snooping group-policy acl-ipv6 3001 version 1-2
!
interface ge 1/0/2
  mld-snooping enable
  mld-snooping group-policy acl-ipv6 3002 version 1-2
!
interface ge 1/0/3
  mld-snooping enable
```

Use the following command to show configurations of the ACL profile.

```
Raisecom#show acl config
!
acl- ipv6 3001
  rule 1 src-ip any dst-ip ff1e::1/128
  rule 1 action permit
  rule 2 src-ip any dst-ip ff1e::2/128
  rule 2 action permit
  rule 3 src-ip any dst-ip ff1e::3/128
  rule 3 action permit
acl- ipv6 3002
  rule 1 src-ip any dst-ip ff1e::4/128
  rule 1 action permit
  rule 2 src-ip any dst-ip ff1e::5/128
  rule 2 action permit
  rule 3 src-ip any dst-ip ff1e::6/128
  rule 3 action permit
```

7 OAM

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

- Introduction
- EFM
- Link-state tracking
- VRRP
- CFM

7.1 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.

OAM mode

The interface enabled with EFM OAM is called the OAM entity. EFM OAM supports the following two connection modes:

- Active mode: the OAM entity in active mode can initiate OAM connection.
- Passive mode: the OAM entity in passive mode just waits for connection request of the active OAM entity. If the OAM entities on both ends of the link are in passive mode, they cannot establish OAM connection.

OAM discovery

In the OAM discovery phase, an OAM entity discovers a remote OAM entity and establishes a session with it.

This phase is initiated by the OAM entity in the active mode. Both OAM entities inform the other of its OAM configurations and Ethernet OAM capabilities supported by the local node by exchanging information OAM PDU, and decide whether to establish the OAM connection. If both ends agree on establishment of the OAM connection, Ethernet OAM protocol will work on the link layer.

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 the timeout time, it judges that connection expires and reconnection is required.

Peer fault notification

When a device fails or becomes unavailable, it will cause network interruption. Therefore, the OAM PDU defines a flag bit (Flag domain) that allows the OAM entity to continuously send Information OAM PDU to the peer, informing them of this fault information.

- Link Fault: the peer link signal is lost, so the OAM PDU is sent once per second.
- Dying Gasp: unpredictable failure of the device occurs, which causes the system to be unable to recover, such as power failure, so the device continuously sends OAM PDUs.
- Critical Event: when an uncertain emergency occurs on the device, such as abnormal temperature, the OAM PDU is continuously sent.

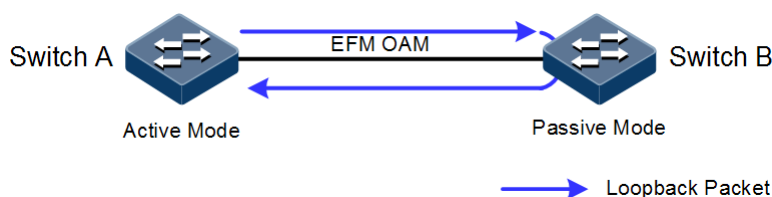
Remote loopback

Remote loopback can be used to locate the area where the fault occurs, and the quality of the link can also be tested with the help of instruments. Regular loopback detection can detect network faults in a timely manner, and locate the specific area where the fault occurs through segmented loopback detection, which helps users clear faults.

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.

As shown in Figure 7-1, local Switch A in the active mode determines the link status by sending packets back.

Figure 7-1 OAM loopback



7.2 EFM

7.2.1 Introduction

Complying with IEEE 802.3ah protocol, Ethernet in the First Mile (EFM) is a link-level Ethernet OAM technology. It provides link connectivity detection, link fault monitoring, and remote fault notification for a link between two directly connected devices. EFM is mainly used for Ethernet links on edges of the network accessed by users.

7.2.2 Preparing for configurations

Scenario

Deploying EFM feature between directly connected devices can efficiently improve Ethernet link management and maintenance capability and ensure stable network operation.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.

7.2.3 Default configurations of EFM

Default configurations of EFM are as below.

Function	Default value
EFM working mode	Active
Period for sending packets	10×100ms
Link timeout	5s
EFM remote loopback status	No responding
Errored frame event monitoring window	1s
Errored frame event monitoring threshold	1 errored frame
Errored frame period event monitoring window	1000ms
Errored frame period event monitoring threshold	1 errored frame
Link errored frame second event monitoring window	100s
Link errored frame second event monitoring threshold	1s
Errored symbol period event monitoring window	1s
Errored symbol period event monitoring threshold	1s
Fault indication status	Enable

7.2.4 Configuring basic functions of EFM

Configure basic functions of EFM for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface interface-type interface-number Example: Raisecom(config)#interface gig Ethernet 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config)#efm max-rate value Example: Raisecom(config-gig Ethernet 1/1/*)#efm max-rate 5	(Optional) configure the maximum transmission rate, which limits the bandwidth occupied by EFM, ensuring that a maximum of a certain number of EFM PDUs can be sent within a certain interval. The range is 1 to 10. The default value is 10. • value: number of sent PDUs per unit time
4	Raisecom(config-gig Ethernet 1/1/*)#efm min-rate value Example: Raisecom(config-gig Ethernet 1/1/*)#efm min-rate 5	(Optional) if the local EFM entity does not receive the EFM PDU from the peer within the discovery timeout, it judges that the discovery connection has failed and the discovery process is restarted. The range is 2 to 30. The default value is 5s. • value: timeout time
5	Raisecom(config-gig Ethernet 1/1/*)#efm mode { active passive } Raisecom(config-gig Ethernet 1/1/*)#exit Example: Raisecom(config-gig Ethernet 1/1/1)#oam active	Configure the working mode of EFM OAM. At least one end is in active mode before configuration; otherwise, link detection cannot proceed. • active: in the active mode, the interface actively sends OAM PDUs to initiate end-to-end discovery or remote loopback processes. • passive: in the passive mode, the interface passively waits for the OAM PDU sent by the peer end.
6	Raisecom(config-gig Ethernet 1/1/*)#exit	Enter global configuration mode.
7	Raisecom(config)#efm { enable disable } Example: Raisecom(config-gig Ethernet 1/1/1)#efm enable	Enable interface EFM OAM. • Enable: enable interface EFM OAM. • Disable: disable interface EFM OAM.

7.2.5 Configuring CFM interface loopback

Configuring OAM remote loopback

OAM provides a link-layer remote loopback mechanism for locating link faults and measuring performance and quality. In link loopback status, the switch sends back all packets except OAM packets received by the link to the peer device. The local device initiates or disables remote loopback through the OAM remote loopback command. The remote device, through the loopback configuration command, controls whether to respond to the loopback command.

Configure OAM remote loopback as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-gigaethernet1/1/*)#efm remote-loopback timeout value Example: Raisecom(config-gigaethernet1/1/*)#efm remote-loopback timeout 5	(Optional) configure the local waiting time for response, which is the response timeout. If no response from the peer is received within this time, the configuration will fail. The range is 1s to 10s. The default value is 10s. value: timeout time
4	Raisecom(config-gigaethernet1/1/*)#efm remote-loopback { supported unsupported } Example: Raisecom(config-gigaethernet1/1/*)#efm min-rate 5	Configure remote loopback to be supported or unsupported. - Supported: supported - Unsupported: unsupported
5	Raisecom(config-gigaethernet1/1/*)#efm remote-loopback start holdtime { <0-1000> default } Example: Raisecom(config-gigaethernet1/1/*)#efm remote-loopback start holdtime 100	Start remote loopback. To avoid the link being unable to forward service data normally for a long time due to user forgetting to stop EFM remote loopback, EFM remote loopback has an automatic cancellation function upon timeout. The holdtime represents the duration of the remote loopback. By default, the duration of remote loopback is 20min minutes. When this time expires, the remote loopback is automatically cancelled.
6	Raisecom(config-gigaethernet1/1/*)#efm mode remote-loopback stop Example: Raisecom(config-gigaethernet1/1/1)#efm mode remote-loopback stop	Stop remote loopback.

7.2.6 Configuring EFM link performance monitoring

Configuring EFM link performance monitoring of the device

Configure EFM link performance monitoring of the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#i n t e r f a c e <i>interface-type</i> <i>interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config- gigaetherne t1/1/*) #efm link-mon itor { supported unsupported } Example: Raisecom(config- gigaetherne t1/1/*) #efm link-mon itor supported	Enable EFM link performance monitoring on the interface. After interface EFM is enabled, it supports link performance detection by default, and collects data every 100ms, and devices with CPU performance limitations cover all dot3ah-enabled interfaces to collect data once per second. • supported: supported • unsupported: not supported
4	Raisecom(config- gigaetherne t1/1/*) #efm link-mon itor symbol-period threshold <i>hold- value</i> window <i>window-value</i>	Configure the errored bit period event monitoring window and threshold (if there are hold-value errors in the window-value symbols, a link error is reported). • symbol period: errored symbol period event. When the number of errored symbol periods received during the monitoring window exceeds the threshold, it is such event. • hold-value: errored symbol period event threshold, ranging from 1 to 65535, an integer, in units of symbols • window-value: errored symbol period event monitoring window, ranging from 1 to 65535, in integer form, multiples of 1000000 symbols
5	Raisecom(config- gigaetherne t1/1/*) #efm link-mon itor frame threshold <i>hold-value</i> window <i>window-value</i>	Configure the errored frame event threshold and monitoring window. • frame: by default, errored frame detection is enabled, the window size is 10s (100 multiples of 100ms), and the threshold is 1 error frame. This means that when an errored frame is detected every 10s, a link error of the errored frame will be detected. • hold-value: errored frame event threshold, ranging from 1 to 65535, an integer, in units of frames • window-value: error frame event monitoring window, ranging from 10 to 600, an integer, being 100 by default, in units of a multiple of 100ms

Step	Command	Description
6	Raisecom(config-gigaetherne1/1/*) #efm link-monitor frame-period threshold hold-value window window-value	Configure the errored frame period threshold and monitoring window. • hold-value: errored frame period threshold, ranging from 1 to 65535, an integer, in units of frames • window-value: error frame period monitoring window, ranging from 1 to 65335, an integer, being 1 by default, in units of a multiple of 10000 frames
7	Raisecom(config-gigaetherne1/1/*) #efm link-monitor frame-second threshold hold-value window window-value	Configure the errored frame second threshold and monitoring window. • hold-value: errored frame period event threshold, ranging from 1 to 65535, an integer, in units of frames • window-value: error frame second event monitoring window, ranging from 1 to 65335, an integer, being 1000 by default, in units of a multiple of 100ms
8	Raisecom(config-gigaetherne1/1/*) #efm link-monitor high-threshold action { disable-on-error trap all }	When one of four types of link performance errors or one of two types of emergency link failures (Link Fault and Critical Event) occurs locally, or when a message of these types is received from the remote end, the device can send an alarm Trap to the server or shut down the interface (emergency events are not supported). When all above operations are performed simultaneously, no operation will be performed. By default, no operation is performed.

7.2.7 Configuring EFM link fault detection

Configure EFM link fault detection as below.

Step	Command	Description
1	Raisecom# configure	Enter global configuration mode.
2	Raisecom(config)# interface interface-type interface-number Example: Raisecom(config)# interface gigaetherne1 1/1/1	Enter physical interface configuration mode. • interface-type: interface type • interface-number: interface ID
3	Raisecom(config-gigaetherne1/1/*)# efm critical-event { supported unsupported } Example: Raisecom(config-gigaetherne1/1/*)# efm critical-event supported	Configure EFM emergency event detection. • supported: supported • unsupported: not supported

7.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show efm session { all interface interface-type interface-number }</code>	Show information about EFM sessions at both ends.
2	<code>Raisecom#show efm status { all interface interface-type interface-number }</code>	Show EFM configurations at both ends.
3	<code>Raisecom#show efm statistics { all interface interface-type interface-number }</code>	Show EFM statistics at both ends.
4	<code>Raisecom#show efm fault-logs { all interface interface-type interface-number }</code>	Show information about EFM error logs at both ends.
5	<code>Raisecom#show efm summary</code>	Show summary of all EFM-enabled interfaces.

7.2.9 Maintenance

Maintain the device as below.

Command	Description
<code>Raisecom(config-gigaethernet1/1/*)#efm fault-logs clear all</code>	Clear EFM OAM link event logs.

7.3 Link-state tracking

7.3.1 Introduction

Link-state tracking is used to provide interface linkage scheme for specific application and it can extend range of link backup. By monitoring uplinks and synchronizing downlinks, add uplink and downlink interfaces to a link-state group. Therefore, the fault of the upstream device can be informed to the downstream device to trigger switching. Link-state tracking can be used to prevent traffic loss due to failure in sensing the uplink fault by the downstream device.

When all uplink interfaces fail, down link interfaces are configured to Down status. When at least one uplink interface recovers, the downlink interface recovers to Up status. Therefore, the fault of the upstream device can be informed to the downlink device immediately. Uplink interfaces are not influenced when the downlink interface fail.

7.3.2 Preparing for configurations

Scenario

When uplink fails, traffic cannot be switched to the standby link if the downlink device fails to be notified in time. Then traffic will be disrupted.

Link-state tracking can be used to add downlink interfaces and uplink interfaces of the middle device to a link-state group and monitor uplink interfaces. When all uplink interfaces fails, the fault of the upstream device can be informed to the downstream device to trigger switching.

Prerequisite

N/A

7.3.3 Default configurations of link-state tracking

Default configurations of link-state tracking are as below.

Function	Default value
Link-state group	N/A
Action for processing faults on the interface	N/A
Link-state group Trap	Disable

7.3.4 Configuring link-state tracking



Note

Link-state tracking supports being configured on the physical interface and LAG interface.

Configure link-state tracking for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#monitor-link group <i>group-number</i>	Create a link-state group, and enable link-state tracking.
3	Raisecom(config-monitorlink-*)#snmp-trap { enable disable }	Configure link-state tracking group Trap.
4	Raisecom(config-monitorlink-*)#add interface <i>interface-type interface-number</i> role uplink	Configure the uplink.
5	Raisecom(config-monitorlink-*)#add interface <i>interface-type interface-number</i> role downlink	Configure the downlink.



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, use the **remove interface *interface-type interface-number*** command to delete an interface.

- In physical interface configuration mode, use the **no monitor-link group group-number** command to delete an interface from the link-state group.

7.3.5 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom# show monitor-link group [group-number]	Show configurations and status of the link-state group.

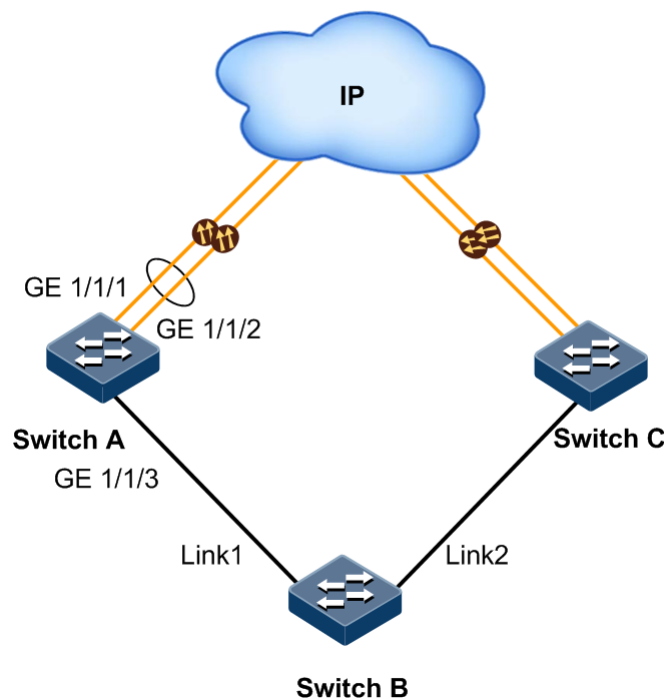
7.3.6 Example for configuring link-state tracking

Networking requirements

As shown in Figure 7-2, to improve network reliability, Link 1 and Link 2 of Switch B are connected to Switch A and Switch C respectively. Link 1 is the active link and Link 2 is the standby link. Link 2 will not be used to forward data until Link 1 is faulty.

Switch A and Switch C are connected to the uplink network in link aggregation mode. When all uplink interfaces on Switch A and Switch C fails, Switch B needs to sense the fault in time and switches traffic to the standby link. Therefore, you should deploy link-state tracking on Switch A and Switch C.

Figure 7-2 Link-state tracking networking



Configuration steps

Configurations of Switch A and Switch C are the same. Take Switch A for example.

Step 1 Create a LAG. Add uplink interfaces GE 1/1/1 and GE 1/1/2 to the LAG.

```
Raisecom#configure
Raisecom(config)#int eth-trunk 1
Raisecom(config-eth-trunk-1)#add interface ge 1/1/1
Raisecom(config-eth-trunk-1)#add interface ge 1/1/2
```

Step 2 Create link-state group 1. Add LAG interfaces to the link-state group.

```
Raisecom(config)#monitor-link group 1
Raisecom(config-monitorlink-1)#add interface eth-trunk 1 role uplink
```

Step 3 Add downlink interface GE 1/1/3 to the link-state group.

```
Raisecom(config-monitorlink-1)#add interface ge 1/1/3 role downlink
```

Checking results

Take Switch A for example. Use the **show monitor-link group** command to show configurations of the link-state group.

```
SwitchA#show monitor-link group 1
Mlink group 1 :
```

```
-----
-----
Snmp trap          : enable
Holdoff time       : 3
Uplink-select      : first-up
Member             Role      State   Status  Linkstate
ge-1/1/3           downlink forward active  up/up
eth-trunk-1        uplink   forward active  up/up
-----
-----
```

Use the **show monitor-link group** command to show configurations of the link-state group after all uplinks of Switch A fails. In this case, you can learn that link-state tracking is performed.

```
SwitchA#show link-state-tracking group 1
Mlink group 1 :
```

```
-----
-----
Snmp trap          : enable
```



```

Holdoff time      : 3
uplink-select    : first-up
Member           Role      State   Status  Linkstate
ge-1/1/3         downlink block   active  up/down
eth-trunk-1      uplink   block   active  up/down
-----
-----

```

7.4 VRRP

7.4.1 Introduction

All hosts in the internal network are configured with the same default route, pointing to the exit gateway, to achieve communication between the hosts and the external network. If the gateway fails, the host with that gateway as the default route will not be able to communicate with the external network.

Virtual Router Redundancy Protocol (VRRP) is a master/standby mode protocol designed to eliminate network failures caused by single point of failure of the default routing device in a static default routing environment. It effectively avoids network disconnection caused by single link failures, and does not need to modify the corresponding routing protocol and other configurations.

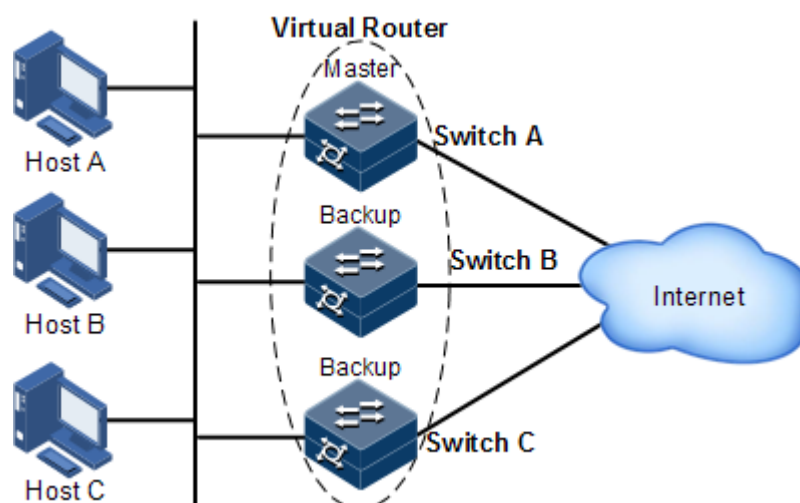
VRRP backup group

VRRP virtualizes two or more routing devices in a local area network into a single device (including a master device and several backup devices), forming a VRRP backup group. The VRRP backup group is functionally equivalent to a virtual router, providing the IP address of the virtual routing device externally.

- Master device: if a device with an external IP address is working properly, it is the master device or elected through algorithm. The master device implements various network functions for IP addresses of virtual routing device. When VRRP is running, the master device sends a VRRP notification packet to the backup device regularly, indicating that it is working normally.
- Backup device: if a device has no external IP address or has a low priority, it is a backup device. The backup device receives notification packets only and do not send them. When the master device fails, VRRP re-elect the master device from the backup devices. The new master device takes over the network functions of the original master device.

When configuring VRRP, configure a backup group number and priority for each routing device. The backup group number is used to group devices, and devices with the same backup group number belong to the same group. Devices in the same group elect the master devices by priority; the one with highest priority becomes the master device, as shown in the following figure.

Figure 7-3 VRRP principles



In the previous figure, Switch A, Switch B, and Switch C form a virtual routing device, which has its own IP address. The host within the local area network take the virtual routing device as the default gateway. The device with the highest priority among Switch A, Switch B, and Switch C is the master device, which carries out the gateway functions, while the other two devices are backup devices.

Working mode of VRRP

In the VRRP backup group, devices have the following two working modes:

- Non-preemptive mode: as long as the master device is functioning properly, even if the backup device is configured with a higher priority, the backup device will not become the master device.
- Preemptive mode: In the VRRP backup group, once a device discovers that its priority is higher than the current master device, it will send a VRRP notification packet to the external network, causing the devices in the backup group to re-elect the master device. Finally, it replaces the original master device. Correspondingly, the original master device will become a backup device.

Working flow of VRRP

VRRP works as below:

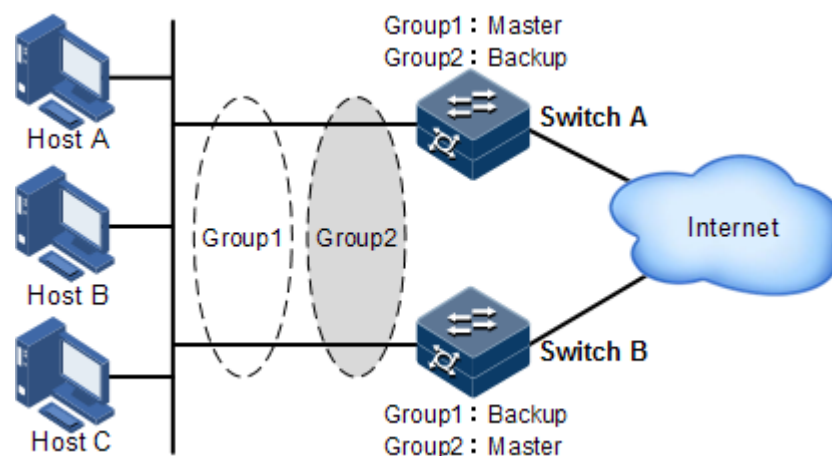
- Step 1 After being enabled with VRRP the device determines its role in the VRRP backup group based on priority. The device with the highest priority is the master while the device with lower priority is the backup. The master device regularly sends VRRP notification packets to notify other devices in the backup group that they are working normally. The backup device starts the timer and waits for the notification packet to arrive.
- Step 2 In pre-emptive mode, after receiving the VRRP notification packet, the backup device compares its own priority with the priority in the notification packet. If its priority is lower than the priority in the notification packet, the backup status will be maintained; otherwise, it will become the master device.
- Step 3 In non-pre-emptive mode, as long as the master device does not fail, the device status in the backup group remains unchanged.

- Step 4 If the timer of the backup device times out, VRRP considers that the master device is no longer functioning properly. At this time, the backup device will consider itself as the master device and send a VRRP notification packet to the external network for a new round of master device election. The newly elected master device will take over the network functions of the original master device and carry out the functions of forwarding packets.

Load balancing

VRRP load balancing refers to establishing two or more VRRP backup groups, with multiple devices simultaneously carrying services. It allows one device to back up multiple backup groups, with different priorities in different backup groups. Load sharing can be implemented through multiple virtual devices. The master devices in each backup group can be different, as shown in the following figure.

Figure 7-4 Principles of VRRP load balancing



Wherein:

- Switch A is the master device in VRRP backup group 1 and the backup device in VRRP backup group 2.
- Switch B is the master device in VRRP backup group 2 and the backup device in VRRP backup group 1.

Some hosts on the network use backup group 1 as the gateway, such as host A and host B. Some hosts on the network use backup group 2 as the gateway, such as host C. In this way, hosts back up each other and also balance load on the network.

7.4.2 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

7.4.3 Default configurations of VRRP

Default configurations of VRRP are as below.

Function	Default value
VRRP status	Enable
VRRP trap status	Disable
VRRP group on the interface	no
VRRP backup group description	no
VRRP backup group status	Disable
Device priority	100
IP owner priority	255
VRRP working mode	Preemption mode
Preemption delay of the VRRP group	0s
Packet sending interval of the VRRP group	1s

7.4.4 Configuration flow

1. Create a VRRP instance.
2. Configure the virtual address of the VRRP instance.
3. Configure the notification interval of VRRP instances (optional).
4. Configure the authentication mode of VRRP instances (optional).
5. Configure VRRP preemption (optional).

7.4.5 Configuring the VRRP backup group

Configure the VRRP backup group for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan*)#vrrp <i>group-id</i>	Create a VRRP backup group.

Step	Command	Description
4	<code>Raisecom(config-vlan*)#vrrp group-id associate-address ipv4-address</code>	Configure the virtual IPv4 address of the VRRP backup group.
5	<code>Raisecom(config-vlan*)#vrrp group-id advertise-interval { interval default }</code>	(Optional) configure the interval for sending VRRP packets. • group-id: VRRP instance ID • (interval default): interval for sending VRRP packets, in units of second, being 1 by default
6	<code>Raisecom(config-vlan*)#vrrp group-id check-ttl { enable disable }</code>	(Optional) configure the TTL of the detection VRRP packet. • group-id: VRRP instance ID • enable: enabled • disable: disabled By default, it is enabled.
7	<code>Raisecom(config-vlan*)#vrrp group-id priority { value default }</code>	(Optional) configure the VRRP instance priority. • group-id: VRRP instance ID • (value default): priority, being 100 by default
8	<code>Raisecom(config-vlan*)#vrrp group-id track bfd-session bfd-id [{ increased reduced } { value default }]</code>	(Optional) bind BFD. • group-id: VRRP instance ID • bfd-id: bfd instance ID • (Optional) increased: increase the priority. • (Optional) reduced: reduce the priority. • (Optional) value default: configure the VRRP instance priority to be reduced when the BFD status is down. It is 10 by default.
8	<code>Raisecom(config-vlan*)#vrrp group-id track interface vlan vlan-id</code>	(Optional) bind the VLAN interface. • group-id: VRRP instance ID • vlan-id: index of the VLAN
9	<code>Raisecom(config-vlan*)#vrrp group-id track admin-vrrp interface vlan vlan-id vrrp-id</code>	(Optional) bind the management VRRP group. • group-id: VRRP instance ID • vlan-id: index of the bound VLAN • vrrp-id: management VRRP instance ID
10	<code>Raisecom(config-vlan*)#vrrp group-id send-packet-mode { v2 v3 v2v3 }</code>	(Optional) configure the version of sent VRRP packets. group-id: VRRP instance ID • v2: send v2 packets. • v3: send v2 packets. • v2v3: send both v2 and v3 packets.

Step	Command	Description
11	<code>Raisecom(config-vlan*)#vrrp group-id authentication-mode { simple md5 } { cipher plain } key</code>	(Optional) configure VRRP authentication, which takes effect on v2 instances. • group-id: VRRP instance ID • simple: simple character authentication • md5: md5 authentication • cipher: shown in cipher text • plain: shown in plain text • key: authentication character
12	<code>Raisecom(config-vlan*)#vrrp group-id holding-multiplier [holding-multiplier-value]</code>	(Optional) configure the VRRP backup timeout multiplier. • group-id: VRRP instance ID • holding-multiplier-value: timeout multiplier (3–10), being 3 by default
13	<code>Raisecom(config-vlan*)#vrrp group-id role admin</code>	(Optional) configure VRRP role management. • group-id: VRRP instance ID
14	<code>Raisecom(config-vlan*)#vrrp admin-vrrp admin-group-id associate-vrrp interface vlan vlan-id member-group-id</code>	(Optional) configure VRRP role management. • group-id: management VRRP instance ID • vlan-id: index of the management VLAN interface • member-group-id: associated VRRP instance ID

7.4.6 Configuring the VRRP6 backup group

Configure the VRRP6 backup group for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface vlan vlan-id</code>	Enter VLAN interface configuration mode.
3	<code>Raisecom(config-vlan*)#vrrp6 group-id</code>	Create a VRRP6 backup group.
4	<code>Raisecom(config-vlan*)#vrrp6 group-id associate-address ipv6-address</code>	Configure the virtual IPv6 address of the VRRP6 backup group.
5	<code>Raisecom(config-vlan*)#vrrp6 group-id advertise-interval { interval default }</code>	(Optional) configure the interval for sending VRRP6 packets. • group-id: VRRP6 instance ID • (interval default): interval for sending VRRP6 packets, in units of second, being 1 by default

Step	Command	Description
6	<code>Raisecom(config-vlan*)#vrrp6 group-id check-ttl { enable disable }</code>	(Optional) configure the TTL of the detection VRRP6 packet. - group-id: VRRP6 instance ID - enable: enabled - disable: disabled By default, it is enabled.
7	<code>Raisecom(config-vlan*)#vrrp6 group-id priority { value default }</code>	(Optional) configure the VRRP6 instance priority. - group-id: VRRP6 instance ID (value default): priority, being 100 by default
8	<code>Raisecom(config-vlan*)#vrrp6 group-id track bfd-session bfd-id [{ increased reduced } { value default }]</code>	(Optional) bind BFD. - group-id: VRRP6 instance ID - bfd-id: bfd instance ID (Optional) increased: increase the priority. (Optional) reduced: reduce the priority. (Optional) value default: configure the VRRP6 instance priority to be reduced when the BFD status is down. It is 10 by default.
9	<code>Raisecom(config-vlan*)#vrrp6 group-id track interface vlan vlan-id</code>	(Optional) bind the VLAN interface. - group-id: VRRP6 instance ID - vlan-id: index of the VLAN
9	<code>Raisecom(config-vlan*)#vrrp6 group-id track admin-vrrp interface vlan vlan-id vrrp-id</code>	(Optional) bind the management VRRP6 group. - group-id: VRRP6 instance ID - vlan-id: index of the bound VLAN - VRRP6-id: management VRRP6 instance ID
10	<code>Raisecom(config-vlan*)#vrrp6 group-id holding-multiplier [holding-multiplier-value]</code>	(Optional) configure the VRRP6 backup timeout multiplier. - group-id: VRRP6 instance ID - holding-multiplier-value: timeout multiplier (3–10), being 3 by default
11	<code>Raisecom(config-vlan*)#vrrp6 group-id role admin</code>	(Optional) configure VRRP6 role management. group-id: VRRP6 instance ID
12	<code>Raisecom(config-vlan*)#vrrp6 admin-vrrp admin-group-id associate-vrrp interface vlan vlan-id member-group-id</code>	(Optional) configure VRRP6 role management. - group-id: management VRRP6 instance ID - vlan-id: index of the management VLAN interface - member-group-id: associated VRRP6 instance ID

7.4.7 Configuring VRRP Trap

Configure VRRP Trap for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#vrrp snmp-trap { enable disable }	Enable or disable the ping function of the virtual IP address of the VRRP backup group. By default, it is enabled.

7.4.8 Configuring the VRRP monitoring interface

Configure the VRRP monitoring interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan)#vrrp group-id track { <i>interface-type</i> <i>interface-number</i> vlan <i>vlan-id</i> } [{ increased reduced } { value default }]	Configure the monitoring interface of VRRP.



Note

reduced priority: it is the reduced priority when the monitored interface changes from the Up status to Down status, an integer, ranging from 1 to 255, needless of manual configuration. The priority of the device in the backup group is reduced by 10, namely, 1–254.

When the monitored interface changes from the Down status to Up status, the original priority is restored. We recommend configuring this parameter on the master device.

7.4.9 Configuring BFD for VRRP

Configure BFD for VRRP for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan)#vrrp group-id track bfd-session <i>bfd-id</i> [{ increased reduced } { value default }]	Configure the VRRP backup group to monitor the BFD session to implement expedited switching.



Note

- **increased priority:** it is the increased priority when the monitored BFD session changes to Down status, an integer, ranging from 1 to 255. The range of priority after increment is 1–254. When the monitored BFD session changes from the Down status to Up status, the original priority is restored. We recommend configuring this parameter on the backup device.
- **reduced priority:** it is the reduced priority when the monitored BFD session changes to Down status, an integer, ranging from 1 to 255. The range of priority after reduction is 1–254. When the monitored BFD session changes from the Down status to Up status, the original priority is restored. We recommend configuring this parameter on the master device.

7.4.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show vrrp	Show the basic status of VRRP.
2	Raisecom# show vrrp role { admin member normal }	Show information about the instance of the specified VRRP role.
3	Raisecom# show vrrp statistics	Show VRRP statistics.
4	Raisecom# show vrrp interface vlan <i>vlan-id</i>	Show VRRP information about the VLAN interface.
5	Raisecom# show vrrp associate interface <i>vlan</i> <i>vlan-id</i> <i>group-id</i>	Show VRRP information about the specified group on the interface.
6	Raisecom# show vrrp binding { admin-vrrp interface <i>vlan</i> <i>vlan-id</i> <i>group-id</i> }	Show binding information about the VRRP management group.

7.5 CFM

7.5.1 Introduction

Connectivity Fault Management (CFM) is a network-level Ethernet OAM technology, providing end-to-end connectivity fault detection, fault notification, fault judgement, and fault location. It is used to diagnose fault actively for Ethernet Virtual Connection (EVC), provide cost-effective network maintenance solution, and improve network maintenance through the fault management function.

The device complies with IEEE 802.1ag and ITU-T Y.1731.

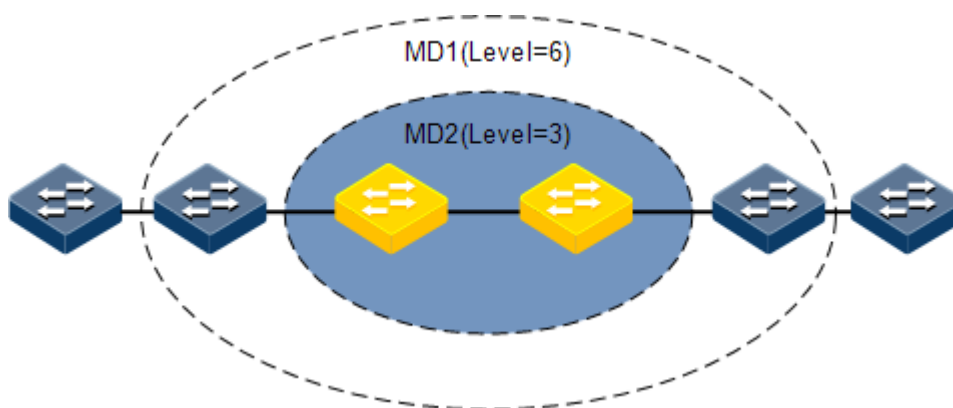
CFM concepts

- MD

Maintenance Domain (MD), also called Maintenance Entity Group (MEG), is a network that runs CFM. It defines network range of OAM management. MD has a level property, with 8 levels (level 0 to level 7). The bigger the number is, the higher the level is and the larger the MD range is. Protocol packets in a lower-level MD will be discarded after entering a higher-level MD. If no Maintenance association End Point (MEP) but a Maintenance association Intermediate Point (MIP) is in a high-level MD, the protocol can traverse the higher-level MD. However, packets in a higher-level MD can traverse lower-level MDs. In the same VLAN range, different MDs can be adjacent, embedded, but not crossed.

As shown in Figure 7-5, MD 2 is in MD 1. Packets in MD 1 need to traverse MD 2. Configure MD 1 to be at level 6, and MD 2 to be at level 3. Then packets in MD 1 can traverse MD 2 and implement connectivity fault management of the whole MD 1. However, packets in MD 2 cannot diffuse into MD 1. MD 2 is a server layer while MD 1 is a client layer.

Figure 7-5 MDs at different levels



- MA

The Maintenance Association (MA) is part of a MD. One MD can be divided into one or multiple MAs. An MA is identified by MD name + MA name.

The MAs can serve the specified VLAN or no VLAN, which are called the MA with VLAN attributes and MA without VLAN attributes respectively.

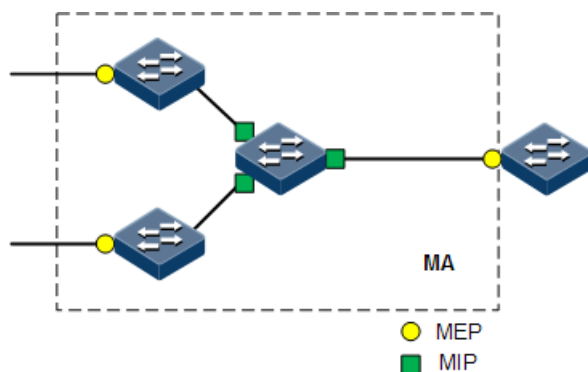
- MEP

As shown in the following figure, the Maintenance Association End Point (MEP) determines the boundary of an MA, identified by the "MEP ID". The MEP has directionality and can be divided into two types: inward MEP and outward MEP.

The inward MEP sends CFM packets outward through all interfaces except the one it belongs to; in other words, it broadcasts in the VLAN served by its MA.

The outward MEP directly sends CFM packets outward through its interface.

Figure 7-6 MEP and MIP



- MIP

As shown in Figure 7-6, the MIP is the internal node of a service instance, which cannot actively send CFM packets but can process and response to LinkTrace Message (LTM) and LoopBack Message (LBM) packets. The MIP is automatically created by the device, and can cooperate with the MEP to implement functions like PING and Tracert.

- MP

The MEP and MIP are called the Maintenance Point (MP).

CFM functions

- Fault detection (Continuity Check, CC)

The function is implemented by periodically sending Continuity Check Messages (CCMs). One MEP sends CCM and other MEPs in the same service instance can verify the RMEP status when receiving this packet. If the device fails or a link is incorrectly configured, MEPs cannot properly receive or process CCMs sent by RMEPs. If no CCM is received by a MEP during 3.5 CCM intervals, it is believed that the link fails. Then a fault Trap will be sent according to configured alarm priority.

- Fault acknowledgement (LoopBack, LB)

This function is used to verify the connectivity between two MPs through the source MEP sending LoopBack Message (LBM) and the destination MP sending LoopBack Reply (LBR). The source MEP sends a LBM to a MP who needs to acknowledge a fault. When receiving the LBM, the MP sends a LBR to the source MEP. If the source MEP receives this LBR, it is believed that the route is reachable. Otherwise, a connectivity fault occurs.

- Fault location (LinkTrace, LT)

The source MEP sends LinkTrace Message (LTM) to the destination MP and all MPs on the LTM transmission route will send a LinkTrace Reply (LTR) to the source MEP. By recording valid LTR and LTM, this function can be used to locate faults.

In general, CFM is an end-to-end OAM technology at the server layer. It helps reduce operation and maintenance cost. In addition, it improves the competitiveness of service providers.

- Alarm inhibition

Alarm inhibition is used to reduce the number of MEP fault alarms. If the MEP does not receive the CCMs from the remote MEP within 3.5 CCM sending periods, it immediately starts to periodically send Alarm Indication Signal (AIS) message, which are sent in the

opposite direction to the CCM. After receiving AIS message, other MEPs will suppress local fault alarms and continue to send AIS messages. Afterwards, if the MEP receives a CCM, it stops sending AIS messages and clears the fault alarm. AIS messages are multicast messages.

- One-way packet loss testing function

One-way Loss measurement (LM) is used to detect one-way packet loss between MEPs. Its implementation is as below: the source MEP sends a Loss Measurement Message (LMM) to the target MEP; after receiving the LMM, the target MEP sends a Loss Measurement Reply (LMR) message to the source MEP. The source MEP calculates the number of lost packets between the source MEP and the target MEP based on two consecutive LMR messages; in other words, starting from receiving the second LMR message, the source MEP calculates the number of lost packets between the source MEP and the target MEP based on the statistics on current LMR messages and previous LMR messages. Both the LMM and LMR messages are unicast messages.

- Delay Measurement (DM)

DM is used to detect the delay of message transmission between MEPs. It is divided into one-way delay test and round-trip delay test, and currently supports the bidirectional delay test only. The implementation of the round-trip delay test is as below: the source MEP sends a Delay Measurement Message (DMM) to the target MEP, which carries its sending time. After receiving the DMM, the target MEP records its receiving time, and then sends a Delay Measurement Reply (DMR) message to the source MEP. This message contains the sending time and receiving time of the DMM message, and the sending time of the DMR message. After receiving the DMR message, the source MEP records its receiving time and calculates the delay and jitter of the link transmission based on it.

In summary, CFM has implemented OAM technologies at the end-to-end service level, reducing the operation and maintenance costs for service providers, and to some extent improving their competitive advantage.

7.5.2 Preparing for configurations

Scenario

To expand application of Ethernet technologies at a carrier-grade network, the Ethernet must ensure the same QoS as the carrier-grade transport network. CFM solves this problem by providing overall OAM tools for the carrier-level Ethernet.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.
- Create VLANs.
- Add interfaces to the VLAN.

7.5.3 Default configurations of CFM

Default configurations of CFM are as below.

Function	Default value
Global CFM status	Disable

Function	Default value
Interval for sending CCMs	1s
Sending CCM by the MEP	Disable
Priority of CFM OAM packets	0

7.5.4 Configuring basic functions of CFM

Configure basic functions of CFM for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#cfm start	Enable global CFM.
3	Raisecom(config)#cfm md md-name format { dns dns-md-format-name mac mac-md-format-name string md-format-name none } level <0-7>	Create a MD, and enter the MD view. If a name is specified for a MD, the format and contents of the MD name in the sent CCM are specified, and the MD name and the name and contents of the MD used in sent packets must be unique in global. Otherwise, the MD will fail to be configured.
4	Raisecom(config-cfm-md-*)#ma ma-name format { icc icc-ma-format-name string ma-format-name }	Create a MA in a MD, and enter the MA view. This command specified the MA name and the format and contents of the MA name in the sent CCM. The MAs in the same MD must be unique.
5	Raisecom(config-cfm-md-* -ma-*)#map vlan vlan-id	Configure the VLAN associated with the MA.
6	Raisecom(config-cfm-md-* -ma-*)#mip create-type { default explicit none }	Configure the MIP creation rules for the current MA. • Default: if a higher-level MEP does not exist on the interface and a lower-level MIP does not exist, a MIP can be created on the interface. In this case, the MIP can be created without configuring the MEP on the interface. • Explicit: if there is a lower-level MEP on the interface without higher-level MEP, and there is no lower-level MIP, a MIP can be created. In this case, a MIP can be created only when if a lower-level MEP has been configured on the interface. • None: the MIP is not automatically created.

Step	Command	Description
7	Raisecom(config-cfm-md-*<i>-ma</i>-*)#mep mep-id <i>mep-id</i> interface <i>interface-type</i> <i>interface-number</i> [inward outward]	Create a MEP within a MA. The requirements for the number and type of MEPs created within the same MA are as below: • The inward ordinary MEP and outward ordinary MEP cannot exist concurrently. • Only one outward interface-type MEP can be created, and multiple inward interface-type MEPs can be created, but only one inward interface-type MEP can be created on the same interface.

7.5.5 Configuring fault detection

Configure fault detection on the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#cfm md <i>md-name</i>	Enter the MD view.
3	Raisecom(config-cfm-md-*)#ma <i>ma-name</i>	Enter the MA view.
4	Raisecom(config-cfm-md-*<i>-ma</i>-*)#ccm-interval { 300Hz 10ms 100ms 1s 10s 1min 10min default }	Configure the interval for sending CCMs by the MEP in the current MA. When the interval is configured to be smaller than 1s, the switching chip must support CFM.
5	Raisecom(config-cfm-md-*<i>-ma</i>-*)#ccm-send [mep <i>mep-id</i>] enable	Enable MEPs to send CCMs.
6	Raisecom(config-cfm-md-*<i>-ma</i>-*)#rmep mep-id <i>mep-id</i> mac <i>mac-address</i>	Configure the static RMEP. This function is used with the CCM packet detection.
7	Raisecom(config-cfm-md-*<i>-ma</i>-*)#ccm-send [mep <i>mep-id</i>] priority { <0-7> default }	Configure the priority of sending CCMs by the MEP in the MA.

7.5.6 Configuring fault acknowledgement

Configure fault acknowledgement for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#service <i>cis-id</i> level <i>level</i>	Enter the MD view.

Step	Command	Description
3	<code>Raisecom(config-cfm-md-*)#ma ma-name</code>	Enter the MA view.
4	<code>Raisecom(config-cfm-md-*<i>ma</i>-*)#ping mep-id mep-id rmep-id mep-id count count-number tlv-type { prbs pbrs-crc null null-crc } tlv-len len priority <0-7></code> <code>Raisecom(config-cfm-md-*<i>ma</i>-*)#ping mep-id mep-id mac { multicast mac-address } count count-number tlv-type { prbs pbrs-crc null null-crc } tlv-len len priority <0-7></code>	Perform Layer 2 PING for acknowledging faults.

7.5.7 Configuring fault location

Configure fault location for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#cfm md md-name</code>	Enter the MD view.
3	<code>Raisecom(config-cfm-md-*)#ma ma-name</code>	Enter the MA view.
4	<code>Raisecom(config-cfm-md-*<i>ma</i>-*)#trace mep-id mep-id rmep-id mep-id ttl ttl fdb <0-1></code> <code>Raisecom(config-cfm-md-*<i>ma</i>-*)#trace mep-id mep-id mac mac-address ttl ttl fdb <0-1></code>	Perform Layer 2 Traceroute for acknowledging faults.

7.5.8 Configuring alarm inhibition

Configure alarm inhibition for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#cfm md md-name</code>	Enter the MD view.
3	<code>Raisecom(config-cfm-md-*)#ma ma-name</code>	Enter the MA view.
4	<code>Raisecom(config-cfm-md-*<i>ma</i>-*)#ais [mep mep-id] interval { 1s 1min default }</code>	Configure the interval for the MEP in the current MA to send AIS packets to the MEP in the higher-level MA.
5	<code>Raisecom(config-cfm-md-*<i>ma</i>-*)#ais [mep mep-id] md-level { <0-7> default }</code>	Configure the level of the AIS packets to be sent by the MEP in the current MA.

Step	Command	Description
6	<code>Raisecom(config-cfm-md-*<i>-ma-</i>*)#ais [mep <i>mep-id</i>] priority { <0-7> defalut }</code>	Configure the priority of the AIS packets to be sent by the MEP in the current MA.
7	<code>Raisecom(config-cfm-md-*<i>-ma-</i>*)#ais [mep <i>mep-id</i>] enable</code>	Enable the MEP to send AIS packets.

7.5.9 Configuring the one-way packet loss test

Configure the one-way packet loss test for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#cfm md <i>md-name</i></code>	Enter the MD view.
3	<code>Raisecom(config-cfm-md-*)#ma <i>ma-name</i></code>	Enter the MA view.
4	<code>Raisecom(config-cfm-md-*<i>-ma-</i>*)#loss-measure mep-id <i>mep-id</i> rmep-id <i>mep-id</i> interval { 100ms 1s } priority <0-7> count <i>count-number</i></code> <code>Raisecom(config-cfm-md-*<i>-ma-</i>*)#loss-measure mep-id <i>mep-id</i> mac <i>mac-address</i> interval { 100ms 1s } priority <0-7> count <i>count-number</i></code>	Perform the one-way packet loss test to test the one-way lost packets between MEPs.

7.5.10 Configuring the round-trip delay test

Configure the round-trip delay test for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#cfm md <i>md-name</i></code>	Enter the MD view.
3	<code>Raisecom(config-cfm-md-*)#ma <i>ma-name</i></code>	Enter the MA view.
4	<code>Raisecom(config-cfm-md-*<i>-ma-</i>*)#delay-measure mep-id <i>mep-id</i> rmep-id <i>mep-id</i> interval { 100ms 1s } priority <0-7> frame-len <i>len</i> count <i>count-number</i></code> <code>Raisecom(config-cfm-md-*<i>-ma-</i>*)#delay-measure mep-id <i>mep-id</i> mac <i>mac-address</i> interval { 100ms 1s } priority <0-7> frame-len <i>len</i> count <i>count-number</i></code>	Perform the round-trip delay test to test the delay of packet transmission between MEPs.

7.5.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show cfm config	Show CFM configurations.
2	Raisecom# show cfm md all	Show configurations of CFM MDs.
3	Raisecom# show cfm ma all	Show configurations of CFM MAs.
4	Raisecom# show cfm mep md md-name ma ma-name mep-id mep-id	Show configurations of CFM MEPs.
5	Raisecom# show cfm rmep md md-name ma ma-name rmep-id mep-id	Show configurations of CFM RMEPs.
6	Raisecom# show cfm mip	Show configurations of CFM MIPs.

7.5.12 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)# clear ethernet cfm errors [level md-level]	Clear errored CCM records.
Raisecom(config)# clear ethernet cfm traceroute-cache	Clear configurations of the LinkTrace database.

7.5.13 Example for configuring CFM

Networking requirements

As shown in Figure 7-7:

The network composed of five devices is divided into MD_A and MD_B, of which the MD levels are 5 and 3 respectively. All interfaces on each device belong to VLAN 100. The MAs in each MD serve the VLAN. It is assumed that the MAC addresses of Device A to Device E are 00:03:56:00:00:01, 00:03:56:00:00:02, 00:03:56:00:00:03, 00:03:56:00:00:04, and 00:03:56:00:00:05 respectively.

The boundary interfaces on MD_A are GE1/0/1 of Device A, GE1/0/3 on Device D, and GE1/0/4 on Device E. All these interfaces are inward MEPs. The boundary interfaces on MD_B are GE1/0/3 on Device B and GE1/0/1 on Device D. All these interfaces are outward MEPs.

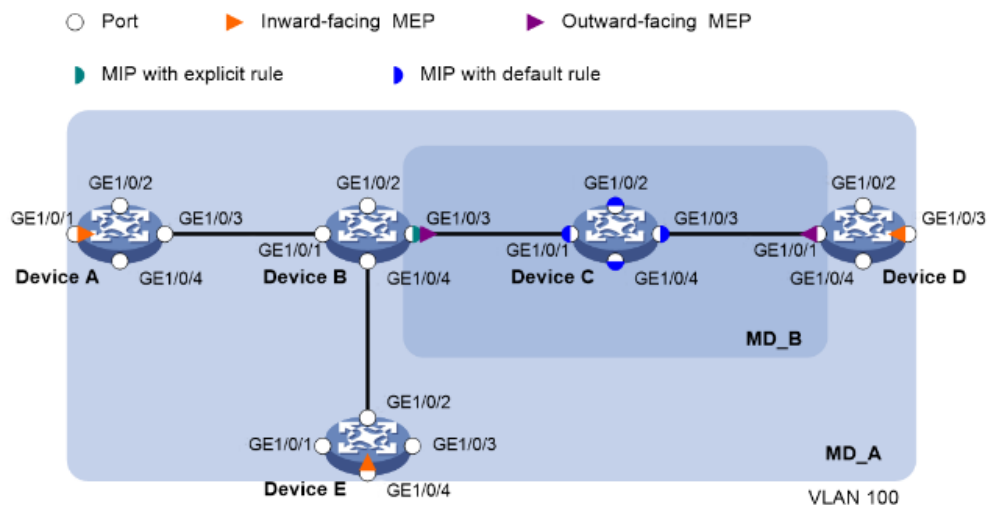
Plan the MIP for MD_A on Device B. This is only configured when there is a low-level MEP on the interface. According to this plan, due to the configuration of the MIP of MD_B on GE1/0/3 on Device B, therefore use the explicit rule to create the MIPs of MD_A on Device B, and use the none rule on other devices.

Plan the MIP for MD_B on Device C. This is configured on all its interfaces. According to this plan, due to the configuration of the MIP of MD_B on Device C, therefore use the default rule, and use the none rule on other devices.

Use CCM to detect the connection status of MEPs in MD_A and MD_B. When a link fault is detected, use the loopback function to locate the fault, use the alarm inhibition function and Ethernet alarm inhibition function to reduce the number of fault alarms.

After obtaining the status of the entire network, use link tracking, one-way packet loss test, and round-trip delay test to detect links for various links.

Figure 7-7 Typical CFM networking



Configuration steps

Step 1 Configure the VLAN and interfaces.

Create VLAN 100 on each device as previously shown. Configure interfaces GE 1/0/1 to GE 1/0/4 to belong to VLAN 100.

Step 2 Enable basic functions of CFM.

