

www.raisecom.com

ISCOM S3600 (A) Series Configuration Guide (CLI) (Rel_03)

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 ©2025

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 ISCOM S3600 (A), 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 S3600 (A) series switch	V7.01	A

Conventions

Symbol conventions

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

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

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

General conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Arial	Paragraphs in Warning, Caution, Notes, and Tip are in Arial.
Boldface	Buttons and navigation 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 03 (2025-01-10)

Third commercial release

- Fixed some known bugs.

Issue 02 (2024-03-30)

Second commercial release

- Fixed some known bugs.

Issue 01 (2024-01-01)

Initial commercial release

Contents

1 Basic configurations	1
1.1 Accessing device	1
1.1.1 Introduction.....	1
1.1.2 Accessing through the Console interface	1
1.1.3 Accessing through Telnet	4
1.1.4 Accessing through SSH.....	7
1.1.5 Accessing from Web	9
1.1.6 Managing users	11
1.1.7 Restoring the user password.....	13
1.1.8 Configuring properties of the terminal	13
1.1.9 Configuring the BootROM password	14
1.2 Loading and upgrade.....	14
1.2.1 Introduction.....	14
1.2.2 Upgrading system software through TFTP CLI	15
1.2.3 Upgrading system software through FTP CLI	15
1.2.4 Checking configurations	16
1.2.5 Specifying the startup OS	16
1.2.6 Showing the system version.....	16
1.3 Time management	17
1.3.1 Introduction.....	17
1.3.2 Preparing for configurations	19
1.3.3 Default configurations.....	19
1.3.4 Configuring NTP	20
1.3.5 Configuring SNTP	22
1.3.6 Checking configurations	22
1.3.7 Example for configuring NTP.....	23
1.4 Interface management	26
1.4.1 Introduction.....	26
1.4.2 Default configurations of interface management	27
1.4.3 Configuring basic attributes of interfaces	27
1.4.4 Configuring interface rate statistics	28
1.4.5 Configuring flow control on interfaces	28

1.4.6 Shutting down/Restarting the interface	29
1.4.8 Showing the priority of management packets	30
1.4.9 Checking configurations	30
2 Ethernet	31
2.1 MAC address table	31
2.1.1 Introduction.....	31
2.1.2 Preparing for configurations	33
2.1.3 Default configurations of MAC address table.....	34
2.1.4 Configuring the static MAC address.....	34
2.1.5 Configuring the blackhole MAC address.....	34
2.1.6 Configuring MAC address learning	35
2.1.7 Configuring the MAC address limit.....	35
2.1.8 Configuring the aging time of MAC addresses.....	35
2.1.9 MAC address flapping detection and protection	35
2.1.10 Checking configurations	36
2.1.11 Maintenance	37
2.1.12 Example for configuring the MAC address table.....	37
2.2 VLAN.....	39
2.2.1 Introduction.....	39
2.2.2 Preparing for configurations	41
2.2.3 Default configurations of VLAN	42
2.2.4 Configuring VLAN attributes	42
2.2.5 Configuring the interface mode	42
2.2.6 Configuring the VLAN on the Access interface	43
2.2.7 Configuring the VLAN on the Trunk interface	43
2.2.8 Configuring the VLAN based on the Hybrid interface	44
2.2.9 Configuring the VLAN based on MAC address	45
2.2.10 Configuring the VLAN based on IP subnet	45
2.2.11 Configuring the VLAN based on protocol	45
2.2.12 Querying VLAN statistics.....	46
2.2.13 Checking configurations	46
2.2.14 Example for configuring VLANs.....	47
2.3 Voice VLAN.....	49
2.3.1 Introduction.....	49
2.3.2 Preparing for configurations	50
2.3.3 Default configurations of the voice VLAN.....	50
2.3.4 Configuring the OUI	51
2.3.5 Enabling the voice VLAN.....	51
2.3.6 Checking configurations	52
2.3.7 Example for adding interfaces to the voice VLAN	52
2.3.8 Example for configuring the IP phone to access voice VLAN packets through LLDP	53

2.4 QinQ.....	55
2.4.1 Introduction.....	55
2.4.2 Preparing for configurations	56
2.4.3 Default configurations of QinQ	57
2.4.4 Configuring basic QinQ.....	57
2.4.5 Configuring selective QinQ	57
2.4.6 Configuring the network-side interface to Trunk mode	58
2.4.7 Configuring the TPID	58
2.4.8 Checking configurations	58
2.4.9 Example for configuring basic QinQ	59
2.4.10 Example for configuring selective QinQ and adding outer VLAN tag to tagged packets	60
2.4.11 Example for configuring selective QinQ and adding double VLAN tags to untagged packets	62
2.5 VLAN mapping.....	63
2.5.1 Introduction.....	63
2.5.2 Preparing for configurations	64
2.5.3 Default configurations of VLAN mapping	64
2.5.4 Configuring VLAN mapping	64
2.5.5 Checking configurations	65
2.5.6 Example for configuring VLAN mapping	65
2.6 MRP/VRP	67
2.6.1 Introduction.....	67
2.6.2 Preparing for configurations	70
2.6.3 Default configurations.....	70
2.6.4 Configuring basic functions of MVRP.....	70
2.6.5 Checking configurations	71
2.6.6 Example for configuring MVRP	71
2.7 VTP	74
2.7.1 Introduction.....	74
2.7.2 Preparing for configurations	75
2.7.3 Default configurations.....	75
2.7.4 Configuring basic functions of VTP	76
2.7.5 Checking configurations	76
2.7.6 Example for configuring VTP.....	76
3 IP services	81
3.1 IP basis	81
3.1.1 Introduction.....	81
3.1.2 Preparing for configurations	82
3.1.3 Default configurations of VLAN interface	82
3.1.4 Configuring the IPv4 address of the VLAN interface	82
3.1.5 Configuring the IPv6 address of the interface.....	82
3.1.6 Checking configurations	83

3.1.7 Example for configuring the VLAN interface to interconnect with the host	83
3.2 Loopback interface	85
3.2.1 Introduction.....	85
3.2.2 Preparing for configurations	85
3.2.3 Default configurations of the Loopback interface.....	86
3.2.4 Configuring the IP address of the Loopback interface	86
3.2.5 Checking configurations	86
3.3 ARP	86
3.3.1 Introduction.....	86
3.3.2 Preparing for configurations	87
3.3.3 Default configurations of ARP	87
3.3.4 Configuring static ARP entries.....	87
3.3.5 Configuring dynamic ARP entries	88
3.3.6 Checking configurations	88
3.3.7 Maintenance.....	88
3.3.8 Example for configuring ARP.....	88
3.4 NDP.....	90
3.4.1 Introduction.....	90
3.4.2 Preparing for configurations	91
3.4.3 Default configurations of NDP	91
3.4.4 Configuring static neighbor entries.....	92
3.4.5 Configuring the aging time of dynamic NDPs.....	92
3.4.6 Checking configurations	92
3.4.7 Maintenance.....	92
3.5 Static route	93
3.5.1 Introduction.....	93
3.5.2 Preparing for configurations	93
3.5.3 Configuring the static route.....	93
3.5.4 Checking configurations	94
3.5.5 Example for configuring the static route	94
3.6 Policy route	96
3.6.1 Introduction.....	96
3.6.2 Preparing for configurations	97
3.6.3 Configuring the static route.....	97
3.6.4 Checking configurations	97
3.6.5 Example for configuring policy route based on ACL	98
3.7 BGP.....	99
3.7.1 Introduction.....	99
3.7.2 Preparing for configurations	110
3.7.3 Default configurations.....	110
3.7.4 Configuring basic functions of BGP	110
3.7.5 Simplifying IBGP network connection	111

3.7.6 Configuring BGP route selection and load balancing	112
3.7.7 Controlling advertisement and receiving of BGP routes	112
3.7.8 Controlling and adjusting the convergence speed of the BGP network	113
3.7.9 Configuring BGP reliability	114
3.7.10 Checking configurations	114
3.7.11 Example for configuring basic functions of BGP	114
3.7.12 Example for configuring interaction between BGP and IGP	118
3.7.13 Example for configuring BGP route aggregation.....	121
3.7.14 Example for configuring BGP community.....	124
3.7.15 Example for configuring BGP route reflector	127
3.7.16 Example for configuring BGP confederation.....	129
3.7.17 Example for configuring BGP route selection	133
3.8 OSPFv2	138
3.8.1 Introduction.....	138
3.8.2 Preparing for configurations	150
3.8.3 Default configurations.....	151
3.8.4 Configuring basic functions of OSPF	151
3.8.5 Configuring the OSPF Stub area.....	152
3.8.6 Configuring the OSPF NSSA area	153
3.8.7 Configure OSPF to redistribute external routes	153
3.8.8 Configuring OSPF route aggregation.....	154
3.8.9 Configuring OSPF virtual connection.....	154
3.8.10 Configuring OSPF authentication	155
3.8.11 Checking configurations	156
3.8.12 Example for configuring basic functions of OSPF	156
3.8.13 Example for configuring the OSPF Stub area	160
3.8.14 Example for configuring the OSPF NSSA area	162
3.8.15 Configuring OSPF to redistribute external routes.....	165
3.8.16 Example for configuring OSPF route aggregation.....	167
3.8.17 Example for configuring OSPF virtual connection	172
3.8.18 Example for configuring OSPF authentication	177
3.9 OSPFv3	180
3.9.1 Introduction.....	180
3.9.2 Preparing for configurations	192
3.9.3 Default configurations.....	192
3.9.4 Configuring basic functions of OSPFv3	193
3.9.5 Configuring the OSPFv3 Stub area.....	194
3.9.6 Configuring the OSPFv3 NSSA area	194
3.9.7 Configure OSPFv3 to redistribute external routes	194
3.9.8 Configuring OSPFv3 route aggregation.....	195
3.9.9 Configuring OSPFv3 virtual connection.....	196
3.9.10 Checking configurations	196

3.9.11 Example for configuring basic functions of OSPFv3	197
3.9.12 Example for configuring the OSPFv3 Stub area	201
3.9.13 Example for configuring the OSPFv3 NSSA area	203
3.9.14 Configuring OSPFv3 to redistribute external routes	207
3.9.15 Example for configuring OSPFv3 route aggregation	210
3.9.16 Example for configuring OSPFv3 virtual connection	215
3.10 IS-IS	219
3.10.3 Default configurations.....	228
3.10.12 Example for configuring basic functions of IS-IS.....	233
3.10.13 Example for configuring ISIS DIS selection.....	237
3.10.14 Configuring IS-IS to redistribute external routes	242
3.10.15 Example for configuring IS-IS verification.....	244
3.11 IS-IS (IPv6)	247
3.11.3 Default configurations.....	248
3.11.12 Example for configuring basic functions of IS-IS (IPv6).....	253
3.12 RIP	257
3.12.1 Introduction.....	257
3.13 RIPng	271
3.13.1 Introduction.....	271
3.13.2 Preparing for configurations	272
3.13.3 Configuring basic functions of RIPng.....	272
3.13.4 Configuring RIPng route.....	273
3.13.5 Adjusting and optimizing the RIPng network	274
3.13.6 Checking results.....	275
3.13.7 Example for configuring basic functions of RIPng.....	276
3.13.8 Example for configuring RIPng to redistribute external routes	281
3.14 Routing policy	283
3.15 ECMP	296
3.15.1 Introduction.....	296
3.15.2 Preparing for configurations	296
3.15.3 Default configurations.....	296
3.15.4 Configuring the ECMP load balancing algorithm	296
3.15.5 Configuring the ECMP profile	297
3.15.6 Checking configurations	297
4 DHCP.....	298
4.1 DHCP Client	298
4.1.1 Introduction.....	298
4.1.2 Preparing for configurations	301
4.1.3 Default configurations of DHCP Client	301
4.1.4 Configuring DHCP Client	301
4.1.5 Checking configurations	302

4.1.6 Example for configuring DHCP Client	302
4.2 DHCP Server.....	304
4.2.1 Introduction.....	304
4.2.2 Preparing for configurations	306
4.2.3 Creating and configuring the IPv4 address pool	307
4.2.4 Enabling DHCP Server on the interface.....	307
4.2.5 Recycling the IP address pool	308
4.2.6 Configuring DHCPv4 Server PING.....	308
4.2.7 Checking configurations	308
4.2.8 Maintenance	309
4.2.9 Example for configuring DHCPv4 Server	309
4.3 DHCP Relay	310
4.3.1 Introduction.....	310
4.3.2 Preparing for configurations	311
4.3.3 Default configurations of DHCP Relay.....	311
4.3.4 Configuring interface DHCP Relay	312
4.3.5 Configuring interface DHCPv6 Relay	312
4.3.6 Configuring DHCP Relay to support Option 82	312
4.3.7 Configuring DHCP Relay to support Option 18/37	313
4.3.8 Checking configurations	314
4.3.9 Maintenance	314
4.3.10 Example for configuring DHCPv4 Relay	314
5 QoS.....	316
5.1 Introduction.....	316
5.1.1 Service models	316
5.2 Priority mapping.....	317
5.2.1 Introduction.....	317
5.2.2 Preparing for configurations	318
5.2.3 Default configurations of basic QoS	319
5.2.4 Configuring types of priorities trusted by the ingress interface	322
5.2.5 Configuring the diffserv profile	323
5.2.6 Configuring IEEE 802.1p/DSCP remarking on the egress interface	324
5.2.7 Checking configurations	324
5.3 Queue scheduling.....	324
5.3.1 Introduction.....	324
5.3.2 Preparing for configurations	326
5.3.3 Default configurations of queue scheduling.....	326
5.3.4 Configuring SP queue scheduling	327
5.3.5 Configuring WRR or SP+WRR queue scheduling	327
5.3.6 Configuring DRR or SP+DRR queue scheduling	327
5.3.7 Configuring queue bandwidth guarantee	328

5.3.8 Checking configurations	328
5.3.9 Maintenance	328
5.3.10 Example for configuring queue scheduling.....	329
5.4 Congestion avoidance	330
5.4.1 Introduction.....	330
5.4.2 Preparing for configurations	331
5.4.3 Default configurations of congestion avoidance	331
5.4.4 Configuring WRED	331
5.4.5 Checking configurations	332
5.5 Rate limiting.....	332
5.5.1 Introduction.....	332
5.5.2 Preparing for configurations	333
5.5.3 Configuring the rate limiting mode.....	333
5.5.4 Configuring rate limiting based on physical interface	333
5.5.5 Configuring rate limiting based on VLAN.....	334
5.5.6 Configuring rate limiting based on LAG	334
5.5.7 Checking configurations	334
5.5.8 Example for configuring rate limiting based on interface.....	335
5.6 Bandwidth rate limiting.....	336
5.6.1 Introduction.....	336
5.6.2 Preparing for configurations	337
5.6.3 Default configurations of bandwidth rate limiting	337
5.6.4 Configuring bandwidth guarantee	337
5.6.5 Checking configurations	341
5.7 ACL-based simplified traffic policy	341
5.7.1 Introduction.....	341
5.7.2 Preparing for configurations	341
6 Multicast	350
6.1 Multicast.....	350
6.2 IGMP Snooping.....	356
6.2.1 Introduction.....	356
6.2.2 Preparing for configurations	356
6.2.3 Default configurations of IGMP Snooping	357
6.2.4 Configuring basic functions of IGMP Snooping.....	357
6.2.5 Configuring IGMP Snooping Querier.....	358
6.2.6 Configuring IGMP Snooping packet suppression	359
6.2.7 Configuring IGMP Snooping multicast copy	359
6.2.8 Configuring the static multicast member of IGMP Snooping	359
6.2.9 Configuring IGMP Snooping Proxy.....	360
6.2.10 Configuring the limit on the number of IGMP Snooping interface multicast groups	360
6.2.11 Configuring the multicast policy of IGMP Snooping.....	361

6.2.12 Configuring the static router interface	361
6.2.13 Configuring IGMP Snooping SSM Mapping	362
6.2.14 Configuring IGMP Snooping multicast MVR	362
6.2.15 Checking configurations	363
6.2.16 Maintenance	363
6.2.17 Example for configuring basic functions of IGMP Snooping	363
6.2.18 Example for configuring the static member of IGMP Snooping	365
6.2.19 Example for configuring IGMP Snooping multicast copy	368
6.2.20 Example for configuring IGMP Snooping Proxy	370
6.2.21 Example for configuring the multicast policy of IGMP Snooping	372
6.3 MLD Snooping	374
6.3.1 Introduction	374
6.3.2 Preparing for configurations	375
6.3.3 Default configurations of MLD Snooping	375
6.3.4 Configuring basic functions of MLD Snooping	376
6.3.5 Configuring MLD Snooping Querier	376
6.3.6 Configuring MLD Snooping packet suppression	377
6.3.7 Configuring MLD Snooping multicast copy	377
6.3.8 Configuring the static multicast member of MLD Snooping	378
6.3.9 Configuring MLD Snooping Proxy	378
6.3.10 Configuring the limit on the number of MLD Snooping interface multicast groups	378
6.3.11 Configuring the multicast policy of MLD Snooping	379
6.3.12 Configuring MLD Snooping SSM Mapping	379
6.3.13 Configuring MLD Snooping multicast MVR	380
6.3.14 Checking configurations	380
6.3.15 Maintenance	381
6.3.16 Example for configuring basic functions of MLD Snooping	381
6.3.17 Example for configuring the static member of MLD Snooping	383
6.3.18 Example for configuring MLD Snooping multicast copy	385
6.3.19 Example for configuring MLD Snooping Proxy	387
6.3.20 Example for configuring the multicast policy of MLD Snooping	389
6.4 IGMP	392
6.4.1 Introduction	392
6.4.2 Preparing for configurations	392
6.4.3 Default configurations of IGMP	392
6.4.4 Enabling IGMP	393
6.4.5 Configuring parameters of the IGMP querier	393
6.4.6 Configuring IGMP immediate leave	394
6.4.7 Checking configurations	394
6.4.8 Maintenance	394
6.4.9 Example for configuring basic functions of IGMP	395
6.5 PIM	397

6.5.1 Introduction.....	397
6.5.2 Preparing for configurations	398
6.5.3 Default configurations of PIM	398
6.5.4 Configuring PIM-DM	399
6.5.5 Configuring PIM-SM	399
6.5.6 Configuring the BSR management domain of PIM-SM	399
6.5.7 Checking configurations	400
6.5.8 Maintenance	400
6.5.9 Example for configuring PIM-DM	401
6.5.10 Example for configuring PIM-SM	406
6.6 MLD	412
6.6.1 Introduction.....	412
6.6.2 Preparing for configurations	413
6.6.3 Default configurations of MLD	413
6.6.4 Enabling MLD	413
6.6.5 Configuring parameters of the MLD querier	414
6.6.6 Configuring MLD immediate leave	414
6.6.7 Checking configurations	414
6.6.8 Maintenance	415
6.6.9 Example for configuring basic functions of MLD	415
6.7 PIMv6.....	415
6.7.1 Introduction.....	415
6.7.2 Preparing for configurations	415
6.7.3 Default configurations of PIMv6	415
6.7.4 Configuring PIMv6-DM	416
6.7.5 Configuring PIM-SM	416
6.7.6 Configuring the BSR management domain of PIM-SM	416
6.7.7 Checking configurations	417
6.7.8 Maintenance	417
6.7.9 Example for configuring PIMv6-DM	417
6.7.10 Example for configuring PIMv6-SM	418
7 OAM	419
7.1 Introduction.....	419
7.2 EFM	421
7.2.1 Introduction.....	421
7.2.2 Preparing for configurations	421
7.2.3 Default configurations of EFM	421
7.2.4 Configuring basic functions of EFM.....	422
7.2.5 Configuring CFM interface loopback	423
7.2.6 Configuring EFM link performance monitoring	424
7.2.7 Configuring EFM link fault detection	425

7.2.8 Checking configurations	425
7.2.9 Maintenance	426
7.3 Link-state tracking	426
7.3.1 Introduction.....	426
7.3.2 Preparing for configurations	426
7.3.3 Default configurations of link-state tracking	427
7.3.4 Configuring link-state tracking	427
7.3.5 Checking configurations	427
7.3.6 Example for configuring link-state tracking	428
7.4 VRRP	430
7.4.1 Introduction.....	430
7.4.2 Preparing for configurations	432
7.4.3 Default configurations of VRRP	433
7.4.4 Configuring the VRRP backup group	433
7.4.5 Configuring the VRRP6 backup group	435
7.4.6 Configuring VRRP Trap.....	436
7.4.7 Configuring the VRRP monitoring interface	436
7.4.8 Configuring BFD for VRRP	437
7.4.9 Configuring NQA for VRRP.....	437
7.4.10 Checking configurations	438
7.4.11 Example for configuring VRRP master/backup	438
7.4.12 Example for configuring the VRRP monitoring interface.....	441
7.4.13 Example for configuring VRRP to monitor the BFD status	443
7.4.14 Example for configuring VRRP to monitor the NQA status	446
7.5 CFM	449
7.5.1 Introduction.....	449
7.5.2 Preparing for configurations	452
7.5.3 Default configurations of CFM	452
7.5.4 Configuring basic functions of CFM	452
7.5.5 Configuring fault detection	453
7.5.6 Configuring fault acknowledgement.....	454
7.5.7 Configuring fault location	454
7.5.8 Configuring alarm inhibition	455
7.5.9 Configuring the one-way packet loss test	455
7.5.10 Configuring the round-trip delay test	456
7.5.11 Checking configurations	456
7.5.12 Example for configuring CFM.....	457
8 Security.....	462
8.1 ACL	462
8.1.1 Introduction.....	462
8.1.2 Preparing for configurations	463

8.1.3 Configuring the ACL	463
8.1.4 Applying the ACL	465
8.1.5 Configuring statistics	466
8.1.6 Configuring rate limiting	466
8.1.7 Configuring the time range	467
8.1.8 Checking configurations	467
8.1.9 Maintenance	467
8.1.10 Example for configuring ACL	468
8.2 AAA	469
8.2.1 Introduction.....	469
8.2.2 Preparing for configurations	471
8.2.3 Default configurations of AAA	471
8.2.4 Configuring the RADIUS server.....	471
8.2.5 Configuring the TACACS+ server	472
8.2.6 Configuring the AAA server group	473
8.2.7 Configuring the AAA mode	473
8.2.8 Checking configurations	474
8.2.9 Example for configuring AAA.....	474
8.3 802.1x.....	477
8.3.1 Introduction.....	477
8.3.2 Preparing for configurations	479
8.3.3 Default configurations of 802.1x	479
8.3.4 Configuring basic functions of 802.1x	480
8.3.5 Configuring 802.1x re-authentication	481
8.3.6 Configuring 802.1x timers	482
8.3.7 Checking configurations	482
8.3.8 Example for configuring 802.1x	482
8.4 PPPoE+	484
8.4.1 Introduction.....	484
8.4.2 Preparing for configurations	485
8.4.3 Default configurations of PPPoE+	486
8.4.4 Configuring basic functions of PPPoE+.....	486
8.4.5 Configuring PPPoE+ packets.....	487
8.4.6 Checking configurations	489
8.4.7 Maintenance	489
8.4.8 Example for configuring PPPoE+	490
8.5 Port security MAC	492
8.5.1 Introduction.....	492
8.5.2 Preparing for configurations	493
8.5.3 Default configurations of port security MAC	493
8.5.4 Configuring basic functions of port security MAC	493
8.5.5 Configuring the sticky secure MAC address.....	494

8.5.6 Checking configurations	495
8.5.7 Maintenance	495
8.5.8 Example for configuring port security MAC	495
8.6 Storm suppression and storm control	497
8.6.1 Introduction.....	497
8.6.2 Preparing for configurations	498
8.6.3 Default configurations of storm suppression and storm control	499
8.6.4 Configuring storm suppression	499
8.6.5 Checking configurations	500
8.6.6 Example for configuring storm suppression	500
8.6.7 Configuring storm control.....	502
8.6.8 Checking configurations	502
8.6.9 Example for configuring storm control	503
8.7 ARP attack protection.....	504
8.7.1 Introduction.....	504
8.7.2 Preparing for configurations	504
8.7.3 Default configurations of ARP attack protection	504
8.7.4 Configuring ARP	504
8.7.5 Checking configurations	506
8.7.6 Example for configuring ARP attack protection	506
8.8 ND Snooping.....	508
8.8.1 Introduction.....	508
8.8.2 Preparing for configurations	509
8.8.3 Default configurations of ND Snooping	509
8.8.4 Configuring ND Snooping	509
8.8.5 Checking configurations	510
8.8.6 Example for configuring ND Snooping	510
8.9 DHCP Snooping.....	512
8.9.1 Introduction.....	512
8.9.2 Preparing for configurations	513
8.9.3 Default configurations of DHCP Snooping.....	514
8.9.4 Configuring DHCP Snooping	514
8.9.5 Configure DHCP Snooping to support Option 82.....	515
8.9.6 Configuring DHCPv6 Snooping	516
8.9.7 Checking configurations	517
8.9.8 Maintenance.....	517
8.9.9 Example for configuring DHCP Snooping.....	518
8.10 IP Source Guard	519
8.10.1 Introduction.....	519
8.10.2 Preparing for configurations	521
8.10.3 Default configurations of IP Source Guard	521
8.10.4 Configuring IP Source Guard binding.....	521

8.10.5 Configuring the interface trust status of IP Source Guard.....	522
8.10.6 Checking configurations	522
8.10.7 Example for configuring IP Source Guard	522
8.11 CPU attack protection	524
8.11.1 Introduction	524
8.11.2 Preparing for configurations.....	524
8.11.3 Configuring rate limiting for CPU attack protection.....	525
8.11.4 Configuring attack traceability for CPU attack protection	526
8.11.5 Checking configurations	527
8.11.6 Maintenance	527
8.11.7 Example for configuring CPU attack protection	527
8.12 MAC address authentication	530
8.12.1 Introduction.....	530
8.12.2 Default configurations.....	530
8.12.3 Configuring MAC address authentication.....	531
8.12.4 Example for configuring MAC address authentication.....	532
8.13 URPF.....	534
8.13.1 Introduction.....	534
8.13.2 Preparing for configurations	534
8.13.3 Configuring global URPF	535
8.13.4 Checking configurations	535
8.14 Time range.....	535
8.14.1 Introduction.....	535
8.14.2 Preparing for configurations	536
8.14.3 Configuring time range	536
8.14.4 Checking configurations	537
8.15 DOS attack prevention	538
8.15.1 Introduction.....	538
8.15.2 Preparing for configurations	539
8.15.3 Default configurations of DOS attack prevention	540
8.15.4 Configuring abnormal packet attack prevention	540
8.15.5 Configuring fragmented packet attack prevention	540
8.15.6 Configuring TCP SYN flood attack prevention	541
8.15.7 Configuring UDP flood attack prevention	541
8.15.8 Configuring ICMP flood attack prevention.....	541
8.15.9 Checking configurations	541
8.15.10 Example for configuring DOS attack prevention.....	542
9 Reliability	544
9.1 Link aggregation	544
9.1.1 Introduction.....	544
9.1.2 Preparing for configurations	545

9.1.3 Default configurations of link aggregation	545
9.1.4 Configuring manual link aggregation	546
9.1.5 Configuring static LACP link aggregation.....	546
9.1.6 Configuring master/slave link aggregation	547
9.1.7 Configuring the load balancing algorithm for the LAG	548
9.1.8 Checking configurations	548
9.1.9 Example for configuring static LACP link aggregation	549
9.2 G.8031.....	551
9.2.1 Introduction.....	551
9.2.2 Preparing for configurations	552
9.2.3 Default configurations of G.8031	553
9.2.4 Creating a G.8031 protection group	553
9.2.5 (Optional) configuring G.8031 switching control	554
9.2.6 Checking configurations	554
9.2.7 Example for configuring G.8031	555
9.3 G.8032.....	557
9.3.1 Introduction.....	557
9.3.2 Preparing for configurations	561
9.3.3 Default configurations of G.8032	562
9.3.4 Creating a G.8032 ring.....	562
9.3.5 Creating a G.8032 tributary ring	563
9.3.6 Configuring G.8032 switching control.....	565
9.3.7 Checking configurations	565
9.3.8 Maintenance.....	565
9.3.9 Example for configuring single ring G.8032	566
9.3.10 Example for configuring intersecting G.8032	568
9.4 STP/RSTP	571
9.4.1 Introduction.....	571
9.4.2 Preparation for configuration	574
9.4.3 Default configurations of STP	574
9.4.4 Enabling STP	575
9.4.5 Configuring STP parameters.....	575
9.4.6 Configuring the root/backup bridge	576
9.4.7 Configuring the RSTP edge interface	576
9.4.8 Configuring the RSTP link type.....	577
9.4.9 Checking configurations	577
9.4.10 Example for configuring STP	578
9.5 MSTP	581
9.5.1 Introduction.....	581
9.5.2 Preparation for configuration	584
9.5.3 Default configurations of MSTP	584
9.5.4 Enabling MSTP.....	585

9.5.5 Configuring the MST region and its maximum number of hops	585
9.5.6 Configuring the root/backup bridge	586
9.5.7 Configuring the interface priority and system priority	587
9.5.8 Configuring the path cost of the interface	588
9.5.9 Configuring the maximum transmission rate on interface	588
9.5.10 Configuring the MSTP timer.....	588
9.5.11 Configuring the edge interface.....	589
9.5.12 Configuring BPDU filtering.....	590
9.5.13 Configuring BPDU Guard.....	590
9.5.14 Configuring STP/RSTP/MSTP mode switching	591
9.5.15 Configuring the link type	592
9.5.16 Configuring root interface protection.....	592
9.5.17 Configuring interface loop guard	593
9.5.18 Configuring TC packet suppression	593
9.5.19 Configuring TC protection.....	594
9.5.20 Checking configurations	594
9.5.21 Maintenance	594
9.5.22 Example for configuring MSTP.....	595
9.6 Loop detection.....	598
9.6.1 Introduction.....	598
9.6.2 Preparing for configurations	600
9.6.3 Default configurations of loop detection.....	600
9.6.4 Configuring loop detection	601
9.6.5 Checking configurations	601
9.6.6 Example for configuring inner loop detection	601
9.7 Interface backup	603
9.7.1 Introduction.....	603
9.7.2 Preparing for configurations	605
9.7.3 Default configurations of interface backup	605
9.7.4 Configuring basic functions of interface backup	606
9.7.5 Configuring FS on interfaces	606
9.7.6 Checking configurations	607
9.7.7 Example for configuring interface backup.....	607
9.8 Interface isolation.....	609
9.8.1 Introduction.....	609
9.8.2 Preparing for configurations	610
9.8.3 Default configurations of interface isolation.....	610
9.8.4 Configuring interface isolation	610
9.8.5 Checking configurations	610
9.8.6 Example for configuring interface isolation.....	611
9.9 L2CP	612
9.9.1 Introduction.....	612

9.9.2 Preparing for configurations	612
9.9.3 Default configurations.....	613
9.9.4 Configuring L2CP	613
9.9.5 Checking configurations	614
9.9.6 Example for configuring L2CP	614
9.10 BFD	615
9.10.1 Introduction.....	615
9.10.2 Preparing for configurations	615
9.10.3 Default configurations.....	615
9.10.4 Configuring BFD static session detection	616
9.10.5 Configuring one-arm echo for BFD	616
9.10.6 Configuring BFD to detection layer 3 eth-trunk	616
9.10.7 Configuring parameters of the BFD session	617
9.10.8 Checking configurations	617
9.10.9 Example for configuring single-hop BFD.....	617
9.11 Link flap protection.....	619
9.11.1 Introduction.....	619
9.11.2 Preparing for configurations.....	619
9.11.3 Default configurations of link flap protection	619
9.11.4 Configuring link flap protection.....	619
9.11.5 Checking configurations	620
9.11.6 Example for configuring link flap protection.....	620
9.12 Interface loopback.....	621
9.12.1 Introduction.....	621
9.12.2 Preparing for configurations	621
9.12.3 Default configurations of interface loopback.....	621
9.12.4 Configuring interface loopback.....	621
9.12.5 Checking configurations	621
9.12.6 Example for configuring interface loopback.....	622
10 System management.....	623
10.1 SNMP.....	624
10.1.1 Introduction.....	624
10.1.2 Preparing for configurations	625
10.1.3 Default configurations of SNMP	625
10.1.4 Configuring basic functions of SNMPv1/SNMPv2c	626
10.1.5 Configuring basic functions of SNMPv3	627
10.1.6 Configuring other information about SNMP	628
10.1.7 Configuring Trap.....	629
10.1.8 Checking configurations	630
10.1.9 Example for configuring SNMPv1/SNMPv2c and Trap.....	630
10.1.10 Example for configuring SNMPv3 and Trap	632

10.2 RMON.....	634
10.2.1 Introduction.....	634
10.2.2 Preparing for configurations	636
10.2.3 Default configurations of RMON	636
10.2.4 Configuring RMON statistics	636
10.2.5 Configuring RMON history statistics	637
10.2.6 Configuring the RMON alarm group	637
10.2.7 Configuring the RMON event group	638
10.2.8 Checking configurations	638
10.2.9 Maintenance	638
10.2.10 Example for configuring the RMON alarm group	639
10.3 LLDP.....	641
10.3.1 Introduction.....	641
10.3.2 Preparing for configurations	643
10.3.3 Default configurations of LLDP	643
10.3.4 Enabling global LLDP	644
10.3.5 Enabling interface LLDP	644
10.3.6 Configuring basic functions of global LLDP	645
10.3.7 Configuring basic functions of interface LLDP	645
10.3.8 Configuring the LLDP alarm	646
10.3.9 Configuring TLV	646
10.3.10 Checking configurations	648
10.3.11 Maintenance	648
10.3.12 Example for configuring LLDP	648
10.4 Port mirroring.....	651
10.4.1 Introduction.....	651
10.4.2 Preparing for configurations	652
10.4.3 Default configurations of port mirroring.....	652
10.4.4 Configuring port mirroring	653
10.4.5 Checking configurations	653
10.4.6 Example for configuring port mirroring.....	654
10.4.7 Example for configuring remote port mirroring.....	655
10.5 Cable diagnosis	656
10.5.1 Introduction.....	656
10.5.2 Preparing for configurations	656
10.5.3 Configuring cable diagnosis.....	656
10.5.4 Checking configurations	656
10.6 UDLD.....	657
10.6.1 Introduction.....	657
10.6.2 Preparing for configurations	657
10.6.3 Default configurations of UDLD	657
10.6.4 Configuring UDLD	658

10.6.5 Checking configurations	658
10.7 Optical module DDM	660
10.7.1 Introduction.....	660
10.7.2 Preparing for configurations	660
10.7.3 Default configurations of optical module DDM	660
10.7.4 Enabling optical module DDM	660
10.7.5 Enabling optical module DDM Trap.....	661
10.7.6 Checking configurations	662
10.8 System log	662
10.8.1 Introduction.....	662
10.8.2 Preparing for configurations	663
10.8.3 Default configurations of system log	663
10.8.4 Configuring basic information about the system log	664
10.8.5 Configuring system log output.....	664
10.8.6 Configuring system log output to Telnet/SSH terminals.....	665
10.8.7 Configuring system log output to the syslog server	665
10.8.8 Checking configurations	666
10.8.9 Maintenance	667
10.8.10 Example for configuring outputting system logs to the log host.....	667
10.9 Alarm management	668
10.9.1 Introduction.....	668
10.9.2 Preparing for configurations	669
10.9.3 Configuring basic functions of alarm management	669
10.9.4 Checking configurations	669
10.10 CPU monitoring	670
10.10.1 Introduction.....	670
10.10.2 Preparing for configurations	670
10.10.3 Default configurations of CPU monitoring.....	671
10.10.4 Configuring the CPU monitoring alarm.....	671
10.10.5 Checking configurations	671
10.11 Memory monitoring	672
10.11.1 Introduction	672
10.11.2 Preparing for configurations.....	672
10.11.3 Configuring memory monitoring	672
10.11.4 Checking configurations	673
10.12 PING	673
10.12.1 Introduction.....	673
10.12.2 Configuring PING.....	673
10.13 Trace.....	674
10.13.1 Introduction.....	674
10.13.2 Configuring IPv4 Trace.....	675
10.13.3 Configuring IPv6 Trace.....	676

10.14 Hardware monitoring	676
10.14.1 Introduction.....	676
10.14.2 Configuring temperature monitoring	676
10.14.3 Configuring power supply monitoring.....	677
10.14.4 Checking configurations	677
10.15 Fan monitoring.....	678
10.15.1 Introduction.....	678
10.15.2 Preparing for configurations	678
10.15.3 Configuring fan monitoring	678
10.15.4 Checking configurations	679
10.16 ISF.....	679
10.16.1 Introduction.....	679
10.16.2 Default configurations.....	682
10.16.3 Configuring ISF	682
10.16.4 Example for configuring ISF	683
10.17 MAD	685
10.17.1 Introduction.....	685
10.17.2 Preparing for configurations	686
10.17.3 Configuring MAD.....	687
10.17.4 Example for configuring MAD	687
10.18 NQA	689
10.18.1 Introduction.....	689
10.18.2 Preparing for configurations	689
10.18.3 Default configurations.....	689
10.18.4 Configure the ICMP-echo test	689
10.18.5 Configuring the UDP-echo test.....	690
10.18.6 Configuring the TCP test.....	691
10.18.7 Configuring the DNS test.....	692
10.18.8 Configuring the HTTP test.....	693
10.18.9 Configuring the FTP test	694
10.18.10 Configuring the SNMP test	694
10.18.11 Configuring test history recording	695
10.18.12 Configuring test statistics	695
10.18.13 Configuring test Trap	696
10.18.14 Checking results	696
10.18.15 Maintenance.....	696
10.18.16 Example for configuring the ICMP-echo test	697
10.19 POE	699
10.19.1 Introduction.....	699
10.19.2 Preparing for configurations	699
10.19.3 Default configurations of PoE.....	699
10.19.4 Enabling PoE	700

10.19.5 Configuring the maximum output power of PoE	700
10.19.6 Configuring power-on and power-off of PoE.....	700
10.19.7 Configuring smart PoE.....	701
10.19.8 Configuring the PD description	702
10.19.9 Checking configurations	702
10.19.10 Maintenance.....	702
10.19.11 Example for configuring PoE.....	702
10.19.12 Example for configuring Smart PoE	704
10.20 Patching.....	705
10.20.1 Introduction.....	705
10.20.2 Preparing for configurations	705
10.20.3 Loading the patch file	705
10.20.4 Activating the patch file	706
10.20.5 Deactivating the patch file	706
10.20.6 Deleting the patch file.....	706
10.20.7 Checking configurations	706
10.20.8 Example for configuring patching.....	707
10.21 Periodically backing up configurations	707
10.21.1 Introduction.....	707
10.21.2 Preparing for configurations	708
10.21.3 Configuring time range	708
10.21.4 Configuring automatic uploading	709
10.21.5 Checking configurations	709
10.21.6 Example for configuring periodic backup.....	709
11 L3VPN services.....	711
11.1 Basic configurations of L3VPN	711
11.1.1 Introduction.....	711
11.1.2 Preparing for configurations.....	712
11.1.3 Creating a VPN instance	712
11.1.4 Binding the VLAN interface with the VPN instance	713
11.1.5 Checking configurations	713
11.1.6 Example for binding the VLAN interface with the VPN instance	713
11.1.7 Example for configuring MCE.....	714
12 GRE.....	721
12.1 Configuring GRE	721
12.1.1 Introduction.....	721
12.1.2 Preparing for configurations	721
12.1.3 Default configurations of GRE	721
12.1.4 Configuring the GRE tunnel	722
12.1.5 Checking configurations	722
12.1.6 Maintenance	723

12.1.7 Example for configuring GRE	723
13 Appendix	728
13.1 Terms	728
13.2 Acronyms and abbreviations	733

Figures

Figure 1-1 Accessing device through PC connected with RJ45 Console interface	2
Figure 1-2 Configuring communication parameters in Hyper Terminal	3
Figure 1-3 Networking with device as Telnet server	5
Figure 1-4 Networking with device as Telnet client	5
Figure 1-5 Basic principles of NTP	18
Figure 1-6 NTP networking	24
Figure 2-1 Forwarding packets according to the MAC address table	32
Figure 2-2 MAC networking	38
Figure 2-3 VLAN partitions	39
Figure 2-4 VLAN and interface isolation networking	47
Figure 2-5 Networking for IP phone to connect to switch	50
Figure 2-6 Networking with adding the interface to the voice VLAN and configuring it to work in the manual mode	52
Figure 2-7 Configuring IP phone to access voice VLAN packets through LLDP	54
Figure 2-8 Principles of basic QinQ	55
Figure 2-9 Basic QinQ networking	59
Figure 2-10 Selective QinQ networking	61
Figure 2-11 Principles of VLAN mapping	63
Figure 2-12 VLAN mapping networking	66
Figure 2-13 Principles of MVRP	69
Figure 2-14 MVRP networking	71
Figure 2-15 VTP principle networking	75
Figure 2-16 VTP application networking	77
Figure 3-1 VLAN interface networking	83
Figure 3-2 Configuring ARP networking	89
Figure 3-3 Principles of NDP address resolution	91

Figure 3-4 Configuring the static route	95
Figure 3-5 Policy route networking.....	98
Figure 3-6 AS_PATH attribute	102
Figure 3-7 NEXT_HOP attribute	103
Figure 3-8 MED attribute	104
Figure 3-9 LOCAL_PREF attribute	104
Figure 3-10 BGP route reflector.....	107
Figure 3-11 BGP route reflector	108
Figure 3-12 BGP confederation.....	108
Figure 3-13 Networking with basic functions of BGP	115
Figure 3-14 Networking with interaction between BGP and IGP	118
Figure 3-15 BGP route aggregation networking	121
Figure 3-16 BGP community networking	125
Figure 3-17 BGP route reflector networking.....	127
Figure 3-18 BGP confederation networking	130
Figure 3-19 BGP route selection application	133
Figure 3-20 OSPF area division	139
Figure 3-21 Example of OSPF router types	140
Figure 3-22 OSPF neighbor status machine	142
Figure 3-23 OSPF interface status machine	143
Figure 3-24 Flow for establishing the adjacency relationship on the OSPF broadcast network OSPF	145
Figure 3-25 OSPF NSSA area	148
Figure 3-26 Networking with basic functions of OSPF	157
Figure 3-27 OSPF Stub area networking	160
Figure 3-28 OSPF NSSA area networking.....	162
Figure 3-29 Networking with OSPF to redistribute external routes	165
Figure 3-30 OSPF route aggregation networking	168
Figure 3-31 OSPF virtual connection networking.....	173
Figure 3-32 OSPF authentication networking.....	177
Figure 3-33 OSPFv3 area division	182
Figure 3-34 Example of OSPFv3 router types	182
Figure 3-35 OSPFv3 neighbor status machine	184
Figure 3-36 OSPFv3 interface status machine	185

Figure 3-37 Flow for establishing the adjacency relationship on the OSPFv3 broadcast network OSPFv3	187
Figure 3-38 OSPFv3 NSSA area	190
Figure 3-39 Networking with basic functions of OSPFv3	197
Figure 3-40 OSPFv3 Stub area networking.....	201
Figure 3-41 OSPFv3 NSSA area networking	203
Figure 3-42 Networking with OSPFv3 to redistribute external routes	208
Figure 3-43 OSPFv3 route aggregation networking.....	210
Figure 3-44 OSPFv3 virtual connection networking.....	215
Figure 3-45 Pseudo node networking.....	221
Figure 3-46 Structure of the IS-IS address	222
Figure 3-47 Flow for establishing broadcast link neighbor relationship	224
Figure 3-48 Flow for synchronizing the LSDB in the P2P link	226
Figure 3-49 Flow for synchronizing the LSDB on the P2P link	227
Figure 3-50 Networking with basic functions of RIP.....	264
Figure 3-51 Networking with RIP to redistributing external routes	269
Figure 3-52 Networking with basic functions of RIP.....	276
Figure 3-53 Networking with RIPng to redistributing external routes	281
Figure 3-54 Networking with the routing policy in IPv4 route redistribution.....	290
Figure 3-55 Networking with the routing policy in IPv6 route redistribution.....	294
Figure 4-1 DHCP typical networking.....	299
Figure 4-2 Structure of a DHCP packet	299
Figure 4-3 DHCP Client networking.....	301
Figure 4-4 DHCP Client networking.....	303
Figure 4-5 DHCP Server and Client networking.....	305
Figure 4-6 Structure of a DHCP packet	305
Figure 4-7 DHCP Server networking	309
Figure 4-8 Typical application of DHCP Relay	311
Figure 4-9 DHCP Relay networking	315
Figure 5-1 SP scheduling	325
Figure 5-2 WRR scheduling.....	325
Figure 5-3 DRR scheduling.....	326
Figure 5-4 Queue scheduling networking	329
Figure 5-5 Rate limiting based on interface	335

Figure 6-1 Multicast transmission networking.....	351
Figure 6-2 Basic concepts in multicast.....	353
Figure 6-3 Mapping between IPv4 multicast address and multicast MAC address	354
Figure 6-4 Operating of IGMP and Layer 2 multicast features	354
Figure 6-5 IGMP Snooping networking.....	357
Figure 6-6 Configuring basic functions of IGMP Snooping	364
Figure 6-7 Configuring the static member of IGMP Snooping	366
Figure 6-8 Configuring IGMP Snooping multicast copy	368
Figure 6-9 Configuring IGMP Snooping Proxy	370
Figure 6-10 Configuring the multicast policy of IGMP Snooping	372
Figure 6-11 MLD Snooping networking	375
Figure 6-12 Configuring basic functions of MLD Snooping	381
Figure 6-13 Configuring the static member of MLD Snooping.....	383
Figure 6-14 Configuring MLD Snooping multicast copy	385
Figure 6-15 Configuring MLD Snooping Proxy	387
Figure 6-16 Configuring the multicast policy of MLD Snooping.....	389
Figure 6-17 Location of IGMP on the multicast network	392
Figure 6-18 Networking with basic functions of IGMP	395
Figure 6-19 Location of PIM on the multicast network	398
Figure 6-20 PIM-DM networking	401
Figure 6-21 PIM-SM networking.....	407
Figure 7-1 OAM loopback	420
Figure 7-2 Link-state tracking networking.....	428
Figure 7-3 VRRP principles	431
Figure 7-4 Principles of VRRP load balancing	432
Figure 7-5 Configuring VRRP master/backup	439
Figure 7-6 Configuring the VRRP monitoring interface	441
Figure 7-7 Configuring the VRRP to monitor the BFD status	444
Figure 7-8 Configuring the VRRP to monitor the NQA status.....	447
Figure 7-9 MDs at different levels	450
Figure 7-10 MEP and MIP	450
Figure 7-11 Typical CFM networking.....	457
Figure 8-1 ACL networking	468

Figure 8-2 Domain-based authentication application networking.....	475
Figure 8-3 802.1x structure	477
Figure 8-4 Dot1x networking.....	483
Figure 8-5 Accessing the network through PPPoE authentication	485
Figure 8-6 PPPoE+ networking.....	490
Figure 8-7 Port security MAC networking.....	496
Figure 8-8 Storm suppression networking	501
Figure 8-9 DAI networking.....	507
Figure 8-10 ND Snooping networking.....	511
Figure 8-11 DHCP Snooping	513
Figure 8-12 DHCP Snooping networking	518
Figure 8-13 Principles of IP Source Guard	520
Figure 8-14 Configuring IP Source Guard	523
Figure 8-15 MAC address authentication networking	532
Figure 8-16 DOS attack prevention.....	542
Figure 9-1 Static LACP mode Link aggregation networking.....	549
Figure 9-2 G.8031 networking	555
Figure 9-3 G.8032 ring networking.....	557
Figure 9-4 Idle state	559
Figure 9-5 Protecting state	559
Figure 9-6 Tributary ring.....	560
Figure 9-7 Single ring G.8032 networking.....	566
Figure 9-8 Intersecting ring G.8032 networking	569
Figure 9-9 Network storm due to loopback.....	572
Figure 9-10 Loop networking with STP.....	573
Figure 9-11 Failure in forwarding VLAN packets due to RSTP	574
Figure 9-12 STP networking	578
Figure 9-13 Basic concepts of the MSTI network.....	582
Figure 9-14 MSTI concepts.....	583
Figure 9-15 Networking with multiple spanning trees instances in MST region	584
Figure 9-16 MSTP networking.....	595
Figure 9-17 Loop detection networking	599
Figure 9-18 Loop detection networking.....	602

Figure 9-19 Principles of interface backup	604
Figure 9-20 Networking with interface backup in different VLANs	605
Figure 9-21 Interface backup networking	608
Figure 9-22 Interface isolation networking	611
Figure 9-23 BPDU Tunnel topology	613
Figure 9-24 Single-hop BFD networking.....	618
Figure 10-1 Principles of SNMP	624
Figure 10-2 SNMPv3 authentication mechanism.....	627
Figure 10-3 SNMPv1/SNMPv2c networking	631
Figure 10-4 SNMPv3 and Trap networking	632
Figure 10-5 RMON networking.....	635
Figure 10-6 RMON networking.....	639
Figure 10-7 Structure of a LLDPDU.....	641
Figure 10-8 Structure of a TLV packet.....	641
Figure 10-9 LLDP networking	649
Figure 10-10 Principles of port mirroring	652
Figure 10-11 Port mirroring networking	654
Figure 10-12 Remote port mirroring networking.....	655
Figure 10-13 Networking of outputting system log to log host	667
Figure 10-14 Principles of PING.....	673
Figure 10-15 Principles of Trace	675
Figure 10-16 Chain topology with 2 member devices	681
Figure 10-17 Ring topology with 2 member devices	681
Figure 10-18 Chain topology with 2 devices for ISF	683
Figure 10-19 Direction connection mode of MAD	686
Figure 10-20 Proxy mode of MAD	686
Figure 10-21 ICMP-echo test networking.....	697
Figure 11-1 Networking before deploying MCE	711
Figure 11-2 Networking after deploying MCE	712
Figure 12-1 GRE networking.....	723

Tables

Table 2-1 Interface mode and packet processing.....	40
Table 4-1 Fields of a DHCP packet	299
Table 4-2 Fields of a DHCP packet	305
Table 5-1 Default mapping from the IEEE 802.1p ingress direction to local priority and color	319
Table 5-2 Default mapping from the IEEE 802.1p egress direction to local priority and color	319
Table 5-3 Default mapping from the DSCP ingress direction to local priority and color	320
Table 5-4 Default mapping from the DSCP egress direction to local priority and color	321
Table 10-1 TLV types	641
Table 10-2 IEEE 802.1 organization-defined TLVs	642
Table 10-3 IEEE 802.3 organization-defined TLVs	642
Table 10-4 Log levels	663

1 Basic configurations

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

- Accessing device
- Loading and upgrade
- Time management
- Interface management

1.1 Accessing device

1.1.1 Introduction

The device can be configured and managed in Command Line Interface (CLI) mode, or Web mode.

The device CLI mode has a variety of configuration modes:

- Console mode: it must use Console mode in the first configuration. The Raisecom device supports the Console interface of the RJ45, M12, Micro USB, and Mini-USB types.
- Telnet mode: the default IP address of the device is 192.168.0.1. To modify it, log on through the Console mode, open Telnet service on the device, configure the IP address, configure the user name and password, use the new IP address, and then take remote Telnet configuration.
- SSH mode: before accessing the device through SSH, you need to log in to the device and start SSH services through the Console interface.

When configuring the device in Web mode, you must first configure the IP address of the VLAN interface on CLI, and then configure the device through the NView NNM system.

1.1.2 Accessing through the Console interface



Note

- The device supports the RJ45 Console interface.

- The device uses the black wiring Console cable. If you are not sure, see the corresponding User Manual or Product Description for this device, or consult our technical personnel.
- The following sections take the RJ45 Console interface for example.

Introduction

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

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

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

Default configurations of the Console interface

Default configurations of the Console interface are as below.

Function	Default value
Transmission rate	115200 baud
Flow control mode	None
Authentication mode	No authentication
Stop bit	1
Data bit	8

Accessing device through Console interface

If you want to access the device through PC through the Console interface, connect Console interface and PC RS-232 serial port, as shown in Figure 1-1; then run the terminal emulation program, such as Hyper Terminal in the Microsoft Windows XP, in PC to configure communication parameters as shown in Figure 1-2, and then log in to the device.

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

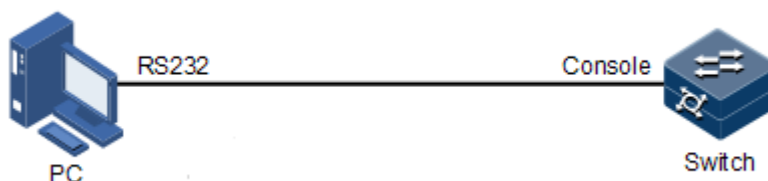
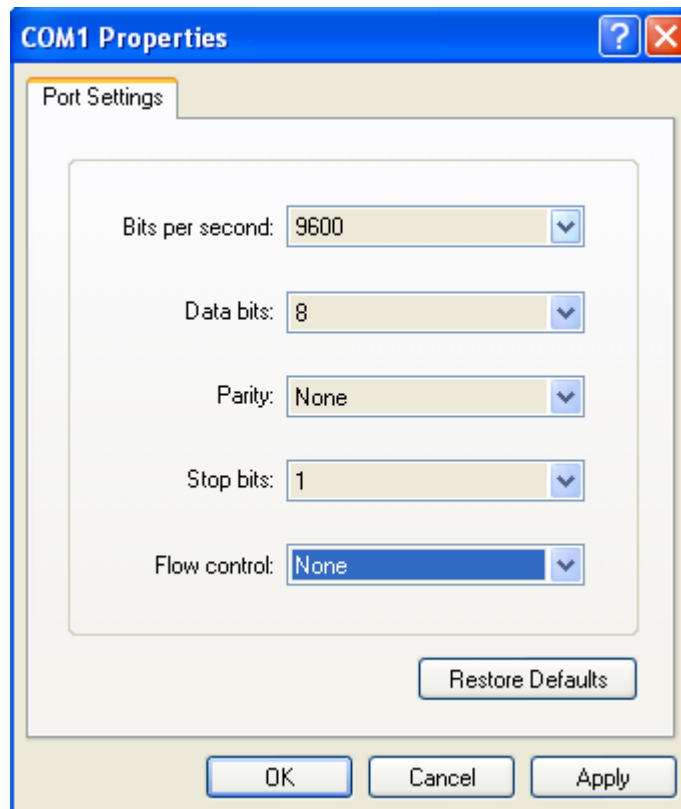


Figure 1-2 Configuring communication parameters in Hyper Terminal



Note

By default, the baud rate of the serial interface is 115200.

Configuring the baud rate of the Console interface

Configure the baud rate of the Console interface for the device as below.

Step	Command	Description
1	Raisecom# configure Raisecom(config)# line console Raisecom(config-line-console)# baudrate { 115200 9600 }	Modify the baud rate of the serial interface.

Configuring the password and authentication mode of the Console interface

Configure the password and authentication mode of the Console interface for the device as below.

Step	Command	Description
1	Raisecom# configure Raisecom(config)# line console password	Configure the password of the Console interface.

Step	Command	Description
2	<pre>Raisecom(config)#line console Raisecom(config-line-console)#login authentication { local password none }</pre>	Configure the authentication mode of the Console interface. • Local: user name password • Password: password of the Console interface • None: no authentication

Checking configurations

Use the following commands to check the configuration results.

No.	Command	Description
1	<pre>Raisecom#show line console information</pre>	Show configurations of the baud rate on the Console interface.

1.1.3 Accessing through Telnet

Introduction



Note

By default, the default management IP address of the device, and the subnet mask is 255.255.255.0. To modify the IP address, log in to the device and configure it. There are no default user name and password for the device. You need to create a user account through the Console interface or on the Telnet page with the default management IP address connection. In Telnet connection status, if you enter the password incorrectly for three 3 times, the Telnet connection will be automatically disconnected.

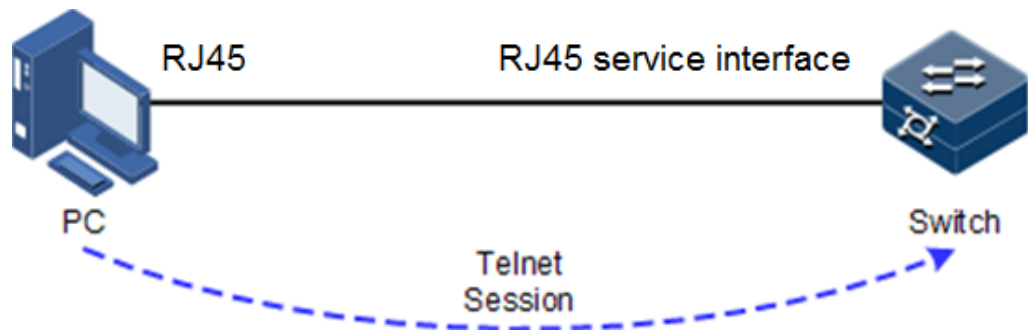
You can use a PC to log in to the device remotely through Telnet. You can log in to a device from PC at first, then Telnet another device on the network. You do not need to connect a PC to each device.

If there is an SNMP interface on the device, use it to log in through Telnet. If there is not, use any interface to enter the management VLAN, and log in through Telnet.

Telnet services provided by the device are as below:

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

Figure 1-3 Networking with device as Telnet server

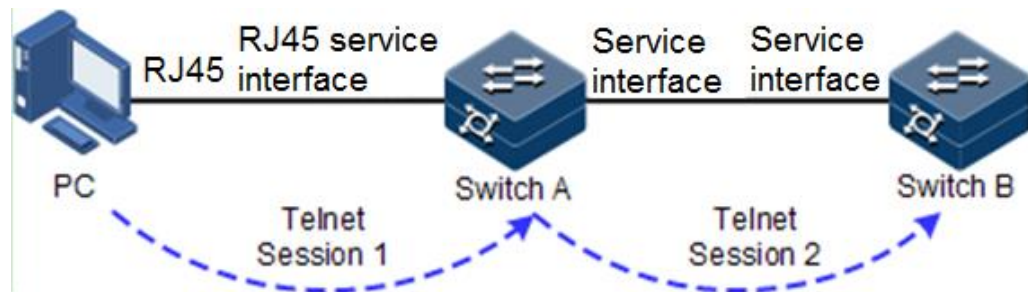


Note

The maximum number of Telnet users supported by the device is 10.

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

Figure 1-4 Networking with device as Telnet client



Default configurations of Telnet Server

Default configurations of Telnet Server are as below.

Function	Default value
Telnet Server status	Enable
Telnet Server listening port number	23
Interface enabled with Telnet Server	All interfaces
Maximum number of Telnet connections	10



Note

When you configure the device through Telnet, do not modify the IP address frequently; otherwise, the current Telnet connection may be disconnected. Then, you have to re-establish the Telnet connection with the new IP address.

Configuring Telnet Server

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

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i> Raisecom(config)#interface ge 1/0/1	Enter VLAN interface configuration mode or out-of-band network management interface configuration mode. Take VLAN interface configuration mode for example.
3	Raisecom(config-vlan*)#ip address <i>ip-address</i> [<i>ip-mask</i>] [<i>sub</i>] Raisecom(config-vlan*)#ipv6 address <i>ipv6-address/prefix-length</i> [<i>eui-64</i>] Raisecom(config-vlan*)#exit	Configure the IP address of the device.
4	Raisecom(config)#telnet server start	Enable Telnet Server.
5	Raisecom(config)#telnet server stop	Release the specified Telnet connection.
6	Raisecom(config)#telnet-ipv6 server start	Enable IPv6 Telnet Server.
7	Raisecom(config)#telnet-ipv6 server stop	Close the specified IPv6 Telnet connection.

Configuring the port number of the Telnet server

The default port number of the Telnet server is 23. You can modify it as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#telnet server port { <i>port-number</i> default }	Modify the port number of the IPv4 Telnet server
3	Raisecom(config)#telnet-ipv6 server start	Enable IPv6 Telnet Server.
4	Raisecom(config)#telnet-ipv6 server port { <i>port-number</i> default }	Modify the port number of the IPv6 Telnet server

Disabling Telnet port

Disable Telnet port on the device as below.

Step	Command	Description
1	<pre>Raisecom(config)#telnet server deny-interface ge 1/0/1* Raisecom(config)#telnet-ipv6 server deny-interface ge 1/0/1*</pre>	Disable a Telnet port from Telnet management. Then, you cannot log in through Telnet through this port. The connected Telnet sessions are not affected by this configuration.

Configuring Telnet Client

Configure Telnet Client on the device as below.

Step	Command	Description
1	<pre>Raisecom#telnet ipv4-address [-p port- id -s source-ipv4-address] Raisecom#telnet-ipv6 ipv6-address [-p port-id -s source-ipv6-address] *</pre>	Log in to another device through Telnet.

Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<pre>Raisecom#show running-config</pre>	Show configurations of Telnet Server.

1.1.4 Accessing through SSH

Introduction

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

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

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

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

The device supports password authentication and public key authentication.

- Password authentication: share the same database with the login authentication. The SSH client only needs to enter the user name and password for remote login to the SSH server. All the data to be transmitted are encrypted, but it cannot prevent attacks from rogue servers.
- Public key authentication: the SSHv2 client is authenticated by the user name, password, and key. Before login, a key pair is generated on the client side, including a host public key and a host private key. The former is stored in the SSH server. The data used for authentication and transmission are encrypted, which prevents attacks from rogue servers.

Default configurations of SSHv2

Default configurations for accessing the device through SSHv2 are as below.

Function	Default value
SSH server status	Disable
Local SSH key pair length	512 bits
Key renegotiation period	0h
SSH authentication method	password
SSH authentication timeout	600s
SSH snooping port number	22
SSH session status	Disable
SSH version	v2
SSH security algorithm mode	Disable

Configuring the SSH server

Configure the SSH server for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#ssh server start	Enable IPv4 SSH Server.
3	Raisecom(config)#ssh server stop	Disable IPv4 SSH Server.
4	Raisecom(config)#ssh-ipv6 server start	Enable IPv6 SSH Server.
5	Raisecom(config)#ssh-ipv6 server stop	Disable IPv6 SSH Server.

Configuring the port number of the SSH server

The default port number of the SSH server is 22. You can modify it as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#ssh server port { port-number default }	Modify the port number of the IPv4 SSH server
3	Raisecom(config)#ssh-ipv6 server start	Enable IPv6 SSH Server.
4	Raisecom(config)#ssh-ipv6 server port { port-number default }	Modify the port number of the IPv6 SSH server

Disabling SSH port

Disable SSH port on the device as below.

Step	Command	Description
1	Raisecom(config)#ssh server deny-interface ge 1/0/1* Raisecom(config)#ssh-ipv6 server deny-interface ge 1/0/1*	Disable a Telnet port from SSH management. Then, you cannot log in through SSH through this port. The connected SSH sessions are not affected by this configuration.

Checking configurations

Use the following commands to check the configuration results.

No.	Command	Description
1	Raisecom#show ssh config	Show SSH configurations.

1.1.5 Accessing from Web

Introduction

To facilitate users to configure and maintain the device, it supports Web network management. Users can use the Web network management to intuitively manage and configure devices under the graphical interface.

The web network management supports the following two text transmission protocols:

- Hypertext Transfer Protocol (HTTP): used to transmit information on Web pages on the network. After HTTP is enabled on the device, the user can log in to the device through HTTP, and access and control the device on the Web interface.
- Secure Hypertext Transfer Protocol (HTTPS): it uses the Secure Sockets Layer (SSL) protocol to ensure that legal clients can access the device in a secure mode. The data

exchanged between the client and the device needs to be encrypted to ensure the security and integrity of data transmission, so as to realize security management of the device.

After Web network management is enabled, remote users can log in to the device through the Web browser and manage it. After Web network management is disabled, all established HTTP/HTTPS connections are disconnected.

Default configurations of Web network management

Default configurations of Web network management are as below.

Function	Default value
HTTP status	Enable

Configuring Web network management

Configure Web network management for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#http server { start stop }	Enable HTTP. Use the stop form of this command to disable this function.
3	Raisecom(config)#https server { start stop }	Enable HTTPS. Use the stop form of this command to disable this function.

Checking configurations

Use the following commands to check the configuration results.

No.	Command	Description
1	Raisecom#show running-config	Show configurations of the device.

Configuring AAA for Web login

Configure AAA for Web login for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#http server login authentication aaa method method [auth-type { pap chap ascii }]	Enable AAA for Web login.

Step	Command	Description
3	Raisecom(config)#http server login authentication local	Enable local authentication for Web login.

1.1.6 Managing users

Introduction

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



Note

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

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

Default configurations of user management

Default configurations of user management are as below.

Function	Default value
Local user information	• User name: raisecom • Password: raisecom • Privilege: 15
New user privilege	15
New user activation status	Activate
New user service type	Console, telnet, SSH, FTP, and HTTP
Password complexity	3
User name complexity	1
Maximum length of the user name	64
Maximum length of the password	64
Defaultly supported special characters	~!@#\$%^&*()_-=+{}[]\ ;':<>"/

Configuring local user management

Configure local user management for the device as below.

Step	Command	Description
1	Raisecom(config)# username <i>user-name</i> password { cipher reversible-cipher plain } <i>password</i> group { administrators operators users guests } domain [telnet ssh http ftp console default all]]	Create or modify the user name and ciphertext password for login.
2	Raisecom(config)# username <i>user-name</i> domain [telnet ssh http ftp console default all] *	Modify the user group domain.
3	Raisecom(config)# username <i>user-name</i> group { administrators operators users guests }	Modify the user group.
4	Raisecom(config)# user password-complex { <i>complex</i> default }	Configure the password complexity.
4	Raisecom(config)# user password-length { <i>length</i> default }	Configure the minimum length of the password.
5	Raisecom(config)# user name-complex { <i>complex</i> default }	Configure the user name complexity. By default, it is 1.
6	Raisecom(config)# user name-length { <i>length</i> default }	Configure the length of the user name. By default, it is 1.
7	Raisecom(config)# username <i>user-name</i> { login-lock manual-lock unlock } [reauth-interval { <i>interval</i> default } fail-count { <i>count</i> default }] *	Configure the type of user locking to login-lock, which allows you to configure the login failure times and re-authentication interval.
8	Raisecom# show user name <i>user-name</i>	Show information about the user.
9	Raisecom# user special-characters <i>CHARLIST</i>	Configure the special characters that can be included in the user name and password.

Note

- Besides the default user, you can create up to 30 local user accounts.
- After configuring the type of user locking to login-lock, you can configure the login failure times and re-authentication interval. By default, the number of login failure times is 3, and the re-authentication interval is 10s. When the login failure times reaches the upper limit in the silence period, the device is in login locking status, so it cannot be logged in to. After the silence period expires, the locking will be released. Or you can use the **unlock** command to manually release the locking.
- If you manually lock login, the device will be permanently locked from login, regardless of the login failure times and re-authentication interval. You can use the **unlock** command to manually release the locking.

1.1.7 Restoring the user password

Introduction

When you forget the password for login, connect a PC to the Console interface on the device, open the Hyper Terminal, enter the temporary password view, obtain a temporary password Serial Number (SN), and generate the temporary password accordingly. After logging in to the device through the temporary password, you can modify the local password.



Note

The operation of restoring the password can be done on the Console terminal only. On the login interface, press **Ctrl+P** to enter the temporary password view. By default, the function of restoring the password is enabled.

Obtaining the temporary password

Step	Command	Description
1	Press Ctrl+P .	Enter the shortcut keys on the Console interface.
2	<code>Raisecom(key)#get temporary-password-serial</code>	Obtain a temporary password SN.
3	<code>Raisecom(key)#check temporary-password password</code>	Check the temporary password.
4	<code>Raisecom(config)#temporary-password { enable disable }</code>	Enable or disable the function of obtaining the temporary password.

1.1.8 Configuring properties of the terminal

Introduction

You can configure properties of the Console, Telnet, or SSH terminal, such as the number of lines in a page for page-by-page scrolling, timeout time, terminal color, case-sensitive input, and Man Machine Interaction (MMI) mode.

Configuring properties of the terminal

Step	Command	Description
1	<code>Raisecom(config)#terminal length { 0 length default }</code>	Configure the number of lines in a page for page-by-page scrolling. • 0: no page-by-page scrolling. The system shows all lines. By default, the number is 24.

Step	Command	Description
2	Raisecom(config)#terminal timeout { 0 timeout }	Configure the timeout time of the terminal. • 0: no timeout By default, the timeout time is 10min.
3	Raisecom(config)#terminal monitor Raisecom(config)#no terminal monitor	Enable or disable terminal information monitoring.
4	Raisecom(config)#terminal mmi-mode { enable disable }	Enable or disable MMI mode of the device.
5	Raisecom(config)#case-sensitive { enable disable }	Enable or disable case-sensitive input.

1.1.9 Configuring the BootROM password

Introduction

You can configure the BootROM password.

Configuring the BootROM password

Step	Command	Description
1	Raisecom(config)#bootrom password password	Configure the BootROM password, a character string.
2	Raisecom(config)#no bootrom password	Clear the BootROM password.
3	Raisecom(config)#show bootrom password	Show the BootROM password.

1.2 Loading and upgrade

1.2.1 Introduction

Loading

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

The device provides several methods to confirm configuration file name on the TFTP server, such as manually entering, obtaining through DHCP, and using default name of the

configuration file. Besides, you can assign certain naming conventions for configuration files, and then the device confirms the name according to naming conventions and its attributes (device type, MAC address, software version, and so on).

Upgrade

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

The device supports the following upgrade mode:

- Upgrade through CLI

1.2.2 Upgrading system software through TFTP CLI

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

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

Upgrade system software through CLI for the device as below.

Step	Command	Description
1	Raisecom# { tftp tftp-ipv6 } get { <i>ipv4-address</i> <i>ipv6-address</i> } <i>remote-file-name</i> [localfile <i>local-file-name</i>]	Download the system boot file through TFTP. This command supports the IPv6 address.
2	Raisecom(config)# upgrade os [localfile <i>local-file-name</i>]	Upgrade the system software.
3	Raisecom# reboot	Restart the device.

1.2.3 Upgrading system software through FTP CLI

Before upgrading system software through CLI, you should establish an FTP environment, and use a PC as the FTP server and the device as the client. Basic requirements are as below.

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

Upgrade system software through CLI for the device as below.

Step	Command	Description
1	Raisecom# { ftp ftp-ipv6 } get { <i>ipv4-address</i> <i>ipv6-address</i> } <i>user-name</i> <i>user-password</i> <i>remote-file-name</i> [localfile <i>local-file-name</i>]	Download the system boot file through FTP. This command supports the IPv6 address.
2	Raisecom(config)# upgrade os [localfile <i>local-file-name</i>]	Upgrade the system software.
3	Raisecom# reboot	Restart the device.

1.2.4 Checking configurations

Use the following commands to check configuration results.

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

1.2.5 Specifying the startup OS

Specify the startup OS for the device as below.

Step	Command	Description
1	Raisecom# boot os { main backup }	Specify the main OS or backup OS as the startup OS. This configuration takes effect on the next startup, and can be performed only when the device supports dual systems. By default, the system starts with the main OS.

1.2.6 Showing the system version

Show the system version for the device as below.

Step	Command	Description
1	Raisecom# show os-package	Show information about the system version, including the versions of the main image and backup image, version size, and compiled time.

1.3 Time management

1.3.1 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 1-5 shows basic principles of NTP. Clock synchronization works as below:

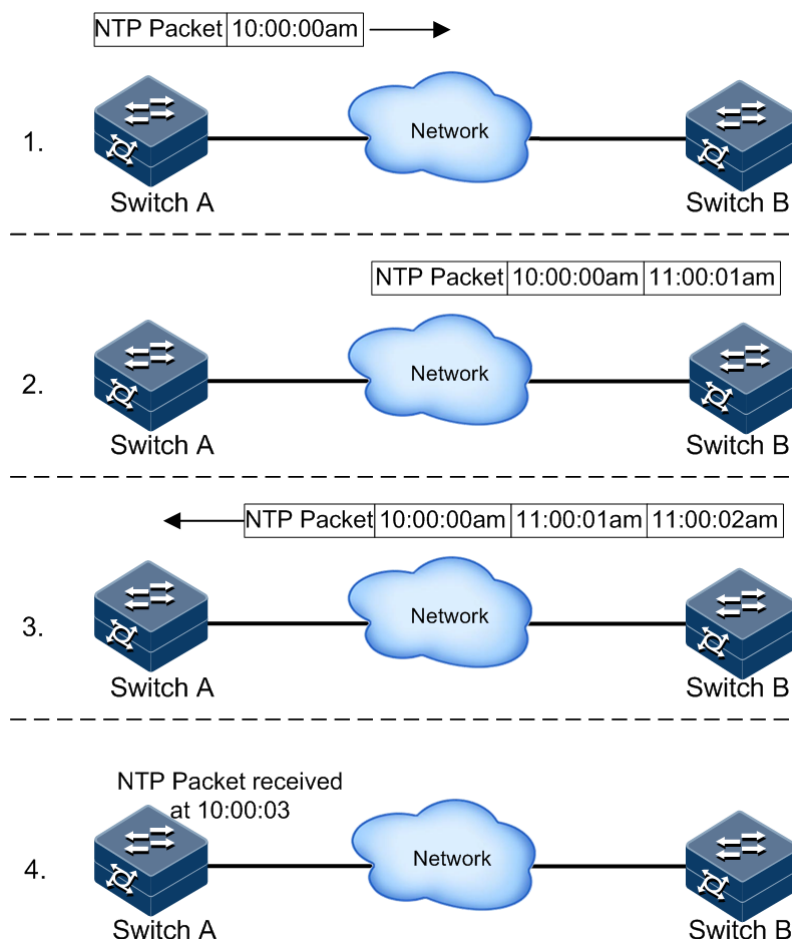
- Step 1 Switch A sends Switch B a NTP message which carries the timestamp of leaving Switch A. The timestamp is 10:00:00am and recorded as t1.
- Step 2 When the message reaches Switch B, it is added with the timestamp of reaching Switch B, which is 11:00:01am and recorded as t2.
- Step 3 When the message 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 1-5 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.

1.3.2 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

1.3.3 Default configurations

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

Function	Default value
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

1.3.4 Configuring NTP

Configuring basic functions of NTP

Configure NTP for the device as below.



Caution

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

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)#ntp 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 16 By default, it is 16.

Step	Command	Description
6	Raisecom(config)#ntp unicast-peer <i>peer-ipv4</i> { version <i>version-id</i> authentication-keyid <i>key-value</i> vpn <i>vpn-name</i> port <i>port-id</i> }	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 unicast-server <i>sserver-ipv4</i> { version <i>version-id</i> authentication-keyid <i>key-value</i> vpn <i>vpn-name</i> port <i>port-id</i> }	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 <i>key-value</i> md5 key { cipher plain } <i>string</i>	(Optional) add the NTP authentication key. • Key-value: key index • Cipher: cipher text • Plain: plaintext • string: key string
4	Raisecom(config)#ntp trusted-keyid <i>key-value</i> enable	(Optional) specify the created key to be trustful. • Key-value: key index

1.3.5 Configuring SNTP

Configuring the SNTP client

Configure the 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.
6	Raisecom(config-sntp)#sntp master	Specify the master clock.
7	Raisecom(config-sntp } sntp stratum <1-15>	Configure the stratum of the system clock.
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.

1.3.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show ntp information	Show local information about NTP.
2	Raisecom#show ntp peer	Show peer information about NTP.
3	Raisecom#show ntp key	Show key information about NTP.
4	Raisecom#show ntp session	Show session information about NTP.
5	Raisecom#show sntp	Show global SNTP configurations.
6	Raisecom#show sntp service	Show configurations of SNTP services.
7	Raisecom#show sntp service verbose	Show detailed configurations of SNTP services.

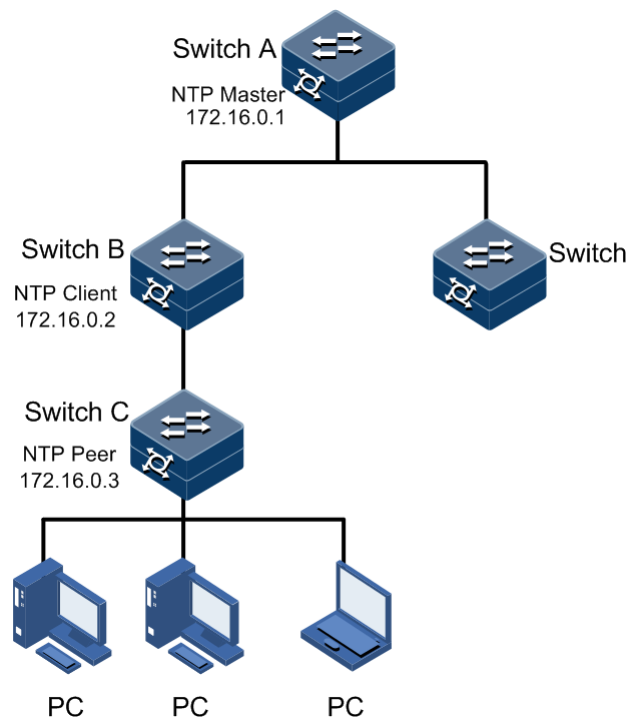
1.3.7 Example for configuring NTP

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 1-6 NTP networking



Configuration steps

Step 1 Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#configure
SwitchA(config)#ntp
SwitchA(config-ntp)#master
SwitchA(config-ntp)#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)#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)#ntp stratum 4
```

Checking results

- Check Switch A.

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

```
SwitchA#show ntp
```

- Check Switch B.

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

```
SwitchB#show ntp
```

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** command to view configurations of Switch C.

```
Raisecom#show ntp
```

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

```
Raisecom#show ntp service
```

1.4 Interface management

1.4.1 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.

1.4.2 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

1.4.3 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/*)#description <i>string</i>	Configure the description of the interface.
4	Raisecom(config-ge-1/0/*)#mtu <i>max-frame-length</i>	Configure the MTU of the interface.
5	Raisecom(config-ge-1/0/*)#negotiation auto { enable disable }	Enable or disable interface auto-negotiation.
6	Raisecom(config-ge-1/0/*)#duplex { full half default }	Configure the duplex mode of the interface.
7	Raisecom(config-ge-1/0/*)#speed { 10 100 1000 default }	Configure the interface rate.

Step	Command	Description
8	<code>Raisecom(config-ge-1/0/*)#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/*)#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/*)#port down-hold-time delay-time-value</code>	Configure the delayed time for processing when the interface status becomes Down.

1.4.4 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/*)#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/*)#reset statistics</code>	Clear interface statistics.

1.4.5 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	<code>Raisecom#configure</code>	Enter global configuration mode.

Step	Command	Description
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical interface configuration mode.
3	<code>Raisecom(config-ge-1/0/*)#flow-control { enable disable }</code>	Configure flow control on the interface.
4	<code>Raisecom#show interface <i>interface-type interface-number</i></code>	Show the detailed information about the interface and the status of flow control.

1.4.6 Shutting down/Restarting the interface

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

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

1.4.7 Configuring the type of tagged packets allowed to pass by the interface

Configure the type of tagged packets allowed to pass by the interface for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical interface configuration mode or link aggregation interface configuration mode.
3	<code>Raisecom(config-ge-1/0/1)#accept-frame-type { all only-tagged }</code>	Configure the type of tagged packets allowed to pass by the interface. • All: configure the interface to allow all tagged and untagged packets to pass. • Only-tagged: configure the interface to allow only tagged packets to pass. By default, it is all.

1.4.8 Showing the priority of management packets

Show the priority of management packets 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-vlanif- *)#packet-priority 8021p <i>value</i>	Configure the priority of management packets.
4	Raisecom(config-vlanif-*)#no packet-priority 8021p	Restore the default priority of management packets.

1.4.9 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 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/VRP
- VTP

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

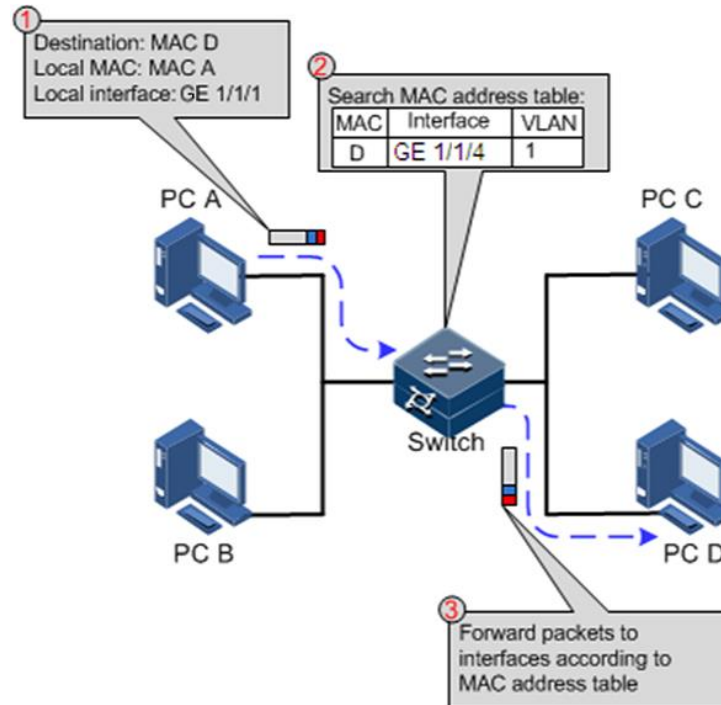
The device supports showing MAC address information by device, interface, or VLAN.

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 vlan <i>vlan-id</i> mac <i>mac-address</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 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>	Enter physical interface configuration mode.
3	Raisecom(config-vlan*)#mac-limit <i>limit-value</i>	Configure the MAC address limit on the interface.

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 <i>period</i> }	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/*)#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 more preferentially the protection action is 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.

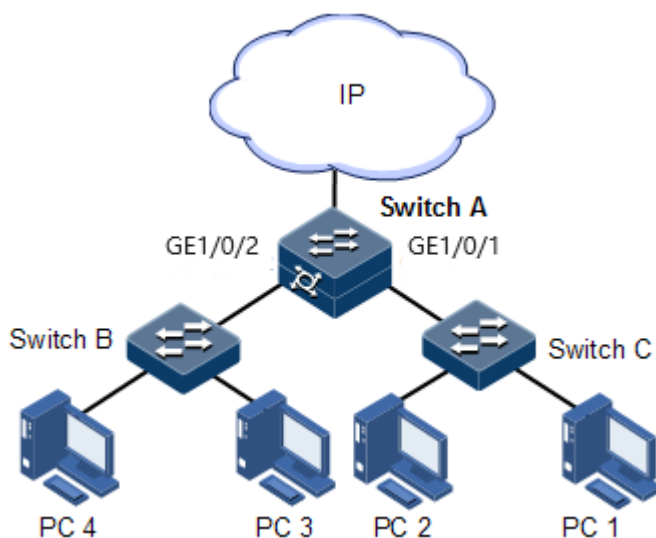
2.1.12 Example for configuring the MAC address table

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 1/0/2, which belongs to VLAN 10.

```
Raisecom(config)#mac-address static unicast 0001.0203.0405 vlan 10 ge
1/0/2
```

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

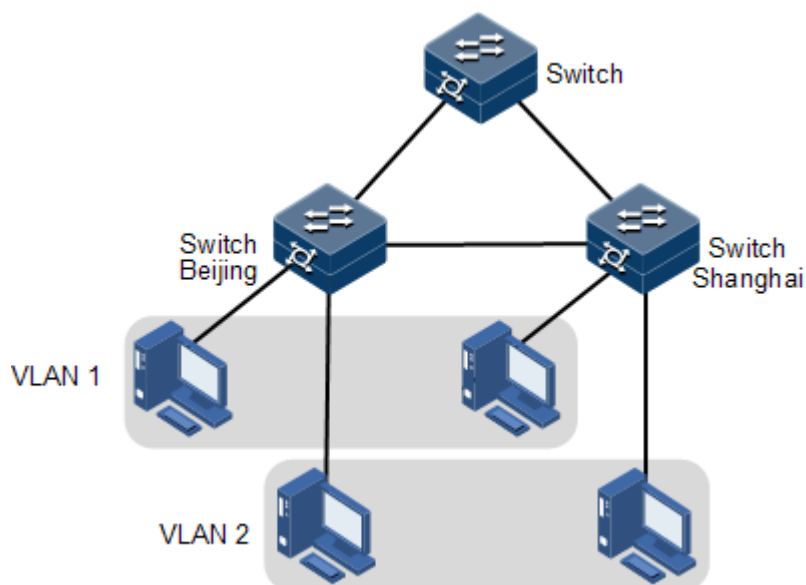
Overview

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 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)#inter face <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</i> <i>vlan-id</i>	Associate a MAC address and mask with a VLAN
3	Raisecom(config)#interface <i>interface-type</i> <i>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</i> [<i>ip-mask</i>] vlan <i>vlan-id</i>	Associate a MAC address with an IP subnet.
3	Raisecom(config)#interface <i>interface-type</i> <i>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-</i> <i>index vid vlan-id</i>	Configure the rule for associating the interface with the protocol VLAN.

2.2.12 Querying VLAN statistics

Query VLAN statistics for the device as below.

Step	Command	Description
1	Raisecom(config-vlan-*)#statistics { enable disable }	Enable VLAN statistics.
2	Raisecom#show vlan [vlan-id] statistics	Show VLAN statistics.
3	Raisecom(config)#reset vlan [vlan-id] statistics	Clear VLAN statistics.

2.2.13 Checking configurations

Use the following commands to check configuration results.

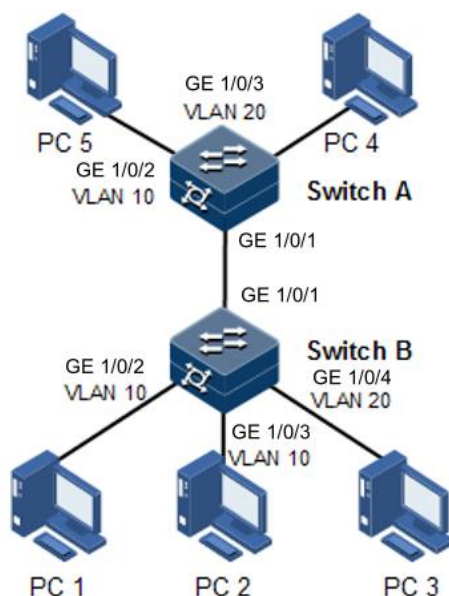
No.	Command	Description
1	Raisecom#show vlan [vlan-list vlan-id]	Show VLAN configurations.
2	Raisecom#show port vlan	Show configurations of the VLAN on the interface.
3	Raisecom# show mac-vlan [id vlan vlan-id]	Show configurations of the MAC VLAN.
4	Raisecom#show ip-subnet- vlan [vlan vlan-id]	Show configurations 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.

2.2.14 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 MMMMMMMM
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 interface interface-type interface-number config** 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.

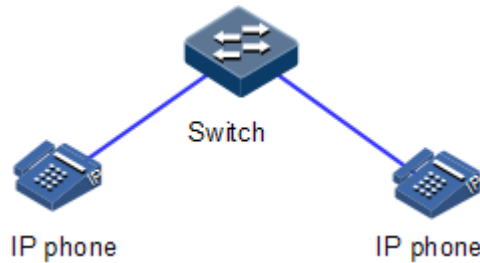
Compared with other methods for managing voice traffic, the voice VLAN has the following advantages:

- 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	Disable
Voice VLAN common working mode	Enable
Automatic mode for the interface to join the voice VLAN	Disable
Manual mode for the interface to join the voice VLAN	Enable
CoS and DSCP of Voice VLAN packets	6 and 46 respectively
QoS trust priority of Voice VLAN	N/A
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 [description word]</i>	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-1/0/*)#voice-vlan <i>vlan-id enable</i>	Enable the voice VLAN.
4	Raisecom(config-ge-1/0/*)# voice-vlan mode { auto manual }	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-1/0/*)#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

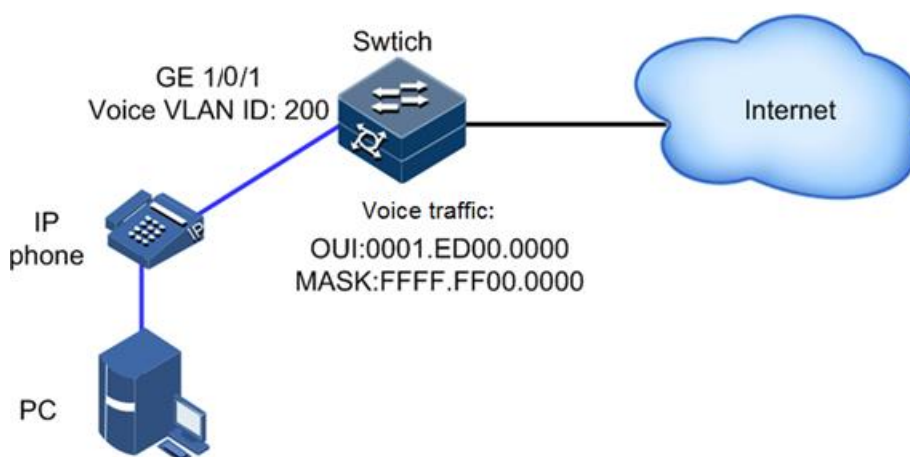
Example for adding interfaces to the voice VLAN and configuring it to work in manual mode

Networking requirements

GE 1/0/1 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 1/0/1 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 1/0/1. 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 the interface to the voice VLAN and configuring it to work in the 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 1/0/1
Raisecom(config-ge-1/0/1)#port link-type trunk
Raisecom(config-ge-1/0/1)#port trunk allow-pass vlan 100
Raisecom(config-ge-1/0/1)#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	manual	disable
			N/A

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

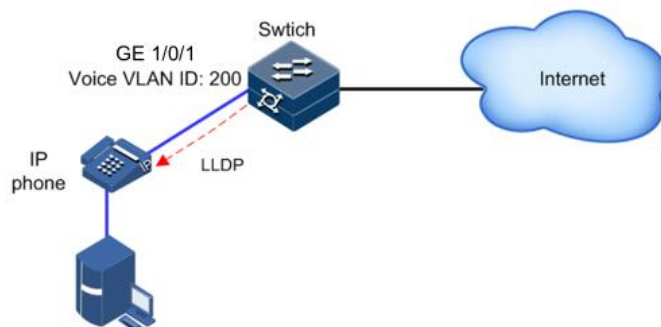
Networking requirements

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 1/0/1 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 1/0/1. 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 1/0/1
Raisecom(config-ge-1/0/1)#port link-type trunk
Raisecom(config-ge-1/0/1)#port trunk allow-pass vlan 100
Raisecom(config-ge-1/0/1)#voice-vlan 200 enable
Raisecom(config-ge-1/0/1)#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 1/0/1
Raisecom(config-ge-1/0/1)#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

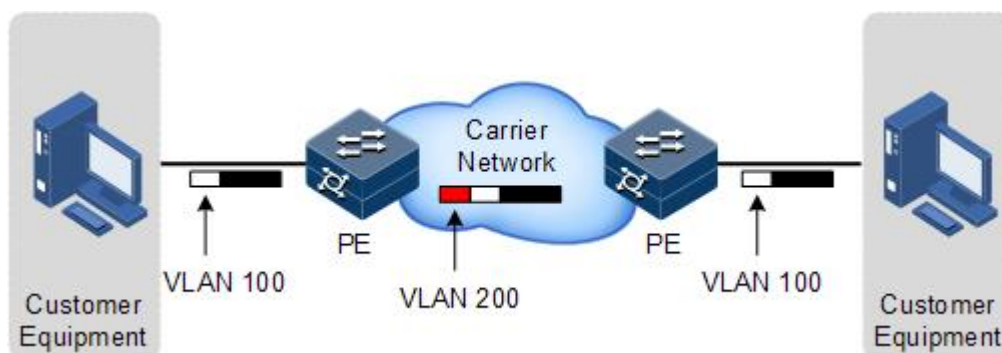
2.4.1 Introduction

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-ge-1/0/1)#port link-type dot1q-tunnel	Enable basic QinQ on the interface.
4	Raisecom(config-ge-1/0/1)#port default vlan <i>vlan-id</i>	Configure basic QinQ, add double Tags, and specify the PVID used by the CVLAN and SVLAN.
5	Raisecom(config-ge-1/0/1)#tpid <i>tpid</i>	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-ge-1/0/1)#inner tpid <i>tpid</i>	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-ge-1/0/*)#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)#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-1/0/*)# switchport 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)#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-1/0/*)#tpid <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.

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

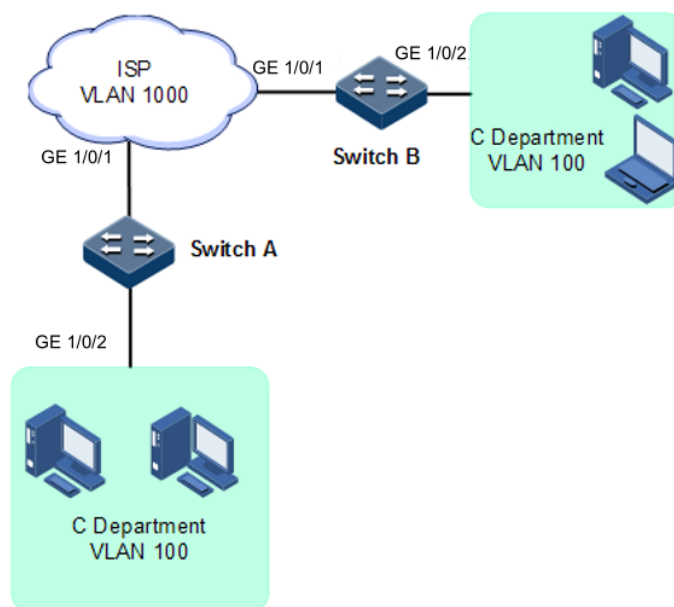
2.4.9 Example for configuring basic QinQ

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

Step 2 Configure basic QinQ on the interface.

```
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port link-type dot1q-tunnel
Raisecom(config-ge-1/0/2)#port default vlan 1000
Raisecom(config-ge-1/0/2)#exit
```

Checking results

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

```
Raisecom#show interface ge 1/0/2 config
!
interface ge 1/0/2
port link-type dot1q-tunnel

port default vlan 1000
```

2.4.10 Example for configuring selective QinQ and adding outer VLAN tag to tagged packets

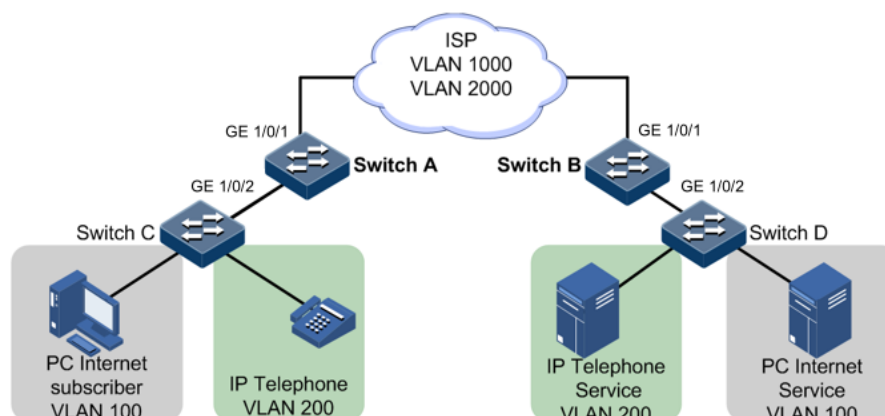
Networking requirements

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 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan 1000,2000
SwitchA(config-ge-1/0/1)#tpid 0x9100
SwitchA(config-ge-1/0/1)#exit
```

Step 2 Enable selective QinQ on GE 1/0/2.

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/2)#port trunk allow-pass vlan 100,200,1000,2000
SwitchA(config-ge-1/0/2)#vlan-stacking vlan 100 stack-vlan 1000
SwitchA(config-ge-1/0/2)#vlan-stacking vlan 200 stack-vlan 2000
SwitchA(config-ge-1/0/2)#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-1/0/2          100/-              -/1000/-
ge-1/0/2          200/-              -/2000/-
```

2.4.11 Example for configuring selective QinQ and adding double VLAN tags to untagged packets

Networking requirements

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

- Configure selective QinQ.
- Add outer Tag VLAN 2000 and inner Tag VLAN 200 to untagged phone services.
- The carrier TPID is 9100.

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 200 and VAN 2000. The TPID is 9100.

```
Raisecom#hostname SwitchA
SwitchA#configure
SwitchA(config)#vlan 200,2000
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 allow-pass vlan 2000
SwitchA(config-ge-1/0/1)#tpid 0x9100
SwitchA(config-ge-1/0/1)#exit
```

Step 2 Enable selective QinQ on GE 1/0/2.

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/2)#port trunk allow-pass vlan 200,2000
SwitchA(config-ge-1/0/2)#vlan-stacking untagged stack-vlan 2000 stack-
inner-vlan 200
SwitchA(config-ge-1/0/2)#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-1/0/2           -/-                      200/2000/-
```

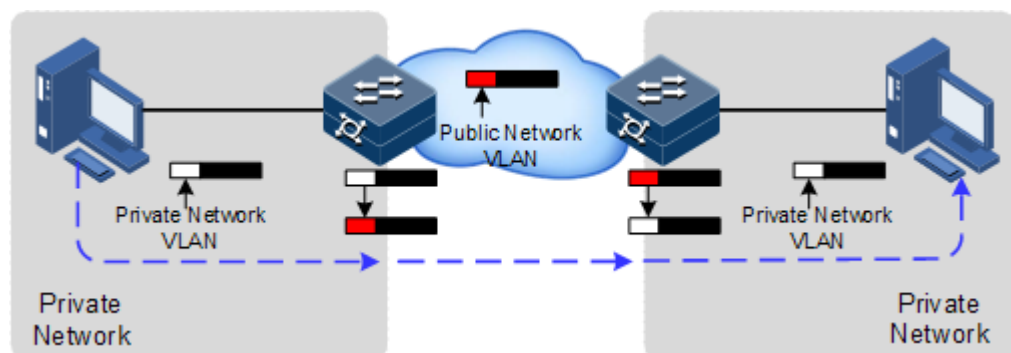
2.5 VLAN mapping

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-1/0/*)#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.
4	Raisecom(config-ge-1/0/*)#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.
5	Raisecom(config-ge-1/0/*)#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.
6	Raisecom(config-ge-1/0/*)#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.

Step	Command	Description
7	<code>Raisecom(config-ge-1/0/*)#vlan-mapping 8021p 802.1p priority map-vlan <i>vlan-id</i> [remark-8021p <i>cos-id</i>]</code>	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	<code>Raisecom#show vlan-mapping interface</code>	Show configurations of VLAN mapping rules on the interface.

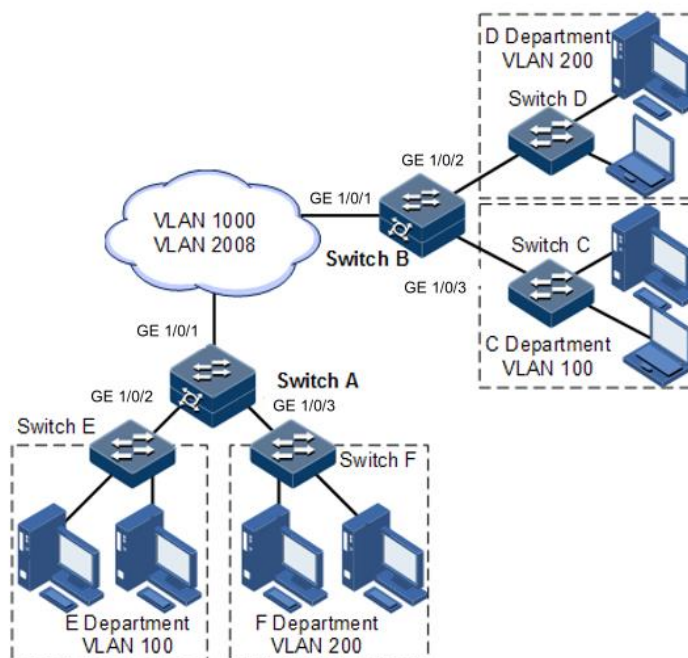
2.5.6 Example for configuring VLAN mapping

Scenario

As shown in Figure 2-12, GE 1/0/2 and GE 1/0/3 on Switch A are connected to Department E using VLAN 100 and Department F using VLAN 200; GE 1/0/2 and GE 1/0/3 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 1/0/1 to Trunk mode, allowing packets of VLAN 1000 and VLAN 2008 to pass.

```
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 allow-pass vlan 1000,2008
SwitchA(config-ge-1/0/1)#exit
```

Step 3 Configure GE 1/0/2 to Trunk mode, allowing packets of VLAN 100 to pass. Configure VLAN mapping rules.

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/2)#port trunk allow-pass vlan 100
```

```
SwitchA(config-ge-1/0/2)#vlan-mapping vlan 100 map-vlan 1000
SwitchA(config-ge-1/0/2)#exit
```

- Step 4 Configure GE 1/0/3 to Trunk mode, allowing packets of VLAN 200 to pass. Configure VLAN mapping rules.

```
SwitchA(config)#interface ge 1/0/3
SwitchA(config-ge-1/0/3)#port link-type trunk
SwitchA(config-ge-1/0/3)#port trunk allow-pass vlan 100
SwitchA(config-ge-1/0/3)#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-1/0/2           inner: -                  inner: -/-
                   outer: 100/-              outer: 1000/-
ge-1/0/3           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.

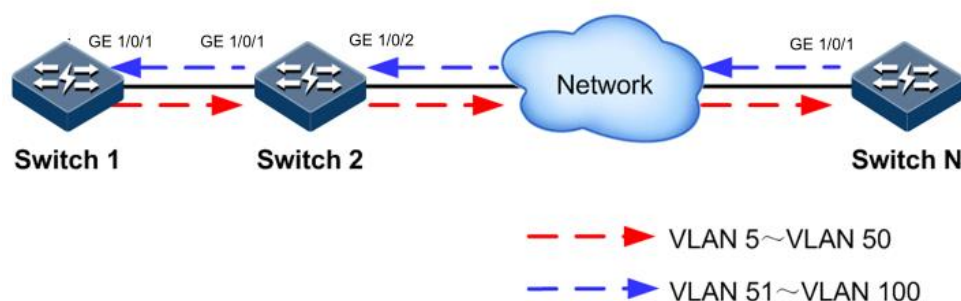
All MRP-supportive switches can receive VLAN registration information from other switches, and dynamically update local VLAN registration information. In addition, all MRP-supportive switches can send local VLAN registration information to other switches so that they have consistent VLAN registration 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 1/0/1 on Switch 1, GE 1/0/1 and GE 1/0/2 on Switch 2, and GE 1/0/1 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-ge-1/0/*)#port link-type trunk	Configure the interface to Trunk mode.
5	Raisecom(config-ge-1/0/*)#mvrp registration { fixed forbidden normal }	Configure the MVRP registration mode.
6	Raisecom(config-ge-1/0/*)#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-number vlan vlan-id</i>	Show configurations of the MVRP timer.

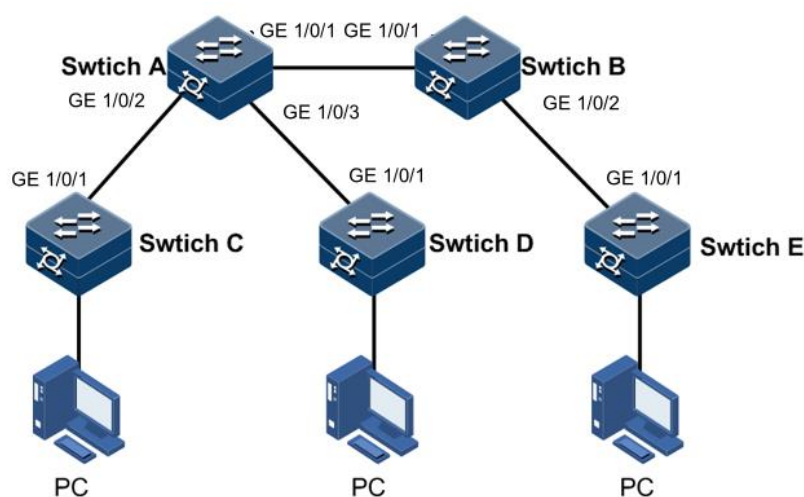
2.6.6 Example for configuring MVRP

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 1/0/1, GE 1/0/2, and GE 1/0/3 on Switch A, GE 1/0/1, GE 1/0/2, and GE 1/0/3 on Switch B, GE 1/0/1 on Switch C, and GE 1/0/1 on Switch D to Trunk mode, and enable MVRP on them. Take GE 1/0/1 on Switch A for example. Configurations of other interfaces are the same.

```
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 allow-pass vlan all
SwitchA(config-ge-1/0/1)#mvrp enable
SwitchA(config-ge-1/0/1)#exit
```

- Step 3 Configure MVRP timers of GE 1/0/1, GE 1/0/2, and GE 1/0/3 on Switch A, GE 1/0/1, GE 1/0/2, and GE 1/0/3 on Switch B, GE 1/0/1 on Switch C, and GE 1/0/1 on Switch D, and enable MVRP on them. Take GE 1/0/1 on Switch A for example. Configurations of other interfaces are the same.

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#mvrp timer join 3000
SwitchA(config-ge-1/0/1)#mvrp timer leave 15000
SwitchA(config-ge-1/0/1)#mvrp timer leave-all 20000
```

Checking results

Use the **show mvrp config** command to show MVRP configurations on the interface.
Take Switch A for example.

```
SwitchA#show mvrp config
```

```
Version          : MVRP_V13.10.00.00
Compliance-GVRP  : disable
Interface        JoinTime(ms)  LeaveTime(ms)  LeaveAllTime(ms)
PeriodicTime(ms) Mode      State
-----
ge 1/0/1         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-1/0/1<->ge-1/0/16      MMMMMMMM
MMMMMMMMM
                        ge-1/0/17<->ge-1/0/32      MMMMMMMM MMMMMMMM
                        ge-1/0/33<->ge-1/0/48      MMMMMMMM MMMMMMMM
                        10ge-1/0/49<->10ge-1/0/54    MMMMMM
2      N/mvrp    tagged:   ge-1/0/1<->ge-1/0/16      M-----
```

```

3      N/mvrp      tagged: ge-1/0/1<->ge-1/0/16      M-----
4      N/mvrp      tagged: ge-1/0/1<->ge-1/0/16      M-----
5      N/mvrp      tagged: ge-1/0/1<->ge-1/0/16      M-----
6      N/mvrp      tagged: ge-1/0/1<->ge-1/0/16      M-----
7      N/mvrp      tagged: ge-1/0/1<->ge-1/0/16      M-----
8      N/mvrp      tagged: ge-1/0/1<->ge-1/0/16      M-----
9      N/mvrp      tagged: ge-1/0/1<->ge-1/0/16      M-----
10     N/mvrp      tagged: ge-1/0/1<->ge-1/0/16      M-----
20     N/mvrp      tagged: ge-1/0/1<->ge-1/0/16      M-----
-----
Total: 11      Static: 1      Dynamic: 10

```

2.7 VTP

2.7.1 Introduction

VLAN Trunk Protocol (VTP) reduces configuration work on the switching network. When a new VLAN is configured on the VTP server, its configurations are broadcasted in the same domain through the switch. This avoids the operation of configuring the same VLAN on each switch.

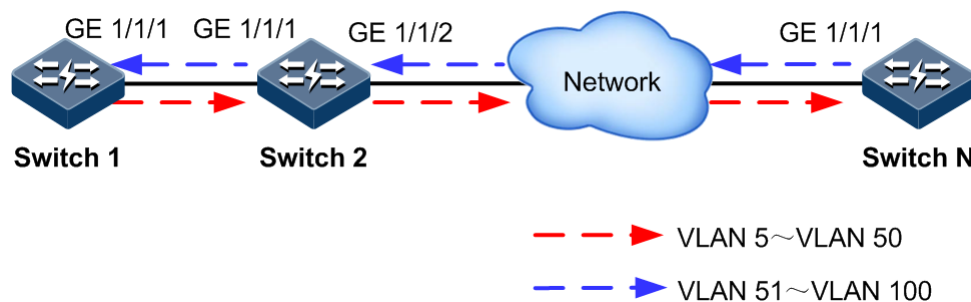
Concepts

- VTP domain: it is also called the VLAN management domain, and it is composed of at least one switch that shares the VTP domain name and is interconnected with others. To use VTP, specified the VTP domain name for each switch. The VTP information is kept in the VTP domain and is synchronized in the same domain.
- Server mode: this mode provides the following VTP messages: the VLAN ID, VLAN name, learned VTP messages with the same domain name, forwarded VTP messages with the same domain name, added VLAN, deleted VLANs, and modified VLANs. After the mode is configured, configure VLANs, including adding VLANs, deleting VLANs, and modifying VLANs. Then, the server advertises the summary notice, carrying VLAN changes of the switch in the VTP domain. Then, the server sends one or more subset notices. Adding, deleting, or modifying a VLAN or change the VLAN name triggers subset notice. To advertise all information to multicast VLANs, the server needs to advertise multiple subnet notices. After the server mode is restarted, the server automatically advertises the summary notice and subnet notices to synchronize information in the VTP domain.
- Client mode: this mode requests the VTP message, learns the VTP message with the same domain name, and forwards the VTP message with the same domain name. You can configure the static VLAN, but it will not be advertised. Configuring the static VLAN does not modify the configuration revision ID. After the static VLAN of the client is deleted, the configuration revision ID of the client is reset to 0, and the client sends an advertisement request to synchronize VLAN information. After a switch is configured to client mode, it sends the notice request to the server, and then it receives the summary notice and subnet notice, thus making own configurations and configurations in the VTP domain consistent.
- Transparent mode: in this mode, the switch does not participate in VTP, so it does not advertise VLAN configurations. In addition, its VLAN database is not synchronized with

the received notice, but it can create and delete local VLANs. However, it does not advertise the changes of these local VLANs to other switches. In this mode, the switch forwards VTP packets. When the VTP switches from the client or server mode to transparent mode, the configuration revision ID is reset to 0. When the switch in transparent mode forwards the VTP message, it checks the domain name and version in the VTP message. Only when they are the same as those of the switch can the switch forward the VTP message.

- **Revision ID:** the VTP notice carries the configuration revision ID, which represents the updating status of the VLAN configuration. The greater the configuration revision ID is, the later the VLAN configuration is. When the client receives configurations with greater ID, it uses the VLAN configuration in the VTP update to override the existing VLAN configuration. When the VLAN configuration (including the creating or deleting a VLAN and modifying the VLAN name) on the server is modified, the configuration revision ID increases and is advertised to the domain.

Figure 2-15 VTP principle networking



Create VLANs 5–50 on switch 1. These VLANs are registered at the receiving interface along the red connection lines above until they are advertised to switch N.

2.7.2 Preparing for configurations

Scenario

The second-layer relay frame is used for VLAN communication among a group of switches. Starting from a central control point, VTP maintains VLAN information of the entire enterprise network and ensures configuration consistency.

Preconditions

- Connect interfaces, configure their physical parameters, and make interfaces Up at the physical layer.
- Add interfaces to VLANs.
- If interfaces are configured with the ring protocol, ensure that they are not blocked by the ring protocol.

2.7.3 Default configurations

Default configurations of VTP

Default configurations of VTP are as below.

Function	Default value
Global VTP status	Disable
Default mode of the VTP domain	Server
VTP version	1

2.7.4 Configuring basic functions of VTP

Configure basic functions of VTP for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#vtp domain <i>name</i>	Create a VTP domain.
3	Raisecom(config)#password <i>password</i>	Configure the password of the VTP domain.
4	Raisecom(config-vtp-domain-test)#mode <i>client</i>	Configure the mode of the VTP domain to client.
5	Raisecom(config-ge-1/0/*)#join vtp domain <i>name</i>	Configure the interface to join the VTP domain.

2.7.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show vtp domain	Show the domain configurations of VTP.
2	Raisecom#show vtp interface	Show the interface status of VTP.

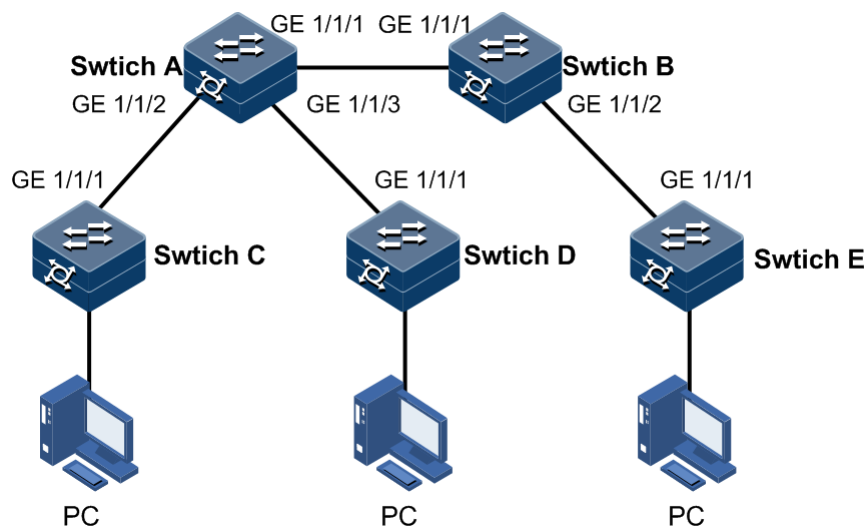
2.7.6 Example for configuring VTP

Networking requirements

To dynamically register and update VLAN information among switches, as shown in Figure 2-16, configure VTP on these switches, with requirements as below:

- Switch A works as the VTP server. Configure static VLANs 5–100.
- Other switches work as VTP clients, receive packets, and create VLANs 5–100.

Figure 2-16 VTP application networking



Configuration steps

Step 1 Create a VTP domain, and configure the working mode of each switch.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#configure
SwitchA(config)#vtp domain A
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#configure
SwitchB(config)#vtp domain A
SwitchB(config-vtp-domain-A)#mode client
```

Configure other switches with the same parameters as those of switch B.

Step 2 Configure GE 1/0/1, GE 1/0/2, and GE 1/0/3 on switch A, GE 1/0/1 and GE 1/0/2 on switch B, GE 1/0/1 on switch C, and GE 1/0/1 on switch D to join the VTP domain. The following section takes GE 1/0/1 on switch A for example. Configure other interfaces with the same command as those of GE 1/0/1 on switch A.

```
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#join vtp domain A
SwitchA(config-ge-1/0/1)#port hybrid vlan 5-100 tagged
SwitchA(config-ge-1/0/1)#exit
```

Step 3 Create VLANs x 5–100 on GE 1/0/1 on switch A.

```
SwitchA(config)#vlan 5-100
```

Checking results

Use the **show vtp domain** command to show configurations of the VTP domain. Take switch B for example.

```
SwitchB#show vtp domain
Domain: 1
Name:      A
Version:   1
Pruning:   Disable
Password:  --
Mode:      client
Configure Revision Num 2
Vlan:      1,5-100
```

Use the **show vtp interface** command to show configurations of the VTP interface. Take switch B for example.

```
SwitchB#show vtp interface
Interface      State      Domain      VlanList
-----
ge-1/0/1       enable     A            2-4094
ge-1/0/2       enable     A            2-4094
```

Use the **show vlan** command to show the status of the interface to join VLANs.

```
SwitchB(config)#show vlan
NOTE:
    S: supervlan      P: pvlan      N: normal

Vlan Type      Ports('M': member , '-': not member)
-----
1   N/static   untagged: ge-1/0/1<->ge-1/0/16      MMMMMMMM
MMMMMMMM
                                ge-1/0/17<->ge-1/0/32      MMMMMMMM MMMMMMMM
                                ge-1/0/33<->ge-1/0/48      MMMMMMMM MMMMMMMM
                                10ge-1/0/49<->10ge-1/0/54      MMMMMM
5   N/vtp      tagged:   ge-1/0/1<->ge-1/0/16      MM-----
6   N/vtp      tagged:   ge-1/0/1<->ge-1/0/16      MM-----
7   N/vtp      tagged:   ge-1/0/1<->ge-1/0/16      MM-----
```


[illegible]

63	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
64	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
65	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
66	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
67	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
68	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
69	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
70	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
71	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
72	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
73	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
74	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
75	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
76	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
77	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
78	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
79	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
80	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
81	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
82	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
83	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
84	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
85	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
86	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
87	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
88	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
89	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
90	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
91	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
92	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
93	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
94	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
95	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
96	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
97	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
98	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
99	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----
100	N/vtp	tagged:	ge-1/0/1<->ge-1/0/16	MM-----	-----

Total: 97 Static: 1 Dynamic: 96

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
- Policy route
- BGP
- OSPFv2
- OSPFv3
- IS-IS
- IS-IS (IPv6)
- RIP
- RIPng
- Routing policy
- ECMP

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 <i>vlan</i> <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.

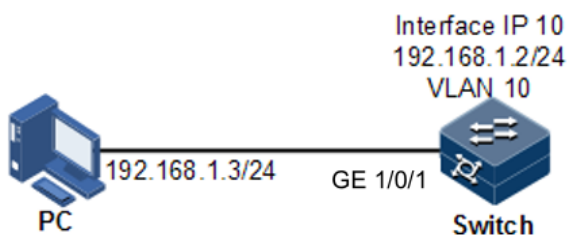
No.	Command	Description
1	Raisecom# show ip interface brief	Show configurations of the IP address of the VLAN interface.
2	Raisecom# show ipv6 interface brief	Show configurations of the IPv6 address of the VLAN interface.

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      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.
3	Raisecom(config-loopback-*)#ip address <i>ip-address</i> [<i>ip-mask</i>] [sub]	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)#arp static ip-address mac-address { ge 10ge 25ge 40ge 100ge 400ge } interface-number	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.
2	Raisecom(config)#arp aging-time { time default }	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 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.

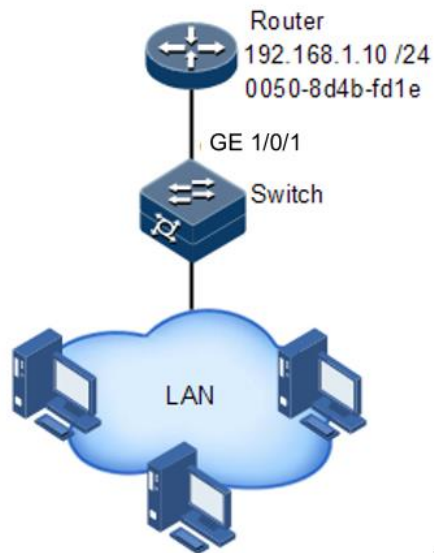
3.3.8 Example for configuring ARP

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)#interface 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)#interface 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)#arp static 192.168.1.10 00:50:8d:4b:fd:1e ge 1/0/1
```

Checking results

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

```
Raisecom#show arp
Arp aging time: 1200 (s)
Arp entry types: D-Dynamic, S-Static, I-Interface, DH-Dhcp, B-Bgp, INV-Invalid
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
```

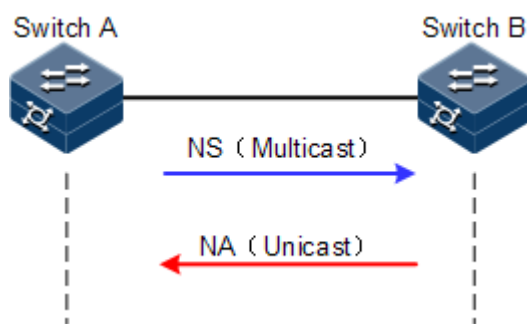
3.4 NDP

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-static <i>ipv6-address mac-address interface-type 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> default }	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
Raisecom(config)# flush ipv6 neighbor [all dynamic static]	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	Raisecom# configure	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.

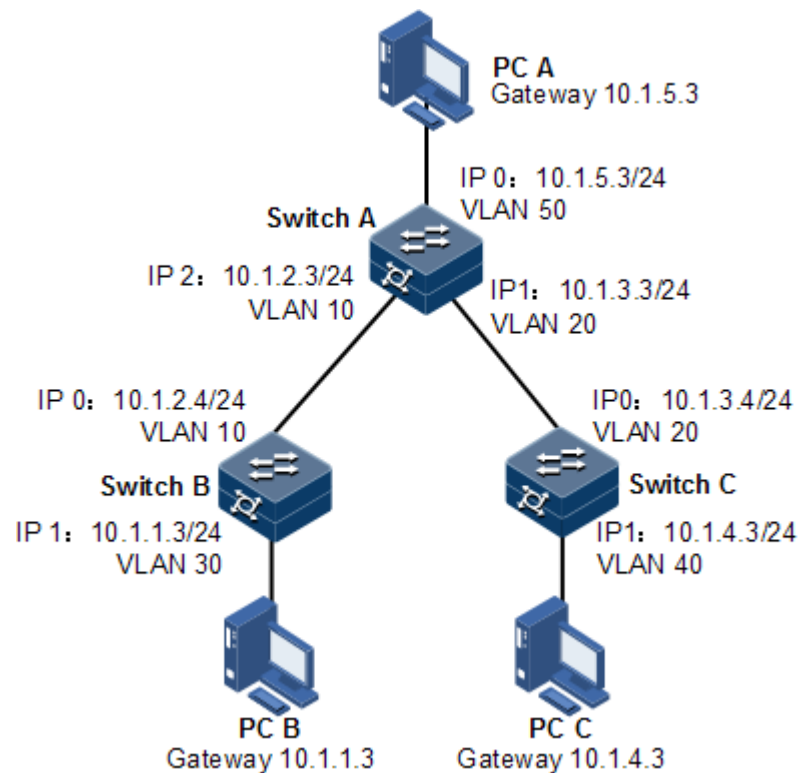
No.	Item	Description
1	Raisecom# show ip route Raisecom# show ipv6 route	Show information about the routing table.
2	Raisecom# show { ip ipv6 } route statistics	Show route statistics.

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
```

3.6 Policy route

3.6.1 Introduction

Overview

Traditionally, common packet forwarding is implemented by querying the forwarding table based on the destination IP address of the packet. When the packet needs to be forwarded based on the source IP address, packet length, or other attribute of the packet, a new routing mechanism is required to control, namely, policy route.

The so-called policy route, as the name suggests, refers to forwarding packets based on a certain policy. Therefore, policy route is a more flexible routing mechanism than destination routing. When forwarding a data packet by a router, the packet is first filtered according to the configured rules. If the match is successful, the packet is forwarded according to a certain forwarding policy. This rule can be based on standard ACL, extended ACL, or packet length. The forwarding policy is to control the packet to be forwarded according to the specified policy route table, and it can also modify the IP precedence of the packet. Therefore, policy route is an effective enhancement to traditional IP routing.

Policy route can meet the requirements of routing based on source IP address, destination IP address, protocol field, TCP source port number, TCP destination port number, UDP source port number, or UDP destination port number. Any IP standard/extended ACL that can be configured can be used as a matching rule for policy route for forwarding.

Policy route determine the next hop forwarding address or default IP address of an IP packet, not simply based on the destination IP address but rather a comprehensive consideration of multiple factors. For example, policy route can select the path for the data packet based on the Differential Service Code Point (DSCP) field, source port number, destination port number, and source IP address. Policy route can implement traffic engineering to some extent,

allowing flows of different Quality of Service (QoS) or data of different properties (voice and FTP) to take different paths.

Policy route provides network managers with stronger control over packet forwarding and storage than traditional routing protocols. Traditionally, the router uses the routing tables derived from routing protocols to forward packets based on the destination address. Policy route has stronger capabilities and is more flexible to use than traditional routing. It allows network managers to choose forwarding paths based on not only the destination address but also protocol type, packet size, application, or IP source address. A policy can be defined as the QoS for packet forwarding on the network based on load balancing across multiple routers or total traffic.

The implementation of policy route relies on the support of the chip. Policy route converts software entries into hardware entries, and stores them on the chip through the commands or other configuration interfaces. When traffic passes the chip, the chip will filter traffic according to the policy route hardware table.

3.6.2 Preparing for configurations

Scenario

Policy route can be configured when you need to control IP packet forwarding based on policy. Policy route needs to be manually configured by users, through which packets can be forwarded according to matching rules.

Prerequisites

Configure the matching rules for the ACLs.

3.6.3 Configuring the static route

Configure the static route for the device as below.

Step	Command	Description
1	Raisecom# configure	Enter global configuration mode.
2	Raisecom(config)# policy-route <i>policy-name</i> { permit deny } node <i>node-number</i>	Configure the policy route template.
	Raisecom(config-policy-route-test-1)# if-match acl-ipv4 <i>acl-number1</i>	Configure the matching rule for the ACL.
	Raisecom(config-policy-route-test-1)# apply ip-address next-hop <i>ip-address</i>	Configure the next hop address of packets.
3	Raisecom(config-ge-1/0/1)# policy-route bind-policy <i>policy-name</i>	Apply the policy route to the physical interface.

3.6.4 Checking configurations

Use the following commands to check configuration results.

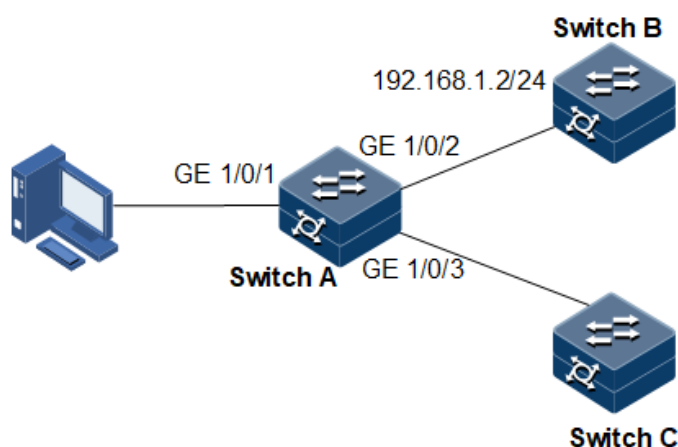
No.	Command	Description
1	Raisecom#show policy-route	Show information about all or a specified policy route.
2	Raisecom#show policy-route config	Show configurations of the policy route.

3.6.5 Example for configuring policy route based on ACL

Networking requirements

As shown below, define a policy route named aaa. GE interface 1/0/2 sends the IP packets received from GE interface 1/0/1, with the IP address of the next hop as 192.168.1.2. Other packets are forwarded according to the result of querying the routing table.

Figure 3-5 Policy route networking



Configuration steps

Step 1 Define the ACL, making ACL filter 1 match IP packets.

```

switch(config)#acl-ipv4 1001
switch(configure-acl-ipv4-1001)#rule 1 src-ip any dst-ip any
switch(configure-acl-ipv4-1001)#rule 1 action permit
  
```

Step 2 Define the rule and action of the policy.

```

switch(config)#policy-route policy1 permit node 1
switch(config-policy-route-aaa-1)#if-match acl-ipv4 1001
switch(config-policy-route-aaa-1)#apply ip-address next-hop 192.168.1.2
switch(config-policy-route-aaa-1)#quit
  
```

Step 3 Enable the policy on the interface.

```
Raisecom(config-ge-1/0/*)#policy-route bind-policy policy1
```

Checking results

```
switch(config-ge-1/0/1)#show ip policy-route policy1
policy-route : policy1
Node 1 : permit
if-match acl-ipv4 1001
apply ip-address next-hop 192.168.1.2
enabled port : ge-1/0/1
```

3.7 BGP

3.7.1 Introduction

Functions

BGP is an External Gateway Protocol (EGP) that differs from Internal Gateway Protocols (IGP) such as OSPF and RIP. Its focus is not on discovering and calculating routes, but on controlling route advertisement and selecting the best route.