```
DeviceA#configure
DeviceA(config)#cfm start
DeviceA(config)#cfm md MD_A format none level 5
DeviceA(config-cfm-md-MD_A)#ma 1 format icc 1
DeviceA(config-cfm-md-MD_A-ma-1)#map vlan 100
DeviceA(config-cfm-md-MD_A-ma-1)#mip create-type none
DeviceA(config-cfm-md-MD_A-ma-1)#mep mep-id 1001 interface ge 1/0/1
inward
DeviceA(config-cfm-md-MD_A-ma-1)#end
```

```
DeviceB#configure
DeviceB(config)#cfm start
DeviceB(config)#cfm md MD_A format none level 5
DeviceB(config-cfm-md-MD_A)#ma 1 format icc 1
DeviceB(config-cfm-md-MD_A-ma-1)#map vlan 100
```

```
DeviceB(config-cfm-md-MD_A-ma-1)#mip create-type explicit
DeviceB(config-cfm-md-MD_A-ma-1)#end
DeviceB#configure
DeviceB(config)#cfm md MD_B format none level 3
DeviceB(config-cfm-md-MD_B)#ma 2 format icc 2
DeviceB(config-cfm-md-MD_B-ma-2)#map vlan 100
DeviceB(config-cfm-md-MD_B-ma-2)#mep mep-id 2001 interface ge 1/0/3
outward
DeviceB(config-cfm-md-MD_B-ma-2)#end

DeviceC#configure
DeviceC(config)#cfm start
DeviceC(config)#cfm md MD_B format none level 3
DeviceC(config-cfm-md-MD_B)#ma 2 format icc 2
DeviceC(config-cfm-md-MD_B-ma-2)#map vlan 100
DeviceC(config-cfm-md-MD_B-ma-2)#end

DeviceD#configure
DeviceD(config)#cfm start
DeviceD(config)#cfm md MD_A format none level 5
DeviceD(config-cfm-md-MD_A)#ma 1 format icc 1
DeviceD(config-cfm-md-MD_A-ma-1)#map vlan 100
DeviceD(config-cfm-md-MD_A-ma-1)#mip create-type none
DeviceD(config-cfm-md-MD_A-ma-1)#mep mep-id 4002 interface ge 1/0/3
inward
DeviceD(config-cfm-md-MD_A-ma-1)#end
DeviceD#configure
DeviceD(config)#cfm md MD_B format none level 3
DeviceD(config-cfm-md-MD_B)#ma 2 format icc 2
DeviceD(config-cfm-md-MD_B-ma-2)#map vlan 100
DeviceD(config-cfm-md-MD_B-ma-2)#mip create-type none
DeviceD(config-cfm-md-MD_B-ma-2)#mep mep-id 4001 interface ge 1/0/1
outward
DeviceD(config-cfm-md-MD_B-ma-2)#end

DeviceE#configure
DeviceE(config)#cfm start
DeviceE(config)#cfm md MD_A format none level 5
DeviceE(config-cfm-md-MD_A)#ma 1 format icc 1
DeviceE(config-cfm-md-MD_A-ma-1)#map vlan 100
DeviceE(config-cfm-md-MD_A-ma-1)#mip create-type none
DeviceE(config-cfm-md-MD_A-ma-1)#mep mep-id 5001 interface ge 1/0/4
inward
DeviceE(config-cfm-md-MD_A-ma-1)#end
```

Step 3 Configure CCM.

```
DeviceA#configure
DeviceA(config)#cfm md MD_A
DeviceA(config-cfm-md-MD_A)#ma 1
DeviceA(config-cfm-md-MD_A-ma-1)#ccm-send mep-id 1001 enable
DeviceA(config-cfm-md-MD_A-ma-1)#end
```

```
DeviceB#configure
DeviceB(config)#cfm md MD_B
DeviceB(config-cfm-md-MD_B)#ma 2
DeviceB(config-cfm-md-MD_B-ma-2)#ccm-send mep-id 2001 enable
DeviceB(config-cfm-md-MD_B-ma-2)#end
```

```
DeviceD#configure
DeviceD(config)#cfm md MD_A
DeviceD(config-cfm-md-MD_A)#ma 1
DeviceD(config-cfm-md-MD_A-ma-1)#ccm-send mep-id 4002 enable
DeviceD(config-cfm-md-MD_A-ma-1)#end
```

```
DeviceD#configure
DeviceD(config)#cfm md MD_B
DeviceD(config-cfm-md-MD_B)#ma 2
DeviceD(config-cfm-md-MD_B-ma-2)#ccm-send mep-id 4001 enable
DeviceD(config-cfm-md-MD_B-ma-2)#end
```

```
DeviceE#configure
DeviceE(config)#cfm md MD_A
DeviceE(config-cfm-md-MD_A)#ma 1
DeviceE(config-cfm-md-MD_A-ma-1)#ccm-send mep-id 5001 enable
DeviceE(config-cfm-md-MD_A-ma-1)#end
```

Step 4 Verify loopback.

Enable loopback on Device A. Check the link status of MEPs 1001 to 5001 in MA 1.

```
DeviceA#configure
DeviceA(config)#cfm md MD_A
DeviceA(config-cfm-md-MD_A)#ma 1
DeviceA(config-cfm-md-MD_A-ma-1)#ping mep-id 1001 rmep-id 5001 count 5
tlv-type null tlv-len 50 priority 0
```

Pinging 00-03-56-00-00-05 with tlv len 50 of data:

```
Reply from 00-03-56-00-00-05: bytes=59 time=2ms
Reply from 00-03-56-00-00-05: bytes=59 time=3ms
Reply from 00-03-56-00-00-05: bytes=59 time=2ms
Reply from 00-03-56-00-00-05: bytes=59 time=3ms
Reply from 00-03-56-00-00-05: bytes=59 time=2ms
```

```
Packets: Sent = 5, Received = 5, Lost = 0 <0.00% loss>
Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Step 5 Verify linktrace.

Search for the path of MEPs 1001 to 5001 in MA 1 on Device A.

```
DeviceA#configure
DeviceA(config)#cfm md MD_A
DeviceA(config-cfm-md-MD_A)#ma 1
```

```
DeviceA(config-cfm-md-MD_A-ma-1)#trace mep-id 1001 rmep-id 5001 ttl 16  
fdb 0
```

Tracing the route to 00-03-56-00-00-05 over a maximum of 16 hops:

Hop-Num	TTL	MAC	Last-MAC	IsMep	Relay	Action
1	15	0003:5600:0005	0003:5600:0001	IsMep	Hit	

Step 6 Perform the one-way packet loss test.

Perform the one-way packet loss test on MEPs 1001 to 4002 in MA 1 on Device A.

```
DeviceA#configure  
DeviceA(config)#cfm md MD_A  
DeviceA(config-cfm-md-MD_A)#ma 1  
DeviceA(config-cfm-md-MD_A-ma-1)#loss-measure mep-id 1001 rmep-id 4002  
interval 1s priority 0 count 5  
Info: Single-ended loss measurement will take some time.
```

Single-ended loss measurement statistics for remote mep 4002 in md MD_A
ma 1:

Packets: Sent = 5, Received = 5, Lost = 0
Far-end frame loss rate : Minimum = 0%, Maximum = 0%, Average = 0%
Near-end frame loss rate: Minimum = 0%, Maximum = 0%, Average = 0%

Step 7 Perform the round-trip delay test.

Perform the round-trip delay test on MEPs 1001 to 4002 in MA 1 on Device A.

```
DeviceA#configure  
DeviceA(config)#cfm md MD_A  
DeviceA(config-cfm-md-MD_A)#ma 1  
DeviceA(config-cfm-md-MD_A-ma-1)#delay-measure mep-id 1001 rmep-id 4002  
interval 1s priority 0 frame-len 64 count 5  
Info: Two-way delay measurement will take some time.
```

Two-way delay measurement statistics for remote mep 4002 in md MD_A ma 1:

Packets: Sent = 5, Received = 5, Lost = 0
Delay Time : Minimum = 1396455us, Maximum = 2219010us, Average =
1785922us
Delay variation: Minimum = 146221us, Maximum = 707088us, Average =
436789us

Checking results

Use the **show cfm config** command to show CFM configurations.

```
DeviceA#show cfm config
```

```
!  
cfm start  
cfm md MD_A format string MD_A level 5  
  mip create-type none  
  ma 1 format string 1  
  map vlan 100  
  mep mep-id 1001 interface ge 1/0/1 inward  
  ccm-send mep-id 1001 enable
```

8 Security

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

- ACL
- AAA
- 802.1x
- PPPoE+
- Port security MAC
- Storm suppression and storm control
- ARP attack protection
- ND Snooping
- DHCP Snooping
- IP Source Guard
- CPU attack protection

8.1 ACL

8.1.1 Introduction

Access Control List (ACL) is a set of ordered rules, which can control the device to receive or refuse some data packets.

You need to configure rules on the network to prevent illegal packets from affecting network performance and determine the packets allowed to pass. These rules are defined by ACL.

ACL is a series of rule composed of permit | deny sentences. The rules are described according to source address, destination address, and port number of data packets. The device judges receiving or rejecting packets according to the rules.

8.1.2 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. The discarding action includes sending packets to the CPU. When the ACL denies a destination MAC address, the source MAC address of the corresponding packet will not be learnt and shown.

- Basic IPv4 ACL: define classification rules according to attributes carried in the header of IP packets, such as the source IP address and destination IP address.
- Extended IPv4 ACL: define classification rules according to attributes carried in the header of IP packets, such as the source IP address, destination IP address, bearing protocol type, and TCP or UDP port number (being 0 by default). This type can restrict Telnet/SSH login.
- MAC ACL: define classification rules according to attributes carried in the header of Layer 2 frames, such as the source MAC address, destination MAC address, and Layer 2 protocol type. When ACL denies packets with a destination MAC address, the device will not learn and show the source MAC address.
- User ACL: this type can perform the AND operation with the mask from a specified byte in the packet header or IP header, compares the character string extracted from the packet with the user-defined character string, and thus find matching packets. This type supports matching any field in the first 64 bytes of the Ethernet frame.
- IPv6 ACL: define classification rules according to attributes carried in the header of IP packets, such as the source IPv6 address, destination IPv6 address, IPv6 bearing protocol type, and TCP or UDP port number (being 0 by default). This type can restrict Telnet/SSH login.
- Advanced ACL: define classification rules according to attributes carried in the header of Layer 2 frames, such as the source MAC address and destination MAC address, and attributed carried in the header of IP packets, such as the source IP address and destination IP address.

There are 4 ACL modes according to different application environments:

- ACL based on device
- ACL based on interface
- ACL based on flow from the ingress interface to egress interface
- ACL based on VLAN

Prerequisite

N/A

8.1.3 Configuring the ACL

Configure ACL for the device as below. Steps 3–7 are optional.

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

Step	Command	Description
2	<pre> Raisecom(config)#acl-12 <i>acl-number</i> [name <i>acl-name</i>] Raisecom(config)#acl-ipv4 <i>acl-number</i> [name <i>acl-name</i>] Raisecom(config)#acl-ipv6 <i>acl-number</i> [name <i>acl-name</i>] Raisecom(config)#acl-hybrid <i>acl-number</i> [name <i>acl-name</i>] Raisecom(config)#acl-mps <i>acl-number</i> [name <i>acl-name</i>] </pre>	Create an ACL, and enter ACL configuration mode. • When the ACL number is 1–1000, this configuration enters basic MAC ACL configuration mode. • When the ACL number is 1001–2000, this configuration enters basic IPv4 ACL configuration mode. • When the ACL number is 2001–3000, this configuration enters extended hybrid ACL configuration mode. • When the ACL number is 3001–4000, this configuration enters IPv6 ACL configuration mode. • When the ACL number is 4001–5000, this configuration enters MPLS ACL configuration mode.
3	<pre> Raisecom(configure-acl-ipv4-*)#rule <i>rule-id</i> src-ip <i>ip-address</i> dst-ip <i>ip-address</i> Raisecom(configure-acl-ipv4-*)#rule <i>rule-id</i> icmp src-ip <i>ip-address</i> dst-ip <i>ip-address</i> icmp-type <i>icmp-type</i> icmp-code <i>icmp-code</i> [fragment] Raisecom(configure-acl-ipv4-*)#rule <i>rule-id</i> tcp src-ip <i>ip-address</i> src-port port dst-ip <i>ip-address</i> dst-port <i>port</i> { syn synack ack fin } [fragment] Raisecom(configure-acl-ipv4-*)#rule <i>rule-id</i> igmp src-ip <i>ip-address</i> dst-ip <i>ip-address</i> [fragment] Raisecom(configure-acl-ipv4-*)#rule <i>rule-id</i> udp src-ip { <i>ip-address</i> src-port port dst-ip <i>ip-address</i> dst-port <i>port</i> [fragment] </pre>	Configure the matching rules for IP ACL.

Step	Command	Description
4	<pre>Raisecom(configure-acl-12-*)#rule rule-id src-mac mac-address dst-mac mac-address Raisecom(configure-acl-12-*)#rule rule-id src-mac mac-address dst-mac mac-address eth-type { ip arp <0x0600-0xfffe> } Raisecom(configure-acl-12-*)#rule rule-id src-mac mac-addr dst-mac mac-address { inner-vlan outer-vlan } vlan-id 8021p cos</pre>	Configure the matching rules for MAC ACL.
5	<pre>Raisecom(configure-acl-ipv6-*)#rule rule-id src-ip ipv6-address dst-ip ipv6-address Raisecom(configure-acl-ipv6-*)#rule rule-id tcp src-ip ipv6-address src-port port dst-ip ipv6-address dst-port port { syn synack ack fin } Raisecom(configure-acl-ipv6-*)#rule rule-id udp src-ip ipv6-address src-port port dst-ip ipv6-address dst-port port Raisecom(configure-acl-ipv6-*)#rule rule-id icmp src-ip ipv6-address dst-ip ipv6-address icmp-type icmp-type icmp-code icmp-code [fragment]</pre>	Configure the matching rule for IPv6 ACL.
6	<pre>Raisecom(configure-acl-ipv4-*)#rule rule-id action { permit deny mirror redirect counter }</pre>	Configure the action for basic IP ACL.

8.1.4 Applying the ACL

Apply the ACL for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface interface-type interface-number	Enter physical interface configuration mode, or VLAN interface configuration mode. Take physical interface configuration mode for example.
3	<pre>Raisecom(config-ge-1/1/*)#acl-12 in acl-num</pre>	Apply ACL to the interface.
	Raisecom(config-ge-1/1/*)#acl-12 in name	Apply ACL to the interface.
4	Raisecom(config-ge-1/1/*)#exit	Return to global configuration mode.

8.1.5 Configuring statistics

Configure statistics for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#counter <i>counter-id</i> { packet byte all } sort { green red greenred greenyellow redyellow total }	Create a statistic rule.
3	Raisecom(configure-acl-12-*)#rule <i>rule-id</i> meter <i>meter-id</i>	Apply the statistic rule to the ACL.

8.1.6 Configuring the ACL IP list

Configure the ACL IP list for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#time-range list <i>id</i>	Create a period.

Step	Command	Description
3	<pre> Raisecom(config-timerange-*)#time- range timerange-id absolute from <0- 23>:<0-59>:<0-59> <2001-2036>/<1- 12>/<1-31> to <0-23>:<0-59>:<0-59> <2001-2036>/<1-12>/<1-31> Raisecom(config-timerange-*)#time- range timerange-id everyhour <0- 59>:<0-59> to <0-59>:<0-59> Raisecom(config-timerange-*)#time- range timerange-id everyday <0- 23>:<0-59>:<0-59> to <0-23>:<0- 59>:<0-59> Raisecom(config-timerange-*)#time- range timerange-id everyweek <0- 23>:<0-59>:<0-59> { mon tue wed thu fri sat sun } to <0-23>:<0- 59>:<0-59> { mon tue wed thu fri sat sun } Raisecom(config-timerange-*)#time- range timerange-id everymonth <0- 23>:<0-59>:<0-59> <1-31> to <0- 23>:<0-59>:<0-59> <1-31> Raisecom(config-timerange-*)#time- range timerange-id everyweekend <0- 23>:<0-59>:<0-59> to <0-23>:<0- 59>:<0-59> Raisecom(config-timerange-*)#time- range timerange-id everyyear <0- 23>:<0-59>:<0-59> <1-12>/<1-31> to <0-23>:<0-59>:<0-59> <1-12>/<1-31> </pre>	Create a period, and apply it to the ACL rule.
4	<pre> Raisecom(configure-acl-12-*)#rule rule-id time-range timerange-list-id </pre>	Apply the period to the ACL.

8.1.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show acl config	Show ACL configurations.
2	Raisecom#show acl interface	Show ACL configurations on the interface.
3	Raisecom#show acl statistics	Show ACL statistics.
4	Raisecom#show time-range list	Show period configurations.

8.1.8 Maintenance

Maintain the device as below.

Command	Description
<code>Raisecom(config)#reset acl statistics [acl acl-id rule rule-id direction { in out }]</code>	Clear statistics on global ACL.
<code>Raisecom(config)#reset acl statistics interface interface-type interface-number [acl acl-id rule rule-id direction { in out }]</code>	Clear statistics on interface ACL.

8.2 AAA

8.2.1 Introduction

AAA

Authentication, Authorization, and Accounting (AAA) is a management mechanism for network security. AAA adopts a client/server structure and provides three security functions of authentication, authorization, and accounting.

- **Authentication:** confirm the identity of the remote user accessing the network, and determine whether the visitor is a legitimate network user.
- **Authorization:** grant different permissions to different users to limit the services that users can use. For example, the administrator authorizes office users to access and print files on the server, but other temporary visitors do not have this permission.
- **Accounting:** record all operations during the user's use of network services, including the type of service used, starting time, data flow, to collect and record the user's use of network resources, and implement the accounting for time and traffic. It also has a monitoring effect on the network.

AAA adopts a client/server structure. The client runs on the NAS (Network Access Server), which is responsible for verifying user identity and managing user access. The server centrally manages user information.

AAA can be implemented through multiple protocols that specify how user information is communicated between the NAS and the server. Currently, the device supports the Remote Authentication Dial-In User Service (RADIUS) protocol and Terminal Access Controller Access Control System (TACACS+).

RADIUS

Remote Authentication Dial In User Service (RADIUS) is a standard communication protocol that provides centralized authentication of remote access users. RADIUS uses UDP as the transmission protocol (port 1812 and port 1813) which has a good instantaneity; at the same time, RADIUS features good reliability by supporting retransmission mechanism and standby server mechanism.

- **RADIUS authentication**

RADIUS adopts client/server mode. The network access device is used as client of RADIUS server. The RADIUS server receives user connection requests, authenticates users, and replies them with configurations for providing services. In this way, RADIUS can control user to access devices and network, thus improving network security.

Communication between clients and RADIUS server is authenticated by the shared key, which will not be transmitted on the network. Besides, any user password to be transmitted between clients and RADIUS server must be encrypted to prevent it from being intercepted through sniffing through any insecure network.

- RADIUS accounting

RADIUS accounting is used on users that have passed RADIUS authentication. When a user logs in, the device sends an Account-Start packet to the RADIUS accounting server. During user login, the device sends Account-Update packets to the RADIUS accounting server according to the accounting policy. When the user logs off, the device sends an Account-Stop packet, which contains user online time, to the RADIUS accounting server. The RADIUS accounting server can record the access time and operations of each user through these packets.

TACACS+

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 UDP 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.

8.2.2 Preparing for configurations

Scenario

To control users' access to devices and the network, you can deploy the RADIUS/TACACS+ server to authenticate and account users. The device can work as an agent of the RADIUS/TACACS+ server, and authorize users with access rights according to the feedback by the RADIUS/TACACS+ server. TACACS+ is more secure and reliable than RADIUS.

Prerequisite

N/A

8.2.3 Default configurations of AAA

Function	Default value
Response timeout time of the RADIUS authentication server	60s
Times for retransmitting RADIUS packets	3
Interval for retransmitting RADIUS packets	2s
Response timeout time of the TACACS+ authentication server	60s

Function	Default value
TCP connection timeout time and packet receiving timeout time of the TACACS+ authentication server	2s

8.2.4 Configuring the RADIUS server

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#aaa	Enter AAA configuration mode.
3	Raisecom(config-aaa)#radius-server deadtime { second default }	Configure the response timeout time of the RADIUS authentication server, in units of second, being 60 by default.
4	Raisecom(config-aaa)#radius-server max-retransmit { <0-5> default }	Configure the times for retransmitting RADIUS packets, being 3 by default.
5	Raisecom(config-aaa)#radius-server retransmit-interval { <1-10> default }	Configure the global interval for retransmitting RADIUS packets, being 2s by default.
6	Raisecom(config-aaa)#radius-server host server-name ip-address ip-address key key [acct-port port-id auth-port port-id deadtime { second default } max-retransmit { <0-5> default } retransmit-interval { <1-10> default } source-ip ip-address [source-vpn-instance vpn-name] vpn-instance vpn-name]	Create an IPv4 RADIUS server.
7	Raisecom(config-aaa)#radius-server host server-name ip6-address ipv6-address key key [acct-port port-id auth-port port-id deadtime { second default } max-retransmit { <0-5> default } retransmit-interval { <1-10> default } source-ip6 ipv6-address [source-vpn-instance vpn-name] vpn-instance vpn-name]	Create an IPv6 RADIUS server.

8.2.5 Configuring the TACACS+ server

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#aaa	Enter AAA configuration mode.
3	Raisecom(config-aaa)#tacacs-server deadtime { second default }	Configure the response timeout time of the TACACS+ authentication server, in units of second, being 60 by default.
4	Raisecom(config-aaa)#tacacs-server timeout { <1-10> default }	Configure the TCP connection timeout time and packet receiving timeout time of the TACACS+ authentication server, being 2s by default.
5	Raisecom(config-aaa)#tacacs-server host server-name ip-address ip-address key key [deadtime { second default } port port-id single-connection { enable disable } timeout { <1-10> default } source-ip ip-address [source-vpn-instance vpn-name] vpn-instance vpn-name]	Create an IPv4 TACACS+ server.
6	Raisecom(config-aaa)#tacacs-server host server-name ip6-address ipv6-address key key [deadtime { second default } port port-id single-connection { enable disable } timeout { <1-10> default } source-ip6 ipv6-address [source-vpn-instance vpn-name] vpn-instance vpn-name]	Create an IPv6 TACACS+ server.

8.2.6 Configuring the AAA server group

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#aaa	Enter AAA configuration mode.
3	Raisecom(config-aaa)#server-group group-name { radius-server tacacs-server } server-name	Create an AAA server group, or add servers to the AAA server group.

8.2.7 Configuring the AAA mode

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#aaa	Enter AAA configuration mode.
3	Raisecom(config-aaa)#aaa authentication { dot1x ppp login mac-authen enable } method <i>method-name</i> first { <i>group-name</i> local } second { <i>group-name</i> local none } third { <i>group-name</i> local none }	Configure the AAA authentication modes. Note: up to 2 modes can be configured for an AAA server group.
4	Raisecom(config-aaa)#aaa authorization { login cmd } method <i>method-name</i> first { <i>group-name</i> local } second { <i>group-name</i> local none } third { <i>group-name</i> local none }	Configure the AAA authorization modes. Note: up to 2 modes can be configured for an AAA server group.
5	Raisecom(config-aaa)#aaa authentication { dot1x ppp login mac-authen } method <i>method-name</i> first { <i>group-name</i> local } second { <i>group-name</i> local none } third { <i>group-name</i> local none }	Configure the AAA accounting modes. Note: up to 2 modes can be configured for an AAA server group.

8.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show aaa config	Show AAA configurations.
2	Raisecom#show aaa information	Show global information about AAA.
3	Raisecom#show aaa server	Show information about AAA servers.
4	Raisecom#show aaa server-group	Show information about AAA server groups.
5	Raisecom#show aaa method	Show information about AAA modes.

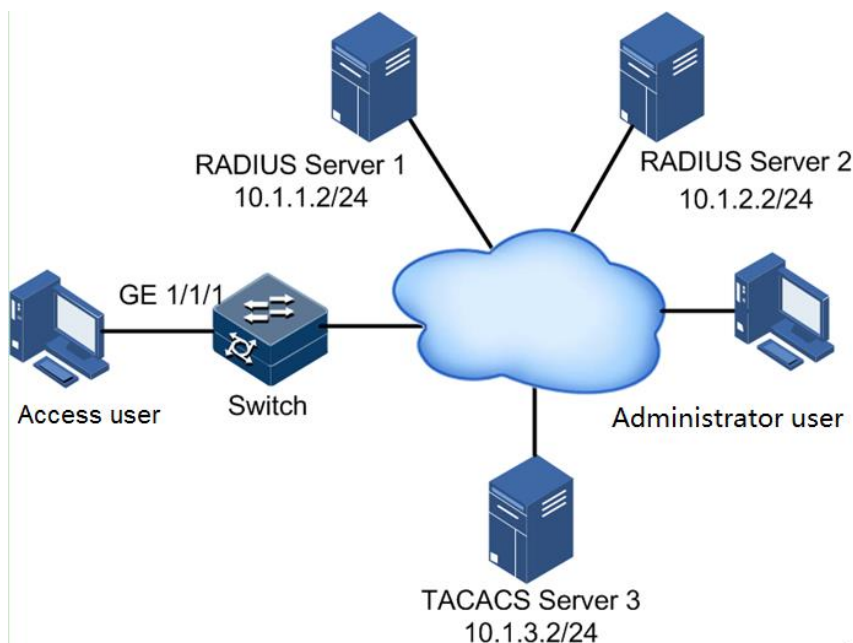
8.2.9 Example for configuring AAA

Networking requirement

As shown in Figure 8-1, to make access users and the administrator user to access different servers, configurations are as below:

- Configure the IP address, VLAN, and route on the switch for user connection and authentication.
- Create a local user account. Configure the AAA template and scheme for the administrator user. Use TACACS server 3 for authentication and authorization. Use RADIUS server 2 for accounting.
- Enable Dot1x. Configure the AAA template and scheme for access users. Use RADIUS server 1 for authentication, accounting, and authorization.

Figure 8-1 Domain-based authentication application networking



Configuration steps

Step 1 Configure the IP address.

```
Raisecom#configure
Raisecom(config)#interface vlan 1
Raisecom(config-vlanif-1)#ip address 10.1.0.254/24
Raisecom(config-vlanif-1)#exit
Raisecom(config)#ip route-static 0.0.0.0 0.0.0.0 10.1.0.1
```

Step 2 Configure the AAA server.

```
Raisecom(config)#aaa
Raisecom(config-aaa)#radius-server host Server1 ip-address 10.1.1.2
Raisecom(config-aaa)#radius-server host Server2 ip-address 10.1.2.2
Raisecom(config-aaa)#tacacs-server host Server3 ip-address 10.1.3.2
```

Step 3 Configure the AAA server group.

```
Raisecom(config-aaa)#server-group Group1 radius-server Server1
Raisecom(config-aaa)#server-group Group2 radius-server Server2
Raisecom(config-aaa)#server-group Group3 tacacs-server Server3
```

Step 4 Configure the AAA mode.

```
Raisecom(config-aaa)#aaa authentication login method Method1 first Group3
Raisecom(config-aaa)#aaa authorization login method Method2 first Group3
Raisecom(config-aaa)#aaa accounting login method Method3 first Group2
Raisecom(config-aaa)#aaa authentication dot1x method Method4 first Group1
Raisecom(config-aaa)#aaa accounting dot1x method Method5 first Group1
switch(config-aaa)#exit
```

Step 5 Configure the authentication mode, authorization mode, and accounting mode for management users.

```
Raisecom(config)#line vty * *
Raisecom(config-line)#login authentication aaa method Method1
Raisecom(config-line)#login authorization aaa method Method2
Raisecom(config-line)#login accounting aaa method Method3
Raisecom(config-line)#exit
```

Step 6 Configure the authentication mode, authorization mode, and accounting mode for access users.

```
Raisecom(config)#dot1x start
Raisecom(config)#interface ge 1/1/1
Raisecom(config-ge-1/1/1)#dot1x enable
Raisecom(config-ge-1/1/1)#dot1x aaa-authentication Method4
Raisecom(config-ge-1/1/1)#dot1x aaa-accounting Method5
Raisecom(config-ge-1/1/1)#exit
```

Checking results

Step 1 Use the **show aaa config** command to show configurations of the RADIUS server.

```
Raisecom#show aaa config
Version : AAA_V7.00.00.00
!
aaa
radius-server host Server1 ip-address 10.1.1.2
radius-server host Server2 ip-address 10.1.2.2
tacacs-server host Server3 ip-address 10.1.3.2
server-group Group1 radius-server Server1
server-group Group2 radius-server Server2
```

```
server-group Group3 tacacs-server Server3
aaa authentication login method Method1 first Group3
aaa authorization login method Method2 first Group3
aaa accounting login method Method3 first Group2
aaa authentication dot1x method Method4 first Group1
aaa accounting dot1x method Method5 first Group1
```

8.3 802.1x

8.3.1 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.

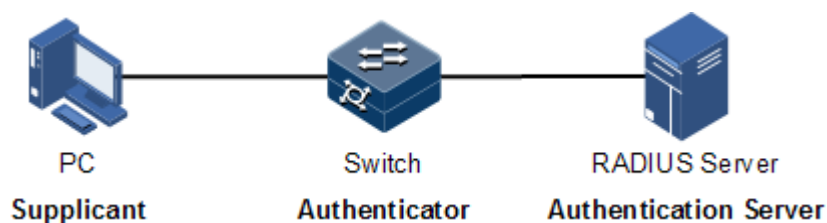
It is used to authenticate and control access devices at the physical layer of the network device. It defines a point-to-point connection mode between the device interface and user devices. User devices, connected to the interface, can access resources in the LAN if they are authenticated. Otherwise, they cannot access resources in the LAN through the switch.