- BGP uses TCP as its transport layer protocol (port number 179), which improves the reliability of the protocol.
- BGP supports Classless Inter Domain Routing (CIDR).
- When routes are updated, BGP only sends updated routes, greatly reducing the bandwidth occupied by BGP route advertisement, making it suitable for advertising a large amount of routing information on the Internet.
- BGP routing completely solves the routing loop problem by carrying AS path information.
- BGP provides rich routing policies that enable flexible filtering and selection of routes.
- BGP is easy to expand and can adapt to new developments on the network.

Basic concepts of BGP

- The Autonomous System (AS): the AS refers to an IP network under the jurisdiction of an entity that has the same routing policy. Each AS in the BGP network is assigned a unique AS ID to distinguish different ASs. The AS ID is divided into the 2-byte AS ID and 4-byte AS ID, The 2-byte AS ID ranges from 1 to 65535 while the 4-byte AS ID ranges from 1 to 4294967295. Devices that support 4-byte AS IDs are compatible with devices that support 2-byte AS IDs.
- BGP classification: BGP is divided into External/Exterior BGP (EBGP) and Internal/Interior BGP (IBGP) according to its operating mode.

- EBGp: BGP running between different ASs is called EBGp. To prevent loops between ASs, the BGP device discards routes with local AS IDs when receiving routes sent by EBGp peers.
- IBGP: BGP running within the same AS is called IBGP. To prevent loops within the AS, BGP devices do not notify other IBGP peers of the routes learned from IBGP peers and establish a full connection with all IBGP peers.
- Roles in BGP packet exchange: there are two roles in exchanging BGP packets.
 - Speaker: the device that sends BGP packets is called a BGP speaker, which receives or generates new packets and advertises them to other BGP speakers.
 - Peer: speakers who exchange packets with each other are called peers.
- Router ID of BGP: The router ID of BGP is a 32-bit value used to identify BGP devices, usually in the form of an IPv4 address, carried in the Open message sent during BGP session establishment. When establishing BGP sessions between peers, each BGP device must have a unique Router ID; otherwise, BGP connections cannot be established between peers.

BGP4 peer

The BGP neighbors, also known as peers, are divided into two types. If two peers exchanging BGP packets belong to different ASs, then they are EBGp peers. If two peers exchanging BGP packets belong to the same AS, then they are IBGP peers. BGP connections must also be established between different boundary routers within an AS to transmit routing information through the entire AS.

IBGP peers may not necessarily be physically directly connected, but they must be fully logically connected. In most cases, there is a physical direct link between EBGp peers, but if this cannot be achieved, the logical link can be configured.

BGP advertises the routes obtained from EBGp to all its BGP peers, including IBGP and EBGp, but it does not advertise the routes obtained from IBGP to its IBGP peers. When EBGp is notified, ensure that IGP is synchronized with BGP. Synchronization refers to BGP advertising the route to other ASs until IGP advertises the same route in this AS. In other words, when BGP advertises a route to other ASs, it ensures that the internal routers in this AS are aware of the route.

BGP4 route advertisement

A route is generally generated from within the AS, discovered and calculated by some internal routing protocol to reach the boundaries of the AS, and advertised to other ASs through EBGp connections by the Autonomous System Boundary Router (ASBR).

During the advertisement process, a route may pass several ASs, which are called transitional ASs. If these ASs have multiple boundary routers, these routers run IBGP to exchange routing information. At this point, the internal router does not need to know these external routes, and they only need to maintain IP connectivity between boundary routers. After the route reaches the boundary of the AS, if the internal router needs to know the external route, the ASBR can redistribute the route into the internal routing protocol. The number of external routes is too large to usually exceed the processing capacity of internal routers. Therefore, when the ASBR redistributes external routes, it needs to filter or aggregate routes to reduce the number of them. In extreme cases, default routes are used.

BGP4 messages

BGP peers exchange information through the following types of BGP messages. The Keepalive message is periodically sent while others are sent as triggered.

- Open message: used to establish a BGP peer connection. The Open message is the first message after the TCP connection established by the BGP neighbor, which includes the current protocol version, AS ID, router ID, and some optional parameters. If the other party cannot reach an agreement on certain parameters in the message, BGP neighbors cannot be established.
- KeepAlive message: used to maintain BGP connection. Once both parties reach an agreement on the content of the Open message, a KeepAlive message is periodically sent to detect the status of neighbors. If a KeepAlive message sent by a neighbor is not received within a certain period of time, one party considers that the neighbor has malfunctioned.
- Update message: used to exchange routing information between peers. The Update message is used to carry routing information, including various attributes of the route, and BGP uses this message to notify neighbors of routing information.
- Notification message: used to interrupt BGP connections. Once an error occurs during BGP operation, a Notification message will be sent, indicating the cause of the error.
- Route-refresh message: used to request peers to resend routing information after changing routing policies. Only BGP devices that support the route refresh capability can send and respond to this message.

Attributes of BGP4 routes

The route attribute is a specific description of the route, and all BGP route attributes can be divided into four categories:

- Well-known mandatory: all BGP devices can recognize such attributes, which must exist in the Update message. If such attributes are missing, the routing information will be incorrect.
- Well-known discretionary: all BGP devices can recognize this type of attributes, which are not required to exist in the Update message; in other words, even if this type of attributes is missing, the routing information will remain correct.
- Optional transitive: an attribute that has transitivity between ASs. The BGP device may not support this attribute, but it will still receive such attribute and pass it to other peers.
- Optional non-transitive: the BGP device may not recognize this type of attribute. If the BGP device does not recognize this type of attribute, it will ignore the attribute and will not notify other peers.

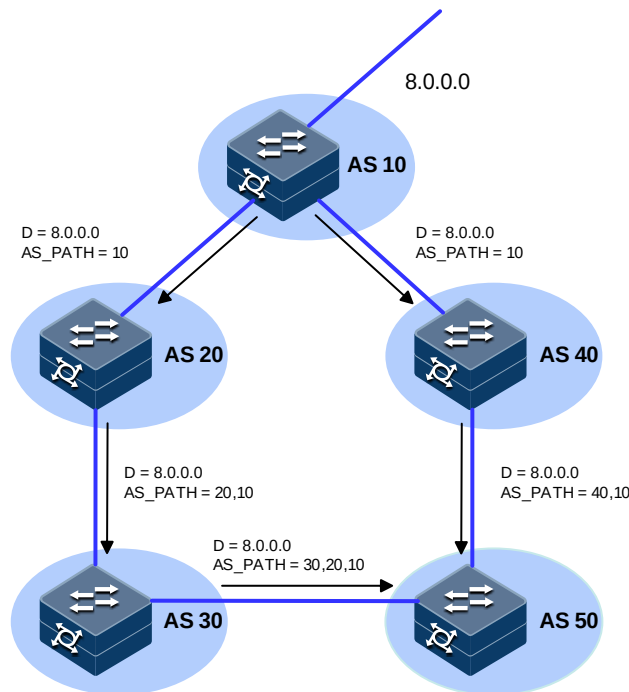
The following ones are common BGP route attributes:

- Origin attribute (well-known mandatory): it defines the origin of the routing information, and identifies how a BGP route is generated. It has the following three types:
 - IGP: high priority. The route is generated within the AS.
 - EGP: medium priority. The route is learnt by EGP.
 - Incomplete: low priority. The origin of the route cannot be determined. For example, the route is redistributed from other routing protocols.
- AS_Path attribute (well-known mandatory): the AS_PATH attribute records all the AS IDs that a route needs to pass through from the local to the destination address. When a BGP router announces a route to another AS, it adds the local AS ID to the AS_PATH list. The BGP router that receives this route can determine the AS that needs to pass through

to reach the destination address based on the AS_PATH attribute. There are two types of AS_PATH attributes:

- AS-SEQUENCE: the AS IDs are arranged in a certain sequence. As shown in the figure below, the adjacent AS IDs closest to the local AS are ranked first, while the other AS IDs are arranged in sequence.
- AS-SET: the AS IDs are simply listed without any sequence.

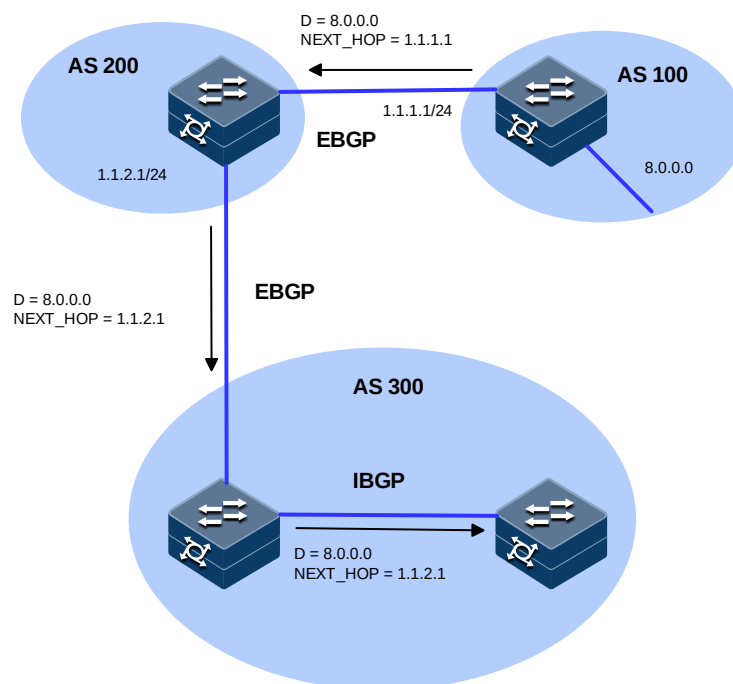
Figure 3-6 AS_PATH attribute



- The AS_PATH attribute has the following usages:
 - Avoiding the forming of routing loops: if the local AS ID is already included in the AS_PATH attribute of the route received by the BGP router, the BGP router considers a routing loop to have occurred by default and will not receive the route.
 - Impacting on route selection: When other factors are the same, BGP will prioritize routes with shorter paths. For example, in the above figure, the BGP router in AS 50 chooses the path passing through AS 40 as the optimal route to the destination address 8.0.0.0. Users can use routing policies to artificially increase the length of AS paths, in order to more flexibly control the selection of BGP paths.
 - Filtering routes: by configuring the AS path filtering list, routes can be filtered based on the AS IDs contained in the AS-PATH attribute.
- Next_Hop attribute (well-known mandatory): the NEXT_HOP attribute value of BGP is not necessarily the IP address of the neighbor router. As shown below, the NEXT_HOP attribute values has the following types:
 - When the BGP speaker sends the generated routes to all neighbors, it configures the NEXT_HOP attribute of the route information to the IP address of the interface connected to peer.
 - When the BGP speaker sends the received route to the EBGP peer, it configures the NEXT_HOP attribute of the route information to the IP address of the interface connected to peer.

- When the BGP speaker sends the route obtained from the EBGP neighbor to the IBGP neighbor, it does not change the NEXT_HOP attribute of the route information.

Figure 3-7 NEXT_HOP attribute

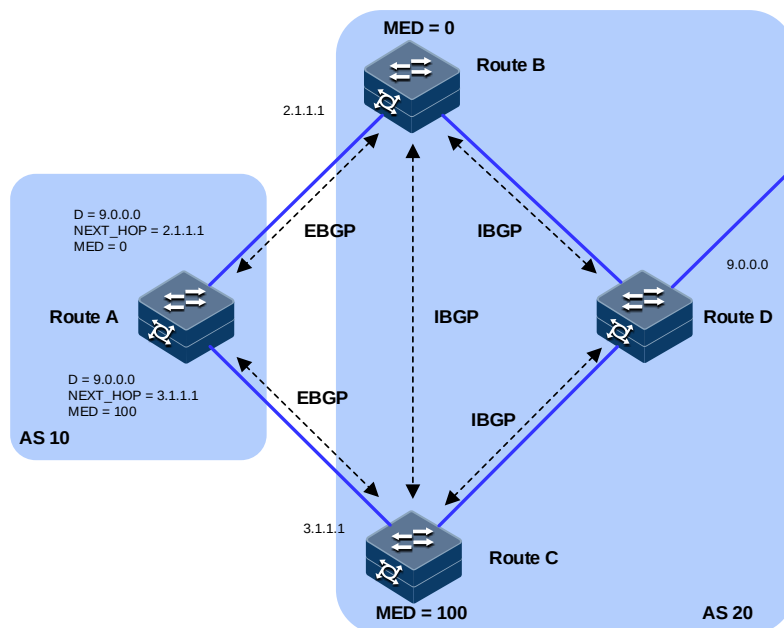


- Multi-Exit Discriminator (MED) (optional non-transitive)

The MED attribute is only exchanged between adjacent ASs, and the ASs that receives this attribute do not notify other ASs.

The MED attribute is equivalent to the metrics used by IGP, which is used to determine the optimal route for traffic entering the AS. When a BGP router obtains multiple routes with the same destination address but different next hops through different EBGP peers, under the same other conditions, the one with the smaller MED value will be prioritized as the optimal route. As shown in the figure below, the flow from AS 10 to AS 20 chooses router B as the entrance. Usually, BGP only compares the MED attribute values of routes from the same AS.

Figure 3-8 MED attribute

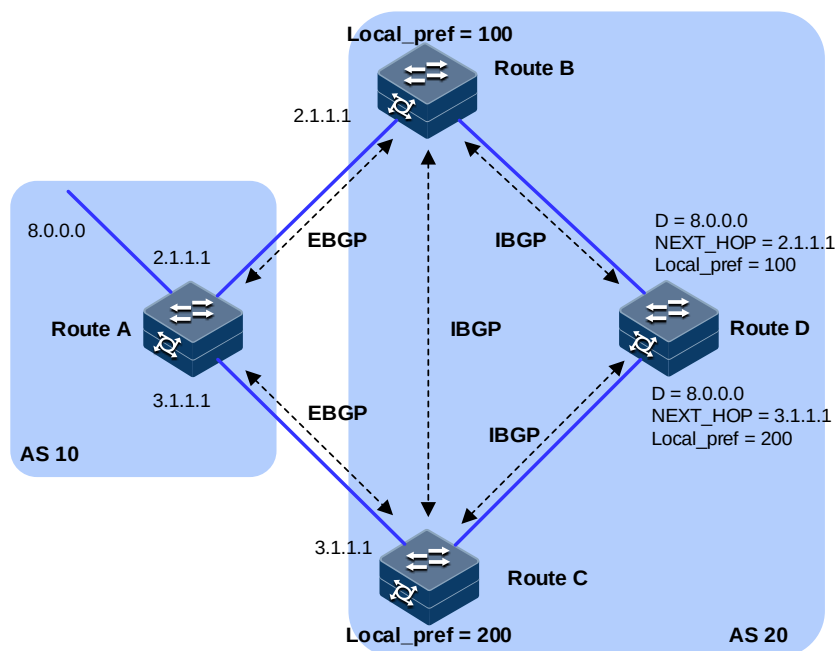


- Local_Pref attribute (well-known discretionary)

The LOCAL-PREF attribute is only exchanged between IBGP peers and is not advertised to other ASs. It indicates the priority of the BGP router.

The LOCAL-PREF attribute is used to determine the optimal route for traffic leaving the AS. When the BGP router obtains multiple routes with the same destination address but different next hops through different IBGP peers, it will prioritize the route with a higher value of the LOCAL-PREF attribute. As shown in the figure below, the flow from AS 20 to AS 10 chooses Router C as the exit.

Figure 3-9 LOCAL_PREF attribute



- Community attributes (optional transitive)

BGP groups routes with the same characteristics into a group, which is called a community. It identifies the community to which the route belongs by carrying community attributes in the route. Groups have no physical boundaries, and routes from different ASs can belong to the same group.

As needed, a route can carry one or more community attribute values (each community attribute value is represented by a 4-byte integer). The router that receives the route can make appropriate adjustments to the route by comparing the group attribute values (such as deciding whether to advertise the route or within what scope), without the need to match complex filtering rules, thus simplifying the application of routing policies and reducing the difficulty of maintenance and management.

- The following are well known community attributes:
 - INTERNET: by default, all routes belong to the INTERNET community. Routes with this attribute can be advertised to all BGP peers.
 - NO-EXPORT: the route with this attribute cannot be advertised outside the local AS after they are received. If a confederation is used, the route cannot be advertised outside the confederation, but can be advertised to other sub-ASs within the confederation.
 - NO_ADVERTISE: after a route with this attribute is received, it cannot be advertised to any other BGP peer.
 - NO-EXPORT-SUBCONFED: after a route with this attribute is received, it cannot be advertised outside the local AS, nor can it be advertised to other sub-ASs in the confederation.

In addition to well known community attributes, users can also use the community attribute list to customize community attributes for more flexible control of routing policies.

Policies for BGP4 to selecting routes

- Select the route with the highest local priority (Local-Pref).
- Optimal aggregation route (the aggregation route has higher priority than non-aggregation route).
- Select the route with the shortest AS path (AS-Path).
- Compare the Origin attributes, and select routes with IGP, EGP, and Incomplete Origin types in sequence.
- Select the route with the lowest MED value.
- Select routes learned from EBGp (EBGP routes have higher priority than IBGP routes).
- Select the route with the lowest metric for the internal IGP in the AS.
- Select the route advertised by the switch with the smallest router ID.
- Compare the IP addresses of peers, and select the route learnt from the peer with the smaller IP address.

Policies for BGP4 to advertise routes

- When there are multiple active routes, the BGP speaker only advertises the optimal route to the peer.
- The BGP speaker only publishes their own routes to peers.
- The BGP speaker advertises the route obtained from EBGp to all its BGP peers except the peer that advertises the BGP peer (including EBGp peers and IBGP peers).

- The BGP speaker does not advertise routes obtained from IBGP to the IBGP peers.
- The BGP speaker advertises the route obtained from IBGP to its EBGP peer (without enabling BGP and IGP synchronization).
- Once the connection is established, the BGP speaker advertises all its BGP routes to the new peer.

BGP4 route aggregation

On the large-scale networks, the BGP routing table is large, so using route aggregation can greatly reduce the size of the BGP routing table.

Route aggregation is actually the process of merging multiple routes. In this way, BGP can only announce the aggregated routes when notifying peers, rather than announcing all specific routes.

BGP4 route attenuation

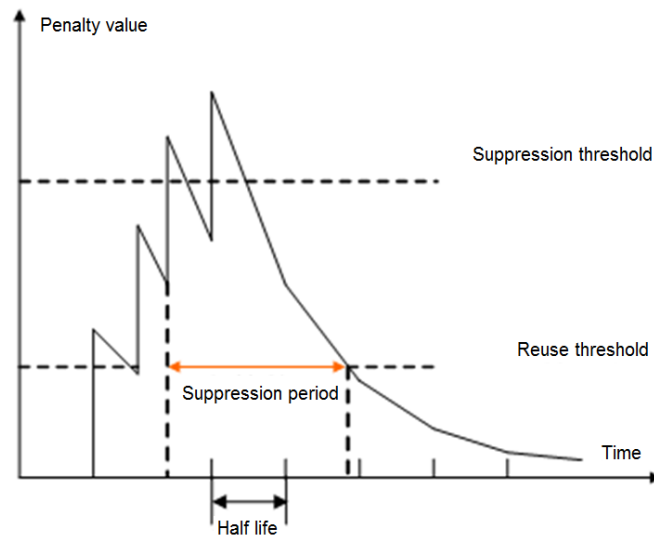
When a route changes, the routing protocol advertise route update to neighbors, and the router that receives the route update needs to recalculate the route and modify the routing table. If routing flapping occurs, namely, unstable routing which is a certain route repeatedly disappears and re-appears in the routing table, this consumes a large amount of bandwidth and CPU resources. In severe cases, this affects the normal operation of the network.

In most cases, BGP is applied in complex network environments with frequent routing changes. To prevent the adverse effects of persistent routing flapping, BGP uses attenuation to suppress unstable routing.

BGP attenuation uses a penalty value to measure the stability of a route, and the higher the penalty value is, the more unstable the route is. Every time when a route changes from reachable status to unreachable status or the properties of reachable routes change, BGP adds a certain penalty value to this route (fixed by the system at 1000 and cannot be modified). When the penalty value exceeds the suppression threshold, this route is suppressed and does not participate in route selection. After the penalty value reaches the configured upper threshold, it cannot continue to increase.

If a flapping route stops flapping, its penalty value will gradually decrease. After each period expires, the penalty value will be decreased by half, which is called the half life. When the penalty value is lower than the reuse threshold, this route becomes available and participates in route selection.

Figure 3-10 BGP route reflector



BGP4 community

A peer group can enable a group of peers to share the same policy, and by using a community it can enable a group of BGP routers in multiple ASs to share the same policy. A community is a routing attribute that is advertised between BGP peers and is not limited by the AS scope.

The BGP router can change the original community attributes of a route before advertising it to other peers.

In addition to using well known community attributes, users can also use community attribute filters to filter and customize extended community attributes for more flexible control of routing policies.

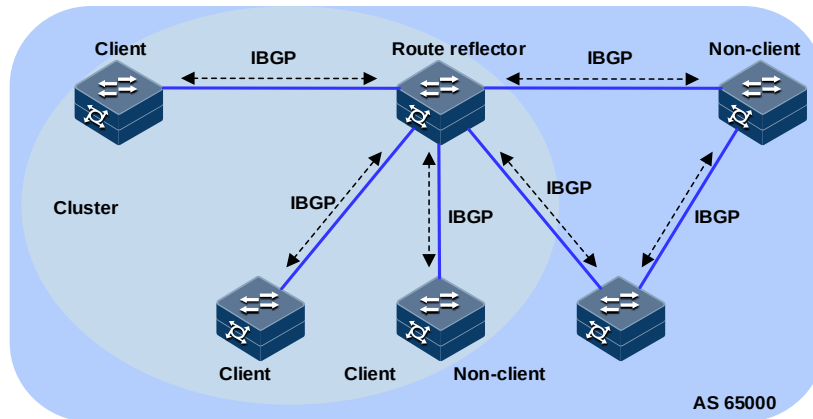
BGP4 route reflector

To ensure the connectivity between IBGP peers, establish a fully connected relationship between IBGP peers. Assuming that there are n switches within an AS, and the number of IBGP connections that should be established is $n*(n-1)/2$. When there are many IBGP peers, they consume a lot of network and CPU resources.

Route reflection can solve this problem. Within an AS, one switch serves as a Route Reflector (RR) while the other switches establish an IBGP connection between the client and the RR. The RR transmits (reflects) routing information between clients, and there is no need to establish a BGP connection between clients.

A BGP router that is neither a reflector nor a client is called a non-client. A fully connected relationship must still be established between the non-client and RR, as well as between all non-clients.

Figure 3-11 BGP route reflector



BGP4 confederation

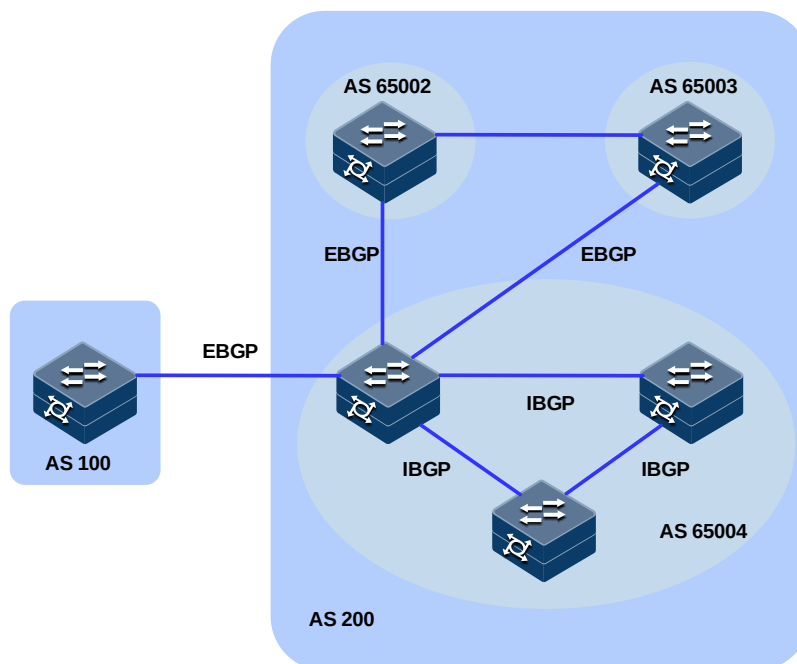
The confederation is another method of dealing with the surge of IBGP network connections within an AS. It divides an AS into several sub-ASs, with IBGP peers within each sub AS establishing a fully connected relationship and EBGP connection relationships between sub-ASs.

In the view of the BGP speaker who does not belong to the confederation, multiple sub-ASs belonging to the same confederation are a whole, and the outside world does not need to know the situation of internal sub-ASs. The confederation ID is the AS ID that identifies the confederation as a whole.

The defect of confederations is that when a confederation transits from non-confederation, switches are required to be reconfigured and the logical topology needs to be changed.

On large BGP networks, route reflectors and confederations can be used simultaneously.

Figure 3-12 BGP confederation



BGP4 MP-BGP

Traditional BGP-4 can manage the routing information of IPv4 only, and it is limited in advertising across ASs when using applications that use other network layer protocols (such as IPv6).

To provide support for multiple network layer protocols, IETF has extended BGP-4 to form MP-BGP. The current MP-BGP standard is RFC2858 (Multiprotocol extensions for BGP-4, a multi-protocol extension of BGP-4).

MP-BGP can transmit routing information for various network layer protocols, such as IPv4 multicast, IPv6 unicast, IPv6 multicast, and VPNv4.

MP-BGP forward compatibility means that switches that support BGP extension can communicate with switches that do not support BGP extension.

Extended attributes of MP-BGP

In the messages used by MP-BGP, three pieces of information related to IPv4 are carried by the Update message, which are NLRI, Next-Hop in the path attribute, and Aggregator in the path attribute (which contains the IP address of the BGP speaker forming the aggregated route).

To support multiple network layer protocols, BGP-4 needs to reflect the information of network layer protocols to NLRI and Next-Hop. Two new path attributes have been introduced in MP-BGP:

- **MP-REACH-NLRI:** Multiprotocol Reachable NLRI. It is used to advertise reachable routes and next hop information.
- **MP_UNREACH-NLRI:** Multiprotocol Unreachable NLRI. It is used to revoke unreachable routes.

Both attributes are optional non-transitive, so the BGP speaker that does not provide multi-protocol capabilities ignores the information of these two attributes and not transmit them to other neighbors.

Address family

MP-BGP uses Address Family and Subsequent Address Family to distinguish the network layer protocol that contains routing information in the MP-REACH-NLRI attribute and MP_UNREACH-NLRI attribute. For example, if the Address Family Identifier (AFI) in the MP-REACH-NLRI attribute is 2 and the Subsequent Address Family Identifier (SAFI) is 1, it indicates that the attribute carries IPv6 unicast routing information. For some values of address families, refer to RFC1700 (Assigned Numbers). MP-BGP extension applications, including VPN extension and IPv6 extension, should be configured in their respective address family views for different extensions.

BFD for BGP

Bidirectional Forwarding Detection (BFD) in IPv4 provides faster link fault detection for BGP.

BFD can quickly detect link fault between BGP peers and report them to BGP, thus implementing fast convergence of BGP routes.

BFD GR

When BGP restarts, this can cause peer relationships to be re-established and forwarding interruptions. Graceful Restart (GR) can avoid traffic interruptions.

3.7.2 Preparing for configurations

Scenario

BGP is another external gateway protocol designed to replace the original EGP. Unlike the original EGP, BGP can perform routing optimization, avoid routing loops, transmit routes more efficiently, and maintain a large amount of routing information.

Prerequisites

The network layer connection between adjacent nodes is reachable.

3.7.3 Default configurations

Default configurations of BGP are as below.

Function	Default value
Global BGP status	Disable
Interval for sending Keepalive messages	30s
Hold time of the peer neighbor relation	90s

3.7.4 Configuring basic functions of BGP

Configure basic functions of BGP for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#bgp as-number	Start BGP, specify the local AS ID, and enter the BGP view.
3	Raisecom(config-bgp)#router-id ipv4-address	Configure the Router ID of BGP.
4	Raisecom(config-bgp)#neighbor { ipv4-address ipv6-address } remote-as as-number	Create a BGP peer.
5	Raisecom(config-bgp)#neighbor ipv4-address update-source ipv4-address Raisecom(config-bgp)#neighbor ipv6-address update-source ipv6-address	Configure the source IP address to be used upon initiating connection.
6	Raisecom (config-bgp)#neighbor { ipv4-address ipv6-address } password { cipher cipher-password plain plain-password }	Configure the BGP peer to perform MD5 authentication on BGP messages upon establishing TCP connections.

Step	Command	Description
7	Raisecom(config-bgp)# neighbor { <i>ipv4-address</i> <i>ipv6-address</i> } ebgp-multihop	Configure the BGP peer to support multi-hop EBGp.
8	Raisecom(config-bgp)# ipv4-family { unicast vpn-instance <i>vpn-instance-name</i> }	Enter the BGP IPv4 unicast or BGP-VPN instance address family view.
9	Raisecom(config-bgp)# ipv6-family { unicast vpn-instance <i>vpn-instance-name</i> }	Enter the BGP IPv6 unicast or BGP-VPN instance address family view.
10	Raisecom(config-bgp-af-*)# neighbor { <i>ipv4-address</i> <i>ipv6-address</i> } enable	Enable the function of exchanging routing information with the specified peer.
11	Raisecom(config-bgp-af-*)# network { <i>ipv4-address/mask-length</i> <i>ipv6-address/mask-length</i> }	Configure the local network routes advertised by BGP; in other words, add the routes in the local routing table to the BGP routing table in static mode, and advertise them to the peer.
12	Raisecom(config-bgp-af-*)# import-route { connected isis [<i>process-id</i>] ospf [<i>process-id</i>] rip [<i>process-id</i>] static } [med <i>med</i> route-policy <i>route-policy-name</i>]	Redistribute routing information about other protocols.

3.7.5 Simplifying IBGP network connection

Simplify IBGP network connection for the device as below.

Step	Command	Description
1	Raisecom(config-bgp-af-*)# neighbor { <i>ipv4-address</i> <i>ipv6-address</i> } route-reflector-client	Configure the local device as the route reflector, and configure the neighbor as the client of the route reflector.
2	Raisecom(config-bgp-af-*)# cluster-id <i>cluster-id</i>	Configure the cluster ID of the route reflector.
3	Raisecom(config-bgp)# confederation identifier <i>as-number</i>	Configure the confederation ID.
4	Raisecom(config-bgp)# confederation peer-as <i>as-number-list</i>	Configure the IDs of the sub-ASs that belong to the same confederation.

3.7.6 Configuring BGP route selection and load balancing

Configure BGP route selection and load balancing for the device as below.

Step	Command	Description
1	<code>Raisecom(config-bgp-af-*)#preference { external { <i>preference</i> default } internal { <i>preference</i> default } local { <i>preference</i> default } }*</code>	Configure the priorities of the external route, internal route, and local route.
2	<code>Raisecom(config-bgp-af-*)#neighbor { <i>ipv4-address</i> <i>ipv6-address</i> } next-hop-local</code>	Configure the next hop property as own IP address when advertising routes to the IBGP peer.
3	<code>Raisecom(config-bgp-af-*)#neighbor { <i>ipv4-address</i> <i>ipv6-address</i> } preference { <i>preference</i> default }</code>	Assign the preferential value to the route received from the peer.
4	<code>Raisecom(config-bgp-af-*)#default local-preference { <i>local-preference</i> default }</code>	Configure the default local priority of BGP.
5	<code>Raisecom(config-bgp)#neighbor { <i>ipv4-address</i> <i>ipv6-address</i> } allow-as-loop { <i>number</i> default }</code>	Configure the local AS ID to appear in the AS_PATH attribute of the route received from the peer, and configure the times of appearance to be allowed.
6	<code>Raisecom(config-bgp-af-*)#default local-med { <i>local-med</i> default }</code>	Configure the default MED of BGP routes.
7	<code>Raisecom(config-bgp-af-*)#community { <i>community-number</i> noadvertise noexport } { additive replace none }</code>	Configure the BGP community attributes.
8	<code>Raisecom(config-bgp-af-*)#neighbor { <i>ipv4-address</i> <i>ipv6-address</i> } advertise-community</code>	Configure the device to advertise the community attributes to the peer.

3.7.7 Controlling advertisement and receiving of BGP routes

Control advertisement and receiving of BGP routes for the device as below.

Step	Command	Description
1	Raisecom(config-bgp-af-*)#summary automatic enable	Enable automatic aggregation (in the BGP-IPv4 unicast address family view or BGP-VPN instance IPv4 address family view).
2	Raisecom(config-bgp-af-*)#summary ipv4-address/prefix-length [aggregated-only]* Raisecom(config-bgp-af-*)#ipv6 summary ipv6-address/prefix-length [aggregated-only]*	Create an aggregation item in the BGP routing table.
3	Raisecom(config-bgp-af-*)#filter-policy import route-policy route-policy-name	Configure the global importing filtering policy of BGP.
4	Raisecom(config-bgp-af-*)#filter-policy export [static connected rip ospf isis] route-policy route-policy-name	Configure the global exporting filtering policy of BGP.

3.7.8 Controlling and adjusting the convergence speed of the BGP network

Control and adjust the convergence speed of the BGP network for the device as below.

Step	Command	Description
1	Raisecom(config-bgp)#neighbor { ipv4-address ipv6-address } connect-retry-interval { seconds default }	Configure the connection retry interval of the peer.
2	Raisecom(config-bgp)#neighbor { ipv4-address ipv6-address } keepalive-timer { keepalive-time default } hold-timer { hold-time default }	Configure the KeepAlive time and hold time of the BGP session between the local router and specified peer.
3	Raisecom(config-bgp)#neighbor { ipv4-address ipv6-address } advertisement-interval { seconds default }	Configure the advertisement interval.
4	Raisecom(config-bgp-af-*)#dampening half-life-reach { half-life-time default } reuse { reuse default } suppress { suppress default } ceiling { max default }	Configure parameters of route suppression.
5	Raisecom(config-bgp-af-*)#dampening enable	Enable route suppression.

3.7.9 Configuring BGP reliability

Configure BGP reliability for the device as below.

Step	Command	Description
1	Raisecom(config-bgp)#graceful-restart enable	Enable BGP GR.
2	Raisecom(config-bgp)#graceful-restart timer restart { timer default }	Configure the time for the peer to wait for re-establishing the BGP session.
3	Raisecom(config-bgp)#graceful-restart timer selection-deferral { timer default }	Configure the time for the local to wait for the End-Of-RIB tag.
4	Raisecom(config-bgp)#neighbor { ipv4-address ipv6-address } bfd enable	Create a BFD session for the peer.

3.7.10 Checking configurations

Use the following commands to check configuration results.

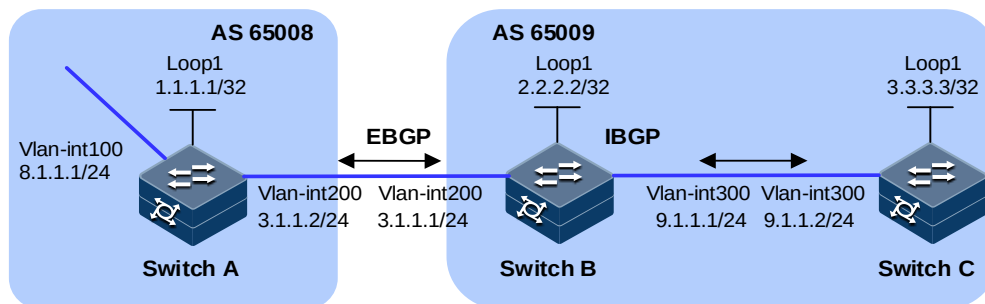
No.	Command	Description
1	Raisecom#show bgp config	Show BGP configurations.
2	Raisecom#show bgp neighbor [ip-address ipv4-address ipv6-address ipv6-address]	Show the status of the BGP peer.
3	Raisecom#show bgp ip-route Raisecom#show bgp ipv6-route	Show the BGP routing table.

3.7.11 Example for configuring basic functions of BGP

Networking requirements

As shown below, all switches run BGP. EBGP is required to be established between switch A and switch B. IBGP is required to be established between switch B and switch C. In this way, switch C can access the 8.1.1.0/24 network segment directly connected to switch A.

Figure 3-13 Networking with basic functions of BGP



Configuration steps

Step 1 Configure IP addresses of the interfaces.

Step 2 Configure the IBGP connection.

Use OSPF inside AS 65009. Ensure that the route between switch B and Loopback interface on switch C is reachable and the route between switch C and Loopback interface on switch B is reachable.

```
SwitchB#configure
SwitchB(config)#ospf 1
SwitchB(config-ospf-1)#router-id 2.2.2.2
SwitchB(config-ospf-1)#network 2.2.2.2 255.255.255.255 area 0
SwitchB(config-ospf-1)#network 9.1.1.0 255.255.255.0 area 0
SwitchB(config-ospf-1)#end
```

```
SwitchC#configure
SwitchC(config)#ospf 1
SwitchC(config-ospf-1)#router-id 3.3.3.3
SwitchC(config-ospf-1)#network 3.3.3.3 255.255.255.255 area 0
SwitchC(config-ospf-1)#network 9.1.1.0 255.255.255.0 area 0
SwitchC(config-ospf-1)#end
```

To prevent unstable interface status from causing route flapping, this example uses the Loopback interface to create an IBGP peer.

```
SwitchB#configure
SwitchB(config)#bgp 65009
SwitchB(config-bgp)#neighbor 3.3.3.3 remote-as 65009
SwitchB(config-bgp)#neighbor 3.3.3.3 update-source 2.2.2.2
SwitchB(config-bgp)#end
```

```
SwitchC#configure
SwitchC(config)#bgp 65009
SwitchC(config-bgp)#neighbor 2.2.2.2 remote-as 65009
SwitchC(config-bgp)#neighbor 2.2.2.2 update-source 3.3.3.3
SwitchC(config-bgp)#end
```

Step 3 Configure the EBGp connection.

The two routers in the EBGp neighbor relationship (usually belonging to two different carriers) are located in different AS domains, and the route to the Loopback interface on the peer end is generally unreachable. Therefore, the directly connected IP address is generally used to establish BGP neighbors.

Because switch C is required to access the 8.1.1.0/24 network segment directly connected to Switch A, the 8.1.1.0/24 network segment route is advertised to the BGP routing table after the EBGp connection is established.

```
SwitchA#configure
SwitchA(config)#bgp 65008
SwitchA(config-bgp)#neighbor 3.1.1.1 remote-as 65009
SwitchA(config-bgp)#ipv4-family unicast
SwitchA(config-bgp-af-ipv4)#network 8.1.1.0/24
SwitchA(config-bgp-af-ipv4)#end
```

```
SwitchB#configure
SwitchB(config)#bgp 65009
SwitchB(config-bgp)#neighbor 3.1.1.2 remote-as 65008
SwitchB(config-bgp)#exit
SwitchB(config)#show bgp neighbor
```

```
BGP local router ID :2.2.2.2
Local AS number :65009
Total number of neighbors :2
Neighbors in established state:2
Neighbor          Ver AS      MsgIn    MsgOut    Up/Down
State/Change      VpnInstance
3.1.1.2            4  65008    65        64        00:26:44 Established/1
N/A
3.3.3.3            4  65009    78        78        00:32:19 Established/1
N/A
```

As you can see, the BGP connection between switch B and switch C and that between switch B and on switch A are already established.

Use the following command to show the BGP routing table of each switch.

```
SwitchA#configure
SwitchA(config)#show bgp ip-route
```

DestAddr/Prefixlen	Neighbor	Nexthop	Protocol
Med	LocalPrf	Origin	Vpn-Instance
		As-Path	
8.1.1.0/24	0.0.0.0	0.0.0.0	other
0	IGP	public	0
Total:1			

```
SwitchB#configure
SwitchB(config)#show bgp ip-route
DestAddr/Prefixlen      Neighbor      Nexthop      Protocol
Med      LocalPrf      Origin      Vpn-Instance  As-Path
-----
8.1.1.0/24      3.1.1.2      3.1.1.2      bgp      0
0      IGP      public      AS_SEQUENCE 65008
-----
Total:1
```

```
SwitchC#configure
SwitchC(config)#show bgp ip-route
DestAddr/Prefixlen      Neighbor      Nexthop      Protocol
Med      LocalPrf      Origin      Vpn-Instance  As-Path
-----
8.1.1.0/24      2.2.2.2      3.1.1.2      bgp      0
100      IGP      public      AS_SEQUENCE 65008
-----
Total:1
```

As you can see from the routing table, switch A has not learnt any route inside AS 65009, and switch C has learnt the 8.1.1.0 route inside AS 65008, which is an invalid route because the next hop 3.1.1.2 is unreachable.

Step 4 Configure the EBGp connection.

Configure BGP on switch B to redistribute the directly connected route so that switch A can learn the route in the 9.1.1.0/24 network segment and switch C can learn the route in the 3.1.1.0/24 network segment.

```
SwitchB#configure
SwitchB(config)#bgp
SwitchB(config-bgp)#ipv4-family unicast
SwitchB(config-bgp-af-ipv4)#import-route connected
SwitchB(config-bgp-af-ipv4)#end
```

Use the following command to show the BGP routing tables of switch A and switch C.

```
SwitchA#configure
SwitchA(config)#show bgp ip-route
DestAddr/Prefixlen      Neighbor      Nexthop      Protocol
Med      LocalPrf      Origin      Vpn-Instance  As-Path
-----
-----
```

```

2.2.2.2/32          3.1.1.1          3.1.1.1          bgp      0
0          Incomplete public          AS_SEQUENCE 65009
3.1.1.0/24         3.1.1.1          3.1.1.1          bgp      0
0          Incomplete public          AS_SEQUENCE 65009
8.1.1.0/24         0.0.0.0          0.0.0.0          other    0
0          IGP      public
9.1.1.0/24         3.1.1.1          3.1.1.1          bgp      0
0          Incomplete public          AS_SEQUENCE 65009

```

Total:4

SwitchC#configure

SwitchC(config)#show bgp ip-route

DestAddr/Prefixlen	Neighbor	Nexthop	Protocol
Med	LocalPrf	Origin	Vpn-Instance
		As-Path	
2.2.2.2/32	2.2.2.2	2.2.2.2	bgp 0
100	Incomplete	public	
3.1.1.0/24	2.2.2.2	2.2.2.2	bgp 0
100	Incomplete	public	
8.1.1.0/24	2.2.2.2	3.1.1.2	bgp 0
100	IGP	public	AS_SEQUENCE 65008
9.1.1.0/24	2.2.2.2	2.2.2.2	bgp 0
100	Incomplete	public	

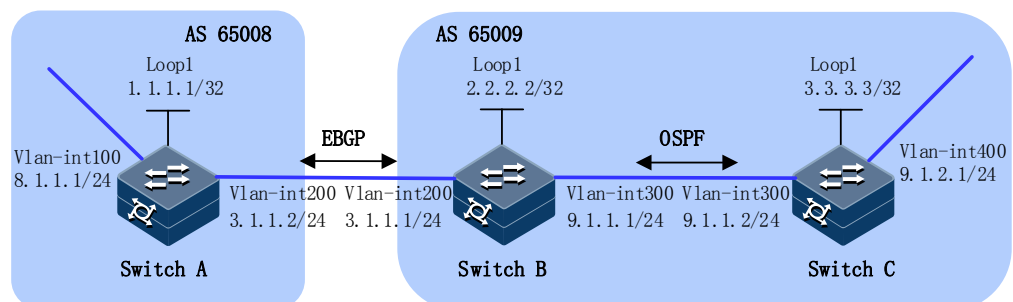
Total:4

3.7.12 Example for configuring interaction between BGP and IGP

Networking requirements

As shown below, all devices of company A are in AS 65008, all devices of company B are in AS 65009, AS 65008 and AS 65009 are connected by switch A and switch B. Switch A is required to access the 9.1.2.0/24 network segment in AS 65009. Switch C is required to access the 8.1.2.0/24 network segment in AS 65008.

Figure 3-14 Networking with interaction between BGP and IGP



Configuration steps

Step 1 Configure IP addresses of interfaces.

Step 2 Configure OSPF.

Configure OSPF in AS 65009 so that switch B can learn routes in the 9.1.2.0/24 network segment.

```
SwitchB#configure
SwitchB(config)#ospf 1
SwitchB(config-ospf-1)#router-id 2.2.2.2
SwitchB(config-ospf-1)#network 2.2.2.2 255.255.255.255 area 0
SwitchB(config-ospf-1)#network 9.1.1.0 255.255.255.0 area 0
SwitchB(config-ospf-1)#end
```

```
SwitchC#configure
SwitchC(config)#ospf 1
SwitchC(config-ospf-1)#router-id 3.3.3.3
SwitchC(config-ospf-1)#network 9.1.1.0 255.255.255.0 area 0
SwitchC(config-ospf-1)#import-route connect
SwitchC(config-ospf-1)#end
```

Step 3 Configure the EBGp connection.

Configure the EBGp connection. Advertise the 8.1.1.0/24 network segment to the BGP routing table on switch A so that switch B can learn routes in the 8.1.1.0/24 network segment.

```
SwitchA#configure
SwitchA(config)#bgp 65008
SwitchA(config-bgp)#neighbor 3.1.1.1 remote-as 65009
SwitchA(config-bgp)#ipv4-family unicast
SwitchA(config-bgp-af-ipv4)#network 8.1.1.0/24
SwitchA(config-bgp-af-ipv4)#end
```

```
SwitchB#configure
SwitchB(config)#bgp 65009
SwitchB(config-bgp)#neighbor 3.1.1.2 remote-as 65008
SwitchB(config-bgp)#end
```

Step 4 Configure interaction between BGP and IGP.

Configure BGP to redistribute OSPF routes on switch B so that switch A can learn routes in the 9.1.2.0/24 network segment.

Configure OSPF to redistribute BGP routes on switch B so that switch C can learn routes in the 8.1.1.0/24 network segment.

```
SwitchB#configure
SwitchB(config)#bgp
```

```
SwitchB(config-bgp)#ipv4-family unicast
SwitchB(config-bgp-af-ipv4)#import-route ospf 1
SwitchB(config-bgp-af-ipv4)#end
SwitchB#configure
SwitchB(config)#ospf 1
SwitchB(config-ospf-1)#import-route bgp
SwitchB(config-ospf-1)#end
```

Use the following command to show the BGP routing table of switch A.

```
SwitchA#configure
SwitchA(config)#show bgp ip-route
```

DestAddr/Prefixlen	Neighbor	Nexthop	Protocol
Med	LocalPrf	Origin	Vpn-Instance
As-Path			
2.2.2.2/32	3.1.1.1	3.1.1.1	bgp
0	Incomplete	public	AS_SEQUENCE 65009
3.3.3.3/32	3.1.1.1	3.1.1.1	bgp
0	Incomplete	public	AS_SEQUENCE 65009
8.1.1.0/24	0.0.0.0	0.0.0.0	other
0	IGP	public	
9.1.1.0/24	3.1.1.1	3.1.1.1	bgp
0	Incomplete	public	AS_SEQUENCE 65009
9.1.2.0/24	3.1.1.1	3.1.1.1	bgp
0	Incomplete	public	AS_SEQUENCE 65009

Total:5

Use the following command to show the OSPF routing table of switch C.

```
SwitchC#configure
SwitchC(config)#show ospf route
```

OSPF Process 1

RouteType	Prefix	PathType	Cost	Cost2	NextHop
ASBR	2.2.2.2/32	INTRA	1	0	9.1.1.1
0.0.0.0	0				0:01:33
Network	2.2.2.2/32	INTRA	2	0	9.1.1.1
0.0.0.0	N/A				0:01:33
Network	8.1.1.0/24	ASE2	1	1	9.1.1.1
0.0.0.0	N/A				0:01:33
Network	9.1.1.0/24	INTRA	1	0	9.1.1.2
0.0.0.0	N/A				0:01:38

Route :

ABR	ASBR	Network	Intra	Inter	External
0	1	3	2	0	1

Path :

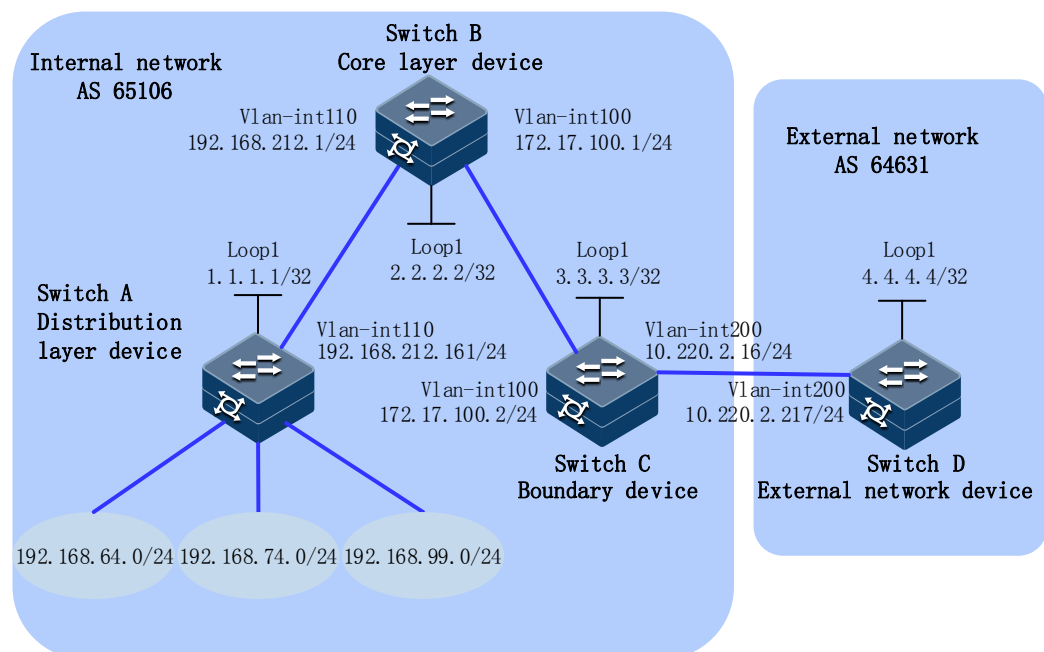
ABR	ASBR	Network	Intra	Inter	External
0	1	3	2	0	1

3.7.13 Example for configuring BGP route aggregation

Networking requirements

As shown below, by establishing an EBGP connection between the boundary device Switch C and the external network device Switch D, the company's internal network and external network can be interconnected. Within the company, a static route is configured between the core layer device Switch B and the aggregation layer device Switch A, while OSPF is configured between Switch B and Switch C. The static route is redistributed into OSPF route to implementing interoperability within the company internal network, including three network segments: 192.168.64.0/24, 192.168.74.0/24, and 192.168.99.0/24. Configure route aggregation on Switch C to aggregate the routes of these three network segments into one route to reduce the number of routes advertised through BGP.

Figure 3-15 BGP route aggregation networking



Configuration steps

- Step 1 Configure IP addresses of interfaces.
- Step 2 Configure a static route between Switch A and Switch B.

```
SwitchA#configure
SwitchA(config)#ip route-static 0.0.0.0 0.0.0.0 192.168.212.1

SwitchB#configure
```

```
SwitchB(config)#ip route-static 192.168.64.0 255.255.255.0
192.168.212.161
SwitchB(config)#ip route-static 192.168.74.0 255.255.255.0
192.168.212.161
SwitchB(config)#ip route-static 192.168.99.0 255.255.255.0
192.168.212.161
```

Step 3 Configure OSPF between Switch B and Switch C, and redistribute the static route.

```
SwitchB#configure
SwitchB(config)#ospf 1
SwitchB(config-ospf-1)#network 172.17.100.0 255.255.255.0 area 0
SwitchB(config-ospf-1)#import-route static
SwitchB(config-ospf-1)#end
```

```
SwitchC#configure
SwitchC(config)#ospf 1
SwitchC(config-ospf-1)#network 172.17.100.0 255.255.255.0 area 0
SwitchC(config-ospf-1)#network 10.220.2.0 255.255.255.0 area 0
SwitchC(config-ospf-1)#end
```

Check the routing table on switch C. As you can see, switch C has learnt routes to the 192.168.64.0/24, 192.168.74.0/24, and 192.168.99.0/24 network segments through OSPF.

```
SwitchC#configure
SwitchC(config-ospf-1)#show ospf route
  OSPF Process 1
  RoutType Prefix          PathType Cost    Cost2    NextHop
BackupNextHop AreaId Time
ASBR 2.2.2.2/32          INTRA    1        0        172.17.100.1
0.0.0.0 0 0:00:17
Network 10.220.2.0/24    INTRA    1        0        10.220.2.16
0.0.0.0 N/A 0:01:01
Network 172.17.100.0/24    INTRA    1        0        172.17.100.2
0.0.0.0 N/A 0:00:20
Network 192.168.64.0/24    ASE2     1        1        172.17.100.1
0.0.0.0 N/A 0:00:17
Network 192.168.74.0/24    ASE2     1        1        172.17.100.1
0.0.0.0 N/A 0:00:17
Network 192.168.99.0/24    ASE2     1        1        172.17.100.1
0.0.0.0 N/A 0:00:17
Route :
ABR ASBR Network Intra Inter External
0 1 5 2 0 3

Path :
ABR ASBR Network Intra Inter External
0 1 5 2 0 3
```

Step 4 Configure BGP between Switch C and Switch D, and redistribute the OSPF routes.

```
SwitchC#configure
SwitchC(config)#bgp 65106
SwitchC(config-bgp)#router-id 3.3.3.3
SwitchC(config-bgp)#neighbor 10.220.2.217 remote-as 64631
SwitchC(config-bgp)#ipv4-family unicast
SwitchC(config-bgp-af-ipv4)#import-route ospf
SwitchC(config-bgp-af-ipv4)#end
```

```
SwitchD#configure
SwitchD(config)#bgp 64631
SwitchD(config-bgp)#router-id 4.4.4.4
SwitchD(config-bgp)#neighbor 10.220.2.16 remote-as 65106
SwitchD(config-bgp)#end
```

Check the routing table on switch D. As you can see, switch D has learnt routes to the 192.168.64.0/24, 192.168.74.0/24, and 192.168.99.0/24 network segments through BGP. Switch D can ping through hosts in these segments.

```
SwitchD#configure
SwitchD(config-bgp)#show ip route
Max Routing Number Limit: 131072
Max Destination Number Limit: 771
Routing Tables:
```

Destination	Gateway	Pre/Cost	Proto	Interface	
Mpls	Status	Vpn-Instance			
4.4.4.4/32	4.4.4.4	0/0	local	loopback-1	no
Up	N/A				
10.220.2.0/24	10.220.2.217	0/0	local	vlan-200	no
Up	N/A				
10.220.2.217/32	10.220.2.217	0/0	local	vlan-200	no
Up	N/A				
127.0.0.1/32	127.0.0.1	0/0	local	loopback-0	no
Up	N/A				
172.17.100.0/24	10.220.2.16	255/1	bgp	vlan-200	no
Up	N/A				
192.168.64.0/24	10.220.2.16	255/1	bgp	vlan-200	no
Up	N/A				
192.168.74.0/24	10.220.2.16	255/1	bgp	vlan-200	no
Up	N/A				
192.168.99.0/24	10.220.2.16	255/1	bgp	vlan-200	no
Up	N/A				
Total: 8	Static: 0	Down: 0		Destination: 8	

- Step 5 Configure route aggregation on switch C to aggregate 192.168.64.0/24, 192.168.74.0/24, and 192.168.99.0/24 into 192.168.64.0/18 and to suppression the advertisement of specific routes.

```
SwitchC#configure
SwitchC(config)#bgp
SwitchC(config-bgp)#ipv4-family unicast
SwitchC(config-bgp-af-ipv4)#summary 192.168.64.0/18 aggregated-only
SwitchC(config-bgp-af-ipv4)#end
```

Check the routing table on switch D. As you can see, the routes to the 192.168.64.0/24, 192.168.74.0/24, and 192.168.99.0/24 into 192.168.64.0/18 segments on switch D is aggregated into one route 192.168.64.0/18. Switch D can ping through hosts in these segments.

```
SwitchD#configure
SwitchD(config-bgp)#show ip route
Max Routing Number Limit: 131072
Max Destination Number Limit: 771
Routing Tables:
```

Destination Mpls	Status	Gateway Vpn-Instance	Pre/Cost	Proto	Interface	
4.4.4.4/32	Up	4.4.4.4	0/0	local	loopback-1	no
10.220.2.0/24	Up	10.220.2.217	0/0	local	vlan-200	no
10.220.2.217/32	Up	10.220.2.217	0/0	local	vlan-200	no
127.0.0.1/32	Up	127.0.0.1	0/0	local	loopback-0	no
172.17.100.0/24	Up	10.220.2.16	255/1	bgp	vlan-200	no
192.168.64.0/18	Up	10.220.2.16	255/0	bgp	vlan-200	no

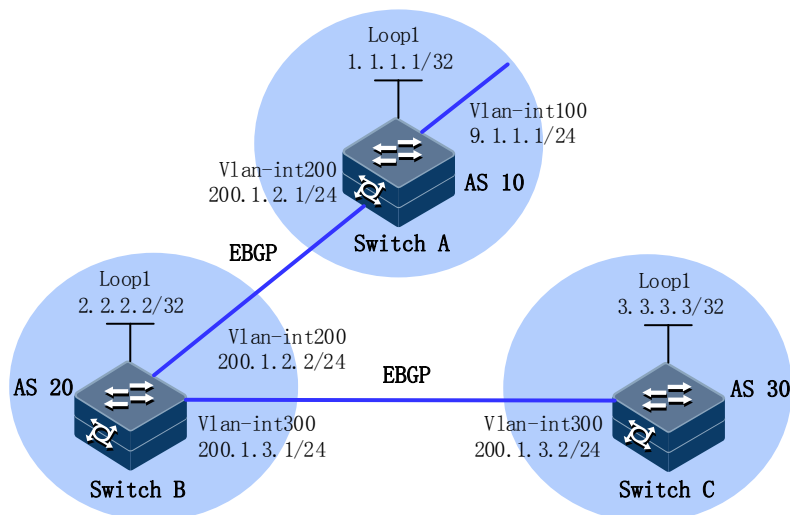
Total: 6		Static: 0	Down: 0		Destination: 6	

3.7.14 Example for configuring BGP community

Networking requirements

As shown below, EBGp connections are established between Switch B and Switch A, and between Switch B and Switch C. By configuring the NO-EXPORT community attribute on Switch A, the routes advertised by AS 10 to AS 20 are not advertised by AS 20 to other ASs.

Figure 3-16 BGP community networking



Configuration steps

Step 1 Configure IP addresses of interfaces.

Step 2 Configure EGBP.

```
SwitchA#configure
SwitchA(config)#bgp 10
SwitchA(config-bgp)#router-id 1.1.1.1
SwitchA(config-bgp)#neighbor 200.1.2.2 remote-as 20
SwitchA(config-bgp)#ipv4-family unicast
SwitchA(config-bgp-af-ipv4)#network 9.1.1.0/24
SwitchA(config-bgp-af-ipv4)#end
```

```
SwitchB#configure
SwitchB(config)#bgp 20
SwitchB(config-bgp)#router-id 2.2.2.2
SwitchB(config-bgp)#neighbor 200.1.2.1 remote-as 10
SwitchB(config-bgp)#neighbor 200.1.3.2 remote-as 30
SwitchB(config-bgp)#end
```

```
SwitchC#configure
SwitchC(config)#bgp 30
SwitchC(config-bgp)#router-id 3.3.3.3
SwitchC(config-bgp)#neighbor 200.1.3.1 remote-as 20
```

Use the following commands to show the routing tables of Switch B and Switch C.

```
SwitchB#configure
SwitchB(config)#show bgp ip-route
```

DestAddr/Prefixlen	Neighbor	Nexthop	Protocol
Med	LocalPrf	Origin	Vpn-Instance
		As-Path	

```

-----
9.1.1.0/24      200.1.2.1      200.1.2.1      bgp      0
0      IGP      public      AS_SEQUENCE 10
-----
Total:1

SwitchC#configure
SwitchC(config)#show bgp ip-route
DestAddr/PrefixLen  Neighbor      Nexthop      Protocol
Med      LocalPrf  Origin      Vpn-Instance  As-Path
-----
9.1.1.0/24      200.1.3.1      200.1.3.1      bgp      0
0      IGP      public      AS_SEQUENCE 20,10
-----
Total:1

```

As you can see, Switch C has learnt the route to the 9.1.1.0/24 from Switch B.

Step 3 Configure attributes of the BGP community.

```

SwitchA#configure
SwitchA(config)#bgp
SwitchA(config-bgp)#ipv4-family unicast
SwitchA(config-bgp-af-ipv4)#community noexport additive
SwitchA(config-bgp-af-ipv4)#neighbor 200.1.2.2 advertise-community

```

Use the following commands to show the routing tables of Switch B and Switch C.

```

SwitchB#configure
SwitchB(config)#show bgp ip-route destination-address 9.1.1.0/24
BGP routing table entry information

Network      :9.1.1.0/24
Peer         :200.1.2.1
NextHop      :200.1.2.1
Protocol     :bgp
Med          :0
Local Preference  :0
As-Path      :AS_SEQUENCE 10
Origin       :IGP
Best         :True
InLabel      :0
OutLabel     :0
AtomicAggr   :0
HWState      :1
HWUpdateTime  :0h:2m:58s

```



```

SummaryRoute      :0
SummaryFilter      :0
WaitDelete        :0
BestSysroute      :1
MPLSUpdate        :0
ImportFiltered    :0
IGPSyncwait       :0
SourceVRF         :0
Damp Supressed    :N
DirectNexthop     :200.1.2.1
Less Priority Reason :none
Community         :ffffff01
VPN-Instance      :public
  
```

```

SwitchC#configure
SwitchC(config)#show bgp ip-route
  
```

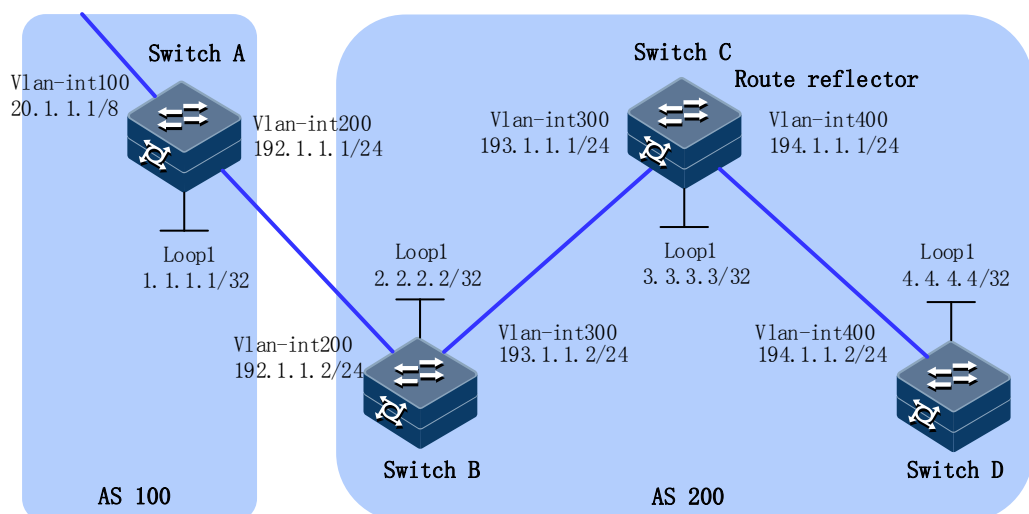
You can see the configured community properties in the BGP routing table on Switch B. Switch B does not advertise the route to 9.1.1.0/24 through BGP.

3.7.15 Example for configuring BGP route reflector

Networking requirements

As shown below, all switches are running BGP. Switch A establishes an EBGP connection with Switch B, and Switch C establishes an IBGP connection with Switch B and Switch D. Switch C serves as a route reflector, while Switch B and Switch D are the clients of Switch C. Switch D can learn route 20.0.0.0/8 through Switch C.

Figure 3-17 BGP route reflector networking



Configuration steps

Step 1 Configure IP addresses of interfaces.

Step 2 Configure OSPF in AS 200.

```
SwitchB#configure
SwitchB(config)#ospf 1
SwitchB(config-ospf-1)#router-id 2.2.2.2
SwitchB(config-ospf-1)#network 193.1.1.0 255.255.255.0 area 0
SwitchB(config-ospf-1)#network 2.2.2.2 255.255.255.255 area 0
SwitchB(config-ospf-1)#end
```

```
SwitchC#configure
SwitchC(config)#ospf 1
SwitchC(config-ospf-1)#router-id 3.3.3.3
SwitchC(config-ospf-1)#network 193.1.1.0 255.255.255.0 area 0
SwitchC(config-ospf-1)#network 194.1.1.0 255.255.255.0 area 0
SwitchC(config-ospf-1)#network 3.3.3.3 255.255.255.255 area 0
```

```
SwitchD#configure
SwitchD(config)#ospf 1
SwitchD(config-ospf-1)#router-id 4.4.4.4
SwitchD(config-ospf-1)#network 194.1.1.0 255.255.255.0 area 0
SwitchD(config-ospf-1)#network 4.4.4.4 255.255.255.255 area 0
SwitchD(config-ospf-1)#end
```

Step 3 Configure BGP connections.

```
SwitchA#configure
SwitchA(config)#bgp 100
SwitchA(config-bgp)#router-id 1.1.1.1
SwitchA(config-bgp)#neighbor 192.1.1.2 remote-as 200
SwitchA(config-bgp)#ipv4-family unicast
SwitchA(config-bgp-af-ipv4)#network 20.0.0.0/8
SwitchA(config-bgp-af-ipv4)#end
```

```
SwitchB#configure
SwitchB(config)#bgp 200
SwitchB(config-bgp)#router-id 2.2.2.2
SwitchB(config-bgp)#neighbor 192.1.1.1 remote-as 100
SwitchB(config-bgp)#neighbor 193.1.1.1 remote-as 200
SwitchB(config-bgp)#ipv4-family unicast
SwitchB(config-bgp-af-ipv4)#neighbor 193.1.1.1 next-hop-local
SwitchB(config-bgp-af-ipv4)#end
```

```
SwitchC#configure
SwitchC(config)#bgp 200
SwitchC(config-bgp)#router-id 3.3.3.3
SwitchC(config-bgp)#neighbor 193.1.1.2 remote-as 200
SwitchC(config-bgp)#neighbor 194.1.1.2 remote-as 200
SwitchC(config-bgp)#end
```

```
SwitchD#configure
SwitchD(config)#bgp 200
```

```
SwitchD(config-bgp)#router-id 4.4.4.4
SwitchD(config-bgp)#neighbor 194.1.1.1 remote-as 200
SwitchD(config-bgp)#end
```

Step 4 Configure the route reflector.

```
SwitchC#configure
SwitchC(config)#bgp
SwitchC(config)#ipv4-family unicast
SwitchC(config-bgp-af-ipv4)#neighbor 193.1.1.2 route-reflector-client
SwitchC(config-bgp-af-ipv4)#neighbor 194.1.1.2 route-reflector-client
SwitchC(config-bgp-af-ipv4)#end
```

Use the following commands to show the BGP routing tables of Switch B and Switch D.

```
SwitchB#configure
SwitchB(config)#show bgp ip-route
```

DestAddr/Prefixlen	Neighbor	Nexthop	Protocol
Med	LocalPrf	Origin	Vpn-Instance
As-Path			
20.0.0.0/8	192.1.1.1	192.1.1.1	bgp
0	IGP	public	AS_SEQUENCE 100

Total:1

```
SwitchD#configure
SwitchD(config)#show bgp ip-route
```

DestAddr/Prefixlen	Neighbor	Nexthop	Protocol
Med	LocalPrf	Origin	Vpn-Instance
As-Path			
20.0.0.0/8	194.1.1.1	193.1.1.2	bgp
100	IGP	public	AS_SEQUENCE 100

Total:1

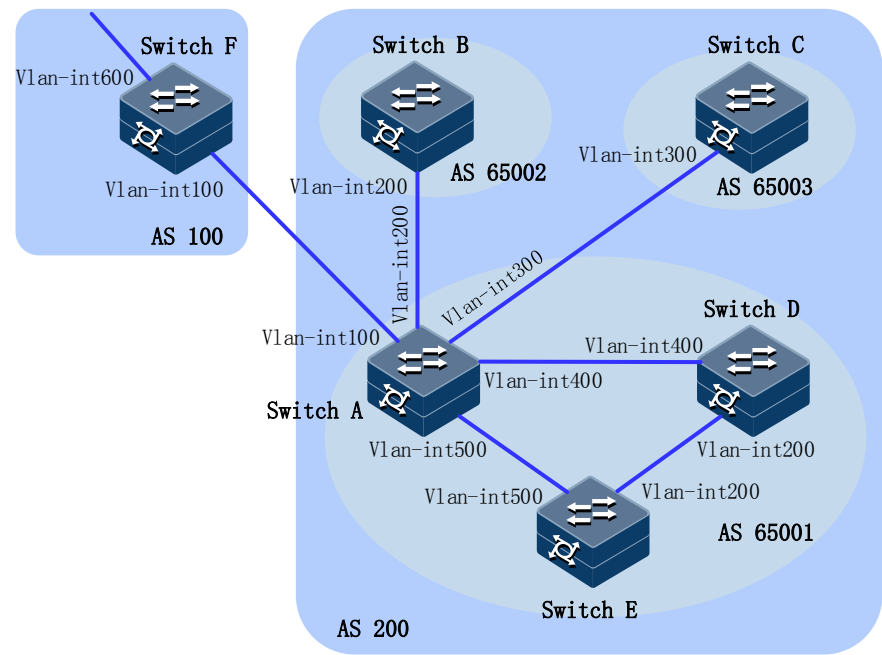
As you can see, Switch D has learnt route 20.0.0.0/8 from Switch C.

3.7.16 Example for configuring BGP confederation

Networking requirements

As shown below, there are multiple BGP switches in AS 200. To reduce the number of IBGP connections, they are now divided into three sub-ASs: AS 65001, AS 65002, and AS 65003. The three switches in AS 65001 are fully connected through IBGP.

Figure 3-18 BGP confederation networking



Device	Interface	IP address
Switch A	Vlan-int100	200.1.1.1/24
	Vlan-int200	10.1.1.1/24
	Vlan-int300	10.1.2.1/24
	Vlan-int400	10.1.3.1/24
	Vlan-int500	10.1.4.1/24
Switch B	Vlan-int200	10.1.1.2/24
Switch C	Vlan-int300	10.1.2.2/24
Switch D	Vlan-int200	10.1.5.1/24
	Vlan-int400	10.1.3.2/24
Switch E	Vlan-int200	10.1.5.2/24
	Vlan-int500	10.1.4.2/24
Switch F	Vlan-int100	200.1.1.2/24
	Vlan-int600	9.1.1.1/24

Configuration steps

- Step 1 Configure IP addresses of interfaces.
- Step 2 Configure BGP confederation.

```
SwitchA#configure
SwitchA(config)#bgp 65001
SwitchA(config-bgp)#router-id 1.1.1.1
SwitchA(config-bgp)#confederation identifier 200
SwitchA(config-bgp)#confederation peer-as 65002,65003
SwitchA(config-bgp)#neighbor 10.1.1.2 remote-as 65002
SwitchA(config-bgp)#neighbor 10.1.2.2 remote-as 65003
SwitchA(config-bgp)#ipv4-family unicast
SwitchA(config-bgp-af-ipv4)#neighbor 10.1.1.2 next-hop-local
SwitchA(config-bgp-af-ipv4)#neighbor 10.1.2.2 next-hop-local
SwitchA(config-bgp-af-ipv4)#end
```

```
SwitchB#configure
SwitchB(config)#bgp 65002
SwitchB(config-bgp)#router-id 2.2.2.2
SwitchB(config-bgp)#confederation identifier 200
SwitchB(config-bgp)#confederation peer-as 65001,65003
SwitchB(config-bgp)#neighbor 10.1.1.1 remote-as 65001
SwitchB(config-bgp)#end
```

```
SwitchC#configure
SwitchC(config)#bgp 65003
SwitchC(config-bgp)#router-id 3.3.3.3
SwitchC(config-bgp)#confederation identifier 200
SwitchC(config-bgp)#confederation peer-as 65001,65002
SwitchC(config-bgp)#neighbor 10.1.2.1 remote-as 65001
SwitchC(config-bgp)#end
```

Step 3 Configure IBGP connections in AS 65001.

```
SwitchA#configure
SwitchA(config)#bgp 65001
SwitchA(config-bgp)#neighbor 10.1.3.2 remote-as 65001
SwitchA(config-bgp)#neighbor 10.1.4.2 remote-as 65001
SwitchA(config-bgp)#ipv4-family unicast
SwitchA(config-bgp-af-ipv4)#neighbor 10.1.3.2 next-hop-local
SwitchA(config-bgp-af-ipv4)#neighbor 10.1.4.2 next-hop-local
SwitchA(config-bgp-af-ipv4)#end
```

```
SwitchD#configure
SwitchD(config)#bgp 65001
SwitchD(config-bgp)#router-id 4.4.4.4
SwitchD(config-bgp)#confederation identifier 200
SwitchD(config-bgp)#neighbor 10.1.3.1 remote-as 65001
SwitchD(config-bgp)#neighbor 10.1.5.2 remote-as 65001
SwitchD(config-bgp)#end
```

```
SwitchE#configure
SwitchE(config)#bgp 65001
SwitchE(config-bgp)#router-id 5.5.5.5
SwitchE(config-bgp)#confederation identifier 200
SwitchE(config-bgp)#neighbor 10.1.4.1 remote-as 65001
SwitchE(config-bgp)#neighbor 10.1.5.1 remote-as 65001
```

```
SwitchE(config-bgp)#end
```

Step 4 Configure the EBGp connection between AS 100 and AS 200.

```
SwitchA#configure
SwitchA(config)#bgp 65001
SwitchA(config-bgp)#neighbor 200.1.1.2 remote-as 100
SwitchA(config-bgp)#end
```

```
SwitchF#configure
SwitchF(config)#bgp 100
SwitchF(config-bgp)#router-id 6.6.6.6
SwitchF(config-bgp)#neighbor 200.1.1.1 remote-as 200
SwitchF(config-bgp)#ipv4-family unicast
SwitchF(config-bgp-af-ipv4)#network 9.1.1.0/24
SwitchF(config-bgp-af-ipv4)#end
```

Step 5 Check configurations.

```
SwitchB#configure
SwitchB(config)#show bgp ip-route
```

DestAddr/Prefixlen	Neighbor	Nexthop	Protocol
Med	LocalPrf	Origin	Vpn-Instance
As-Path			
9.1.1.0/24	10.1.1.1	10.1.1.1	bgp
100	IGP	public	AS_CONFED_SEQUENCE 65001

Total:1

```
SwitchC#configure
SwitchC(config)#show bgp ip-route
```

DestAddr/Prefixlen	Neighbor	Nexthop	Protocol
Med	LocalPrf	Origin	Vpn-Instance
As-Path			
9.1.1.0/24	10.1.2.1	10.1.2.1	bgp
100	IGP	public	AS_CONFED_SEQUENCE 65001

Total:1

```
SwitchD#configure
SwitchD(config)#show bgp ip-route
```

DestAddr/Prefixlen	Neighbor	Nexthop	Protocol
Med	LocalPrf	Origin	Vpn-Instance
As-Path			

```
9.1.1.0/24      10.1.3.1      10.1.3.1      bgp      0
100      IGP      public      AS_SEQUENCE 100
-----
Total:1
```

Switch F only needs to establish an EBGP connection with Switch A, without establishing connections with Switch B and Switch C. It can also transmit routing information to Switch B and Switch C through confederation.

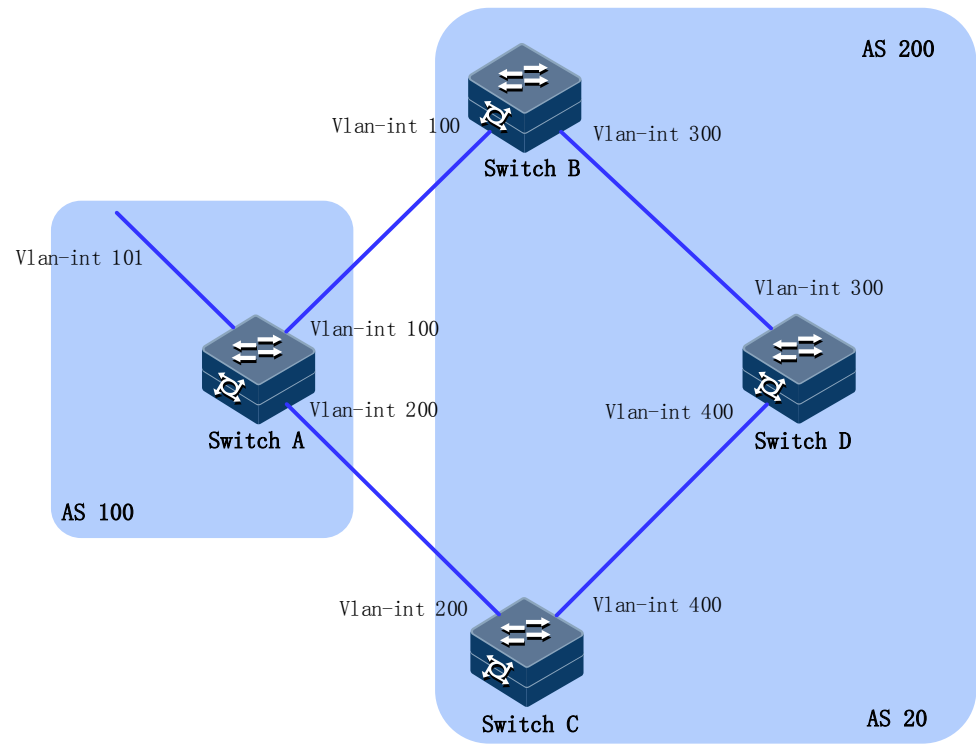
Switch B and Switch D are in the same confederation, but belong to different sub-ASs. They both obtain external routing information through Switch A, and the generated BGP routing table entries are also consistent, equivalent to being in the same AS but not physically fully connected.

3.7.17 Example for configuring BGP route selection

Networking requirements

As shown below, all routers are running BGP. EBGP is running between Switch A and Switch B or Switch C. IBGP is running between Switch D and Switch B or Switch C. OSPF is running in AS 200. Configure the routing policy so that Switch D prefers the 1.0.0.0/8 route learned from Switch C.

Figure 3-19 BGP route selection application



Device	Interface	IP address
Switch A	Vlan-int101	1.0.0.1/8

	Vlan-int100	192.1.1.1/24
	Vlan-int200	193.1.1.1/24
Switch B	Vlan-int100	192.1.1.2/24
	Vlan-int300	194.1.1.2/24
Switch C	Vlan-int400	195.1.1.2/24
	Vlan-int200	193.1.1.2/24
Switch D	Vlan-int400	195.1.1.1/24
	Vlan-int300	194.1.1.1/24

Configuration steps

Step 1 Configure IP addresses of interfaces.

Step 2 Configure OSPF to run between Switch B or Switch C and Switch D.

```
SwitchB#configure
SwitchB(config)#ospf 1
SwitchB(config-ospf-1)#network 192.1.1.0 255.255.255.0 area 0
SwitchB(config-ospf-1)#network 194.1.1.0 255.255.255.0 area 0
SwitchB(config-ospf-1)#end
```

```
SwitchC#configure
SwitchC(config)#ospf 1
SwitchC(config-ospf-1)#network 193.1.1.0 255.255.255.0 area 0
SwitchC(config-ospf-1)#network 195.1.1.0 255.255.255.0 area 0
SwitchC(config-ospf-1)#end
```

```
SwitchD#configure
SwitchD(config)#ospf 1
SwitchD(config-ospf-1)#network 194.1.1.0 255.255.255.0 area 0
SwitchD(config-ospf-1)#network 195.1.1.0 255.255.255.0 area 0
SwitchD(config-ospf-1)#end
```

Step 3 Configure BGP connections.

```
SwitchA#configure
SwitchA(config)#bgp 100
SwitchA(config-bgp)#neighbor 192.1.1.2 remote-as 200
SwitchA(config-bgp)#neighbor 193.1.1.2 remote-as 200
SwitchA(config-bgp)#ipv4-family unicast
SwitchA(config-bgp-af-ipv4)#network 1.0.0.0/8
SwitchA(config-bgp-af-ipv4)#end
```

```
SwitchB#configure
```



```
SwitchB(config)#bgp 200
SwitchB(config-bgp)#neighbor 192.1.1.1 remote-as 100
SwitchB(config-bgp)#neighbor 194.1.1.1 remote-as 200
SwitchB(config-bgp)#end
```

```
SwitchC#configure
SwitchC(config)#bgp 200
SwitchC(config-bgp)#neighbor 193.1.1.1 remote-as 100
SwitchC(config-bgp)#neighbor 195.1.1.1 remote-as 200
SwitchC(config-bgp)#end
```

```
SwitchD#configure
SwitchD(config)#bgp 200
SwitchD(config-bgp)#neighbor 194.1.1.2 remote-as 200
SwitchD(config-bgp)#neighbor 195.1.1.2 remote-as 200
SwitchD(config-bgp)#end
```

- Step 4 Configure different attributes of the 1.0.0.0/8 route so that Switch D preferentially selects the route learnt from Switch C.

Method one: configure a higher MED attribute value for the 1.0.0.0/8 route advertised to peer 192.1.1.2 on Switch A so that Switch D preferentially selects the route learned from Switch C.

```
SwitchA#configure
SwitchA(config)#route-policy apply_med_100 permit node 10
SwitchA(config-route-policy-apply_med_100-10)#apply cost 100
SwitchA(config-route-policy-apply_med_100-10)#exit
SwitchA(config)#route-policy apply_med_50 permit node 10
SwitchA(config-route-policy-apply_med_50-10)#apply cost 50
SwitchA(config-route-policy-apply_med_50-10)#exit
SwitchA(config)#bgp
SwitchA(config-bgp)#ipv4-family unicast
SwitchA(config-bgp-af-ipv4)#neighbor 192.1.1.2 filter-policy export
route-policy apply_med_100
SwitchA(config-bgp-af-ipv4)#neighbor 193.1.1.2 filter-policy export
route-policy apply_med_50
SwitchA(config-bgp)#end
```

Use the following command to show the BGP routing table of Switch D.

```
SwitchD#configure
SwitchD(config)#show bgp ip-route destination-address 1.0.0.0/8
BGP routing table entry information

Network          :1.0.0.0/8
Peer              :194.1.1.2
NextHop           :192.1.1.1
Protocol          :bgp
Med               :100
Local Preference  :100
```

```

As-Path           :AS_SEQUENCE 100
Origin            :IGP
Best              :False
InLabel           :0
OutLabel          :0
AtomicAggr        :0
HWState           :0
HWUpdateTime       :0h:1m:43s
SummaryRoute      :0
SummaryFilter     :0
WaitDelete        :0
BestSysroute      :0
MPLSUpdate        :0
ImportFiltered    :0
IGPSyncwait       :0
SourceVRF         :0
Damp Supressed    :N
DirectNexthop     :194.1.1.2
Less Priority Reason :none
VPN-Instance      :public
BGP routing table entry information

Network           :1.0.0.0/8
Peer              :195.1.1.2
NextHop           :193.1.1.1
Protocol          :bgp
Med               :50
Local Preference  :100
As-Path           :AS_SEQUENCE 100
Origin            :IGP
Best              :True
InLabel           :0
OutLabel          :0
AtomicAggr        :0
HWState           :1
HWUpdateTime       :0h:1m:13s
SummaryRoute      :0
SummaryFilter     :0
WaitDelete        :0
BestSysroute      :1
MPLSUpdate        :0
ImportFiltered    :0
IGPSyncwait       :0
SourceVRF         :0
Damp Supressed    :N
DirectNexthop     :195.1.1.2
Less Priority Reason :none
VPN-Instance      :public

```

As you can see, the 1.0.0.0/8 route learnt by Switch D from Switch C is optimal.

Method two: configure different local priorities for the 1.0.0.0/8 route on Switch B and Switch C respectively so that Switch D prefers the routes learned from Switch C. On Switch C, the local priority is 200 (the default local priority is 100).

```
SwitchC#configure
SwitchC(config)#bgp
SwitchC(config-bgp)#ipv4-family unicast
SwitchC(config-bgp-af-ipv4)#default local-preference 200
SwitchC(config-bgp-af-ipv4)#end
```

Use the following command to show the BGP routing table of Switch D.

```
SwitchD#configure
SwitchD(config)#show bgp ip-route destination-address 1.0.0.0/8
BGP routing table entry information
```

```
Network          :1.0.0.0/8
Peer             :194.1.1.2
NextHop          :192.1.1.1
Protocol         :bgp
Med              :0
Local Preference :100
AS-Path          :AS_SEQUENCE 100
Origin           :IGP
Best             :False
InLabel          :0
OutLabel         :0
AtomicAggr       :0
HWState          :0
HWUpdateTime     :0h:0m:45s
SummaryRoute     :0
SummaryFilter    :0
WaitDelete       :0
BestSysroute     :0
MPLSUpdate       :0
ImportFiltered   :0
IGPSyncwait      :0
SourceVRF        :0
Damp Supressed   :N
DirectNexthop    :194.1.1.2
Less Priority Reason :local preference
VPN-Instance     :public
BGP routing table entry information
```

```
Network          :1.0.0.0/8
Peer             :195.1.1.2
NextHop          :193.1.1.1
Protocol         :bgp
Med              :0
Local Preference :200
AS-Path          :AS_SEQUENCE 100
Origin           :IGP
Best             :True
InLabel          :0
OutLabel         :0
AtomicAggr       :0
HWState          :1
```

```

HWUpdateTime           :0h:1m:35s
SummaryRoute           :0
SummaryFilter          :0
WaitDelete             :0
BestSysroute           :1
MPLSUpdate             :0
ImportFiltered         :0
IGPSyncwait            :0
SourceVRF              :0
Damp Supressed         :N
DirectNexthop          :195.1.1.2
Less Priority Reason    :none
VPN-Instance           :public

```

As you can see, the 1.0.0.0/8 route learnt by Switch D from Switch C is optimal.

3.8 OSPFv2

3.8.1 Introduction

Functions

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) developed by the IETF organization based on link status.

OSPF has the following features:

- Wide adaptability: support networks of various scales and up to hundreds of routers.
- Fast convergence: send update packets immediately after the topology of the network changes, and enable other nodes in the AS to quickly synchronize this change.
- No loop: OSPF calculates routes by using the shortest path tree algorithm based on the collected link status. The algorithm ensures that OSPF does not generate self-loop routes.
- Area division: allow the network of an AS to be divided into areas for management, and further abstract the routing information transmitted between areas, reducing the occupied network bandwidth.
- Equivalent route: support multiple equivalent routes to the same destination address.
- Route classification: use 4 different types of routes. In order of priority, they are: intra-area route, inter-area route, type-1 external route, and type-2 external route.
- Packet verification: support verifying packets based on interface to ensure security of packet interaction.
- Multicast sending: along the link that can send multicast packets, send protocol packets by using the multicast addresses to reduce interference with other devices.

OSPF router ID

If a router wants to run OSPF, it must have a router ID. The router ID is a 32-bit unsigned integer that is the unique identifier of a router in an AS. The ID of the router can be manually configured or automatically generated by the system, which automatically selects the greatest

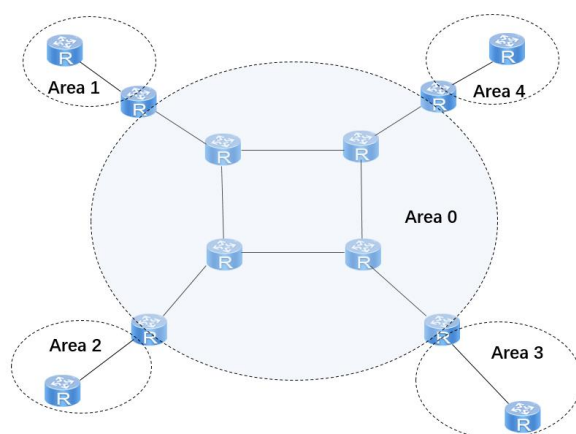
address from the IP addresses of the current interface as the router ID. If the system is not currently configured with any IP address, OSPF cannot be started.

OSPF area division

With the increasing scale of the network, when all devices on a large network run OSPF, the increase in the number of devices will cause the Link State Database (LSDB) to be very large, occupying a lot of storage space, increasing the complexity of running the SPF algorithm, and resulting in a heavy burden on the devices. After the network scale increases, the probability of topology changes also increases, and the network often becomes "turbulent", causing a large number of OSPF packets to be transmitted on the network, reducing the bandwidth utilization of the network. The even more serious situation is that each change will cause all devices on the network to perform routing calculations again.

To address the previous issues, OSPF divides an AS into different areas. Areas logically divide routers into different groups, and each area is identified by an area ID. The boundary of an area is a router, not a link. A network segment (link) can belong to only one area, or each interface running OSPF must indicate the area to which it belongs.

Figure 3-20 OSPF area division

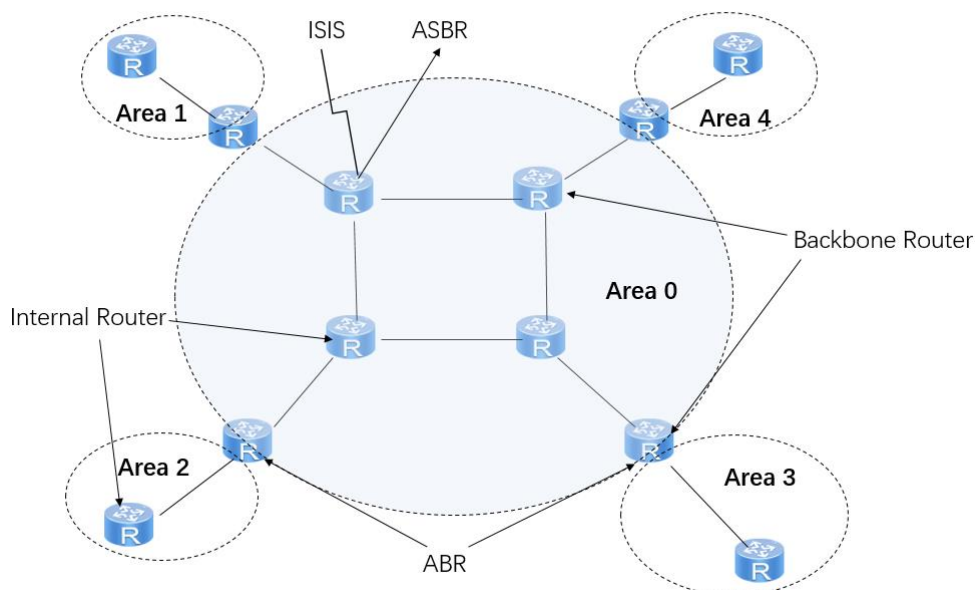


After dividing areas, route aggregation can be performed on the Area Boundary Router (ABR) to reduce the number of LSAs notified to other areas. In addition, dividing areas can also minimize the impact of network topology changes.

The types of OSPF areas include common areas, Stub areas, and NSSA areas.

OSPF router types

Figure 3-21 Example of OSPF router types



- Internal Router: all interfaces of this type of routes belong to the same OSPF area.
- ABR: this type of devices can belong to two or more areas simultaneously, but one of them must be a backbone area. The ABR is used to connect the backbone area and non-backbone area, and it can be physically or logically connected to the backbone area.
- Backbone router: this type of devices has at least one interface belonging to the backbone area. All ABRs and internal devices located in Area 0 are backbone routers.
- Autonomous System Boundary Router (ASBR): a device that exchanges routing information with other ASs is called the ASBR. The ASBR may not necessarily be located at the boundary of an AS, and it may be a device within the area or an ABR. As long as an OSPF device redistributes external routing information, it becomes an ASBR.

OSPF packets

OSPF has the following five types of protocol packets:

- Hello packet: sent periodically to discover and maintain OSPF neighbor relationships.
- Database Description (DD) packet: describe the summary information of the local LSDB, and is used for database synchronization when two routers begin to establish adjacency.
- Link State Request (LSR) packet: request the required LSA from the other party.
- Link State Update (LSU) packet: send the required LSA to the other party.
- Link State Acknowledgment (LSAck) packet: confirm the received LSA.

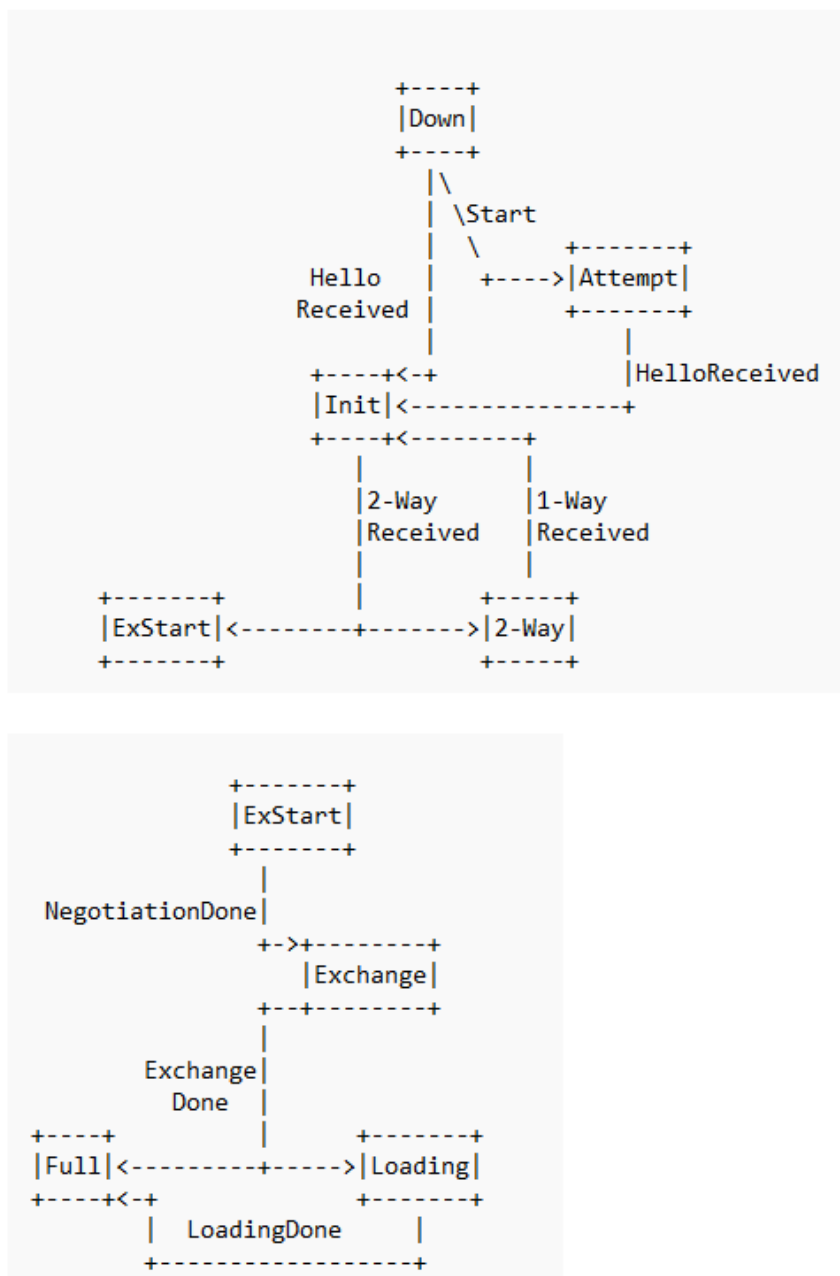
OSPF LSA types

The description of routing information in OSPF is encapsulated and advertised in LSA. Common LSA types include:

- Router LSA (Type1): each router generates a description of the router link status and cost, which is advertised within its respective area.
- Network LSA (Type2): generated by the DR, describing the link status of this network segment and being advertised within its respective area
- Network Summary LSA (Type3): generated by the ABR, describing the routing of a certain network segment within an area and being advertised to other areas.
- ASBR Summary LSA (Type4): generated by the ABR, describing the route to the ASBR and being advertised to the relevant area
- AS External LSA (Type5): generated by the ASBR, describing the routing to the outside of the AS and being advertised to all areas (except the Stub area and NSSA).
- NSSA LSA (Type7): generated by ASBR, describing the routing to the outside of the AS, and being advertised within the NSSA area only
- Opaque LSA (Type9/Type10/Type11): the Opaque LSA provides a universal mechanism for extending OSPF.

OSPF neighbor status machine

Figure 3-22 OSPF neighbor status machine



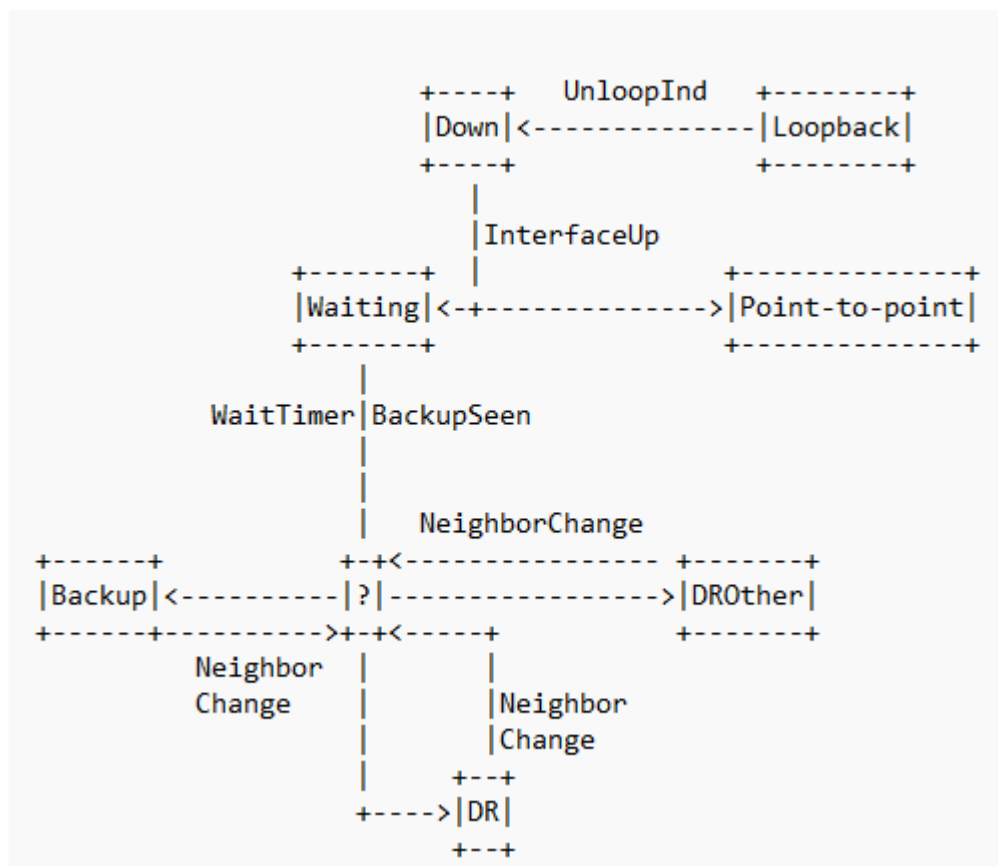
Concepts in the neighbor status machine:

- **Down**: initial stage of neighbor sessions. It indicates that no Hello packet has been received from neighboring devices within the time interval between neighbor failures.
- **Attempt**: regularly send Hello messages to manually configured neighbors in this status. Note that the Attempt status is applicable to NBMA interfaces only.
- **Init**: this status indicates that the neighbor's Hello packet has been received, but the other end has not received the Hello packet sent by the local end.

- 2-way: they are neighbors to each other. This status indicates that both parties have received Hello packet from the peer end and established a neighbor relationship. If no adjacency relationship is formed, the neighbor status machine stays in this status; otherwise, it enters the Exstart status.
- Exstart: negotiate master/slave relationship. Establishing a master/slave relationship is to ensure orderly transmission in subsequent DD packet exchanges.
- Exchange: Exchange DD packets. The local device describes the local LSDB as a DD packet and sends it to neighboring devices.
- Loading: synchronize the LSDB. Both devices send LSR packets to neighbors to request the peer LSA and to synchronize the LSDB.
- Full: establish adjacency. The LSDBs of both devices are synchronized, and the local device and neighboring device have established adjacency status.

OSPF interface status machine

Figure 3-23 OSPF interface status machine



Concepts in the OSPF interface status machine:

- Down: initial status of the interface status
- Loopback: in this status, the interface between the router and the network is looped back.
- Waiting: Only applicable to broadcast and NBMA interface types, attempting to identify DR and BDR on the network at this stage.

- Point-to-point: only applicable to interfaces with point-to-point, point-to-multipoint, and virtual connections. In this status, the device attempts to establish an adjacency relationship with the router on the other end of the interface.
- DR: in this status, the DR of the network successfully connected with the router attempts to establish adjacency with other routers.
- Backup: in this status, the BDR of the network successfully connected with the router attempts to establish adjacency with other routers.
- DROther: in this state, the DROther of the network successfully connected with the router establishes adjacency with the DRs and BDRs.

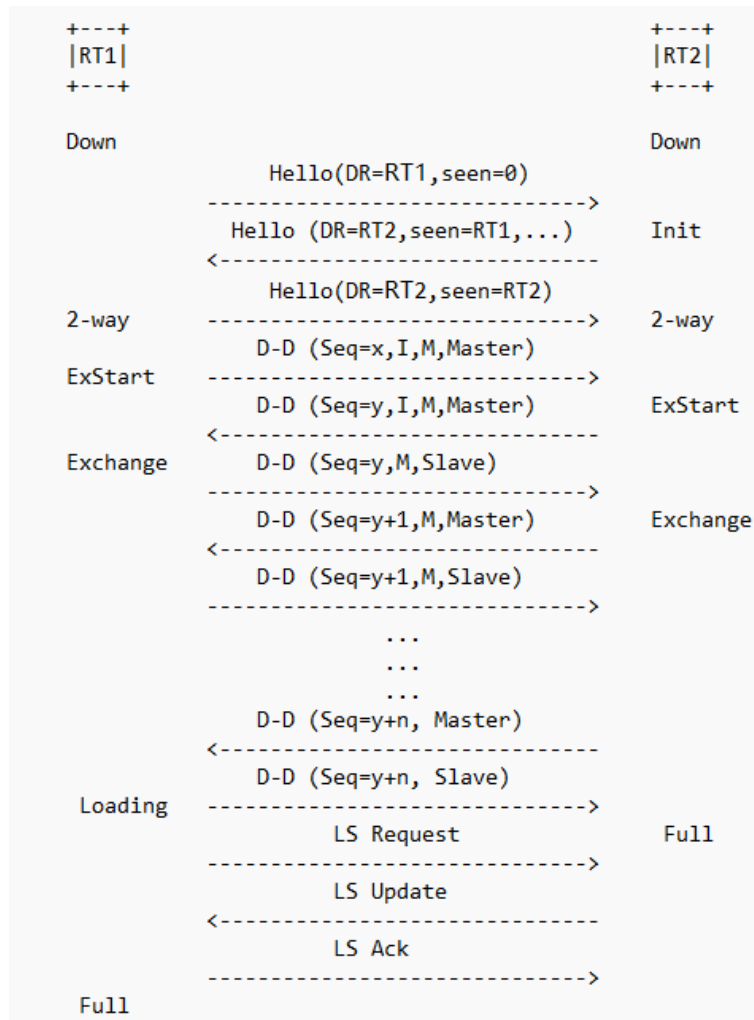
OSPF neighbor and adjacency

In OSPF, the neighbor and adjacency are two different concepts.

- Neighbor relationship: after the OSPF router is started, it will send Hello packets outward through the OSPF interface. The OSPF router that receives the Hello packet checks some parameters defined in the packet. If both parties agree, they will establish a neighbor relationship.
- Adjacency relationship: not all parties establishing a neighbor relationship may be able to establish an adjacency relationship, which depends on the type of the network. Only when both parties successfully exchange DD packets and exchange LSAs can they establish a true adjacency relationship.

The flow for establishing the adjacency relationship on the OSPF broadcast network is as below.

Figure 3-24 Flow for establishing the adjacency relationship on the OSPF broadcast network
OSPF



Both RT1 and RT2 are connected to the broadcast network. Assume that RT2 is the DR of the network, and the Router ID of RT2 is higher than that of Router RT1.

- Step 1 Establish a neighbor relationship. RT1 activates OSPF on an interface connected to a broadcast network, and will start sending Hello packets. At this point, Router A considers itself a DR router, but is unsure about its neighbor. RT2 receives this Hello packet (changing the neighbor status machine to Init status) and indicates in its next hello packet that it is the DR. RT1 received the Hello packet from RT2. This in turn causes RT1 to transit to the 2-way status and to start the adjacency process.
- Step 2 Negotiate master/slave relationship, and exchange the DD packet.

RT1 first sends a DD packet claiming to be the Master (MS=1) and specifying the sequence number Seq=x. I=1 indicates that this is the first DD packet, which does not contain a summary of LSA and is only used to negotiate the master/slave relationship. M=1 indicates that this is not the last packet.

After receiving the DD packet from RT1, RT2 changes the neighbor status machine of RT1 to Exstart and responds with a DD packet. Due to the large Router ID of RT2, RT2 considers itself as the master in the packet and redefines the sequence number Seq=y.

After receiving the packet, RT1 agrees to change RT2 as Master and changes the neighbor status machine of RT2 to Exchange. RT1 uses the sequence number Seq=y of RT2 to send a new DD packet, which officially sends the summary of LSA, confirming which LSA in the database need to be updated in this way. RT1 configures MS to 0 in the packet, indicating that it is Slave.

After receiving the packet, RT2 changes the neighbor status machine of RT1 to Exchange and sends a new DD packet to describe its LSA summary. At this time, RT2 changes the sequence number of the packet to Seq=y+1.

The above process continues, and RT1 confirms receipt of the RT2 packet by repeating the sequence number of RT2. RT2 confirms receipt of packets of Router A by adding 1 to the serial number Seq. When sending the last DD packet, write M=0 in the packet.

Step 3 Synchronize the LSDB (LSA request, LSA transmission, and LSA response).

After receiving the last DD packet, RT1 discovers that there is an LSA in RT2 database that it does not have, and changes the neighbor status machine to the Loading status.

RT2 has discovered the LSA for RT1, and RT2 already has it. There is no need to request it again. RT2 changes the neighbor status machine of RT1 to the Full status.

RT1 sends an LSR packet to RT2, requesting an update to the LSA. RT2 responds to RT1 request with an LSU packet. After receiving the LSU packet, RT1 sends an LSack packet as acknowledgment.

The above process continues until the LSA in RT1 is completely synchronized with the LSA in RT2, and then, RT1 changes the neighbor status machine of RT2 to the Full status. After the router exchanges DD packets and updates all LSAs, the adjacency relationship is established.

Calculating OSPF routes

The flow for calculating OSPF routes is as below:

- Step 1 Each OSPF router generates a Link State Advertisement (LSA) based on its surrounding network topology, and sends the LSA to other OSPF routers on the network through update packets.
- Step 2 Each OSPF router collects LSAs sent by other routers, and all LSAs form the Link State Database (LSDB), which describes the network topology of the entire AS.
- Step 3 OSPF routers convert LSDB into a weighted directed graph, which is a true reflection of the entire network topology. The directed graph obtained by each OSPF router is exactly the same.
- Step 4 Each OSPF router uses the SPF algorithm to calculate a shortest path tree roots in itself based on a directed graph, which provides routes to each node in the AS.

OSPF backbone area

After OSPF divides areas, not all areas have equal relationships. One of the areas is unique and commonly referred to as the backbone area, with an area ID of 0.

The backbone area is responsible for routing between areas, and forwards routing information between non-backbone areas. OSPF has the following related rules:

All non-backbone areas must be connected to the backbone area. The backbone area itself must also maintain connectivity. However, in practical applications, the previous requirements may not be met due to limitations, such as network topology; in this case, the OSPF virtual connection can be configured to meet the requirements.

OSPF virtual connection

A virtual connection refers to a logical connection channel established between two ABRs through a non-backbone area. It is equivalent to a point-to-point connection between two ABRs. The area that provides a non-backbone internal route for both ends of the virtual connection is called the Transit Area.

Virtual connections have the following features:

- The two ends of the virtual connection must be ABR.
- Virtual connections must be configured at both ends in order for them to take effect.
- Virtual connections can configure interface parameters, such as the interval between sending HELLO messages, just like physical interfaces.

When two ABRs directly transmit OSPF packets, the OSPF router between them only serves to forward packets. Because the destination address of packets is not these routers, these packets are transparent to them and are only forwarded as regular IP packets.

OSPF Stub area

The Stub area has the following features:

- The ABR in the Stub area does not advertise the external routes received from the AS. In these areas, the size of the routing table of the routes and the amount of routing information transmitted are greatly reduced.
- The Stub area is an optional configuration attribute, and not every area meets the configuration criteria. Generally, the Stub area is a non-backbone area located at the boundary of an AS with only one ABR.
- To ensure reachable routes to outside of the AS, the ABR in the Stub area generates a default route and advertises it to other non-ABR routers in the Stub area.

Notes on configuring the Stub area:

- The backbone area cannot be configured as a Stub area.
- If you want to configure an area as a Stub area, all routers in that area must have a configured Stub area.
- The ASBR cannot exist within the Stub area; in other words, routes outside the AS cannot be advertised within this area. Virtual connections cannot pass through the Stub area.

OSPF NSSA area

A new type of area is added in RFC1587 NSSA Option: NSSA area. A new type of LSA is also added: NSSA LSA (also known as Type7 LSA).

The NSSA area is actually a deformation of the Stub area, and it has many similarities with the Stub area. The difference between them is that the NSSA area can redistribute and advertise external routes from the AS to the entire OSPF AS, without learning external routes from other areas of the OSPF network.

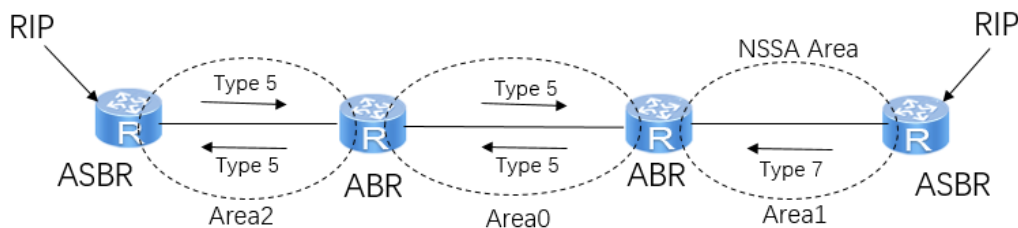
The NSSA area has the following features:

- Similar to the Stub area, the NSSA area cannot be configured with virtual connections.
- Similar to the Stub area, the NSSA area also does not allow AS External LSA (namely, Type5 LSA injection is not allowed, but Type7 LSA injection is allowed). The Type7

LSA is generated by the ASBR in the NSSA area and is advertised within the NSSA region. When Type7 LSA reaches the ABR of NSSA, the ABR converts Type7 LSA into AS External LSA and advertise it to other regions.

As shown in the figure, the AS running OSPF includes three areas: Area 1, Area 2, and Area 0.

Figure 3-25 OSPF NSSA area



Area 1 is defined as the NSSA area. The non-OSPF network connected to area 1 and area 2 runs RIP. After the RIP route received from the RIP network in Area 1 is advertised to the NSSA ASBR, the NSSA ASBR generates the Type7 LSA and advertises it within Area 1. When the Type7 LSA reaches NSSA ABR, it is converted to Type5 LSA and advertised to areas 0 and 2. On the other hand, the RIP route received by area 2 from the RIP network is generated into Type-5 LSA, which is advertised in the OSPF AS through the ASBR of area 2. But because Area 1 is an NSSA area, Type-5 LSA will not reach Area 1.

OSPF route aggregation

Route aggregation refers to that the ABR aggregate routing information with the same prefix together to form a route and advertise it to other areas.

After an AS is divided into different area, route aggregation can be used between areas to reduce routing information, to reduce the size of routing tables, and to improve the computational speed of routers.

OSPF has two route aggregation modes:

- ABR aggregation

When the ABR sends routing information to other regions, it generates the Type3 LSA on a network segment basis. If there are some continuous network segments in the area, they can be aggregated into one network segment through the route aggregation command. In this way, the ABR sends only one aggregated LSA, and all LSAs within the specified aggregated network segment range will not be sent separately.

For example, there are three routes within areas 1, 19.1.1.0/24, 19.1.2.0/24, and 19.1.3.0/24. If route aggregation is configured on the ABR at this time to aggregate the three routes into one route 19.1.0.0/16, the ABR will generate only one aggregated LSA and advertise it to routers in other areas.

- ASBR aggregation

After route aggregation is configured, if the local device is an ASBR, it will aggregate Type5 LSA within the redistributed aggregation address range. When the NSSA area is configured, the Type7 LSA within the redistributed aggregation address range will be aggregated. If the local device is both the ASBR and ABR, it aggregates the Type5 LSA converted from the Type7 LSA.

OSPF route types

OSPF divides routes into four levels in order of priority: intra-area route, inter-area route, Type1 external route, and Type2 external route.

- Intra-area route (AS internal route): The routes within and between AS areas describe the network structure within the AS. By default, the protocol priority for these two types of routes is 10.
- Inter-area route (AS external route): the external route describes how to choose a route to a destination address outside of the AS. OSPF divides the redistributed AS external route into two types: Type1 and Type2. By default, the protocol priority for these two types of routes is 150.
 - Type1 external route: the received IGP route (such as the static route and RIP route). Due to the high-level of trustworthiness of this type of routes, the calculated cost of the external route is the same as that of the internal route in the AS, and is comparable to the cost of OSPF own route. The cost of the Type1 external route is equal to the cost from the router to the corresponding ASBR plus the cost from the ASBR to the destination address of the route.
 - Type2 external route: EGP route. Due to the low reliability of this type of routes, OSPF assumes that the cost from the ASBR to the outside of the AS is much greater than the cost to the ASBR within the AS. So when the route cost is calculated, the former will be mainly considered; in other words, the cost to the Type2 external route = the cost from the ASBR to the destination address of the route. If the cost values calculated by two routes are equal, then consider the cost from this router to the corresponding ASBR.

OSPF network types

OSPF divides networks into the following four types based on link layer protocol types:

- Broadcast type: OSPF takes the default type of the network type as broadcast. On this type of networks, protocol packets are typically sent in multicast format (224.0.0.5 and 224.0.0.6).
- Non Broadcast Multi Access (NBMA) type: on this type of network, protocol packets are sent in unicast form.
- Point to Multipoint (P2MP) type: P2MP must be forcibly changed from other network types. The common practice is to change the non-fully-connected NBMA to the P2MP network. On this type of network, protocol packets are sent in multicast format (224.0.0.5).
- Point to Point (P2P) type: on this type of network, protocol packets are sent in multicast form (224.0.0.5).

OSPF DR and BDR

On broadcast networks and NBMA networks, routing information must be transmitted between any two routers. If there are n routers on the network, establishing $n \times (n-1)/2$ adjacency relationships is required. This causes multiple transmissions due to the route change of any router, thus wasting bandwidth resources.

To address this issue, OSPF defines Designated Router(DR), Backup Designated Router (BDR), and routers other than DR and BDR (DROthers).

- DR: all routers send information to the DR only, who broadcasts the network link status.

- BDR: if the DR fails due to some fault, the routers on the network must re-elect the DR and synchronize with the new DR. This takes a long time, during which the routing calculation is incorrect. To shorten this process, OSPF proposes the concept of the BDR. The BDR is actually a backup of the DR, and is also elected when the DR is elected. The BDR establishes adjacency relationships with all routers in this network segment and exchanges routing information. When the DR fails, the BDR will immediately become the DR. Because there is no need for re-elections and the adjacency relationship has been established in advance, this process is very brief. Of course at this point, a new BDR needs to be re-elected, although it still takes a long time, the election will not affect the routing calculation.
- DROther: the DROthers do not establish adjacency relationships or exchange any routing information. This reduces the number of adjacency relationships between routers on the broadcast network and NBMA network.

The DR and BDR are not artificially specified, but are jointly elected by all routers in this network segment. The DR priority of a router interface determines its eligibility for DR and BDR elections. The routers with the DR priority greater than 0 in this network segment can be considered as candidates. The DR and BDR are elected as below:

- Step 1 Each router writes its elected DR into a Hello packet and sends the Hello packet to other routers in the network segment.
- Step 2 If two routers in the same network segment simultaneously declare themselves as the DR, the one with the higher DR priority wins. If the priority is equal, the one with the greater Router ID wins. If a router has a priority of 0, it will not be elected as the DR or BDR.

DR/BDR election has the following features:

- The DR is elected on the broadcasting interface or NBMA interface only. There is no need to elect the DR on the P2P or P2MP interface.
- The DR refers to the concept within a certain network segment, specifically for the interface on routers. A certain router may be a DR in terms of one interface and a BDR or DROther in terms of another interface.
- If the DR and BDR are elected, when a new router is added with the highest DR priority, it will not immediately become a DR in that network segment.
- The DR may not necessarily be the router with the highest DR priority. Similarly, the BDR may not necessarily be the router with the second highest DR priority.

Authenticating OSPF packets

OSPF supports authenticating packets. Only authenticated OSPF packets can be received; otherwise, no normal neighbor relationship can be established.

3.8.2 Preparing for configurations

Scenario

After basic functions of OSPF are configured, you can establish the Layer 3 network through OSPF.

Prerequisites

Configure IP addresses of interfaces so that the adjacent nodes can access each other at the network layer.

3.8.3 Default configurations

Default configurations of OSPF are as below.

Function	Default value
OSPF	Disable
Interval for sending Hello packets	10s
Neighbor invalid time	40s
Referential bandwidth for calculating the interface cost	100Mbit/s

3.8.4 Configuring basic functions of OSPF

Configure basic functions of OSPF for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)# ospf process-id [vpn-instance name]	Start the OSPF process, and enter the OSPF view. The default process-id is 1. The vpn-instance is the VPN instance. If the vpn-instance is specified, the OSPF process belongs to the VPN instance; otherwise, it belongs to the public network instance.
3	Raisecom(config-ospf-1)#router-id ipv4-address	Configure the ID of the OSPF process. Ensure that the router ID is globally unique. If no router ID is configured, the system chooses one from IP addresses of the current interface as the router ID.
4	Configuration in the instance Raisecom(config-ospf-1)#network network-address network-mask area area-id Configuration on the interface Raisecom (config-vlanif-1)# ospf process-id area area-id	There are two methods to enable OSPF on the interface and create OSPF areas. • Configure the OSPF area and the network segments in the OSPF area. When the IP address of the interface meets requirements for the network segment, the interface can run OSPF normally. • Configure the instance run by the interface and OSPF area. When these two configuration methods conflict, the interface configuration prevails.

Step	Command	Description
5	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode. Take the VLAN interface for example.
6	Raisecom (config-vlanif-1)# ospf if-type { broadcast nbma p2p p2multip }	(Optional) configure the network type of the interface.
7	Raisecom(config)# ospf process-id [vpn-instance name]	Enter the OSPF view.
8	Raisecom(config-ospf-1)# peer ipv4-address priority priority	(Optional) configure the neighbor of the NBMA network.
9	Raisecom(config-ospf-1)# maximum load-balancing number	(Optional) configure the maximum number of OSPF equivalent routes.
10	Raisecom(config-ospf-1)# rfc1583 compatible { enable disable }	(Optional) configure the rule for selecting external routes compatible with RFC1583.
11	Raisecom(config-ospf-1)# preference preference-value { route-policy name }	Configure the priorities of OSPF intra-domain routes and inter-domain routes.
12	Raisecom(config-ospf-1)# preference ase preference-value { route-policy name }	Configure the priority of OSPF external routes.

3.8.5 Configuring the OSPF Stub area

Configure the OSPF Stub area for the device as below.

Step	Command	Description
1	Raisecom# configure	Enter global configuration mode.
2	Raisecom(config)# ospf process-id { vpn-instance name }	Enter the OSPF view.
3	Raisecom(config-ospf-1)# area area-id stub { no-summary-lsa }	Configure the area as the Stub area. The area cannot be the backbone area. No-summary: prohibit the ABR from sending Summary LSA to the Stub area. This parameter can take effect in the area only when the stub command is configured on the ABR.

3.8.6 Configuring the OSPF NSSA area

Configure the OSPF NSSA area for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)# ospf process-id [vpn-instance name]	Enter the OSPF view.
3	Raisecom(config- ospf-1)# area area-id nssa { no-summary- lsa }	Configure the area as the NSSA area. The area cannot be the backbone area. No-summary: prohibit the ABR from sending Summary LSA to the NSSA area.
4	Raisecom(config- ospf-1)# area area-id nssa default-cost cost	(Optional) configure the cost of the default route of the Type 3 LSA sent by the ABR to the NSSA area.
5	Raisecom(config- ospf-1)# area area-id nssa translator { always candidate }	In the candidate status, the NSSA area automatically selects an ABR as the converter according to the rules, converting Type 7 LSA into Type 5 LSA. By configuring a certain ABR with the translator always parameter, you can specify it as a translator.

3.8.7 Configure OSPF to redistribute external routes

Configure OSPF to redistribute external routes for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#ospf process-id [vpn-instance name]	Enter the OSPF view.
3	Raisecom(config-ospf- 1)#import-route { connect static rip bgp isis ospf } [cost { cost inherit } route-policy name]	Redistribute routing information about other protocols. The cost parameter is the default metric for OSPF to redistribute external routes. The inherit parameter indicates that the cost of the redistributed route is the cost value of the route. If no cost is specified, the default cost value configured by the default route-attribute command is used. The route-policy parameter is used to bind the routing policy and to filter routes to be redistributed.

3.8.8 Configuring OSPF route aggregation

Configure OSPF route aggregation for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)# ospf process-id [vpn-instance name]	Enter the OSPF view.
3	Raisecom(config-ospf-1)# area area-id abr-summary {dest-address/dest-masklen dest-address/dest-mask }	Configure ABR route aggregation of OSPF.
4	Raisecom(config-ospf-1)# area area-id nssa summary {dest-address/dest-masklen dest-address/dest-mask }	Configure route aggregation for conversion from type-7 LAS into type-5 LAS on the local router.
5	Raisecom(config-ospf-1)# asbr-summary {dest-address/dest-masklen dest-address/dest-mask }	Configure ASBR route aggregation of OSPF.
6	Raisecom(config-ospf-1)# asbr-summary { connect static rip bgp isis ospf } {dest-address/dest-masklen dest-address/dest-mask }	Configure ASBR route aggregation of OSPF for routes redistributed from a protocol.
7	Raisecom(config-ospf-1)# asbr-summary { rip isis ospf } process-id {dest-address/dest-masklen dest-address/dest-mask }	Configure ASBR route aggregation of OSPF for routes redistributed from a protocol and an instance.

3.8.9 Configuring OSPF virtual connection

Configure OSPF virtual connection for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)# ospf process-id [vpn-instance name]	Enter the OSPF view.
3	Raisecom(config-ospf-1)# area area-id virtual-link ipv4-address	Create a virtual connection, and configure it.

Step	Command	Description
4	Raisecom(config-ospf-1)# area <i>area-id</i> virtual-link <i>ipv4-address</i> hello-interval <i>value</i>	(Optional) configure the interval for sending Hello packets of the virtual connection.
5	Raisecom(config-ospf-1)# area <i>area-id</i> virtual-link <i>ipv4-address</i> dead-interval <i>value</i>	(Optional) configure the neighbor invalid time of the virtual connection.
6	Raisecom(config-ospf-1)# area <i>area-id</i> virtual-link <i>ipv4-address</i> retransmit-interval <i>value</i>	(Optional) configure the interval for retransmitting LSA of the virtual connection.
7	Raisecom(config-ospf-1)# area <i>area-id</i> virtual-link <i>ipv4-address</i> transmit-delay <i>value</i>	(Optional) configure the delay for transmitting LAS of the virtual connection.

3.8.10 Configuring OSPF authentication

Configure OSPF 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 interface configuration mode.
3	Raisecom (config-vlanif-1)# ospf authentication md5 <i>key-id</i> { cipher plain } <i>KEY</i>	Configure the interface authentication mode of OSPF to MD5.
4	Raisecom (config-vlanif-1)# ospf authentication simple { cipher plain } <i>KEY</i>	Configure the interface authentication mode of OSPF to simple.
5	Raisecom(config)# ospf process-id [vpn-instance <i>name</i>]	Enter the OSPF view.
6	Raisecom(config-ospf-1)# area <i>area-id</i> authentication md5 <i>key-id</i> { cipher plain } <i>KEY</i>	Configure the area authentication of OSPF to MD5.
7	Raisecom(config-ospf-1)# area <i>area-id</i> authentication simple { cipher plain } <i>KEY</i>	Configure the area authentication of OSPF to simple.
8	Raisecom(config-ospf-1)# area <i>area-id</i> virtual-link <i>ipv4-address</i> authentication md5 <i>key-id</i> { cipher plain } <i>KEY</i>	Configure the virtual connection packet authentication of OSPF to MD5.

Step	Command	Description
9	Raisecom(config-ospf-1)# area <i>area-id</i> virtual-link <i>ipv4-address</i> authentication simple { cipher plain } KEY	Configure the virtual connection packet authentication of OSPF to simple.

3.8.11 Checking configurations

Use the following commands to check configuration results.

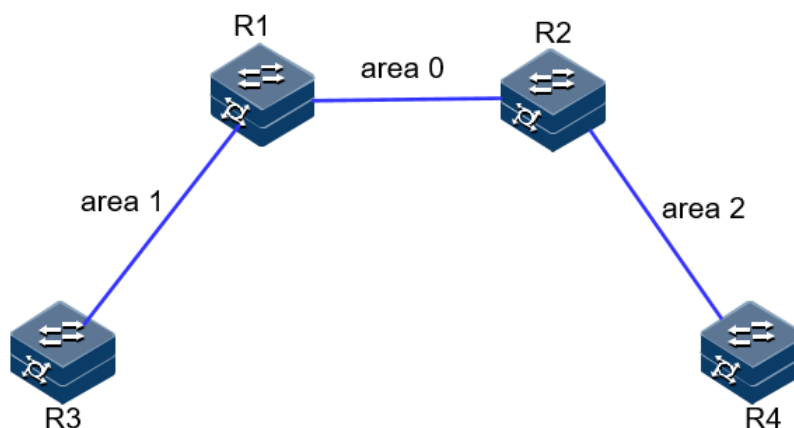
Step	Command	Description
1	Raisecom#show ospf interface	Show the OSPF interface.
2	Raisecom# show ospf process <i>process-id</i>	Show the OSPF instance.
3	Raisecom# show ospf area	Show the OSPF area.
4	Raisecom# show ospf neighbor	Show the OSPF neighbor. After the peer is configured accordingly, neighbor relation can be established.
5	Raisecom# show ospf route	Show the OSPF routing table.
6	Raisecom# show ospf database	Show the OSPF database.
7	Raisecom# show ospf import-route	Show routes redistributed from OSPF.
8	Raisecom# show ospf virtual-link	Show information about the OSPF virtual connection.
9	Raisecom#show ospf interface <i>interface-type interface-number</i>	Show detailed information about the OSPF interface.
10	Raisecom# show ospf area <i>area-id area-id</i>	Show detailed information about the area.
11	Raisecom# show ospf information	Show global information about OSPF.