802.1x structure

As shown in Figure 8-2, 802.1x authentication uses Client/Server mode, including the following 3 parts:

- Supplicant: a user-side device installed with the 802.1x client software (such as Windows XP 802.1x client), such as a PC
- Authenticator: an access control device supporting 802.1x authentication, such as a switch
- Authentication Server: a device used for authenticating, authorizing, and accounting users. Generally, the RADIUS server is taken as the 802.1x authentication server.

Figure 8-2 802.1x structure



Interface access control modes

The authenticator uses the authentication server to authenticate clients that need to access the LAN and controls interface authorized/ unauthorized status through the authentication results. You can control the access status of an interface by configuring access control modes on the interface. 802.1x authentication supports the following 3 interface access control modes:

- Protocol authorized mode (auto): the protocol state machine determines the authorization and authentication results. Before clients are successfully authenticated, only EAPoL packets are allowed to be received and sent. Users are disallowed to access network

resources and services provided by the switch. If clients are authorized, the interface is switched to the authorized state, allowing users to access network resources and services provided by the switch.

- Force interface authorized mode (authorized-force): the interface is in authorized state, allowing users to access network resources and services provided by the switch without being authorized and authenticated.
- Force interface unauthorized mode (unauthorized-force): the interface is in unauthorized mode. Users are disallowed to access network resources and services provided by the switch; in other words, users are disallowed to be authenticated.

802.1x authentication procedure

The 802.1x system supports the authentication process between the supplicant and the RADIUS server through EAP relay and EAP termination.

- EAP relay

The supplicant and the authentication server exchange information through the Extensible Authentication Protocol (EAP) packet while the supplicant and the authenticator exchange information through the EAP over LAN (EAPoL) packets. The EAP packet is encapsulated with authentication data. This authentication data will be encapsulated into the RADIUS packet to be transmitted to the authentication server through a complex network. This procedure is called EAP relay.

Both the authenticator and the supplicant can initiate the 802.1x authentication procedure. This document takes the supplicant for example, as shown below:

- Step 1 The user enters the user name and password. The supplicant sends an EAPoL-Start packet to the authenticator to start the 802.1x authentication.
- Step 2 The authenticator sends an EAP-Request/Identity to the supplicant, asking the user name of the supplicant.
- Step 3 The supplicant replies an EAP-Response/Identity packet to the authenticator, which includes the user name.
- Step 4 The authenticator encapsulates the EAP-Response/Identity packet to the RADIUS packet and sends the RADIUS packet to the authentication server.
- Step 5 The authentication server compares the received user name with the one in the database, finds the password for the user, and encrypts the password with a randomly-generated encryption word. Meanwhile it sends the encryption word to the authenticator who then sends the encryption word to the supplicant.
- Step 6 The supplicant encrypts the password with the received encryption password, and sends the encrypted password to the authentication server.
- Step 7 The authentication server compares the received encrypted password with the one generated by itself. If identical, the authenticator modifies the interface state to authorized state, allowing users to access the network through the interface and sends an EAP-Success packet to the supplicant. Otherwise, the interface is in unauthorized state and sends an EAP-Failure packet to the supplicant.

- EAP termination

Terminate the EAP packet at the device and map it to the RADIUS packet. Use standard RADIUS protocol to finish the authorization, authentication, and accounting procedure. The

device and RADIUS server adopt Password Authentication Protocol (PAP)/Challenge Handshake Authentication Protocol (CHAP) to perform authentication.

In the EAP termination mode, the random encryption character, used for encrypting the password, is generated by the device. And then the device sends the user name, random encryption character, and encrypted password to the RADIUS server for authentication.

802.1x timers

802.1x authentication involves the following 5 timers:

- Reauth-period: re-authorization timer. After the period is exceeded, the device re-initiates authorization.
- Quiet-period: quiet timer. When user authorization fails, the device needs to keep quiet for a period. After the period is exceeded, the device re-initiates authorization. During the quiet time, the device does not process authorization packets.
- Tx-period: transmission timeout timer. When the device sends a Request/Identity packet to users, the device will initiate the timer. If users do not send an authorization response packet during the tx-period, the device will re-send an authorization request packet. The device sends this packet three times in total.
- Supp-timeout: Supplicant authorization timeout timer. When the device sends a Request/Challenge packet to users, the device will initiate supp-timeout timer. If users do not send an authorization response packet during the supp-timeout, the device will re-send the Request/Challenge packet. The device sends this packet twice in total.
- Server-timeout: authentication server timeout timer. The timer defines the total timeout of sessions between the authorizer and RADIUS server. When the configured time expires, the authenticator will end the session with the RADIUS server and start a new authorization process.

802.1x guest VLAN

On the network, users not authenticated by 802.1x can access limited resources. When the guest VLAN is configured, the device adds the guest VLAN tag to the untagged packet and allows it to pass the interface.

- Authentication based on interface: after authentication is successful, the device deletes the guest VLAN of the interface.
- Authentication based on user: after authentication is successful, the device reserves the guest VLAN of the interface.
- The guest VLAN cannot be the super VLAN or the voice VLAN.

8.3.2 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 device.

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 device can ping through the RADIUS server successfully.

8.3.3 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	macbased
RADIUS server expiration timer	10s
Re-authentication	Enable
802.1x re-authentication timer	3600s
802.1x quiet timer	60s
Transmission timeout timer	30s
Maximum number of users	128

8.3.4 Configuring basic functions of 802.1x



Caution

Only one user authentication request is processed on an interface at a time.

Configure basic functions of 802.1x for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#dot1x { start stop }	Enable or disable global 802.1x.
3	Raisecom(config)#dot1x aaa authentication method <i>method-name</i>	Configure the AAA mode for global 802.1x authentication.
4	Raisecom(config)#dot1x max-user <i>user-number</i>	Configure the maximum number of users for global 802.1x.

Step	Command	Description
5	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
6	Raisecom(config-ge-1/0/*)#dot1x enable	Enable interface 802.1x.
7	Raisecom(config-ge-1/0/*)#dot1x port-control { auto force-auth force-unauth }	Configure access control mode on the interface.
8	Raisecom(config-ge-1/0/*)#dot1x port-method { mac port }	Configure the interface authentication mode.
9	Raisecom(config-ge-1/0/*)#dot1x max-user <i>user-number</i>	Configure the maximum number of users allowed to be authenticated by the 802.1x interface.
10	Raisecom(config-ge-1/0/*)#authentication guest-vlan <i>vlan-id</i>	Configure the Guest VLAN of the specified interface, which takes effect on both 802.1x and MAC authentication.
11	Raisecom(config-ge-1/0/*)#dot1x critical-vlan <i>vlan-id</i>	Configure the critical VLAN of 802.1x on the specified interface.
12	Raisecom(config-ge-1/0/*)#dot1x restrict-vlan <i>vlan-id</i>	Configure the restrict VLAN of 802.1x on the specified interface.
13	Raisecom(config-ge-1/0/*)#dot1x reauthenticate all user	Manually trigger reauthentication of 802.1x users on the specified interface.
14	Raisecom(config-ge-1/0/*)#dot1x delete all user	Force 802.1x users on the interface to be offline.
15	Raisecom(config-ge-1/0/*)#dot1x quiet { disable enable }	Enable or disable silence of 802.1x users on the interface.
16	Raisecom(config-ge-1/0/*)#dot1x quiet-times <i>times</i>	Configure the times of authentication failures for 802.1x users to trigger silence, being 3 by default.



Note

If 802.1x is disabled in global/interface configuration mode, it cannot be enabled on the interface.

8.3.5 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 device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config-ge-1/0/*)#dot1x reauthenticate { enable disable }	Enable 802.1x re-authentication.

8.3.6 Configuring 802.1x timers

Configure 802.1x timers for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config-ge-1/0/*)#dot1x reauthenticate period time	Configure the time of the re-authentication timer.
4	Raisecom(config-ge-1/0/*)#dot1x timer quiet-period time	Configure the time of the quiet timer.
5	Raisecom(config-ge-1/0/*)#dot1x supp period time	Configure the Request/MD5 Challenge request packet timeout timer.
6	Raisecom(config-ge-1/0/*)#dot1x server-timeout period time	Configure the authentication server timeout timer.
7	Raisecom(config-ge-1/0/*)#dot1x tx period time	Configure the Request/Identity request packet timeout timer.

8.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show dot1x config	Show all 802.1x configurations.
2	Raisecom#show dot1x information	Show 802.1x statistics.
3	Raisecom#show dot1x user	Show user information about 802.1x authentication.

No.	Command	Description
4	Raisecom#show dot1x <i>interface-type interface-number</i>	Show statistics and configurations of 802.1x authentication on the interface.

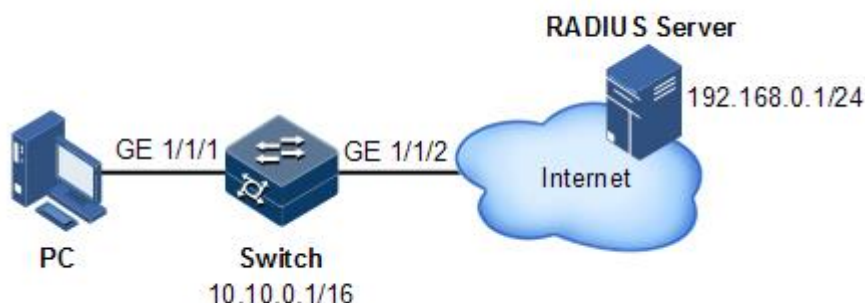
8.3.8 Example for configuring 802.1x

Networking requirements

As shown in Figure 8-3, 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.
- After the PC passes authentication, the Switch will start reauthentication every 600s.

Figure 8-3 Dot1x networking



Configuration steps

Step 1 Configure the IP addresses of the Switch and RADIUS server.

```

Raisecom#configure
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 10.10.0.1/16
Raisecom(config-vlan1)#exit
Raisecom(config)#ip route 0.0.0.0 0.0.0.0 10.10.0.2
Raisecom(config)#exit
Raisecom(config)#aaa
Raisecom(config-aaa)#radius-server host server1 ip-address 192.168.0.1
key 12345
Raisecom(config-aaa)#server-group grp1 radius- server server1
Raisecom(config-aaa)#aaa authentication dot1x method d1 first grp1
  
```

Step 2 Enable global 802.1x and interface 802.1x.

```
Raisecom#configure
Raisecom(config)#dot1x start
Raisecom(config)#dot1x aaa authentication method d1
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#dot1x enable
Raisecom(config-ge-1/0/1)#dot1x reauthenticate period 600
```

Checking results

Use the **show dot1x** command to show 802.1x configurations on the interface.

```
Raisecom#show dot1x interface ge 1/0/1
Interface                : ge 1/0/1
  Authentication Guest Vlan : n/a
Max User Num              : 1
Default Max User Num      : 1
Current User Num          : 1
Authen Success User Num   : 0
Authen Fail User Num      : 1
Authen Timeout User Num   : 1
Authenticating User Num   : 0
Authentication Method      : n/a
  Accounting Method       : n/a
Quiet                     : Disable
Reauthentication          : Enable
  Reauthentication Period : 3600
Mac Bypass                : Disable
Offline Detect            : Disable
Restrict Vlan              : n/a
Critical Vlan              : n/a
TX Period                  : 30
Supp Timeout Period       : 5
Server time Period        : 120
Port Control              : Auto
  Port Method              : Mac Based
Port Auth State            : Unauthenticated
Auth Method                : Chap
Not Eapol Trigger         : Disable
Trigger Authen Type       : None
Trigger Auth Pkt Type     : ARP NDP DHCP DHCP6
Rx Eapol Start Pkt Num    : 61
Rx Eapol Logoff Pkt Num   : 0
Rx Eap Identity Pkt Num   : 12
Rx Eap MD5 Pkt Num        : 5
Tx Eap Success Pkt Num    : 0
Tx Eap Fail Pkt Num       : 11
Tx Eap Identity Pkt Num   : 6
Tx Eap MD5 Pkt Num        : 5
```

8.4 PPPoE+

8.4.1 Introduction

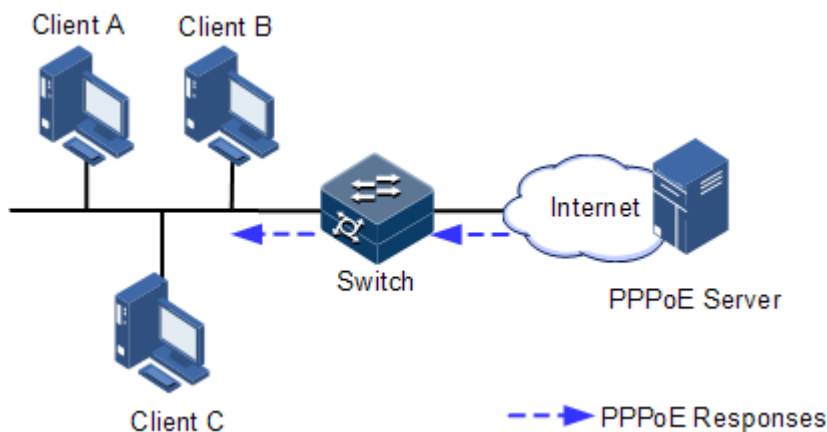
PPPoE Intermediate Agent (PPPoE+) is used to process authentication packets. PPPoE+ adds more information about access devices into the authentication packet to bind account and access device so that the account is not shared and stolen, and the carrier's and users' interests are protected. This provides 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 Client/Server mode, as shown in Figure 8-4. 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 8-4 Accessing the network through PPPoE authentication



To access the network through PPPoE authentication, you need to pass through the following 2 stages: discovery stage (authentication stage) and session stage. PPPoE+ is used to process packets at the discovery stage. The following steps show the whole discovery stage.

- Step 1 To access the network through PPPoE authentication, the client sends a broadcast packet PPPoE Active Discovery Initiation (PADI). This packet is used to query the authentication server.
- Step 2 After receiving the PADI packet, the authentication server replies a unicast packet PPPoE Active Discovery Offer (PADO).
- Step 3 If multiple authentication servers reply PADO packets, the client selects one from them and then sends a unicast PPPoE Active Discovery Request (PADR) to the authentication server.
- Step 4 After receiving the PADR packet, if the authentication server believes that the user is legal, it sends a unicast packet PPPoE Active Discovery Session-confirmation (PADS) to the client.

PPPoE is used to add user identification information in to PADI and PADR. Therefore, the server can identify whether the user identification information is identical to the user account for assigning resources.

8.4.2 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

8.4.3 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/Outer VLAN ID/Inner VLAN ID
Attached string of Circuit ID	N/A
Padded MAC address of Remote ID	MAC address of the switch
Padding mode of Remote ID	Binary
Interface trusted status	Untrusted
Policy for processing received packets	Overwriting



Note

By default, PPPoE packets are forwarded without being attached with any information.

8.4.4 Configuring basic functions of PPPoE+



Caution

PPPoE+ is used to process PADI and PADR packets. It is designed for the PPPoE client. Generally, PPPoE+ is only enabled on interfaces that are connected to the PPPoE client. Trusted interfaces are interfaces through which the switch is connected to the PPPoE server. PPPoE+ and trusted interface are exclusive; in other words, an interface enabled with PPPoE+ cannot be configured as a trusted interface.

Enabling PPPoE+

After global PPPoE+ and interface PPPoE+ is enabled, PPPoE authentication packets sent to the interface will be attached with user information and then are forwarded to the trusted interface.

Enable PPPoE+ for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#pppoeplus start	Enable global PPPoE+.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
4	Raisecom(config-ge-1/0/1)#pppoeplus enable	Enable interface PPPoE+.

Configuring the PPPoE trusted interface

The PPPoE trusted interface can be used to lower the CPU utilization. It does not forward its received PPPoE packets to the CPU but sends them to the switching chip for direct forwarding. It is usually the interface connected to the PPPoE server.

Configure the PPPoE trusted interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config-ge-1/0/1)#pppoeplus trust	Configure the PPPoE trusted interface.

8.4.5 Configuring PPPoE+ packets

PPPoE is used to process a specified Tag in PPPoE packets. This Tag contains Circuit ID and Remote ID.

- Circuit ID: it is padded with the interface ID, affiliated VLAN IDs (inner VLAN ID and outer VLAN ID).
- Remote ID: it is padded with the MAC address of the interface that receives the client request packets or the MAC address of the switch.

Configuring the Circuit ID

The Circuit ID has 3 padding modes: ascii mode, common mode, and user-define mode.

- Ascii: the Circuit ID is padded with the string configured by CLI.
- Common: the Circuit ID is the default value.
- User-define: the Circuit ID is padded with the user-defined format.

Configure the Circuit ID for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#pppoeplus circuit-id { ascii common user-define } string	Configure the Circuit ID of the switch (no string needs to be configured in common mode).
3	Raisecom(config)#interface interface-type interface-number	Enter Layer 2 physical interface configuration mode.
4	Raisecom(config-ge-1/0/1)#pppoeplus circuit-id { ascii common user-define } string	Configure the Circuit ID on the interface (no string needs to be configured in common mode. If the Circuit ID is configured in both interface configuration mode and global configuration mode, the interface configuration takes effect preferentially).

Configuring the Remote ID

The Remote ID has 3 padding modes: ascii mode, common mode, and user-define mode.

- Ascii: the Remote ID is padded with the string configured by CLI.
- Common: the Remote ID is the default value.
- User-define: the Remote ID is padded with the user-defined format.

Configure the Remote ID for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#pppoeplus remote-id { ascii common user-define } string	Configure the Remote ID of the switch (no string needs to be configured in common mode).
3	Raisecom(config)#interface interface-type interface-number	Enter Layer 2 physical interface configuration mode.

Step	Command	Description
4	Raisecom(config-ge-1/0/1)#pppoeplus remote-id { ascii common user-define string }	Configure the Remote ID on the interface (no string needs to be configured in common mode. If the Remote ID is configured in both interface configuration mode and global configuration mode, the interface configuration takes effect preferentially).

Configuring Tag overriding

Tags of some fields may be forged by the client because of some reasons, so the original Tags need to be overridden.

- After the policy for processing received PPPoE+ Tag packets is configured to overwrite, if the PPPoE packet already carries the information field Tag, the information field Tag will be replaced.
- After the policy for processing received PPPoE+ Tag packets is configured to hold, if the PPPoE packet already carries the information field Tag, the information field Tag will be kept.
- After the policy for processing received PPPoE+ Tag packets is configured to discard, if the PPPoE packet already carries the information field Tag, the information field Tag will be discarded.

Configure Tag overriding for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#pppoeplus policy { drop keep replace }	Configure the policy for processing received PPPoE+ Tag packets.

8.4.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show pppoeplus config	Show PPPoE+ configurations.
2	Raisecom#show pppoeplus statistic [interface-type interface-number]	Show PPPoE+ statistics.

8.4.7 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)#reset pppoeplus statistic { all [interface-type interface-number] }	Clear PPPoE+ statistics. The device supports clearing PPPoE+ statistics on the specified interface.

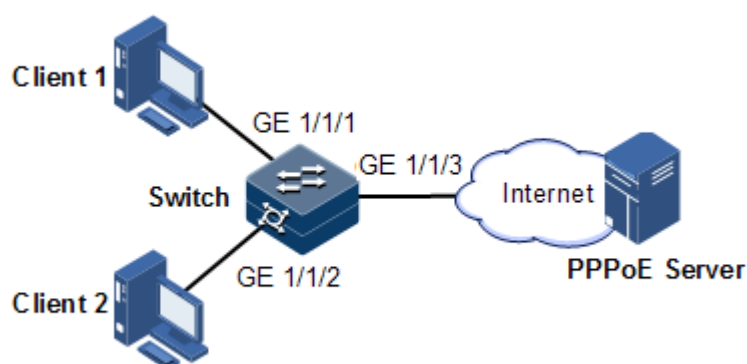
8.4.8 Example for configuring PPPoE+

Networking requirements

As shown in Figure 8-5, 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 type of the Circuit ID to user-define, in the format of interface ID + outer VLAN ID + device name. Configure the type of the Remote ID to ascii and the contents to 01:02:03:04:05:06.
- Configure the policy for processing received PPPoE Tag packets on interfaces GE 1/1/1 and GE 1/1/2.

Figure 8-5 PPPoE+ networking



Configuration steps

Step 1 Enable global PPPoE+, and PPPoE on GE 1/1/1 and GE 1/1/2.

```

Raisecom(config)#pppoeplus enable
Raisecom(config)#interface ge 1/1/1
Raisecom(config-ge-1/1/1)#pppoeplus enable
Raisecom(config-ge-1/1/1)#exit
Raisecom(config)#interface ge 1/1/2
Raisecom(config-gigaethernet1/1/2)#pppoeplus enable
  
```

Step 2 Configure interface GE 1/1/3 to the trusted interface.

```
Raisecom#configure
Raisecom(config)#interface ge 1/1/3
Raisecom(config-ge-1/1/3)#pppoeplus trust
Raisecom(config-ge-1/1/3)#exit
```

Step 3 Configure the format of the Circuit ID and Remote ID on interfaces GE 1/1/1 and GE 1/1/2.

```
Raisecom(config)#pppoeagent circuit-id user-
defined %portname:%svlan:%devicename
Raisecom(config)#pppoeplus remote-id ascii 01:02:03:04:05:06
```

Step 4 Configure the policy for processing received PPPoE+ Tag packets on interfaces GE 1/1/1 and GE 1/1/2.

```
Raisecom(config)#interface ge 1/1/1
Raisecom(config-ge-1/1/1)#pppoeplus policy keep
Raisecom(config-ge-1/1/1)#exit
Raisecom(config)#interface ge 1/1/2
Raisecom(config-ge-1/1/2)#pppoeplus policy drop
Raisecom(config-ge-1/1/2)#exit
```

Checking results

Use the **show pppoeplus config** command to show PPPoE+ configurations.

```
Raisecom#show pppoeplus config
!
pppoeplus start
!
interface ge 1/1 /1
pppoeplus enable
pppoeplus policy keep
pppoeplus circuit-id user-defined %portname:%svlan:%devicename
!
interface ge 1/1/2
pppoeplus enable
pppoeplus policy drop
pppoeplus remote-id ascii 01:02:03:04:05:06
!
interface ge 1/0/3
pppoeplus enable
pppoeplus trust
```

8.5 Port security MAC

8.5.1 Introduction

Port security MAC is used for the switching device on the edge of the network user side. It can ensure security of accessed data on an interface, and control the incoming packets according to the source MAC address.

You can enable port security MAC to limit and distinguish which users can access the network through secure interfaces. Only secure MAC addresses can access the network, unsecure MAC addresses will be dealt with as configured interface access violation mode.

Secure MAC address classification

Secure MAC addresses supported by the device are divided into the following three categories:

- 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 to the sticky secure MAC address if necessary, so as not to be aged and supports auto-loading.

- Sticky secure MAC address

The sticky secure MAC address is generated from the manual configuration of user in secure interface or converted from secure MAC address. Different from the 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 secure MAC addresses learnt from an interface will be converted to sticky secure MAC addresses.
- When sticky learning is disabled, all sticky secure MAC addresses on an interface will be converted to secure MAC addresses.

Processing mode for violating port security MAC

When the number of secure MAC addresses has already reached the maximum number, inputting of packets from a strange source MAC address will be regarded as a violation operation. For the illegal user access, there are different processing modes for configuring the switch according to secure MAC violation policy:

- Protect mode: for illegal access users, the secure interface will discard the user's packets directly.
- Restrict mode: for illegal access users, the secure interface will discard the user's packets, and the console will print Syslog information and send an alarm to the NMS.

- Shutdown mode: for illegal access users, the secure interface will discard the user's packets, and the console will print Syslog information, send an alarm to the NMS, and then shut down the secure interface.



Caution

When the MAC address is flapping, in other words, secure interface A is accessed by a user corresponding to a secure MAC address that is already on secure interface B, secure interface A will process the access as violation.

8.5.2 Preparing for configurations

Scenario

To ensure the security of data accessed by the interface of the switch, you can control the incoming packets according to source MAC address. With port security MAC, you can configure the feature of permitting specified users to access the interface, or permitting specified number of users to access from this interface only. However, when the number of users exceeds the limit, the accessed packets will be processed in accordance with port security MAC violation policies.

Prerequisite

N/A

8.5.3 Default configurations of port security MAC

Default configurations of port security MAC are as below.

Function	Default value
Interface secure MAC	Disable
Dynamic secure MAC sticky learning	Disable
Port secure MAC Trap	Disable
Processing mode for port secure MAC violation	Restrict
Maximum number of port security MAC	1024

8.5.4 Configuring basic functions of port security MAC



Caution

- We do not recommend enabling port security MAC on member interfaces of the LAG.
- We do not recommend using the MAC address management function to configure static MAC addresses when port security MAC is enabled.
- When the 802.1x interface adopts a MAC address-based authentication mode, port security MAC and 802.1x are mutually exclusive. We do not recommend co-configuring them concurrently.

- Port security MAC and interface-/interface VLAN-based MAC number limit are mutually exclusive, which cannot be configured concurrently.

Configure basic functions of port security MAC for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config-ge-1/0/1)#port-security enable	Enable port security MAC.
4	Raisecom(config-ge-1/0/1)#port-security maximum <i>maximum</i>	Configure the maximum number of secure MAC addresses.
5	Raisecom(config-ge-1/0/1)#port-security protect-action { protect restrict shutdown }	Configure the secure MAC violation mode.
6	Raisecom(config-ge-1/0/1)#shutdown Raisecom(config-ge-1/0/1)#no shutdown	Re-enable the interface which is shut down due to violating port security MAC.
7	Raisecom(config)#port-security error-down recovery-interval <i>second</i>	(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 re-enable this interface which is shut down due to violating port security MAC. When the interface is Up, the configured secure MAC violation mode will continue to be valid.

8.5.5 Configuring the 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 device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config-ge-1/0/1)#port-security enable	Enable port security MAC.

Step	Command	Description
4	Raisecom(config-ge-1/0/1)#port-security mac-address sticky enable	Enable sticky secure MAC learning.
5	Raisecom(config-ge-1/0/1)#port-security mac-address sticky vlan <i>vlan-id</i> mac <i>mac-address</i>	Manually configure sticky secure MAC addresses.



Note

After sticky secure MAC address learning is enabled, the dynamic secure MAC address will be converted to the sticky secure MAC address; the manually configured sticky secure MAC address will take effect.

8.5.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show mac-address config	Show configurations of port security MAC.
2	Raisecom#show mac-address { security sticky }	Show information about entries of secure MAC addresses.

8.5.7 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)#no mac-address { security sticky } [<i>interface-type interface-number</i>]	Clear the specified type of secure MAC addresses.

8.5.8 Example for configuring port security MAC

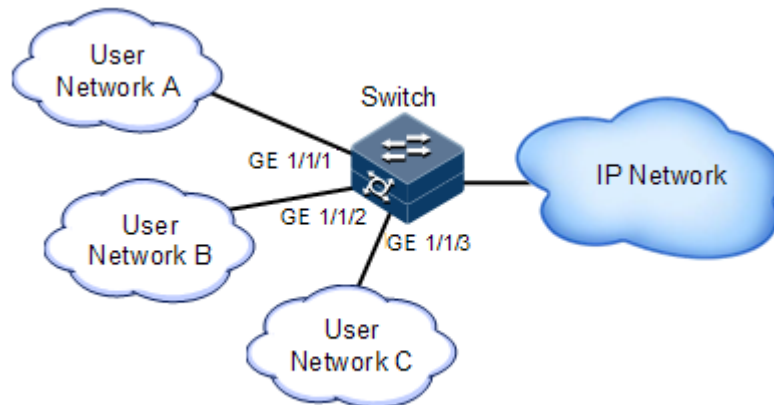
Networking requirements

As shown in Figure 8-6, 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 violation mode is Protect mode.
- GE 1/1/2 allows up to 2 users to access the network. MAC addresses of the 2 users are determined through learning. 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. The violation mode is Shutdown mode.

Figure 8-6 Port security MAC networking



Configuration steps

Step 1 Configure the secure MAC address on GE 1/0/1.

```
Raisecom#configure
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port-security enable
Raisecom(config-ge-1/0/1)#port-security maximum 3
Raisecom(config-ge-1/0/1)#port-security mac-address sticky enable
Raisecom(config-ge-1/0/1)#port-security mac-address sticky vlan 1 mac
00:00:00:00:00:01
Raisecom(config-ge-1/0/1)#quit
```

Step 2 Configure the secure MAC address on GE 1/1/2.

```
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port-security enable
Raisecom(config-ge-1/0/2)#port-security maximum 2
Raisecom(config-ge-1/0/2)#port-security protect-action restrict
Raisecom(config-ge-1/0/2)# quit
```

Step 3 Configure the secure MAC address for GE 1/1/3.

```
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port-security enable
Raisecom(config-ge-1/0/3)#port-security maximum 1
Raisecom(config-ge-1/0/3)#port-security protect-action shutdown
Raisecom(config-ge-1/0/3)#port-security mac-address sticky enable
Raisecom(config-ge-1/0/3)#port-security mac-address sticky vlan 1
```

```
mac 00:00:00:00:00:02
Raisecom(config-ge-1/0/3)#quit
```

Checking results

Use the **show mac-address config** command to show configurations of port security MAC.

```
Raisecom#show mac-address config
!
mac-address aging-time 500
!
interface ge 1/0/1
port-security enable
port-security maximum 3
port-security mac-address sticky enable
!
interface ge 1/0/2
port-security enable
port-security maximum 2
!
interface ge 1/0/3
port-security enable
port-security protect-action shutdown
port-security mac-address sticky enable
```

Use the **show mac-address sticky** command to show configurations and learning of secure MAC addresses.

```
Raisecom(config)#show mac-address sticky
```

MacAddress	VLAN/VSI/BD	Learned-From	Type	Valid
0000:0000:0001	1/--/--	ge-1/0/1	sticky	yes
0000:0000:0002	1/--/--	ge-1/0/3	sticky	yes

Total:2	Static:0	Dynamic:0	Blackhole:0	
Sticky:2	Security:0	Snooping:0		

8.6 Storm suppression and storm control

8.6.1 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.

Storm suppression and storm control can restrict broadcast flow generated from network and prevent broadcast storm from occurring when the broadcast flow increases sharply, thus ensuring normal forwarding of common packets.

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 device 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 suppression

Storm suppression allows an interface to filter broadcast packets received by the interface. After storm suppression is enabled, when the number of received broadcast packets reaches the pre-configured threshold, the device will take the corresponding action.

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 broadcast 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 suppression and storm control

Storm suppression and storm control are performed in the following forms:

- 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
- Percent: the percentage of the maximum interface rate allowed to pass, supported by the physical interface only

8.6.2 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

8.6.3 Default configurations of storm suppression and storm control

Default configurations of storm suppression and storm control are as below.

Function	Default value
Broadcast storm suppression status	Disable
Unknown unicast storm suppression status	Disable
Unknown multicast storm suppression status	Disable
Action for storm control on the interface	N/A
Restoration period of the interface	30s
Interface storm control Trap	Disable
Broadcast storm control status	Disable
Unknown unicast storm control status	Disable
Unknown multicast storm control status	Disable

8.6.4 Configuring storm suppression



Caution

- Storm suppression and VLAN-based rate limiting are exclusive. We do not recommend enabling them on the same interface concurrently.
- Storm suppression and storm control cannot be concurrently configured on the same interface.

Configure storm suppression for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config- gigaethernet1/1/*)#storm- suppression { unknown-unicast unknown-multicast broadcast } min-rate { kbps mbps gbps } rate-value max-rate { kbps mbps gbps } rate-value	Enable storm suppression on the physical interface, and configure the BPS storm suppression threshold.

Step	Command	Description
	Raisecom(config-gigaethernet1/1/*)#storm-suppression { unknown-unicast unknown-multicast broadcast } min-rate <i>rate-value</i> max-rate <i>rate-value</i>	Enable storm suppression on the physical interface, and configure the PPS storm suppression threshold.
	Raisecom(config-port-channel*)#storm-suppression { unknown-unicast unknown-multicast broadcast } min-rate percent <i>rate-value</i> max-rate percent <i>rate-value</i>	Enable storm suppression on the physical interface, and configure the percentage storm suppression threshold.
4	Raisecom(config-gigaethernet1/1/*)#storm-suppression action { block error-down none }	Configure the action for storm suppression on the interface.
5	Raisecom(config-gigaethernet1/1/*)#storm-suppression interval { <1-200> default }	Configure the restoration period of the shutdown interface.
6	Raisecom(config-gigaethernet1/1/*)#storm-suppression snmp-trap enable	Enable or disable storm suppression Trap.
7	Raisecom(config-gigaethernet1/1/*)#exit	Return to global configuration mode.

8.6.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show storm-suppression interface [<i>interface-type</i> <i>interface-number</i>]	Show configurations of storm suppression on the interface.
2	Raisecom#show storm-suppression information	Show global configurations of storm suppression.

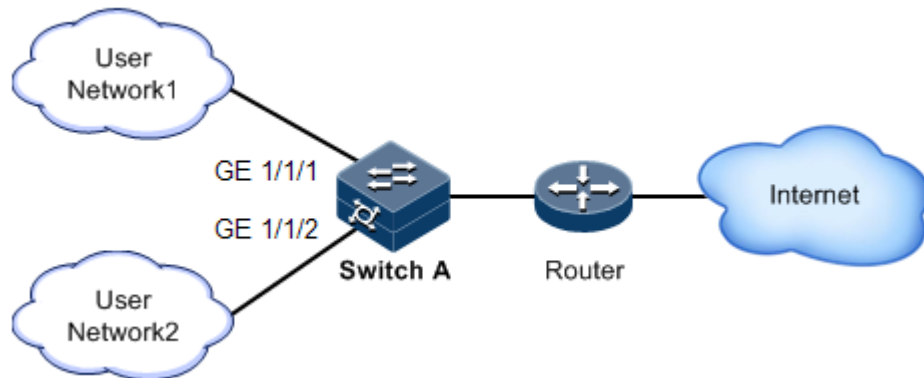
8.6.6 Example for configuring storm suppression

Networking requirements

As shown in Figure 8-7, when GE 1/1/1 and GE 1/1/2 on the Switch receive excessive unknown unicast packets or broadcast packets, Switch A forwards these packets to all interfaces except the Rx interface, which may cause broadcast storm and lower forwarding performance of Switch A.

To restrict impacts on Switch A caused by broadcast storm, you need to configure storm suppression on Switch A to restrict broadcast packets from user networks 1 and 2, with the threshold of 640 pps.

Figure 8-7 Storm suppression networking



Configuration steps

Enable storm suppression, and configure the threshold for storm suppression.

```

Raisecom(config)#interface ge 1/1/1
Raisecom(config-ge-1/1/1)#storm-suppression broadcast min-rate kbps 320
max-rate kbps 640
Raisecom(config-ge-1/1/1)#storm-suppression action error-down
Raisecom(config-ge-1/1/1)#exit
Raisecom(config)#interface ge 1/1/2
Raisecom(config-ge-1/1/2)#storm-suppression broadcast min-rate kbps 320
max-rate kbps 640
Raisecom(config-ge-1/1/2)#storm-suppression action error-down
  
```

Checking results

Use the **show storm-suppression** command to show configurations of storm suppression.

```

Raisecom#show storm-suppression interface
NOTE :
  UNMC: unknown multicast ; BC: broadcast ; UNC: unknown unicast
  Interface      Type              State  RateMode  Min/MaxRate
  Action/Status  Interval
-----
ge-1/1/1        UNC              disable bps  n/a        none/normal
5
                UNMC              disable bps  n/a        none/normal
5
  
```

```

5          BC      enable bps      320/640 (kbit/s)      none/errordown
ge-1/1/2
none/normal          5
          UNMC    disable bps      n/a                  none/normal
5
          BC      enable bps      320/640                (kbit/s)
none/errordown      5
-----
-----

```

8.6.7 Configuring storm control



Caution

- Storm control and VLAN-based rate limiting are exclusive. We do not recommend enabling them on the same interface concurrently.
- Storm control and storm control cannot be concurrently configured on the same interface.

Configure storm control for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config-gigaethernet1/1/*)#storm-control { unknown-unicast unknown-multicast broadcast unicast multicast } cir { kbits mbps gbps } <i>cir-value</i> cbs { bytes kbytes mbytes } <i>cbs-value</i>	Enable storm control on the interface, and configure the BPS storm control threshold.
	Raisecom(config-gigaethernet1/1/*)#storm-control { unknown-unicast unknown-multicast broadcast unicast multicast } pps <i>pps-value</i>	Enable storm control on the physical interface, and configure the PPS storm control threshold.
	Raisecom(config-port-channel*)#storm-control { unknown-unicast unknown-multicast broadcast unicast multicast } percent <i><1-100></i>	Enable storm control on the physical interface, and configure the percentage storm control threshold.
4	Raisecom(config-gigaethernet1/1/*)#exit	Return to global configuration mode.

8.6.8 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 on the interface.

8.6.9 Example for configuring storm control

Networking requirements

When GE 1/1/1 and GE 1/1/2 on the Switch receive excessive unknown unicast packets or broadcast packets, Switch A forwards these packets to all interfaces except the Rx interface, which may cause broadcast storm and lower forwarding performance of Switch A.

To restrict impacts on Switch A caused by broadcast storm, you need to configure storm control on Switch A to restrict broadcast packets from user networks 1 and 2, with the CIR of 640 kbit/s, CBS of 6400 Kbytes, and discarding exceeding packets.

Configuration steps

Configure the threshold for storm control.

```
Raisecom(config)#interface ge 1/1/1
Raisecom(config-ge-1/1/1)#storm-control broadcast cir kbps 640 cbs kbytes 6400
Raisecom(config-ge-1/1/1)#exit
Raisecom(config)#interface ge 1/1/2
```

Checking results

Use the **show storm-control** command to show configurations of storm control.

```
Raisecom#show storm-control interface
NOTE :
  UNC: unknown unicast ; UNMC: unknown multicast ; NC: known unicast
  NMC: known multicast ; MC: all multicast ; UC: all unicast ; BC:
broadcast
Interface          Type      State      RateMode  RateValue
-----
ge-1/1/1           UNC       disable    pps       n/a
                  UNMC      disable    pps       n/a
                  BC        enable     bps       cir: 640(kbit/s),cbs:
6553600(byte)
                  UC        disable    pps       n/a
                  MC        disable    pps       n/a
ge-1/1/2           UNC       disable    pps       n/a
                  UNMC      disable    pps       n/a
```

6553600(byte)	BC	enable	bps	cir: 640(kbit/s),cbs:
	UC	disable	pps	n/a
	MC	disable	pps	n/a

8.7 ARP attack protection

8.7.1 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 to alter the ARP table of the gateway or host. When they send excessive IP packets, whose IP addresses cannot be resolved, to the device, they will cause the following harms:

- The device sends excessive ARP request packets to the destination network segment, so this network segment is overburdened.
- The device repeatedly resolves destination IP addresses, so the CPU is overburdened.

To prevent these harms due to attacks on IP packets, the device supports ARP attack protection.

Prerequisite

N/A

8.7.2 Default configurations of ARP attack protection

N/A

8.7.3 Configuring ARP

Configure ARP for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#arp -antiattack src-ip enable	Configure ARP conflict detection for ARP source IP addresses. By searching the ARP table using the source IP address in the ARP packet, if the corresponding ARP table entry is found and the corresponding MAC address in the ARP table entry is inconsistent with the source MAC address in the ARP packet, it is considered an ARP conflict. The ARP packet will be discarded to prevent attackers from tampering with the MAC address in the ARP table.

Step	Command	Description
3	Raisecom(config)#arp -antiattack src-mac enable	Configure ARP conflict detection for ARP source MAC addresses. By searching the ARP table using the source MAC address in the ARP packet, if the corresponding ARP table entry is found and the corresponding IP address in the ARP table entry is inconsistent with the source IP address in the ARP packet, it is considered an ARP conflict. The ARP packet will be discarded to prevent attackers from tampering with the IP address in the ARP table.
4	Raisecom(config)#arp -antiattack arp- cheat enable	Configure ARP spoofing detection of counterfeiting the device. After the detection device receives the source or destination IP address, and the source MAC address and ARP packet type in the ARP packet, it determines whether the ARP packet is an attack packet counterfeiting the device. If it detects the packet as an attack packet, it will discard the ARP packet and sends a gratuitous ARP of the device.
5	Raisecom(config)#arp -antiattack gratuitous-arp enable	Configure gratuitous ARP packets to be actively discarded. After this function is enabled, the device directly discards gratuitous ARP packets, which can prevent the device from processing a large number of gratuitous ARP packets, resulting in CPU overload and inability to process other services.
6	Raisecom(config)#arp -antiattack gateway- cheat enable	Configure ARP gateway anti-conflict. This function can prevent users from impersonating the gateway to send ARP packets and illegally modifying ARP entries of other users on the network. ARP gateway anti-conflict and dynamic ARP inspection cannot be configured concurrently.
7	Raisecom(config- vlan*)#arp- antiattack check user-bind enable Or Raisecom(config-ge- */*/*)#arp- antiattack check user-bind enable	Configure Dynamic ARP Inspection (DAI). After DAI is enabled, when the device receives an ARP packet, it compares the source IP, source MAC, interface and VLAN information about the ARP packet with the information in the DHCP Snooping binding table. If the information matches, it considers the user a legitimate user and allows the user of the ARP packet to pass. Otherwise, it considers the user an attacker and discards the ARP packet. This feature is applicable to DHCP Snooping scenarios only.