3.8.12 Example for configuring basic functions of OSPF

Networking requirements

As shown below, all routers run OSPF and divide the entire AS into three areas, where Router 1 and Router 2 are ABRs for forwarding routes between areas. After configuration is complete, each router should learn the routes to all network segments within the AS.

Figure 3-26 Networking with basic functions of OSPF



Configuration steps

Step 1 Configure IP addresses of interfaces.

- IP addresses of two interfaces on R1: 1.1.1.1/24 and 3.1.1.1/24
- IP addresses of two interfaces on R2: 1.1.1.2/24 and 4.1.1.2/24
- IP address of one interface on R3: 3.1.1.3/24
- IP address of one interface on R4: 4.1.1.4/24

Step 2 Configure OSPF.

R1:

```
Raisecom-R1#configure
Raisecom-R1(config)#ospf 1
Raisecom-R1(config-ospf-1)#router-id 1.1.1.1
Raisecom-R1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
Raisecom-R1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
Raisecom-R1(config-ospf-1)#
```

R2:

```
Raisecom-R2#configure
Raisecom-R2(config)#ospf 1
Raisecom-R2(config-ospf-1)#router-id 2.2.2.2
Raisecom-R2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
Raisecom-R2(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2
Raisecom-R2(config-ospf-1)#
```

R3:

```
Raisecom-R3#configure
Raisecom-R3(config)#ospf 1
Raisecom-R3(config-ospf-1)#router-id 3.3.3.3
Raisecom-R3(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
Raisecom-R3(config-ospf-1)#
```

R4:

```
Raisecom-R4#configure
Raisecom-R4(config)#ospf 1
Raisecom-R4(config-ospf-1)#router-id 4.4.4.4
Raisecom-R4(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2
Raisecom-R4(config-ospf-1)#
```

Step 3 Verify configuration results.

Use the **show ospf neighbor** command to show the result of establishing the neighbor relation.

R1:

```
Raisecom-R1(config)#show ospf neighbor
```

```
OSPF Process 1
IpAddress NeighborID Priority State Aging UpTime Interface
-----
1.1.1.2 2.2.2.2 1 full 38 0:00:32 vlan-10
3.1.1.3 3.3.3.3 1 full 35 0:05:04 vlan-13
-----
Down:0 Attempt:0 Init:0 TwoWay:0 ExchangeStart:0 Exchange:0
Loading:0 Full:2
```

R2:

```
Raisecom-R2(config)#show ospf neighbor
```

```
OSPF Process 1
IpAddress NeighborID Priority State Aging UpTime Interface
-----
1.1.1.1 1.1.1.1 1 full 39 0:01:41 vlan-10
4.1.1.4 4.4.4.4 1 full 39 0:01:40 vlan-24
-----
Down:0 Attempt:0 Init:0 TwoWay:0 ExchangeStart:0 Exchange:0
Loading:0 Full:2
```


Use the **show ospf database** command to show the database.

Raisecom-R1(config)#**show ospf database**
Database of OSPF Process 1

Router LSA (area 0)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.1	1.1.1.1	291	0x80000002	0xe05f	36
2.2.2.2	2.2.2.2	292	0x80000002	0xa294	36
Network LSA (area 0)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.2	2.2.2.2	292	0x80000001	0x83bd	32
SummaryNetwork LSA (area 0)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
3.1.1.0	1.1.1.1	563	0x80000002	0x173b	28
4.1.1.0	2.2.2.2	291	0x80000002	0xeb61	28
Router LSA (area 1)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.1	1.1.1.1	563	0x80000002	0xfa42	36
3.3.3.3	3.3.3.3	563	0x80000002	0x7bb0	36
Network LSA (area 1)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
3.1.1.1	1.1.1.1	563	0x80000001	0xd36c	32
SummaryNetwork LSA (area 1)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.0	1.1.1.1	292	0x80000002	0x3123	28
4.1.1.0	1.1.1.1	290	0x80000001	0x163b	28

Use the **show ospf route** command to show the routing table.

Raisecom-R1(config)#**show ospf route**

OSPF Process 1						
RoutType	Prefix		PathType	Cost	Cost2	NextHop
BackupNextHop	AreaId	Time				
ABR	2.2.2.2/32		INTRA	1	0	1.1.1.2
0.0.0.0	0	0:06:38				
Network	1.1.1.0/24		INTRA	1	0	1.1.1.1
0.0.0.0	N/A	0:06:40				
Network	3.1.1.0/24		INTRA	1	0	3.1.1.1
0.0.0.0	N/A	0:11:12				
Network	4.1.1.0/24		INTER	2	0	1.1.1.2
0.0.0.0	N/A	0:06:38				
Route :						
ABR	ASBR	Network	Intra	Inter	External	
1	0	3	2	1	0	

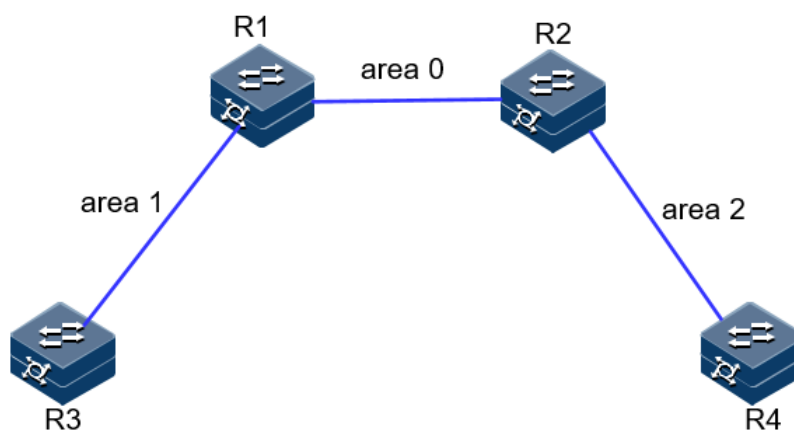
Path :						
ABR	ASBR	Network	Intra	Inter	External	
1	0	3	2	1	0	

3.8.13 Example for configuring the OSPF Stub area

Networking requirements

As shown below, all routers run OSPF and divide the entire AS into three areas, where Router 1 and Router 2 are ABRs for forwarding routes between areas.

Figure 3-27 OSPF Stub area networking



Configuration steps

Step 1 Configure basic functions of OSPF.

Step 2 Configure area 1 as the stub area.

R1:

```
Raisecom-R1#configure
Raisecom-R1(config)#ospf 1
Raisecom-R1(config-ospf-1)#area 1 stub
```

R3:

```
Raisecom-R3#configure
Raisecom-R3(config)#ospf 1
Raisecom-R3(config-ospf-1)#area 1 stub
```

Step 3 Configure R4 to redistribute type-5 LSA of 100.1.1.1.

```
Raisecom-R4(config)#ip route-static 100.1.1.1 255.255.255.255 4.1.1.5
Raisecom-R4(config)#ospf 1
Raisecom-R4(config-ospf-1)#import-route static
```

Step 4 Verify configuration results.

When the R3 area is a common area, the routing table contains the external routes for the AS.

```
Raisecom-R3(config)#show ospf route
OSPF Process 1
RoutType Prefix PathType Cost Cost2 NextHop
BackupNextHop AreaId Time
ABR 1.1.1.1/32 INTRA 1 0 3.1.1.1
0.0.0.0 1 0:00:05
ASBR 4.4.4.4/32 INTER 3 0 3.1.1.1
0.0.0.0 0 0:00:00
Network 1.1.1.0/24 INTER 2 0 3.1.1.1
0.0.0.0 N/A 0:00:05
Network 3.1.1.0/24 INTRA 1 0 3.1.1.3
0.0.0.0 N/A 0:00:07
Network 4.1.1.0/24 INTER 3 0 3.1.1.1
0.0.0.0 N/A 0:00:05
Network 100.1.1.1/32 ASE2 3 1 3.1.1.1
0.0.0.0 N/A 0:00:05
Route :
ABR ASBR Network Intra Inter External
1 1 4 1 2 1
Path :
ABR ASBR Network Intra Inter External
1 1 4 1 2 1
```

When the R3 area is configured as the stub area, external routes for the AS disappear, and instead a default route to the external part of the area appears.

```
Raisecom-R3(config)#show ospf route
OSPF Process 1
RoutType Prefix PathType Cost Cost2 NextHop
BackupNextHop AreaId Time
ABR 1.1.1.1/32 INTRA 1 0 3.1.1.1
0.0.0.0 1 0:00:07
Network 0.0.0.0/0 INTER 2 0 3.1.1.1
0.0.0.0 N/A 0:00:07
Network 1.1.1.0/24 INTER 2 0 3.1.1.1
0.0.0.0 N/A 0:00:07
Network 3.1.1.0/24 INTRA 1 0 3.1.1.3
0.0.0.0 N/A 0:00:12
Network 4.1.1.0/24 INTER 3 0 3.1.1.1
0.0.0.0 N/A 0:00:07
Route :
```

ABR	ASBR	Network	Intra	Inter	External
1	0	4	1	3	0

Path :

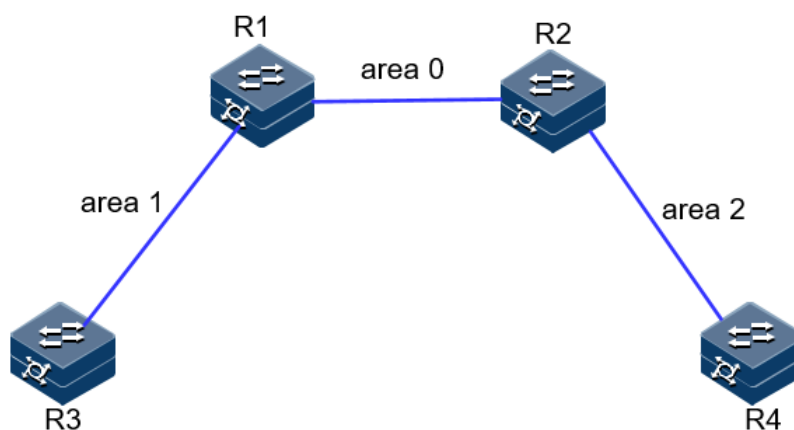
ABR	ASBR	Network	Intra	Inter	External
1	0	4	1	3	0

3.8.14 Example for configuring the OSPF NSSA area

Networking requirements

As shown below, all routers run OSPF and divide the entire AS into three areas, where Router 1 and Router 2 are ABRs for forwarding routes between areas.

Figure 3-28 OSPF NSSA area networking



Configuration steps

Step 1 Configure basic functions of OSPF.

Step 2 Configure area 1 as the NSSA area.

R1:

```

Raisecom-R1#configure
Raisecom-R1(config)#ospf 1
Raisecom-R1(config-ospf-1)#area 1 nssa

```

R3:

```

Raisecom-R3#configure
Raisecom-R3(config)#ospf 1
Raisecom-R3(config-ospf-1)#area 1 nssa

```

Step 3 Configure R4 to redistribute type-5 LSA of 100.1.1.1.

```
Raisecom-R4(config)#ip route-static 100.1.1.1 255.255.255.255 4.1.1.5
Raisecom-R4(config)#ospf 1
Raisecom-R4(config-ospf-1)#import-route static
```

Step 4 Verify configuration results.

Compared with the database in the common area, the database of the NSSA area has an extra type NSSA LSA, and there is no external LSA of 100.1.1.1 on the R3.

```
Raisecom-R3(config)#show ospf database
Database of OSPF Process 1
```

Router LSA (area 1)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.1	1.1.1.1	1763	0x8000001b	0x6aad	36
3.3.3.3	3.3.3.3	1762	0x8000001b	0xe424	36

Network LSA (area 1)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
3.1.1.3	3.3.3.3	1762	0x8000001a	0xb85c	32

SummaryNetwork LSA (area 1)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.0	1.1.1.1	6	0x8000001b	0x86ac	28
4.1.1.0	1.1.1.1	6	0x8000001b	0x69c5	28

NSSA LSA (area 1)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.0	1.1.1.1	6	0x8000001b	0x9c17	36

Step 5 Configure R3 to redistribute the static route of 200.1.1.0.

```
Raisecom-R3(config)#ip route-static 200.1.1.0 255.255.255.0 3.1.1.1
Raisecom-R3(config)#ospf 1
Raisecom-R3(config-ospf-1)#import-route static
```

Step 6 Verify configuration results.

There are type-5 LSA and NSSA LSA of 200.1.1.0 on R3.

```
Raisecom-R3(config)#show ospf database
Database of OSPF Process 1
```

Router LSA (area 1)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len

1.1.1.1	1.1.1.1	286	0x8000001c	0x68ae	36
3.3.3.3	3.3.3.3	194	0x8000001d	0xe61e	36

Network LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
3.1.1.3	3.3.3.3	286	0x8000001b	0xb65d	32

SummaryNetwork LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.0	1.1.1.1	330	0x8000001b	0x86ac	28
4.1.1.0	1.1.1.1	330	0x8000001b	0x69c5	28

NSSA LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.0	1.1.1.1	330	0x8000001b	0x9c17	36
200.1.1.0	3.3.3.3	0	0x80000001	0x1bd1	36

ASExternal LSA

LinkId	ADV Router	Age	Seq#	CheckSum	Len
200.1.1.0	3.3.3.3	0	0x80000001	0x9163	36

Check the routing table and database of R4. There are the 200.1.1.0 route and LSA.

Raisecom-R4(config)#show ospf route

```

OSPF Process 1
RoutType Prefix          PathType Cost    Cost2    NextHop
BackupNextHop AreaId Time
ABR      2.2.2.2/32         INTRA    1        0        4.1.1.2
0.0.0.0  2          0:03:46
ASBR     1.1.1.1/32         INTER    2        0        4.1.1.2
0.0.0.0  0          0:00:00
ASBR     3.3.3.3/32         INTER    3        0        4.1.1.2
0.0.0.0  0          0:00:00
Network  1.1.1.0/24         INTER    2        0        4.1.1.2
0.0.0.0  N/A         13:59:11
Network  3.1.1.0/24         INTER    3        0        4.1.1.2
0.0.0.0  N/A         13:59:11
Network  4.1.1.0/24         INTRA    1        0        4.1.1.4
0.0.0.0  N/A         13:59:13
Network  200.1.1.0/24        ASE2     3        1        4.1.1.2
0.0.0.0  N/A         0:03:46

```

Route :

ABR	ASBR	Network	Intra	Inter	External
1	2	4	1	2	1

Path :

ABR	ASBR	Network	Intra	Inter	External
1	2	4	1	2	1

Raisecom-R4(config)#show ospf database

Database of OSPF Process 1

Router LSA (area 2)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
2.2.2.2	2.2.2.2	1782	0x8000001d	0xb65d	36
4.4.4.4	4.4.4.4	1403	0x8000001e	0x3bc4	36
Network LSA (area 2)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
4.1.1.4	4.4.4.4	1782	0x8000001c	0x4cc0	32
SummaryNetwork LSA (area 2)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.0	2.2.2.2	1783	0x8000001e	0xda59	28
3.1.1.0	2.2.2.2	1781	0x8000001c	0xce64	28
SummaryASBR LSA (area 2)					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.1	2.2.2.2	589	0x8000001b	0xc86c	28
3.3.3.3	2.2.2.2	454	0x80000001	0xaa9b	28
ASExternal LSA					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
100.1.1.1	4.4.4.4	1400	0x8000001b	0x91a3	36
200.1.1.0	1.1.1.1	262	0x80000001	0xcd2f	36

3.8.15 Configuring OSPF to redistribute external routes

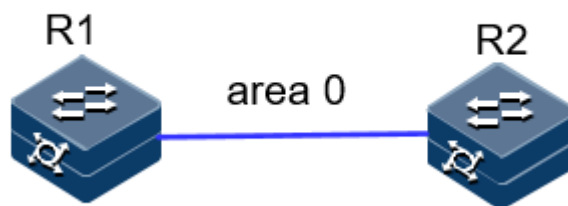
Networking requirements

As shown below, both routers are running OSPF and are configured as region 0. Assume that R1 needs to redistribute external routes to OSPF, R1 has the static route 100.1.1.0/24 and local route 200.1.1.1/32, but external routes have the following requirements:

- Accept all direct routing and use default configuration.
- Receive all static routes and configure the cost of routes to 2000.

After configuration is complete, each device should learn the routing to all network segments within the AS.

Figure 3-29 Networking with OSPF to redistribute external routes



Configuration steps

Step 1 Configure IP addresses of interfaces.

- IP address of one interface on R1: 1.1.1.1/24
- IP address of one interface on R2: 1.1.1.2/24

Step 2 Configure OSPF.

R1:

```
Raisecom-R1#configure
Raisecom-R1(config)#ospf 1
Raisecom-R1(config-ospf-1)#router-id 1.1.1.1
Raisecom-R1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
Raisecom-R1(config-ospf-1)#
```

R2:

```
Raisecom-R2#configure
Raisecom-R2(config)#ospf 1
Raisecom-R2(config-ospf-1)#router-id 2.2.2.2
Raisecom-R2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
Raisecom-R2(config-ospf-1)#
```

Step 3 Configure redistribution.

```
Raisecom-R1#configure
Raisecom-R1(config)#ospf 1
Raisecom-R1(config-ospf-1)#import-route connect
Raisecom-R1(config-ospf-1)#import-route static cost 2000
```

Step 4 Check configuration results.

```
Raisecom-R1(config)#show ospf import-route
Import Route of OSPF(1)
dest          mask          nexthop        cost    proto  pid
1.1.1.0       255.255.255.0 1.1.1.1        1       connect 0
100.1.1.0     255.255.255.0 1.1.1.3        60      static  0
200.1.1.1     255.255.255.255 200.1.1.1      1       connect 0
Raisecom-R1(config)#show ospf database ls-type as-external-lsa
Database of OSPF Process 1
```

ASExternal LSA						
LinkId	ADV Router	Age	Seq#	Checksum	Len	
1.1.1.0	1.1.1.1	324	0x80000001	0xdce9	36	
100.1.1.0	1.1.1.1	21	0x80000001	0x4a40	36	
200.1.1.1	1.1.1.1	285	0x80000001	0x7b86	36	

Use the following command to show the routing table on R2.

```
Raisecom-R2(config)#show ospf route
OSPF Process 1
RoutType Prefix          PathType Cost    Cost2    NextHop
BackupNextHop AreaId Time
ASBR      1.1.1.1/32             INTRA    1        0        1.1.1.1
0.0.0.0    0          0:00:38
Network   1.1.1.0/24             INTRA    1        0        1.1.1.2
0.0.0.0    N/A        0:09:33
Network   100.1.1.0/24           ASE2     1        2000     1.1.1.3
0.0.0.0    N/A        0:00:38
Network   200.1.1.1/32           ASE2     1        1        1.1.1.1
0.0.0.0    N/A        0:05:02
Route :
ABR      ASBR      Network Intra    Inter    External
0        1        3        1        0        2

Path :
ABR      ASBR      Network Intra    Inter    External
0        1        3        1        0        2
```

3.8.16 Example for configuring OSPF route aggregation

Networking requirements

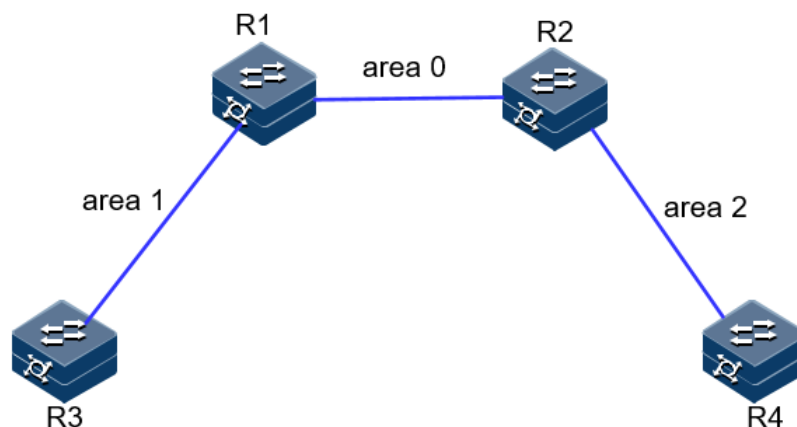
As shown below, the network requirement are as below: there are intra-area routes of 10.1.1.1/32, 10.1.2.1/32, 20.1.1.1/32, and 20.1.2.1/32 in area 2; aggregate 10.1.1.1/32 and 10.1.2.1/32 into 10.1.0.0/16 for advertisement; 20.1.1.1/32 and 20.1.2.1/32 will not be redistributed into other regions.

R4 has external routes of 30.1.1.1/32 and 30.1.2.1/32, which are required to be advertised to other regions.

The device capability in area 1 is too poor to receive a large number of external routes, but R3 has external routes of 40.1.1.1/32 and 40.1.1.2/32, which are required to be advertised to other regions.

According to the above requirements, configure aggregation and filtering entries for area 2, and configure NSSA attributes for area 1.

Figure 3-30 OSPF route aggregation networking



Configuration steps

Step 1 Configure basic functions of OSPF.

Step 2 Configure area 1 as the NSSA area.

R1:

```
Raisecom-R1#configure
Raisecom-R1(config)#ospf 1
Raisecom-R1(config-ospf-1)#area 1 nssa
```

R3:

```
Raisecom-R3#configure
Raisecom-R3(config)#ospf 1
Raisecom-R3(config-ospf-1)#area 1 nssa
```

Step 3 Show the route entries and database before route aggregation.

```
Raisecom-R2(config)#show ospf route
OSPF Process 1
RoutType Prefix PathType Cost Cost2 NextHop
BackupNextHop AreaId Time
ABR 1.1.1.1/32 INTRA 1 0 1.1.1.1
0.0.0.0 0 0:02:22
ASBR 1.1.1.1/32 INTRA 1 0 1.1.1.1
0.0.0.0 0 0:02:22
ASBR 3.3.3.3/32 INTER 2 0 1.1.1.1
0.0.0.0 0 0:02:22
```

```

ASBR    4.4.4.4/32      INTRA    1      0      4.1.1.4
0.0.0.0      0      0:00:00
Network  1.1.1.0/24      INTRA    1      0      1.1.1.2
0.0.0.0      N/A      14:59:45
Network  3.1.1.0/24      INTER    2      0      1.1.1.1
0.0.0.0      N/A      14:59:44
Network  4.1.1.0/24      INTRA    1      0      4.1.1.2
0.0.0.0      N/A      14:59:44
Network  10.1.1.1/32     INTRA    2      0      4.1.1.4
0.0.0.0      N/A      0:05:20
Network  10.1.2.1/32     INTRA    2      0      4.1.1.4
0.0.0.0      N/A      0:05:15
Network  20.1.1.1/32     INTRA    2      0      4.1.1.4
0.0.0.0      N/A      0:05:07
Network  20.1.2.1/32     INTRA    2      0      4.1.1.4
0.0.0.0      N/A      0:05:06
Network  30.1.1.1/32     ASE2     1      1      4.1.1.3
0.0.0.0      N/A      0:04:07
Network  30.1.2.1/32     ASE2     1      1      4.1.1.3
0.0.0.0      N/A      0:04:03
Network  40.1.1.1/32     ASE2     2      1      1.1.1.1
0.0.0.0      N/A      0:02:24
Network  40.1.1.2/32     ASE2     2      1      1.1.1.1
0.0.0.0      N/A      0:02:22
Route :
ABR      ASBR      Network  Intra    Inter    External
1        3        11      6        1        4

Path :
ABR      ASBR      Network  Intra    Inter    External
1        3        11      6        1        4

```

Step 4 Configure ABR aggregation on R2. Aggregate 10.1.1.1/32 and 10.1.2.1/32 into 10.1.0.0/16 for advertisement; 20.1.1.1/32 and 20.1.2.1/32 will not be advertised after aggregation.

```

Raisecom-R2#configure
Raisecom-R2(config)#ospf 1
Raisecom-R2(config-ospf-1)#area 2 abr-summary 10.1.0.0/16 advertise
Raisecom-R2(config-ospf-1)#area 2 abr-summary 20.1.0.0/16 no-advertise

```

Step 5 Verify configuration results.

The routing table of R1 contains the 10.1.0.0/16 route only, without 10.1.1.1/32, 10.1.2.1/32, 20.1.1.1/32, and 20.1.2.1/32.

```

Raisecom-R1(config)#show ospf route
OSPF Process 1
  RoutType Prefix          PathType Cost    Cost2    NextHop
BackupNextHop    AreaId Time

```

```

ABR      2.2.2.2/32      INTRA    1      0      1.1.1.2
0.0.0.0      0      0:00:11
ASBR     4.4.4.4/32      INTER    2      0      1.1.1.2
0.0.0.0      0      0:00:11
ASBR     3.3.3.3/32      INTRA    1      0      3.1.1.3
0.0.0.0      0      0:00:00
Network   1.1.1.0/24      INTRA    1      0      1.1.1.1
0.0.0.0      N/A      15:09:50
Network   3.1.1.0/24      INTRA    1      0      3.1.1.1
0.0.0.0      N/A      14:19:11
Network   4.1.1.0/24      INTER    2      0      1.1.1.2
0.0.0.0      N/A      15:09:48
Network  10.1.0.0/16      INTER    3      0      1.1.1.2
0.0.0.0      N/A      0:06:36
Network  30.1.1.1/32      ASE2     2      1      1.1.1.2
0.0.0.0      N/A      0:14:12
Network  30.1.2.1/32      ASE2     2      1      1.1.1.2
0.0.0.0      N/A      0:14:08
Network  40.1.1.1/32      ASE2     1      1      3.1.1.2
0.0.0.0      N/A      0:00:14
Network  40.1.1.2/32      ASE2     1      1      3.1.1.2
0.0.0.0      N/A      0:00:11
Route :
ABR      ASBR      Network  Intra    Inter    External
1        2        8        2        2        4

Path :
ABR      ASBR      Network  Intra    Inter    External
1        2        8        2        2        4

```

Step 6 Configure ASBR aggregation on R4. Aggregate 30.1.1.1/32 and 30.1.2.1/32 into 30.1.0.0/16.

```

Raisecom-R4#configure
Raisecom-R4(config)#ospf 1
Raisecom-R4(config-ospf-1)#asbr-summary 30.1.0.0/16

```

Step 7 Verify configuration results.

Check the routing table and database of R2. The aggregation is successful.

```

Raisecom-R2(config)#show ospf route
OSPF Process 1
RoutType Prefix          PathType Cost   Cost2   NextHop
BackupNextHop AreaId Time
ABR      1.1.1.1/32      INTRA    1      0      1.1.1.1
0.0.0.0      0      0:01:33
ASBR     1.1.1.1/32      INTRA    1      0      1.1.1.1
0.0.0.0      0      0:01:33
ASBR     3.3.3.3/32      INTER    2      0      1.1.1.1
0.0.0.0      0      0:01:33

```

```

ASBR    4.4.4.4/32      INTRA    1      0      4.1.1.4
0.0.0.0      0      0:00:00
Network  1.1.1.0/24      INTRA    1      0      1.1.1.2
0.0.0.0      N/A      15:14:02
Network  3.1.1.0/24      INTER    2      0      1.1.1.1
0.0.0.0      N/A      15:14:01
Network  4.1.1.0/24      INTRA    1      0      4.1.1.2
0.0.0.0      N/A      15:14:01
Network  10.1.1.1/32      INTRA    2      0      4.1.1.4
0.0.0.0      N/A      0:19:37
Network  10.1.2.1/32      INTRA    2      0      4.1.1.4
0.0.0.0      N/A      0:19:32
Network  20.1.1.1/32      INTRA    2      0      4.1.1.4
0.0.0.0      N/A      0:19:24
Network  20.1.2.1/32      INTRA    2      0      4.1.1.4
0.0.0.0      N/A      0:19:23
Network  30.1.0.0/16      ASE2     1      1      4.1.1.4
0.0.0.0      N/A      0:01:34
Network  40.1.1.1/32      ASE2     2      1      1.1.1.1
0.0.0.0      N/A      0:04:26
Network  40.1.1.2/32      ASE2     2      1      1.1.1.1
0.0.0.0      N/A      0:04:23

```

Route :

ABR	ASBR	Network	Intra	Inter	External
1	3	10	6	1	3

Path :

ABR	ASBR	Network	Intra	Inter	External
1	3	10	6	1	3

Raisecom-R2(config)#show ospf database ls-type as-external-lsa
Database of OSPF Process 1

ASExternal LSA						
LinkId	ADV Router	Age	Seq#	Checksum	Len	
30.1.0.0	4.4.4.4	110	0x80000001	0xe0c1	36	
40.1.1.1	1.1.1.1	283	0x80000001	0xf9a1	36	
40.1.1.2	1.1.1.1	279	0x80000001	0xefaa	36	

Step 8 Configure NSSA aggregation on R1 to aggregate NSSA LSA generated on R3 upon conversion.

```

Raisecom-R1#configure
Raisecom-R1(config)#ospf 1
Raisecom-R1(config-ospf-1)#area 1 nssa summary 40.1.1.0/24 advertise

```

Step 9 Check configuration results.

Aggregate external LSA generated by R1.

```
Raisecom-R2(config)#show ospf route
OSPF Process 1
RoutType Prefix          PathType Cost  Cost2  NextHop
BackupNextHop AreaId Time
ABR 1.1.1.1/32 INTRA 1 0 1.1.1.1
0.0.0.0 0 0:00:54
ASBR 1.1.1.1/32 INTRA 1 0 1.1.1.1
0.0.0.0 0 0:00:54
ASBR 3.3.3.3/32 INTER 2 0 1.1.1.1
0.0.0.0 0 0:00:54
ASBR 4.4.4.4/32 INTRA 1 0 4.1.1.4
0.0.0.0 0 0:00:00
Network 1.1.1.0/24 INTRA 1 0 1.1.1.2
0.0.0.0 N/A 15:18:01
Network 3.1.1.0/24 INTER 2 0 1.1.1.1
0.0.0.0 N/A 15:18:00
Network 4.1.1.0/24 INTRA 1 0 4.1.1.2
0.0.0.0 N/A 15:18:00
Network 10.1.1.1/32 INTRA 2 0 4.1.1.4
0.0.0.0 N/A 0:23:36
Network 10.1.2.1/32 INTRA 2 0 4.1.1.4
0.0.0.0 N/A 0:23:31
Network 20.1.1.1/32 INTRA 2 0 4.1.1.4
0.0.0.0 N/A 0:23:23
Network 20.1.2.1/32 INTRA 2 0 4.1.1.4
0.0.0.0 N/A 0:23:22
Network 30.1.0.0/16 ASE2 1 1 4.1.1.4
0.0.0.0 N/A 0:05:33
Network 40.1.1.0/24 ASE2 1 2 1.1.1.1
0.0.0.0 N/A 0:00:54
Route :
ABR ASBR Network Intra Inter External
1 3 9 6 1 2

Path :
ABR ASBR Network Intra Inter External
1 3 9 6 1 2
Raisecom-R2(config)#show ospf database ls-type as-external-lsa
Database of OSPF Process 1

ASExternal LSA
LinkId ADV Router Age Seq# CheckSum Len
30.1.0.0 4.4.4.4 337 0x80000001 0xe0c1 36
40.1.1.0 1.1.1.1 58 0x80000001 0xb7ea 36
```

3.8.17 Example for configuring OSPF virtual connection

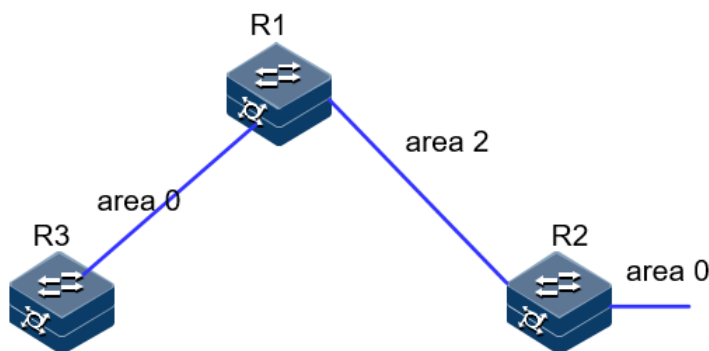
Networking requirements

After OSPF regions are divided, OSPF routing updates between non-backbone regions are complete through exchange between backbone regions. Therefore, OSPF requires all non-backbone regions to be connected to the backbone regions, and requires backbone regions to

be connected. However, in practical applications, due to various limitations, this requirement may not be met. In this case, configuring OSPF virtual connections can solve this problem.

As shown below, R3 is located in area 0; R1 connects area 0 and area 2 while R2 connects area 0 and area 2. At this point, area 0 is segmented and the internal routes of area 2 cannot be learned within area 0; area 2 cannot learn the internal routes of area 0 and the routes of other areas. At this point, configure a virtual connection between R1 and R4 to connect to area 0.

Figure 3-31 OSPF virtual connection networking



Configuration steps

Step 1 Configure IP addresses of interfaces.

- IP addresses of two interfaces on R1: 1.1.1.1/24 and 3.1.1.1/24
- IP address of one interface on R2: 1.1.1.2/24 and the IP address of the loopback address 2.2.2.2/32
- IP address of one interface on R3: 3.1.1.3/24 and the IP address of the loopback address 3.3.3.3/32

Step 2 Configure OSPF.

R1:

```
Raisecom-R1#configure
Raisecom-R1(config)#ospf 1
Raisecom-R1(config-ospf-1)#router-id 1.1.1.1
Raisecom-R1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 2
Raisecom-R1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 0
Raisecom-R1(config-ospf-1)#
```

R2:

```
Raisecom-R2#configure
Raisecom-R2(config)#ospf 1
Raisecom-R2(config-ospf-1)#router-id 2.2.2.2
Raisecom-R2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 2
Raisecom-R2(config-ospf-1)#network 2.2.2.2 255.255.255.255 area 0
```

```
Raisecom-R2(config-ospf-1)#
```

R3:

```
Raisecom-R3#configure
Raisecom-R3(config)#ospf 1
Raisecom-R3(config-ospf-1)#router-id 3.3.3.3
Raisecom-R3(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 0
Raisecom-R3(config-ospf-1)#network 3.3.3.3 255.255.255.255 area 0
Raisecom-R3(config-ospf-1)#
```

Step 3 Check configuration results.

```
Raisecom-R1#show ospf neighbor
```

```

OSPF Process 1
  IpAddress      NeighborID      Priority  State      Aging
  UpTime        Interface
-----
  1.1.1.2        2.2.2.2        1        full       37      0:06:10
vlan-10
  3.1.1.3        3.3.3.3        1        full       30      0:04:57
vlan-13
-----
  Down:0        Attempt:0      Init:0        TwoWay:0      ExchangeStart:0
Exchange:0
  Loading:0      Full:2

```

R2 fails to learn the route to 3.3.3.3. R1 or R2 also fails to learn the route to 2.2.2.2.

```
Raisecom-R2(config)#show ospf route
```

```

OSPF Process 1
  RoutType Prefix      PathType Cost  Cost2  NextHop
BackupNextHop AreaId Time
  ABR      1.1.1.1/32      INTRA    1     0      1.1.1.1
0.0.0.0    2      0:07:41
  Network  1.1.1.0/24      INTRA    1     0      1.1.1.2
0.0.0.0    N/A    0:09:38
  Network  2.2.2.2/32      INTRA    1     0      2.2.2.2
0.0.0.0    N/A    0:09:20
Route :
  ABR      ASBR      Network  Intra  Inter  External
  1        0        2        2      0      0
Path :

```



```

ABR      ASBR      Network  Intra  Inter  External
1         0         2         2         0         0

Raisecom-R1#show ospf route
OSPF Process 1
RoutType Prefix          PathType Cost   Cost2   NextHop
BackupNextHop AreaId Time
ABR      2.2.2.2/32        INTRA    1      0        1.1.1.2
0.0.0.0   2      0:08:38
Network  1.1.1.0/24            INTRA    1      0        1.1.1.1
0.0.0.0   N/A    0:09:55
Network  3.1.1.0/24            INTRA    1      0        3.1.1.1
0.0.0.0   N/A    0:08:42
Network  3.3.3.3/32            INTRA    2      0        3.1.1.3
0.0.0.0   N/A    0:08:38
Route :
ABR      ASBR      Network  Intra  Inter  External
1         0         3         3         0         0

Path :
ABR      ASBR      Network  Intra  Inter  External
1         0         3         3         0         0

```

Step 4 Configure virtual connection.

R1:

```

Raisecom-R1#configure
Raisecom-R1(config)#ospf 1
Raisecom-R1(config-ospf-1)#area 2 virtual-link 2.2.2.2

```

R2:

```

Raisecom-R2#configure
Raisecom-R2(config)#ospf 1
Raisecom-R2(config-ospf-1)#area 2 virtual-link 1.1.1.1

```

Step 5 Check configuration results.

Check whether the virtual connection is established normally.

```

Raisecom-R1(config)#show ospf virtual-link
OSPF Process 1
Area Id           :2
Enable Status     :Enable
State             :pointToPoint
Event Change      :3
Hello Interval    :10

```

```

Retransmit Interval      :5
Transmit Delay           :1
Dead Interval            :40
Auth Type                 :0(None)
Neighbor Address          :1.1.1.2
Neighbor Router Id        :2.2.2.2
Neighbor State            :full
Neighbor Event Count      :5
Neighbor Retransmit Queue Length:0
Neighbor Options          :0x2

```

Check whether the routing table is learnt normally.

Raisecom-R1(config)#show ospf route

```

OSPF Process 1
RoutType Prefix          PathType Cost  Cost2  NextHop
BackupNextHop AreaId Time
ABR      2.2.2.2/32        INTRA   1     0      1.1.1.2
0.0.0.0   2      0:01:45
Network  1.1.1.0/24        INTRA   1     0      1.1.1.1
0.0.0.0   N/A    0:13:44
Network  2.2.2.2/32        INTRA   2     0      1.1.1.2
0.0.0.0   N/A    0:01:45
Network  3.1.1.0/24        INTRA   1     0      3.1.1.1
0.0.0.0   N/A    0:12:31
Network  3.3.3.3/32        INTRA   2     0      3.1.1.3
0.0.0.0   N/A    0:12:27
Route :
ABR      ASBR    Network Intra  Inter External
2        0        4      4      0      0

Path :
ABR      ASBR    Network Intra  Inter External
1        0        4      4      0      0

```

Raisecom-R2(config)#show ospf route

```

OSPF Process 1
RoutType Prefix          PathType Cost  Cost2  NextHop
BackupNextHop AreaId Time
ABR      1.1.1.1/32        INTRA   1     0      1.1.1.1
0.0.0.0   2      0:02:23
Network  1.1.1.0/24        INTRA   1     0      1.1.1.2
0.0.0.0   N/A    0:14:58
Network  2.2.2.2/32        INTRA   1     0      2.2.2.2
0.0.0.0   N/A    0:14:40
Network  3.1.1.0/24        INTRA   2     0      1.1.1.1
0.0.0.0   N/A    0:02:23
Network  3.3.3.3/32        INTRA   3     0      1.1.1.1
0.0.0.0   N/A    0:02:23
Route :
ABR      ASBR    Network Intra  Inter External
2        0        4      4      0      0

```

Path :
ABR ASBR Network Intra Inter External
1 0 4 4 0 0

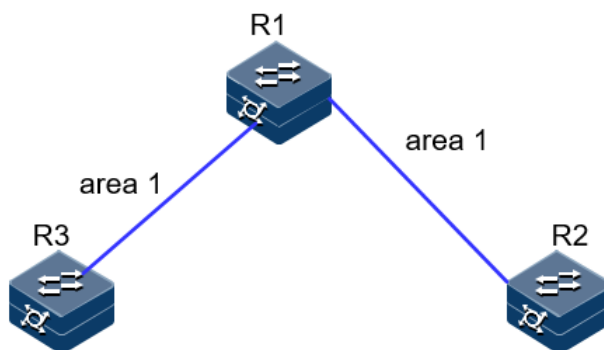
3.8.18 Example for configuring OSPF authentication

Networking requirements

As shown below, R1, R2, and R3 are all located in area 0. Establish a virtual connection between R2 and R3, with configuration requirements as below:

- Simple password authentication is used between R1 and R2, with the password of test.
- R2 and R3 establish a virtual connection, using MD5 authentication with the password of aaa and ID of 100.
- R1 and R3 use MD5 authentication, with the password of ccc and ID of 110.

Figure 3-32 OSPF authentication networking



Configuration steps

Step 1 Configure IP addresses of interfaces.

- IP addresses of two interfaces on R1: 1.1.1.1/24 and 3.1.1.1/24
- IP address of one interface on R2: 1.1.1.2/24
- IP address of one interface on R3: 3.1.1.3/24

Step 2 Configure OSPF.

R1:

```

Raisecom-R1#configure
Raisecom-R1(config)#ospf 1
Raisecom-R1(config-ospf-1)#router-id 1.1.1.1
Raisecom-R1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 1
Raisecom-R1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
Raisecom-R1(config-ospf-1)#
  
```

R2:

```
Raisecom-R2#configure
Raisecom-R2(config)#ospf 1
Raisecom-R2(config-ospf-1)#router-id 2.2.2.2
Raisecom-R2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 1
Raisecom-R2(config-ospf-1)#area 1 virtual-link 3.3.3.3
Raisecom-R2(config-ospf-1)#
```

R3:

```
Raisecom-R3#configure
Raisecom-R3(config)#ospf 1
Raisecom-R3(config-ospf-1)#router-id 3.3.3.3
Raisecom-R3(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
Raisecom-R3(config-ospf-1)#area 1 virtual-link 2.2.2.2
Raisecom-R3(config-ospf-1)#
```

Step 3 Check configuration results.

```
Raisecom-R1#show ospf neighbor
  OSPF Process 1
  IpAddress      NeighborID      Priority  State      Aging
  UpTime        Interface
-----
1.1.1.2         2.2.2.2         1        full        36      0:00:14
vlan-12
3.1.1.3         3.3.3.3         1        full        38      0:01:12
vlan-13
-----
Down:0          Attempt:0        Init:0          Twoway:0        ExchangeStart:0
Exchange:0
Loading:0        Full:2
```

```
Raisecom-R2(config)#show ospf virtual-link
  OSPF Process 1
  Area Id          :1
  Enable Status     :Enable
  State             :pointToPoint
  Event Change      :3
  Hello Interval    :10
  Retransmit Interval :5
  Transmit Delay    :1
  Dead Interval     :40
  Auth Type         :0(None)
  Neighbor Address   :3.1.1.3
  Neighbor Router Id :3.3.3.3
```

```
Neighbor State           :full
Neighbor Event Count     :5
Neighbor Retransmit Queue Length:0
Neighbor Options         :0x2
```

Step 4 Configure authentication between R1 and R2 and between R1 and R3, and enter interface configuration mode.

R1:

```
Raisecom-R1(config)#interface vlan 12
Raisecom-R1(config-vlanif-12)#ospf authentication simple plain test
Raisecom-R1(config-vlanif-12)#exit
Raisecom-R1(config)#interface vlan 13
Raisecom-R1(config-vlanif-13)#ospf authentication md5 110 plain ccc
Raisecom-R1(config-vlanif-13)#exit
```

R2:

```
Raisecom-R2(config)#interface vlan 12
Raisecom-R2(config-vlanif-12)#ospf authentication simple plain test
Raisecom-R2(config-vlanif-12)#exit
Raisecom-R2(config)#ospf 1
Raisecom-R2(config-ospf-1)#area 1 virtual-link 3.3.3.3 authentication md5
100 plain aaa
```

R3:

```
Raisecom-R3(config)#interface vlan 13
Raisecom-R3(config-vlanif-13)#ospf authentication md5 110 plain ccc
Raisecom-R3(config-vlanif-13)#exit
Raisecom-R3(config)#ospf 1
Raisecom-R3(config-ospf-1)#area 1 virtual-link 2.2.2.2 authentication md5
100 plain aaa
```

Step 5 Check configuration results.

Check whether the neighbor relation is established normally.

```
Raisecom-R1(config)#show ospf neighbor
```

```
OSPF Process 1
IpAddress      NeighborID      Priority State      Aging
UpTime        Interface
```

```

-----
1.1.1.2      2.2.2.2      1      full      39      0:00:02
vlan-12
3.1.1.3      3.3.3.3      1      full      39      0:00:12
vlan-13
-----
Down:0      Attempt:0      Init:0      TwoWay:0      ExchangeStart:0
Exchange:0
Loading:0      Full:2

```

```

Raisecom-R2(config)#show ospf virtual-link
OSPF Process 1
Area Id      :1
Enable Status :Enable
State        :pointToPoint
Event Change :15
Hello Interval :10
Retransmit Interval :5
Transmit Delay :1
Dead Interval :40
Auth Type    :2(MD5 Key)
MD5 Key ID   :100
MD5 Key      :aaa
Neighbor Address :3.1.1.3
Neighbor Router Id :3.3.3.3
Neighbor State :full
Neighbor Event Count :5
Neighbor Retransmit Queue Length:0
Neighbor Options :0x2

```

3.9 OSPFv3

3.9.1 Introduction

Functions

OSPFv3 is an OSPF routing protocol (RFC2740) running on IPv6, which is enhanced on the basis of OSPFv2 and is an independent routing protocol. The working principle of OSPFv3, in aspects of the Hello packet, status machine, LSDB, flooding mechanism, and routing calculation, and so on, is consistent with OSPFv2. OSPFv3 divides the AS into one or more logically defined areas and advertises routes in the form of LSA. OSPFv3 relies on the interaction of OSPFv3 packets among devices within the OSPFv3 area to implement unified routing information. OSPFv3 packets are encapsulated within IPv6 packets and can be sent in both unicast and multicast formats.

Comparison of OSPFv3 with OSPFv2

OSPFv3 is based on links, not network segments. IPv6 is based on links rather than network segments. In this way, when OSPFv3 is configured, do not consider whether it is configured in the same network segment. As long as devices are on the same link, they can establish a connection directly without being configured with the global IPv6 address.

OSPFv3 removed the meaning of IP addresses to separate the topology and addresses. OSPFv3 can calculate the OSPFv3 topology without relying on the configuration of IPv6 global addresses.

The packet and LSA format of OSPFv3 have changed. The OSPFv3 packet does not contain an IP address. The router LSA and network LSA of OSPFv3 do not contain IP addresses. The IP address section is advertised by two new types of LSA (Link LSA and Intra-area Prefix LSA).

OSPFv3 utilizes IPv6 link local addresses to discover neighbors and automatically configure IPv6 link local addresses on the same link. OSPFv3 is a routing protocol running on IPv6, which also uses link local addresses to maintain neighbors and synchronize LSA databases.

OSPFv3 removes all authentication fields, but directly uses IPv6 authentication and security processing instead of its own authentication. When it is used, the protocol itself needs to be considered.

Two new types of LSAs are added:

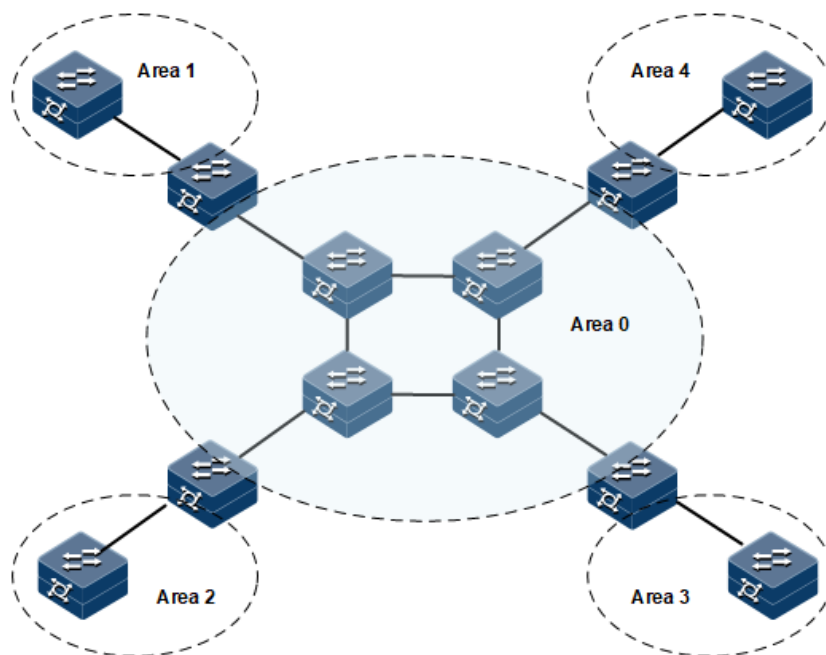
- Link LSA: used by routers to advertise the corresponding link local addresses and their configured IPv6 global addresses on each link, only flooded within the link
- Intra-area Prefix LSA: used to announce the IPv6 global addresses of this router or network (broadcast network and NBMA) to others, flooded within the area

OSPFv3 area division

With the increasing scale of the network, when all devices on a large network run OSPFv3, the increase in the number of devices will cause the Link State Database (LSDB) to be very large, occupying a lot of storage space, increasing the complexity of running the SPF algorithm, and resulting in a heavy burden on the devices. After the network scale increases, the probability of topology changes also increases, and the network often becomes "turbulent", causing a large number of OSPFv3 packets to be transmitted on the network, reducing the bandwidth utilization of the network. The even more serious situation is that each change will cause all devices on the network to perform routing calculations again.

To address the previous issues, OSPFv3 divides an AS into different areas. Areas logically divide routers into different groups, and each area is identified by an area ID. The boundary of an area is a router, not a link. A network segment (link) can belong to only one area, or each interface running OSPFv3 must indicate the area to which it belongs.

Figure 3-33 OSPFv3 area division

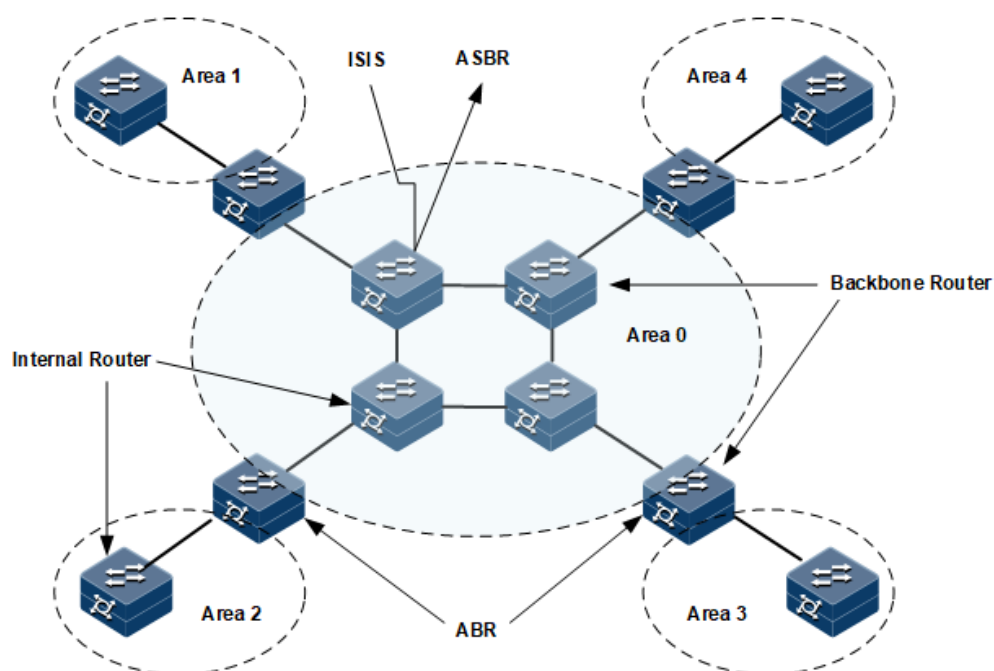


After dividing areas, route aggregation can be performed on the Area Boundary Router (ABR) to reduce the number of LSAs notified to other areas. In addition, dividing areas can also minimize the impact of network topology changes.

The types of OSPFv3 areas include common areas, Stub areas, and NSSA areas.

OSPFv3 router types

Figure 3-34 Example of OSPFv3 router types



- Internal Router: all interfaces of this type of routes belong to the same OSPFv3 area.

- ABR: this type of devices can belong to two or more areas simultaneously, but one of them must be a backbone area. The ABR is used to connect the backbone area and non-backbone area, and it can be physically or logically connected to the backbone area.
- Backbone router: this type of devices has at least one interface belonging to the backbone area. All ABRs and internal devices located in Area 0 are backbone routers.
- Autonomous System Boundary Router (ASBR): a device that exchanges routing information with other ASs is called the ASBR. The ASBR may not necessarily be located at the boundary of an AS, and it may be a device within the area or an ABR. As long as an OSPFv3 device redistributes external routing information, it becomes an ASBR.

OSPFv3 packets

OSPFv3 has the following five types of protocol packets:

- Hello packet: sent periodically to discover and maintain OSPFv3 neighbor relationships.
- Database Description (DD) packet: describe the summary information of the local LSDB, and is used for database synchronization when two routers begin to establish adjacency.
- Link State Request (LSR) packet: request the required LSA from the other party.
- Link State Update (LSU) packet: send the required LSA to the other party.
- Link State Acknowledgment (LSAck) packet: confirm the received LSA.

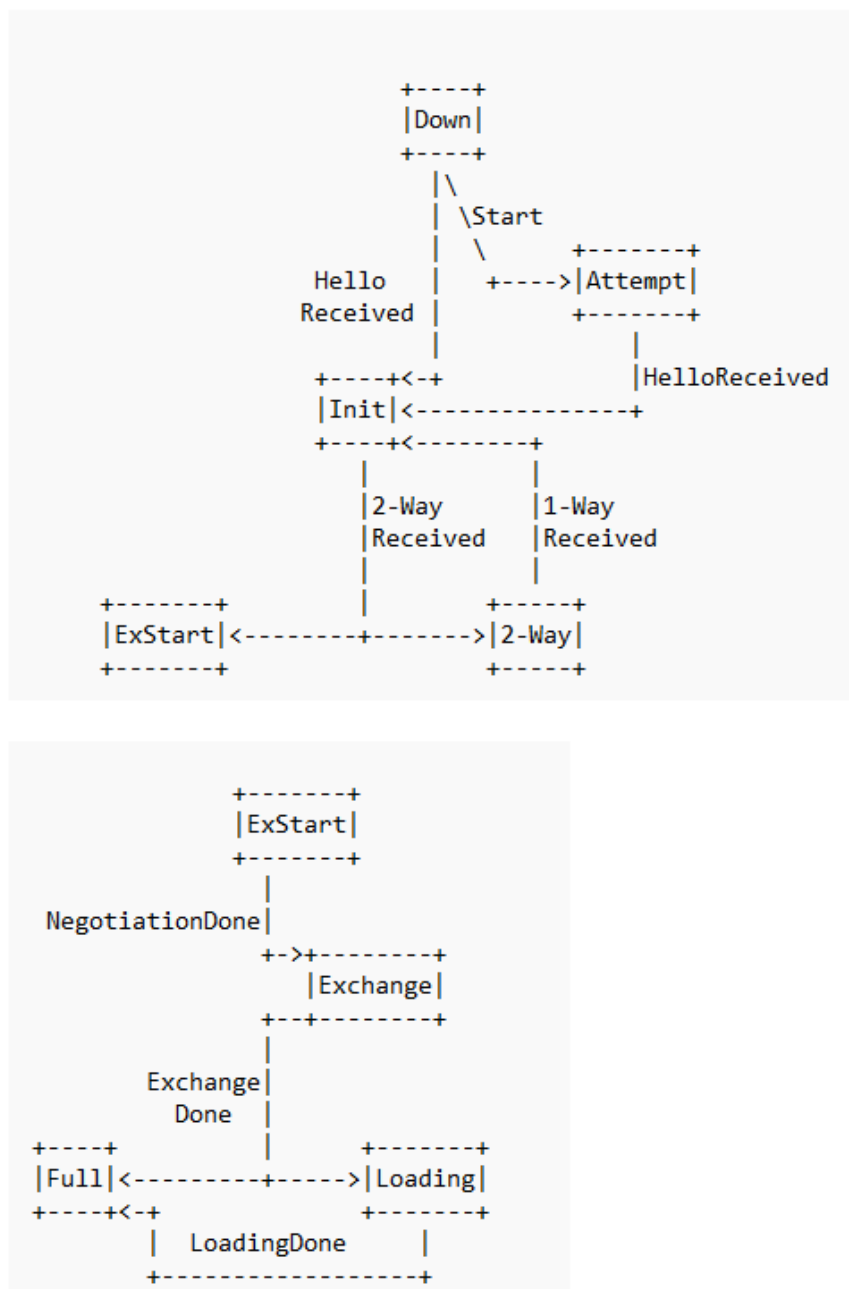
OSPFv3 LSA types

The description of routing information in OSPFv3 is encapsulated and advertised in LSA. Common LSA types include:

- Router LSA (Type1): each router generates a description of the router link status and cost, which is advertised within its respective area.
- Network LSA (Type2): generated by the DR, describing the status of this link and being advertised within its respective area
- Inter-Area-Prefix-LSA (Type3): generated by the ABR, describing the routing of a certain network segment within an area and being advertised to other areas.
- Inter-Area-Router-LSA LSA (Type4): generated by the ABR, describing the route to the ASBR and being advertised to the relevant area
- AS External LSA (Type5): generated by the ASBR, describing the routing to the outside of the AS and being advertised to all areas (except the Stub area and NSSA).
- NSSA LSA (Type7): generated by ASBR, describing the routing to the outside of the AS, and being advertised within the NSSA area only
- Link LSA (Type8): each device generates a Link LSA for each link, describing the link local address and IPv6 prefix address on this link, and providing link options that are configured in Network LSA. The Link LSA is advertised within this link.
- Intra-area Prefix LSA (Type9): each device and DR generates one or more such LSAs, which are advertised within its respective area. The LSA generated by the device describes the IPv6 prefix address associated with the route LSA. The LSA generated by the DR describes the IPv6 prefix address associated with network LSA.

OSPFv3 neighbor status machine

Figure 3-35 OSPFv3 neighbor status machine



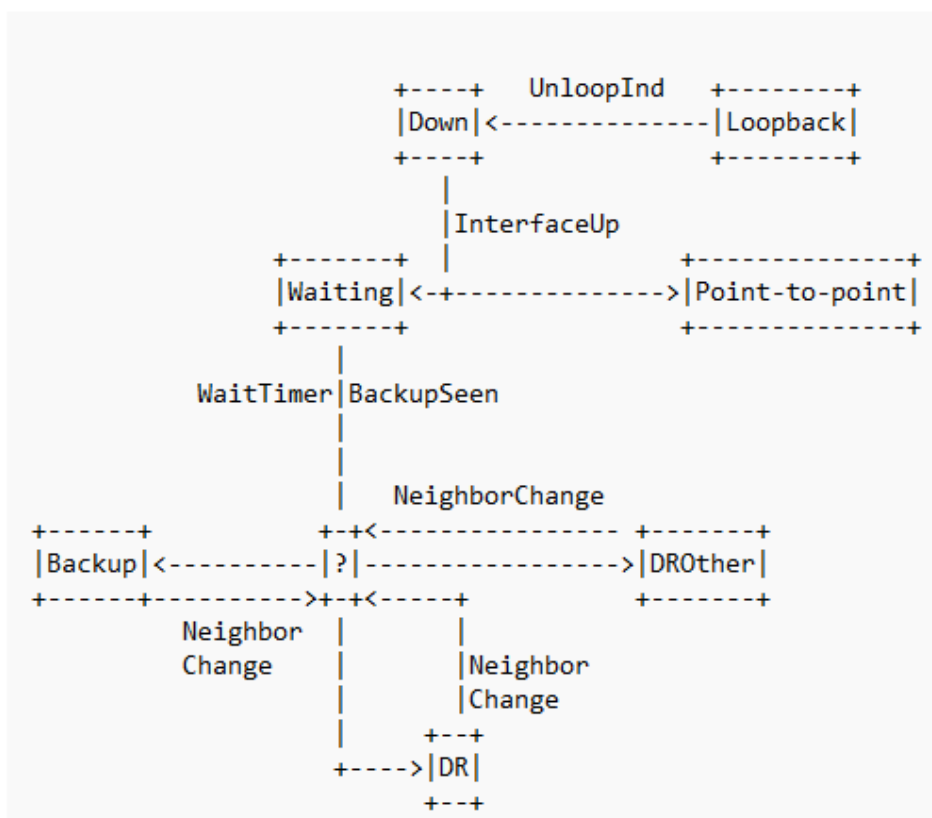
Concepts in the neighbor status machine:

- **Down**: initial stage of neighbor sessions. It indicates that no Hello packet has been received from neighboring devices within the time interval between neighbor failures.
- **Attempt**: regularly send Hello messages to manually configured neighbors in this status. Note that the Attempt status is applicable to NBMA interfaces only.
- **Init**: this status indicates that the neighbor's Hello packet has been received, but the other end has not received the Hello packet sent by the local end.

- 2-way: they are neighbors to each other. This status indicates that both parties have received Hello packet from the peer end and established a neighbor relationship. If no adjacency relationship is formed, the neighbor status machine stays in this status; otherwise, it enters the Exstart status.
- Exstart: negotiate master/slave relationship. Establishing a master/slave relationship is to ensure orderly transmission in subsequent DD packet exchanges.
- Exchange: Exchange DD packets. The local device describes the local LSDB as a DD packet and sends it to neighboring devices.
- Loading: synchronize the LSDB. Both devices send LSR packets to neighbors to request the peer LSA and to synchronize the LSDB.
- Full: establish adjacency. The LSDBs of both devices are synchronized, and the local device and neighboring device have established adjacency status.

OSPFv3 interface status machine

Figure 3-36 OSPFv3 interface status machine



Concepts in the OSPFv3 interface status machine:

- Down: initial status of the interface status
- Loopback: in this status, the interface between the router and the network is looped back.
- Waiting: Only applicable to broadcast and NBMA interface types, attempting to identify DR and BDR on the network at this stage.
- Point-to-point: only applicable to interfaces with point-to-point, point-to-multipoint, and virtual connections. In this status, the device attempts to establish an adjacency relationship with the router on the other end of the interface.

- DR: in this status, the DR of the network successfully connected with the router attempts to establish adjacency with other routers.
- Backup: in this status, the BDR of the network successfully connected with the router attempts to establish adjacency with other routers.
- DROther: in this state, the DROther of the network successfully connected with the router establishes adjacency with the DRs and BDRs.

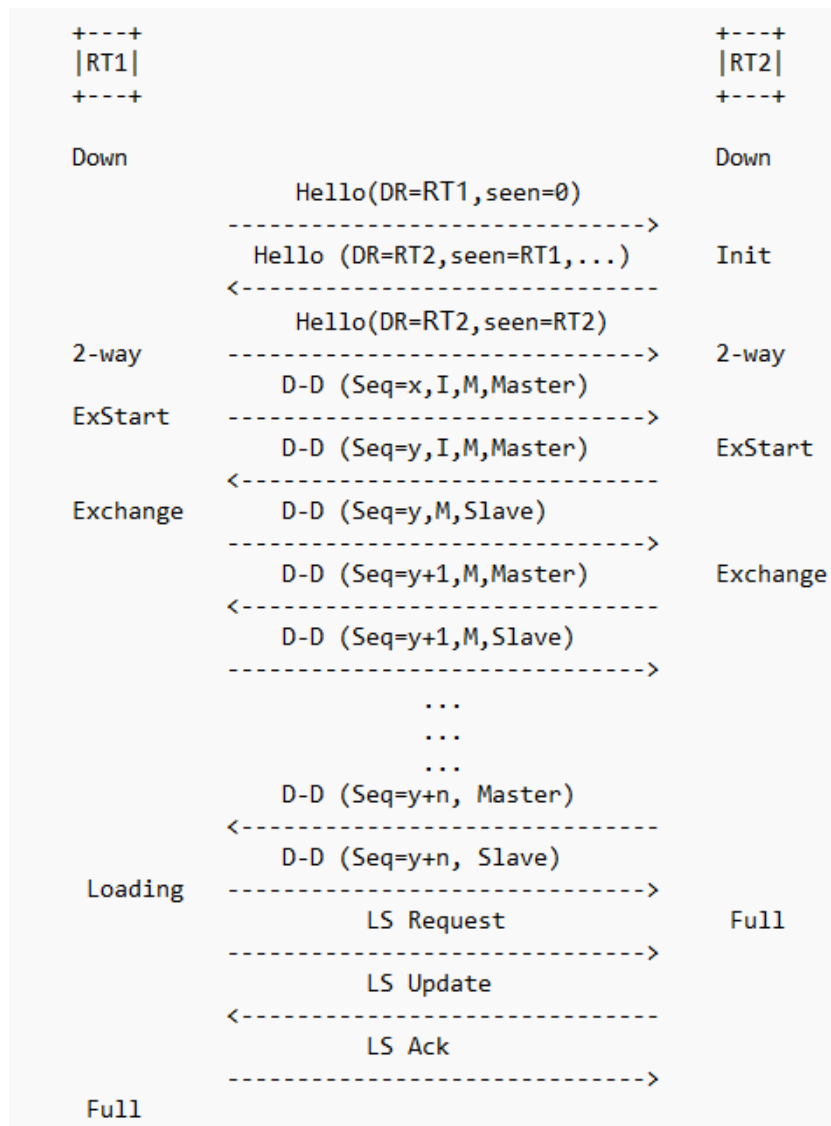
OSPFv3 neighbor and adjacency

In OSPFv3, the neighbor and adjacency are two different concepts.

- Neighbor relationship: after the OSPFv3 router is started, it will send Hello packets outward through the OSPFv3 interface. The OSPFv3 router that receives the Hello packet checks some parameters defined in the packet. If both parties agree, they will establish a neighbor relationship.
- Adjacency relationship: not all parties establishing a neighbor relationship may be able to establish an adjacency relationship, which depends on the type of the network. Only when both parties successfully exchange DD packets and exchange LSAs can they establish a true adjacency relationship.

The flow for establishing the adjacency relationship on the OSPFv3 broadcast network is as below.

Figure 3-37 Flow for establishing the adjacency relationship on the OSPFv3 broadcast network OSPFv3



Both RT1 and RT2 are connected to the broadcast network. Assume that RT2 is the DR of the network, and the Router ID of RT2 is higher than that of Router RT1.

- Step 1 Establish a neighbor relationship. RT1 activates OSPFv3 on an interface connected to a broadcast network, and will start sending Hello packets. At this point, Router A considers itself a DR router, but is unsure about its neighbor. RT2 receives this Hello packet (changing the neighbor status machine to Init status) and indicates in its next hello packet that it is the DR. RT1 received the Hello packet from RT2. This in turn causes RT1 to transit to the 2-way status and to start the adjacency process.

- Step 2 Negotiate master/slave relationship, and exchange the DD packet.

RT1 first sends a DD packet claiming to be the Master (MS=1) and specifying the sequence number Seq=x. I=1 indicates that this is the first DD packet, which does not contain a summary of LSA and is only used to negotiate the master/slave relationship. M=1 indicates that this is not the last packet.

After receiving the DD packet from RT1, RT2 changes the neighbor status machine of RT1 to Exstart and responds with a DD packet. Due to the large Router ID of RT2, RT2 considers itself as the master in the packet and redefines the sequence number Seq=y.

After receiving the packet, RT1 agrees to change RT2 as Master and changes the neighbor status machine of RT2 to Exchange. RT1 uses the sequence number Seq=y of RT2 to send a new DD packet, which officially sends the summary of LSA, confirming which LSA in the database need to be updated in this way. RT1 configures MS to 0 in the packet, indicating that it is Slave.

After receiving the packet, RT2 changes the neighbor status machine of RT1 to Exchange and sends a new DD packet to describe its LSA summary. At this time, RT2 changes the sequence number of the packet to Seq=y+1.

The above process continues, and RT1 confirms receipt of the RT2 packet by repeating the sequence number of RT2. RT2 confirms receipt of packets of Router A by adding 1 to the serial number Seq. When sending the last DD packet, write M=0 in the packet.

Step 3 Synchronize the LSDB (LSA request, LSA transmission, and LSA response).

After receiving the last DD packet, RT1 discovers that there is an LSA in RT2 database that it does not have, and changes the neighbor status machine to the Loading status.

RT2 has discovered the LSA for RT1, and RT2 already has it. There is no need to request it again. RT2 changes the neighbor status machine of RT1 to the Full status.

RT1 sends an LSR packet to RT2, requesting an update to the LSA. RT2 responds to RT1 request with an LSU packet. After receiving the LSU packet, RT1 sends an LSAck packet as acknowledgment.

The above process continues until the LSA in RT1 is completely synchronized with the LSA in RT2, and then, RT1 changes the neighbor status machine of RT2 to the Full status. After the router exchanges DD packets and updates all LSAs, the adjacency relationship is established.

Calculating OSPFv3 routes

The flow for calculating OSPFv3 routes is as below:

- Step 1 Each OSPFv3 router generates a Link State Advertisement (LSA) based on its surrounding network topology, and sends the LSA to other OSPFv3 routers on the network through update packets.
- Step 2 Each OSPFv3 router collects LSAs sent by other routers, and all LSAs form the Link State Database (LSDB), which describes the network topology of the entire AS.
- Step 3 OSPFv3 routers convert LSDB into a weighted directed graph, which is a true reflection of the entire network topology. The directed graph obtained by each OSPFv3 router is exactly the same.
- Step 4 Each OSPFv3 router uses the SPF algorithm to calculate a shortest path tree roots in itself based on a directed graph, which provides routes to each node in the AS.

OSPFv3 backbone area

After OSPFv3 divides areas, not all areas have equal relationships. One of the areas is unique and commonly referred to as the backbone area, with an area ID of 0.

The backbone area is responsible for routing between areas, and forwards routing information between non-backbone areas. OSPFv3 has the following related rules:

All non-backbone areas must be connected to the backbone area. The backbone area itself must also maintain connectivity. However, in practical applications, the previous requirements may not be met due to limitations, such as network topology; in this case, the OSPFv3 virtual connection can be configured to meet the requirements.

OSPFv3 virtual connection

A virtual connection refers to a logical connection channel established between two ABRs through a non-backbone area. It is equivalent to a point-to-point connection between two ABRs. The area that provides a non-backbone internal route for both ends of the virtual connection is called the Transit Area.

Virtual connections have the following features:

- The two ends of the virtual connection must be ABR.
- Virtual connections must be configured at both ends in order for them to take effect.
- Virtual connections can configure interface parameters, such as the interval between sending HELLO messages, just like physical interfaces.
- When two ABRs directly transmit OSPFv3 packets, the OSPFv3 router between them only serves to forward packets. Because the destination address of packets is not these routers, these packets are transparent to them and are only forwarded as regular IP packets.

OSPFv3 Stub area

The Stub area has the following features:

- The ABR in the Stub area does not advertise the external routes received from the AS. In these areas, the size of the routing table of the routes and the amount of routing information transmitted are greatly reduced.
- The Stub area is an optional configuration attribute, and not every area meets the configuration criteria. Generally, the Stub area is a non-backbone area located at the boundary of an AS with only one ABR.
- To ensure reachable routes to outside of the AS, the ABR in the Stub area generates a default route and advertises it to other non-ABR routers in the Stub area.

Notes on configuring the Stub area:

- The backbone area cannot be configured as a Stub area.
- If you want to configure an area as a Stub area, all routers in that area must have a configured Stub area.
- The ASBR cannot exist within the Stub area; in other words, routes outside the AS cannot be advertised within this area. Virtual connections cannot pass through the Stub area.

OSPFv3 NSSA area

A new type of area is added in RFC1587 NSSA Option: NSSA area. A new type of LSA is also added: NSSA LSA (also known as Type7 LSA).

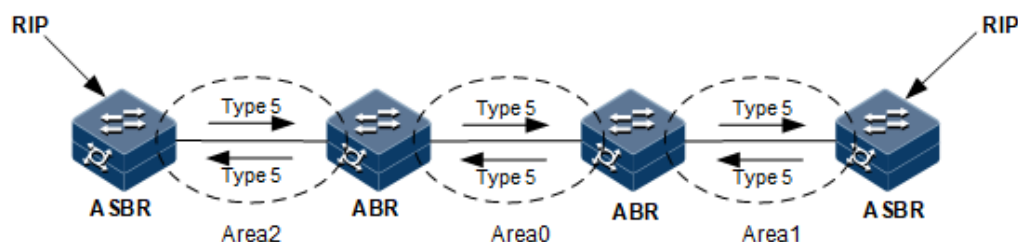
The NSSA area is actually a deformation of the Stub area, and it has many similarities with the Stub area. The difference between them is that the NSSA area can redistribute and advertise external routes from the AS to the entire OSPFv3 AS, without learning external routes from other areas of the OSPFv3 network.

The NSSA area has the following features:

- Similar to the Stub area, the NSSA area cannot be configured with virtual connections.
- Similar to the Stub area, the NSSA area also does not allow AS External LSA (namely, Type5 LSA injection is not allowed, but Type7 LSA injection is allowed). The Type7 LSA is generated by the ASBR in the NSSA area and is advertised within the NSSA region. When Type7 LSA reaches the ABR of NSSA, the ABR converts Type7 LSA into AS External LSA and advertise it to other regions.

As shown in the figure, the AS running OSPFv3 includes three areas: Area 1, Area 2, and Area 0.

Figure 3-38 OSPFv3 NSSA area



Area 1 is defined as the NSSA area. The non-OSPFv3 network connected to area 1 and area 2 runs RIP. After the RIP route received from the RIP network in Area 1 is advertised to the NSSA ASBR, the NSSA ASBR generates the Type7 LSA and advertises it within Area 1. When the Type7 LSA reaches NSSA ABR, it is converted to Type5 LSA and advertised to areas 0 and 2. On the other hand, the RIP route received by area 2 from the RIP network is generated into Type-5 LSA, which is advertised in the OSPFv3 AS through the ASBR of area 2. But because Area 1 is an NSSA area, Type-5 LSA will not reach Area 1.

OSPFv3 route aggregation

Route aggregation refers to that the ABR aggregate routing information with the same prefix together to form a route and advertise it to other areas.

After an AS is divided into different area, route aggregation can be used between areas to reduce routing information, to reduce the size of routing tables, and to improve the computational speed of routers.

OSPFv3 has two route aggregation modes:

- ABR aggregation

When the ABR sends routing information to other regions, it generates the Type3 LSA on a network segment basis. If there are some continuous network segments in the area, they can be aggregated into one network segment through the route aggregation command. In this way, the ABR sends only one aggregated LSA, and all LSAs within the specified aggregated network segment range will not be sent separately.

For example, there are three routes within areas 1, 19.1.1.0/24, 19.1.2.0/24, and 19.1.3.0/24. If route aggregation is configured on the ABR at this time to aggregate the three routes into one route 19.1.0.0/16, the ABR will generate only one aggregated LSA and advertise it to routers in other areas.

- ASBR aggregation

After route aggregation is configured, if the local device is an ASBR, it will aggregate Type5 LSA within the redistributed aggregation address range. When the NSSA area is configured, the Type7 LSA within the redistributed aggregation address range will be aggregated. If the local device is both the ASBR and ABR, it aggregates the Type5 LSA converted from the Type7 LSA.

OSPFv3 route types

OSPFv3 divides routes into four levels in order of priority: intra-area route, inter-area route, Type1 external route, and Type2 external route.

- Intra-area route (AS internal route): The routes within and between AS areas describe the network structure within the AS. By default, the protocol priority for these two types of routes is 10.
- Inter-area route (AS external route): the external route describes how to choose a route to a destination address outside of the AS. OSPFv3 divides the redistributed AS external route into two types: Type1 and Type2. By default, the protocol priority for these two types of routes is 150.
 - Type1 external route: the received IGP route (such as the static route and RIP route). Due to the high-level of trustworthiness of this type of routes, the calculated cost of the external route is the same as that of the internal route in the AS, and is comparable to the cost of OSPFv3 own route. The cost of the Type1 external route is equal to the cost from the router to the corresponding ASBR plus the cost from the ASBR to the destination address of the route.
 - Type2 external route: EGP route. Due to the low reliability of this type of routes, OSPFv3 assumes that the cost from the ASBR to the outside of the AS is much greater than the cost to the ASBR within the AS. So when the route cost is calculated, the former will be mainly considered; in other words, the cost to the Type2 external route = the cost from the ASBR to the destination address of the route. If the cost values calculated by two routes are equal, then consider the cost from this router to the corresponding ASBR.

OSPFv3 DR and BDR

On broadcast networks and NBMA networks, routing information must be transmitted between any two routers. If there are n routers on the network, establishing $n \times (n-1)/2$ adjacency relationships is required. This causes multiple transmissions due to the route change of any router, thus wasting bandwidth resources.

To address this issue, OSPFv3 defines Designated Router(DR), Backup Designated Router (BDR), and routers other than DR and BDR (DROthers).

- DR: all routers send information to the DR only, who broadcasts the network link status.
- BDR: if the DR fails due to some fault, the routers on the network must re-elect the DR and synchronize with the new DR. This takes a long time, during which the routing calculation is incorrect. To shorten this process, OSPFv3 proposes the concept of the BDR. The BDR is actually a backup of the DR, and is also elected when the DR is elected. The BDR establishes adjacency relationships with all routers in this network segment and exchanges routing information. When the DR fails, the BDR will immediately become the DR. Because there is no need for re-elections and the adjacency relationship has been established in advance, this process is very brief. Of course at this point, a new BDR needs to be re-elected, although it still takes a long time, the election will not affect the routing calculation.

- DROther: the DROthers do not establish adjacency relationships or exchange any routing information. This reduces the number of adjacency relationships between routers on the broadcast network and NBMA network.

The DR and BDR are not artificially specified, but are jointly elected by all routers in this network segment. The DR priority of a router interface determines its eligibility for DR and BDR elections. The routers with the DR priority greater than 0 in this network segment can be considered as candidates. The DR and BDR are elected as below:

- Step 1 Each router writes its elected DR into a Hello packet and sends the Hello packet to other routers in the network segment.
- Step 2 If two routers in the same network segment simultaneously declare themselves as the DR, the one with the higher DR priority wins. If the priority is equal, the one with the greater Router ID wins. If a router has a priority of 0, it will not be elected as the DR or BDR.

DR/BDR election has the following features:

- The DR is elected on the broadcasting interface or NBMA interface only. There is no need to elect the DR on the P2P or P2MP interface.
- The DR refers to the concept within a certain network segment, specifically for the interface on routers. A certain router may be a DR in terms of one interface and a BDR or DROther in terms of another interface.
- If the DR and BDR are elected, when a new router is added with the highest DR priority, it will not immediately become a DR in that network segment.
- The DR may not necessarily be the router with the highest DR priority. Similarly, the BDR may not necessarily be the router with the second highest DR priority.

3.9.2 Preparing for configurations

Scenario

After basic functions of OSPFv3 are configured, you can establish the basic OSPFv3 network.

Prerequisites

Configure IPv6 capabilities of interfaces so that the adjacent nodes can access each other at the network layer.

3.9.3 Default configurations

Default configurations of OSPFv3 are as below.

Function	Default value
OSPFv3	Disable
Interval for sending Hello packets	10s
Neighbor invalid time	40s
Referential bandwidth for calculating the interface cost	100Mbit/s

3.9.4 Configuring basic functions of OSPFv3

Configure basic functions of OSPFv3 for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)# ospfv3 process-id [vpn-instance name]	Start the OSPFv3 process, and enter the OSPFv3 view. The default process-id is 1. The vpn-instance is the VPN instance. If the vpn-instance is specified, the OSPFv3 process belongs to the VPN instance; otherwise, it belongs to the public network instance.
3	Raisecom(config-ospfv3-1)#router-id ipv4-address	Configure the ID of the OSPFv3 process. Ensure that the router ID is globally unique. If no router ID is configured, the system chooses one from IP addresses of the current interface as the router ID.
4	Raisecom(config)# interface interface-type interface- number	Enter interface configuration mode. Take the VLAN interface for example.
5	Raisecom (config-vlanif-1)# ospfv3 process-id area area- id	Enable OSPFv3 on the interface and create OSPFv3 areas. Configure the instance run by the interface and OSPFv3 area.
6	Raisecom (config-vlanif-1)# ospfv3 if-type { broadcast p2p }	(Optional) configure the network type of the interface.
7	Raisecom(config)# ospfv3 process-id [vpn-instance name]	Enter the OSPFv3 view.
8	Raisecom(config-ospfv3-1)# maximum load-balancing { load-balancing-number default }	(Optional) configure the maximum number of OSPFv3 equivalent routes.
9	Raisecom(config-ospfv3-1)# preference preference-value { route-policy name }	Configure the priorities of OSPFv3 intra-domain routes and inter-domain routes.
10	Raisecom(config-ospfv3-1)# preference ase preference- value [route-policy name]	Configure the priority of OSPFv3 external routes.

3.9.5 Configuring the OSPFv3 Stub area

Configure the OSPFv3 Stub area for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)# ospfv3 process-id { vpn-instance name }	Enter the OSPFv3 view.
3	Raisecom(config-ospfv3-1)# area area-id stub { no-summary-lsa }	Configure the area as the Stub area. The area cannot be the backbone area. No-summary: prohibit the ABR from sending Summary LSA to the Stub area. This parameter can take effect in the area only when the stub command is configured on the ABR.

3.9.6 Configuring the OSPFv3 NSSA area

Configure the OSPFv3 NSSA area for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)# ospfv3 process-id { vpn-instance name }	Enter the OSPFv3 view.
3	Raisecom(config-ospfv3-1)# area area-id nssa { no-summary-lsa }	Configure the area as the NSSA area. The area cannot be the backbone area. No-summary: prohibit the ABR from sending Summary LSA to the NSSA area.
4	Raisecom(config-ospfv3-1)# area area-id nssa translator { always candidate }	In the candidate status, the NSSA area automatically selects an ABR as the converter according to the rules, converting Type 7 LSA into Type 5 LSA. By configuring a certain ABR with the translator always parameter, you can specify it as a translator.

3.9.7 Configure OSPFv3 to redistribute external routes

Configure OSPFv3 to redistribute external routes for the device as below.

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

Step	Command	Description
2	Raisecom(config)# ospfv3 process-id { vpn-instance name }	Enter the OSPFv3 view.
3	Raisecom(config-ospfv3-1)# import-route { connect static rip bgp isis ospf } { cost { cost inherit } route-policy name }	Redistribute routing information about other protocols. The cost parameter is the default metric for OSPFv3 to redistribute external routes. The inherit parameter indicates that the cost of the redistributed route is the cost value of the route. If no cost is specified, the default cost value configured by the default route-attribute command is used. The route-policy parameter is used to bind the routing policy and to filter routes to be redistributed.

3.9.8 Configuring OSPFv3 route aggregation

Configure OSPFv3 route aggregation for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)# ospfv3 process- id [vpn-instance NAME]	Enter the OSPFv3 view.
3	Raisecom(config-ospfv3-1)# area area-id abr-summary dst- address/dst-maskLen { advertise no-advertise } [cost { cost- value inherit-minimum }]	Configure ABR route aggregation of OSPFv3.
4	Raisecom(config-ospfv3-1)# area area-id nssa summary dst- address/dst-maskLen { advertise no-advertise } [cost { cost- value inherit-minimum }]	Configure route aggregation for conversion from type-7 LAS into type-5 LAS on the local router.
5	Raisecom(config-ospfv3-1)# asbr- summary dst-address/dst-maskLen	Configure ASBR route aggregation of OSPFv3.
6	Raisecom(config-ospfv3-1)# asbr- summary { connect static rip bgp isis ospf } dst- address/dst-maskLen [advertise { enable disable } translate { enable disable } cost { cost default } type { cost- type default }]*	Configure ASBR route aggregation of OSPFv3 for routes redistributed from a protocol.

3.9.9 Configuring OSPFv3 virtual connection

Configure OSPFv3 virtual connection for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)# ospfv3 process-id { vpn-instance name }	Enter the OSPFv3 view.
3	Raisecom(config-ospfv3-1)# area area-id virtual-link ipv4-address	Create a virtual connection, and configure it.
4	Raisecom(config-ospfv3-1)# area area-id virtual-link ipv4-address hello-interval value	(Optional) configure the interval for sending Hello packets of the virtual connection.
5	Raisecom(config-ospfv3-1)# area area-id virtual-link ipv4-address dead-interval value	(Optional) configure the neighbor invalid time of the virtual connection.
6	Raisecom(config-ospfv3-1)# area area-id virtual-link ipv4-address retransmit-interval value	(Optional) configure the interval for retransmitting LSA of the virtual connection.
7	Raisecom(config-ospfv3-1)# area area-id virtual-link neighbor-address transmit-delay value	(Optional) configure the delay for transmitting LAS of the virtual connection.

3.9.10 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom#show ospfv3 interface	Show the OSPFv3 interface.
2	Raisecom# show ospfv3 process process-id	Show the OSPFv3 instance.
3	Raisecom# show ospfv3 area	Show the OSPFv3 area.
4	Raisecom# show ospfv3 neighbor	Show the OSPFv3 neighbor. After the peer is configured accordingly, neighbor relation can be established.
5	Raisecom# show ospfv3 route	Show the OSPFv3 routing table.
6	Raisecom# show ospfv3 database	Show the OSPFv3 database.
7	Raisecom# show ospfv3 import-route	Show routes redistributed from OSPFv3.

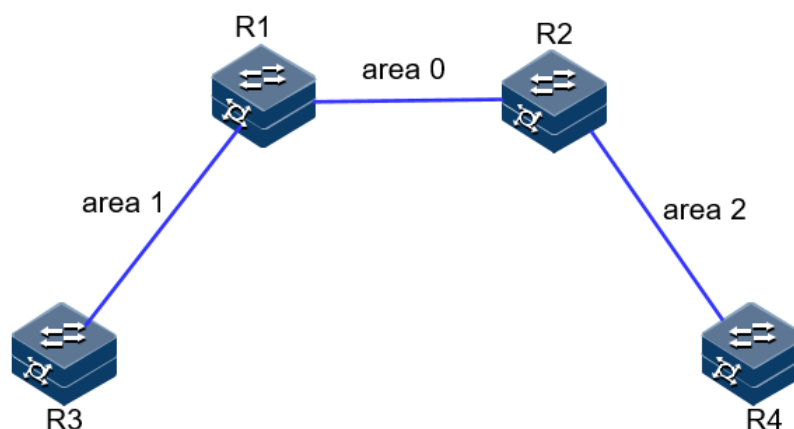
Step	Command	Description
8	Raisecom# show ospfv3 virtual-link	Show information about the OSPFv3 virtual connection.
9	Raisecom# show ospfv3 interface <i>interface-type interface-number</i>	Show detailed information about the interface.
10	Raisecom# show ospfv3 area area-id area-id	Show detailed information about the area.
11	Raisecom# show ospfv3 information	Show global information about OSPFv3.

3.9.11 Example for configuring basic functions of OSPFv3

Networking requirements

As shown below, all routers run OSPFv3 and divide the entire AS into three areas, where Router 1 and Router 2 are ABRs for forwarding routes between areas. After configuration is complete, each router should learn the routes to all network segments within the AS.

Figure 3-39 Networking with basic functions of OSPFv3



Configuration steps

Step 1 Configure IPv6 addresses and IPv6 capabilities of interfaces.

- Establish neighboring interfaces between R1 and R2 by using VLAN 12.
- Establish neighboring interfaces between R1 and R3 by using VLAN 13.
- Establish neighboring interfaces between R2 and R4 by using VLAN 24.

Step 2 Configure OSPFv3.

R1:

```
Raisecom-R1#configure
Raisecom-R1(config)#ospfv3 1
Raisecom-R1(config-ospfv3-1)#router-id 1.1.1.1
Raisecom-R1(config-ospfv3-1)#exit
Raisecom-R1(config)#interface vlan 13
Raisecom-R1(config-vlanif-13)#ospfv3 1 area 1
Raisecom-R1(config-vlanif-13)#exit
Raisecom-R1(config)#interface vlan 12
Raisecom-R1(config-vlanif-12)#ospfv3 1 area 0
Raisecom-R1(config-vlanif-12)#exit
```

R2:

```
Raisecom-R2#configure
Raisecom-R2(config)#ospfv3 1
Raisecom-R2(config-ospfv3-1)#router-id 2.2.2.2
Raisecom-R2(config-ospfv3-1)#exit
Raisecom-R2(config)#interface vlan 12
Raisecom-R2(config-vlanif-12)#ospfv3 1 area 0
Raisecom-R2(config-vlanif-12)#exit
Raisecom-R2(config)#interface vlan 24
Raisecom-R2(config-vlanif-24)#ospfv3 1 area 2
Raisecom-R2(config-vlanif-24)#exit
```

R3:

```
Raisecom-R3#configure
Raisecom-R3(config)#ospfv3 1
Raisecom-R3(config-ospfv3-1)#router-id 3.3.3.3
Raisecom-R3(config-ospfv3-1)#exit
Raisecom-R3(config)#interface vlan 13
Raisecom-R3(config-vlanif-13)#ospfv3 1 area 1
Raisecom-R3(config-vlanif-13)#exit
```

R4:

```
Raisecom-R4#configure
Raisecom-R4(config)#ospfv3 1
Raisecom-R4(config-ospfv3-1)#router-id 4.4.4.4
Raisecom-R4(config-ospfv3-1)#exit
Raisecom-R4(config)#interface vlan 24
Raisecom-R4(config-vlanif-24)#ospfv3 1 area 2
Raisecom-R4(config-vlanif-24)#exit
```

Step 3 Verify configuration results.

R1:

OspfV3 Process 1						
NeighborId	Priority	State	Interface	Instance	Aging	
UpTime	IpAddress					

2.2.2.2	1	Full	vlan-12	0	36	1:20:40
fe80::f2f1:f2ff:fef3:201						
3.3.3.3	1	Full	vlan-13	0	32	1:13:54
fe80::f2f1:f2ff:fef3:301						

Down:0	Attempt:0	Init:0	TwoWay:0	ExchangeStart:0		
Exchange:0						
Loading:0	Full:2					

R2:

```

OspfV3 Process 1
NeighborId      Priority  State      Interface      Instance  Aging
UpTime    IpAddress
-----
1.1.1.1      1      Full      vlan-12      0      38      1:27:13
fe80::f2f1:f2ff:fe3:101
4.4.4.4      1      Full      vlan-24      0      28      0:10:27
fe80::f2f1:f2ff:fe3:101
-----
Down:0      Attempt:0      Init:0      TwoWay:0      ExchangeStart:0
Exchange:0
Loading:0      Full:2

```

Use the **show ospfv3 database** command to show the database.

Router Link State (Area 0.0.0.0)					
LinkId	ADV Router	Age	Seq#	Checksum	Len
0.0.0.0	1.1.1.1	77	0x80000002	0x1660	40

```

0.0.0.0          2.2.2.2          78      0x80000009  0xe981      40

      Network Link State (Area 0.0.0.0)
LinkId          ADV Router      Age      Seq#          CheckSum      Len
64.0.0.13       2.2.2.2          78      0x80000001  0xa423      32

      Inter Area Prefix Link State (Area 0.0.0.0)
LinkId          ADV Router      Age      Seq#          CheckSum      Len
Prefix
0.0.0.2         1.1.1.1          118     0x80000001  0x4c8d      36
13::/64
0.0.0.2         2.2.2.2          409     0x80000004  0xf4cc      36
24::/64

      Intra Area Prefix Link State (Area 0.0.0.0)
LinkId          ADV Router      Age      Seq#          CheckSum      Len
0.0.3.232       2.2.2.2          78      0x80000001  0x83e6      44

      Link(Type-8) State(interface vlan-12 Area 0.0.0.0)
LinkId          ADV Router      Age      Seq#          CheckSum      Len
64.0.0.13       1.1.1.1          118     0x80000001  0x4d41      76
64.0.0.13       2.2.2.2          448     0x80000004  0x780d      76

      Router Link State (Area 0.0.0.1)
LinkId          ADV Router      Age      Seq#          CheckSum      Len
0.0.0.0         1.1.1.1          119     0x80000005  0x82ea      40
0.0.0.0         3.3.3.3          120     0x80000009  0x3b27      40

      Network Link State (Area 0.0.0.1)
LinkId          ADV Router      Age      Seq#          CheckSum      Len
64.0.0.14       3.3.3.3          120     0x80000001  0x9e20      32

      Inter Area Prefix Link State (Area 0.0.0.1)
LinkId          ADV Router      Age      Seq#          CheckSum      Len
Prefix
0.0.0.2         1.1.1.1          118     0x80000001  0x409a      36
12::/64
0.0.0.3         1.1.1.1          72      0x80000001  0x15b1      36
24::/64

      Intra Area Prefix Link State (Area 0.0.0.1)
LinkId          ADV Router      Age      Seq#          CheckSum      Len
0.0.3.232       3.3.3.3          120     0x80000001  0xb5aa      44

      Link(Type-8) State(interface vlan-13 Area 0.0.0.1)
LinkId          ADV Router      Age      Seq#          CheckSum      Len
64.0.0.14       1.1.1.1          122     0x80000001  0x8ffb      76
64.0.0.14       3.3.3.3          36      0x80000004  0xeb90      76

```

Use the **show ospfv3 route** command to show the routing table.

```

Raisecom-R1(config)#show ospfv3 route
Ospfv3 Process 1

```

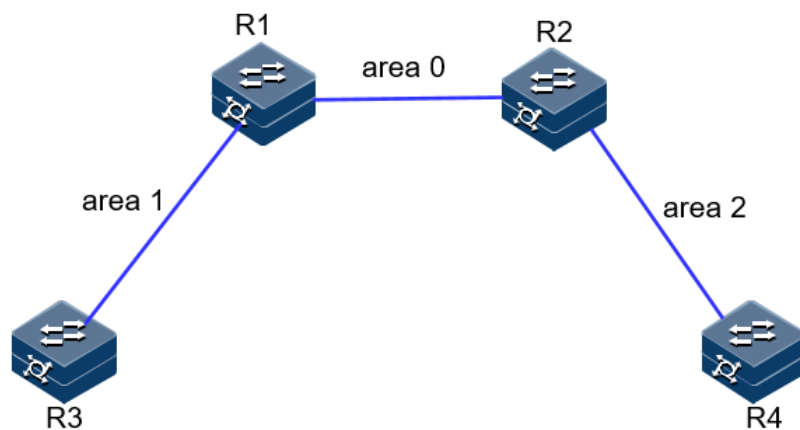
RoutType	Prefix	AreaId	PathType	Cost	Cost2
NextHopIf	NextHopNbr	Backu			
pNextHop					
ABR	2.2.2.2/32	0.0.0.0	INTRA	1	0
vlan-12	fe80::f2f1:f2ff:fef3:201	::			
PREFIX	12::/64	0.0.0.0	INTRA	1	0
vlan-12	12::	::			
PREFIX	13::/64	0.0.0.1	INTRA	1	0
vlan-13	13::	::			
PREFIX	24::/64	0.0.0.0	INTER	2	0
vlan-12	fe80::f2f1:f2ff:fef3:201	::			
Route:					
Prefix(Intra	Inter	External)	ABR	ASBR	External
3	2	0	0	1	0
Path:					
Prefix(Intra	Inter	External)	ABR	ASBR	External
3	2	0	0	1	0

3.9.12 Example for configuring the OSPFv3 Stub area

Networking requirements

As shown below, all routers run OSPFv3 and divide the entire AS into three areas, where Router 1 and Router 2 are ABRs for forwarding routes between areas.

Figure 3-40 OSPFv3 Stub area networking



Configuration steps

Step 1 Configure basic functions of OSPFv3.

Step 2 Configure area 1 as the stub area.

R1:

```
Raisecom-R1#configure
Raisecom-R1(config)#ospfv3 1
Raisecom-R1(config-ospfv3-1)#area 1 stub
```

R3:

```
Raisecom-R3#configure
Raisecom-R3(config)#ospfv3 1
Raisecom-R3(config-ospfv3-1)#area 1 stub
```

Step 3 Configure R4 to redistribute type-5 LSA of 100.1.1.1.

```
Raisecom-R4(config)#ipv6 route-static 100::1 128 1::3
Raisecom-R4(config)#ospfv3 1
Raisecom-R4(config-ospfv3-1)#import-route static
```

Step 4 Verify configuration results.

When the R3 area is a common area, the routing table contains the external routes for the AS.

```
Raisecom-R3(config)#show ospfv3 route
Ospfv3 Process 1
RoutType Prefix AreaId PathType Cost Cost2
NextHopIf NextHopNbr Backu
pNextHop
ABR 1.1.1.1/32 0.0.0.1 INTRA 1 0
vlan-13 fe80::f2f1:f2ff:fe3:101 ::
ASBR 4.4.4.4/32 0.0.0.1 INTER 3 0
vlan-13 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 12::/64 0.0.0.1 INTER 2 0
vlan-13 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 13::/64 0.0.0.1 INTRA 1 0
vlan-13 13:: ::
PREFIX 24::/64 0.0.0.1 INTER 3 0
vlan-13 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 100::1/128 n/a EXTERNAL_2 3 1
vlan-13 fe80::f2f1:f2ff:fe3:101 ::
Route:
Prefix(Intra Inter External)ABR ASBR External
4 1 0 1 1 1
Path:
Prefix(Intra Inter External)ABR ASBR External
4 1 0 1 1 1
```

When the R3 area is configured as the stub area, external routes for the AS disappear, and instead a default route to the external part of the area appears.

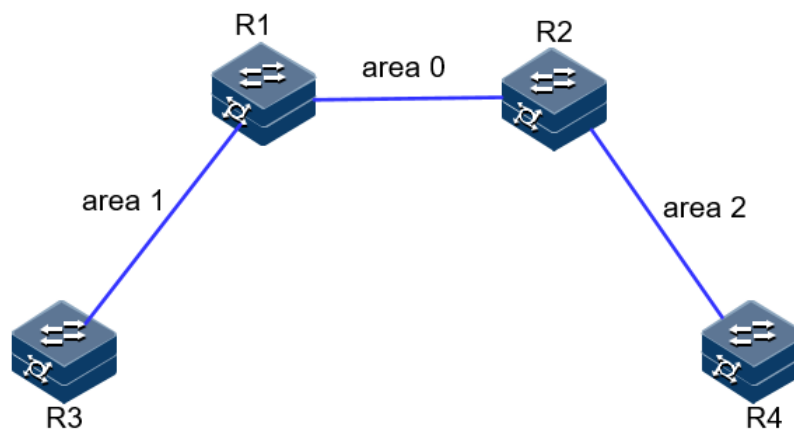
```
Raisecom-R3(config)#show ospfv3 route
Ospfv3 Process 1
RoutType Prefix AreaId PathType Cost Cost2
NextHopIf NextHopNbr Backu
pNextHop
ABR 1.1.1.1/32 0.0.0.1 INTRA 1 0
vlan-13 fe80::f2f1:f2ff:fef3:101 ::
PREFIX ::/0 0.0.0.1 INTER 2 0
vlan-13 fe80::f2f1:f2ff:fef3:101 ::
PREFIX 12::/64 0.0.0.1 INTER 2 0
vlan-13 fe80::f2f1:f2ff:fef3:101 ::
PREFIX 13::/64 0.0.0.1 INTRA 1 0
vlan-13 13:: ::
PREFIX 24::/64 0.0.0.1 INTER 3 0
vlan-13 fe80::f2f1:f2ff:fef3:101 ::
Route:
Prefix(Intra Inter External)ABR ASBR External
4 1 0 0 1 0
Path:
Prefix(Intra Inter External)ABR ASBR External
4 1 0 0 1 0
```

3.9.13 Example for configuring the OSPFv3 NSSA area

Networking requirements

As shown below, all routers run OSPFv3 and divide the entire AS into three areas, where Router 1 and Router 2 are ABRs for forwarding routes between areas.

Figure 3-41 OSPFv3 NSSA area networking



Configuration steps

Step 1 Configure basic functions of OSPFv3.

Step 2 Configure area 1 as the NSSA area.

R1:

```
Raisecom-R1#configure
Raisecom-R1(config)#ospfv3 1
Raisecom-R1(config-ospfv3-1)#area 1 nssa
```

R3:

```
Raisecom-R3#configure
Raisecom-R3(config)#ospfv3 1
Raisecom-R3(config-ospfv3-1)#area 1 nssa
```

Step 3 Configure R4 to redistribute type-5 LSA of 100.1.1.1.

```
Raisecom-R4(config)#ipv6 route-static 100::1 128 1::3
Raisecom-R4(config)#ospfv3 1
Raisecom-R4(config-ospfv3-1)#import-route static
```

Step 4 Verify configuration results.

Compared with the database in the common area, the database of the NSSA area has an extra type NSSA LSA, and there is no external LSA of 100::1 on the R3.

```
Raisecom-R3(config)#show ospfv3 database
Database of OSPFv3 Process 1
```

```

Router Link State (Area 0.0.0.1)
LinkId      ADV Router  Age      Seq#       CheckSum   Len
0.0.0.0      1.1.1.1     5        0x80000004 0xa64      40
0.0.0.0      3.3.3.3     4        0x80000002 0xc8a2     40

Network Link State (Area 0.0.0.1)
LinkId      ADV Router  Age      Seq#       CheckSum   Len
64.0.0.14   1.1.1.1     5        0x80000001 0x1fa1     32

Inter Area Prefix Link State (Area 0.0.0.1)
LinkId      ADV Router  Age      Seq#       CheckSum   Len
Prefix
0.0.0.8     1.1.1.1     195      0x80000001 0x4d0      36
12::/64
```

```

0.0.0.9          1.1.1.1          195      0x80000001  0xd8e7      36
24::/64

```

Intra Area Prefix Link State (Area 0.0.0.1)

```

LinkId          ADV Router      Age      Seq#          CheckSum      Len
0.0.3.232       1.1.1.1          5        0x80000001  0x8de2      44

```

Nssa Link State (Area 0.0.0.1)

```

LinkId          ADV Router      Age      Seq#          CheckSum      Len
Prefix
0.0.0.1         1.1.1.1          195      0x80000001  0x4de7
28      ::/0

```

Link(Type-8) State(interface vlan-13 Area 0.0.0.1)

```

LinkId          ADV Router      Age      Seq#          CheckSum      Len
64.0.0.14       1.1.1.1          195      0x80000001  0xb3d1      76
64.0.0.14       3.3.3.3          11       0x80000001  0x1663      76

```

Step 5 Configure R3 to redistribute the static route of 200::1.

```

Raisecom-R3(config)#ipv6 route-static 200::1 128 13::5
Raisecom-R3(config)#ospfv3 1
Raisecom-R3(config-ospfv3-1)#import-route static

```

Step 6 Verify configuration results.

There are type-5 LSA and NSSA LSA of 200::1 on R3.

```

Raisecom-R3(config)#show ospfv3 database
Database of OSPFV3 Process 1

```

Router Link State (Area 0.0.0.1)

```

LinkId          ADV Router      Age      Seq#          CheckSum      Len
0.0.0.0         1.1.1.1          106      0x80000004  0xa64       40
0.0.0.0         3.3.3.3          30       0x80000003  0xcc9b      40

```

Network Link State (Area 0.0.0.1)

```

LinkId          ADV Router      Age      Seq#          CheckSum      Len
64.0.0.14       1.1.1.1          106      0x80000001  0x1fa1      32

```

Inter Area Prefix Link State (Area 0.0.0.1)

```

LinkId          ADV Router      Age      Seq#          CheckSum      Len
Prefix
0.0.0.8         1.1.1.1          296      0x80000001  0x4d0       36
12::/64
0.0.0.9         1.1.1.1          296      0x80000001  0xd8e7      36
24::/64

```

Intra Area Prefix Link State (Area 0.0.0.1)

```

LinkId          ADV Router      Age      Seq#          CheckSum      Len

```

```

0.0.3.232      1.1.1.1      106      0x80000001    0x8de2      44

      Nssa Link State (Area 0.0.0.1)
LinkId      ADV Router      Age      Seq#      CheckSum      Len
Prefix
0.0.0.1      1.1.1.1      296      0x80000001    0x4de7
28    ::/0
0.0.0.2      3.3.3.3      28       0x80000001    0xe6ad      44
200::1/128

      Link(Type-8) State(interface vlan-13 Area 0.0.0.1)
LinkId      ADV Router      Age      Seq#      CheckSum      Len
64.0.0.14    1.1.1.1      296      0x80000001    0xb3d1      76
64.0.0.14    3.3.3.3      112      0x80000001    0x1663      76

      AS External Link State
LinkId      ADV Router      Age      Seq#      CheckSum      Len
Prefix
0.0.0.2      3.3.3.3      28       0x80000001    0x2155      44
200::1/128

```

Check the routing table and database of R4. There are the 200::1 route and LSA.

Raisecom-R4(config)#**show ospfv3 database**
Database of OSPFV3 Process 1

```

      Router Link State (Area 0.0.0.2)
LinkId      ADV Router      Age      Seq#      CheckSum      Len
0.0.0.0      2.2.2.2      1222     0x80000005    0x73e3      40
0.0.0.0      4.4.4.4      1187     0x80000004    0x3c13      40

      Network Link State (Area 0.0.0.2)
LinkId      ADV Router      Age      Seq#      CheckSum      Len
64.0.0.25    2.2.2.2      1221     0x80000002    0xc0ed      32

      Inter Area Prefix Link State (Area 0.0.0.2)
LinkId      ADV Router      Age      Seq#      CheckSum      Len
Prefix
0.0.0.4      2.2.2.2      189      0x80000004    0x8c9       36
12::/64
0.0.0.6      2.2.2.2      154      0x80000005    0x4c8       36
13::/64

      Inter Area Router Link State (Area 0.0.0.2)
LinkId      ADV Router      Age      Seq#      CheckSum      Len
Prefix
0.0.0.1      2.2.2.2      337      0x80000001    0xa0f       32
1.1.1.1
0.0.0.2      2.2.2.2      69       0x80000001    0x62ae      32
3.3.3.3

      Intra Area Prefix Link State (Area 0.0.0.2)
LinkId      ADV Router      Age      Seq#      CheckSum      Len

```



```
0.0.3.232      2.2.2.2      1221      0x80000002      0x63e7      44
```

```
Link(Type-8) State(interface vlan-24 Area 0.0.0.2)
```

LinkId	ADV Router	Age	Seq#	CheckSum	Len
64.0.0.25	2.2.2.2	430	0x80000005	0x5bf8	76
64.0.0.25	4.4.4.4	1260	0x80000002	0xd57b	76

```
AS External Link State
```

LinkId	ADV Router	Age	Seq#	CheckSum	Len
Prefix 0.0.0.2	1.1.1.1	68	0x80000001	0x5d21	44
200::1/128					
0.0.0.2	4.4.4.4	1185	0x80000001	0xf77b	44
100::1/128					

```
Raisecom-R4(config)#show ospfv3 route
```

```
Ospfv3 Process 1
RoutType Prefix AreaId PathType Cost Cost2
NextHopIf NextHopNbr Backu
pNextHop
ABR 2.2.2.2/32 0.0.0.2 INTRA 1 0
vlan-24 fe80::f2f1:f2ff:fe3:201 ::
ASBR 1.1.1.1/32 0.0.0.2 INTER 2 0
vlan-24 fe80::f2f1:f2ff:fe3:201 ::
ASBR 3.3.3.3/32 0.0.0.2 INTER 3 0
vlan-24 fe80::f2f1:f2ff:fe3:201 ::
PREFIX 12::/64 0.0.0.2 INTER 2 0
vlan-24 fe80::f2f1:f2ff:fe3:201 ::
PREFIX 13::/64 0.0.0.2 INTER 3 0
vlan-24 fe80::f2f1:f2ff:fe3:201 ::
PREFIX 24::/64 0.0.0.2 INTRA 1 0
vlan-24 24:: ::
PREFIX 200::1/128 n/a EXTERNAL_2 2 1
vlan-24 fe80::f2f1:f2ff:fe3:201 ::
Route:
Prefix(Intra Inter External)ABR ASBR External
4 1 0 1 1 2
Path:
Prefix(Intra Inter External)ABR ASBR External
4 1 0 1 1 2
```

3.9.14 Configuring OSPFv3 to redistribute external routes

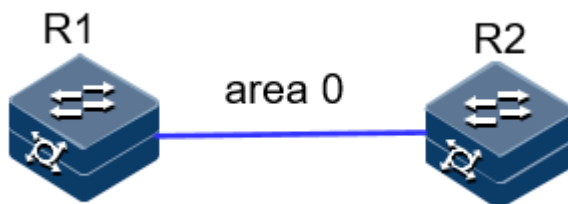
Networking requirements

As shown below, both routers are running OSPFv3 and are configured as region 0. Assume that R1 needs to redistribute external routes to OSPFv3, R1 has the static route 30::1/128 and local route 40::1/128, but external routes have the following requirements:

- Accept all direct routing and use default configuration.
- Receive all static routes and configure the cost of routes to 2000.

After configuration is complete, each device should learn the routing to all network segments within the AS.

Figure 3-42 Networking with OSPFv3 to redistribute external routes



Configuration steps

Step 1 Configure IP addresses of interfaces.

- IP address of one interface on R1: 1.1.1.1/24
- IP address of one interface on R2: 1.1.1.2/24

Step 2 Configure OSPFv3.

R1:

```
Raisecom-R1#configure
Raisecom-R1(config)#ospfv3 1
Raisecom-R1(config-ospfv3-1)#router-id 1.1.1.1
Raisecom-R1(config-ospfv3-1)#exit
Raisecom-R1(config)#interface vlan 12
Raisecom-R1(config-vlanif-12)#ospfv3 1 area 0
Raisecom-R1(config-vlanif-12)#exit
```

R2:

```
Raisecom-R2#configure
Raisecom-R2(config)#ospfv3 1
Raisecom-R2(config-ospfv3-1)#router-id 2.2.2.2
Raisecom-R2(config-ospfv3-1)#exit
Raisecom-R2(config)#interface vlan 12
Raisecom-R2(config-vlanif-12)#ospfv3 1 area 0
```

Step 3 Configure redistribution.

```
Raisecom-R1#configure
Raisecom-R1(config)#ospfv3 1
Raisecom-R1(config-ospfv3-1)#import-route connect
Raisecom-R1(config-ospfv3-1)#import-route static cost 2000
```

Step 4 Check configuration results.

```
Raisecom-R1(config)#show ospfv3 import-route
Import Route of OSPF(1)
dest          cost    proto  pid
1::/64        1       connect 0
30::1/128     60      static  0
40::1/128     1       connect 0
Raisecom-R1(config)#show ospfv3 database ls-type external
Database of OSPFv3 Process 1
```

AS External Link State					
LinkId	ADV Router	Age	Seq#	CheckSum	Len
Prefix					
0.0.0.2	1.1.1.1	35	0x80000001	0x8bed	44
30::1/128					
0.0.0.3	1.1.1.1	32	0x80000001	0x5d6a	36
1::/64					
0.0.0.4	1.1.1.1	32	0x80000001	0x3608	44
40::1/128					

Use the following command to show the routing table on R2.

```
Raisecom-R2(config)#show ospfv3 route
Ospfv3 Process 1
RoutType Prefix          AreaId      PathType    Cost    Cost2
NextHopIf NextHopNbr              Backu
pNextHop
ASBR 1.1.1.1/32             0.0.0.0     INTRA       1        0
vlan-12 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 1::/64                n/a         EXTERNAL_2  1        1
vlan-12 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 12::/64              0.0.0.0     INTRA       1        0
vlan-12 12::              ::
PREFIX 30::1/128          n/a         EXTERNAL_2  1       2000
vlan-12 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 40::1/128          n/a         EXTERNAL_2  1        1
vlan-12 fe80::f2f1:f2ff:fe3:101 ::
Route:
Prefix(Intra Inter External)ABR ASBR External
4 1 0 3 0 1
Path:
Prefix(Intra Inter External)ABR ASBR External
4 1 0 3 0 1
```

3.9.15 Example for configuring OSPFv3 route aggregation

Networking requirements

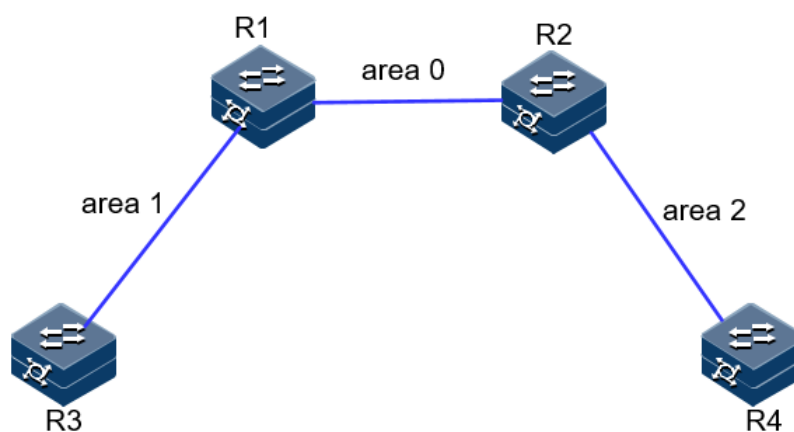
As shown below, the network requirement are as below: there are intra-area routes of 10::1/128, 10::2/128, 20::1:1/112, and 20::2:1/112 in area 2; aggregate 10::1/128 and 10::2/128 into 10::0/112 for advertisement; 20::1:1/112 and 20::2:1/112 will not be redistributed into other regions.

R4 has external routes of 30::1/128 and 30::2/128, which are required to be advertised to other regions.

The device capability in area 1 is too poor to receive a large number of external routes, but R3 has external routes of 200::1/128 and 200::2/128, which are required to be advertised to other regions.

According to the above requirements, configure aggregation and filtering entries for area 2, and configure NSSA attributes for area 1.

Figure 3-43 OSPFv3 route aggregation networking



Configuration steps

Step 1 Configure basic functions of OSPFv3.

Step 2 Configure area 1 as the NSSA area.

R1:

```
Raisecom-R1#configure
Raisecom-R1(config)#ospfv3 1
Raisecom-R1(config-ospfv3-1)#area 1 nssa
```

R3:

```
Raisecom-R3#configure
```

```
Raisecom-R3(config)#ospfv3 1
Raisecom-R3(config-ospfv3-1)#area 1 nssa
```

Step 3 Show the route entries and database before route aggregation.

```
Raisecom-R2(config)#show ospfv3 route
Ospfv3 Process 1
RoutType Prefix AreaId PathType Cost Cost2
NextHopIf NextHopNbr Backu
pNextHop
ABR 1.1.1.1/32 0.0.0.0 INTRA 1 0
vlan-12 fe80::f2f1:f2ff:fe3:101 ::
ASBR 1.1.1.1/32 0.0.0.0 INTRA 1 0
vlan-12 fe80::f2f1:f2ff:fe3:101 ::
ASBR 3.3.3.3/32 0.0.0.0 INTER 2 0
vlan-12 fe80::f2f1:f2ff:fe3:101 ::
ASBR 4.4.4.4/32 0.0.0.2 INTRA 1 0
vlan-24 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 10::1/128 0.0.0.2 INTRA 2 0
vlan-24 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 10::2/128 0.0.0.2 INTRA 2 0
vlan-24 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 12::/64 0.0.0.0 INTRA 1 0
vlan-12 12:: ::
PREFIX 13::/64 0.0.0.0 INTER 2 0
vlan-12 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 20::1:0/112 0.0.0.2 INTRA 2 0
vlan-24 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 20::2:0/112 0.0.0.2 INTRA 2 0
vlan-24 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 24::/64 0.0.0.2 INTRA 1 0
vlan-24 24:: ::
PREFIX 30::1/128 n/a EXTERNAL_2 1 1
vlan-24 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 30::2/128 n/a EXTERNAL_2 1 1
vlan-24 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 200::1/128 n/a EXTERNAL_2 1 1
vlan-12 fe80::f2f1:f2ff:fe3:101 ::
PREFIX 200::2/128 n/a EXTERNAL_2 1 1
vlan-12 fe80::f2f1:f2ff:fe3:101 ::

Route:
Prefix(Intra Inter External)ABR ASBR External
11 6 0 4 1 3

Path:
Prefix(Intra Inter External)ABR ASBR External
11 6 0 4 1 3
```

Step 4 Configure ABR aggregation on R2. Aggregate 10::1/128 and 10::2/128 into 10::0/112 for advertisement; 20::1:1/112 and 20::2:1/112 will not be advertised after aggregation.

```
Raisecom-R2#configure
Raisecom-R2(config)#ospfv3 1
Raisecom-R2(config-ospfv3-1)#area 2 abr-summary 10::0/112 advertise
Raisecom-R2(config-ospfv3-1)#area 2 abr-summary 20::0/98 not-advertise
```

Step 5 Verify configuration results.

The routing table of R1 contains the 10::/112 route only, without 10::1/128, 10::2/128, 20::1/112, and 20::2/112.

```
Raisecom-R1(config)#show ospfv3 route
Ospfv3 Process 1
RoutType Prefix AreaId PathType Cost Cost2
NextHopIf NextHopNbr Backu
pNextHop
ABR 2.2.2.2/32 0.0.0.0 INTRA 1 0
vlan-12 fe80::f2f1:f2ff:fef3:201 ::
ASBR 4.4.4.4/32 0.0.0.0 INTER 2 0
vlan-12 fe80::f2f1:f2ff:fef3:201 ::
ASBR 3.3.3.3/32 0.0.0.1 INTRA 1 0
vlan-13 fe80::f2f1:f2ff:fef3:301 ::
PREFIX 10::/112 0.0.0.0 INTER 3 0
vlan-12 fe80::f2f1:f2ff:fef3:201 ::
PREFIX 12::/64 0.0.0.0 INTRA 1 0
vlan-12 12:: ::
PREFIX 13::/64 0.0.0.1 INTRA 1 0
vlan-13 13:: ::
PREFIX 24::/64 0.0.0.0 INTER 2 0
vlan-12 fe80::f2f1:f2ff:fef3:201 ::
PREFIX 30::1/128 n/a EXTERNAL_2 2 1
vlan-12 fe80::f2f1:f2ff:fef3:201 ::
PREFIX 30::2/128 n/a EXTERNAL_2 2 1
vlan-12 fe80::f2f1:f2ff:fef3:201 ::
PREFIX 200::1/128 n/a EXTERNAL_2 1 1
vlan-13 fe80::f2f1:f2ff:fef3:301 ::
PREFIX 200::2/128 n/a EXTERNAL_2 1 1
vlan-13 fe80::f2f1:f2ff:fef3:301 ::
Route:
Prefix(Intra Inter External)ABR ASBR External
8 2 0 4 1 2
Path:
Prefix(Intra Inter External)ABR ASBR External
8 2 0 4 1 2
```

Step 6 Configure ASBR aggregation on R4. Aggregate 30::1/128 and 30::2/128 into 30::0/112.

```
Raisecom-R4#configure
Raisecom-R4(config)#ospfv3 1
Raisecom-R4(config-ospfv3-1)#asbr-summary 30::0/112
```

Step 7 Verify configuration results.

Check the routing table and database of R2. The aggregation is successful.

Raisecom-R2(config)#show ospfv3 database 1s-type external

Database of OSPFv3 Process 1

AS External Link State					
LinkId Prefix	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.2 200::1/128	1.1.1.1	1590	0x80000001	0x5d21	44
0.0.0.3 200::2/128	1.1.1.1	488	0x80000001	0x6d0f	44
0.0.0.5 30::/112	4.4.4.4	23	0x80000001	0x86cb	44

Raisecom-R2(config)#show ospfv3 route

OspfV3 Process 1

RoutType	Prefix	AreaId	PathType	Cost	Cost2
NextHopIf	NextHopNbr		Backu		
pNextHop					
ABR	1.1.1.1/32	0.0.0.0	INTRA	1	0
vlan-12	fe80::f2f1:f2ff:fe3:101	::			
ASBR	1.1.1.1/32	0.0.0.0	INTRA	1	0
vlan-12	fe80::f2f1:f2ff:fe3:101	::			
ASBR	3.3.3.3/32	0.0.0.0	INTER	2	0
vlan-12	fe80::f2f1:f2ff:fe3:101	::			
ASBR	4.4.4.4/32	0.0.0.2	INTRA	1	0
vlan-24	fe80::f2f1:f2ff:fe3:101	::			
PREFIX	10::1/128	0.0.0.2	INTRA	2	0
vlan-24	fe80::f2f1:f2ff:fe3:101	::			
PREFIX	10::2/128	0.0.0.2	INTRA	2	0
vlan-24	fe80::f2f1:f2ff:fe3:101	::			
PREFIX	12::/64	0.0.0.0	INTRA	1	0
vlan-12	12::	::			
PREFIX	13::/64	0.0.0.0	INTER	2	0
vlan-12	fe80::f2f1:f2ff:fe3:101	::			
PREFIX	20::1:0/112	0.0.0.2	INTRA	2	0
vlan-24	fe80::f2f1:f2ff:fe3:101	::			
PREFIX	20::2:0/112	0.0.0.2	INTRA	2	0
vlan-24	fe80::f2f1:f2ff:fe3:101	::			
PREFIX	24::/64	0.0.0.2	INTRA	1	0
vlan-24	24::	::			
PREFIX	30::/112	n/a	EXTERNAL_2	1	1
vlan-24	fe80::f2f1:f2ff:fe3:101	::			
PREFIX	200::1/128	n/a	EXTERNAL_2	1	1
vlan-12	fe80::f2f1:f2ff:fe3:101	::			
PREFIX	200::2/128	n/a	EXTERNAL_2	1	1
vlan-12	fe80::f2f1:f2ff:fe3:101	::			

Route:

Prefix(Intra	Inter	External)	ABR	ASBR	External
10	6	0	3	1	3

```

Path:
Prefix(Intra Inter External)ABR      ASBR      External
10    6      0      3      1      3

```

Step 8 Configure NSSA aggregation on R1 to aggregate NSSA LSA generated on R3 upon conversion.

```

Raisecom-R1#configure
Raisecom-R1(config)#ospfv3 1
Raisecom-R1(config-ospfv3-1)#area 1 nssa summary 200::/112 advertise

```

Step 9 Check configuration results.

Aggregate external LSA generated by R1.

```

Raisecom-R2(config)#show ospfv3 route
Ospfv3 Process 1
RouteType Prefix          AreaId      PathType    Cost    Cost2
NextHopIf  NextHopNbr              Backu
pNextHop
ABR         1.1.1.1/32              0.0.0.0     INTRA       1       0
vlan-12     fe80::f2f1:f2ff:fe3:101 ::
ASBR        1.1.1.1/32              0.0.0.0     INTRA       1       0
vlan-12     fe80::f2f1:f2ff:fe3:101 ::
ASBR        3.3.3.3/32              0.0.0.0     INTER       2       0
vlan-12     fe80::f2f1:f2ff:fe3:101 ::
ASBR        4.4.4.4/32              0.0.0.2     INTRA       1       0
vlan-24     fe80::f2f1:f2ff:fe3:101 ::
PREFIX      10::1/128                0.0.0.2     INTRA       2       0
vlan-24     fe80::f2f1:f2ff:fe3:101 ::
PREFIX      10::2/128                0.0.0.2     INTRA       2       0
vlan-24     fe80::f2f1:f2ff:fe3:101 ::
PREFIX      12::/64                  0.0.0.0     INTRA       1       0
vlan-12     12::                     ::
PREFIX      13::/64                  0.0.0.0     INTER       2       0
vlan-12     fe80::f2f1:f2ff:fe3:101 ::
PREFIX      20::1:0/112              0.0.0.2     INTRA       2       0
vlan-24     fe80::f2f1:f2ff:fe3:101 ::
PREFIX      20::2:0/112              0.0.0.2     INTRA       2       0
vlan-24     fe80::f2f1:f2ff:fe3:101 ::
PREFIX      24::/64                  0.0.0.2     INTRA       1       0
vlan-24     24::                     ::
PREFIX      30::/112                  n/a         EXTERNAL_2  1       1
vlan-24     fe80::f2f1:f2ff:fe3:101 ::
PREFIX      200::/112                 n/a         EXTERNAL_1  3       0
vlan-12     fe80::f2f1:f2ff:fe3:101 ::
Route:
Prefix(Intra Inter External)ABR      ASBR      External
9      6      0      2      1      3

```



```

Path:
Prefix(Intra Inter External)ABR      ASBR      External
9      6      0      2      1      3

Raisecom-R2(config)#show ospfv3 database ls-type external
Database of OSPFv3 Process 1

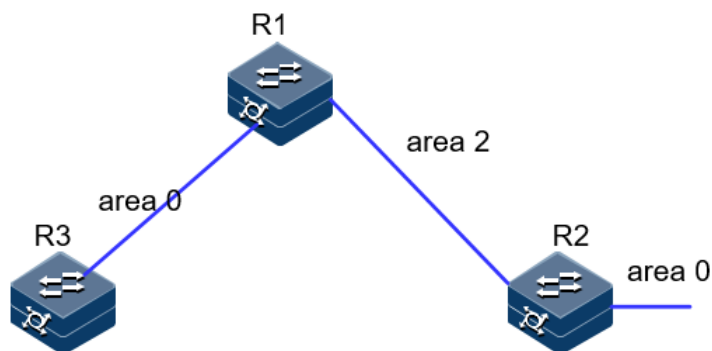
      AS External Link State
LinkId      ADV Router      Age      Seq#      CheckSum      Len
Prefix
0.0.0.4      1.1.1.1      22      0x80000001  0xb8d7      44
200::/112
0.0.0.5      4.4.4.4      180     0x80000001  0x86cb      44
30::/112
  
```

3.9.16 Example for configuring OSPFv3 virtual connection

Networking requirements

As shown below, R3 is located in area 0; R1 connects area 0 and area 2 while R2 connects area 0 and area 2. At this point, area 0 is segmented and the internal routes of area 2 cannot be learned within area 0; area 2 cannot learn the internal routes of area 0 and the routes of other areas. At this point, configure a virtual connection between R1 and R4 to connect to area 0.

Figure 3-44 OSPFv3 virtual connection networking



Configuration steps

Step 1 Configure IP addresses of interfaces.

- Establish neighboring interfaces between R1 and R2 by using VLAN 12.
- Establish neighboring interfaces between R1 and R3 by using VLAN 13.
- Add loopback interface 1 to R2, and configure its IPv6 address to 22::2/128.
- Add loopback interface 1 to R3, and configure its IPv6 address to 33::3/128.

Step 2 Configure OSPFv3.

R1:

```
Raisecom-R1#configure
Raisecom-R1(config)#ospfv3 1
Raisecom-R1(config-ospfv3-1)#router-id 1.1.1.1
Raisecom-R1(config-ospfv3-1)#exit
Raisecom-R1(config)#interface vlan 13
Raisecom-R1(config-vlanif-13)#ospfv3 1 area 0
Raisecom-R1(config-vlanif-13)#exit
Raisecom-R1(config)#interface vlan 12
Raisecom-R1(config-vlanif-12)#ospfv3 1 area 2
Raisecom-R1(config-vlanif-12)#exit
```

R2:

```
Raisecom-R2#configure
Raisecom-R2(config)#ospfv3 1
Raisecom-R2(config-ospfv3-1)#router-id 2.2.2.2
Raisecom-R2(config-ospfv3-1)#exit
Raisecom-R2(config)#interface vlan 12
Raisecom-R2(config-vlanif-12)#ospfv3 1 area 2
Raisecom-R2(config-vlanif-12)#exit
Raisecom-R2(config)#interface loopback 1
Raisecom-R2(config-loopback-1)#ospfv3 1 area 0
```

R3:

```
Raisecom-R3#configure
Raisecom-R3(config)#ospfv3 1
Raisecom-R3(config-ospfv3-1)#router-id 3.3.3.3
Raisecom-R3(config-ospfv3-1)#exit
Raisecom-R3(config)#interface vlan 13
Raisecom-R3(config-vlanif-13)#ospfv3 1 area 0
Raisecom-R3(config-vlanif-13)#exit
Raisecom-R3(config)#interface loopback 1
Raisecom-R3(config-loopback-1)#ospfv3 1 area 0
```

Step 3 Check configuration results.

```
Raisecom-R1(config)#show ospfv3 neighbor
```

```
Ospfv3 Process 1
NeighborId      Priority  State    Interface    Instance  Aging
UpTime   IpAddress
-----
2.2.2.2          1      Full    vlan-12      0         34      0:01:52
fe80::f2f1:f2ff:fe3:201
```

```

3.3.3.3          1          Full   vlan-13          0          29          0:01:40
fe80::f2f1:f2ff:fef3:301
-----
Down:0          Attempt:0          Init:0          TwoWay:0          ExchangeStart:0
Exchange:0
Loading:0          Full:2

```

R2 fails to learn the route to 33::3. R1 or R2 also fails to learn the route to 22::2.