Step	Command	Description
8	<pre>Raisecom(config- vlan*)#arp- antiattack check user-bind check-item { interface ip- address mac- address } Or Raisecom(config-ge- */*/*)#arp- antiattack check user-bind check-item { vlan ip-address mac-address }</pre>	Configure DAI items. The three DAI items can be combined freely. By default, they are all selected.

8.7.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<pre>Raisecom#show arp- antiattack config</pre>	Show configurations of ARP attack protection.

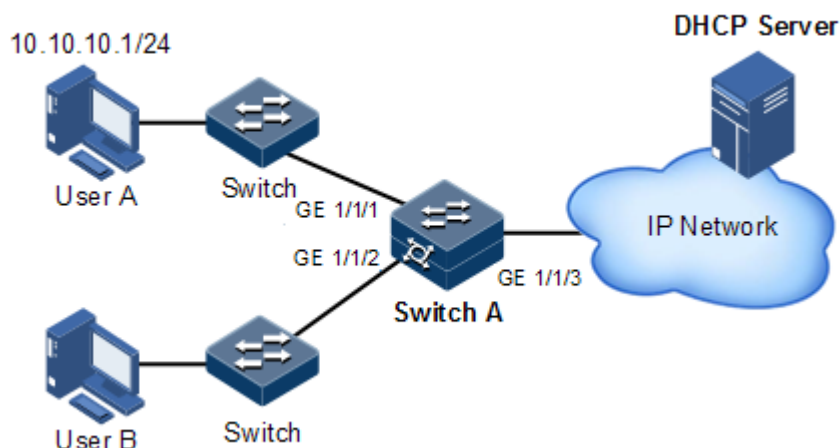
8.7.5 Example for configuring ARP attack protection

Networking requirements

To prevent ARP attacks shown below, configure ARP attack protection on Switch A with the following requirements:

- Disallow gratuitous ARP messages to pass. Enable ARP conflict detection for ARP source IP addresses and source MAC addresses, and the ARP spoofing detection for impersonating this device.
- Switch A serves as the gateway for User A. Enable ARP gateway anti-conflict.
- Clear configurations of the ARP gateway anti-conflict on Switch A. Switch A provides Layer 2 accessibility from User B to the DHCP server. Configure DAI on GE 1/1/2.

Figure 8-8 DAI networking



Step 1 Configure ARP conflict detection for ARP source IP addresses.

```
Raisecom#configure
Raisecom(config)#arp-antiattack src-ip enable
```

Step 2 Configure ARP conflict detection for ARP source MAC addresses.

```
Raisecom(config)#arp-antiattack src-mac enable
```

Step 3 Enable ARP spoofing impersonating the device.

```
Raisecom(config)#arp-antiattack arp-cheat enable
```

Step 4 Enable active discarding of gratuitous ARP packets.

```
Raisecom(config)#arp-antiattack gratuitous-arp enable
```

Step 5 Enable ARP gateway anti-conflict.

```
Raisecom(config)#arp-antiattack gateway-cheat enable
```

Step 6 Enable DAI. To enable DAI, disable ARP gateway anti-conflict in advance.

```
Raisecom(config)#arp-antiattack gateway-cheat disable
Raisecom(config)#interface ge 1/1/2
Raisecom(config-ge-1/1/2)#arp-antiattack check user-bind enable
Raisecom(config-ge-1/1/2)#exit
Raisecom(config)#
```

Checking results

Use the **show arp-antiattack config** command to show configurations of ARP attack protection.

```
Raisecom#show arp-antiattack config
Version: ANTIARP_VL2.10.00.00
!
arp-antiattack src-ip enable
arp-antiattack src-mac enable
arp-antiattack arp-cheat enable
arp-antiattack gratuitous-arp enable
arp-antiattack gateway-cheat enable

Raisecom#show arp-antiattack config
Version: ANTIARP_VL2.10.00.00
!
arp-antiattack src-ip enable
arp-antiattack src-mac enable
arp-antiattack arp-cheat enable
arp-antiattack gratuitous-arp enable
!
interface ge 1/1/2
  arp-antiattack check user-bind enable
```

8.8 ND Snooping

8.8.1 Introduction

Neighbor Discovery (ND) is a group of messages or processes for determining relations between neighboring nodes. Its messages replace IPv4 Address Resolution Protocol (ARP), ICMP Router Discovery (RD), and ICMP Redirect messages, and it also supports the following functions:

- Detecting address conflicts
- Resolving the neighbor address
- Determining neighbor reachability
- Configuring the IP address of the host

ND Snooping is used on the switch to check user validity. It normally forwards ND packets of authorized users and discards those of unauthorized users, thus preventing attacks from pseudo users and gateways.

User validity check is used to determine whether a user is an authorized user of the VLAN to which the interface receiving the ND packet belongs, according to the source IPv6 address and source MAC address carried in the ND packet.

ND Snooping divides interfaces of the access device into the following two types:

- ND trusted interface: this interface does not check user validity, but normally forward ND packets.
- ND untrusted interface: the device takes RA packets received by the ND untrusted interface illegal and thus discards them directly. The device checks NA/RS/NS packets received by the ND untrusted interface and matches them with the binding table; when they do not comply with the binding table relation, the device takes them illegal and discards them. The device normally forward packets of other types received by the ND untrusted interface.

8.8.2 Preparing for configurations

Scenarios

ND Snooping is used to prevent common ND spoofing attacks on the network, thus able to isolate ND packets from unauthorized sources. You can configure the trusted status of an interface to trust ND packets or not and configure the binding table to determine whether ND packets comply with requirements.

Prerequisite

N/A

8.8.3 Default configurations of ND Snooping

Default configurations of ND Snooping are as below.

Function	Default value
Interface trusted status of ND Snooping	Untrusted
Global ND Snooping status	Disable
Interface ND Snooping status	Disable
RA Snooping interface trusted status	Disable

8.8.4 Configuring ND Snooping

Enable static binding of ND Snooping for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#nd-snooping start	Enable global ND Snooping.

Step	Command	Description
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode or VLAN interface configuration mode.
4	Raisecom(config-ge-1/1/*)#nd-snooping enable	Enable ND Snooping on the interface that is connected to the gateway.
5	Raisecom(config-ge-1/1/*)#nd-snooping trust	Configure the interface that is connected to the gateway as a trusted interface.
6	Raisecom(config)#nd-snooping check { na ns rs } enable	Enable validity check on NS/NA/RS packets by ND Snooping.

8.8.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show nd-snooping config	Show configurations of ND Snooping.
2	Raisecom#show nd-snooping user-bind	Show the user binding table of ND Snooping.
3	Raisecom#show nd-snooping prefix	Show the prefix table of ND Snooping.

8.8.6 Maintenance

Maintain the device as below.

No.	Command	Description
1	Raisecom(config)#clear ipv6 nd snooping statistics [interface <i>interface-type interface-number]</i>	Clear statistics on ND Snooping user packets received by the device.
2	Raisecom(config)#clear ipv6 nd snooping ip-address <i>ipv6-address</i> vlan <i>vlan-id</i>	Delete entries dynamically learnt by ND Snooping in a specified VLAN.

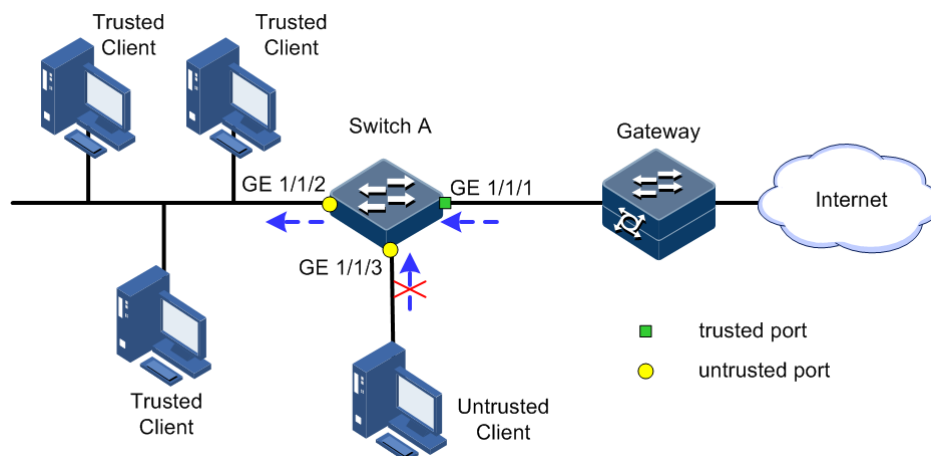
8.8.7 Example for configuring ND Snooping

Networking requirements

As shown in Figure 8-9, the host of a LAN user is connected to the gateway by Switch A. It has to obtain the IPv6 address through stateless automatic configuration according to the

prefix assigned by the gateway to the user network because no DHCPv6 server is deployed on the network. To prevent illegal users from sending NA/NS/RS/RA packets, which causes legal hosts to fail to obtain IPv6 addresses, enable ND Snooping on Switch A to intercept illegal packets.

Figure 8-9 ND Snooping networking



Configuration steps

Step 1 Create VLAN 10 on Switch A, and activate it.

Configure Switch.

```
Raisecom#configure
Raisecom(config)#hostname SwitchA
SwitchA(config)#vlan 10
```

Step 2 Add GE 1/1/2 on Switch A to VLAN 10 in Access mode. Configure it to Trunk mode, allowing packets of VLAN 10 to pass.

```
SwitchA(config)#interface ge 1/1/2
SwitchA(config-ge-1/1/2)#port link-type access
SwitchA(config-ge-1/1/2)#port default vlan 10
SwitchA(config-ge-1/1/2)#exit
SwitchA(config)#interface ge 1 /1/1
SwitchA(config-ge-1/1/1)#port link-type trunk
SwitchA(config-gigaethernet1/1/1)#port trunk allow-pass vlan 10
SwitchB(config-gigaethernet1/1/1)#exit
```

Step 3 Enable global ND Snooping and enable ND Snooping in VLAN 10. Configure GE 1/1/1 as the trusted interface.

```
SwitchA(config)#nd-snooping start
```

```
SwitchA(config)#vlan 10
SwitchA(config-vlan-10)#nd-snooping enable
SwitchA(config-vlan-10)#exit
SwitchA(config)#interface ge 1/1/1
SwitchA(config-ge-1/1/1)#nd-snooping enable
SwitchA(config-ge-1/1/1)#nd-snooping trust
SwitchA(config-ge-1/1/1)#exit
```

Step 4 Enable validity check on ND packets.

```
SwitchA(config)#nd-snooping check na enable
SwitchA(config)#nd-snooping check ns enable
SwitchA(config)#nd-snooping check rs enable
```

Checking results

Use **show nd-snooping config** command to check configurations of ND Snooping.

```
Raisecom#show nd-snooping config
!
nd-snooping start
nd-snooping check na enable
nd-snooping check ns enable
nd-snooping check rs enable
!
vlan 10
  nd-snooping enable
!
interface ge 1/1/1
nd-snooping enable
nd-snooping trust
```

8.9 DHCP Snooping

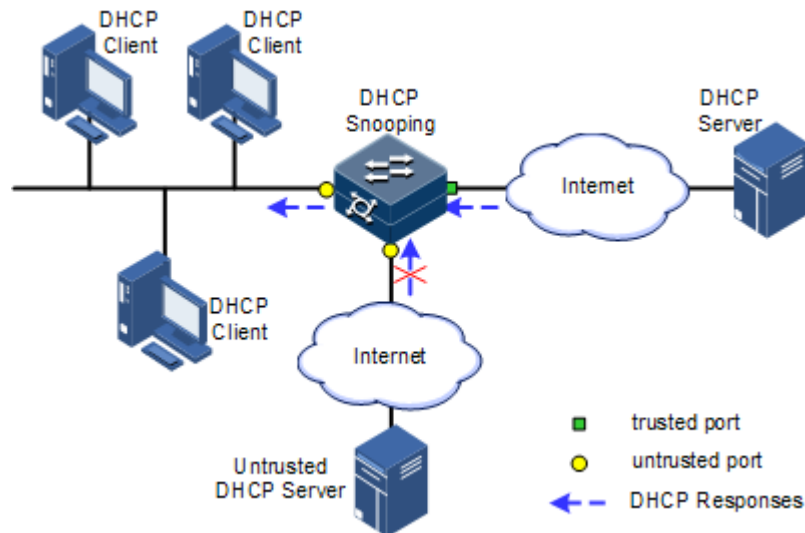
8.9.1 Introduction

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 8-10, to make DHCP client obtain the IP address from a legal DHCP server, the DHCP Snooping security system permits you to configure an interface as the trusted interface or untrusted interface: the trusted interface forwards DHCP packets normally; the untrusted interface discards reply packets from the DHCP server.

Figure 8-10 DHCP Snooping



- Record mapping between DHCP client IP address and MAC address.

DHCP Snooping records entries through monitor request and reply packets received by the trusted interface, including client MAC address, obtained IP address, DHCP client connected interface and VLAN of the interface. Then implement following by the record information:

- ARP detection: judge legality of a user that sends ARP packet and avoid ARP attack from illegal users.
- IP Source Guard: filter packets forwarded by interfaces by dynamically getting DHCP Snooping entries to avoid illegal packets to pass the interface.
- VLAN mapping: modify mapped VLAN of packets sent to users to original VLAN by searching IP address, MAC address, and original VLAN information in DHCP Snooping entry corresponding to the mapped VLAN.

The Option field in DHCP packet records position information about DHCP clients. The Administrator can use this Option field to locate DHCP clients and control client security and accounting.

If the device is configured with DHCP Snooping to support Option function:

- When the device receives a DHCP request packet, it processes packets according to Option field included or not, filling mode, and processing policy configured by user, then forwards the processed packet to DHCP server.
- When the device 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.

8.9.2 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

8.9.3 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	Disable
Interface trusted/untrusted status	Untrust
DHCP Snooping in support of Option 82	Disable

8.9.4 Configuring DHCP Snooping

Generally, you must ensure that the device 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 device will do nothing to Option fields in packets. For packets without Option fields, the device 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 device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#dhcp-snooping start	Enable global DHCP Snooping.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
4	Raisecom(config-ge-1/0/*)#dhcp-snooping enable	Enable interface DHCP Snooping. This function supports the QinQ interface.
5	Raisecom(config-ge-1/0/*)#dhcp-snooping trust	Configure the trusted interface of DHCP Snooping.
6	Raisecom(config-ge-1/0/*)#dhcp-snooping max-user-number <i>number</i>	Configure the maximum number of entries in the DHCP Snooping binding table.
7	Raisecom(config-ge-1/0/*)#dhcp-snooping server-filter enable	Configure DHCP Snooping to trust server configurations.

Step	Command	Description
8	Raisecom(config-ge-1/0/*)#dhcp-snooping check user-bind enable	Configure matching detection between DHCP packets and binding table.
9	Raisecom(config-ge-1/0/*)#dhcp-snooping check mac-address enable	Check whether the MAC address in the header of request packets sent by DHCP users.
10	Raisecom(config-ge-1/0/*)#dhcp-snooping option82 enable	Configure DHCP Snooping to support Option 82.
11	Raisecom(config)#exit	Return to global configuration mode.

8.9.5 Configure DHCP Snooping to support Option 82

Configure DHCP Snooping to support Option 82 for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#dhcp-snooping start	Enable global DHCP Snooping.
3	Raisecom(config)#interface interface-type interface-number	Enter physical interface configuration mode.
4	Raisecom(config-ge-1/0/*)#dhcp-snooping enable	Enable interface DHCP Snooping.
5	Raisecom(config-ge-1/0/*)#dhcp-snooping option82 enable	Configure global DHCP Snooping to support Option 82.
6	Raisecom(config-ge-1/0/*)#exit	Return to global configuration mode.

8.9.6 Configuring DHCPv6 Snooping

Configure DHCPv6 Snooping for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#dhcp-snooping start	Enable global DHCPv6 Snooping.
3	Raisecom(config)#interface interface-type interface-number	Enter physical interface configuration mode.
4	Raisecom(config-ge-1/0/*)#dhcp6-snooping enable	Enable interface DHCPv6 Snooping.
5	Raisecom(config-ge-1/0/*)#dhcpv6-snooping trust	Configure the trusted interface of DHCPv6 Snooping.

Step	Command	Description
6	Raisecom(config-ge-1/0/*)#dhcpv6-snooping max-user-number <i>number</i>	Configure the maximum number of entries in the DHCPv6 Snooping binding table.
7	Raisecom(config-ge-1/0/*)#dhcpv6-snooping option18 enable	Configure DHCP Snooping to support Option 18.
8	Raisecom(config-ge-1/0/*)#dhcpv6-snooping option37 enable	Configure DHCPv6 Snooping to support Option 37.

8.9.7 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom#show dhcp-snooping config	Show configurations of DHCP Snooping.
2	Raisecom#show dhcp-snooping user-bind	Show configurations of the DHCP Snooping binding table.
3	Raisecom#show dhcp-snooping statistics	Show statistics on DHCP Snooping statistics.
4	Raisecom#show dhcp-snooping interface	Show configurations of DHCP Snooping interfaces.
5	Raisecom#show dhcpv6-snooping config	Show configurations of DHCPv6 Snooping.
6	Raisecom#show dhcpv6-snooping user-bind	Show configurations of the DHCPv6 Snooping binding table.
7	Raisecom#show dhcpv6-snooping statistics	Show statistics on DHCPv6 Snooping statistics.
8	Raisecom#show dhcpv6-snooping interface	Show configurations of DHCPv6 Snooping interfaces.

8.9.8 Maintenance

Maintain the device as below.

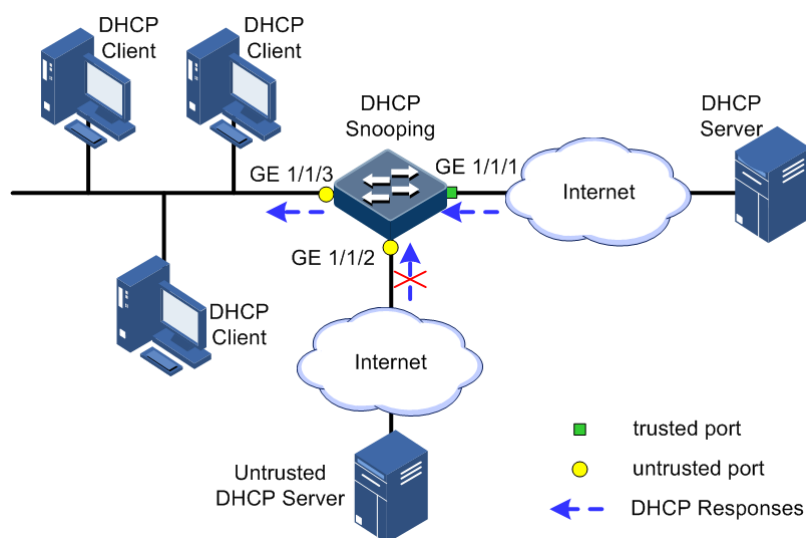
Command	Description
Raisecom(config)#reset dhcp-snooping user-bind [<i>ip-address</i> interface <i>interface-type</i> <i>interface-number</i> vlan <i>vlan-id</i>]	Clear information about the IPv4 binding table.
Raisecom(config)#reset dhcpv6-snooping user-bind [<i>ipv6-address</i> interface <i>interface-type</i> <i>interface-number</i> vlan <i>vlan-id</i>]	Clear information about the IPv6 binding table.

8.9.9 Example for configuring DHCP Snooping

Networking requirements

As shown in Figure 8-11, 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 about circuit ID sub-option to raisecom on GE 1/1/3, and padding information about remote ID sub-option to user01.

Figure 8-11 DHCP Snooping networking



Configuration steps

Step 1 Configure global DHCP Snooping.

```
Raisecom#configure
Raisecom(config)#dhcp-snooping start
```

Step 2 Configure the trusted interface.

```
Raisecom(config)#interface ge 1/1/1
Raisecom(config-ge-1/1/1)#dhcp-snooping enable
Raisecom(config-ge-1/1/1)#dhcp-snooping trust
Raisecom(config-ge-1/1/1)#exit
```

Step 3 Configure DHCP Relay to support Option 82 field and configure Option 82 field.

```
Raisecom(config)#interface ge 1/1/3
Raisecom(config-ge-1/1/3)#dhcp-snooping enable
```

```
Raisecom(config-ge-1/1/3)#dhcp-snooping option82 enable
Raisecom(config-ge-1/1/3)#dhcp-snooping option82 remote-id format default
Raisecom(config-ge-1/1/3)#dhcp-snooping option82 remote-id ascii user01
Raisecom(config-ge-1/1/3)#dhcp-snooping option82 circuit-id format
default
Raisecom(config-ge-1/1/3)#dhcp-snooping option82 circuit-id ascii
raisecom
Raisecom(config-ge-1/1/3)#exit
```

Checking results

Use the **show dhcp-snooping config** command to show configurations of DHCP Snooping.

```
Raisecom#show dhcp-snooping config

Version : DHCP Snooping V7.00.03.00
!
dhcp-snooping start
!
interface ge 1/1/1
  dhcp-snooping enable
  dhcp-snooping trust
!
interface ge 1/1/3
  dhcp-snooping enable
  dhcp-snooping option82 enable
  dhcp-snooping option82 remote-id format default
  dhcp-snooping option82 remote-id ascii user01
  dhcp-snooping option82 circuit-id format default
  dhcp-snooping option82 circuit-id ascii raisecom
.....
```

8.10 IP Source Guard

8.10.1 Introduction

IP Source Guard is used to filter and control the packets received by the interface, usually configured on the interface of the access user side to prevent illegal user packets from passing through, thereby limiting the illegal use of network resources (such as illegal hosts impersonating legitimate user IPs to access the network) and improving the security of the interface.

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:

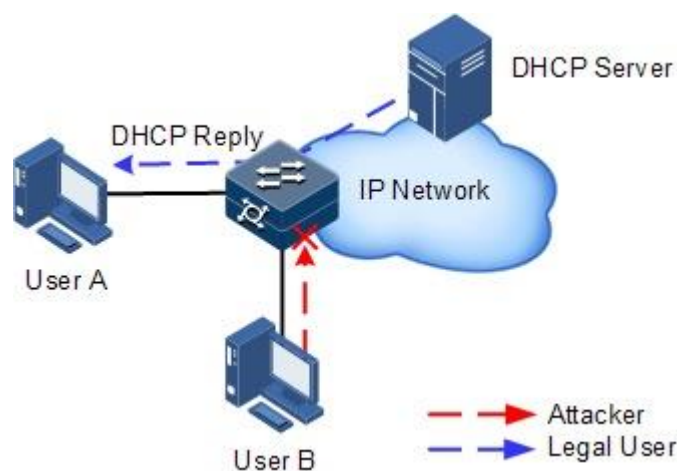
- Static binding: configure binding information manually and generate binding entry to complete the interface control, which fits for the case where the number of hosts is small or where you need to perform separate binding on a single host.
- Dynamic binding: obtain binding information automatically 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 device. The IP source binding table is taken as the basis for each interface to test received data packets. Figure 8-12 shows principles of IP Source Guard.

- If the received IP packets meet the relationship of Port/IP/MAC/VLAN binding entries in IP source binding table, forward these packets.
- If the received IP packets are DHCP data packets, forward these packets.
- Otherwise, discard these packets.

Figure 8-12 Principles of IP Source Guard



Before forwarding IP packets, the device 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.

8.10.2 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.

8.10.3 Default configurations of IP Source Guard

Default configurations of IP Source Guard are as below.

Function	Default value
Interface IP Source Guard status	Disable

8.10.4 Configuring IP Source Guard binding

Configuring IP Source Guard static binding

Configure IP Source Guard static binding for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#user-bind static ip ip-address / any mac mac-address / any [interface <i>interface-type interface-number</i>] vlan vlan-id / any	Enable IPv6 static binding.
3	Raisecom(config)#user-bind static ip6 ipv6-address / any mac mac-address / any [interface <i>interface-type interface-number</i>] vlan vlan-id / any	Configure IPv6 static binding.

8.10.5 Configuring the interface trust status of IP Source Guard

Configure the interface trust status of IP Source Guard for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-ge-1/0/*)#ip source check user-bind enable	Enable interface IP Source Guard.

8.10.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show user-bind config	Show configurations of IP Source Guard.
2	Raisecom#show ip source check user-bind	Show information about the interface enabled with IP Source Guard.

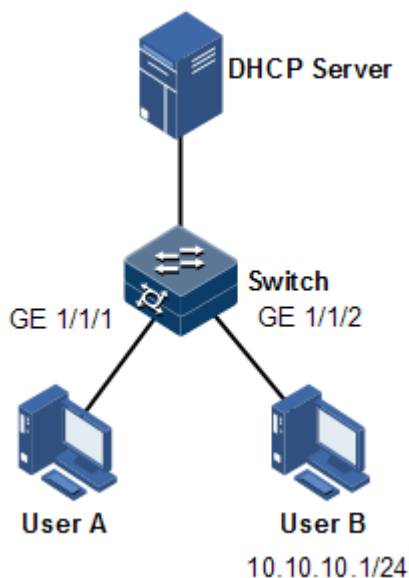
8.10.7 Example for configuring IP Source Guard

Networking requirements

As shown in Figure 8-13, to prevent IP address embezzlement, you need to configure IP Source Guard on the Switch.

- The Switch permits all IP packets on GE 1/1/1 to pass.
- GE 1/1/2 permits those IP packets to pass, of which the IP address is 10.10.10.1, the subnet mask is 255.255.255.0, and the status meets the dynamic binding learnt by DHCP Snooping.
- Other interfaces only permit the packets meeting DHCP Snooping learnt dynamic binding to pass.

Figure 8-13 Configuring IP Source Guard



Configuration steps

Step 1 Configure IP Source Guard.

```
Raisecom#configure
Raisecom(config)#int ge 1/1/2
Raisecom(config-ge-1/1/2)#ip source check user-bind enable
Raisecom(config-ge-1/1/2)#exit
Raisecom(config)#int ge 1/1/*
Raisecom(config-ge-1/1/*)#ip source check user-bind enable
Raisecom(config-ge-1/1/*)#exit
```

Step 2 Configure static binding entries.

```
Raisecom(config)#user-bind static ip 10.10.10.1 mac any interface ge
1/1/2 vlan any
```

Step 3 Configure DHCP Snooping on interface GE 1/1/2 and other interfaces.

Checking results

Use the **show user-bind config** command to show configurations of IP Source Guard.

```
Raisecom#show user-bind config
!
user-bind static ip 10.10.10.1 mac any interface ge 1/1/2 vlan any
```

```
!
interface ge 1/1/2
ip source check user-bind enable
!
interface ge 1/1/*
ip source check user-bind enable
```

Use the **show ip source check user-bind** command to show information about the interface enabled with IP Source Guard.

```
Raisecom#show ip source check user-bind
Interface          Check-Item          Alarm    Limit    DropPkts
-----
ge-1/1/2           ip,mac,vlan         disable  100      0
ge-1/1/*           ip,mac,vlan         disable  100      0
-----
```

8.11 CPU attack protection

8.11.1 Preparing for configurations

Scenario

When the device 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 attack protection helps efficiently limit the rate of packets which enters the CPU.

Prerequisite

N/A

8.11.2 Configuring CPU attack protection



Caution

Configurations of CPU protection affect other protocol modules, so we do not recommend modifying them. Only professional personnel can modify them.

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

Step	Command	Description
2	Raisecom(config)#cpu-defend policy test	Configure the policy of CPU attack protection. When the device is started, the default policy is issued and bound. The default policy cannot be modified, but the policy bound with the device can be modified.
3	Raisecom(config-cpudefend-policy-test)#car packet-type { arp bfd dhcpreply dhcprequest igmp l2cp ll2dp mld stp-customer telnet ... } pps pps-value	Configure the rate limit of the specified protocol packet type in the policy. The protocol packet types supported by the device depend on protocols supported by the device.
4	Raisecom(config)#cpu-defend bind-policy test	Configure CPU attack protection. The bound policy cannot be modified. To modify it, cancel the binding in advance.

8.11.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show cpu-defend config	Show configurations of CPU attack protection.
2	Raisecom#show cpu-defend statistics	Show statistics on CPU attack protection.

8.11.4 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)#reset cpu-defend statistics	Clear global statistics on CPU attack protection.

9 Reliability

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

- Link aggregation
- G.8032
- STP/RSTP
- MSTP
- Loop detection
- Interface backup
- Interface isolation

9.1 Link aggregation

9.1.1 Introduction

Link aggregation refers to aggregating multiple physical Ethernet interfaces to a Link Aggregation Group (LAG) and taking multiple physical links in the same LAG as one logical link. Link aggregation helps share traffic among members in the LAG. Besides effectively improving reliability on links between two devices, link aggregation helps gain higher bandwidth without upgrading hardware.

Generally, the link aggregation consists of manual link aggregation, static Link Aggregation Control Protocol (LACP) link aggregation, and dynamic LACP link aggregation.

- Manual link aggregation

All interfaces in the aggregation group forward data and share the load traffic equally. This is applicable to two directly connected devices of which one cannot use LACP.

- Manual master/slave link aggregation

There are two interfaces in the aggregation group. They back up each other. One is in the Active status, and the other is in the shutdown status. This is applicable when one end cannot use LACP.

- Static LACP aggregation

The aggregation group selects the active end and active interface through LACP protocol. The Active interface is used for forwarding data while the inactive interface is used for backing up links. This is applicable when LACP is supported by devices at both ends.

- Static LACP active/standby link aggregation

There are two interfaces in the aggregation group. They back up each other. One is in the Active status, and the other is in the Shutdown status. This is applicable when both devices support LACP.

9.1.2 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.

9.1.3 Default configurations of link aggregation

Default configurations of link aggregation are as below.

Function	Default value
Load balancing mode	src-dst-mac
LACP system priority	32768
LACP interface priority	32768
LACP interface mode	active
LACP timeout mode	slow
Minimum number of active interfaces	1
Maximum number of active interfaces	8

9.1.4 Configuring manual link aggregation

Configure manual link aggregation for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#int eth-trunk <i>trunk-number</i>	Enter aggregation group configuration mode.
3	Raisecom(config-eth-trunk-*)#mode manual	Configure the working mode of the LAG to manual link aggregation.
4	Raisecom(config-eth-trunk-*)#active-linknumber { max min } { <1-8> default }	Configure the maximum or minimum number of active links in LACP LAG. By default, the maximum number is 8 while the minimum is 1.
5	Raisecom(config-eth-trunk-*)#add interface <i>interface-type interface-number</i>	Add the interface to the LAG.
6	Raisecom(config-eth-trunk-*)#exit	Enter global configuration mode.

9.1.5 Configuring static LACP link aggregation

Configure static LACP link aggregation for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#lacp system-priority <i>system-priority</i>	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	Raisecom(config)#int eth-trunk <i>trunk-number</i>	Enter aggregation group configuration mode.
4	Raisecom(config-eth-trunk-*)#mode lacp-static	Configure the working mode of the LAG to static LACP LAG.
5	Raisecom(config-eth-trunk-*)#lacp timeout { fast slow }	Configure the LACP timeout mode. By default, it is slow.

Step	Command	Description
6	<code>Raisecom(config-eth-trunk-*)#active-linknumber { max min } { <1-8> default }</code>	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-eth-trunk-*)#lACP preempt enable</code>	Enable priority preempt on the LAG.
8	<code>Raisecom(config-eth-trunk-*)#lACP preempt delay time</code>	Configure the WTR time on the interface.
9	<code>Raisecom(config-eth-trunk-*)#add interface interface-type interface-number</code>	Add the interface to the LAG.
10	<code>Raisecom(config-ge-1/1/*)#lACP priority priority</code>	Configure the interface LACP priority. The priority affects election for the default interface for LACP. The smaller the value is, the higher the priority is. By default, it is 32768.
11	<code>Raisecom(config-ge-1/1/*)#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 speed, interface highest LACP priority, and interface minimum ID. The interface is in active status by default, the interface with identical speed, identical peer and identical device operation key is also in active status; other interfaces are in standby status.

9.1.6 Configuring master/slave link aggregation

Configure master/slave link aggregation for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#int eth-trunk trunk-number</code>	Enter aggregation group configuration mode.
3	<code>Raisecom(config-eth-trunk-*)#mode { manual lACP-static } active-standby</code>	Configure the working mode of the LAG to manual master/slave link aggregation or static LACP master/slave link aggregation.

Step	Command	Description
4	Raisecom(config-eth-trunk-*) #add primary interface <i>interface-type interface-number</i>	Configure the master interface of the LAG.
5	Raisecom(config-eth-trunk-*) #add secondary interface <i>interface-type interface-number</i>	Configure the slave interface of the LAG.
6	Raisecom(config-eth-trunk-*) #revert enable Raisecom(config-eth-trunk-*) #wait-to-store <i>time</i>	Configure the revertive mode and WTR time of the LAG. By default, the mode is non-revertive.
7	Raisecom(config-eth-trunk-*) #exit	Return to global configuration mode.



Note

Before configuring the revertive mode of the LAG to non-revertive, use the **master-port** command to configure the master interface

9.1.7 Configuring the load balancing algorithm for the LAG

Configure the load balancing algorithm for the LAG for the device as below.

Step	Command	Description
1	Raisecom #configure	Enter global configuration mode.
2	Raisecom(config) #int eth-trunk <i>trunk-number</i>	Enter aggregation group configuration mode.
3	Raisecom(config-eth-trunk-*) #load-balance { src-mac dst-mac srcdst-mac src-ip dst-ip srcdst-ip default }	Configure the load balancing algorithm for the LAG globally. By default, the system adopts the src-dst-mac mode; in other words, the system chooses the forwarding interface according to the OR result of the source MAC address and destination MAC address.

9.1.8 Checking configurations

Use the following commands to check configuration results.

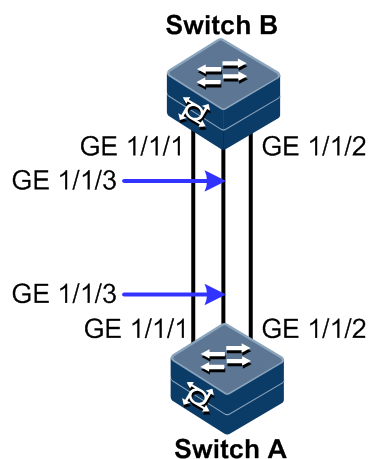
No.	Command	Description
1	Raisecom#show lacp eth-trunk trunk-number	Show the local system LACP interface status, flag, interface priority, administration key, operation key, and interface status machine status. The information about LACP neighbors include the tag, interface priority, device ID, Age, operation key value, interface ID, and interface status machine status.
2	Raisecom#show lacp statistics interface eth-trunk trunk-number	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.
3	Raisecom#show lacp information	Show the global LACP status of the local system, MAC addresses, and time of each timer.
4	Raisecom#show interface eth-trunk trunk-number	Show link aggregation status of the current system, load balancing mode of link aggregation, all LAG member interfaces, and active member interfaces.  Note The active member interface refers to the one whose interface status is Up.

9.1.9 Example for configuring static LACP link aggregation

Networking requirements

As shown in Figure 9-1, to improve link reliability between Switch A and Switch B, you can configure static LACP link aggregation. That is to add GE 1/1/1, GE 1/1/2, and GE 1/1/3 to one LAG.

Figure 9-1 Static LACP mode Link aggregation networking



Configuration steps

Step 1 Create static LACP link aggregation on Switch A. Configure Switch A as the active end.

```
Raisecom#hostname SwitchA
SwitchA#configure
SwitchA(config)#larp system-priority 1000
SwitchA(config)#int eth-trunk 1
SwitchA(config-eth-trunk-1)#mode larp-static
SwitchA(config-eth-trunk-1)#add interface ge 1/1/1
SwitchA(config-eth-trunk-1)#add interface ge 1/1/2
SwitchA(config-eth-trunk-1)#add interface ge 1/1/3
SwitchA(config-eth-trunk-1)#exit
```

Step 2 Configure static LACP LAG on Switch B.

```
Raisecom#hostname SwitchB
SwitchB#configure
SwitchB(config)#int eth-trunk 1
SwitchB(config-eth-trunk-1)#mode larp-static
SwitchB(config-eth-trunk-1)#add interface ge 1/1/1
SwitchB(config-eth-trunk-1)#add interface ge 1/1/2
SwitchB(config-eth-trunk-1)#add interface ge 1/1/3
SwitchB(config-eth-trunk-1)#exit
```

Checking results

Use the **show larp eth-trunk 1** command to show global configurations of the static LACP link aggregation on Switch A.

```
SwitchA#show larp eth-trunk 1
-----
-----
LACP Status           : master
System Priority        : 1000
System Mac Address     : f0:f1:f2:f3:01:01
Member ports number    : 3
Max Active ports number : 8
LACP timeout          : slow
Preempt state          : disable
Preempt delay          : 30(s)

ge-1/1/1 :
Port Status : Up and bind
Local information:
  Mode   Flags  PortPri  AdminKey  OperKey  PortId  State  Status
  active slow  32768    1         1      449    0x3d  selected
Partner information:
```

```

        SysPri  Flags  PortPri  AdminKey  OperKey  PortId  State  DeviceID
        32768   slow   32768    0         1        449   0x3d
0xf0f1f2f30201

ge-1/1/2 :
Port Status : Up and bind
Local information:
  Mode      Flags  PortPri  AdminKey  OperKey  PortId  State  Status
  active    slow   32768    1         1        450   0x3d   selected
Partner information:
  SysPri  Flags  PortPri  AdminKey  OperKey  PortId  State  DeviceID
  32768   slow   32768    0         1        450   0x3d
0xf0f1f2f30201

ge-1/1/3 :
Port Status : Up and bind
Local information:
  Mode      Flags  PortPri  AdminKey  OperKey  PortId  State  Status
  active    slow   32768    1         1        451   0x3d   selected
Partner information:
  SysPri  Flags  PortPri  AdminKey  OperKey  PortId  State  DeviceID
  32768   slow   32768    0         1        451   0x3d
0xf0f1f2f30201
-----
-----

```

9.2 G.8032

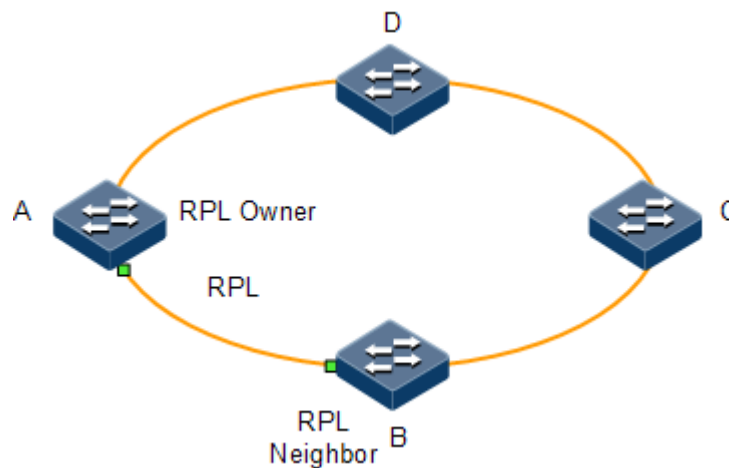
9.2.1 Introduction

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.

G.8032 concepts

Figure 9-2 G.8032 ring networking



The basic concepts of G.8032 Ethernet Ring Protection Switching as shown in Figure 9-2 include:

- RPL (Ring Protection Link): a link between RPL nodes. Under normal conditions, the nodes at both ends of the link are blocked to prevent loops on the ring. There can be only one RPL for each ring.
- RPL Owner: a node connected to the RPL. It is specified by the user to block or unblock the traffic at one end of the RPL. Under normal conditions, RPL Owners are responsible for blocking traffic on the RPL interface to prevent service loops.
- RPL Neighbor: a node connected to the other end of the RPL. It cooperates with the RPL Owner to complete protection switching.
- Protocol VLAN: an independent VLAN path adopted by the G.8032 for the delivery of R-APS packets.
- Block VLAN: different from the protocol VLAN which carries R-APS packets, it is a service VLAN used for the delivery of service information.
- R-APS messages: the fast-switching protocol packets in the G.8032 standard, including the following types:
 - FS (Forced Switch): message sent regularly by the FS node to implement forced switching.
 - SF (Signal Failed): message sent regularly by the fault node to report error information.
 - MS (Manual Switch): message sent regularly by the MS node for executing manual switching.
 - NR, RB (No Request Request Block): message sent regularly by RPL Owner to notify other nodes on the link when there are no faults or manual commands. When RPL is blocked by the RPL Owner, this message will be sent regularly.
 - NR (No Request): when faults or management commands are cleared, this message is sent

Four timers including Guard Timer, Wait To Restore (WTR) Timer, (Wait To Block) (WTB) Timer, and Holdoff Timer, will be used in the ring protection switching.