Raisecom-R1(config)#show ospfv3 route

```

Ospfv3 Process 1
RoutType Prefix          AreaId          PathType      Cost    Cost2
NextHopIf NextHopNbr          Backu
pNextHop
ABR      2.2.2.2/32          0.0.0.2        INTRA         1       0
vlan-12  fe80::f2f1:f2ff:fef3:201  ::
PREFIX   12::/64          0.0.0.2        INTRA         1       0
vlan-12  12::              ::
PREFIX   13::/64          0.0.0.0        INTRA         1       0
vlan-13  13::              ::
PREFIX   33::3/128        0.0.0.0        INTRA         2       0
vlan-13  fe80::f2f1:f2ff:fef3:301  ::
Route:
Prefix(Intra Inter External)ABR    ASBR    External
3      3      0      0      1      0

Path:
Prefix(Intra Inter External)ABR    ASBR    External
3      3      0      0      1      0

```

Raisecom-R2(config)#show ospfv3 route

```

Ospfv3 Process 1
RoutType Prefix          AreaId          PathType      Cost    Cost2
NextHopIf NextHopNbr          Backu
pNextHop
ABR      1.1.1.1/32          0.0.0.2        INTRA         1       0
vlan-12  fe80::f2f1:f2ff:fef3:101  ::
PREFIX   12::/64          0.0.0.2        INTRA         1       0
vlan-12  12::              ::
PREFIX   22::2/128        0.0.0.0        INTRA         1       0
loopback-1 22::2          ::
Route:
Prefix(Intra Inter External)ABR    ASBR    External
2      2      0      0      1      0

Path:
Prefix(Intra Inter External)ABR    ASBR    External
2      2      0      0      1      0

```

Step 4 Configure virtual connection.

R1:

```
Raisecom-R1#configure
Raisecom-R1(config)#ospfv3 1
Raisecom-R1(config-ospfv3-1)#area 2 virtual-link 2.2.2.2
```

R2:

```
Raisecom-R2#configure
Raisecom-R2(config)#ospfv3 1
Raisecom-R2(config-ospfv3-1)#area 2 virtual-link 1.1.1.1
```

Step 5 Check configuration results.

Check whether the virtual connection is established normally.

```
Raisecom-R1(config)#show ospfv3 virtual-link
Ospfv3 Process 1
Area Id           :0.0.0.2
Neighbor Id       :2.2.2.2
Local Interface   :2.2.2.2
State             :pointToPoint
Event Change      :1
Hello Interval    :10(s)
Retransmit Interval :5(s)
Transmit Delay    :1(s)
Dead Interval     :60(s)
Link Lsa Count    :0
Link LSA CksumSum :0
Neighbor Prefix   :12::2
Neighbor State    :Full
Neighbor Event Change :4
```

Check whether the routing table is learnt normally.

```
Raisecom-R1(config)#show ospfv3 route
Ospfv3 Process 1
RoutType Prefix          AreaId      PathType  Cost  Cost2
NextHopIf NextHopNbr      Backu
pNextHop
ABR      2.2.2.2/32             0.0.0.2    INTRA     1     0
vlan-12  fe80::f2f1:f2ff:fe3:201 ::
PREFIX  12::/64                0.0.0.2    INTRA     1     0
vlan-12  12::                   ::
PREFIX  12::1/128              0.0.0.2    INTRA     0     0
vlan-12  12::1                  ::
```

```

    PREFIX 12::2/128          0.0.0.2          INTRA      1      0
vlan-12   fe80::f2f1:f2ff:fef3:201      ::
    PREFIX 13::/64           0.0.0.0          INTRA      1      0
vlan-13   13::                ::
    PREFIX 22::2/128         0.0.0.0          INTRA      2      0
vlan-12   fe80::f2f1:f2ff:fef3:201      ::
    PREFIX 33::3/128         0.0.0.0          INTRA      2      0
vlan-13   fe80::f2f1:f2ff:fef3:301      ::
Route:
Prefix(Intra Inter External)ABR      ASBR      External
6      6      0      0      2      0

Path:
Prefix(Intra Inter External)ABR      ASBR      External
6      6      0      0      1      0

Raisecom-R2(config)#show ospfv3 route
Ospfv3 Process 1
RoutType Prefix          AreaId      PathType   Cost   Cost2
NextHopIf NextHopNbr      Backu
pNextHop
ABR      1.1.1.1/32          0.0.0.2     INTRA      1      0
vlan-12   fe80::f2f1:f2ff:fef3:101      ::
    PREFIX 12::/64          0.0.0.2     INTRA      1      0
vlan-12   12::                ::
    PREFIX 12::1/128         0.0.0.2     INTRA      1      0
vlan-12   fe80::f2f1:f2ff:fef3:101      ::
    PREFIX 12::2/128         0.0.0.2     INTRA      0      0
vlan-12   12::2                ::
    PREFIX 13::/64           0.0.0.0     INTRA      2      0
vlan-12   fe80::f2f1:f2ff:fef3:101      ::
    PREFIX 22::2/128         0.0.0.0     INTRA      1      0
loopback-1 22::2                ::
    PREFIX 33::3/128         0.0.0.0     INTRA      3      0
vlan-12   fe80::f2f1:f2ff:fef3:101      ::
Route:
Prefix(Intra Inter External)ABR      ASBR      External
6      6      0      0      2      0

Path:
Prefix(Intra Inter External)ABR      ASBR      External
6      6      0      0      1      0

```

3.10 IS-IS

3.10.1 Introduction

Basic concepts

Intermediate System to Intermediate System intra-domain routing information exchange protocol (IS-IS) was originally a dynamic routing protocol designed by the International

Organization for Standardization (ISO) for its Connectionless Network Protocol (CLNP). IS-IS belongs to the Internal Gateway Protocol (IGP) used within ASs. IS-IS is a link status protocol that uses the Shortest Path First (SPF) algorithm for routing calculations. IS-IS can support large and medium-sized networks, and its routing convergence speed is fast, making it an alternative to OSPF. In the mid-1990s, some carriers chose IS-IS as their network IGP because integrating IS-IS can support both CLNP and IP and smoothly transition from early OSI networks to IP networks becomes easy.

IS-IS has the following concepts:

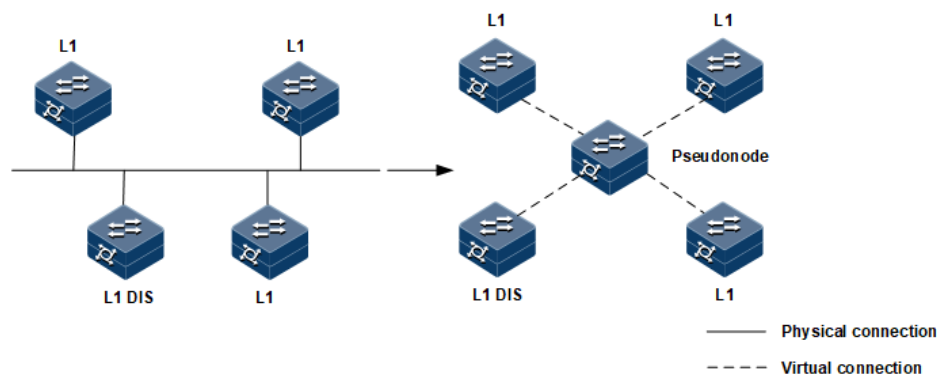
- **Intermediate System (IS):** intermediate system. Equivalent to a router in TCP/IP, it is the basic unit for generating and advertising routing information in IS-IS. In the following text, IS and router have the same meaning.
- **Routing Domain (RD):** routing domain. In a routing domain, a group of ISs exchange routing information through the same routing protocol.
- **Area:** a subdivision unit of a routing domain. IS-IS allows the entire routing domain to be divided into multiple areas.
- **Link State Database (LSDB):** link state database. All network connectivity states form a link state database, with at least one LSDB in each IS. The IS uses the SPF algorithm and LSDB to generate its own routes.
- **Link State Protocol Data Unit (LSP):** link state packet. In IS-IS, each IS generates at least one LSP, which contains all link state information of this IS. Each IS collects all LSPs within its own domain and forms its own locally generated LSP to form its own LSDB.
- **Level-1 route:** also known as intra-area route, existing between different ISs within the same area. When the IS wants to send a packet to another IS, it checks the destination address in the packet. If it finds the destination address located on different subnets within the area, it will choose the optimal path for forwarding; otherwise, IS forwards the data to the nearest Level-1-2 router in this area, and then the Level-1-2 router is responsible for forwarding data.
- **Level-2 route:** also known as inter-area route, existing between areas within the same route domain. When the destination address is in different areas, the IS sends a packet to the nearest Level-2 IS, which is responsible for forwarding the packet to another area.
- **Level-1 router (L1 router):** responsible for routes within the area and only maintaining one Level-1 LSDB. This LSDB contains route information for the local area and forwards packets outside the area to the nearest Level-1-2 router.
- **Level-2 router (L2 router):** responsible for inter-area route and only maintaining one Level-2 LSDB. This LSDB contains route information between areas. All Level-2 routers and Level-1-2 routers form the backbone network of the route domain, and they are responsible for communication between different areas. The backbone network must be physically continuous.
- **Level-1-2 router (L1/L2 router):** routers that are both the Level-1 router and Level-2 router are called Level-1-2 routers. The Level-1-2 router maintains two LSDBs, with the Level-1 LSDB used for intra-area routing and Level-2 LSDB used for inter-area routing.

DIS and pseudo node

On a broadcast network, IS-IS needs to select one router from all routers as the Designated Intermediate System (DIS). The DIS is used to create and update pseudo nodes, and is responsible for generating the Link State Protocol Data Unit (LSP) for pseudo nodes, which describes the present network devices on this network.

A pseudo node is a virtual node used to simulate a broadcast network, not a real router. In IS-IS, the pseudo node is identified by the System ID of the DIS and the one-byte Circuit ID (non-zero).

Figure 3-45 Pseudo node networking



Using pseudo nodes can simplify network topology and reduce the length of LSP generated by routers. In addition, when the network changes, the number of LSPs to be generated is also be reduced, and the resource consumption of SPF is reduced.

The Level-1 DIS and Level-2 DIS are elected separately, and you can configure different priorities for electing DISs at different levels. The router with the highest priority is elected as DIS. If there are multiple routers with the highest priority, the router with the highest MAC address will be elected. Different levels of DISs can be the same router or different routers.

The differences between the IS-IS DIS and OSPF Designated Router (DR) are as below:

- On the IS-IS broadcasting network routers with the priority of 0 also participate in the election of the DIS, while routers with priority 0 in OSPF do not participate in the election of the DR.
- On the IS-IS broadcasting network, when a new router is added and meets the conditions to become a DIS, the router will be elected as the new DIS, and the original pseudo node will be deleted. This change will cause new LSP flooding. In OSPF, when a new router is added, even if its DR priority value is the highest, it will not immediately become the DR in that network segment.
- On the IS-IS broadcasting network, routers of the same level in the same network segment form the adjacency relationship, including all non-DIS routers. In OSPF, routers establish the adjacency relationship with the DR and BDR only.

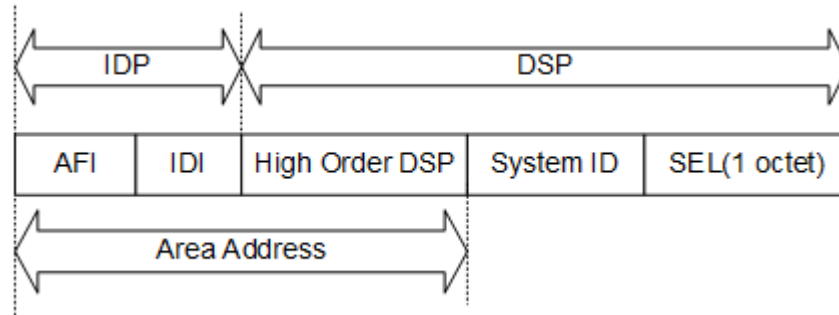
Structure of the IS-IS address

The Network Service Access Point (NSAP) is an address used in the OSI protocol to locate resources. The address structure of the NSAP is shown in Figure 3-46, which consists of Initial Domain Part (IDP) and Domain Specific Part (DSP). The length of both IDP and DSP is variable. The NSAP has a maximum total length of 20 bytes and a minimum of 8 bytes.

- IDP is equivalent to the primary network number in an IP address. It is regulated by ISO and consists of two parts: Authority and Format Identification (AFI) and Initial Domain Identification (IDI). The AFI represents the address allocation authority and address format while the IDI is used to identify domains.
- DSP is equivalent to the subnet number and host address in the IP address. It consists of three parts: High Order DSP, System ID, and SEL. The High Order DSP is used to divide

areas. The System ID is used to distinguish hosts. The SEL (NSAP selector) is used to indicate service types.

Figure 3-46 Structure of the IS-IS address



- **Area Address:** IDP and High Order DSP together can identify both the routing domain and the area within the routing domain, so they are collectively referred to as the area address, which is equivalent to the area number in OSPF. All routers within the same Level-1 area must have the same area address while routers within the Level-2 area can have different area addresses. Generally, a router needs to be configured with only one area address, and all nodes in the same area must have the same area address. To support smooth area merging, splitting, and conversion, configure a maximum of three domain addresses for one IS-IS process in the implementation by the device.
- **System ID:** the System ID is used to uniquely identify a host or router within an area. Its length is fixed at 48 bits (6 bytes) in the implementation by the device.

In practical applications, the Router ID is generally used to correspond with the System ID. Assume that a router uses the IP address 192.168.1.1 of interface Loopback0 as its Router ID, the System ID used by it in IS-IS can be converted as below.

- Expand each decimal digit of IP address 192.168.1.1 to 3 bits, and fill in 0s before any less than 3 bits to obtain 192.168.001.001.
- Divide the expanded address into three parts. Each consists of four digits, resulting in 1921.6800.1001. The recombined 1921.6800.1001 is the System ID.
- There can be different methods for specifying the actual System ID, but ensure that the host or router can be uniquely identified.
- **SEL:** the function of SEL is similar to the "protocol identifier" in IP, and different transmission protocols correspond with different SELs. The SEL on the IP is always 00.

The Network Entity Title (NET) refers to the network layer information of the device itself, which can be regarded as a special type of NSAP (SEL=00). The length of NET is the same as that of the NSAP, with a maximum of 20 bytes and a minimum of 8 bytes. When configuring IS-IS on a router, consider NET only, needless of focusing on the NSAP. For example, if the NET is ab.cdef.1234.5678.9abc.00, then, the area address is ab.cdef, the System ID is 1234.5678.9abc, and the SEL is 00.

IS-IS packet types

There are several types of IS-IS packets: Hello PDU (Protocol Data Unit), LSP, and SNP.

- **Hello PDU:** Hello packets are used to establish and maintain neighbor relationships, also known as IIH (IS to IS Hello PDUs). Among them, the Level-1 IS-IS on the broadcast network uses Level-1 LAN IIH; the Level-2 IS-IS on the broadcasting network uses Level-2 LAN IIH; on non-broadcast networks, P2P IIH is used. Their packet formats are

different. P2P IIH, compared with LAN IIH, has an additional Local Circuit ID field representing the local link ID, but the Priority field representing the priority of DIS on the broadcast network and the LAN ID field representing DIS and pseudo node System IDs are missing.

- **Link State PDU (LSP):** the LSP is used to exchange link state information. LSP is divided into two types: Level-1 LSP and Level-2 LSP. The Level-1 LSP is transmitted by Level-1 IS-IS, the Level-2 LSP is transmitted by Level-2 IS-IS, and both types of LSPs can be transmitted by the Level 1-2 IS-IS. The main fields in the LSP are explained as below:
 - **ATT field:** when Level-1-2 IS-IS transmits the Level-1 LSP within the Level-1 area, if the ATT bit is configured in the Level-1 LSP, this indicates that Level-1 IS-IS in that area can access the external area through this Level-1-2 IS-IS.
 - **LSDB Overload (OL) field:** overload flag bit. The LSP with the overload flag may still spread on the network, but it will not be used when routes are calculated through overloaded routers. After the overload bit is configured on the router, other routers will not use this router for forwarding when performing SPF calculations, but only calculate the direct connection route on that node.
 - **IS Type field:** used to indicate whether the IS-IS type that generates this LSP is Level-1 or Level-2 IS-IS (01 represents Level-1; 11 represents Level-2).
- **Sequence Number PDU (SNP):** the SNP synchronizes each LSDB by describing all or part of the LSPs in the database, thereby maintaining the integrity and synchronization of the LSDB. SNPs include the Complete SNP (CSNP) and Partial SNP (PSNP), which can be further divided into the Level-1 CSNP, Level-2 CSNP, Level-1 PSNP, and Level-2 PSNP. The CSNP includes summary information about all LSPs in the LSDB, thus synchronizing the LSDB between adjacent routers. On a broadcasting network, the CSNP is periodically sent by the DIS (with a default sending period of 10s). On the point-to-point chain, the CSNP is sent only when the adjacency relationship is first established. The PSNP only lists the sequence numbers of one or more recently received LSPs, and it can confirm multiple LSPs at once. When the LSDB is not synchronized, the PSNP is also used to request neighbors to send new LSPs. The variable length field in the IS-IS packet consists of multiple TLV (Type Length Value) triplets. Its format is shown in the figure. TLV is also known as Code Length Value (CLV). Different types of PDUs contain different TLVs.

	No. of Octets
Type	1
Length	1
Value	Length

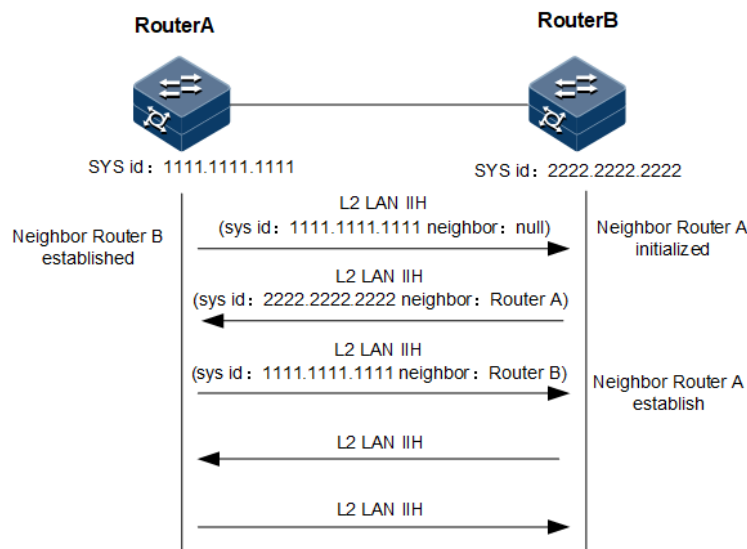
TLV Type	Name	PDU type for application
1	Area Addresses	IIH and LSP
2	IS Neighbors (LSP)	LSP
4	Partition Designated Level2 IS	L2 LSP
6	IS Neighbors (MAC Address)	LAN IIH
7	IS Neighbors (SNPA Address)	LAN IIH
8	Padding	IIH

TLV Type	Name	PDU type for application
9	LSP Entries	SNP
10	Authentication Information	IIH, LSP, and SNP
128	IP Internal Reachability Information	LSP
129	Protocols Supported	IIH and LSP
130	IP External Reachability Information	L2 LSP
131	Inter-Domain Routing Protocol Information	L2 LSP
132	IP Interface Address	IIH and LSP

Establishing IS-IS neighbor relation

IS-IS is a link state routing protocol, where each router generates an LSP that contains link state information for all IS-IS-enabled interfaces on that router. After the IS-IS adjacency relationship with adjacent devices is established and the LSDBs of local devices are updated, LSDBs can be synchronized with the LSDBs of other devices on the entire IS-IS network. Then, calculate the IS-IS route by using the SPF algorithm based on the LSDB. If this IS-IS route is the optimal route to the destination address, it will be sent to the IP routing table and guide the forwarding of packets. Two routers running IS-IS must first establish a neighbor relationship before implementing routing functions and exchanging protocol packets. The methods of establishing neighbor relationships for IS-IS vary with different types of networks.

Figure 3-47 Flow for establishing broadcast link neighbor relationship



- Step 1 Router A broadcasts Level-2 LAN IIH, which does not contain the neighbor identification.
- Step 2 After receiving this packet, Router B identifies itself and Router A neighbor status as Initial. Then, Router B replies to Router A with Level-2 LAN IIH, which identifies Router A as a neighbor of Router B.

Step 3 After receiving this packet, Router A identifies its neighbor status with Router B as Up. Then, Router A sends a Level-2 LAN IIH to Router B, which identifies Router B as a neighbor of Router A.

Step 4 After receiving this packet, Router B identifies its neighbor status with Router A as Up. In this way, the two routers successfully establish a neighbor relationship.

On the broadcast network, the DIS needs to be elected. Therefore, after establishing a neighbor relationship, the router waits for two Hello packet intervals before conducting DIS elections. The Hello packet contains the Priority field, and the one with the highest Priority value will be elected as the DIS of the broadcast network. If the priority is the same, the interface with the greater MAC address is elected as the DIS.

- Establishing neighbor relationships in P2P links
- On P2P links, establishing neighbor relationships is different from broadcasting links. It is divided into the two-handshaking mechanism and three-handshaking mechanism.
- Two-handshaking mechanism: as long as the router receives a Hello packet from the other end, it unilaterally declares the neighbor as Up and establishes a neighbor relationship.
- Three-handshake mechanism: this establishes neighbor relationships by sending P2P IS-IS Hello PDUs three times, similar to the establishment of broadcast neighbor relationships.

IS-IS establishes neighbor relationships based on the following principles:

- Only adjacent routers at the same level are likely to become neighbors.
- For Level-1 routers, the area number must be consistent.
- The network type of the IS-IS interface at both ends of the link must be consistent.
- The addresses of the IS-IS interfaces at both ends of the link must be in the same network segment.

IS-IS LSP exchange process

Causes of generating LSPs

All routers within the IS-IS routing domain generate LSPs, and the following events trigger a new LSP:

- Neighbor Up or Down
- IS-IS-related interface Up or Down
- The redistributed IP route change
- Inter-area IP route change
- The interface is assigned a new metric value.
- Periodic update
- Receiving the processing of a new LSP by a neighbor
- Merging the received new LSP into own LSDB and marking it as flooding
- Sending a new LSP to an interface other than the receiving interface
- Neighbors broadcast to other neighbors.

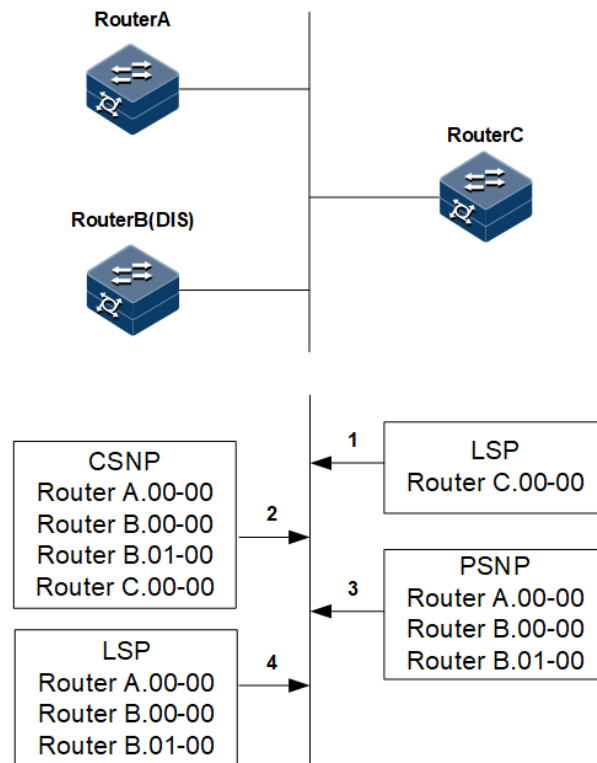
LSP flooding

Flooding of LSP packets refers to a method in which a router notifies neighboring routers of its LSP, and the neighboring routers transmit the same LSP packet to other neighbors except

for the sending router, and gradually transmit the LSP to all routers in the entire system. Through this flooding, every router within the entire system can have the same LSP information and maintain synchronization with the LSDB.

Each LSP has a 4-byte SN that identifies itself. The SN in the first LSP packet sent during router startup is 1. In the future, when a new LSP needs to be generated, the SN of the new LSP is added by one to the previous LSP SN. A higher SN means an updated LSP.

Figure 3-48 Flow for synchronizing the LSDB in the P2P link



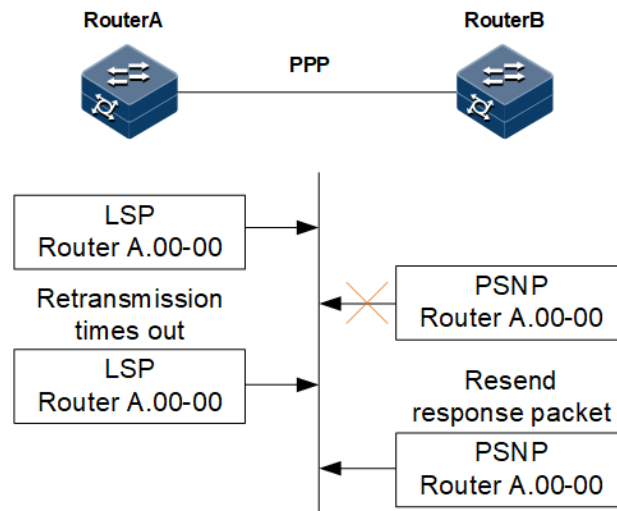
- Step 1 As shown in the figure, the newly added router Router C first sends a Hello packet to establish a neighbor relationship with the routers in the broadcast domain.
- Step 2 Router C waits for the LSP refresh timer to time out, and then sends its own LSP to the multicast address (Level-1:01-80-C2-00-00-14; Level-2:01-80-C2-00-15). In this way, all neighbors on the network receive the LSP.
- Step 3 The DIS in this network segment adds the LSP received from Router C to the LSDB, waits for the CSNP packet timer to time out, and sends the CSNP packet for LSDB synchronization within the network.
- Step 4 Router C receives a CSNP packet from the DIS, compares it with its own LSDB, and then sends a PSNP packet to DIS requesting an LSP that it does not have.
- Step 5 After receiving the PSNP packet request, the DIS sends the corresponding LSP to Router C for LSDB synchronization.

In the previous process, the DIS LSDB is updated as below:

- Step 1 The DIS receives an LSP and searches for the corresponding record in the database. If there is no LSP, the DIS adds it to the database and broadcasts contents of the new database.

- Step 2 If the received LSP SN is greater than the local LSP SN, the DIS replaces the local LSP with the received LSP, and broadcasts contents of the new database. If the received LSP SN is smaller than the local LSP SN, the DIS sends a local LSP packet to the ingress interface.
- Step 3 If both SNs are equal, the DIS compares the Remaining Lifetime. If the Remaining Lifetime of the received LSP is less than the Remaining Lifetime of the local LSP, replace the local LSP with the received LSP, and broadcasts contents of the new database. If the Remaining Lifetime of the received LSP is greater than the Remaining Lifetime of the local LSP, the DIS sends a local LSP packet to the ingress interface.
- Step 4 If both SNs and Remaining Lifetimes are equal, the DIS compares the Checksum. If the Checksum of the received LSP is greater than that of the local LSP, replace the local LSP with the received LSP, and broadcasts contents of the new database. If the Checksum of the received LSP is smaller than that of the local LSP, the DIS sends a local LSP packet to the ingress interface.
- Step 5 If both SNs, Remaining Lifetimes, and Checksums are equal, the DIS does not forward the packet.

Figure 3-49 Flow for synchronizing the LSDB on the P2P link



- Step 1 Router A establishes the neighbor relationship with Router B.
- Step 2 Router A and Router B sends CSNP to each other. If the LSDB and CSNP are not synchronized on the peer device, Router A or Router B sends the PSNP request to obtain the corresponding LSP.
- Step 3 As shown in Figure above, assume that Router B requests the corresponding LSP from Router A. When Router A sends the LSP requested by Router B, it starts the LSP retransmission timer and waits for the PSNP sent by Router B to acknowledge the receipt of the LSP.
- Step 4 After the interface LSP retransmission timer times out, if Router A has not received the PSNP packet sent by Router B as a response, it resends the LSP until the PSNP packet is received.

The device LSDB in P2P links is updated as below:

- Step 1 If the received LSP is smaller than the local SN, directly send the local LSP to the other party, and then wait for the other party to send itself a PSNP packet as acknowledgment; if the received LSP is greater than the local SN, save the new LSP in the own LSDB, acknowledge the receipt of the LSP through a PSNP packet, and finally send the new LSP to neighbors other than the one who sent the LSP.

- Step 2 If the received LSP SN is the same as the local one, compare the Remaining Lifetime. If the Remaining Lifetime of the received LSP is less than the Remaining Lifetime of the local LSP, save the received LSP in the LSDB and send a PSNP packet to acknowledge the receipt of the LSP. Then, send the LSP to neighbors other than the one who sent the LSP; if the Remaining Lifetime of the received LSP is greater than the Remaining Lifetime of the local LSP, send the local LSP directly to the other party and wait for the other party to send a PSNP packet as acknowledgment.
- Step 3 If the SNs of the received LSP and the local LSP are the same and the Remaining Lifetime is not 0, compare the Checksum. If the Checksum of the received LSP is greater than that of the local LSP, save the received LSP in the LSDB and send a PSNP packet to acknowledge the receipt of the LSP. Then, send the LSP to neighbors other than those who sent the LSP; if the Checksum of the received LSP is less than the Checksum of the local LSP, send the local LSP directly to the other party, and then wait for the other party to send itself a PSNP packet as acknowledgment.
- Step 4 If the received LSP and local LSP have the same SN, Remaining Lifetime, and Checksum, the packet will not be forwarded.

3.10.2 Preparing for configurations

Scenario

IS-IS belongs to IGP. It is used internally in the ASs. IS-IS is also a link state protocol that uses the Shortest Path First (SPF) algorithm for routing calculations.

Prerequisites

The neighboring nodes are reachable at the network layer.

3.10.3 Default configurations

Default configurations of IS-IS are as below.

Function	Default value
Global IS-IS status	Disable
DIS priority	64
Device level	level-1-2
Interval for sending Hello packets	10s
Interval for updating LSPs	900s
Maximum valid time for LSPs	1200s

3.10.4 Configuring basic functions of IS-IS

Configure basic functions of IS-IS for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#isis <i>Process id</i>	Create an IS-IS process, and enter the IS-IS view.
3	Raisecom(config-isis-1)#network-entity net	Configure the NET of IS-IS so that IS-IS can actually start.
4	Raisecom(config-isis-1)#is-type { level-1 level-1-2 level-2 }	When the level is Level-2, the device can form a neighbor relationship with Level-2 devices in the same or different areas, or Level-1-2 devices in other areas, and only maintain one Level-2 LSDB. Routers that are both the Level-1 router and Level-2 router are called Level-1-2 routers, which can form Level-1 neighbor relationships with Level-1 and Level-1-2 routers in the same area, and Level-2 neighbor relationships with Level-2 and Level-1-2 routers in other areas. The Level-1 router must be connected to other areas through the Level-1-2 router. The Level-1-2 router maintains two LSDBs, with the Level-1 LSDB used for intra-area routing and Level-2 LSDB used for inter-area routing.
5	Raisecom(config-vlanif-1)#isis enable [<i>instance-id</i>]	Enable the IS-IS interface.
6	Raisecom (config-vlanif-1)#isis circuit-level { level-1 level-2 level-1-2 default }	Configure the interface level.
7	Raisecom (config-vlanif-1)#isis dis-priority { priority-value default } [<i>level-1</i> <i>level-2</i>]	Specify the priority of the router.
8	Raisecom (config-vlanif-1)#isis circuit-type { broadcast p2p }	Configure the IS-IS link type. By default, it is broadcast.

3.10.5 Configuring security of the IS-IS network

Configure security of the IS-IS network for the device as below.

Step	Command	Description
1	Raisecom(config-isis-1)#area-authentication-mode { simple md5 } { cipher plain } password [snp-packet { authentication-avoid send-only } all-send-only]	Configure the IS-IS area authentication password, and configure the ISIS area to authenticate the received Level-1 routing information packets (LSP and SNP) in a predetermined mode and password. It can also be used to add authentication information to the sent Level-1 packets.
2	Raisecom(config-isis-1)#domain-authentication-mode { simple md5 } { cipher plain } password [snp-packet { authentication-avoid send-only } all-send-only]	Configure the authentication password of the IS-IS routing domain, and configure the ISIS route domain to authenticate the received Level-1-2 routing information packets (LSP and SNP) in a predetermined mode and password.
3	Raisecom(config-vlanif-1)#isis authentication-mode { simple md5 } { cipher plain } password { level-1 level-2 p2p }	Configure the IS-IS interface to authenticate Hello packets in the specified mode and password, and add authentication information in the sent Hello packets.

3.10.6 Configuring IS-IS route selection

Configure IS-IS route selection for the device as below.

Step	Command	Description
1	Raisecom(config-isis-1)#preference { priority default }	Configure the priority of IS-IS routes.
2	Raisecom(config-isis-1)#cost-style { narrow wide compatible narrow-compatible wide-compatible default } { level-1 level-2 }	Configure the device to receive the routes with the types of narrow and wide but to send the routes with the type of narrow only.
3	Raisecom(config-isis-1)#maximum load-balancing { load-balancing-number default }	Configure the maximum number of equivalent routes for forming load balancing.
4	Raisecom(config-isis-1)#import-route level-2 to level-1	Redistribute routes in the Level-2 area into the Level-1 area. By default, routes in the Level-2 area are not distributed into the Level-1 area.

3.10.7 Configuring exchange of ISIS routing information

Configure exchange of ISIS routing information for the device as below.

Step	Command	Description
1	<code>Raisecom(config-isis-1)#default-route-originate { none level-1 level-2 level-1-2 }</code>	Configure the IS-IS router to generate the default route.
2	<code>Raisecom(config-isis-1)#import-route { connect static rip ospf bgp isis } { level-1 level-2 level-1-2 } [cost { cost-value default inherit } route-policy policy-name]*</code>	Redistribute other routes.
3	<code>Raisecom(config-isis-1)#filter-policy import route-policy route-policy-name</code>	Configure the filtering policy for the IS-IS to be added to the IP routing table.
4	<code>Raisecom(config-isis-1)#summary ip-address/maskLen { level-1 level-2 }</code>	Excess route entries can reduce the speed for looking up the routing table and increase management complexity when data are forwarded. By configuring route aggregation, the size of the routing table can be reduced.

3.10.8 Configuring IS-IS route convergence

Configure IS-IS route convergence for the device as below.

Step	Command	Description
1	<code>Raisecom(config-vlanif-1)#isis hello-interval { interval-value default } [level-1 level-2]</code>	Configure the interval for sending Hello packets in IS-IS.
2	<code>Raisecom(config-vlanif-1)#isis hello-multiplier { multiple-value default } [level-1 level-2]</code>	Configure the multiplier of sending Hello packets to neighbors in IS-IS.
3	<code>Raisecom(config-vlanif-1)#isis csnp-interval { interval-value default } [level-1 level-2]</code>	Configure the interval for sending CSNP packets at the specified level.

Step	Command	Description
4	<code>Raisecom(config-vlanif-1)#isis psnp-interval { interval-value default } [level-1 level-2]</code>	Configure the interval for sending PSNP packets at the specified level.
5	<code>Raisecom(config-isis-1)#lsp-max-lifetime { max-life-value default }</code>	Configure the interval for updating the link state packets of the route.
6	<code>Raisecom(config-isis-1)#lsp-generation max-interval { max-interval default } init-interval { int-interval default } incr-interval { incr-interval default } [level-1 level-2]</code>	Configure the delay for generating LSPs by the specified IS-IS process.

3.10.9 Configuring IS-IS reliability

Configure IS-IS reliability for the device as below.

Step	Command	Description
1	<code>Raisecom(config-vlanif-1)#isis bfd { enable disable }</code>	Enable or disable IS-IS BFD on the specified interface, and establish a BFD session with default parameters.

3.10.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show isis config</code>	Show IS-IS configurations.
2	<code>Raisecom#show isis database</code>	Show the ISIS LSDB.
3	<code>Raisecom#show isis interface</code>	Show information or detailed information about IS-IS interfaces.
4	<code>Raisecom#show isis route</code>	Show IS-IS routing information.
5	<code>Raisecom#show isis neighbor</code>	Show information about IS-IS neighbors.

3.10.11 IS-IS

Configure the device as below.

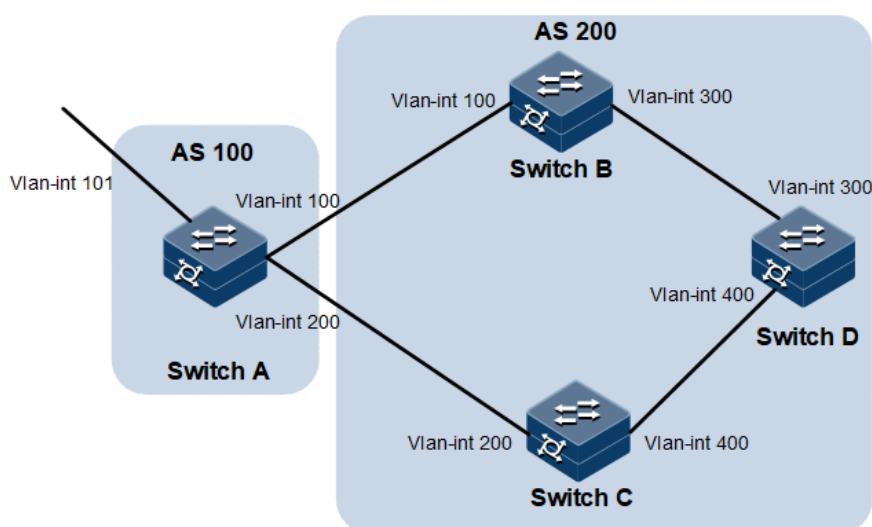
Step	Command	Description
1	Raisecom(config-isis-1)#reset isis { isis-instance all }	Reset all or the specified IS-IS instance.

3.10.12 Example for configuring basic functions of IS-IS

Networking requirements

As shown below, Switch A, Switch B, Switch C, and Switch D belong to the same AS. They are required to be reachable from each other on the IP network through IS-IS.

Switch A and Switch B are Level-1 switches. Switch D is the Level-2 switch. As the Level-1-2 switch, Switch C connects two ASs. The AS IDs of the Switch A, Switch B, and Switch C are 10 while that of Switch D is 20.



Configuration steps

Step 1 Configure IP addresses of interfaces.

Step 2 Configure IS-IS.

Configure Switch A:

```

SwitchA#configure
SwitchA(config)#isis 1
SwitchA(config-isis-1)#is-type level-1
SwitchA(config-isis-1)#network-entity 10.0000.0000.0001.00
SwitchA(config-isis-1)#quit
SwitchA(config)#int vlan 100
SwitchA(config-vlanif-100)#isis enable 1
SwitchA(config-vlanif-100)#quit
    
```

Configure Switch B:

```
SwitchB#configure
SwitchB(config)#isis 1
SwitchB(config-isis-1)#is-type level-1
SwitchB(config-isis-1)#network-entity 10.0000.0000.0002.00
SwitchB(config-isis-1)#quit
SwitchB(config)#int vlan 200
SwitchB(config-vlanif-200)#isis enable 1
SwitchB(config-vlanif-200)#quit
```

Configure Switch C:

```
SwitchC#configure
SwitchC(config)#isis 1
SwitchC(config-isis-1)#network-entity 10.0000.0000.0003.00
SwitchC(config-isis-1)#quit
SwitchC(config)#int vlan 100
SwitchC(config-vlanif-100)#isis enable 1
SwitchC(config-vlanif-100)#quit
SwitchC(config)#int vlan 200
SwitchC(config-vlanif-200)#isis enable 1
SwitchC(config-vlanif-200)#quit
SwitchC(config)#int vlan 300
SwitchC(config-vlanif-300)#isis enable 1
SwitchC(config-vlanif-300)#quit
```

Configure Switch D:

```
SwitchD#configure
SwitchD(config)#isis 1
SwitchD(config-isis-1)#is-type level-2
SwitchD(config-isis-1)#network-entity 20.0000.0000.0004.00
SwitchD(config-isis-1)#quit
SwitchD(config)#int vlan 300
SwitchD(config-vlanif-300)#isis enable 1
SwitchD(config-vlanif-300)#quit
```

Checking results

Use the following commands to show the ISIS database and LSP.

```
SwitchA(config)#show isis database
```

Database Information for IS-IS(1)

```

Level-1 Link State Database
The total number of isis 1 database is: 5
#      ID                      Level Seq      Checksum Lifetime Length
ATT/P/OL
1      0000.0000.0001.00-00    1      3      52707      958      69
0/0/0
2      0000.0000.0001.01-00    1      1      8889      958      52
0/0/0
3      0000.0000.0002.00-00    1      3      7823      829      69
0/0/0
4      0000.0000.0002.01-00    1      1      13222     829      52
0/0/0
5      0000.0000.0003.00-00    1      7      24706     968     112
1/0/0

```

SwitchB(config)#show isis database

Database Information for IS-IS(1)

```

Level-1 Link State Database
The total number of isis 1 database is: 5
#      ID                      Level Seq      Checksum Lifetime Length
ATT/P/OL
1      0000.0000.0001.00-00    1      3      52707      958      69
0/0/0
2      0000.0000.0001.01-00    1      1      8889      958      52
0/0/0
3      0000.0000.0002.00-00    1      3      7823      829      69
0/0/0
4      0000.0000.0002.01-00    1      1      13222     829      52
0/0/0
5      0000.0000.0003.00-00    1      7      24706     968     112
1/0/0

```

SwitchC(config)#show isis database

Database Information for IS-IS(1)

```

Level-1 Link State Database
The total number of isis 1 database is: 5
#      ID                      Level Seq      Checksum Lifetime Length
ATT/P/OL
1      0000.0000.0001.00-00    1      3      52707      958      69
0/0/0
2      0000.0000.0001.01-00    1      1      8889      958      52
0/0/0
3      0000.0000.0002.00-00    1      3      7823      829      69
0/0/0
4      0000.0000.0002.01-00    1      1      13222     829      52
0/0/0
5      0000.0000.0003.00-00    1      7      24706     968     112
1/0/0

```

```

Level-2 Link State Database
The total number of isis 1 database is: 3
#      ID                      Level Seq      Checksum Lifetime Length
ATT/P/OL
6      0000.0000.0003.00-00    2      5        42205      957      101
0/0/0
7      0000.0000.0003.03-00    2      1        18060      732      52
0/0/0
8      0000.0000.0004.00-00    2      5        20494      708      84
0/0/0
L1 Database Count :5
L2 Database Count :3

```

SwitchD(config)#show isis database

```

Database Information for IS-IS(1)

Level-2 Link State Database
The total number of isis 1 database is: 3
#      ID                      Level Seq      Checksum Lifetime Length
ATT/P/OL
1      0000.0000.0003.00-00    2      5        42205      957      101
0/0/0
2      0000.0000.0003.03-00    2      1        18060      732      52
0/0/0
3      0000.0000.0004.00-00    2      5        20494      708      84
0/0/0

```

Show the ISIS routes of each switch. There should be a default route in the routing table of the Level-1 switch, and its next hop is the Level-1-2 switch. There should be all Level-1 and Level-2 routes in the routing table of the Level-2 switch.

SwitchA(config)#show isis route

```

ISIS process 1
Level Dst                      Nexthop      MAC          Cost    Time
Level-1 0.0.0.0/0                    10.1.1.1     f0f1:f2f3:0101 10
0:10:56
Level-1 10.1.1.0/24                10.1.1.2     0000:0000:0000 10
0:11:31
Level-1 10.1.2.0/24                10.1.1.1     f0f1:f2f3:0101 20
0:10:56
Level-1 192.168.0.0/24              10.1.1.1     f0f1:f2f3:0101 20
0:10:56

```

SwitchB(config)#show isis route

```

ISIS process 1
Level Dst                      Nexthop      MAC          Cost    Time
Level-1 0.0.0.0/0                    10.1.2.1     f0f1:f2f3:0101 10
0:13:47
Level-1 10.1.1.0/24                10.1.2.1     f0f1:f2f3:0101 20
0:11:49

```

```

Level-1 10.1.2.0/24          10.1.2.2          0000:0000:0000    10
0:14:04
Level-1 192.168.0.0/24      10.1.2.1          f0f1:f2f3:0101    20
0:13:47

```

SwitchC(config)#show isis route

ISIS process 1

Level	Dst	NextHop	MAC	Cost	Time
Level-1	10.1.1.0/24	10.1.1.1	0000:0000:0000	10	
Level-1	10.1.2.0/24	10.1.2.1	0000:0000:0000	10	
Level-1	192.168.0.0/24	192.168.0.1	0000:0000:0000	10	
Level-2	172.16.0.0/16	192.168.0.2	00e0:fcd7:47d1	10	
Level-2	10.1.1.0/24	10.1.1.1	0000:0000:0000	10	
Level-2	10.1.2.0/24	10.1.2.1	0000:0000:0000	10	
Level-2	192.168.0.0/24	192.168.0.1	0000:0000:0000	10	

SwitchD(config)#show isis route

ISIS process 1

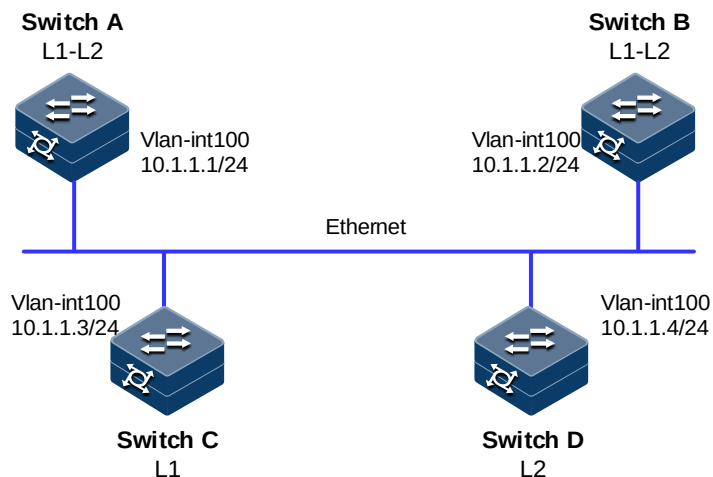
Level	Dst	NextHop	MAC	Cost	Time
Level-2	172.16.0.0/16	172.16.0.1	00e0:fcd7:47d1	10	
Level-2	10.1.1.0/24	192.168.0.1	0000:0000:0000	10	
Level-2	10.1.2.0/24	192.168.0.1	0000:0000:0000	10	
Level-2	192.168.0.0/24	192.168.0.2	0000:0000:0000	10	

3.10.13 Example for configuring ISIS DIS selection

Networking requirements

As shown below, Switch A, Switch B, Switch C, and Switch D run IS-IS to interconnect with each other, and they belong to the same area 10. The network type is broadcast (Ethernet).

Switch A and Switch B are Level-1-2 switches. Switch C is the Level-1 switch. Switch D is the Level-2 switch. It is required to configure Switch A as the Level-1-2 DIS by changing the DIS priority of the interface.



Configuration steps

Step 1 Configure IP addresses of interfaces.

Step 2 Configure IS-IS.

Configure Switch A:

```
SwitchA#configure
SwitchA(config)#isis 1
SwitchA(config-isis-1)#network-entity 10.0000.0000.0001.00
SwitchA(config-isis-1)#quit
SwitchA(config)#int vlan 100
SwitchA(config-vlanif-100)#isis enable 1
SwitchA(config-vlanif-100)#quit
```

Configure Switch B:

```
SwitchB#configure
SwitchB(config)#isis 1
SwitchB(config-isis-1)#network-entity 10.0000.0000.0002.00
SwitchB(config-isis-1)#quit
SwitchB(config)#int vlan 100
SwitchB(config-vlanif-100)#isis enable 1
SwitchB(config-vlanif-100)#quit
```

Configure Switch C. Configure its level-1 priority to 127.

```
SwitchC#configure
SwitchC(config)#isis 1
SwitchC(config-isis-1)#network-entity 10.0000.0000.0003.00
SwitchC(config-isis-1)#quit
SwitchC(config)#int vlan 100
```



```
SwitchC(config-vlanif-100)#isis enable 1
SwitchC(config-vlanif-100)#isis dis-priority 127 level-1
SwitchC(config-vlanif-100)#quit
```

Configure Switch D. Configure its level-2 priority to 127.

```
SwitchD#configure
SwitchD(config)#isis 1
SwitchD(config-isis-1)#network-entity 10.0000.0000.0004.00
SwitchD(config-isis-1)#quit
SwitchD(config)#int vlan 100
SwitchD(config-vlanif-100)#isis enable 1
SwitchC(config-vlanif-100)#isis dis-priority 127 level-2
SwitchD(config-vlanif-100)#quit
```

Use the following command to show information about IS-IS neighbors on Switch A.

```
SwitchA(config)#show isis neighbor
```

```
Neighbor information for IS-IS(1)
The total number of isis(1) neighbor is:6
```

Interface	Level	ID	MAC	Priority	HoldTime
vlan-100	L1	0000.0000.0002	f0f1.f2f3.0201	64	15
UpTime		State	Name		
days 0:01:11		up			
vlan-100	L2	0000.0000.0002	f0f1.f2f3.0201	64	11
days 0:01:32		up			
vlan-100	L1	0000.0000.0003	f0f1.f2f3.0301	64	29
days 0:01:12		up			
vlan-100	L2	0000.0000.0003	f0f1.f2f3.0301	64	23
days 0:01:12		up			
vlan-100	L1	0000.0000.0004	f0f1.f2f3.0401	64	23
days 0:00:23		up			
vlan-100	L2	0000.0000.0004	f0f1.f2f3.0401	64	24
days 0:00:48		up			

Use the following command to show information about IS-IS neighbors on Switch B.

```
SwitchB(config)#show isis neighbor
```

```
Neighbor information for IS-IS(1)
The total number of isis(1) neighbor is:6
```

Interface	Level	ID	MAC	Priority	HoldTime
vlan-100	L2	0000.0000.0001	f0f1.f2f3.0101	64	19
UpTime		State	Name		
days 0:00:48		up			

```

vlan-100      L1      0000.0000.0001    f0f1.f2f3.0101    64      21      0
days 0:00:47      up
vlan-100      L1      0000.0000.0003    f0f1.f2f3.0301    64      21      0
days 0:00:30      up
vlan-100      L2      0000.0000.0003    f0f1.f2f3.0301    64      27      0
days 0:00:30      up
vlan-100      L1      0000.0000.0004    f0f1.f2f3.0401    64      27      0
days 0:00:08      up
vlan-100      L2      0000.0000.0004    f0f1.f2f3.0401    64      26      0
days 0:00:08      up

```

Use the following command to show information about IS-IS neighbors on Switch C.

SwitchC(config)#**show isis neighbor**

```

Neighbor information for IS-IS(1)
The total number of isis(1) neighbor is:6
Interface   Level  ID          MAC          Priority  HoldTime
UpTime      State   Name
vlan-100    L2      0000.0000.0002  f0f1.f2f3.0201  64      26      0
days 0:00:36      up
vlan-100    L2      0000.0000.0001  f0f1.f2f3.0101  64      13      0
days 0:00:34      up
vlan-100    L1      0000.0000.0002  f0f1.f2f3.0201  64      21      0
days 0:00:35      up
vlan-100    L1      0000.0000.0004  f0f1.f2f3.0401  64      28      0
days 0:00:14      up
vlan-100    L2      0000.0000.0004  f0f1.f2f3.0401  64      27      0
days 0:00:09      up
vlan-100    L1      0000.0000.0001  f0f1.f2f3.0101  64      24      0
days 0:00:05      up

```

Use the following command to show information about IS-IS neighbors on Switch D.

SwitchD(config)#**show isis neighbor**

```

Neighbor information for IS-IS(1)
The total number of isis(1) neighbor is:6
Interface   Level  ID          MAC          Priority  HoldTime
UpTime      State   Name
vlan-1      L1      0000.0000.0003  f0f1.f2f3.0301  64      22      0
days 0:00:25      up
vlan-1      L2      0000.0000.0003  f0f1.f2f3.0301  64      27      0
days 0:00:30      up
vlan-1      L2      0000.0000.0002  f0f1.f2f3.0201  64      25      0
days 0:00:37      up
vlan-1      L1      0000.0000.0002  f0f1.f2f3.0201  64      29      0
days 0:00:31      up
vlan-1      L2      0000.0000.0001  f0f1.f2f3.0101  64      19      0
days 0:00:19      up

```

```
vlan-1      L1      0000.0000.0001    f0f1.f2f3.0101    64      28      0
days 0:00:10      up
```

Use the following command to show information about IS-IS interfaces on Switch A.

SwitchD(config)#show isis interface

```

                        Interface information for IS-IS(1)
The total number of isis(1) interface is:1
Interface          CircID Adminstate Type          Level MeshEnable
SmallHello
vlan-1              1      on      broadcast    L1-2 N/A          false
```

Use the following command to check whether the Level-1 DIS of the IS-IS databases is **0000.0000.0003.01-00** and Level-2 DIS of the IS-IS databases is **0000.0000.0004.01-00**.

SIM-MPU(config)#show isis database

```

                        Database Information for IS-IS(1)

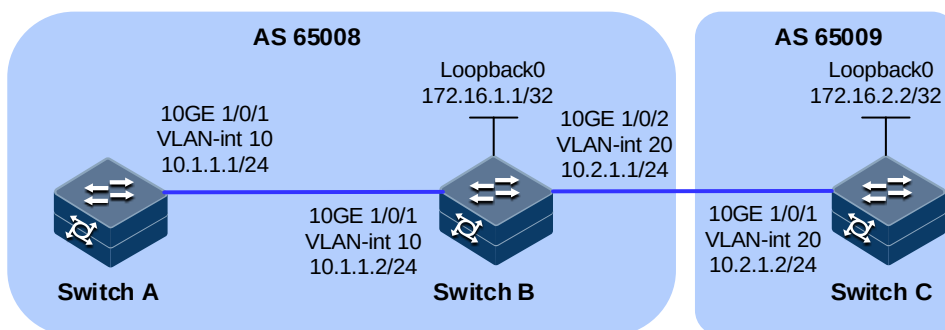
                        Level-1 Link State Database
The total number of isis 1 database is: 5
#   ID                      Level Seq          Checksum Lifetime Length
ATT/P/OL
1   0000.0000.0001.00-00    1     4           1448     1147     69
0/0/0
2   0000.0000.0002.00-00    1     3           7312     1134     69
0/0/0
3   0000.0000.0003.00-00    1     2          13176     1133     69
0/0/0
4   0000.0000.0003.01-00    1     3          16247    1134    74    0/0/0
5   0000.0000.0004.00-00    1     3          18018     1143     69
0/0/0

                        Level-2 Link State Database
The total number of isis 1 database is: 5
#   ID                      Level Seq          Checksum Lifetime Length
ATT/P/OL
6   0000.0000.0001.00-00    2     3          12668     1138     69
0/0/0
7   0000.0000.0002.00-00    2     3          18021     1137     69
0/0/0
8   0000.0000.0003.00-00    2     3          23374     1141     69
0/0/0
9   0000.0000.0004.00-00    2     2          29238     1144     69
0/0/0
10  0000.0000.0004.01-00    2     1          12423    1144    74    0/0/0
L1 Database Count :5
L2 Database Count :5
```

3.10.14 Configuring IS-IS to redistribute external routes

Networking requirements

As shown below, Switch A and Switch B belong to the same AS, and they have established the IS-IS neighbor relationship. Establish the EBGP connection between Switch B and Switch C. It is now required to communicate among each network segments and to change the metrics when AS 65008 sends routing information to AS 65009.



Configuration steps

Step 1 Configure IP addresses of interfaces.

Step 2 Configure IS-IS and BGP.

Configure Switch A:

```
SwitchA#configure
SwitchA(config)#isis 1
SwitchA(config-isis-1)#network-entity 10.0000.0000.0001.00
SwitchA(config-isis-1)#quit
SwitchA(config)#int vlan 10
SwitchA(config-vlanif-10)#isis enable 1
SwitchA(config-vlanif-10)#quit
```

Configure Switch B:

```
SwitchB#configure
SwitchB(config)#isis 1
SwitchB(config-isis-1)#network-entity 10.0000.0000.0002.00
SwitchB(config-isis-1)#import-route bgp
SwitchB(config-isis-1)#quit
SwitchB(config)#int vlan 10
SwitchB(config-vlanif-10)#isis enable 1
SwitchB(config-vlanif-10)#quit
SwitchB(config)#int vlan 20
SwitchB(config-vlanif-20)#isis enable 1
SwitchB(config-vlanif-20)#quit

SwitchB(config)#bgp 65008
```

```
SwitchB(config-bgp)#router-id 172.16.1.1
SwitchB(config-bgp)#peer 10.2.1.2 as-number 65009
SwitchB(config-bgp)#ipv4-family unicast
SwitchB(config-bgp-af-ipv4)#neighbor 10.2.1.2 enable
SwitchB(config-bgp-af-ipv4)#network 10.2.1.0/24
```

Configure Switch C. BGP redistributes a 192.168.1.0/24 static route.

```
SwitchC#configure
SwitchC(config)#ip route-static 192.168.1.0 255.255.255.0 10.2.1.3
SwitchC(config)#bgp 65009
SwitchC(config-bgp)#router-id 172.16.2.2
SwitchC(config-bgp)#peer 10.2.1.1 as-number 65008
SwitchC(config-bgp)#ipv4-family unicast
SwitchC(config-bgp-af-ipv4)#neighbor 10.2.1.1 enable
SwitchC(config-bgp-af-ipv4)#network 10.2.1.0/24
SwitchC(config-bgp-af-ipv4)#import-route static
```

Use the following commands to show information about IS-IS routes on each router. There is a BGP route entry on Switch B. There are routes of the **192.168.1.0/24** network segment on the IS-IS and IP routing table on Switch A.

```
SwitchA(config)#show isis route
```

```
ISIS process 1
Level Dst NextHop MAC Cost Time
Level-1 10.1.1.0/24 10.1.1.1 0000:0000:0000 10
0:12:20
Level-1 10.2.1.0/24 10.1.1.2 f0f1:f2f3:0101 20
0:12:03
Level-1 192.168.1.0/24 10.1.1.2 f0f1:f2f3:0101 10 0:10:30
Level-2 10.1.1.0/24 10.1.1.1 0000:0000:0000 10
0:12:20
Level-2 10.2.1.0/24 10.1.1.2 f0f1:f2f3:0101 20
0:12:03
Level-2 192.168.1.0/24 10.1.1.2 f0f1:f2f3:0101 10 0:10:30
```

```
SwitchA(config)#show ip route
Max Routing Number Limit: 131072
Max Destination Number Limit: 771
Routing Tables:
```

Destination	Gateway	Pre/Cost	Proto	Interface
Mpls	Status	Vpn-Instance		
10.1.1.0/24	10.1.1.1	0/0	local	vlan-10
Up	N/A			
	10.1.1.1	50/10	isis	vlan-10
Up	N/A			

```

10.1.1.1/32      10.1.1.1      0/0      local  vlan-10      no
Up      N/A
10.2.1.0/24      10.1.1.2      50/20     isis   vlan-10      no
Up      N/A
127.0.0.1/32     127.0.0.1      0/0      local  loopback-0    no
Up      N/A
192.168.1.0/24 10.1.1.2      50/10     isis   vlan-10      no   up   N/A
SwitchB(config)#show isis route

```

```

ISIS process 1
Level   Dst                Nexthop          MAC              Cost    Time
Level-1 10.1.1.0/24          10.1.1.2         0000:0000:0000   10
0:13:51
Level-1 10.2.1.0/24          10.2.1.1         0000:0000:0000   10
0:14:07
Level-2 10.1.1.0/24          10.1.1.2         0000:0000:0000   10
0:13:51
Level-2 10.2.1.0/24          10.2.1.1         0000:0000:0000   10
0:14:07

```

```

SwitchB(config)#show ip route
Max Routing Number Limit: 131072
Max Destination Number Limit: 771
Routing Tables:

```

Destination	Gateway	Pre/Cost	Proto	Interface
Mpls	Status	Vpn-Instance		
10.1.1.0/24	10.1.1.2	0/0	local	vlan-10
Up	N/A			
	10.1.1.2	50/10	isis	vlan-10
Up	N/A			
10.1.1.2/32	10.1.1.2	0/0	local	vlan-10
Up	N/A			
10.2.1.0/24	10.2.1.1	0/0	local	vlan-20
Up	N/A			
	10.2.1.1	50/10	isis	vlan-20
Up	N/A			
10.2.1.1/32	10.2.1.1	0/0	local	vlan-20
Up	N/A			
127.0.0.1/32	127.0.0.1	0/0	local	loopback-0
Up	N/A			
172.16.1.1/32	172.16.1.1	0/0	local	loopback-1
Up	N/A			
192.168.1.0/24	10.2.1.2	255/60	bgp	vlan-20
			no	Up
				N/A

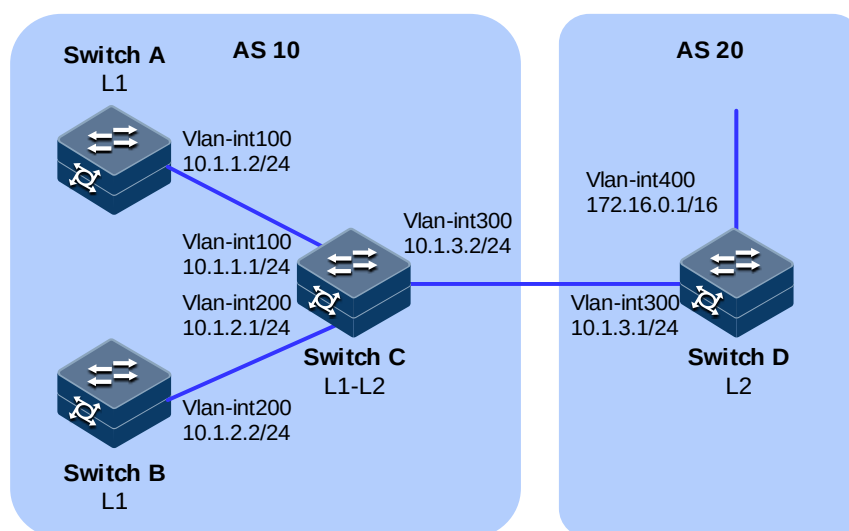
Total: 9 Static: 0 Down: 0 Destination: 7

3.10.15 Example for configuring IS-IS verification

Networking requirements

As shown below, Switch A, Switch B, Switch C, and Switch D belong to the same routing domain. They are required to implement IP network interconnection through IS-IS. Wherein, Switch A, Switch B, and Switch C belong to the same area Area 10. Switch D belongs to the other area Area 20.