- Guard Timer: used for filtering invalid R-APS packets which may cause incorrect protection switching of nodes on the ring. Especially in a large ring network, the immediate restoration after the node failure may trigger a fault notification from the neighboring node. Then, the link will be Down again. If the notification is caused by this node, the problem can be solved by configuring ring Guard Timer.
- WTR Timer: when the working path is back to normal, the WTR Timer on the RPL Owner starts. When WTR Timer expires, the service is recovered to the working path. WTR Timer is used to avoid frequent switching caused by the instability of the working path.
- WTB Timer: it is used to delay RPL interface blocking when clearing manual commands in the revertive mode. In this way, the interface shock caused by re-blocking can be avoided.
- Holdoff Timer: when one or more faults are detected, initiate the Holdoff Timer if the configured value of Holdoff is not 0. The system will delay sending fault notification before the Holdoff Timer expires; namely, the ring protection switching is delayed for a period so that the frequent switching caused by the link shock can be avoided. When the Holdoff Timer expires, the link will be checked no matter whether the fault that triggers the start of this timer exists or not. If faults are detected, the notification will be sent to the protection switch.

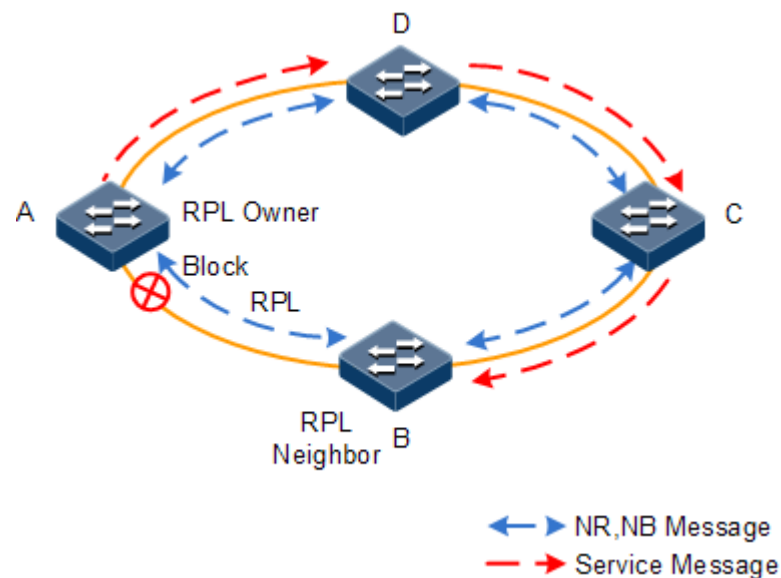
Ring states

G.8032 defines five node states on the ring network.

- Idle State: the normal working state without faults.
- Protecting State: a state when the link fault is detected. The automatic switching process is triggered by detection of the Operation, Administration and Maintenance (OAM) CCM.
- Pending State: a state before the faults are recovered.
- FS State: a state when issuing the forced switching command.
- MS State: a state when issuing the manual switching command

G.8032 Ethernet ring is in Idle state when there are no faults in the system or the faults are being corrected, as shown in Figure 9-3.

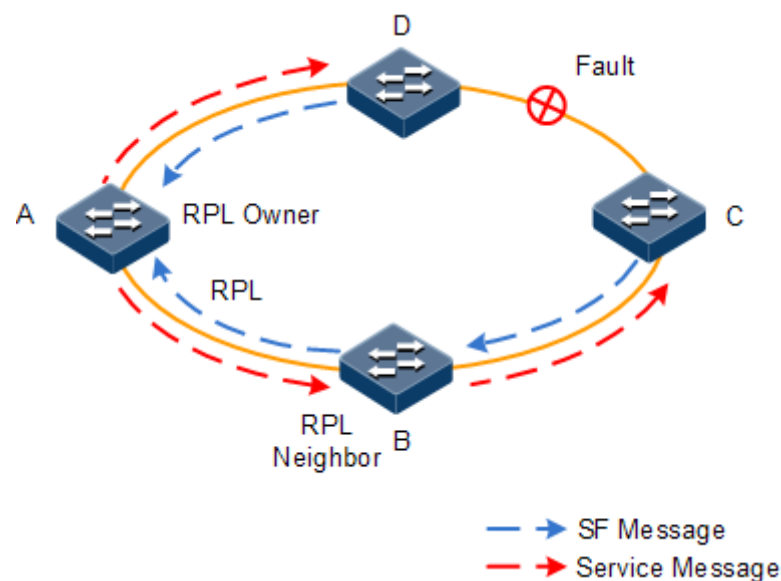
Figure 9-3 Idle state



As shown in Figure 9-3, the link in idle state has the following features.

- All the nodes are connected in a ring topology.
- G.8032 sends NR-RB messages constantly to show that no faults exist. It blocks RPL link to prevent loops within a ring.
- The neighboring nodes monitor each link by using CCM in the Ethernet OAM.
- G.8032 triggers ring protection switching through SF (Signal Faults) when the faults are detected on the ring.

Figure 9-4 Protecting state



As shown in Figure 9-4, the protection switching is initiated automatically when the faults are detected on the ring.

- When the Holdoff Timer expires, the nodes at both ends of the failed link are triggered by the RPL Owner to block this link, and send SF messages to other nodes on the ring to

report the fault. As shown in Figure 9-4, Node C and Node D send SF messages to other nodes when the link between them fails.

- Triggered by SF messages, the RPL Owner unblocks all the blocked interfaces and all the nodes start to clear FDB. Then the ring is in the protecting state.

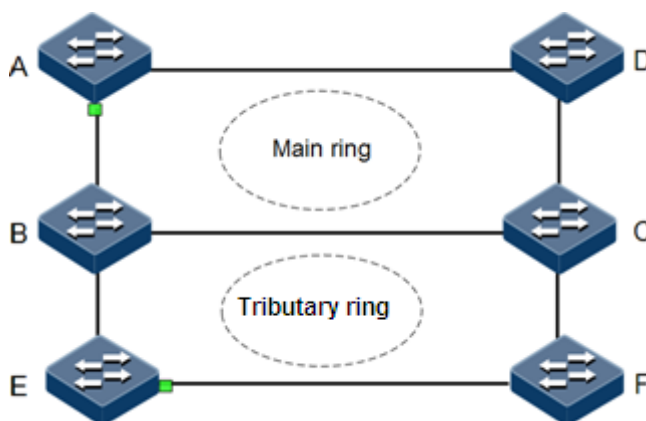
When the faults are recovered, the link is switched to faults recovery.

- The nodes at both ends of the failed link remain blocked. When the Guard Timer expires, Node C and Node D send R-APS NR messages to other nodes, indicating no local requests.
- The WTR Timer is started immediately when the RPL Owner receives the first NR message.
- When the WTR expires, RPL Owner blocks RPL and sends a R-APS (NR, RB) message. This means that no local request exists and RPL is blocked.
- After receiving the message, other nodes will refresh the MAC address and forward FDB. The node that sends NR messages stop sending packets periodically, and unblocks the blocked interfaces.
- All the nodes on the link are back to the idle state.

Tributary ring

The revised edition of G.8032 has added Ethernet multi-ring protection solutions. Through interconnected nodes (that connect multiple rings), the tributary ring is connected to other rings or networks as an affiliate to the existing ring network. The tributary ring is not closed and the interconnected nodes do not belong to the tributary ring.

Figure 9-5 Tributary ring



As shown in Figure 9-5, the path between the interconnected nodes B and C is called R-APS virtual path which is designed for the interconnected nodes in the interconnected topology. If the interconnected ring has a R-APS virtual path, the main ring will act as a virtual path, which means the APS messages of the tributary ring will be sent to the main ring. If not, the main ring will not provide a virtual path for the tributary ring, which means the messages will be terminated at the interconnected nodes. The main ring and the tributary ring act independently, with each of them setting its own RPL Owner. The protection of multiple rings is similar to that of the single ring, with each of them tackling the failures within each ring. When the shared link between interconnected nodes fails, the main ring is switched to the Protecting State while the tributary ring remains unchanged.

Because the data of a tributary ring is sent through the main ring, the MAC address table of the tributary ring will be stored on the device of the main ring. When a tributary ring fails, it notifies the main ring through the Propagate switch of the immediate need to update FDB to avoid traffic loss.

Ring mode

The difference between the revertive mode and the non-revertive mode is as below:

- Revertive mode: when WTR Timer expires, the traffic is forwarded over the link of previous state (the one before the failure).
- Non-revertive mode: when WTR Timer expires, the traffic is not forwarded over the link of previous state (the one before the failure). By default, the protection ring is configured to this mode.

The virtual path of a tributary ring is as below:

- With mode: the tributary ring supports R-APS virtual path. The main ring provides a channel for APS messages of the tributary ring. The APS messages are received by the interconnected nodes in the tributary ring and sent to the main ring. The communication between interconnected nodes in the tributary ring is implemented through the main ring.
- Without mode: the tributary ring does not support R-APS virtual path. The APS messages of the tributary ring are terminated at the interconnected nodes and will not be sent to the main ring. In this mode, the tributary ring cannot block the tributary protocol VLAN so that packets of the tributary ring can pass the owner.

9.2.2 Preparing for configurations

Scenario

With the development of Ethernet to Telecom-grade network, voice and video multicast services have higher requirements on Ethernet redundant protection and fault-recovery time. The existing STP has a second-level fault clearance time, which is far from meeting reliability requirement. 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 device supports the single ring, intersecting ring, and tangent ring.

G.8032 provides a mode for detecting faults based on physical interface. The device 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.

9.2.3 Default configurations of G.8032

Default configurations of G.8032 are as below.

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

9.2.4 Creating a G.8032 ring

Configure the G.8032 ring for the device 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 9.2.5 Creating a G.8032 tributary ring.
- The ERPS ring interface must work in switch mode.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#g8032	Enter the G.8032 node.
3	Raisecom(config-g8032)#g8032 instance <i>instance-id</i> control-vlan <i>vlan-id</i>	Create an instance, and specified the controlling VLAN. If the revertive disable parameter is configured, the protection ring becomes the non-revertive mode. When the working link is recovered in revertive mode, traffic is switched back to the working link from the protection link, while the traffic will not be switched in non-revertive mode. By default, the protection link is in revertive mode.

Step	Command	Description
4	Raisecom(config-g8032)#g8032 instance <i>instance-id</i> vlan <i>vlan-id</i>	Specify the data VLAN.
5	Raisecom(config-g8032)#g8032 instance <i>instance-id</i> rpl { port1 port2 none }	Configure the RPL interface.
6	Raisecom(config-g8032)#g8032 instance <i>instance-id</i> role { rpl-owner-node neighbor none }	Configure the role.
7	Raisecom(config-g8032)#g8032 instance <i>instance-id</i> port1 <i>interface-type interface-</i> <i>number</i>	Configure interface 1.
8	Raisecom(config-g8032)#g8032 instance <i>instance-id</i> port2 <i>interface-type interface-</i> <i>number</i>	Configure interface 2.
9	Raisecom(config)#g8032 instance <i>instance-id</i> version { v1 v2 }	Configure the protocol version. The protocol version of all nodes on a protection ring should be identical. In protocol version 1, protection rings are distinguished based on the protocol VLAN. Therefore, you need to configure different protocol VLANs for protection rings. We recommend configuring different protocol VLANs for protection rings even if protocol version 2 is used.
10	Raisecom(config)#g8032 instance <i>instance-id</i> guard- timer <i>guard-time</i>	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.
11	Raisecom(config)#g8032 instance <i>instance-id</i> wtr- timer <i>wtr-time</i>	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.

Step	Command	Description
12	<code>Raisecom(config)#g8032 instance <i>instance-id</i> holdoff- timer <i>holdoff-time</i></code>	Configure the ring Hold-off timer. After the Hold-off timer is configured, the system will delay processing the fault when the working line fails. In other words traffic is delayed to be switched to the protection line. This helps prevent frequent switching caused by working line vibration.  Note If the ring Hold-off timer value is too great, it may influence 50ms switching performance. Therefore, we recommend configuring the ring Hold-off timer value to 0.

9.2.5 Creating a 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 9.2.4 Creating a 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 instance ID of the tributary ring must be greater than that of that main ring.
- Configurations of non-intersecting nodes of the intersecting ring are identical to those of the single/tangent ring. For details, see section 9.2.4 Creating a G.8032 ring.
- The ERPS ring interface must work in switch mode.

Configure the G.8032 tributary ring for device as below.

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

Step	Command	Description
2	<pre>Raisecom(config)#ethernet ring-protection <i>ring-id</i> { east west } { <i>interface-type</i> <i>interface-number</i> port- channel <i>port-channel-</i> <i>number</i> } node-type rpl- owner [not-revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-</i> <i>list</i>]</pre>	Create an instance, and specified the controlling VLAN. If the revertive disable parameter is configured, the protection ring becomes the non-revertive mode. If the not-revertive parameter is used, the protection ring changes to non-revertive mode. When the working link is recovered in revertive mode, traffic is switched back to the working link from the protection link, while the traffic will not be switched in non-revertive mode. By default, the protection link is in revertive mode.  Note The link between the two intersecting nodes belongs to the main ring, so you can configure only one of interface 1 and interface 2 when configuring the tributary ring.
3	<pre>Raisecom(config- g8032)#g8032 instance <i>instance-id</i> vlan <i>vlan-id</i></pre>	Specify the data VLAN.
4	<pre>Raisecom(config- g8032)#g8032 instance <i>instance-id</i> virtual- channel <i>vlan-id</i></pre>	Specify the virtual channel VLAN.
5	<pre>Raisecom(config- g8032)#g8032 instance <i>instance-id</i> rpl { port1 port2 none }</pre>	Configure the RPL interface.
6	<pre>Raisecom(config- g8032)#g8032 instance <i>instance-id</i> role { rpl- owner-node neighbor none }</pre>	Configure the role.
7	<pre>Raisecom(config- g8032)#g8032 instance <i>instance-id</i> port1 <i>interface-type</i> <i>interface-</i> <i>number</i></pre>	Configure interface 1. If this configuration occurs on the intersecting node, interface 1 and interface 2 cannot be concurrently configured.
8	<pre>Raisecom(config- g8032)#g8032 instance <i>instance-id</i> port1 <i>interface-type</i> <i>interface-</i> <i>number</i></pre>	Configure interface 2. If this configuration occurs on the intersecting node, interface 1 and interface 2 cannot be concurrently configured.

9.2.6 Configuring G.8032 switching control

Configure G.8032 switching control for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config-g8032)#g8032 instance instance-id { port1 port2 } force-switch	Switch the traffic on the protection ring to interface 1 or 2 forcedly. FS can be configured on multiple interfaces of multiple ring nodes.
3	Raisecom(config-g8032)#g8032 instance instance-id { port1 port2 } manual-switch	Switch the traffic on the protection ring to the interface 1 or 2 manually. Its priority is lower than the one of FS and APS. MS can be configured on one interface of a ring node.



Note

By default, traffic is automatically switched to the other line when the current line fails to forward traffic.

9.2.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show g8032 interface	Show the interface status of the G.8032 ring.
2	Raisecom#show g8032 instance	Show the status of the G.8032 ring.

9.2.8 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)#g8032 instance instance-id clear	Clear the effect of the ring protection control command (force-switch, manual-switch, WTR timer timeout, and WTB timer timeout).

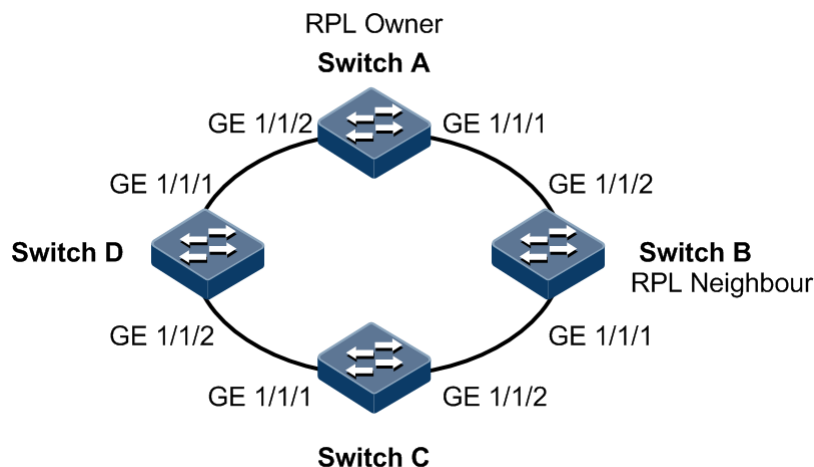
9.2.9 Example for configuring single ring G.8032

Networking requirements

As show in Figure 9-6, to improve Ethernet reliability, Switch A, Switch B, Switch C, and Switch D build up a G.8032 single ring.

- Switch A is the RPL Owner; Switch B is the RPL Neighbor; the RPL link between Switch A and Switch B is blocked.
- The ID of protocol VLAN is 1 and the blocked VLANs range from 2 to 10.

Figure 9-6 Single ring G.8032 networking



Configuration steps

Step 1 Add interfaces to VLANs 2–10.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#configure
SwitchA(config)#interface ge 1/1/1 to ge 1/1/2
SwitchA(config-ge-1/1/1->ge-1/1/2)#port link-type trunk
SwitchA(config-ge-1/1/1->ge-1/1/2)#port trunk allow-pass vlan 2-10
SwitchA(config-ge-1/1/1->ge-1/1/2)#exit
```

Configurations of Switch B, Switch C, and Switch D are the same as those of Switch A.

Step 2 Create ERPS protection ring.

Configure Switch A.

```
SwitchA(config)#g8032
SwitchA(config-g8032)#g8032 instance 1 control-vlan 1
SwitchA(config-g8032)#g8032 instance 1 vlan 2-10
```

```
SwitchA(config-g8032)#g8032 instance 1 rpl port1
SwitchA(config-g8032)#g8032 instance 1 role rpl-owner-node
SwitchA(config-g8032)#g8032 instance 1 port1 ge 1/1/1
SwitchA(config-g8032)#g8032 instance 1 port2 ge 1/1/2
```

Configure Switch B.

```
SwitchB(config)#g8032
SwitchB(config-g8032)#g8032 instance 1 control-vlan 1
SwitchB(config-g8032)#g8032 instance 1 vlan 2-10
SwitchB(config-g8032)#g8032 instance 1 rpl port1
SwitchB(config-g8032)#g8032 instance 1 role neighbor
SwitchB(config-g8032)#g8032 instance 1 port1 ge 1/1/2
SwitchB(config-g8032)#g8032 instance 1 port2 ge 1/1/1
```

Configure Switch C.

```
SwitchC(config)#g8032
SwitchC(config-g8032)#g8032 instance 1 control-vlan 1
SwitchC(config-g8032)#g8032 instance 1 vlan 2-10
SwitchC(config-g8032)#g8032 instance 1 port1 ge 1/1/2
SwitchC(config-g8032)#g8032 instance 1 port2 ge 1/1/1
```

Configure Switch D.

```
SwitchD(config)#g8032
SwitchD(config-g8032)#g8032 instance 1 control-vlan 1
SwitchD(config-g8032)#g8032 instance 1 vlan 2-10
SwitchD(config-g8032)#g8032 instance 1 port1 ge 1/1/2
SwitchD(config-g8032)#g8032 instance 1 port2 ge 1/1/1
```

Checking results

Use the **show g8032 interface** command to show configurations of the G.8032 protection ring on the switch.

Take Switch A for example. RPL link is blocked to avoid loops. After the WTR timer expires, information about ring status is as below.

```
SwitchA#show g8032 interface
```

	Instance	Interface	Role	Type	Operate	Forward	Rx-
Count	Tx-Count						

```

-----
1          ge 1/1/1      port1  rpl    working  blocking  0      15
1          ge 1/1/2      port2  normal working  forwarding 0:::
11
-----
-----

```

Manually disconnect the link between Switch B and Switch C to emulate a fault. Use the following command to show G.8032 protection ring status on Switch A again. The RPL link switches to the forwarding status.

```

SwitchA#show g8032 interface
          :::Instance Interface      Role   Type   Operate  Forward
Rx-Count Tx-Count
-----
1          ge 1/1/1      port1  rpl    working  forwarding 16      41
1          ge 1/1/2      port2  normal failed   blocking  18      42
-----
-----

```

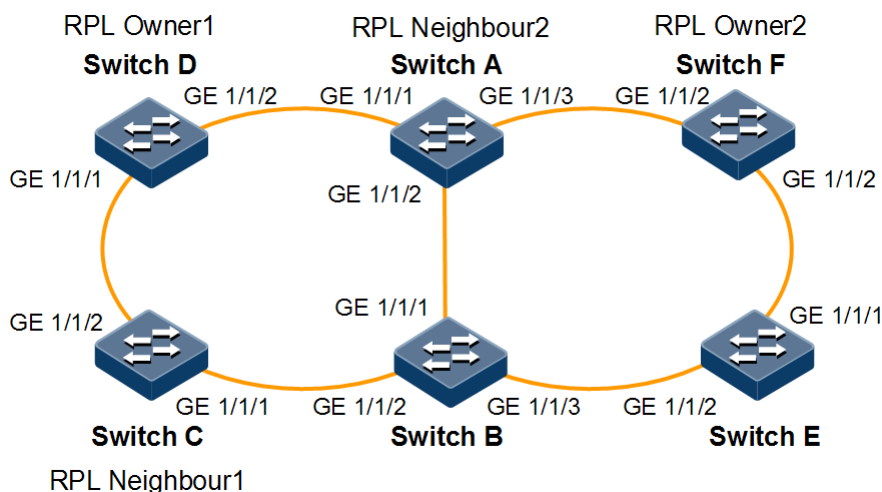
9.2.10 Example for configuring intersecting G.8032

Networking requirements

As shown in Figure 9-7, to improve Ethernet reliability, Switch A, Switch B, Switch C, Switch D, Switch E, and Switch F form an intersecting ERPS network.

- Switch A, Switch B, Switch C, and Switch D form the main ring. Switch D is the main ring RPL Owner, Switch C is main ring RPL Neighbor. The blocked interface is Gigaethernet 1/1/1 on Switch D. The ID of the protocol VLAN is 1.
- Switch A, Switch B, Switch E, and Switch F form a tributary ring. Switch F is the tributary ring RPL Owner. Switch A is tributary ring RPL Neighbor. The blocked interface is Gigaethernet 1/3/1 on Switch F. The protocol VLAN is 4094.
- The blocked VLANs for the main ring and tributary ring range from VLANs 1 to 4094 by default.

Figure 9-7 Intersecting ring G.8032 networking



Configuration steps

Step 1 Create a 4094 and add interfaces to the VLAN.

Configure Switches A and B.

```
Switch#configure
Switch(config)#vlan 1-4094
Switch(config)#interface ge 1/1/1 to ge 1/1/3
Switch(config- ge-1/1/1->ge-1/1/3)#port link-type trunk
Switch(config-ge-1/1/1->ge-1/1/3)#port trunk allow-pass vlan all
Switch(config-ge-1/1/1->ge-1/1/3)#exit
```

Configure Switches C, D, E, and F.

```
Switch#configure
Switch(config)#vlan 1-4094
Switch(config)#interface ge 1/1/1 to ge 1/1/2
Switch(config-ge-1/1/1->ge-1/1/2)#port link-type trunk
Switch(config-ge-1/1/1->ge-1/1/2)#port trunk allow-pass vlan all
Switch(config-ge-1/1/1->ge-1/1/2)#exit
```

Step 2 Create a main ring for G.8032 protection ring.

Configure Switches A and B.

```
Switch(config)#g8032
Switch(config-g8032)#g8032 instance 1 control-vlan 1
Switch(config-g8032)#g8032 instance 1 vlan 1-4094
Switch(config-g8032)#g8032 instance 1 port1 ge 1/1/1
Switch(config-g8032)#g8032 instance 1 port2 ge 1/1/2
```

Configure Switch C.

```
Switch(config)#g8032
Switch(config-g8032)#g8032 instance 1 control-vlan 1
Switch(config-g8032)#g8032 instance 1 vlan 1-4094
Switch(config-g8032)#g8032 instance 1 rpl port2
Switch(config-g8032)#g8032 instance 1 role neighbour
Switch(config-g8032)#g8032 instance 1 port1 ge 1/1/1
Switch(config-g8032)#g8032 instance 1 port2 ge 1/1/2
```

Configure Switch D.

```
Switch(config)#g8032
Switch(config-g8032)#g8032 instance 1 control-vlan 1
Switch(config-g8032)#g8032 instance 1 vlan 1-4094
Switch(config-g8032)#g8032 instance 1 rpl port1
Switch(config-g8032)#g8032 instance 1 role rpl-onwer-node
Switch(config-g8032)#g8032 instance 1 port1 ge 1/1/1
Switch(config-g8032)#g8032 instance 1 port2 ge 1/1/2
```

Step 3 Configure a tributary ring for G.8032.

Configure Switch A.

```
Switch(config)#g8032
Switch(config-g8032)#g8032 instance 2 control-vlan 4094
Switch(config-g8032)#g8032 instance 2 vlan 1-4094
Switch(config-g8032)#g8032 instance 2 rpl port1
Switch(config-g8032)#g8032 instance 2 role rpl-onwer-node
Switch(config-g8032)#g8032 instance 2 port1 ge 1/1/3
Switch(config-g8032)#g8032 instance 2 virtual-channel 3
```

Configure Switch B.

```
Switch(config)#g8032
Switch(config-g8032)#g8032 instance 2 control-vlan 4094
Switch(config-g8032)#g8032 instance 2 vlan 1-4094
Switch(config-g8032)#g8032 instance 2 port1 ge 1/1/3
Switch(config-g8032)#g8032 instance 2 virtual-channel 3
```

Configure Switch E.

```
Switch(config)#g8032
Switch(config-g8032)#g8032 instance 2 control-vlan 4094
Switch(config-g8032)#g8032 instance 2 vlan 1-4094
Switch(config-g8032)#g8032 instance 2 port1 ge 1/1/1
Switch(config-g8032)#g8032 instance 2 port2 ge 1/1/2
```

Configure Switch F.

```
Switch(config)#g8032
Switch(config-g8032)#g8032 instance 2 control-vlan 4094
Switch(config-g8032)#g8032 instance 2 vlan 1-4094
Switch(config-g8032)#g8032 instance 2 rpl port1
Switch(config-g8032)#g8032 instance 2 role rpl-onwer-node
Switch(config-g8032)#g8032 instance 2 port1 ge 1/1/1
Switch(config-g8032)#g8032 instance 2 port2 ge 1/1/2
```

Checking results

Use the **show g8032 interface** command to show configurations of the G.8032 protection ring on the switch.

Use the command on Switch A, Switch D, and Switch F respectively. The result should be as below after the WTR timer expires.

SwitchD#**show g8032 interface**

Count	Tx-Count	Instance	Interface	Role	Type	Operate	Forward	Rx-
1			ge 1/1/1	port1	rpl	working	blocking	0 :::
15								
		1	ge 1/1/2	port2	normal	working	forwarding	
0 :::				11				

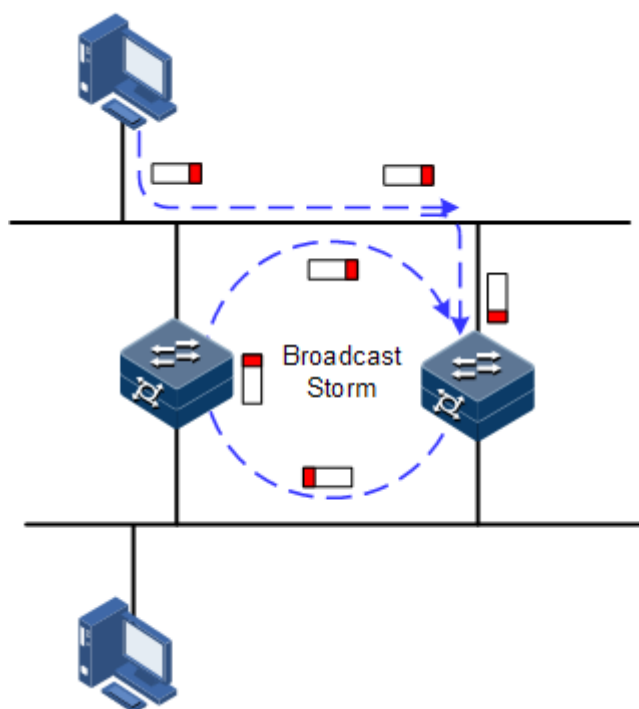
9.3 STP/RSTP

9.3.1 Introduction

STP

With the increasing complexity of network structure and growing number of switches on the network, the Ethernet network loops become the most prominent problem. Because of the packet broadcast mechanism, a loop causes the network to generate storms, exhaust network resources, and have serious impact to forwarding normal data. The network storm caused by the loop is shown in Figure 9-8.

Figure 9-8 Network storm due to loopback

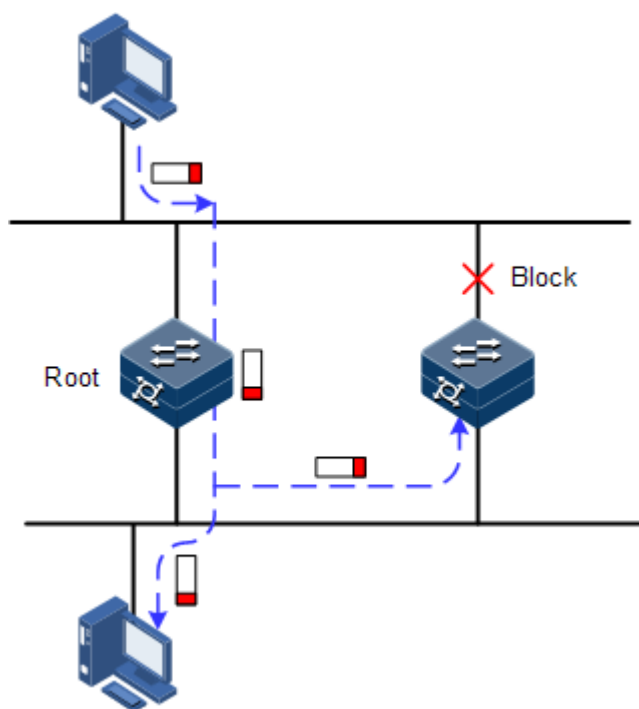


Spanning Tree Protocol (STP) is compliant to IEEE 802.1d standard and used to remove data physical loop in data link layer in the LAN.

The device 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 device logically according to the selection results, and finally trims the loop network structure to tree network structure without loop which takes a device 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 9-9 shows loop networking with STP.

Figure 9-9 Loop networking with STP



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

The major disadvantage of STP is the slow convergence speed.

RSTP

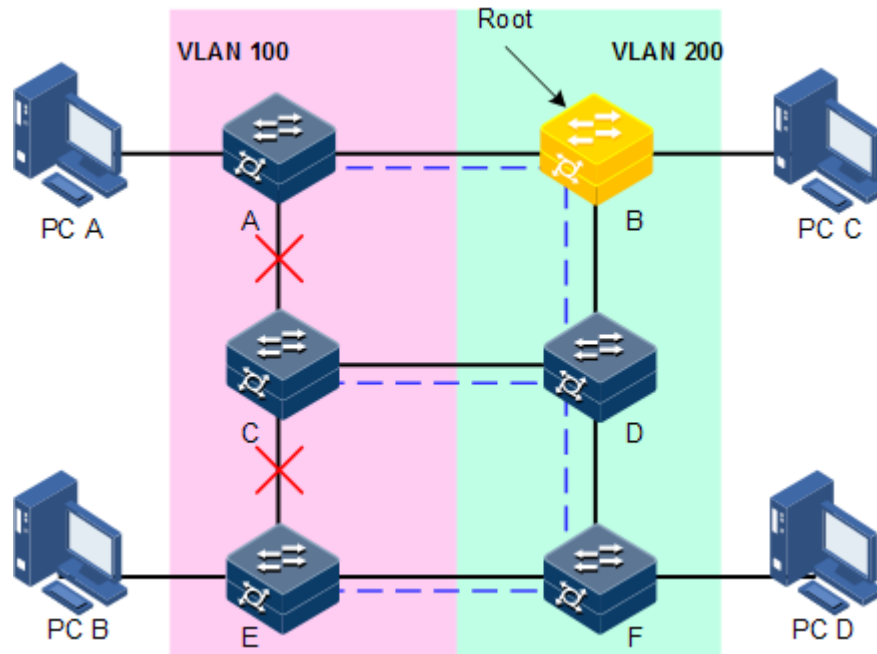
For improving the slow convergent speed of STP, IEEE 802.1w establishes Rapid Spanning Tree Protocol (RSTP), which increases the mechanism to change interface blocking state to forwarding state, speed up the topology convergence rate.

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

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

- The whole switching network has only one spanning tree, which will lead to longer convergence time on a larger network.
- After a link is blocked, it does not carry traffic any more, causing waste of bandwidth.
- Packet of partial VLAN cannot be forwarded when network structure is unsymmetrical. As shown in Figure 9-10, 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 9-10 Failure in forwarding VLAN packets due to RSTP



9.3.2 Preparation for configuration

Networking situation

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

Preconditions

N/A

9.3.3 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

9.3.4 Enabling STP

Enable STP for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#stp mode { stp rstp mstp default }	Configure spanning tree mode.
3	Raisecom(config)#interface <i>interface-type interface-</i> <i>number</i>	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
4	Raisecom(config-ge- 1/1/*)#stp enable	Enable interface STP.

9.3.5 Configuring STP parameters

Configure STP parameters for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#stp priority <i>priority-value</i>	Configure device priorities.
3	Raisecom(config)#interface <i>interface-</i> <i>type interface-number</i> Raisecom(config-ge-1/1/*)#stp priority <i>priority-value</i>	Configure interface priorities on the device.
4	Raisecom(config-ge-1/1/*)#stp path- cost <i>cost-value</i>	Configure the path cost of the interface on the device.
5	Raisecom(config)#stp hello-time <i>value</i>	Configure the value of Hello Time.
6	Raisecom(config)#stp forward-delay <i>value</i>	Configure forward delay.
7	Raisecom(config)#stp max-age <i>value</i>	Configure the maximum age.
8	Raisecom(config)#stp pathcost-standard { dot1d-1998 dot1t }	Configure the standard for calculating path cost of the panning tree.

9.3.6 Configuring the 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 quick to change to forward status.

The real port will change to false edge interface after receiving BPDU when it is in force-true mode; when the interface is in enable mode, whether it is true or false edge interface in real operation, it will maintain the disable mode until the configuration is changed.

By default, all interfaces on the device are configured to disable.

Configure the edge interface for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-ge- 1/1/*)#stp edge-port { enable disable }	Configure attributes of the RSTP edge interface.

9.3.7 Configuring the RSTP link type

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

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

Configure the link type for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-ge- 1/1/*)#stp point-to-point { force-true force-false auto }	Configure the link type for interface.

9.3.8 Checking configurations

Use the following commands to check configuration results.

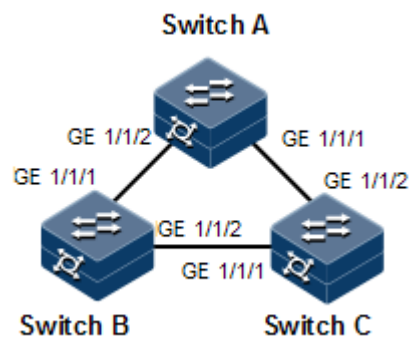
No.	Command	Description
1	Raisecom#show stp information	Show basic configurations of STP.
2	Raisecom#show stp interface	Show configurations of the spanning tree on the interface.
3	Raisecom#show stp bridge	Show information about the root bridge of STP.

9.3.9 Example for configuring STP

Networking requirements

As shown in Figure 9-11, 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 9-11 STP networking



Configuration steps

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

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#configure
SwitchA(config)#stp mode stp
```

Configure Switch B.

```
Raisecom#hostname SwitchB
```

```
SwitchB#configure
SwitchB(config)#stp mode stp
```

Configure Switch C.

```
Raisecom#hostname SwitchC
SwitchC#configure
SwitchC(config)#stp mode stp
```

Step 2 Configure interface modes on three switches.

Configure Switch A.

```
SwitchA(config)#interface ge 1/1/1
SwitchA(config-ge-1/1/1)#port link-type trunk
SwitchA(config-ge-1/1/1)#stp enable
SwitchA(config-ge-1/1/1)#exit
SwitchA(config)#interface ge 1/1/2
SwitchA(config-ge-1/1/2)#port link-type trunk
SwitchA(config-ge-1/1/2)#stp enable
SwitchA(config-ge-1/1/2)#exit
```

Configure Switch B.

```
SwitchB(config)#interface ge 1/1/1
SwitchB(config-ge-1/1/1)#port link-type trunk
SwitchB(config-ge-1/1/1)#stp enable
SwitchB(config-ge-1/1/1)#exit
SwitchB(config)#interface ge 1/1/2
SwitchB(config-ge-1/1/2)#port link-type trunk
SwitchB(config-ge-1/1/2)#stp enable
SwitchB(config-ge-1/1/2)#exit
```

Configure Switch C.

```
SwitchC(config)#interface ge 1/1/1
SwitchC(config-ge-1/1/1)#port link-type trunk
SwitchC(config-ge-1/1/1)#stp enable
SwitchC(config-ge-1/1/1)#exit
SwitchC(config)#interface ge 1/1/2
SwitchC(config-ge-1/1/2)#port link-type trunk
SwitchC(config-ge-1/1/2)#stp enable
SwitchC(config-ge-1/1/2)#exit
```

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

Configure Switch A.

```
SwitchA(config)#stp priority 0
SwitchA(config)#interface ge 1/1/2
SwitchA(config-ge-1/1/2)#stp path-cost 10
```

Configure Switch B.

```
SwitchB(config)#interface ge 1/1/1
SwitchB(config-ge-1/1/1)#stp path-cost 10
```

Checking results

Use the **show stp** command to show bridge status.

Take Switch A for example.

```
SwitchA#show stp information
```

```
-----
Mode                               : stp
Trap state                         : disable
Bridge type                        : customer
BPDU Guard state                   : disable
TC protection state                 : disable
TC protection threshold             : 2
Hello time                         : 2
Max age                            : 20
Forward delay                      : 15
Max hops                           : 20
Time factor                        : 6
Format selector                    : 0
Revision level                     : 0
Config name                        : region
TC flush arp state                  : disable
Migration time                     : 3
Pathcost standard                   : dot1t
TC holdoff time                     : 10
Transmit limit                      : 6 (packets/s)
Link detection state                : enable
                                     Edge
default state                       : disable
-----
```

Use the **show stp interface** command to show the interface status.

Take Switch A for example.

SwitchA#**show stp interface**

MSTID	Port	Role	State	Protection	Region

0	ge-1/1/1				designated
forward	--	different			
			0	ge-1/1/2	designated
forward	--	different			

9.4 MSTP

9.4.1 Introduction

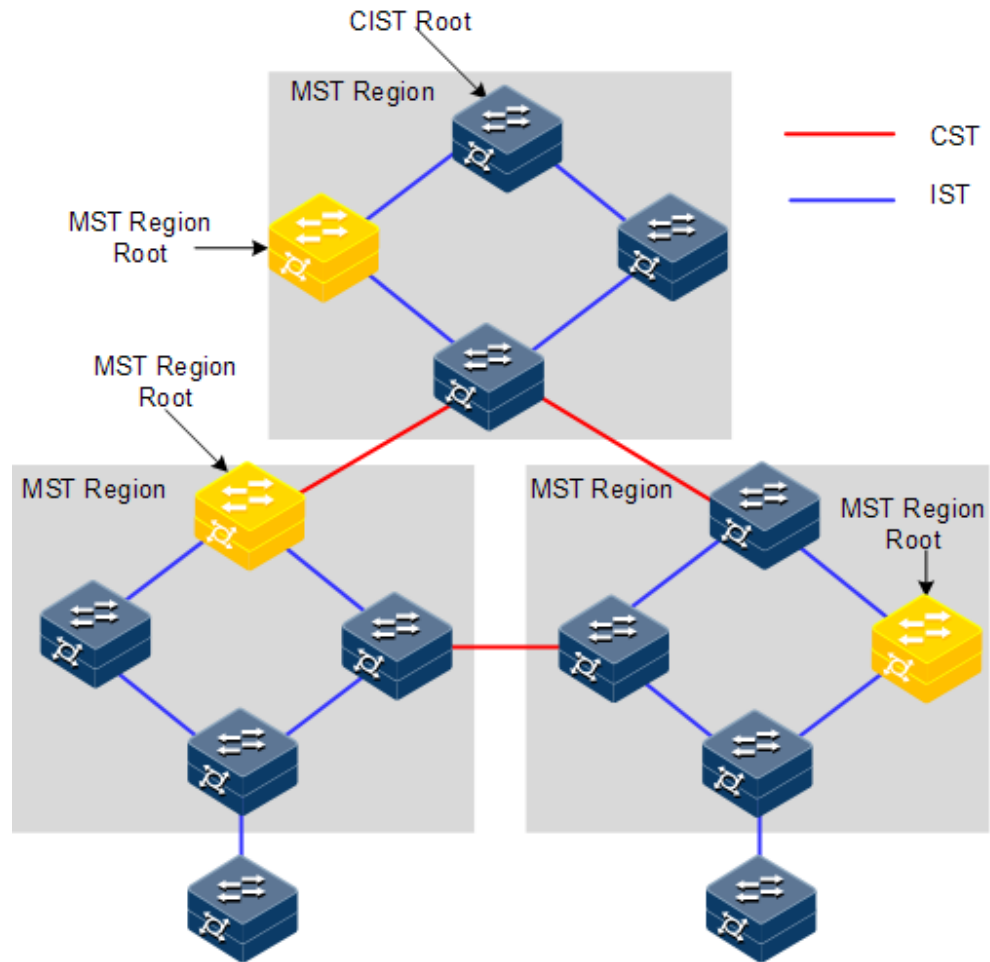
Multiple Spanning Tree Protocol (MSTP) is defined by IEEE 802.1s. Recovering the disadvantages of STP and RSTP, the MSTP implements fast convergence and distributes different VLAN flow following its own path to provide an excellent load balancing mechanism.

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

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

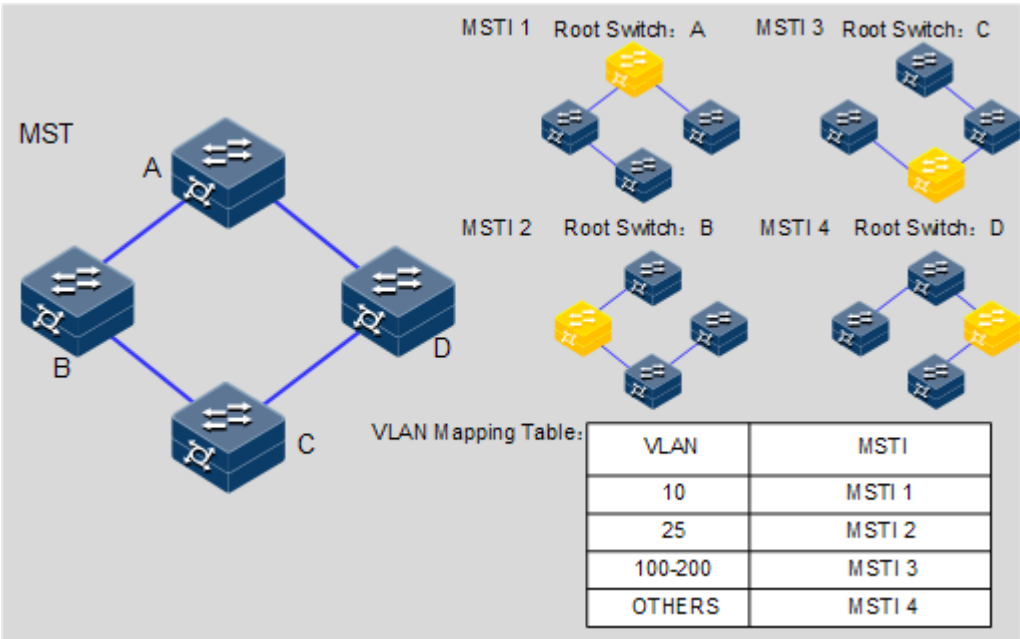
Compared with STP and RSTP, MSTP also introduces total root (CIST Root) and region root (MST Region Root) concepts. The total root is a global concept; all switches running STP/RSTP/MSTP can have only one total root, which is the CIST Root. The region root is a local concept, which is relative to an instance in a region. As shown in Figure 9-12, all connected devices only have one total root, and the number of region root contained in each region is associated with the number of instances.

Figure 9-12 Basic concepts of the MSTI network



There can be different MST instance in each MST region, which associates VLAN and MSTI by configuring the VLAN mapping table (relationship table of VLAN and MSTI). The concept sketch map of MSTI is shown in Figure 9-13.

Figure 9-13 MSTI concepts

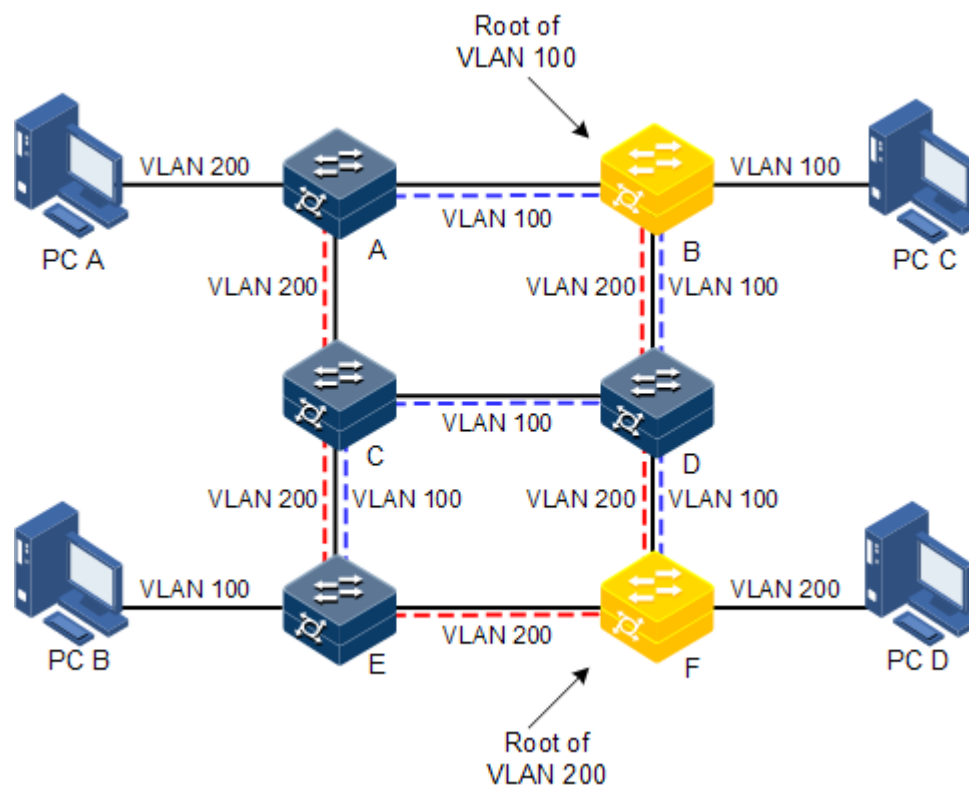


Note

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

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

Figure 9-14 Networking with multiple spanning trees instances in MST region



Apply MSTP to the network as shown in Figure 9-14. 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.

9.4.2 Preparation for configuration

Scenario

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

Prerequisite

N/A

9.4.3 Default configurations of MSTP

Default configurations of MSTP are as below.

Function	Default value
Global MSTP status	Disable
Interface MSTP status	Enable
Maximum number of hops in the MST region	20
MSTP priority of the device	32768
MSTP priority of the interface	128
Path cost of the interface	0
Maximum number of packets sent within each Hello time	3
Max Age timer	20s
Hello Time timer	2s
Forward Delay timer	15s
Revision level of the MST region	0
TC protection	Disable
TC protection threshold	1

9.4.4 Enabling MSTP

Enable MSTP for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#stp mode mstp	Configure the spanning tree mode to MSTP.
3	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical interface configuration mode or aggregation group configuration mode. Take physical interface configuration mode for example.
4	Raisecom(config-ge-1/1/*)#stp enable	Enable interface STP.

9.4.5 Configuring the MST region and its maximum number of hops

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

The MST region scale is restricted by the maximum number of hops. Starting from the root bridge of spanning tree in the region, the number of forwarding hops decreases by 1 when the configuration message (BPDU) passes a device; the device discards the configuration

message whose number of hops is 0. The device exceeding the maximum number of hops cannot join spanning tree calculation, so the MST region scale is restricted.

Configure the MSTP region and its maximum number of hops for the device as below.

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



Note

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

9.4.6 Configuring the root/backup bridge

Two methods for MSTP root selection are as below:

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

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



Note

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

Configure the root bridge or backup bridge for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#spanning-tree [instance instance-id] root { primary secondary }	Configure the device as the root bridge or backup bridge of a STP instance.



Note

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

9.4.7 Configuring the interface priority and system priority

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

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

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

Configure the interface priority and system priority for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-ge-1/1/*)#stp [instance <i>instance-id</i>] priority <i>priority-value</i> Raisecom(config-ge-1/1/*)#exit	Configure the interface priority for a STP instance.
4	Raisecom(config)#stp [instance <i>instance-id</i>] priority <i>priority-value</i>	Configure the 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.

9.4.8 Configuring the path cost of the interface

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

By default, the 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 device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-ge-1/1/*)#stp [instance <i>instance-id</i>] path- cost <i>cost-value</i>	Configure the path cost of the interface.

9.4.9 Configuring the 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 the maximum transmission rate on the interface for the device as below.

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

9.4.10 Configuring the MSTP timer

- Hello Time: the interval for the device to send BPDUs. It is used to detect whether a link fails on the device. The device sends Hello packets to other devices around in the Hello time to check if there is fault in the link. The default value is 2s. You can adjust the

interval value according to network conditions. Reduce the interval when network link changes frequently to enhance the stability of STP. However, increasing the interval reduces CPU utilization rate for STP.

- **Forward Delay:** the time parameter to ensure the safe transit of device status. Link fault causes the network to recalculate spanning tree, but the new configuration message recalculated cannot be transmitted to the whole network immediately. There may be temporary loop if the new root interface and designated interface start transmitting data at once. This protocol adopts status remove system: before the root interface and designated interface starts forwarding data, it needs a medium status (learning status); after delay for the interval of Forward Delay, it enters forwarding status. The delay guarantees the new configuration message to be transmitted through whole network. You can adjust the delay according to actual condition; in other words, reduce it when network topology changes infrequently and increase it under opposite conditions.
- **Max Age:** the bridge configurations used by STP have a life time that is used to judge whether the configurations are outdated. The device 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 device as below.

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

9.4.11 Configuring the edge interface

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

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

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

By default, all interfaces on the device are configured in auto-detection attribute.

Configure the edge interface for the device as below.

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

Step	Command	Description
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical interface configuration mode or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-ge-1/1/*)#stp edge-port { enable disable }	Configure attributes of the edge interface.

9.4.12 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 device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical interface configuration mode or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-ge-1/1/*)#stp bpdu-filter enable { enable disable }	Configure BPDU filtering on the edge interface.

9.4.13 Configuring BPDU Guard

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

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

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

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

Configure BPDU Guard for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#stp bpdu-protection enable	Enable BPDU Guard.

Step	Command	Description
3	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter physical interface configuration mode or aggregation group configuration mode. Take physical interface configuration mode for example.
4	<code>Raisecom(config-ge-1/1/*)#stp bpdu-protection error-down recovery-interval interval</code>	Configure the recovery interval of 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.

9.4.14 Configuring STP/RSTP/MSTP mode switching

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

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

Configure the STP/RSTP/MSTP mode switching for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#stp mode { stp rstp mstp }</code>	Configure the spanning tree mode.
3	<code>Raisecom(config-ge-1/1/*)#stp mcheck</code>	(Optional) forcibly configure the interface to MSTP mode.

9.4.15 Configuring the link type

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

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

Configure the link type for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-ge-1/1/*)#stp point-to-point { force-true force-false auto }	Configure the link type of the interface.

9.4.16 Configuring root interface isolation

The bridge will re-elect a root interface when it receives a packet with higher priority, which influences network connectivity and also consumes CPU resource. For the MSTP network, if someone sends BPDUs with higher priority, the network may become unstable due to continuous election.

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

Configure root interface isolation for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-ge-1 /1/*)#stp root-guard enable	Enable/Disable root interface isolation.

9.4.17 Configuring interface loopguard

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

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

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



Note

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

Configure interface loop protection for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-ge-1/1/*)#stp loop-guard enable	Configure interface loopguard attributes.

9.4.18 Configuring TC packet suppression

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

Configure TC packet suppression for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-ge-1/1/*)#stp tc-restriction enable	Configure TC packet suppression.

9.4.19 Configuring TC protection

TC protection prevents BPDU attacks related to topology change, thus enhancing security of the device and network.

- After TC protection is enabled, the device receives TC packets of which the number is within the threshold in the Hello Time of STP, and discards TC packets beyond the threshold in the Hello Time. The device recalculates the number of received TC packets from the next Hello Time.
- After TC protection is disabled, the device will process all TC packets. When it is attacked by massive TC packets, services may be interrupted, and the device may malfunction due to too high CPU utilization.

Configure TC protection for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#stp tc-protection threshold <i>threshold-value</i>	Configure the TC protection threshold.
3	Raisecom(config)#stp tc-protection enable	Configure TC protection.

9.4.20 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show stp information	Show basic configurations of STP.
2	Raisecom#show stp interface	Show STP configurations on the interface.
3	Raisecom#show stp bridge	Show information about the STP root bridge.
4	Raisecom#show stp instance	Show configurations of the MST region.

9.4.21 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config-ge-1/1/*)#reset stp statistics	Clear statistics about spanning tree on the interface.

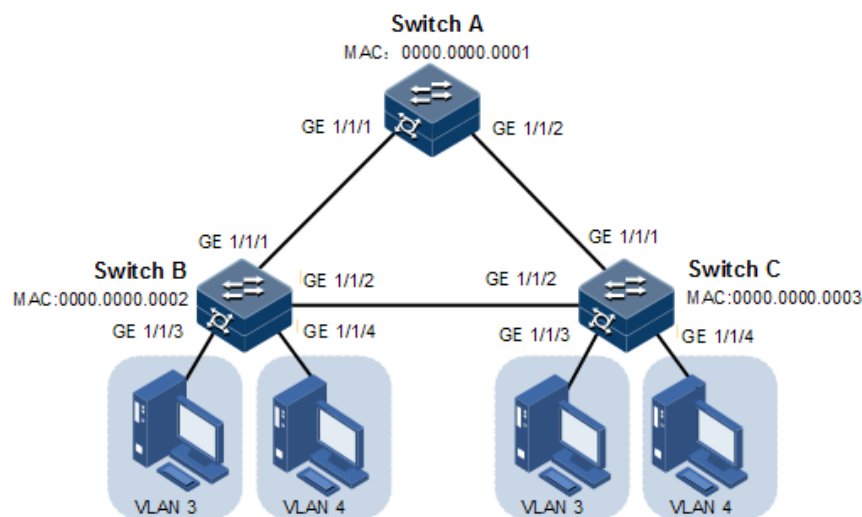
9.4.22 Example for configuring MSTP

Networking requirements

As shown in Figure 9-15, three devices are connected to form a ring network through MSTP, with the region name aaa. Switch B, connected with a PC, belongs to VLAN 3. Switch C,

connected with another PC, belongs to VLAN 4. Instance 3 is associated with VLAN 3. Instant 4 is associated with VLAN 4. Configure the priorities so that the root bridge of instance 3 is Switch A and the root bridge of instance 4 is Switch B. In this way, packets of VLAN 3 and VLAN 4 are forwarded respectively in two paths, which eliminates loops and implements load balancing.

Figure 9-15 MSTP networking



Configuration steps

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

Configure Switch A.

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

Configure Switch B.

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

Configure Switch C.

```
Raisecom#hostname SwitchC
SwitchC#configure
```

```
SwitchC(config)#vlan 3,4
```

- 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 ge 1/1/1
SwitchA(config-ge-1/1/1)#port link-type trunk
SwitchA(config-ge-1/1/1)#port trunk allow-pass vlan all
SwitchA(config-ge-1/1/1)#exit
SwitchA(config)#interface ge 1/1/2
SwitchA(config-ge-1/1/2)#port link-type trunk
SwitchA(config-ge-1/1/2)#port trunk allow-pass vlan all
SwitchA(config-ge-1/1/2)#exit
```

Configure Switch B.

```
SwitchB(config)#interface ge 1/1/1
SwitchB(config-ge-1/1/1)#port link-type trunk
SwitchB(config-ge-1/1/1)#port trunk allow-pass vlan all
SwitchB(config-ge-1/1/1)#exit
SwitchB(config)#interface ge t 1/1/2
SwitchB(config-ge-1/1/2)#switchport mode trunk
SwitchB(config-ge-1/1/2)#port trunk allow-pass vlan all
SwitchB(config-ge-1/1/2)#exit
SwitchB(config)#interface ge 1/1/3
SwitchB(config-ge-1/1/3)#switchport access vlan 3
SwitchB(config-ge-1/1/3)#exit
SwitchB(config)#interface ge 1/1/4
SwitchB(config-ge-1/1/4)#switchport access vlan 4
SwitchB(config-ge-1/1/4)#exit
```

Configure Switch C.

```
SwitchC(config)#interface ge 1/1/1
SwitchC(config-ge-1/1/1)#port link-type trunk
SwitchC(config-ge-1/1/1)#port trunk allow-pass vlan all
SwitchC(config-ge-1/1/1)#exit
SwitchC(config)#interface ge t 1/1/2
SwitchC(config-ge-1/1/2)#switchport mode trunk
SwitchC(config-ge-1/1/2)#port trunk allow-pass vlan all
SwitchC(config-ge-1/1/2)#exit
SwitchC(config)#interface ge 1/1/3
SwitchC(config-ge-1/1/3)#switchport access vlan 3
```

```
SwitchC(config-ge-1/1/3)#exit
SwitchC(config)#interface ge 1/1/4
SwitchC(config-ge-1/1/4)#switchport access vlan 4
SwitchC(config-ge-1/1/4)#exit
```

- Step 3 Configure spanning tree mode of Switch A, Switch B, and Switch C to MSTP, and enable STP. Enter MSTP configuration mode, and configure the region name to aaa and revision version to 0. Map instance 3 to VLAN 3, and instance 4 to VLAN 4. Exit MST configuration mode.

Configure Switch A.

```
SwitchA(config)#stp mode mstp
SwitchA(config)#stp config-name aaa
SwitchA(config)#stp revision-level 0
SwitchA(config)#stp instance 3 vlan 3
SwitchA(config)#stp instance 4 vlan 4
SwitchA(config)#stp instance 3 priority 0
SwitchA(config)#interface ge 1/1/1
SwitchA(config-ge-1/1/1)#stp enable
SwitchA(config-ge-1/1/1)#exit
SwitchA(config)#interface ge 1/1/2
SwitchA(config-ge-1/1/2)#stp enable
```

Configure Switch B.

```
SwitchB(config)#stp mode mstp
SwitchB(config)# stp config-name aaa
SwitchB(config)#stp revision-level 0
SwitchB(config)#stp instance 3 vlan 3
SwitchB(config)#stp instance 4 vlan 4
SwitchA(config)#stp instance 4 priority 0
SwitchB(config)#interface ge 1/1/1
SwitchB(config-ge-1/1/1)#stp enable
SwitchB(config-ge-1/1/1)#exit
SwitchB(config)#interface ge 1/1/2
SwitchB(config-ge-1/1/2)#stp enable
```

Configure Switch C.

```
SwitchC(config)#stp mode mstp
SwitchC(config)#stp config-name aaa
SwitchC(config)#stp revision-level 0
SwitchC(config)#stp instance 3 vlan 3
SwitchC(config)#stp instance 4 vlan 4
SwitchC(config)#interface ge 1/1/1
SwitchC(config-ge-1/1/1)#stp enable
SwitchC(config-ge-1/1/1)#exit
```

```
SwitchC(config)#interface ge 1/1/2
SwitchC(config-ge-1/1/2)#stp enable
```

- 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-gigaethernet1/1/1)#spanning-tree instance 3 inter-path-
cost 500000
```

Checking results

Use the **show stp interface** command to show the interface status of the MST region.

Take Switch C for example.

```
SwitchA#show stp interface
```

MSTID	Port	Role	State	Protection	Region
0	ge-1/1/1	root	forward	--	same
0	ge-1/1/2	alternate	discarding	--	same
3	ge-1/1/1	root	forward	--	same
3	ge-1/1/2	alternate	discarding	--	same
4	ge-1/1/1	alternate	discarding	--	same
4	ge-1/1/2	root	forward	--	same

9.5 Loop detection

9.5.1 Introduction

Loop detection can address the influence on network caused by a loop, providing the self-detection, fault-tolerance, and robustness.

During loop detection, an interface enabled with loop detection periodically sends loop detection packets (Hello packets). Under normal conditions, the edge interface should not receive any loop detection packets because loop detection is applied to the edge interface. However, if the edge interface receives a loop detection packet, it is believed that a loop occurs on the network. There are two conditions that an edge interface receives a loop detection packet: receiving a loop detection packet from itself or receiving a loop detection packet from other devices, which can be told by comparing the MAC address of the device and the MAC address carried in the packet.

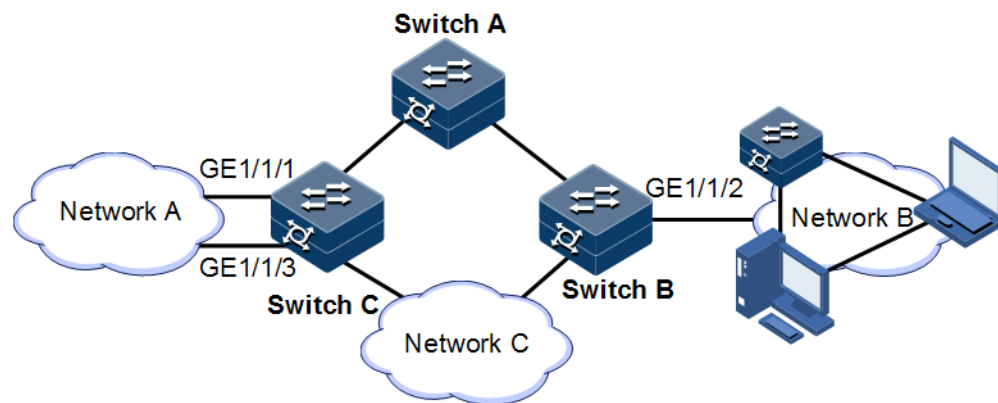
Loop types

Common loop types include self-loop and inner loop.

As shown in Figure 9-16, Switch B and Switch C are connected to the user network.

- Self-loop: a user loop on the same Ethernet interface of the same device. User network B has a loop, which forms self-loop on GE 1/1/2 on Switch B.
- Inner loop: a loop forming on different Ethernet interfaces of the same device. GE 1/1/1 and GE 1/1/3 on Switch C forms an inner loop with the user network A.

Figure 9-16 Loop detection networking



Principles for processing loops

The device processes loops as below:

- If the device sending the loop detection packet is the one receiving the packet but the interface sending the packet and the interface receiving the packet are different, process the interface with the smaller interface ID to eliminate the loop (inner loop).
- If the interface sending the packet and the interface receiving the packet are the same, process the interface to eliminate the loop (self-loop).

In Figure 9-16, 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 GE 1/1/2.
- Inner loop: Switch C receives the loop detection packets sent by it and the interface sending the packet and the interface receiving the packet are the same, the configured loop detection action will be taken to eliminate the loop on the interface with a bigger interface ID, namely, GE 1/1/1.

Action for processing loops

The action for processing loops is the method for the device to use upon loop detection. You can define different actions on the specified interface according to actual situations, including:

- Block: block the interface and send a Trap.
- Trap-only: send a Trap only.
- Shutdown: shut down the interface and send a Trap.

- Shutdown-restore: send a Trap, shut down the interface, and wait to restore.

Loop detection modes

The loop detection mode is port mode.

When a loop occurs, the system blocks the interface and sends Trap in the loopback processing mode of Block, or shuts down the physical interface and sends Trap information in the loopback processing mode of shutdown.

If the loop detection processing mode is Trap-only, the device sends Traps only.

Loop restoration

After an interface is shut down, you can configure automatic restoration after a specified period.

9.5.2 Preparing for configurations

Scenario

On the network, hosts or Layer 2 devices connected to access devices may form a loop intentionally or involuntarily. Enable loop detection on downlink interfaces on all access devices to avoid the network congestion generated by unlimited copies of data traffic. Once a loopback is detected on an interface, the interface will be blocked.

Prerequisite

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

9.5.3 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	5s
Mode for processing detected loops	Block
Loop detection period	1s
Loop detection mode	vlan mode

9.5.4 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 device as below.

Step	Command	Description
1	Raisecom# configure	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config-ge- 1/1/*)# loopback-detect mode vlan	Configure loop detection based on VLAN.
4	Raisecom(config-ge- 1/1/*)# loopback-detect vlan <i>vlan-list</i>	Configure the VLAN for sending packets.
5	Raisecom(config-ge- 1/1/*)# loopback-detect action block	Configure the action taken for loops.
6	Raisecom(config)# loopback-detect interval <i>interval</i>	Configure the interval for sending packets.

9.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show loopback-detection [<i>interface-type interface interface-</i> <i>number</i>] [detail]	Show configurations of loop detection on the interface.

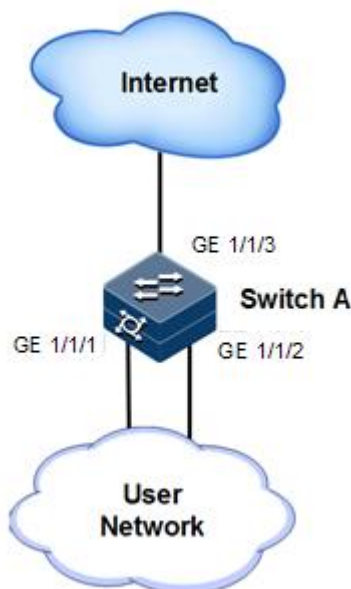
9.5.6 Example for configuring inner loop detection

Networking requirements

As shown in Figure 9-17, GE 1/1/2 and GE 1/1/3 on Switch A are connected to the user network. To avoid loops on the user network, enable loop detection on Switch A to detect loops on user network, and then take actions accordingly. Detailed requirements are as below:

- Enable loop detection on GE 1/1/2 and GE 1/1/3.
- Configure the interval for sending loop detection packets to 3s.
- Configure the VLAN for sending loop detection packets to VLAN 3.
- Configure the loop detection processing action to discarding, namely, sending Trap and blocking the interface.

Figure 9-17 Loop detection networking



Configuration steps

Step 1 Create VLAN 3, and add interfaces to VLAN 3.

```
Raisecom#configure
Raisecom(config)#vlan 3
Raisecom(config)#interface ge 1/1/1
Raisecom(config-ge-1/1/1)#port link-type hybrid
Raisecom(config-ge-1/1/1)#port hybrid vlan 3 untagged
Raisecom(config-ge-1/1/1)#exit
Raisecom(config)#interface ge 1/1/2
Raisecom(config-ge-1/1/2)#port link-type hybrid
Raisecom(config-ge-1/1/2)#port hybrid vlan 3 untagged
Raisecom(config-ge-1/1/2)#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 ge 1/1/1
Raisecom(config-ge-1/1/1)#loopback-detect enable
Raisecom(config-ge-1/1/1)#loopback-detect action block
Raisecom(config-ge-1/1/1)#loopback-detect vlan 3
Raisecom(config-ge-1/1/1)#loopback-detect interval 3
Raisecom(config-ge-1/1/1)#exit
Raisecom(config)#interface ge 1/1/2
Raisecom(config-ge-1/1/2)#loopback-detect enable
Raisecom(config-ge-1/1/2)#loopback-detect action block
Raisecom(config-ge-1/1/2)#loopback-detect vlan 3
```

```
Raisecom(config-ge-1/1/2)#loopback-detect interval 3
```

Checking results

Use the **show loopback-detection** command to show loop detection status.

```
Raisecom#show loopback-detect interface
```

	Interface	Enable	Action	Loop-
Status				

ge-1/1		/1	enable	block
none-loop				
ge-1/1/2	enable	block		none-loop

9.6 Interface backup

9.6.1 Introduction

In dual uplink networking, Spanning Tree Protocol (STP) is used to block the redundancy link and implements backup. Though STP can meet users' backup requirements, it fails to meet switching requirements. Though Rapid Spanning Tree Protocol (RSTP) is used, the convergence is second level only. This is not a satisfying performance parameter for high-end Ethernet switch which is applied to the core of the carrier-grade network.

Interface backup, targeted for dual uplink networking, implements redundancy backup and quick switching through working and protection lines. It ensures performance and simplifies configurations.

Interface backup is another STP solution. When STP is disabled, you can realize basic link redundancy by manually configuring interfaces. If the switch is enabled with STP, you should disable interface backup because STP has provided similar functions.

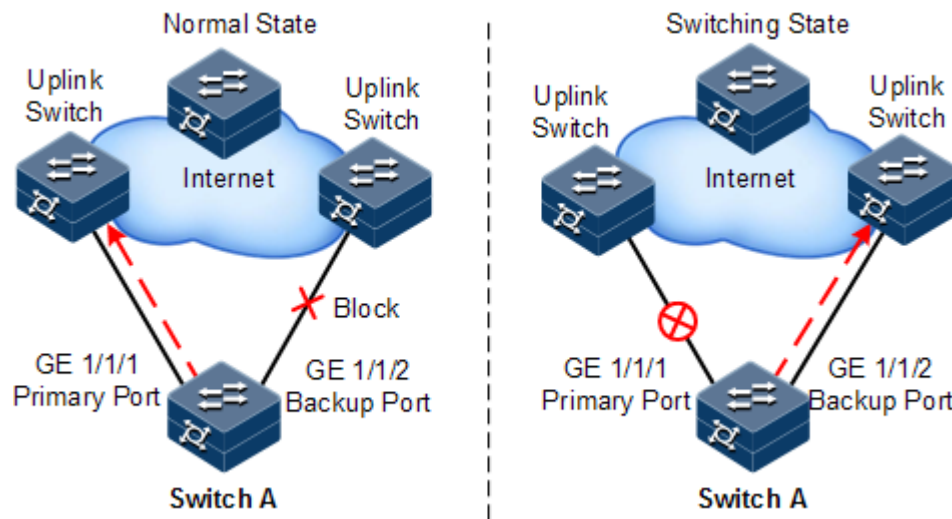
When the primary link fails, traffic is switched to the backup link. In this way, not only 50ms fast switching is ensured, but also configurations are simplified.

Principles of interface backup

Interface backup is implemented by configuring the interface backup group. Each interface backup group contains a primary interface and a backup interface. The link, where the primary interface is, is called a primary link while the link, where the backup interface is, is called the backup interface. Member interfaces in the interface backup group supports physical interfaces and LAGs. However, they do not support Layer 3 interfaces.

In the interface backup group, when an interface is in Forward status, the other interface is in Block status. At any time, only one interface is in Forward status. When the Forward interface fails, the Block interface is switched to the Forward status.

Figure 9-18 Principles of interface backup



As shown in Figure 9-18, 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 9-19.

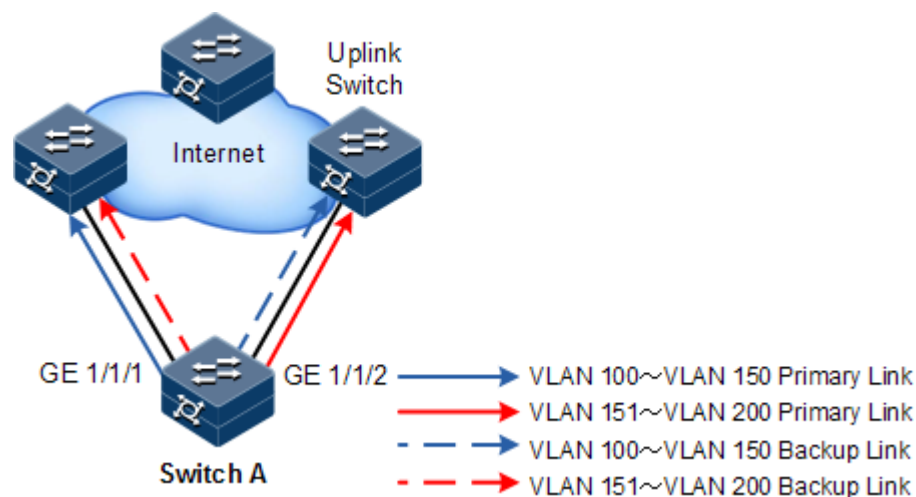


Figure 9-19 Networking with interface backup in different VLANs

In different VLANs, the forwarding status is shown as below:

- Under normal conditions, configure Switch A in VLANs 100–150.
- In VLANs 100–150, GE 1/1/1 is the primary interface and GE 1/1/2 is the backup interface.
- In VLANs 151–200, GE 1/1/2 is the primary interface and GE 1/1/1 is the backup interface.
- GE 1/1/1 forwards traffic of VLANs 100–150, and GE 1/1/2 forwards traffic of VLANs 151–200.
- When GE 1/1/1 fails, GE 1/1/2 forwards traffic of VLANs 100–200.
- When GE 1/1/1 restores normally and keeps Forward for a period (restore-delay), GE 1/1/1 forwards traffic of VLANs 100–150, and GE 1/1/2 forwards VLANs 151–200.

Interface backup is used to balance service load in different VLANs without depending on configurations of uplink switches, thus facilitating users' operation.

9.6.2 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

9.6.3 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

9.6.4 Configuring basic functions of interface backup

Configure basic functions of interface backup for the device as below.



Caution

Interface backup may interfere with STP, loop detection, and G.8032. We do not recommend configuring them concurrently on the same interface.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#protect-link group <i>group-id</i>	Create a backup group.
3	Raisecom(config-protectlink-*)#protect-vlan <i>vlan-list</i>	Configure the specified VLAN list.
4	Raisecom(config-protectlink-*)#add interface <i>interface-type interface-number</i> role master	Specify the master interface.
5	Raisecom(config-protectlink-*)#add interface <i>interface-type interface-number</i> role slave	Specify the backup interface.
6	Raisecom(config-protectlink-*)#port backup fault-detect lldp	Configure LLDP fault detection.
7	Raisecom(config-protectlink-*)#reverse { enable disable }	Configure restoration mode.
8	Raisecom(config-protectlink-*)#reverse time <i>interval</i>	Configure the restoration time.



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.

9.6.5 Configuring FS on interfaces



Caution

After FS is successfully configured, the primary/backup link will be switched; in other words, the current link is switched to the backup link.

Configure FS on interfaces for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#protect-link group <i>group-id</i>	Enter physical interface configuration mode or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-protectlink-*)#manual-switch	Configure FS on the interface.

9.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show protect-link interface	Show status information about interface backup.
2	Raisecom#show protect-link group	Show configurations of the interface backup group.

9.6.7 Example for configuring interface backup

Networking requirements

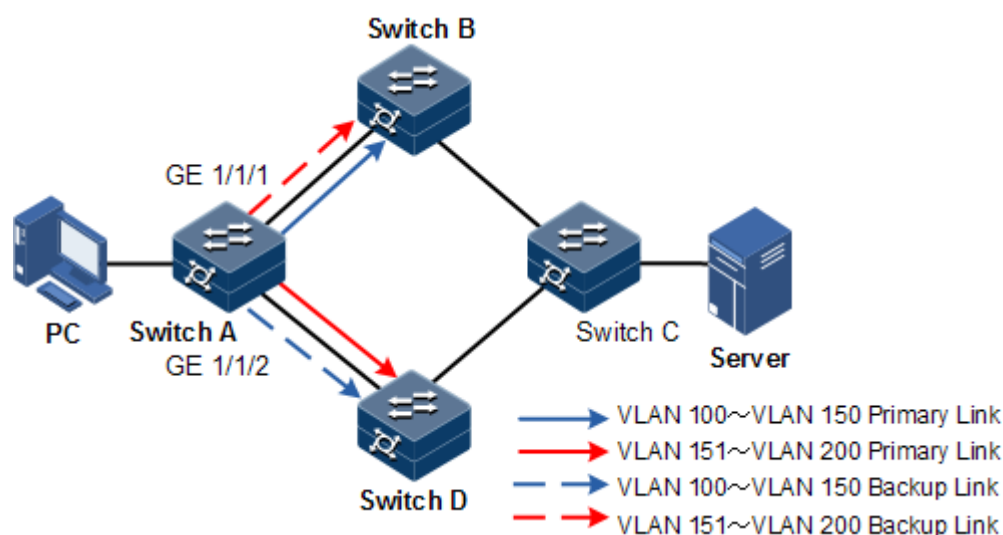
As shown in Figure 9-20, the PC accesses the server through the Switch. To implement a reliable remote access from the PC to the server, configure an interface backup group on Switch A and specify the VLAN list so that the two interfaces concurrently forward services in different VLANs and balance load. 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 9-20 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#configure
Raisecom(config)#vlan 100-200
```

```
Raisecom(config)#interface ge 1/1/1
Raisecom(config-ge-1/1/1)#port link-type trunk
Raisecom(config-ge-1/1/1)#port trunk allow-pass vlan 100-200
Raisecom(config-ge-1/1/1)#exit
Raisecom(config)#interface ge 1/1/2
Raisecom(config-ge-1/1/2)#port link-type trunk
Raisecom(config-ge-1/1/2)#port trunk allow-pass vlan 100-200
Raisecom(config-ge-1/1/2)#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)#protect-link group 1
Raisecom(config-protectlink-1)#protect-vlan 100-150
Raisecom(config-protectlink-1)#add interface ge 1/1/1 role master
Raisecom(config-protectlink-1)#add interface ge 1/1/2 role slave
```

- 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)#protect-link group 2
Raisecom(config-protectlink-1)#protect-vlan 151-200
Raisecom(config-protectlink-1)#add interface ge 1/1/2 role master
Raisecom(config-protectlink-1)#add interface ge 1/1/1 role slave
```

Checking results

Use the **show protect-link interface** command to show status of interface backup under normal or faulty conditions.

When both GE 1/1/1 and GE 1/1/2 are Forward, GE 1/1/1 forwards traffic of VLANs 100–150, and GE 1/1/2 forwards traffic of VLANs 151–200.

```
Raisecom#show protect-link interface
```

Interface	Group	Role	State	Status	Linkstate

ge-1/1/1	1	master	forward	active	up/up
ge-1/1/2	1	slave	block	active	up/up
ge-1/1/1	2	slave	block	active	up/up
ge-1/1/2	2	master	forward	active	up/up

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 protect-link interface**

Interface	Group	Role	State	Status	Linkstate

ge-1/1/1	1	master	block	active	up/down
ge-1/1/2	1	slave	forward	active	up/up
ge-1/1/1	2	slave	block	active	up/down
ge-1/1/2	2	master	forward	active	up/up

9.7 Interface isolation

9.7.1 Introduction

With interface isolation, you can add an interface, which needs to be controlled, to an interface isolation group, isolating Layer 2/Layer 3 data in the interface isolation group. This can provide physical isolation between interfaces, enhance network security, and provide flexible networking scheme for users.

After being configured with interface isolation, interfaces in an interface isolation group cannot transmit packets to each other. Interfaces in and out of the interface isolation group can communicate with each other.

9.7.2 Preparing for configurations

Scenario

Interface isolation can implement mutual isolation of interfaces in the same VLAN, enhance network security and provide flexible networking solutions for you.

Prerequisite

N/A

9.7.3 Default configurations of interface isolation

Default configurations of interface isolation are as below.

Function	Default value
Interface isolation status of each interface	Disable

9.7.4 Configuring interface isolation

Configure interface isolation for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#port-isolate group <i>group-id</i>	Create an interface isolation group.
3	Raisecom(config-isolate-group-1)#add interface <i>interface-type interface-number</i>	Add interfaces to the interface isolation group.

9.7.5 Checking configurations

Use the following commands to check configuration results.

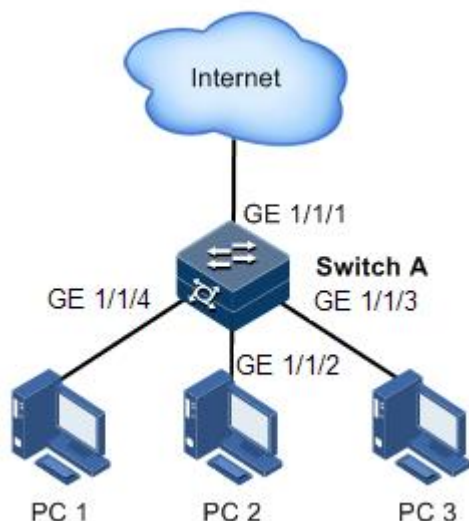
No.	Command	Description
1	Raisecom#show port-isolate information	Show configurations of interface isolation.
2	Raisecom#show port-isolate group	Show configurations of the interface isolation group.

9.7.6 Example for configuring interface isolation

Networking requirements

As shown in Figure 9-21, to prevent PC 1 and PC 2 from interconnecting with each other and to enable them to interconnect with PC 3 respectively, enable interface isolation on GE 1/1/4 and GE 1/1/2 on Switch A.

Figure 9-21 Interface isolation networking



Configuration steps

Step 1 Create an interface isolation group.

```
Raisecom#configure
Raisecom(config)#port-isolate group 1
```

Step 2 Add interfaces to the interface isolation group.

```
Raisecom(config-isolate-group-1)#add interface ge 1/1/4
Raisecom(config-isolate-group-1)#add interface ge 1/1/2
```

Checking results

Use the **show port-isolate group** command to show configurations of interface isolation.

```
Raisecom#show switchport protect
          GroupId      Ports
```

```
-----
1         ge-1   /1/2   ge-1/   1/4
-----
```

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 2, so interface isolation has taken effect.

10 System management

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

- SNMP
- RMON
- LLDP
- Port mirroring
- Cable diagnosis
- UDLD
- Optical module DDM
- System log
- Alarm management
- CPU monitoring
- Memory monitoring
- PING
- Trace
- Hardware monitoring
- Fan monitoring

10.1 SNMP

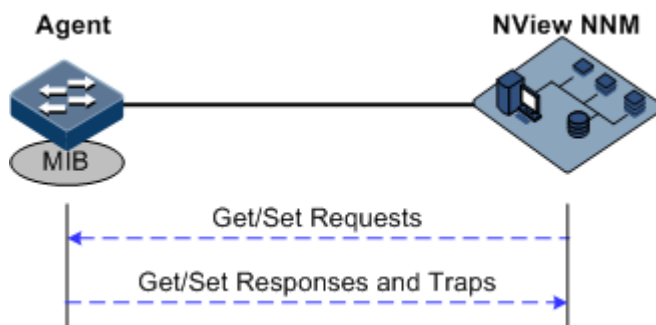
10.1.1 Introduction

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 10-1 shows the SNMP principle.

Figure 10-1 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 device when conditions are satisfied; replying module sends Trap packets to the NView NNM system through agent to report current status of the device.



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 device, 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 used to encrypt packets transmitted between the network management system and agents, thus preventing interception.

The device 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 device.

MIB stores information in a tree structure, and its root is on the top, without name. Nodes of the tree are the managed objects, which take a uniquely path starting from root (OID) for identification. SNMP packets can access network devices by checking the nodes in MIB tree directory.

The device supports standard MIB and Raisecom-customized MIB.

10.1.2 Preparing for configurations

Scenario

To log in to the device through NMS, configure SNMP basic functions for the device in advance.

Prerequisite

Configure the routing protocol and ensure that the route between the device and NMS is reachable.

10.1.3 Default configurations of SNMP

Default configurations of SNMP are as below.

Function	Default value
SNMP service	Disabled by default. You need to enable it.
SNMP view	Internet views (default)
SNMP community	public and private communities (default)
SNMP access group	Not existing (default)
SNMP user	Not existing (default)
Mapping relationship between SNMP user and access group	N/A

Function	Default value
Logo and the contact method of the administrator	support@Raisecom.com
Device physical location	World China Raisecom
Trap	Enable
SNMP target host address	N/A
SNMP engine ID	800022B603000000111233

10.1.4 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 device 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 device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#snmp server start	Start SNMP Server.
3	Raisecom(config)#snmp mib-view <i>view-name</i> { included excluded } <i>oid-tree</i> { mask <i>subtree-mask</i> }	Create an 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.
4	Raisecom(config)#snmp community { read write } { cipher plain } <i>community-name</i> { mib-view <i>view-name</i> acl-ipv4 <i>acl-ipv4-number</i> acl-ipv6 <i>acl-ipv6-number</i> }	Create a community name, and configure the corresponding view and authority. Use default view internet if mib view <i>view-name</i> option is empty.

10.1.5 Configuring basic functions of SNMPv3

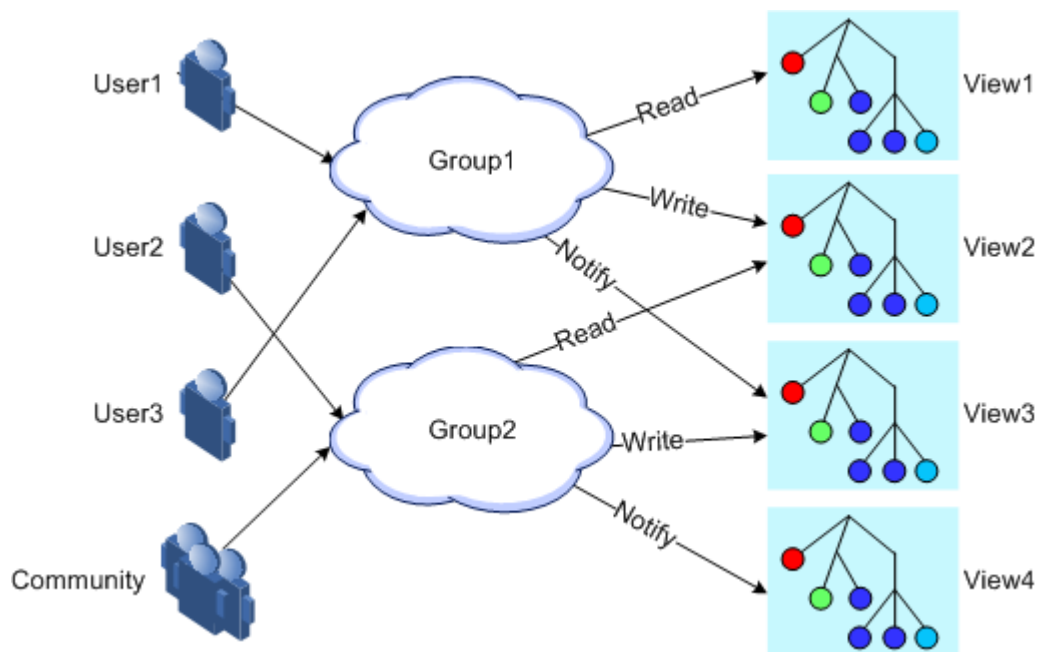
SNMPv3 uses USM over user authentication mechanism. USM comes up with the concept of access group: one or more users correspond to one access group, each access group configures

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 10-2, 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 10-2 SNMPv3 authentication mechanism



Configure basic functions of SNMPv3 for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#snmp mib-view <i>view-name { included excluded }</i> <i>oid-tree { mask subtree-mask }</i>	Create an 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.
3	Raisecom(config)#snmp group <i>group-name</i> { authentication privacy noauthentication } { read-view <i>read-view-name</i> write-view <i>write-view-name</i> notify-view <i>notify-view-name</i> }	Configure the access group.

Step	Command	Description
4	<code>Raisecom(config)#snmp user user-name group group-name authentication { md5 sha } authpassword privacy { des aes } privkeypassword</code>	Create a user account, bind it to a group, and configure the authentication and encryption.
5	<code>Raisecom(config)#snmp user user-name group group-name authentication { md5 sha } authpassword</code>	Create a user account, bind it to a group, and configure the authentication mode.
6	<code>Raisecom(config)#snmp user user-name group group-name { acl-ipv4 acl-ipv4-number acl-ipv6 acl-ipv6-number }</code>	Create a user account, and bind it to an access group.

10.1.6 Configuring other information about SNMP

SNMPv1, SNMPv2c, and SNMPv3 support configuring the following information.

Configure other information about SNMP for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#snmp contact string</code>	Configure the contact method.
3	<code>Raisecom(config)#snmp location location-string</code>	Specify the physical location of the device.
4	<code>Raisecom(config)#snmp auth-fail-reply { enable disable }</code>	Configure whether to send the SNMP response packet upon authentication failure.
5	<code>Raisecom(config)#snmp auth-trap { enable disable }</code>	Configure whether to enable authentication Trap.
6	<code>Raisecom(config)#snmp fail-count fail-count-value</code>	Configure the times of SNMP authentication times.
7	<code>Raisecom(config)#snmp reauth-interval reauth-interval-value</code>	Configure the SNMP re-authentication time.
8	<code>Raisecom(config)#snmp packet max-size { size-value default }</code>	Configure the maximum length of received and sent SNMP packets.
9	<code>Raisecom(config)#snmp reply-source-ip { enable disable }</code>	Configure the IP address to be input as the source IP address of the response packet.
10	<code>Raisecom(config)#snmp udp-port { port-number default }</code>	Configure the SNMP port number.

10.1.7 Configuring Trap



Note

Trap configurations on SNMPv1, SNMPv2c, and SNMPv3 are identical except for Trap target host configurations. Configure Trap as required.

Trap is unrequested information sent by the device to the NMS automatically, which is used to report some critical events.

Before configuring Trap, you need to perform the following configurations:

- Configure basic functions of SNMP. For SNMPv1/v2c, configure the community name; for SNMPv3, configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the device and NMS is available.

Configure SNMP Trap for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#snmp server { start stop }	Start SNMP Server.
3	Raisecom(config)#snmp trap-host <i>ip-address { v1 v2 } { port</i> <i>port-id securityname security-</i> <i>name vpn-instance vpn-name }</i>	Configure the SNMPv1 or SNMPv2c Trap target host (IPv4).
4	Raisecom(config)#snmp-ipv6 trap- host <i>ipv6-address { v1 v2 }</i> { port <i>port-id securityname</i> <i>security-name vpn-instance vpn-</i> <i>name }</i>	Configure the SNMPv1 or SNMPv2c Trap target host (IPv6).
5	Raisecom(config)#snmp-server trap- source <i>interface-type interface-</i> <i>number</i>	Configure the SNMPv3 Trap target host (IPv4).
6	Raisecom(config)#snmp-server trap- source <i>ip-address</i>	Configure the SNMPv3 Trap target host (IPv6).

10.1.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show snmp information	Show SNMP basic configurations, including the local SNMP engine ID, logo and contact method of the administrator, physical location of the device, Trap status, SNMP service status, and SNMP service port number.
2	Raisecom#show snmp group	Show configurations of the SNMP access group.

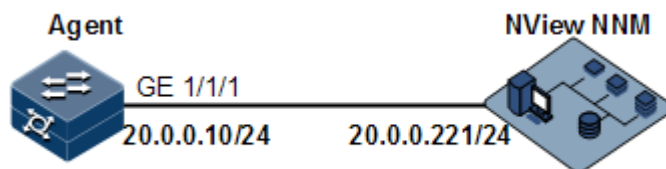
No.	Command	Description
3	Raisecom#show snmp community	Show configurations of the SNMP community.
4	Raisecom#show snmp config	Show basic configurations of SNMP.
5	Raisecom#show snmp trap-host	Show Trap target host information.
6	Raisecom#show snmp statistics	Show SNMP statistics.
7	Raisecom#show snmp user	Show information about SNMP users.
8	Raisecom#show snmp mib-view	Show information about SNMP views.

10.1.9 Example for configuring SNMPv1/SNMPv2c and Trap

Networking requirements

As shown in Figure 10-3, the route between the NView NNM system and the device is available. The NView NNM system can check the MIB under view corresponding to the remote Switch by SNMPv1/SNMPv2c, and the device can send Trap automatically to the NView NNM system in emergency.

Figure 10-3 SNMPv1/SNMPv2c networking



Configuration steps

Step 1 Configure the IP address of the device.

```

Raisecom#configure
Raisecom(config)#interface meth 0/0/0
Raisecom(config-meth-0/0/0)#ip address 192.168.62.100/24
Raisecom(config-meth-0/0/0)#quit
  
```

Step 2 Start SNMP Server.

```

Raisecom(config)#snmp server start
  
```

Step 3 Configure Trap sending.

```
Raisecom(config)#snmp trap-host 192.168.62.1 v2
```

Checking results

Use the **show ip interface** command to show configurations of the IP address.

```
Raisecom#show ip interface
```

						Total number:
2	Interface	State(a/o)	Addr/Prefix	Role	Type	vpn-
	instance					

	loopback-0		up/up	127.0.	0.1/8	primary
	auto	N/A				
			meth-0/0/0		up/up	
	192.168.62.100/24	primary	static	N/A		

Use the **show snmp config** command to show SNMP configurations.

```
Raisecom#show snmp config

Software Version: SNMP_VL3.00.00.00
!
snmp server start
snmp trap-host 192.168.62.1 securityname
AJ35GrrnpX3xRv_UdbJBIGs13Dwxp932i15pfskvs8X-GN6R49ihEydRaxBXkm5V-w
```

Use the **show snmp trap-host** command to show configurations of the target host.

```
Raisecom#show snmp trap-host

Trap-host : 192.168.62.1
-----
Status           : ACTIVE
Udp Port         : 162
MP Modle        : V2
Security Level   : None
Security Name    :
AJ35GrrnpX3xRv_UdbJBIGs13Dwxp932i15pfskvs8X-GN6R49ihEydRaxBXkm5V-w
```

Vpn Instance Name : public

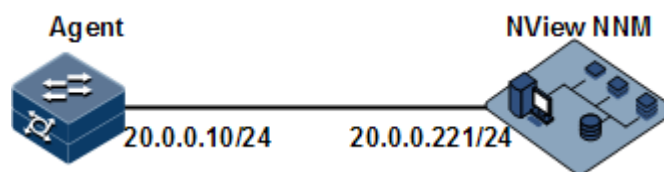
10.1.10 Example for configuring SNMPv3 and Trap

Networking requirements

As shown in Figure 10-4, the route between the NView NNM system and device is available, the NView NNM system monitors the Agent through SNMPv3, and the device can send Trap automatically to the NView NNM system when the Agent is in emergency.

By default, there is VLAN 1 on the device and all physical interfaces belong to VLAN 1.

Figure 10-4 SNMPv3 and Trap networking



Configuration steps

Step 1 Configure the IP address of the device.

```
Raisecom#configure
Raisecom(config)#interface meth 0/0/0
Raisecom(config-meth-0/0/0)#ip address 192.168.62.100/24
Raisecom(config-meth-0/0/0)#quit
```

Step 2 Configure SNMPv3 access.

Start SNMP Server.

```
Raisecom(config)#snmp server start
```

Create an access group named g1. The security level is authentication without encryption.

```
Raisecom(config)#snmp group g1 authentication
```

Create a user named u1. The security level is authentication without encryption. Bind it with group g1. Use the MD5 algorithm. The password is raisecom.

```
Raisecom(config)#snmp user u1 group g1 authentication md5 raisecom
```

- Step 3 Configure Trap sending. The trap-host type must be consistent with the user authentication type, without containing relation.

```
Raisecom(config)#snmp trap-host 192.168.62.1 v3 authentication  
securityname u1
```

Checking results

Use the **show snmp group** command to show configurations of the SNMP access group.

```
Raisecom#show snmp group
Group          Security    ReadView
Writeview      NotifyView
-----
g1             authNoPriv internet    -
-
-----
```

Use the **show snmp user** command to show mapping between users and access groups.

```
Raisecom#show snmp user
Auth  Priv  Filter  User          Group
-----
u1    -      -      g1            MD5    no-priv N/A
-----
```

Use the **show snmp trap-host** command to show configurations of the Trap target host.

```
Raisecom#show snmp trap-host
Trap-host : 192.168.62.1
-----
Status      : ACTIVE
Udp Port    : 162
MP Modle    : V3
Security Level : Auth
Security Name : u1
```

```
Vpn Instance Name      : public
-----
```

Use the **show snmp config** command to show all configurations.

```
Raisecom#show snmp config
                                     Software Version:  SNMP_VL3.00.00.00
!
snmp server start
snmp trap-host 192.168.62.1 v3 authentication securityname u1
snmp group g1 authentication
snmp user u1 group g1 authentication md5
ACS87nMCx4RbzvvPS5l03zDtbzu5xyzSZaDGmHOuqsc0
```

10.2 RMON

10.2.1 Introduction

Remote Network Monitoring (RMON) is a standard stipulated by Internet Engineering Task Force (IETF) for network data monitoring through different network Agents and NMS.

RMON is achieved based on SNMP architecture, including the NView NNM system and the Agent running on network devices. On the foundation of SNMP, increase the subnet flow, statistics, and analysis used to achieve the monitoring to one segment and the whole network, while SNMP only can monitor the partial information about a single device and it is difficult for it to monitor one segment.

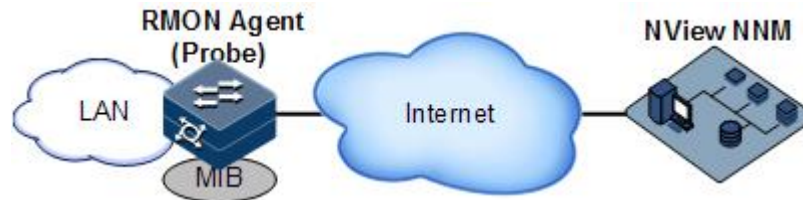
The RMON Agent is commonly referred to as the probe program. The RMON Probe can take the communication subnet statistics and performance analysis. Whenever it finds network failure, RMON Probe can report the NView NNM system, and describes the capture information under unusual circumstances so that the NView NNM system does not need to poll the device constantly. Compared with SNMP, RMON can monitor remote devices more actively and more effectively, network administrators can track the network, segment or device malfunction more quickly. This method reduces the data flows between the NView NNM system and Agent, makes it possible to manage large networks simply and powerfully, and makes up the limitations of SNMP in growing distributed Internet.

RMON Probe collects data in the following modes:

- Distributed RMON. The NMS obtains network management information and controls network resources directly from RMON Probe through dedicated RMON Probe collection data.
- Embedded RMON. Embed RMON Agent directly to network devices (such as switches) to make them with RMON Probe function. The NMS will collect network management information through the basic operation of SNMP and the exchange data information about RMON Agent.

The Raisecom device is embedded with RMON. As shown in Figure 10-5, the device 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 10-5 RMON networking



RMON MIB can be divided into nine groups according to function. Currently, there are four function groups achieved: statistics group, history group, alarm group, and event group.

- **Statistic group:** collect statistics on each interface, including receiving packets accounts and size distribution statistics.
- **History group:** similar with statistic group, it only collects statistics in an assigned detection period.
- **Alarm group:** monitor an assigned MIB object and configure upper threshold and lower threshold in assigned interval, trigger an event if the monitor object receives threshold value.
- **Event group:** cooperating with alarm group. When an alarm triggers an event, it records the event, such as sending Trap, and writes the event into log.

10.2.2 Preparing for configurations

Scenario

RMON helps monitor and account network traffics.

Compared with SNMP, RMON is a more high-efficient monitoring method. After you specifying the alarm threshold, the device actively sends alarms when the threshold is exceeded without obtaining variable information. This helps reduce traffic of Central Office (CO) and managed devices and facilitates network management.

Prerequisite

The route between the device and the NView NNM system is reachable.

10.2.3 Default configurations of RMON

Default configurations of RMON are as below.

Function	Default value
Statistics group	N/A
History group	Disable
Alarm group	N/A
Event group	N/A

10.2.4 Configuring RMON statistics

RMON statistics is used to gather statistics on an interface, including the number of received packets, undersized/oversized packets, collision, CRC and errors, discarded packets, fragments, unicast packets, broadcast packets, multicast packets, and received packet size.

Configure RMON statistics for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-ge-1/0/*)#rmon statistics <i>index-number</i> { owner <i>owner-name</i> }	Enable RMON statistics on an interface and configure related parameters.



Note

When using the **no rmon statistics** *index-number* command on the interface to disable RMON statistics on an interface, you cannot continue to obtain the interface statistics, but the interface can still count data.

10.2.5 Configuring RMON history statistics

Configure RMON history statistics for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
2	Raisecom(config-ge-1/0/*)#rmon history <i>index-number</i> bucket <i>buckets-</i> <i>number</i> interval <i>sampling-interval</i> { owner <i>owner-name</i> }	Enable RMON history statistics on an interface and configure related parameters.



Note

When you use the **no rmon history** *index-number* command on the interface to disable RMON historical statistics on an interface, the interface will not count data and clear all historical data collected previously.

10.2.6 Configuring the RMON alarm group

Configure one RMON alarm group instance (alarm-id) to monitor one MIB variable (*object-id*). When the value of monitoring data exceeds the defined threshold, an alarm event will generate. Record the log to send Trap to network management station according to the definition of alarm event.

The monitored MIB variable must be real, and the data value type is correct.

- If the configured variable does not exist or value type variable is incorrect, return error.
- In the successfully configured alarm, if the variable cannot be collected later, close the alarm; reconfigure the alarm if you want to monitor the variable again.

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 device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#rmon alarm <i>alarm-id</i> <i>object-id</i> <i>query-interval</i> { absolute delta } rising-threshold <i>rising-threshold</i> rising-event falling-threshold <i>falling-threshold</i> falling-event { startup-alarm { rising falling risingorfalling } owner <i>owner-name</i> }	Add alarm instances to the RMON alarm group and configure related parameters.

10.2.7 Configuring the RMON event group

Configure the RMON event group for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#rmon event <i>event-id</i> { log trap both } { description <i>string</i> owner <i>owner-name</i> }	Add events to the RMON event group and configure processing modes of events.

10.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show rmon config	Show RMON configurations.
2	Raisecom#show rmon alarm	Show information about RMON alarm groups.
3	Raisecom#show rmon event	Show information about RMON event groups.
4	Raisecom#show rmon statistics	Show information about RMON statistics groups.

No.	Command	Description
5	Raisecom#show rmon history	Show information about RMON history statistics groups.
6	Raisecom#show rmon history index-number	Show information about the specified RMON history statistics group.
7	Raisecom#show rmon history statistics	Show statistics on the specified RMON history statistics group.
8	Raisecom#show rmon log	Show log information about the RMON event group.

10.2.9 Example for configuring the RMON alarm group

Networking requirements

As shown in Figure 10-6, the device 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 1/0/1. When packets received on GE 1/0/1 exceeds the threshold in a period, logs are recorded and Trap is sent.

Figure 10-6 RMON networking



Configuration steps

- Step 1 Create an event with index ID 1, used to record and send logs with description string of Falling-etherStatsBroadcastPkts. The owner of logs is system.

```

Raisecom#configure
Raisecom(config)#rmon event 1 both description Falling-
etherStatsBroadcastPkts owner system
  
```

- Step 2 Create a statistics table on interface GE 1/0/1. Its owner is system.

```
Raisecom(config-ge-1/0/1)#rmon statistics 1 owner system
```

- Step 3 Create an alarm item with index ID 10, used to monitor MIB variable etherStatsBroadcastPkts.1, namely, 1.3.6.1.2.1.16.1.1.1.6.1, every 20s. If the variable increases to be greater than 100 or smaller than 15, the Trap alarm will be triggered. The owner of alarm message is also system.

```
Raisecom(config)#rmon alarm 10 1.3.6.1.2.1.16.1.1.1.6.1 20 absolute  
rising-threshold 100 1 falling-threshold 15 1 owner system
```

Checking results

Use the **show rmon alarm** command to check whether there is information about event group events on the device.

```
Raisecom#show rmon alarm  
RMON Alarm :10  
Interval:20  
Source OID:1.3.6.1.2.1.16.1.1 .1.6.1  
Sample Type:absolute value  
Alarm Value:0  
Startup Alarm:risingOrFallingAlarm  
Rising Threshold:100  
Rising Event:1  
Falling Threshold:15  
Falling Event:1  
Owner:system  
Status:valid
```

Use the **show rmon event** command to check whether there is information about alarm group on the device.

```
Raisecom#show rmon event  
RMON Event :1  
Type:trap&log  
Status:valid  
Lastsent time:0 days 12 hours 6 minutes 1 seconds  
Description:Falling-etherStatsBroadcastPkts  
Owner:system
```

Use the **show rmon log** command to check whether there is log information about event records on the device.

```
Raisecom#show rmon log
```

```
RMON Log:1/1
      Time:0 days 12 hours 6 minutes 1 seconds
      Description:alarm falling 10,1.3.6.1.2.1.16.1.1.1.6.1,1,0,15
```

When an alarm event is triggered, you can also check related information in the alarm management part of the NView NNM system.

10.3 LLDP

10.3.1 Introduction

With the enlargement of network scale and increase of network devices, the network topology becomes more and more complex and network management becomes more important. A lot of network management software adopts auto-detection function to trace changes of network topology, but most of the software can only analyze the Layer 3 network and cannot ensure the interfaces to be connected to other devices.

Link Layer Discovery Protocol (LLDP) is based on IEEE 802.1ab standard. The NMS can fast grip the Layer 2 network topology and changes.

LLDP organizes the local device information in different Type Length Value (TLV) and encapsulates in Link Layer Discovery Protocol Data Unit (LLDPDU) to transmit to straight-connected neighbour. It also saves the information from neighbour as standard Management Information Base (MIB) for the NMS querying and judging link communication.

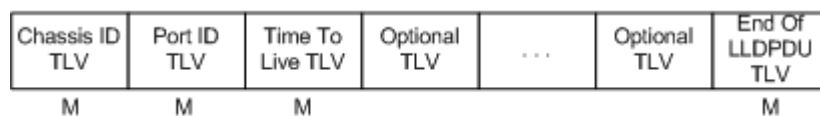
LLDP packet

The LLDP packet is used to encapsulate LLDPDU Ethernet packet in data unit and transmitted by multicast.

LLDPDU is the data unit of LLDP. The device encapsulates local information in TLV before forming LLDPDU, then several TLV fit together in one LLDPDU and encapsulated in Ethernet data for transmission.

As shown in Figure 10-7, LLDPDU is made by several TLV, including 4 mandatory TLV and several optional TLV.

Figure 10-7 Structure of a LLDPDU



M - mandatory TLV required for all LLDPDUs

As shown in Figure 10-8, each TLV denotes a piece of information at local. For example, the device ID and interface ID correspond with the Chassis ID TLV and Port ID TLV respectively, which are fixed TLVs.

Figure 10-8 Structure of a TLV packet

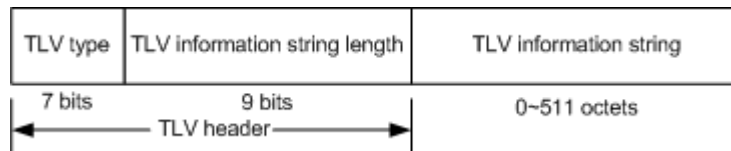


Table 10-1 lists TLV types. At present only types 0-8 are used.

Table 10-1 TLV types

TLV type	Description	Optional/Required
0	End Of LLDPDU	Required
1	Chassis ID	Required
2	Interface number	Required
3	Time To Live	Required
4	Interface description	Optional
5	System name	Optional
6	System description	Optional
7	System capabilities	Optional
8	Management address	Optional

Organization-defined TLVs are optional TLVs and are advertised in the LLDPDU as required. Table 10-2 and Table 10-3 list common organization-defined TLVs.

Table 10-2 IEEE 802.1 organization-defined TLVs

Type	Description
Port VLAN ID TLV	VLAN ID on the interface
Port And Protocol VLAN ID TLV	Protocol VLAN ID on the interface
VLAN Name TLV	VLAN name on the interface
Protocol Identity TLV	Type of the protocol supported by the interface

Table 10-3 IEEE 802.3 organization-defined TLVs

Type	Description
MAC/PHY Configuration//Status TLV	Rate and duplex mode of the interface, whether auto-negotiation is supported or enabled
Power Via MDI TLV	Power supply capability on the interface

Type	Description
Link Aggregation TLV	Link aggregation capability on the interface and current link aggregation status
Maximum Frame Size TLV	Size of the maximum frame able to be transmitted by the interface

Principles

LLDP is a kind of point-to-point one-way issuance protocol, which notifies local device link status to peer end by sending LLDPDU (or sending LLDPDU when link status changes) periodically from the local end to the peer end.

The procedure of packet exchange:

- When the local device transmits packet, it gets system information required by TLV from the NMS 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 device sends a LLDP packet to the peer. To avoid sending LLDP packet continuously because of frequency change of device status, you can configure a delay timer for sending the LLDP packet.

The aging time of Time To Live (TTL) in local device information about the neighbour node can be adjusted by modifying the parameter values of aging coefficient, sends LLDP packets to neighbour node, after receiving LLDP packets, neighbour node will adjust the aging time of its neighbour nodes (sending side) information. Aging time formula, $TTL = \text{Min} \{ 65535, (\text{interval} \times \text{hold-multiplier}) \}$:

- Interval indicates the time period to send LLDP packets from neighbor node.
- Hold-multiplier refers to the aging coefficient of device information in neighbor node.

10.3.2 Preparing for configurations

Scenario

When you obtain connection information between devices through NView NNM system for topology discovery, the device 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

10.3.3 Default configurations of LLDP

Default configurations of LLDP are as below.

Function	Default value
Global LLDP status	Disable
LLDP interface status	Enable
Delay timer	2s
Period timer	30s
Aging coefficient	4
Restart timer	2s
LLDP alarm status	Enable
Alarm notification timer	5s
Destination MAC address of LLDP packets	0180.c200.000e

10.3.4 Enabling global LLDP



Caution

After global LLDP is disabled, you cannot re-enable it immediately. Global LLDP cannot be enabled unless the restart timer times out.

When you obtain connection information between devices through the NView NNM system for topology discovery, the device 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 device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#lldp { start stop }	Enable or disable global LLDP. • Start: enable global LLDP. • stop: disable global LLDP.

10.3.5 Enabling interface LLDP

Enable interface LLDP for the device as below.

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

Step	Command	Description
3	<pre>Raisecom(config- gigaethernet1/1/*)#lldp admin- status { tx-only rx-only rx- tx disable } Example: Raisecom(config- gigaethernet1/1/1)#lldp admin- status tx-only</pre>	Enable or disable interface LLDP. • Tx-only: send LLDP packets only. • Rx-only: receive LLDP packets only. • Rx-tx: send and receive LLDP packets. • Disable: disable LLDP.

10.3.6 Configuring basic functions of global 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 global LLDP for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	<pre>Raisecom(config)#lldp tx-interval { <5- 32768> default } Example: Raisecom(config)#lldp tx-interval 10</pre>	(Optional) configure the period timer of the LLDP packet. • Second: period for sending LLDP packets, an integer, ranging from 5 to 32768, in units of second • Default: 2s
3	<pre>Raisecom(config)#lldp tx-delay { <1-8192> default } Example: Raisecom(config)#lldp tx-delay 5</pre>	(Optional) configure the delay timer of the LLDP packet. • Second: period for delaying to send LLDP packets, an integer, ranging from 1 to 8192, in units of second • Default: 2s
4	<pre>Raisecom(config)#lldp reinit-delay { <1-10> default } Example: Raisecom(config)#lldp reinit-delay 5</pre>	(Optional) configure the restart timer. After global LLDP is disabled, you can re-enable global LLDP only after the delay timer expires. • Second: period for delaying to re-enable LLDP, an integer, ranging from 1 to 10, in units of second • Default: 2s
5	<pre>Raisecom(config)#lldp tx-hold { <2-10> default } Example: Raisecom(config)#lldp tx-hold 2</pre>	(Optional) configure the restart timer. After global LLDP is disabled, you can re-enable global LLDP only after the delay timer expires. • Multiple: multiple, an integer, ranging from 2 to 10 • Default: 4

10.3.7 Configuring basic functions of interface LLDP

Configure basic functions of interface LLDP for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i> Example: Raisecom(config)#interface <i>gigaethernet</i> <i>1/1/1</i>	(Optional) configure the period timer of the LLDP packet. • Second: period for sending LLDP packets, an integer, ranging from 5 to 32768, in units of second • Default: 2s
3	Raisecom(config-gigaethernet1/1/*)#lldp management-address { A.B.C.D } { enable disable }	(Optional) configure the management address of LLDP on the interface. • A.B.C.D: management address • Enable: enabled • Disable: disabled

10.3.8 Configuring the LLDP alarm

When the network changes, you need to enable LLDP alarm notification function to send topology update alarm to the NView NNM system immediately.

Configure the LLDP alarm for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#lldp notification { enable disable }	Enable or disable LLDP Trap.
3	Raisecom(config)#lldp notification-interval { <5-3600> default } Example: Raisecom(config)#lldp notification-interval 10	(Optional) configure the LLDP neighbor change notification period timer. • Second: period for notifying LLDP neighbor change, an integer, ranging from 5 to 3600, in units of second • Default: 5s

10.3.9 Configuring TLV

Configure TLV for the device as below.

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

Step	Command	Description
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-gigaethernet1/1/*)#lldp basic-tlv-tx { port-description system-name system-description system-capability all } { enable disable }	(Optional) configure the basic TLV of LLDP packets on the interface. • Port-description: interface description • System-name: system name • System-description: system description • All: all • Enable: enabled • Disable: disabled
4	Raisecom(config-gigaethernet1/1/*)#lldp dot1-tlv-tx port-vid { enable disable } Raisecom(config-gigaethernet1/1/1)#lldp dot1-tlv-tx protocol-vid <i>vlan-list</i> { enable disable } Raisecom(config-gigaethernet1/1/1)#lldp dot1-tlv-tx vlan-name <i>vlan-list</i> { enable disable }	(Optional) configure the TLV defined by IEEE 802.1 on the interface. • Port-id: interface VLAN ID • Protocol-vid: protocol VLAN ID • Vlan-name: VLAN name • Enable: enabled • Disable: disabled
5	Raisecom(config-gigaethernet1/1/*)#lldp dot3-tlv-tx { mac-phy power link-aggregation max-frame-size all } { enable disable }	(Optional) configure the TLV defined by IEEE 802.3 on the interface. • Mac-phy: interface rate • Power: interface power supply capability • Link-aggregation: link aggregation • Max-frame-size: maximum framelength • All: all • Enable: enabled • Disable: disabled
6	Raisecom(config-gigaethernet1/1/1)#lldp med-tlv-tx { capabilities network-policy location extended-pse extended-pd inventory all } { enable disable }	(Optional) configure MED on the interface. • Capabilities: capabilities • Network-policy: supported applications • Location: location of the interface • Extended-pse: power supply capability • Extended-pd: power supply capability • Inventory: detailed directory • All: all • Enable: enabled • Disable: disabled

10.3.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# show lldp config	Show LLDP configurations.
2	Raisecom# show lldp local [<i>interface-type interface-number</i>]	Show information about the LLDP local system.
3	Raisecom# show lldp remote [<i>interface-type interface-number</i>] [verbose]	Show information about the LLDP neighbor.
4	Raisecom# show lldp statistics [<i>interface-type interface-number</i>]	Show statistics about LLDP packets.
5	Raisecom# show lldp interface [<i>interface-type interface-number</i>]	Show information about LLDP interfaces.

10.3.11 Maintenance

Maintain the device as below.

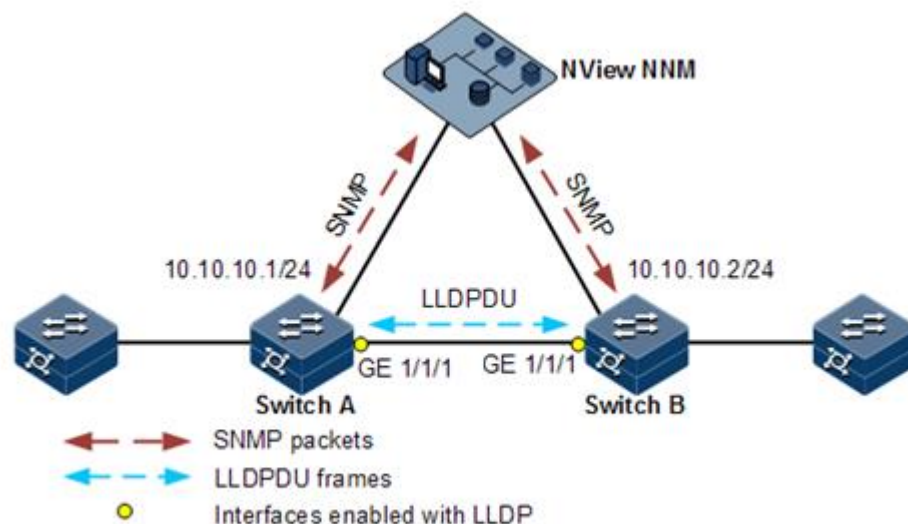
Command	Description
Raisecom(config-gigaethernet1/1/*)# clear lldp port statistics counter	Clear LLDP statistics on the interface.

10.3.12 Example for configuring LLDP

Networking requirements

As shown in Figure 10-9, the Switch is connected to the NView NNM system; enable LLDP between Switch A and Switch B, query Layer 2 link change through the NView NNM system. The neighbor aging, new neighbor and neighbor information changes will be reported as LLDP alarms to the NView NNM system.

Figure 10-9 LLDP networking



Configuration steps

Step 1 Enable global LLDP and LLDP alarm.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#configure
SwitchA(config)#lldp start
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#configure
SwitchB(config)#lldp start
```

Step 2 Configure the management IP address.

Configure Switch A.

```
SwitchA(config)#vlan 10
SwitchA(config)#interface vlan 10
SwitchA(config)#interface gigabitEthernet 1/1/1
SwitchA(config-gigabitEthernet1/1/1)#port hybrid vlan 10 tagged
SwitchA(config-gigabitEthernet1/1/1)#port hybrid pvid 10
SwitchA(config-gigabitEthernet1/1/1)#exit
SwitchA(config)#interface vlan 10
SwitchA(config-vlan1024)#ip address 10.0.0.1/24
```

```
SwitchA(config-vlan1024)#exit
```

Configure Switch B.

```
SwitchB(config)#vlan 10
SwitchB (config)#interface vlan 10
SwitchB (config)#interface gigaethernet 1/1/1
SwitchB (config-gigaethernet1/1/1)#port hybrid vlan 10 tagged
SwitchB (config-gigaethernet1/1/1)#port hybrid pvid 10
SwitchB (config-gigaethernet1/1/1)#exit
SwitchB (config)#interface vlan 10
SwitchB (config-vlan1024)#ip address 10.0.0.2/24
SwitchB (config-vlan1024)#exit
```

Step 3 Configure LLDP attributes.

Configure Switch A.

```
SwitchA(config)#lldp tx-interval 60
SwitchA(config)#lldp tx-delay 9
SwitchA(config)#lldp notification-interval 10
```

Configure Switch B.

```
SwitchB(config)#lldp tx-interval 60
SwitchB(config)#lldp tx-delay 9
SwitchB(config)#lldp notification-interval 10
```

Checking results

Use the **show lldp local config** command to show local configurations.

```
SwitchA#show lldp local
LLDP local:
  Message tx-interval:60(s)
  Message tx-hold:4
  Reinit delay:2(s)
  Tx delay:9(s)
  Notification interval:10(s)
  Chassis type:MAC Address
  Chassis ID:f0f1:f2f3:0101
  System name:SIM-MPU

System desc:ISCOM-SWITCH-SIM
```

```

System supported:Bridge/Switch,Router
System capenabled:Bridge/Switch,Router

Port ge-1/0/1:
  Admin status:TxRx
  Trap enable:no
  Support tlv:port-description,system-name,system-description,system-
capability
  Enabled tlv:port-description,system-name,system-description,system-
capability
  Port type:interface name
  Port ID:GE1/0/1
  Port description:GE1/0/1 SNMP-Index:537397249
  Number of remote system:1
  Number of MED remote system:0
.....

```

Use the **show lldp remote** command to show neighbor information.

```

SwitchA#show lldp remote
  Interface      Index TTL(s)  ChassId      PortId
  SysName      Vlan
ge-1/0/1        1    116    f0f1:f2f3:0201  GE1/0/1
SIM-MPU 10
ge-1/0/2        2    116    f0f1:f2f3:0201  GE1/0/2
SIM-MPU --
.....

```

10.4 Port mirroring

10.4.1 Introduction

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

Figure 10-10 Principles of port mirroring

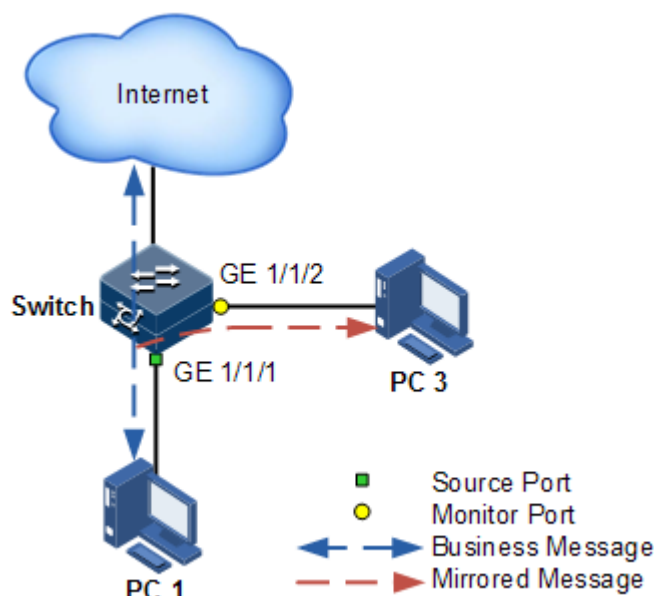


Figure 10-10 shows principles of port mirroring. PC 1 is connected to the external network by the GE 1/1/1; PC 3 is the monitor PC, connecting the external network by GE 1/1/2.

When monitoring packets from the PC 1, you need to assign GE 1/1/1 to connect to PC 1 as the mirror source port, enable port mirroring on the ingress port and assign GE 1/1/2 as monitor port to mirror packets to destination port.

When service packets from PC 1 enter the device, the device will forward and copy them to monitor port (GE 1/1/2). The monitor device connected to the monitor port can receive and analyze these mirrored packets.

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

10.4.2 Preparing for configurations

Scenario

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

Port mirroring copies the port flow monitored to a monitor port or CPU to obtain the ingress/egress port failure or abnormal flow of data for analysis, discovers the root cause, and solves them timely.

Prerequisite

N/A

10.4.3 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

10.4.4 Configuring port mirroring

Configure port mirroring for the device as below.

Step	Configure	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#mirror group group-number <i>interface-type</i> <i>interface-number</i> { rspan <i>vlan-id</i> tpid { standard protocol-id } }	Configure the port mirroring group. • group-number: group ID, ranging from 1 to 4 • interface-type: interface type • interface-number: in the form of unit/slot/port, with the range depending on the interface type • vlan-id: VLAN ID of the remote mirroring, ranging from 1 to 4094 • standard: specified to the standard value 0x8100 • protocol-id: protocol ID of the outer tag of the current interface, ranging from 0x0 to 0xffff
3	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical interface configuration mode.
4	Raisecom(config-ge-1/0/1)#mirror { ingress egress both } group <i>group-number</i>	Configure the port mirroring rule. • { ingress egress both } : ingress, egress, or both directions of the mirroring • Group-number: mirroring group ID, ranging from 1 to 4
5	Raisecom(config-ge-1/0/1)#mirror ingress mac AA:BB:CC:DD:EE:FF/M group <i>group-number</i>	Configure the port+MAC mirroring rule. • Ingress: ingress direction of the mirroring • AA:BB:CC:DD:EE:FF/M: specifying the matching source MAC address • Group-number: mirroring group ID, ranging from 1 to 4

10.4.5 Default configurations of VLAN mirroring

Default configurations of VLAN mirroring are as below.

Function	Default value
VLAN mirroring status	Disable
Mirroring the source port	N/A

10.4.6 Configuring VLAN mirroring

Configure VLAN mirroring for the device as below.

Step	Configure	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mirror group group-number interface-type interface-number { rspan vlan-id tpid { standard protocol-id } }</code>	Configure the VLAN mirroring group. • group-number: group ID, ranging from 1 to 4 • interface-type: interface type • interface-number: in the form of unit/slot/port, with the range depending on the interface type • vlan-id: VLAN ID of the remote mirroring, ranging from 1 to 4094 • standard: specified to the standard value 0x8100 • protocol-id: protocol ID of the outer tag of the current interface, ranging from 0x0 to 0xffff
3	<code>Raisecom(config)#interfa ce vlan vlan-id</code>	Enter VLAN interface configuration mode.
4	<code>Raisecom(config-vlanif- 10)#mirror { ingress egress both } group group-number</code>	Configure the port mirroring rule. • { ingress egress both }: ingress, egress, or both directions of the mirroring • Group-number: mirroring group ID, ranging from 1 to 4
5	<code>Raisecom(config-vlanif- 10)#mirror ingress mac AA:BB:CC:DD:EE:FF/M group group-number</code>	Configure the port+MAC mirroring rule. • Ingress: ingress direction of the mirroring • AA:BB:CC:DD:EE:FF/M: specifying the matching source MAC address • Group-number: mirroring group ID, ranging from 1 to 4

Caution

- Before enabling remote port mirroring, disable MAC address learning of the remote mirroring VLAN on the devices so as to enable the mirroring function to work properly.
- Ensure that mirroring packets between the source device and destination device can be forwarded on Layer 2. The intermediate device interfaces connecting to the source device and destination device must allow packets of the remote mirroring VLAN to pass.
- When configuring the source mirroring port, you cannot add it to the remote mirroring VLAN; otherwise, port mirroring will malfunction.
- The created remote mirroring VLAN cannot be used as the service VLAN; otherwise, port mirroring will malfunction.

10.4.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show mirror group	Show configurations of mirroring groups.
2	Raisecom#show mirror interface	Show mirroring configurations on the interface.

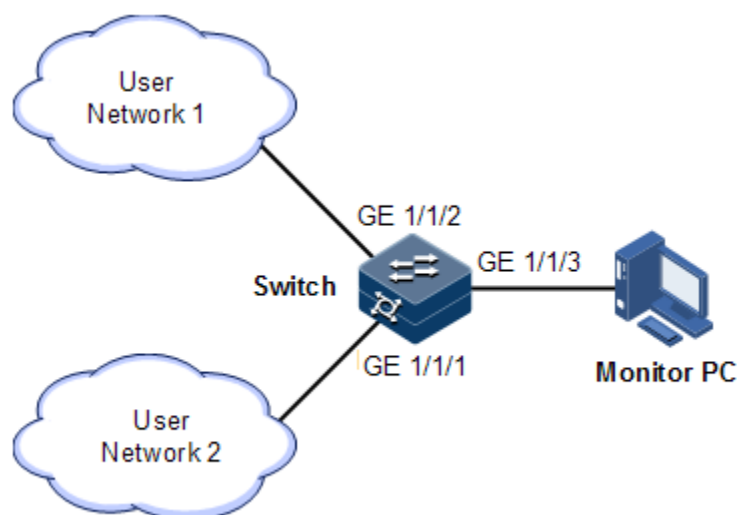
10.4.8 Example for configuring port mirroring

Networking requirements

As shown in Figure 10-11, the network administrator wants to monitor user network 1 through the monitor device, then to catch the fault or abnormal data flow for analyzing and discovering faults and then solve them in time.

The device is disabled with storm control and automatic packets sending. User network 1 accesses the device through GE 1/1/1, user network 2 accesses the device through GE 1/1/2, and the data monitor device is connected to GE 1/1/3.

Figure 10-11 Port mirroring networking



Configuration steps

Enable port mirroring on the Switch.

```

Raisecom#configure
Raisecom(config)#mirror group 1 interface gigabitEthernet 1/1/3
Raisecom(config)#interface gigabitEthernet 1/1/2
Raisecom(config-gigabitEthernet1/1/2)#mirror ingress group 1
  
```

Checking results

Use the **show mirror** command to show configurations of port mirroring.

```
Raisecom#show mirror group
Mirror group 1 is set to interface ge-1/1/3
Mirror group type: Local
Raisecom#show mirror interface
  Interface  Mac-address/Mask  Mirror-group  Direction
-----
ge-1/1/3    1/1          ----          1
ingress
-----
```

10.5 Cable diagnosis

10.5.1 Introduction

The device supports cable diagnosis, which helps you detect lines.

Cable diagnosis contains the following results:

- Detection result of the Tx cable
- Errored location of the Tx cable
- Detection result of the Rx cable
- Errored location of the Rx cable

10.5.2 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

10.5.3 Configuring cable diagnosis

Configure cable diagnosis for the device as below.

Step	Command	Description
1	Raisecom(config)#virtual-cable-test force-detect	Enable global cable diagnosis. This command conducts cable diagnosis on all supportive interfaces.
2	Raisecom(config-ge-1/0/5)#virtual-cable-test	Enable interface cable diagnosis.



Note

When you enable the function of not restarting the interface upon cable diagnosis, the interface that is in Up status will be restarted once and then obtain cable diagnosis data. Then, when cable diagnosis is ongoing, the interface that is in Up status will not be restarted but directly read cable diagnosis data saved in the buffer, and the interface that is in Down status will obtain the length to the faulty point during cable diagnosis. The newly inserted interface will automatically execute cable diagnosis and save results in the buffer.

10.5.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show cable-diagnostics [<i>interface-type interface-number</i>]	Show results of cable diagnosis.

10.6 UDLD

10.6.1 Introduction

UniDirectional Link Detection (UDLD) is used to monitor configurations of the physical connection by the fiber or Ethernet cable. When a unidirectional link (transmitting data in only one direction) is present, UDLD can detect it, shut down the corresponding interface, and send a Trap. The unidirectional link may cause various problems, such as the spanning tree problems which may cause a loop.

10.6.2 Preparing for configurations

Scenario

When a unidirectional link (transmitting data in only one direction) is present, UDLD can detect the fault, shut down the corresponding interface, and send a Trap.

UDLD identifies peer devices and detects unidirectional links through the interaction protocol message (DLDPDU) with the other party. It has seven statuses: Init, Linkdown, Linkup, Advertisement, Detect, and Disable.

Prerequisite

Devices at both ends of the link should support UDLD.

10.6.3 Default configurations of UDLD

Default configurations of UDLD are as below.

Function	Default value
UDLD	Disable

10.6.4 Configuring UDLD

Configure UDLD for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#udld error-down recovery { disable enable }	Enable or disable unidirectional link recovery.
3	Raisecom(config)#udld error-down recovery-interval interval	Configure the recovery time for the unidirectional link. By default, it is 45s.
4	Raisecom(config)#udld work-mode { aggressive normal }	Configure the UDLD working mode to aggressive or normal.
5	Raisecom(config)#udld advertise-interval interval	Configure the interval for sending advertise packet events by UDLD. By default, it is 7s.
6	Raisecom(config)#udld global up-delay time	Configure the global time for the interface to delay to be Up when the unidirectional link is restored.
7	Raisecom(config)#udld snmp-trap { disable enable }	Enable or disable UDLP Trap.
8	Raisecom(config)#udld uni-shutdown { auto manual }	Configure the mode for shutting down the faulty interface and restoring the faulty interface upon detection of the interface being unidirectionally connected by UDLD.
9	Raisecom(config)#interface interface-type primary-interface-number Raisecom(config-ge-1/0/*)#udld { disable enable }	Enable or disable UDLD on the interface.
10	Raisecom(config-ge-1/0/*)#udld aggressive { disable enable }	Enable or disable the aggressive UDLD working mode of the interface.

Step	Command	Description
12	<code>Raisecom(config-ge-1/0/*)#udld rx-mode { normal rxloss }</code>	Configure whether to perform the error-down or Up action by focusing the RXLOS and other messages of the optical module.
13	<code>Raisecom(config-ge-1/0/*)#udld up-delay time</code>	Configure the time for the interface to delay to be Up when the unidirectional link is restored.

10.6.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show udld config</code>	Show UDLD configurations.
2	<code>Raisecom#show udld interface</code>	Show the protocol status of all interface enabled with UDLD.
3	<code>Raisecom#show udld local</code>	Show local information about UDLD.
4	<code>Raisecom#show udld peer</code>	Show neighbor information about UDLD.

10.7 Optical module DDM

10.7.1 Introduction

Optical module Digital Diagnostics Monitoring (DDM) on the device supports Small Form-factor Pluggable (SFP) and 10GE SFP+ diagnosis.

The fault diagnostics function of SFP provides the system a performance monitor method. The network administrator analysis the monitor data provided by SFP to predict the age of transceiver, isolate system fault and authenticate modules compatibility during installation.

The performance parameters of optical module which are monitored by optical module DDM are as below:

- Modular temperature
- Inner power voltage
- Tx offset current
- Tx optical power
- Rx optical power

When the performance parameters reach alarm threshold or status information changes, the corresponding Trap alarm will be generated.

10.7.2 Preparing for configurations

Scenario

Fault diagnostics f optical modules provide a method for detecting SFP performance parameters. You can predict the service life of optical module, isolate system fault and check its compatibility during installation through analyzing monitoring data.

Prerequisite

The optical module used on the device is required to be certified by Raisecom. If the optical module of other manufacturers is used, it may lead to unstable services, lack of support for diagnosis, or inaccurate diagnostic information.

10.7.3 Default configurations of optical module DDM

Default configurations of optical module DDM are as below.

Function	Default value
Interface optical module DDM Trap	Disable

10.7.4 Enabling optical module DDM

Enable optical module DDM for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#transceiver monitor interval interval	Configure the polling interval for optical module DDM.

10.7.5 Enabling optical module DDM Trap

Enable optical module DDM Trap for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface interface-type interface-number	Enter physical interface configuration mode.
3	Raisecom(config 10ge 1/0/*)#transceiver snmp-trap { enable disable }	Enable interface optical module DDM Trap.
4	Raisecom(config 10ge 1/0/*)#transceiver rx-power low-threshold low-threshold-value high-threshold high-threshold-value	Configure the high threshold and low threshold of optical module Rx optical power. When the Rx optical power is smaller than the low threshold or higher than the high threshold, the optical module can send an alarm.
5	Raisecom(config 10ge 1/0/*)#transceiver tx-power low-threshold low-threshold-value high-threshold high-threshold-value	Configure the high threshold and low threshold of optical module Tx optical power. When the Tx optical power is smaller than the low threshold or higher than the high threshold, the optical module can send an alarm.
6	Raisecom(config 10ge 1/0/*)#transceiver temperature low-threshold low-threshold-value high-threshold high-threshold-value	Configure the high threshold and low threshold of optical module temperature. When the temperature is smaller than the low threshold or higher than the high threshold, the optical module can send an alarm.
7	Raisecom(config 10ge 1/0/*)#transceiver voltage low-threshold low-threshold-value high-threshold high-threshold-value	Configure the high threshold and low threshold of optical module voltage. When the voltage is smaller than the low threshold or higher than the high threshold, the optical module can send an alarm.
8	Raisecom(config 10ge 1/0/*)#transceiver bias-current low-threshold low-threshold-value high-threshold high-threshold-value	Configure the high threshold and low threshold of optical module current. When the current is smaller than the low threshold or higher than the high threshold, the optical module can send an alarm.

Step	Command	Description
9	<code>Raisecom(config 10ge 1/0/*)#transceiver tec-current low-threshold <i>low-threshold-value</i> high-threshold <i>high-threshold-value</i></code>	Configure the high threshold and low threshold of optical module TEC current. When the TEC current is smaller than the low threshold or higher than the high threshold, the optical module can send an alarm.

10.7.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show transceiver</code>	Show basic information about the optical module, including wavelength, transmission distance, ID, encoding format, capability code, manufacturer, SN, PN, and other information.
2	<code>Raisecom#show transceiver brief</code>	Show the approximate DDM information about the optical module, including real-time information such as the Tx optical power, Rx optical power, temperature, voltage, and bias current of the optical module.
3	<code>Raisecom#show transceiver verbose</code>	Show the complete information about the optical module, including basic information and DDM information about the optical module.
4	<code>Raisecom#show transceiver config</code>	Show configurations of the optical module.
5	<code>Raisecom#show transceiver interface-type primary-interface-number</code>	Show the basic information about the optical module in the specified interface.
6	<code>Raisecom#show transceiver interface-type primary-interface-number verbose</code>	Show the complete information about the optical module in the specified interface, including basic information and DDM information about the optical module.

10.8 System log

10.8.1 Introduction

The system log refers that the device records the system information and debugging information in a log and sends the log to the specified destination. When the device 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.
- Monitor: send the log message to the monitor, such as Telnet terminal.
- Logfile: send the log message to the Flash of the device.
- Buffer: send the log message to the buffer.
- Trapbuffer: send the log message to the Trap buffer.
- SNMP server: convert logs to Trap and then outputs Trap to the SNMP server.
- Syslog server: send the log message to the Syslog server.
- Smt Email: send the log message to the SMTP Email.

According to the severity level, the log is identified by 8 severity levels, as listed in Table 10-4.

Table 10-4 Log levels

Severity	Level	Description
Emergency	0	The system cannot be used.
Alert	1	Need to deal immediately.
Critical	2	Serious status
Error	3	Errored status
Warning	4	Warning status
Notification	5	Normal but important status
Information	6	Informational event
Debugging	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 error), the information whose level ranges from 0 to 3, in other words, the severity ranges from emergencies to error, can be sent.

10.8.2 Preparing for configurations

Scenario

The device generates the login successes or failures, key information, debugging information, and error information to system log, outputs them as log files, and sends them to the logging host, Console interface, or control console to facilitate checking and locating faults.

Prerequisite

N/A

10.8.3 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 warning (4).
Output log information to files	Enable. The default level is debugging (7).
Output log information to monitor	Enable. The default level is warning (4).
Output log information to buffer	Enable. The default level is debugging (7).
Output log information to SNMP server	Disable. The default level is debugging (7).
Output log information to trapbuffer	Disable. The default level is information (6).
Output log information to syslog server	Disable. The default level is information (6).
Output log information to SNMP Email	Disable. The default level is warning (4).

10.8.4 Configuring basic information about the system log

Configure basic information about the system log for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#logging { on off }	Enable system logs.
3	Raisecom(config)#logging file path { flash ram }	Configure the storage path of the system logs.
4	Raisecom(config)#logging file max-number <i>max-num</i>	Configure the maximum number of log files of the system logs.
5	Raisecom(config)#logging file size kbytes { <i>size-value</i> default }	Configure the size of the system logs.

10.8.5 Configuring system log output

Configure system log output for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#logging module <i>module-name</i> action { console monitor logdfile buffer trap trapbuffer syslog smtp } { log debug trap } { state { enable disable default } level { emergencies alert critical error warning notification information debugging default } }	Configure the output direction of module logs, output enabling status, and output level.

10.8.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show logging information	Show global log configurations.
2	Raisecom#show logging { buffer trap }	Show log or trap buffer information.
3	Raisecom#show logging { buffer trap } { include exclude begin } string <i>string</i>	Show log or trap buffer information and specify string filtering conditions.
4	Raisecom#show logging { buffer trap } size <i>size-number</i>	Show log or trap buffer information and specify the number of entries.
5	Raisecom#show logging { buffer trap } module <i>module-name</i>	Show the logs or trap buffer information of the specified module.
6	Raisecom#show logging { buffer trap } size <i>size-number</i> { include exclude begin } string <i>string</i>	Show log or trap buffer information, specify the number of entries and string filtering conditions.
7	Raisecom#show logging { buffer trap } start-time <i>start-time</i> { end-time <i>end-time</i> }	Show log or trap buffer information and specify the time range for log generation.
8	Raisecom#show logging action	Show the action information of all modules in the log.
9	Raisecom#show logging action { console monitor logfile buffer trap trapbuffer syslog smtp }	Show the specified action information of all modules in the log.
10	Raisecom#show logging error	Show error code information for all module logs.
11	Raisecom#show logging event	Show event information for all module logs.

No.	Command	Description
12	Raisecom#show logging file <i>file-name</i>	Show the content of the specified log file.
13	Raisecom#show logging file <i>file-name</i> { include exclude begin } string <i>string</i>	Show the specified content of the specified log file and specify string filtering conditions.
14	Raisecom#show logging module	Show the information of all module logs, including the module name, module ID, log file name, number of events, and number of error code entries.
15	Raisecom#show logging statistics	Show statistics on log modules.

10.8.7 Maintenance

Maintain the device as below.

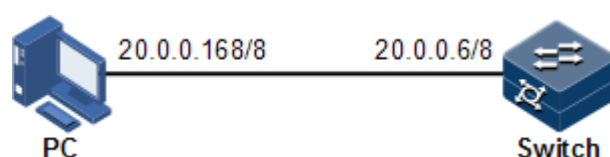
Command	Description
Raisecom(config)#clear logging { buffer trap }	Clear log information in the log or trap buffer.
Raisecom(config)#clear logging statistics	Clear log statistics.
Raisecom(config)#clear logging file all	Clear all log files.
Raisecom(config)#clear logging module <i>module-name</i>	Clear log statistics of the specified module.

10.8.8 Example for configuring outputting system logs to the log host

Networking requirements

As shown in Figure 10-12, configure the system log, and output device log information to the log host for users to check.

Figure 10-12 Networking of outputting system log to log host



Configuration steps

Step 1 Configure the IP address of the device.

```
Raisecom#configure  
Raisecom(config)#interface vlan 1  
Raisecom(config-vlanif-1)#ip address 20.0.0.6 255.0.0.0  
Raisecom(config-vlanif-1)#quit
```

Step 2 Configure the system log to be output to the terminal.

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

Checking results

Use the **show logging information** command to show global configurations of system log.

```
Raisecom#show logging  
information  
-----  
Logging                : on  
Module number          : 125  
Logfile path           : "/ram/log"  
Logfile max size       : 3072 Kb  
Logfile max number     : 3  
Logbuffer Max number   : 2000  
Logbuffer Current  number : 201  
  
Logbuffer history number : 216  
-----
```

10.9 Alarm management

10.9.1 Preparing for configurations

Scenario

When the device fails, alarm management module will collect fault information and output alarm occurrence time, alarm name and description information in log format to help users locate problem quickly.

If the device is configured with the NMS, alarm can be reported directly to the NMS, providing possible alarm causes and treatment recommendations to help users deal with fault.

If the device is configured with hardware monitoring, it will record the hardware monitoring alarm table, generated Syslog, and sent Trap when the operation environment of the device becomes abnormal, and notify the user of taking actions accordingly and prevent faults.

Alarm management facilitates alarm suppression, alarm auto-reporting, alarm monitoring, alarm reverse, alarm delay, alarm memory mode, alarm clear and alarm view directly on the device.

Prerequisite

Hardware environment monitoring alarm output:

- In Syslog output mode: alarms will be generated into system logs. To send alarm to the system log host, configure the IP address of the system log host for the device.
- In Trap output mode: configure the IP address of the NMS for the device.

10.9.2 Configuring basic functions of alarm management

Configure basic information about alarm management for the device as below.

All following steps are optional and no sequence between them.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#alarm snmp { enable disable }	Enable or disable SNMP alarm functions.

10.9.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show alarm information	Show the entries of the alarm management module.
2	Raisecom#show alarm description	Show information about all alarms in the alarm management module. This includes the alarm ID, alarm name, alarm level, corresponding Trap-OID, and description.
3	Raisecom#show alarm { active history all } time-order { object object-name }	Show information about the specified alarm and arrange it in chronological order (active alarm, history alarm, and all alarms).
4	Raisecom#show alarm { active history all } { object object- name }	Show information about the specified alarm (active alarm, history alarm, and all alarms).
6	Raisecom#show alarm object	Show information about the alarm object.

No.	Command	Description
7	Raisecom#show event description	Show information about all events of the alarm management module. This includes the event ID, event name, event level, corresponding Trap-OID, and description.
8	Raisecom#show event { object object-name }	Show all current events in the alarm management module.

10.10 CPU monitoring

10.10.1 Introduction

The device 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.

10.10.2 Preparing for configurations

Scenario

CPU monitoring can provide realtime monitoring to the task status, CPU utilization rate and stack usage in the system, provide CPU utilization rate threshold alarm, detect and eliminate hidden dangers, or help administrator for fault location.

Prerequisite

When the CPU monitoring alarm needs to be output in Trap mode, configure Trap output target host address, which is IP address of NView NNM system.

10.10.3 Default configurations of CPU monitoring

Default configurations of CPU monitoring are as below.

Function	Default value
CPU utilization rate alarm Trap output	Enable
Upper threshold of CPU utilization alarm	80%
Sampling period of CPU utilization	10s

10.10.4 Configuring the CPU monitoring alarm

Configure CPU monitoring alarm for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#cpu { all cpu-index } high-threshold <i>high-threshold-value</i>	Configure the rising threshold of all CPU entries or the specified CPU entry.
3	Raisecom(config)#cpu { all cpu-index } description <i>description-string</i>	Configure the description of all CPU entries or the specified CPU entry.
4	Raisecom(config)#cpu { all cpu-index } snmp-trap { disable enable }	Enable or disable Trap sending for all CPU entries or the specified CPU entry.
5	Raisecom(config)#cpu monitor interval <i>interval-value</i>	Configure the interval for sampling CPU utilization.
6	Raisecom(config)#cpu monitor { disable enable }	Enable or disable CPU utilization monitoring.

10.10.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show cpu	Show CPU utilization.
2	Raisecom#show cpu verbose	Show detailed CPU utilization.
3	Raisecom#show cpu task	Show CPU utilization of each task.

10.11 Memory monitoring

10.11.1 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.

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.

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.

10.11.2 Configuring memory monitoring

Configure memory monitoring for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#memory { all memory-index } high-threshold high-threshold-value	Configure the memory monitoring alarm threshold of all memory entries or the specified memory entry.
3	Raisecom(config)#memory { all memory-index } description description-string	Configure the description of all memory entries or the specified memory entry.
4	Raisecom(config)#memory { all memory-index } snmp-trap { disable enable }	Enable or disable Trap sending for all memory entries or the specified memory entry.
5	Raisecom(config)#memory monitor interval interval-value	Configure the interval for sampling memory utilization.
6	Raisecom(config)#memory monitor { disable enable }	Enable or disable memory utilization monitoring.

10.11.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show memory	Show memory utilization.

No.	Command	Description
2	Raisecom#show memory verbose	Show detailed memory utilization.
3	Raisecom#show memory task	Show memory utilization of each process.

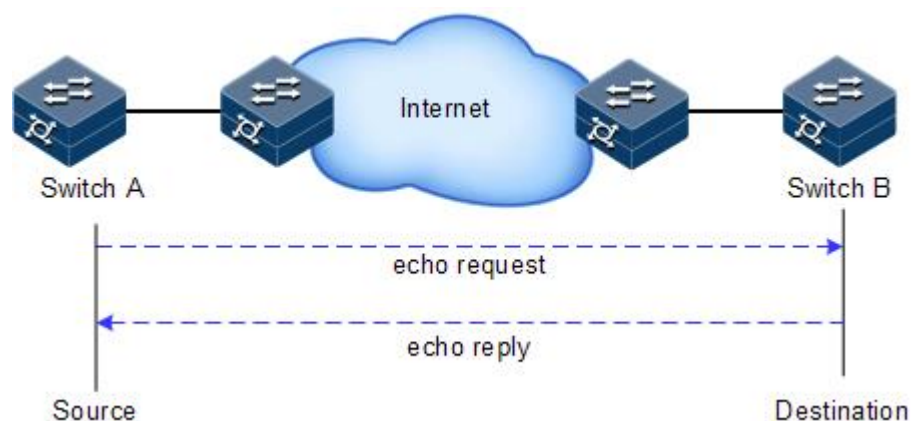
10.12 PING

10.12.1 Introduction

Packet Internet Groper (PING) derives from the sonar location operation, which is used to detect whether the network is normally connected. PING is achieved with ICMP echo packets. If an Echo Reply packet is sent back to the source address during a valid period after the Echo Request packet is sent to the destination address, it indicates that the route between source and destination address is reachable. If no Echo Reply packet is received during a valid period and timeout information is displayed on the sender, it indicates that the route between source and destination addresses is unreachable.

Figure 10-13 shows principles of PING.

Figure 10-13 Principles of PING



10.12.2 Configuring PING

Configure PING for the device as below.

Step	Command	Description
1	<code>Raisecom#ping { ipv4-address hostname } { -n nvalue -system-time -t -q -f -h hvalue -l lengthvalue -w waitvalue -tos tosvalue -m mvalue -dscp dscpvalue -8021p 8021pvalue -range rangevalue -s source-ipv4-address -nexthop next-ipv4-address -vpn-instance vpn-name -eth-trunk trunk-number -bridge-domain bridge-domain-number -loopback loopback-number -vlan vlan-id -ge interface-number1 -10ge interface-number2 -25ge interface-number3 -40ge interface-number4 -100ge interface-number5 -400ge interface-number6 -meth meth-number }</code>	Test the connectivity of the IPv4 network by the ping command.
2	<code>Raisecom#ping-ipv6 { ipv6-address hostname } { -n nvalue -system-time -t -q -f -h hvalue -l lengthvalue -w waitvalue -m mvalue -tc tcvalue -8021p 8021pvalue -range rangevalue -s source-ipv6-adress -nexthop next-ipv6-address -vpn-instance vpn-name -eth-trunk trunk-number -bridge-domain bridge-domain-number -loopback loopback-number -vlan vlan-id -ge interface-number1 -10ge interface-number2 -25ge interface-number3 -40ge interface-number4 -100ge interface-number5 -400ge interface-number6 -meth meth-number }</code>	Test the connectivity of the IPv6 network by the ping command.



Note

The device 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**.

10.13 Trace

10.13.1 Introduction

Similar with PING, Trace is a commonly-used maintenance method in network management. Trace 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

Trace works as below:

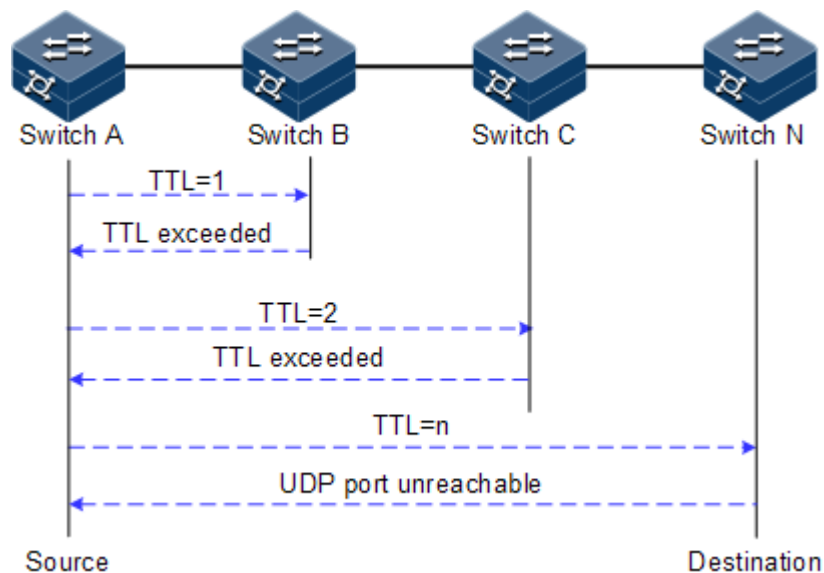
- Step 1 Send a piece of TTL1 sniffer packet (where the UDP port number of the packet is unavailable to any application programs in destination side).
- Step 2 TTL deducts 1 when reaching the first hop. Because the TTL value is 0, in the first hop the device returns an ICMP timeout packet, indicating that this packet cannot be sent.
- Step 3 The sending host adds 1 to TTL and resends this packet.

- Step 4 Because the TTL value is reduced to 0 in the second hop, the device will return an ICMP timeout packet, indicating that this packet cannot be sent.

The previous steps continue until the packet reaches the destination host, which will not return ICMP timeout packets. Because the port number of destination host is not be used, the destination host will send the port unreachable packet and finish the test. Thus, the sending host can record the source address of each ICMP TTL timeout packet and analyze the path to the destination according to the response packet.

Figure 10-14 shows principles of traceroute.

Figure 10-14 Principles of Trace



10.13.2 Configuring IPv4 Trace

Before using Trace, you should configure the IP address and default gateway of the device.

Configure IPv4 Trace for the device as below.

Step	Command	Description
1	<pre>Raisecom#trace ip-address { -n number -r -q -f -fh first-ttl-value -h max-ttl-value -l length-value -w wait-for-each-value -tos tosvalue -m wait-for-send-value -dscp dscpvalue -8021p 8021p-value -range range- value -s source-ip-address -nexthop next- ip-address -vpn-instance vpn-name -eth- trunk trunk-number -bridge-domain bridge- domain-id -loopback loopback-number -vlan vlan-id -ge interface-number1 -10ge interface-number2 -25ge interface-number3 - 40ge interface-number4 -100ge interface- number5 -400ge interface-number6 -meth meth-number }</pre>	Test the connectivity of the IPv4 network and view nodes passed by the packet by the trace command.

10.13.3 Configuring IPv6 Trace

Before using Trace, you should configure the IP address and default gateway of the device.

Configure IPv6 Trace for the device as below.

Step	Command	Description
1	<code>Raisecom#trace-ipv6 ipv6-address { -n number -r -q -f -fh first-ttl-value -h max-ttl-value -l length-value -w wait-for-each-value -m wait-for-send-value -tc traffic-class-value -8021p 8021p-value -range pkt-length-value -s source-ipv6-address -nexthop next-ipv6-address -vpn-instance vpn-name -eth-trunk trunk-number -bridge-domain bridge-domain-id -loopback loopback-number -vlan vlan-id -ge interface-number1 -10ge interface-number2 -25ge interface-number3 -40ge interface-number4 -100ge interface-number5 -400ge interface-number6 -meth meth-number }</code>	Test the connectivity of the IPv6 network and view nodes passed by the packet by the trace command.

10.14 Hardware monitoring



Note

Not all device models support temperature alarms, which depend on the specific device.

10.14.1 Introduction

Hardware environment monitoring mainly refers to monitor the running environment of the device. The monitoring alarm events include the temperature and power supply.

10.14.2 Configuring temperature monitoring

Configure temperature monitoring for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#temperature monitor { disable enable }</code>	Enable or disable temperature monitoring.
3	<code>Raisecom(config)#temperature { all temperature-index } description description-string</code>	Configure the description of all or specified temperature monitoring entries.

Step	Command	Description
4	Raisecom(config)#temperature { all temperature-index } low-threshold <i>low-threshold-value</i> high-threshold <i>high-threshold-value</i>	Configure the high threshold and low threshold for all or specified temperature monitoring entries. When the temperature is smaller than the low threshold or higher than the high threshold, the device can send an alarm.
5	Raisecom(config)#temperature { all temperature-index } snmp-trap { disable enable }	Enable or disable Trap sending for all or specified temperature monitoring entry.

10.14.3 Configuring power supply monitoring

Configure power supply monitoring for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#power monitor { disable enable }	Enable or disable power supply monitoring.
3	Raisecom(config)#power monitor interval <i>interval-value</i>	Configure the period of power supply monitoring. By default, it is 25s.
4	Raisecom(config)#power { all power-index } description <i>description-string</i>	Configure the description of all or specified power supply entry.
5	Raisecom(config)#power { all power-index } snmp-trap { disable enable }	Enable or disable Trap sending for all or specified power supply entry.

10.14.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show temperature config	Show configurations of temperature monitoring.
2	Raisecom#show power config	Show configurations of power supply monitoring.

10.15 Fan monitoring



Note

This section is applicable to the models with fans.

10.15.1 Introduction

The device supports monitoring the fan, including the rotational speed and temperature. It sends Trap when the rotational speed or temperature is abnormal.

The device monitors the fan in two modes:

- Fixed speed mode: forcibly configure the rotational speed of the fan.
- Temperature control mode: the fan adjusts its rotational speed by temperature.

In temperature control mode, when the temperature of the fan is detected to exceed the high threshold, the speed level of the fan will be increased by one gear. If the temperature of the fan is detected to be below the low threshold value, the speed level of the fan will be reduced by one gear.

10.15.2 Preparing for configurations

Scenario

In hot environment, too high temperature affects heat dissipation of the device. Thus fan monitoring must be configured so that the rotational speed is automatically adjusted according to environment temperature and the device runs properly.

Precondition

N/A

10.15.3 Configuring fan monitoring

Configure fan monitoring for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#fan monitor { disable enable }	Enable or disable fan monitoring.
3	Raisecom(config)#fan monitor interval interval-value	Configure the fan monitoring period.
4	Raisecom(config)#fan { all fan-index } mode { speed-level temperature-control }	Configure the mode of all fans or specified fan. • Speed-level: fixed speed level mode • Temperature-control: temperature control mode

Step	Command	Description
5	Raisecom(config)#fan { all <i>fan-index</i> } description <i>description-string</i>	Configure the description of all fans or specified fan.
6	Raisecom(config)#fan { all <i>fan-index</i> } level <i>level-value</i>	Configure the speed level of all fans or specified fan.
7	Raisecom(config)#fan { all <i>fan-index</i> } snmp-trap { disable enable }	Enable or disable TRAP sending for all fans or specified fan.

10.15.4 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom# show fan	Show information fan monitoring, including the current speed and speed level.
2	Raisecom# show fan verbose	Show basic information about the fan.
3	Raisecom# show fan config	Show configurations of fan monitoring.

11 Appendix

This chapter lists terms, acronyms, and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

11.1 Terms

A

Access Control List (ACL)	A series of ordered rules composed of permit deny sentences. These rules are based on the source MAC address, destination MAC address, source IP address, destination IP address, and interface ID. The device determines to receive or refuse the packets based on these rules.
Automatic Laser Shutdown (ALS)	The technology that is used for automatically shutting down the laser to avoid the maintenance and operation risks when the fiber is pulled out or the output power is too great.
Auto-negotiation	The interface automatically chooses the rate and duplex mode according to the result of negotiation. The auto-negotiation process is: the interface adapts its rate and duplex mode to the highest performance according to the peer interface; in other words, both ends of the link adopt the highest rate and duplex mode they both support after auto-negotiation.
Automatic Protection Switching (APS)	APS is used to monitor transport lines in real time and automatically analyze alarms to discover faults. When a critical fault occurs, through APS, services on the working line can be automatically switched to the protection line, thus the communication is recovered in a short period.

C

Challenge Handshake Authentication Protocol (CHAP)	CHAP is a widely supported authentication method in which a representation of the user's password, rather than the password itself, is sent during the authentication process. With CHAP, the remote access server sends a challenge to the remote access client. The remote access client uses a hash algorithm (also known as a hash function) to compute a Message Digest-5 (MD5) hash result based on the challenge and a hash result computed from the user's password. The remote access client sends the MD5 hash result to the remote access server. The remote access server, which also has access to the hash result of the user's password, performs the same calculation using the hash algorithm and compares the result to the one sent by the client. If the results match, the credentials of the remote access client are considered authentic. A hash algorithm provides one-way encryption, which means that calculating the hash result for a data block is easy, but determining the original data block from the hash result is mathematically infeasible.
--	---

D

Dynamic ARP Inspection (DAI)	A security feature that can be used to verify the ARP data packets in the network. With DAI, the administrator can intercept, record, and discard ARP packets with invalid MAC address/IP address to prevent common ARP attacks.
Dynamic Host Configuration Protocol (DHCP)	A technology used for assigning IP address dynamically. It can automatically assign IP addresses for all clients in the network to reduce workload of the administrator. In addition, it can implement centralized management of IP addresses.

E

Ethernet in the First Mile (EFM)	Complying with IEEE 802.3ah protocol, EFM is a link-level Ethernet OAM technology. It provides the link connectivity detection, link fault monitoring, and remote fault notification for a link between two directly-connected devices. EFM is mainly used for the Ethernet link on edges of the network accessed by users.
Ethernet Ring Protection Switching (ERPS)	It is an APS protocol based on ITU-T G.8032 standard, which is a link-layer protocol specially used for the Ethernet ring. In normal conditions, it can avoid broadcast storm caused by the data loop on the Ethernet ring. When the link or device on the Ethernet ring fails, services can be quickly switched to the backup line to enable services to be recovered in time.

F

Full duplex	In a communication link, both parties can receive and send data concurrently.
-------------	---

G

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 provides an interface linkage scheme, extending the range of link backup. Through monitoring upstream links and synchronizing downstream links, faults of the upstream device can be transferred quickly to the downstream device, and primary/backup switching is triggered. In this way, it avoids traffic loss because the downstream device does not sense faults of the upstream link.
---------------------	---

M

Multi-Mode Fiber (MMF)	In this fiber, multi-mode optical signals are transmitted.
------------------------	--

N

Network Time Protocol (NTP)	A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed time server and clients. NTP is used to perform clock synchronization on all devices that have clocks in the network. Therefore, the devices can provide different applications based on a unified time. In addition, NTP can ensure a very high accuracy with an error of 10ms or so.
-----------------------------	---

O

Open Shortest Path First (OSPF)	An internal gateway dynamic routing protocol, which is used to determine the route in an Autonomous System (AS)
---------------------------------	---

Optical Distribution Frame (ODF)	A distribution connection device between the fiber and a communication device. It is an important part of the optical transmission system. It is mainly used for fiber splicing, optical connector installation, fiber adjustment, additional pigtail storage, and fiber protection.
----------------------------------	--

P

Password Authentication Protocol (PAP)	PAP is an authentication protocol that uses a password in Point-to-Point Protocol (PPP). It is a twice handshake protocol and transmits unencrypted user names and passwords over the network. Therefore, it is considered unsecure.
--	--

Point-to-point Protocol over Ethernet (PPPoE)	PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames. With PPPoE, the remote access device can control and account each access user.
---	---

Q

QinQ QinQ is (also called Stacked VLAN or Double VLAN) extended from 802.1Q, defined by IEEE 802.1ad recommendation. Basic QinQ is a simple Layer 2 VPN tunnel technology, encapsulating outer VLAN Tag for client private packets at carrier access end, the packets take double VLAN Tag passing through trunk network (public network). In public network, packets only transmit according to outer VLAN Tag, the private VLAN Tag are transmitted as data in packets.

Quality of Service (QoS) A network security mechanism, used to solve problems of network delay and congestion. When the network is overloaded or congested, QoS can ensure that packets of important services are not delayed or discarded and the network runs high efficiently. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio.

R

Rapid Spanning Tree Protocol (RSTP) Evolution of the Spanning Tree Protocol (STP), which provides improvements in the speed of convergence for bridged networks

Remote Authentication Dial In User Service (RADIUS) RADIUS refers to a protocol used to authenticate and account users in the network. RADIUS works in client/server mode. The RADIUS server is responsible for receiving users' connection requests, authenticating users, and replying configurations required by all clients to provide services for users.

S

Simple Network Management Protocol (SNMP) A network management protocol defined by Internet Engineering Task Force (IETF) used to manage devices in the Internet. SNMP can make the network management system to remotely manage all network devices that support SNMP, including monitoring network status, modifying network device configurations, and receiving network event alarms. At present, SNMP is the most widely-used network management protocol in the TCP/IP network.

Simple Network Time Protocol (SNTP) SNTP is mainly used for synchronizing time of devices in the network.

Single-Mode Fiber (SMF) In this fiber, single-mode optical signals are transmitted.

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.

11.2 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	
MVRP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GMRP	MVRP Multicast Registration Protocol
GPS	Global Positioning System
MVRP	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
RCMP	Raisecom Cluster Management Protocol
RED	Random Early Detection
RH	Relative Humidity
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
ROS	Raisecom Operating System
RPL	Ring Protection Link
RRPS	Raisecom Ring Protection Switching
RSTP	Rapid Spanning Tree Protocol

RSVP	Resource Reservation 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