Configure area verification in area 10 to prevent untrusted routing information to be added to the LSDB of area 10. Configure routing domain verification on Switch C and Switch D to prevent untrusted routing information to be added to the current routing domain. Configure neighbor relationship verification on Switch A, Switch B, Switch C, and Switch D respectively.



Configuration steps

Step 1 Configure IP addresses of interfaces.

Step 2 Configure basic functions of IS-IS.

Configure Switch A:

```
SwitchA#configure
SwitchA(config)#isis 1
SwitchA(config-isis-1)#network-entity 10.0000.0000.0001.00
SwitchA(config-isis-1)#quit
SwitchA(config)#int vlan 100
SwitchA(config-vlanif-100)#isis enable 1
SwitchA(config-vlanif-100)#quit
```

Configure Switch B:

```
SwitchB#configure
SwitchB(config)#isis 1
SwitchB(config-isis-1)#network-entity 10.0000.0000.0002.00
```

```
SwitchB(config-isis-1)#quit
SwitchB(config)#int vlan 200
SwitchB(config-vlanif-200)#isis enable 1
SwitchB(config-vlanif-200)#quit
```

Configure Switch C:

```
SwitchC#configure
SwitchC(config)#isis 1
SwitchC(config-isis-1)#network-entity 10.0000.0000.0003.00
SwitchC(config-isis-1)#quit
SwitchC(config)#int vlan 100
SwitchC(config-vlanif-100)#isis enable 1
SwitchC(config-vlanif-100)#quit
SwitchC(config)#int vlan 200
SwitchC(config-vlanif-200)#isis enable 1
SwitchC(config-vlanif-200)#quit
SwitchC(config)#int vlan 300
SwitchC(config-vlanif-300)#isis enable 1
SwitchC(config-vlanif-300)#quit
```

Configure Switch D:

```
SwitchD#configure
SwitchD(config)#isis 1
SwitchD(config-isis-1)#is-type level-2
SwitchD(config-isis-1)#network-entity 20.0000.0000.0004.00
SwitchD(config-isis-1)#quit
SwitchD(config)#int vlan 300
SwitchD(config-vlanif-300)#isis enable 1
SwitchD(config-vlanif-300)#quit
```

- Step 3 Configure neighbor relationship verification on Switch A, Switch B, Switch C, and Switch D respectively.

Configure neighbor relationship verification in MD5 plain text mode on VLAN interface 100 on Switch A and VLAN interface 100 on Switch C respectively. Verify that if their passwords for verification are the same, they can establish the neighbor relationship.

```
SwitchA(config)#int vlan 100
SwitchA(config-vlanif-100)#isis authentication-mode md5 plain abcd
SwitchA(config-vlanif-100)#quit
SwitchC(config)#int vlan 100
SwitchC(config-vlanif-100)#isis authentication-mode md5 plain abcd
SwitchC(config-vlanif-100)#quit
```


Configure neighbor relationship verification in MD5 plain text mode on VLAN interface 100 on Switch B and VLAN interface 100 on Switch C respectively. Verify that if their passwords for verification are different, they cannot establish the neighbor relationship.

```
SwitchB(config)#int vlan 200
SwitchB(config-vlanif-200)#isis authentication-mode md5 plain abcd
SwitchB(config-vlanif-200)#quit
SwitchC(config)#int vlan 200
SwitchC(config-vlanif-200)#isis authentication-mode md5 plain dcba
SwitchC(config-vlanif-200)#quit
```

Configure area verification in MD5 plain text mode on Switch A and Switch B respectively. Verify that if their passwords for verification are the same, they can learn routes; otherwise, they cannot learn routes.

```
SwitchA(config)#isis 1
SwitchA(config-isis-1)#area-authentication-mode md5 plain abcd
SwitchA(config-isis-1)#quit
SwitchC(config)#isis 1
SwitchC(config-isis-1)#area-authentication-mode md5 plain abcd
SwitchC(config-isis-1)#quit
```

Configure routing domain verification in MD5 plain text mode on Switch C and Switch D respectively. Verify that if their passwords for verification are the same, they can learn routes; otherwise, they cannot learn routes.

```
SwitchC(config)#isis 1
SwitchC(config-isis-1)#domain-authentication-mode md5 plain abcd
SwitchC(config-isis-1)#quit
SwitchD(config)#isis 1
SwitchD(config-isis-1)#domain-authentication-mode md5 plain abcd
SwitchD(config-isis-1)#quit
```

3.11 IS-IS (IPv6)

3.11.1 Introduction

This section describes the differences of IS-IS (IPv6) from IS-IS. For details, see section 3.10 IS-IS.

IS-IS is a dynamic routing protocol based on link state algorithm originally designed for the OSI network. To support IPv4 routes, it is extended to the IPv4 network, and it is called integrated IS-IS.

When the IPv6 network is constructed, a dynamic routing protocol is needed to provide accurate and effective routing information for forwarding IPv6 packets. Based on good extension, IS-IS supports the IPv6 network layer protocols, so it can discover and generate IPv6 routes.

IETF draft-ietf-isis-ipv6-05 stipulates the newly added contents of IS-IS for supporting IPv6. To support the processing and calculation of IPv6 routes, IS-IS added two TLVs and one new Network Layer Protocol Identifier (NLPI):

Two TLVs and NLPI are as below:

- IPv6 Reachability: the type value is 236 (0xEC). It indicates network reachability by defining the prefix and metrics of routing information.
- IPv6 Interface Address: the type value is 232 (0xE8). It corresponds with the IPv4 TLV of IP Interface Address, but differs from the 32-bit IPv4 address with the 128-bit IPv6 address.
- NLPID: it is an 8-bit field for identifying network layer protocol packets. The IPv6 NLPID is 142 (0x8E). If an IS-IS router supports IPv6, it must advertise routing information with this NLPID.

3.11.2 Preparing for configurations

Scenario

IS-IS belongs to IGP. It is used internally in the ASs. IS-IS is also a link state protocol that uses the Shortest Path First (SPF) algorithm for routing calculations.

Prerequisites

The neighboring nodes are reachable at the network layer.

3.11.3 Default configurations

Default configurations of IS-IS (IPv6) are as below.

Function	Default value
Global IS-IS status	Disable
DIS priority	64
Device level	level-1-2
Interval for sending Hello packets	10s
Interval for updating LSPs	900s
Maximum valid time for LSPs	1200s

3.11.4 Configuring basic functions of IS-IS (IPv6)

Configure basic functions of IS-IS (IPv6) for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#isis <i>Process id</i>	Create an IS-IS process, and enter the IS-IS view.
3	Raisecom(config-isis-1)#network-entity net	Configure the NET of IS-IS so that IS-IS can actually start.
4	Raisecom(config-isis-1)#is-type { level-1 level-1-2 level-2 }	Configure the global level. When the level is level-1, the device establishes neighbor relationships with level-1 and level-2 devices only in the same area, and maintains the level-1 LSDB. When the level is Level-2, the device can form a neighbor relationship with Level-2 devices in the same or different areas, or Level-1-2 devices in other areas, and only maintain one Level-2 LSDB. Routers that are both the Level-1 router and Level-2 router are called Level-1-2 routers, which can form Level-1 neighbor relationships with Level-1 and Level-1-2 routers in the same area, and Level-2 neighbor relationships with Level-2 and Level-1-2 routers in other areas. The Level-1 router must be connected to other areas through the Level-1-2 router. The Level-1-2 router maintains two LSDBs, with the Level-1 LSDB used for intra-area routing and Level-2 LSDB used for inter-area routing.
5	Raisecom(config-isis-1)#ipv6 enable [topology { compatible ipv6 standard }]	Enable IPv6 of the IS-IS process. By default, the standard IPv6 is enabled.
6	Raisecom(config-vlanif-1)#isis-ipv6 enable [instance-id]	Enable the IS-IS (IPv6) interface.
7	Raisecom (config-vlanif-1)#isis circuit-level { level-1 level-2 level-1-2 default }	Configure the interface level.
8	Raisecom (config-vlanif-1)#isis dis-priority { priority-value default } [level-1 level-2]	Specify the priority of the router.
9	Raisecom (config-vlanif-1)#isis circuit-type { broadcast p2p }	Configure the IS-IS link type. By default, it is broadcast.

3.11.5 Configuring security of the IS-IS (IPv6) network

Configure security of the IS-IS (IPv6) network for the device as below.

Step	Command	Description
1	Raisecom(config-isis-1)#area-authentication-mode { simple md5 } { cipher plain } password [snp-packet { authentication-avoid send-only } all-send-only]	Configure the IS-IS area authentication password, and configure the ISIS area to authenticate the received Level-1 routing information packets (LSP and SNP) in a predetermined mode and password. It can also be used to add authentication information to the sent Level-1 packets.
2	Raisecom(config-isis-1)#domain-authentication-mode { simple md5 } { cipher plain } password [snp-packet { authentication-avoid send-only } all-send-only]	Configure the authentication password of the IS-IS routing domain, and configure the ISIS route domain to authenticate the received Level-1-2 routing information packets (LSP and SNP) in a predetermined mode and password.
3	Raisecom(config-vlanif-1)#isis authentication-mode { simple md5 } { cipher plain } password { level-1 level-2 p2p }	Configure the IS-IS interface to authenticate Hello packets in the specified mode and password, and add authentication information in the sent Hello packets.

3.11.6 Configuring IS-IS (IPv6) route selection

Configure IS-IS (IPv6) route selection for the device as below.

Step	Command	Description
1	Raisecom(config-isis-1)#ipv6 preference { priority default }	Configure the priority of IS-IS (IPv6) routes.
2	Raisecom(config-isis-1)#cost-style { narrow wide compatible narrow-compatible wide-compatible default } { level-1 level-2 }	Configure the device to receive the routes with the types of narrow and wide but to send the routes with the type of narrow only.
3	Raisecom(config-isis-1)#ipv6 maximum load-balancing { load-balancing-number default }	Configure the maximum number of equivalent IPv6 routes for forming load balancing.
4	Raisecom(config-isis-1)#import-route level-2 to level-1	Redistribute routes in the Level-2 area into the Level-1 area. By default, routes in the Level-2 area are not distributed into the Level-1 area.

3.11.7 Configuring exchange of ISIS (IPv6) routing information

Configure exchange of ISIS (IPv6) routing information for the device as below.

Step	Command	Description
1	Raisecom(config-isis-1)#default-route-originate ipv6 { none level-1 level-2 level-1-2 }	Configure the IS-IS (IPv6) router to generate the default route.
2	Raisecom(config-isis-1)#import-route ipv6 { connect static rip ospf bgp isis } { level-1 level-2 level-1-2 } [cost { cost-value default inherit } route-policy policy-name]*	Redistribute other routes.
3	Raisecom(config-isis-1)#filter-policy import route-policy route-policy-name	Configure the filtering policy for the IS-IS (IPv6) to be added to the IP routing table.
4	Raisecom(config-isis-1)#ipv6 summary ip-address/maskLen { level-1 level-2 }	Excess route entries can reduce the speed for looking up the routing table and increase management complexity when data are forwarded. By configuring route aggregation, the size of the routing table can be reduced.

3.11.8 Configuring IS-IS (IPv6) route convergence

Configure IS-IS (IPv6) route convergence for the device as below.

Step	Command	Description
1	Raisecom(config-vlanif-1)#isis hello-interval { interval-value default } [level-1 level-2]	Configure the interval for sending Hello packets in IS-IS.
2	Raisecom(config-vlanif-1)#isis hello-multiplier { multiple-value default } [level-1 level-2]	Configure the multiplier of sending Hello packets to neighbors in IS-IS.
3	Raisecom(config-vlanif-1)#isis csnp-interval { interval-value default } [level-1 level-2]	Configure the interval for sending CSNP packets at the specified level.

Step	Command	Description
4	<code>Raisecom(config-vlanif-1)#isis psnp-interval { interval-value default } [level-1 level-2]</code>	Configure the interval for sending PSNP packets at the specified level.
5	<code>Raisecom(config-isis-1)#lsp-max-lifetime { max-life-value default }</code>	Configure the interval for updating the link state packets of the route.
6	<code>Raisecom(config-isis-1)#lsp-generation max-interval { max-interval default } init-interval { int-interval default } incr-interval { incr-interval default } { } { level-1 level-2 }</code>	Configure the delay for generating LSPs by the specified IS-IS process.

3.11.9 Configuring IS-IS (IPv6) reliability

Configure IS-IS (IPv6) reliability for the device as below.

Step	Command	Description
1	<code>Raisecom(config-vlanif-1)#isis-ipv6 bfd { enable disable }</code>	Enable or disable IS-IS (IPv6) BFD on the specified interface, and establish a BFD session with default parameters.

3.11.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show isis config</code>	Show IS-IS configurations.
2	<code>Raisecom#show isis database</code>	Show the ISIS LSDB.
3	<code>Raisecom#show isis interface</code>	Show information or detailed information about IS-IS interfaces.
4	<code>Raisecom#show isis-ipv6 route</code>	Show IS-IS (IPv6) routing information.
5	<code>Raisecom#show isis neighbor</code>	Show information about IS-IS neighbors.

3.11.11 Maintenance

Maintain the ISCOM S3600 as below.

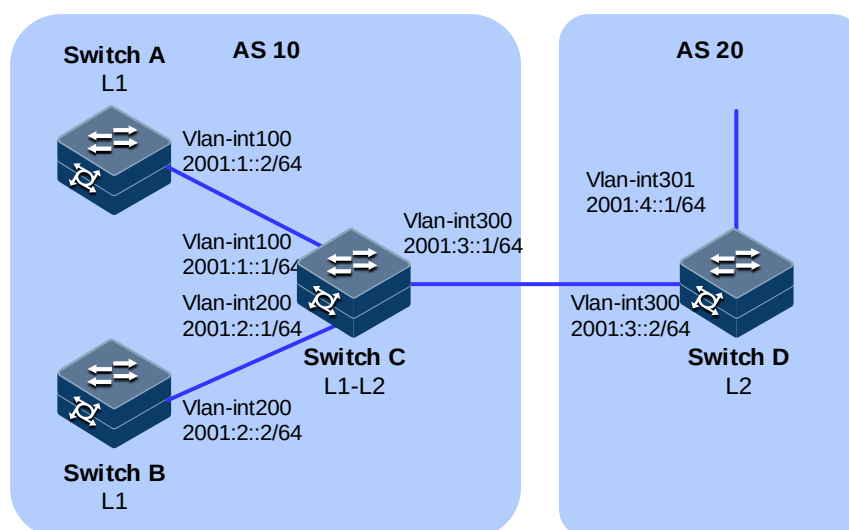
No.	Command	Description
1	<code>Raisecom(config-isis-1)#reset isis { isis-instance all }</code>	Reset all or the specified IS-IS instance.

3.11.12 Example for configuring basic functions of IS-IS (IPv6)

Networking requirements

As shown below, Switch A, Switch B, Switch C, and Switch D belong to the same AS. They are required to be reachable from each other on the IP network through IS-IS.

Switch A and Switch B are Level-1 switches. Switch D is the Level-2 switch. As the Level-1-2 switch, Switch C connects two ASs. The AS IDs of the Switch A, Switch B, and Switch C are 10 while that of Switch D is 20.



Configuration steps

Step 1 Configure IP addresses of interfaces.

Step 2 Configure IS-IS (IPv6).

Configure Switch A:

```

SwitchA#configure
SwitchA(config)#isis 1
SwitchA(config-isis-1)#is-type level-1
SwitchA(config-isis-1)#network-entity 10.0000.0000.0001.00
SwitchA(config-isis-1)#quit
SwitchA(config)#int vlan 100
SwitchA(config-vlanif-100)#isis enable 1
SwitchA(config-vlanif-100)#quit

```

Configure Switch B:

```
SwitchB#configure
SwitchB(config)#isis 1
SwitchB(config-isis-1)#is-type level-1
SwitchB(config-isis-1)#network-entity 10.0000.0000.0002.00
SwitchB(config-isis-1)#ipv6 enable topology standard
SwitchB(config-isis-1)#quit
SwitchB(config)#int vlan 200
SwitchB(config-vlanif-200)#isis enable 1
SwitchB(config-vlanif-200)#quit
```

Configure Switch C:

```
SwitchC#configure
SwitchC(config)#isis 1
SwitchC(config-isis-1)#network-entity 10.0000.0000.0003.00
SwitchC(config-isis-1)#ipv6 enable topology standard
SwitchC(config-isis-1)#quit
SwitchC(config)#int vlan 100
SwitchC(config-vlanif-100)#isis enable 1
SwitchC(config-vlanif-100)#isis enable 1
SwitchC(config-vlanif-100)#isis dis-priority 127
SwitchC(config-vlanif-100)#quit
SwitchC(config)#int vlan 200
SwitchC(config-vlanif-200)#isis enable 1
SwitchC(config-vlanif-100)#isis dis-priority 127
SwitchC(config-vlanif-200)#quit
SwitchC(config)#int vlan 300
SwitchC(config-vlanif-300)#isis enable 1
SwitchC(config-vlanif-100)#isis dis-priority 127
SwitchC(config-vlanif-300)#quit
```

Configure Switch D:

```
SwitchD#configure
SwitchD(config)#isis 1
SwitchD(config-isis-1)#is-type level-2
SwitchD(config-isis-1)#network-entity 20.0000.0000.0004.00
SwitchD(config-isis-1)#ipv6 enable topology standard
SwitchD(config-isis-1)#quit
SwitchD(config)#int vlan 300
SwitchD(config-vlanif-300)#isis enable 1
SwitchD(config-vlanif-300)#quit
```


Checking results

Use the following commands to show the ISIS database and LSP.

SwitchA(config)#**show isis database**

```

Database Information for IS-IS(1)

Level-1 Link State Database
The total number of isis 1 database is: 5
#   ID                               Level Seq          Checksum Lifetime Length
ATT/P/OL
1   0000.0000.0001.00-00            1     5             11192      836      83
0/0/0
2   0000.0000.0002.00-00            1     5             36943      832      83
0/0/0
3   0000.0000.0003.00-00            1     9             11945      818     154
1/0/0
4   0000.0000.0003.01-00            1     1             10925      812      52
0/0/0
5   0000.0000.0003.02-00            1     1             12708      818      52
0/0/0
L1 Database Count :5
L2 Database Count :0

```

SwitchB(config)##**show isis database**

```

Database Information for IS-IS(1)

Level-1 Link State Database
The total number of isis 1 database is: 5
#   ID                               Level Seq          Checksum Lifetime Length
ATT/P/OL
1   0000.0000.0001.00-00            1     5             11192      800      83
0/0/0
2   0000.0000.0002.00-00            1     5             36943      834      83
0/0/0
3   0000.0000.0003.00-00            1     9             11945      794     154
1/0/0
4   0000.0000.0003.01-00            1     1             10925      789      52
0/0/0
5   0000.0000.0003.02-00            1     1             12708      794      52
0/0/0
L1 Database Count :5
L2 Database Count :0

```

SwitchC(config)#**show isis database**

```

Database Information for IS-IS(1)

Level-1 Link State Database
The total number of isis 1 database is: 5
#   ID                               Level Seq          Checksum Lifetime Length
ATT/P/OL
1   0000.0000.0001.00-00            1     5             11192      898      83
0/0/0

```

```

2      0000.0000.0002.00-00    1      5          36943    906      83
0/0/0
3      0000.0000.0003.00-00    1      9          11945    893     154
1/0/0
4      0000.0000.0003.01-00    1      1          10925    887      52
0/0/0
5      0000.0000.0003.02-00    1      1          12708    893      52
0/0/0

```

Level-2 Link State Database

The total number of isis 1 database is: 3

#	ID	Level	Seq	Checksum	Lifetime	Length
6	0000.0000.0003.00-00	2	6	55969	841	143
7	0000.0000.0003.03-00	2	1	18060	821	52
8	0000.0000.0004.00-00	2	6	8674	792	116

ATT/P/OL
L1 Database Count :5
L2 Database Count :3

SwitchD(config)#show isis database

Database Information for IS-IS(1)

Level-2 Link State Database

The total number of isis 1 database is: 3

#	ID	Level	Seq	Checksum	Lifetime	Length
6	0000.0000.0003.00-00	2	6	55969	841	143
7	0000.0000.0003.03-00	2	1	18060	821	52
8	0000.0000.0004.00-00	2	6	8674	792	116

ATT/P/OL
L1 Database Count :0
L2 Database Count :3

Show the ISIS routes of each switch. There should be a default route in the routing table of the Level-1 switch, and its next hop is the Level-1-2 switch. There should be all Level-1 and Level-2 routes in the routing table of the Level-2 switch.

SwitchA(config)#show isis-ipv6 route

ISIS process 1	Level	Dst	Cost	Time	Next hop	MAC
Level-1	::/0				fe80::f2f1:f2ff:fef3:101	
f0f1:f2f3:0101	10	0:02:07				
Level-1	2001:1::/64				2001:1::2	
0000:0000:0000	10	0:03:08				

```

Level-1  2001:2::/64          fe80::f2f1:f2ff:fef3:101
f0f1:f2f3:0101  20      0:02:07
Level-1  2001:3::/64          fe80::f2f1:f2ff:fef3:101
f0f1:f2f3:0101  20      0:02:07
Total:4

```

SwitchB(config)#show isis-ipv6 route

```

ISIS process 1
Level    Dst                      Nexthop                      MAC
Cost    Time
Level-1  ::/0                          fe80::f2f1:f2ff:fef3:101
f0f1:f2f3:0101  10      0:02:46
Level-1  2001:1::/64                      fe80::f2f1:f2ff:fef3:101
f0f1:f2f3:0101  20      0:02:46
Level-1  2001:2::/64                      2001:2::2
0000:0000:0000  10      0:03:18
Level-1  2001:3::/64                      fe80::f2f1:f2ff:fef3:101
f0f1:f2f3:0101  20      0:02:46
Total:4

```

SwitchC(config)#show isis-ipv6 route

```

ISIS process 1
Level    Dst                      Nexthop                      MAC
Cost    Time
Level-1  2001:1::/64                      2001:1::1
0000:0000:0000  10      0:03:55
Level-1  2001:2::/64                      2001:2::1
0000:0000:0000  10      0:03:55
Level-1  2001:3::/64                      2001:3::1
0000:0000:0000  10      0:05:31
Level-2  2001:1::/64                      2001:1::1
0000:0000:0000  10      0:03:55
Level-2  2001:2::/64                      2001:2::1
0000:0000:0000  10      0:03:55
Level-2  2001:3::/64                      2001:3::1
0000:0000:0000  10      0:05:31
Level-2  2001:4::/64                      fe80::2e0:fcff:feda:53e9
00e0:fcda:53e9  10

```

3.12 RIP

3.12.1 Introduction

Function

Routing Information Protocol (RIP) is a relatively simple IGP, mainly used on smaller networks, such as campus networks and simpler regional networks. For more complex environments and large networks, RIP is generally not used.

Due to its relatively simple implementation and much easier configuration, maintenance, and management compared with OSPF and IS-IS, RIP still has a wide range of applications in practical networking.

Basic concepts of RIP

RIP is a protocol based on the Distance-Vector algorithm, which exchanges routing information through UDP packets and uses port number 520.

RIP uses hop count to measure the distance to the destination address, which is called the metric value. In RIP, the number of hops from a router to a network directly connected to it is 0, and the number of hops from a network reachable through a router is 1, and so on. To limit the convergence time, RIP specifies that the metric value should be an integer between 0 and 15, and the number of hops greater than or equal to 16 is defined as infinity. Infinity means that the destination network or host is unreachable. Due to this limitation, RIP is not suitable for application on large networks.

To improve performance and prevent routing loops, RIP supports horizon split and poison reverse.

RIP route database

Each router running RIP manages a route database that contains routing entries to all reachable destinations, which contain the following information:

- Destination address: the address of the host or network
- Next hop address: the IP address of the interface on the adjacent router that needs to be passed through to reach the destination
- Outbound interface: the outbound interface where this router forwards packets
- Metric value: cost of this router for reaching its destination
- Routing time: the time elapsing from the last update of a routing entry to the present. When a routing item is updated, the routing time is reset to 0.
- Route Tag: used to identify external routes, and able to flexibly control routing information in routing policies based on the route tag. For detailed information about routing policies, see section 3.14 Routing policy.

RIP mechanism for preventing routing loops

RIP advertises its neighbors of its own routing table, which may cause routing loops. This can be avoided through the following mechanisms:

- Counting to infinity: define a route with a metric value equal to 16 as unreachable. When a routing loop occurs, the metric value of a certain route will increase to 16, which is considered unreachable.
- Triggered Updates: RIP avoids the possibility of forming routing loops between multiple routers by triggered updates, and can accelerate the convergence speed of the network. When the metric value of a certain route changes, RIP immediately sends update packets to neighboring routers instead of waiting for the update period to expire.
- Split Horizon: the route learned by RIP from a certain interface is not sent back to neighboring routers from that interface. This not only reduces bandwidth consumption, but also prevents routing loops.
- Poison Reverse: After RIP learns a route from an interface, it configures the metric value of the route to 16 (unreachable), and sends the route back to the neighboring router from

the receiving interface. This method can clear useless information in the other party's routing table.

RIP versions

RIP has two versions: RIP-1 and RIP-2.

RIP-1 is a Classful Routing Protocol that only supports broadcasting protocol packets. RIP-1 packets cannot carry mask information and can only recognize routes in natural network segments, such as A, B, and C. Therefore, RIP-1 does not support Discontinuous Subnets.

RIP-2 is a Classless Routing Protocol, which has the following advantages compared with RIP-1:

- Support routing tags, thus flexibly controlling routes in routing policies based on these markers.
- The packet carries mask information and supports route aggregation and Classless Inter Domain Routing (CIDR).
- Support specifying the next hop and selecting the optimal next hop address on the broadcasting network.
- Support multicast routers to send update packets. Only RIP-2 routers can receive update packets, thus reducing resource consumption.
- Support verifying protocol packets in two methods to enhance security: plain text and MD5.

RIP-2 has two packet transmission methods: broadcast and multicast. By default, multicast transmission is used to send packets, and the multicast IP address is 224.0.0.9. When the interface runs in RIP-2 broadcast mode, it can also receive RIP-1 packets.

3.12.2 Preparing for configurations

Scenario

After basic functions of RIP are configured, the Layer 3 network can be constructed through RIP.

Prerequisites

Configure IP addresses of interfaces so that neighboring nodes are reachable at the network layer.

3.12.3 Default configurations

Default configurations of RIP are as below.

Function	Default value
SNMP Trap	Disable

3.12.4 Configuring basic functions of RIP

Configure basic functions of RIP for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#rip [<i>process-id</i>] [vpn-instance <i>NAME</i>]	Create a RIP process, and enter the RIP process configuration view.
3	Raisecom(config-rip-1)#network <i>network-address</i>	Enable RIP in the specified network segment.
4	Raisecom(config-rip-1)#quit	Exit the current view. Enter global configuration mode.
5	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter the interface view. The interface is a Layer 3 physical interface or VLAN interface.
6	Raisecom(config-vlanif-1)#rip <i>process-id</i> enable	Enable RIP on the interface.
7	Raisecom(config-vlanif-1)#rip passive-interface { enable disable }	Configure the interface as the passive interface. By default, this function is disabled, and all interfaces are allowed to send route update packets. If this function is enabled, all interfaces do not send RIP packets.
8	Raisecom(config-vlanif-1)#rip send-version { no-send v1 v1-compatible v2 }	Configure the RIP sending version of the interface.
9	Raisecom(config-vlanif-1)#rip receive-version { v1 v2 v1v2 no-receive }	Configure the RIP receiving version of the interface.

3.12.5 Configuring RIP routing information control

Configure RIP routing information control for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#rip [<i>process-id</i>] [vpn-instance <i>NAME</i>]	Create a RIP process, and enter the RIP process configuration view.
3	Raisecom(config-rip-1)#summary { enable disable }	Enable automatic RIP-2 route aggregation. By default, it is disabled.
4	Raisecom(config-rip-1)#default-route originate { cost (<0-15> default) tag (<0-65535> default)}	Configure RIP to advertise the default route. By default, RIP does not advertise the default route.

Step	Command	Description
5	<code>Raisecom(config-rip-1)#default-route learning (enable disable)</code>	Configure RIP to learn the default route. By default, RIP learns the default route.
6	<code>Raisecom(config-rip-1)#import-route { rip isis ospf } <1-65535> { cost (<0-15> default) } route-policy NAME}</code> <code>Raisecom(config-rip-1)#import-route { static connect ospf bgp isis rip } { cost (<0-15> default) route-policy NAME}</code>	Configure the device to redistribute external routes.
7	<code>Raisecom(config-rip-1)#default-cost (<0-15> default)</code>	Configure the default metric value of redistributed routes. By default, it is 1.
8	<code>Raisecom(config-rip-1)#filter-policy import route-policy NAME</code>	Configure the device to filter received routes in the RIP process. This command filters RIP routes received from neighbors, discards failed routes, and does not advertise failed routes to neighbors.
9	<code>Raisecom(config-rip-1)#filter-policy export route-policy NAME</code> <code>Raisecom(config-rip-1)#filter-policy export { rip isis ospf } <1-65535> route-policy NAME</code> <code>Raisecom(config-rip-1)#filter-policy export { rip isis ospf } <1-65535> route-policy NAME</code> <code>Raisecom(config-rip-1)#filter-policy export { static connect ospf bgp isis rip } route-policy NAME</code>	Configure the device to filter routes to be advertised in the RIP process. This command filters all routes advertised by the device, including the routes redistributed by the import-route command and RIP routes learnt from neighbors.
10	<code>Raisecom(config-rip-1)#preference (<1-255> default)</code>	Configure the priority of RIP routes. By default, it is 100.
11	<code>Raisecom(config-rip-1)#quit</code>	Exit the current view. Enter global configuration mode.
12	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter the interface view. The interface is a Layer 3 physical interface or VLAN interface.

Step	Command	Description
13	Raisecom(config-vlanif-1)#rip metric-in (<0-15> default)	Configure the metric value for the interface to receive RIP routes. By default, it is 0.
14	Raisecom(config-vlanif-1)#rip metric-out (<1-15> default)	Configure the metric value for the interface to advertise RIP routes. By default, it is 0.
15	Raisecom(config-vlanif-1)#rip default-metric (<0-15> default)	Configure the metric value of the default route advertised by the interface. By default, it is 0.
16	Raisecom(config-vlanif-1)#rip summary-address <i>A.B.C.D A.B.C.D</i> [avoid-feedback]	Configure route aggregation on the interface.
17	Raisecom(config-vlanif-1)#rip filter-policy (export import) route-policy <i>NAME</i>	Configure the interface to filter routes to be advertised and received routes.

3.12.6 Adjusting and optimizing the RIP network

Adjust and optimize the RIP network for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#rip [<i>process-id</i>] [vpn-instance <i>NAME</i>]	Create a RIP process, and enter the RIP process configuration view.
3	Raisecom(config-rip-1)#rip timer (<10-3600> default) (<40-14400> default) (<40-14400> default)	Configure RIP timers. By default, the Garbage-collect timer is 120s, the Timeout timer is 180s, the Update timer is 30s.
4	Raisecom(config-rip-1)#check-zero { enable disable }	Configure the zero domain check of RIP-1 packets. By default, it is enabled.
5	Raisecom(config-rip-1)#validate-source-address { enable disable }	Enable the function of check the source IP address of received RIP route updating packets. By default, it is enabled.
6	Raisecom(config-rip-1)#neighbor <i>neighbor-address</i>	Configure RIP neighbors.
7	Raisecom(config-rip-1)#quit	Exit the current view. Enter global configuration mode.

Step	Command	Description
8	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter the interface view. The interface is a Layer 3 physical interface or VLAN interface.
9	<code>Raisecom(config-vlanif-1)#rip split-horizon { enable disable }</code>	Enable horizon split on the interface. By default, it is enabled.
10	<code>Raisecom(config-vlanif-1)#rip poison-reverse { enable disable }</code>	Enable poison reverse on the interface. By default, it is disabled.
11	<code>Raisecom(config-vlanif-1)#rip authentication { md5 md5- compatible } <1-255> (cipher plain) KEY Raisecom(config-vlanif-1)#rip authentication simple { cipher plain) KEY</code>	Configure RIP interface authentication.
12	<code>Raisecom(config-vlanif-1)#rip pkt-transmit interval (<10- 500> default) number (<1- 50> default)</code>	Configure the rate for sending RIP packets. By default, the interval for sending RIP packets is 200ms, and up to 20 RIP packets are sent at a time.
13	<code>Raisecom(config-vlanif-1)#rip bfd { enable disable }</code>	Enable RIP BFD association on the interface.

3.12.7 Checking results

Use the following commands to check configuration results.

Step	Command	Description
1	<code>Raisecom#show rip config</code>	Show all RIP configurations.
2	<code>Raisecom#show rip resource</code>	Show information about RIP resources.
3	<code>Raisecom#show rip [process process-id]</code>	Show information about RIP processes.
4	<code>Raisecom#show rip neighbor [process process-id address neighbor-address]</code>	Show information about RIP neighbors.
5	<code>Raisecom#show rip interface [process process-id vlan <1- 4094>]</code>	Show information about RIP interfaces.
6	<code>Raisecom#show rip bfd session [process process-id]</code>	Show information about RIP BFD sessions.

Step	Command	Description
7	Raisecom#show rip { database route } [process process-id dest dest-address/dest-mask neighbor neighbor-address]	Show information about RIP routes. Use the database parameter to show information about the database. Use the route parameter to show information about effective routes.

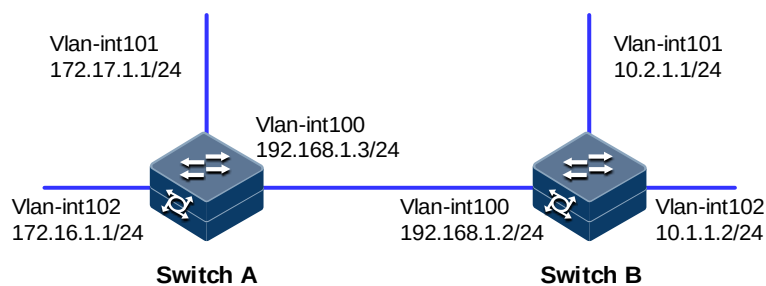
3.12.8 Example for configuring basic functions of RIP

Networking requirements

As shown below, enable RIP on all interfaces on Switch A and Switch B, and interconnect them through RIP-2.

Configure the policy for advertising routes on Switch B to filter out route 10.2.1.0/24 from routes advertised to Switch A. Configure the policy for receiving routes on Switch B to receive route 172.16.1.0/24 only by Switch B.

Figure 3-50 Networking with basic functions of RIP



Configuration steps

- Step 1 Configure IP addresses of interfaces.
- Step 2 Configure basic functions of RIP. The following section uses two different modes for enabling RIP. Choose one as required in actual situations.

Configure Switch A. Enable RIP in the specified network segment.

```

SwitchA#configure
SwitchA(config)#rip 1
SwitchA(config-rip-1)#network 172.16.0.0
SwitchA(config-rip-1)#network 172.17.0.0
SwitchA(config-rip-1)#quit
  
```

Configure Switch B. Enable RIP on the specified interface.

```

SwitchB#configure
  
```

```
SwitchA(config)#rip 1
SwitchA(config-rip-1)#network 172.16.0.0
SwitchA(config-rip-1)#quit
SwitchA(config)#interface vlan 100
SwitchA(config-vlanif-100)#rip 1 enable
SwitchA(config-vlanif-100)#quit
SwitchA(config)#interface vlan 101
SwitchA(config-vlanif-101)#rip 1 enable
SwitchA(config-vlanif-101)#quit
SwitchA(config)#interface vlan 102
SwitchA(config-vlanif-102)#rip 1 enable
SwitchA(config-vlanif-102)#quit
```

Step 3 Check configuration results.

Switch A:

Use the following command to show information about interfaces:

```
SwitchA#show rip interface
```

Interface	Process	State	Addr/Prefix	Send-Version	Recv-Version
vlan-102	1	Up	172.16.1.1/24	RIPv1 Compatible	RIPv1 and RIPv2
vlan-101	1	Up	172.17.1.1/24	RIPv1 Compatible	RIPv1 and RIPv2
vlan-100	1	Up	192.168.1.3/24	RIPv1 Compatible	RIPv1 and RIPv2

Use the following command to show information about neighbors:

```
SwitchA#show rip neighbor
```

Process	Address	Interface	Domain	Version	Update-Time	RecvBadPkt	RecvBadRoute	Key
1	192.168.1.2	vlan-100		2	00:06:30	0		

The total number of rip neighbor is: 1

Switch B:

```
SwitchB#show rip neighbor
```

Process	Address	Interface	Domain	Version	Update-Time	RecvBadPkt	RecvBadRoute	Key
1	192.168.1.3	vlan-100		2	00:07:08	0		

```
-----
-----
The total number of rip neighbor is: 1
```

Use the following command to show information about the database:

SwitchA#show rip database

Process	Destination	Netmask	Gateway	Metric	Age	State
Proto	Tag					
1	10.1.1.0	255.255.255.0	192.168.1.2	1	18	
ACTIVE	rip 0					
1	10.2.1.0	255.255.255.0	192.168.1.2	1	18	
ACTIVE	rip 0					
1	172.16.1.0	255.255.255.0	172.16.1.1	0	0	
ACTIVE	rip 0					
1	172.17.1.0	255.255.255.0	172.17.1.1	0	0	
ACTIVE	rip 0					
1	192.168.1.0	255.255.255.0	192.168.1.3	0	0	
ACTIVE	rip 0					

Total : 5

Switch B:

Use the following command to show information about interfaces:

SwitchA#show rip interface

Interface	Process	State	Addr/Prefix	Send-Version	Recv-Version
vlan-102	1	Up	172.16.1.1/24	RIPv1 Compatible	RIPv1 and RIPv2
vlan-101	1	Up	172.17.1.1/24	RIPv1 Compatible	RIPv1 and RIPv2
vlan-100	1	Up	192.168.1.3/24	RIPv1 Compatible	RIPv1 and RIPv2

Use the following command to show information about neighbors:

SwitchA#show rip neighbor

Process	Address	Interface	Domain	Version	Update-Time
RecvBadPkt	RecvBadRoute	Key			

```

-----
-----
1      192.168.1.2      vlan-100      2      00:09:41      0
0      0
-----
-----

```

The total number of rip neighbor is: 1

Use the following command to show information about the database:

```

SwitchA#show rip database
  Process  Destination      Netmask      Gateway      Metric  Age      State
  Proto   Tag
-----
-----
1      10.1.1.0      255.255.255.0  192.168.1.2   1      23
ACTIVE  rip  0
1      10.2.1.0      255.255.255.0  192.168.1.2   1      23
ACTIVE  rip  0
1      172.16.1.0    255.255.255.0  172.16.1.1    0      0
ACTIVE  rip  0
1      172.17.1.0    255.255.255.0  172.17.1.1    0      0
ACTIVE  rip  0
1      192.168.1.0   255.255.255.0  192.168.1.3   0      0
ACTIVE  rip  0
-----
-----
Total : 5

```

Configure RIP route filtering.

```

SwitchB(config)#ip prefix-list import index 10 permit 172.16.1.0/24
SwitchB(config)#ip prefix-list export index 10 permit 10.1.1.0/24
SwitchB(config)#route-policy import permit node 1
SwitchB(config-route-policy-import-1)#match destination ip-prefix-list
import
SwitchB(config-route-policy-import-1)#quit
SwitchB(config)#route-policy export permit node 1
SwitchB(config-route-policy-export-1)#match destination ip-prefix-list
export
SwitchB(config-route-policy-import-1)#quit
SwitchB(config)#rip 1
SwitchB(config-rip-1)#filter-policy import route-policy import
SwitchB(config-rip-1)#filter-policy export route-policy export

```

Check configuration results.

Switch A:

Use the following command to show information about the database:

```
SwitchA#show rip database
Process Destination Netmask Gateway Metric Age State
Proto Tag
-----
1 10.1.1.0 255.255.255.0 192.168.1.2 1 18
ACTIVE rip 0
1 172.16.1.0 255.255.255.0 172.16.1.1 0 0
ACTIVE rip 0
1 172.17.1.0 255.255.255.0 172.17.1.1 0 0
ACTIVE rip 0
1 192.168.1.0 255.255.255.0 192.168.1.3 0 0
ACTIVE rip 0
-----
Total : 4
```

Switch B:

Use the following command to show information about the database:

```
SwitchB#show rip database
Process Destination Netmask Gateway Metric Age State
Proto Tag
-----
1 10.1.1.0 255.255.255.0 10.1.1.2 0 0 ACTIVE
rip 0
1 10.2.1.0 255.255.255.0 10.2.1.2 0 0 ACTIVE
rip 0
1 172.16.1.0 255.255.255.0 192.168.1.3 1 20
ACTIVE rip 0
1 192.168.1.0 255.255.255.0 192.168.1.2 0 0
ACTIVE rip 0
-----
```

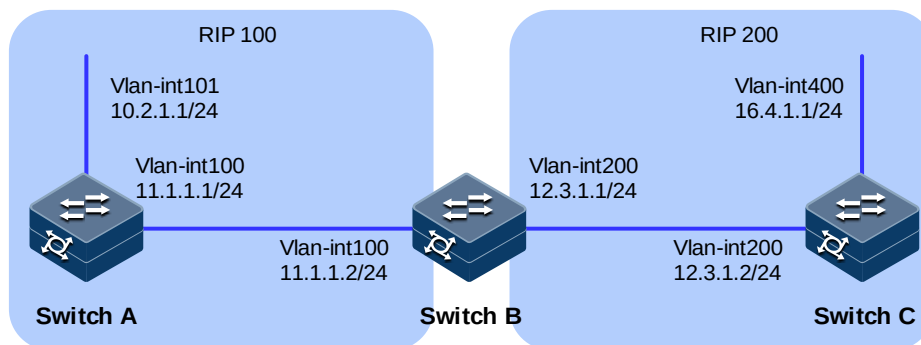
3.12.9 Example for configuring RIP to redistribute external routes

Networking requirements

Run two RIP processes, RIP 100 and RIP200, on Switch B. Switch B exchanges routing information with Switch A through RIP 100, and with Switch C through RIP 200.

Configure RIP process 200 on the Switch B to redistribute external routes, directly connected routes, and the route of RIP process 100. This allows Switch C to learn routes to 10.2.1.0/24 and 11.1.1.0/24, but disallows Switch A to learn routes to 12.3.1.0/24 and 16.4.1.0/24.

Figure 3-51 Networking with RIP to redistributing external routes



Configuration steps

Step 1 Configure IP addresses of interfaces.

Step 2 Configure RIP on devices.

Configure Switch A.

```
SwitchA#configure
SwitchA(config)#rip 100
SwitchA(config-rip-100)#network 10.0.0.0
SwitchA(config-rip-100)#network 11.0.0.0
SwitchA(config-rip-100)#quit
```

Configure Switch B.

```
SwitchB#configure
SwitchB(config)#rip 100
SwitchB(config-rip-100)#network 11.0.0.0
SwitchB(config-rip-100)#quit
SwitchB(config)#rip 200
SwitchB(config-rip-200)#network 12.0.0.0
SwitchB(config-rip-1)#quit
```

Configure Switch C.

```
SwitchC#configure
SwitchC(config)#rip 200
SwitchC(config-rip-200)#network 12.0.0.0
SwitchC(config-rip-200)#network 16.0.0.0
SwitchC(config-rip-200)#quit
```

Check configuration results.

Use the following command to show information about the RIP database on Switch C.

```
SwitchC#show rip database
Process Destination Netmask Gateway Metric Age State
Proto Tag
-----
200 12.3.1.0 255.255.255.0 12.3.1.2 0 0 ACTIVE
rip 0
200 16.4.1.0 255.255.255.0 16.4.1.1 0 0 ACTIVE
rip 0
-----
```

Step 3 Configure devices to redistribute routes.

Configure RIP process 200 of Switch B to redistribute routes of RIP process 100.

```
SwitchB#configure
SwitchB(config)#rip 200
SwitchB(config-rip-200)#import-route rip 100
SwitchB(config-rip-200)#quit
```

Check configuration results.

Use the following command to show information about the RIP database on Switch C.

```
SwitchC#show rip database
Process Destination Netmask Gateway Metric Age State
Proto Tag
-----
200 10.2.1.0 255.255.255.0 12.3.1.1 2 1 ACTIVE
rip 0
200 11.1.1.0 255.255.255.0 12.3.1.1 2 1 ACTIVE
rip 0
200 12.3.1.0 255.255.255.0 12.3.1.2 0 0 ACTIVE
rip 0
200 16.4.1.0 255.255.255.0 16.4.1.1 0 0 ACTIVE
rip 0
-----
Total : 4
```


3.13 RIPng

3.13.1 Introduction

Function

RIP next generation (RIPng) is an extension of the RIP-2 on the original IPv4 network. Most concepts of RIP can be applied to RIPng.

To be applied to IPv6 networks, RIPng has made the following modifications to the original RIP:

- UDP port number: use UDP port 521 to send and receive routing information.
- Multicast address: use FF02:: 9 as the multicast IP address of the RIPng router within the local range of the link.
- Prefix length: the destination address uses a prefix length of 128 bits.
- Next hop address: use a 128-bit IPv6 address.
- Source address: use the link local address FE80::/10 as the source address to send RIPng routing information update packets.

RIPng working mechanism

RIPng is a protocol based on the Distance Vector algorithm. It exchanges routing information through UDP packets and uses port number 521.

RIPng uses hop count to measure the distance to the destination address (also known as metric or cost). In RIPng, the number of hops from one router to its directly connected network is 0, and the number of hops from a router connected to it to another network is 1, and so on. When the hop count is greater than or equal to 16, the destination network or host is defined as unreachable.

RIPng sends route update packets every 30s. If no route update packet is received from the network neighbor within 180s, RIPng marks all routes learned from the neighbor as unreachable. If no routing update packet is received from the neighbor within 120s, RIPng deletes these routes from the routing table.

To improve performance and avoid routing loops, RIPng supports both horizon split and poison reverse. In addition, RIPng can also redistribute routes from other routing protocols.

Each router running RIP manages a route database that contains routing entries to all reachable destinations, which contain the following information:

- Destination address: the address of the host or network
- Next hop address: the IP address of the interface on the adjacent router that needs to be passed through to reach the destination
- Outbound interface: the outbound interface where this router forwards packets
- Metric value: cost of this router for reaching its destination
- Routing time: the time elapsing from the last update of a routing entry to the present. When a routing item is updated, the routing time is reset to 0.
- Route Tag: used to identify external routes, and able to flexibly control routing information in routing policies based on the route tag.

RIPng packet

RIPng has two types of packets: Request packet and Response packet.

When the RIPng router starts or needs to update some routing entries, it will send a Request packet to request the required routing information from neighbors. Usually, request packets are sent in multicast mode.

The Response packet contains information about the local routing table and is generally generated in the following situations:

- Response to a request packet
- Regularly sending update packets
- Triggering updates when routes changes

The RIPng router that receives the Request packet sends it back to the requesting router in the form of a Response packet.

The router that receives the Response packet updates its RIPng routing table. To ensure the accuracy of route, the RIPng router performs validity checks on the received Response packets, such as whether the source IPv6 address is a link local address and whether the port number is correct. It ignores the packets that fail in the check.

3.13.2 Preparing for configurations

Scenario

After basic functions of RIPng are configured, the IPv6 Layer 3 network can be constructed through RIP.

Prerequisites

Enable IPv6 and configure IPv6 addresses of interfaces so that neighboring nodes are reachable at the network layer.

3.13.3 Configuring basic functions of RIPng

Configure basic functions of RIPng for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ripng [process-id] [vpn- instance NAME]	Create a RIPng process, and enter the RIP process configuration view.
4	Raisecom(config-rip-1)#quit	Exit the current view. Enter global configuration mode.
5	Raisecom(config)#interface interface-type interface- number	Enter the interface view. The interface is a Layer 3 physical interface or VLAN interface.
6	Raisecom(config-vlanif- 1)#ripng process-id enable	Enable RIPng on the interface.

3.13.4 Configuring RIPng route

Configure RIPng route for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ripng [<i>process-id</i>] [<i>vpn-instance NAME</i>]	Create a RIPng process, and enter the RIP process configuration view.
3	Raisecom(config-ripng-1)#default-route originate { enable disable }	Configure RIPng to advertise the default route. By default, RIPng does not advertise the default route.
4	Raisecom(config-ripng-1)#default-route learning { enable disable }	Configure RIPng to learn the default route. By default, RIPng learns the default route.
5	Raisecom(config-ripng-1)#import-route { ripng isis ospf } <1-65535> { cost (<0-15> default) route-policy NAME } Raisecom(config-ripng-1)#import-route { static connect bgp ospf isis ripng } { cost (<0-15> default) route-policy NAME }	Configure the device to redistribute external routes.
6	Raisecom(config-ripng-1)#default-cost (<0-15> default)	Configure the default metric value of redistributed routes. By default, it is 1.
7	Raisecom(config-ripng-1)#filter-policy import route-policy NAME	Configure the device to filter received routes in the RIP process. This command filters RIP routes received from neighbors, discards failed routes, and does not advertise failed routes to neighbors.
8	Raisecom(config-ripng-1)#filter-policy export route-policy NAME Raisecom(config-ripng-1)#filter-policy export { ripng isis ospf } <1-65535> route-policy NAME Raisecom(config-ripng-1)#filter-policy export { static connect ospf bgp isis ripng } route-policy NAME	Configure the device to filter routes to be advertised in the RIP process. This command filters all routes advertised by the device, including the routes redistributed by the import-route command and RIP routes learnt from neighbors.
9	Raisecom(config-ripng-1)#preference (<1-255> default)	Configure the priority of RIPng routes. By default, it is 100.

Step	Command	Description
10	Raisecom(config-ripng-1)#quit	Exit the current view. Enter global configuration mode.
11	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter the interface view. The interface is a Layer 3 physical interface or VLAN interface.
12	Raisecom(config-vlanif-1)#ripng metric-in (<0-15> default)	Configure the metric value for the interface to receive RIPng routes. By default, it is 0.
13	Raisecom(config-vlanif-1)#rip metric-out (<1-15> default)	Configure the metric value for the interface to advertise RIPng routes. By default, it is 0.
14	Raisecom(config-vlanif-1)#ripng default-route { only originate } { cost (<1-15> default) }	Configure the interface to generate a default route to the RIPng routing domain.
15	Raisecom(config-vlanif-1)#ripng summary-address <i>X:X::X:X</i> <0-128> { avoid-feedback }	Configure route aggregation on the interface.
16	Raisecom(config-vlanif-1)#ripng filter-policy { export import } route-policy <i>NAME</i>	Configure the interface to filter routes to be advertised and received routes.

3.13.5 Adjusting and optimizing the RIPng network

Adjust and optimize the RIPng network for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ripng [<i>process-id</i>] [vpn-instance <i>NAME</i>]	Create a RIPng process, and enter the RIP process configuration view.
3	Raisecom(config-ripng-1)#timers update (<30-500> default) expire (<120-2000> default) garbage (<120-2000> default)	Configure RIPng timers. By default, the Garbage-collect timer is 120s, the Timeout timer is 180s, the Update timer is 30s.
4	Raisecom(config-ripng-1)#check-zero (enable disable)	Configure the zero domain check of RIPng packets. By default, it is enabled.
5	Raisecom(config-rip-1)#quit	Exit the current view. Enter global configuration mode.

Step	Command	Description
6	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter the interface view. The interface is a Layer 3 physical interface or VLAN interface.
7	Raisecom(config-vlanif-1)#ripng split-horizon { enable disable }	Enable horizon split on the interface. By default, it is enabled.
8	Raisecom(config-vlanif-1)#ripng poison-reverse { enable disable }	Enable poison reverse on the interface. By default, it is disabled.
9	Raisecom(config-vlanif-1)#ripng pkt-transmit interval { <10-500> default } number (<1-50> default)	Configure the rate for sending RIPng packets. By default, the interval for sending RIPng packets is 200ms, and up to 10 RIPng packets are sent at a time.
10	Raisecom(config-vlanif-1)#ripng bfd { enable disable }	Enable RIPng BFD association on the interface.

3.13.6 Checking results

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom#show ripng config	Show all RIPng configurations.
2	Raisecom#show ripng resource	Show information about RIPng resources.
3	Raisecom#show ripng [process <i>process-id</i>]	Show information about RIPng processes.
4	Raisecom#show ripng neighbor [process <i>process-id</i> address <i>neighbor-address</i>]	Show information about RIPng neighbors.
5	Raisecom#show ripng interface [process <i>process-id</i> vlan <1-4094>]	Show information about RIPng interfaces.
6	Raisecom#show ripng bfd session [process <i>process-id</i>]	Show information about RIPng BFD sessions.
7	Raisecom#show ripng { database route } [process <i>process-id</i> dest <i>dest-address/dest-mask</i> neighbor <i>neighbor-address</i>]	Show information about RIPng routes. Use the database parameter to show information about the database. Use the route parameter to show information about effective routes.

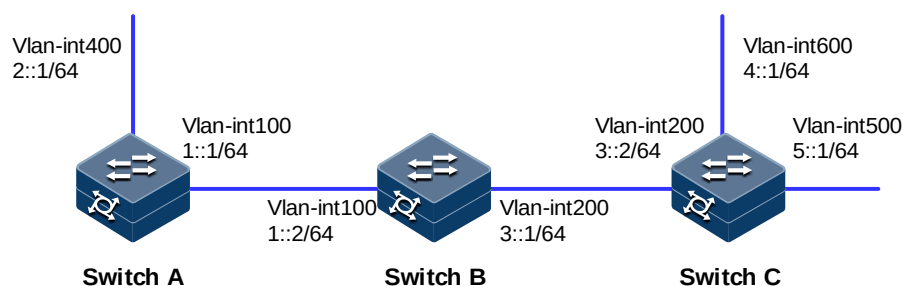
3.13.7 Example for configuring basic functions of RIPng

Networking requirements

Switch A, Switch B, and Switch C are connected and learn IPv6 routing information on the network through RIPng.

Configure Switch B to filter the received route (2:: / 64) from Switch A to prevent it from being added to the routing table of the RIPng process on Switch B. The route advertised to Switch A is only (4:: / 64).

Figure 3-52 Networking with basic functions of RIP



Configuration steps

Step 1 Configure IPv6 addresses of interfaces.

Step 2 Configure basic functions of RIPng.

Configure Switch A.

```
SwitchA#configure
SwitchA(config)#ripng 1
SwitchA(config-ripng-1)#quit
SwitchA(config)#interface vlan 100
SwitchA(config-vlanif-100)#ripng 1 enable
SwitchA(config-vlanif-100)#quit
SwitchA(config)#interface vlan 400
SwitchA(config-vlanif-400)#ripng 1 enable
SwitchA(config-vlanif-400)#quit
```

Configure Switch B.

```
SwitchB#configure
SwitchB(config)#ripng 1
SwitchB(config-ripng-1)#quit
SwitchB(config)#interface vlan 100
SwitchB(config-vlanif-100)#ripng 1 enable
SwitchB(config-vlanif-100)#quit
SwitchB(config)#interface vlan 200
SwitchB(config-vlanif-200)#ripng 1 enable
```

```
SwitchB(config-vlanif-200)#quit
```

Configure Switch C.

```
SwitchC#configure
SwitchC(config)#ripng 1
SwitchC(config-ripng-1)#quit
SwitchC(config)#interface vlan 200
SwitchC(config-vlanif-200)#ripng 1 enable
SwitchC(config-vlanif-200)#quit
SwitchC(config)#interface vlan 500
SwitchC(config-vlanif-500)#ripng 1 enable
SwitchC(config-vlanif-500)#quit
SwitchC(config)#interface vlan 600
SwitchC(config-vlanif-600)#ripng 1 enable
SwitchC(config-vlanif-600)#quit
```

Step 3 Check configuration results.

Switch A:

Use the following command to show information about RIPng interfaces:

```
SwitchA#show ripng interface
```

Interface	Process	State	Passive	Address
vlan-100	1	Up	Disable	fe80::f2f1:f2ff:fef3:101
vlan-400	1	Up	Disable	fe80::f2f1:f2ff:fef3:101

Use the following command to show information about RIPng neighbors:

```
SwitchA#show ripng neighbor
```

Process	Address	Version	LastUpdate	Interface
InbadPacket	InbadRoute			
1	fe80::f2f1:f2ff:fef3:201	Version1	00:06:55	vlan-100
0	0			

Use the following command to show information about RIPng routes:

```
SwitchA#show ripng database
```

Process	Prefix/Prefixlen	Nexthop	Metric	Age
State	Protocol	Tag		

1	1::/64		fe80::f2f1:f2ff:fe3:101	0	0
Active	ripng	0			
1	2::/64		fe80::f2f1:f2ff:fe3:101	0	0
Active	ripng	0			
1	3::/64		fe80::f2f1:f2ff:fe3:201	1	14
Active	ripng	0			
1	4::/64		fe80::f2f1:f2ff:fe3:201	2	14
Active	ripng	0			
1	5::/64		fe80::f2f1:f2ff:fe3:201	2	14
Active	ripng	0			

Total : 5					

Switch B:

Use the following command to show information about RIPng interfaces:

SwitchB#show ripng interface

Interface	Process	State	Passive	Address

vlan-100	1	Up	Disable	fe80::f2f1:f2ff:fe3:201
vlan-200	1	Up	Disable	fe80::f2f1:f2ff:fe3:201

Use the following command to show information about RIPng neighbors:

SwitchB#show ripng neighbor

Process	Address	Version	LastUpdate	Interface

InbadPacket	InbadRoute			
1	fe80::f2f1:f2ff:fe3:101	version1	00:07:35	vlan-100
0	0			
1	fe80::f2f1:f2ff:fe3:301	version1	00:07:21	vlan-200
0	0			

Use the following command to show information about RIPng routes:

SwitchB#show ripng database

Process	Prefix/Prefixlen	NextHop	Metric	Age

State	Protocol	Tag		

1	1::/64	fe80::f2f1:f2ff:fe3:201	0	0
Active	ripng	0		


```

1      2::/64      fe80::f2f1:f2ff:fe3:101      1      1
Active ripng      0
1      3::/64      fe80::f2f1:f2ff:fe3:201      0      0
Active ripng      0
1      4::/64      fe80::f2f1:f2ff:fe3:301      1      9
Active ripng      0
1      5::/64      fe80::f2f1:f2ff:fe3:301      1      9
Active ripng      0

```

```

-----
-----
Total : 5

```

Switch C:

Use the following command to show information about RIPng interfaces:

SwitchC#show ripng interface

```

Interface      Process      State      Passive      Address
-----
vlan-200      1          Up        Disable      fe80::f2f1:f2ff:fe3:301
vlan-500      1          Up        Disable      fe80::f2f1:f2ff:fe3:301
vlan-600      1          Up        Disable      fe80::f2f1:f2ff:fe3:301

```

Use the following command to show information about RIPng neighbors:

SwitchC#show ripng neighbor

```

Process      Address      Version      LastUpdate      Interface
InbadPacket  InbadRoute
1          fe80::f2f1:f2ff:fe3:201      version1      00:08:01      vlan-200
0          0

```

Use the following command to show information about RIPng routes:

SwitchC#show ripng database

```

Process      Prefix/Prefixlen      Nexthop      Metric      Age
State      Protocol      Tag
-----
1      1::/64      fe80::f2f1:f2ff:fe3:201      1      27
Active ripng      0
1      2::/64      fe80::f2f1:f2ff:fe3:201      2      27
Active ripng      0
1      3::/64      fe80::f2f1:f2ff:fe3:301      0      0
Active ripng      0

```

```

1      4::/64      fe80::f2f1:f2ff:fef3:301    0    0
Active ripng      0
1      5::/64      fe80::f2f1:f2ff:fef3:301    0    0
Active ripng      0

```

```

-----
Total : 5

```

Step 4 Configure route filtering.

```

SwitchB(config)#ipv6 prefix-list export index 10 permit 4::/64
SwitchB(config)#ipv6 prefix-list import index 10 permit 2::/64
SwitchB(config)#route-policy export permit node 1
SwitchB(config-route-policy-export-1)#match destination ipv6-prefix-list
export
SwitchB(config-route-policy-export-1)#quit
SwitchB(config)#route-policy import deny node 1
SwitchB(config-route-policy-import-1)#match destination ipv6-prefix-list
import
SwitchB(config-route-policy-import-1)#quit
SwitchB(config)#route-policy import permit node 2
SwitchB(config-route-policy-import-2)#quit
SwitchB(config)#ripng 1
SwitchB(config-ripng-1)#filter-policy import route-policy import
SwitchB(config-ripng-1)#filter-policy export route-policy export

```

Check configuration results.

Use the following command to show information about the RIPng routing table of Switch A and Switch B:

```
SwitchA#show ripng database
```

Process	Prefix/Prefixlen	Nexthop	Metric	Age
State	Protocol	Tag		

```

-----
1      1::/64      fe80::f2f1:f2ff:fef3:101    0    0
Active ripng      0
1      2::/64      fe80::f2f1:f2ff:fef3:101    0    0
Active ripng      0
1      4::/64      fe80::f2f1:f2ff:fef3:201    2    12
Active ripng      0

```

```

-----
Total : 3

```

```
SwitchB#show ripng database
```

Process	Prefix/Prefixlen	Nexthop	Metric	Age
State	Protocol	Tag		

1	1::/64		fe80::f2f1:f2ff:fe3:201	0	0
Active	ripng	0			
1	3::/64		fe80::f2f1:f2ff:fe3:201	0	0
Active	ripng	0			
1	4::/64		fe80::f2f1:f2ff:fe3:301	1	19
Active	ripng	0			
1	5::/64		fe80::f2f1:f2ff:fe3:301	1	19
Active	ripng	0			
Total : 4					

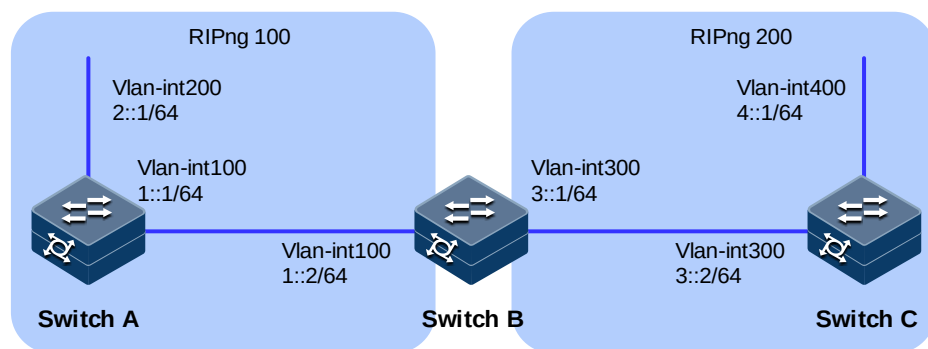
3.13.8 Example for configuring RIPng to redistribute external routes

Networking requirements

Run two RIPng processes, RIPng 100 and RIPng200, on Switch B. Switch B exchanges routing information with Switch A through RIPng 100, and with Switch C through RIPng 200.

Configure route redistribution on Switch B to redistribute RIPng routes of different RIPng processes into the peer process.

Figure 3-53 Networking with RIPng to redistributing external routes



Configuration steps

Step 1 Configure IPv6 addresses of interfaces.

Step 2 Configure RIPng on devices.

Configure Switch A.

```
SwitchA#configure
SwitchA(config)#ripng 100
SwitchA(config-ripng-100)#quit
SwitchA(config)#interface vlan 100
SIM-MPU(config-vlanif-100)#ripng 100 enable
SwitchA(config-vlanif-100)#quit
```

```
SwitchA(config)#interface vlan 200
SIM-MPU(config-vlanif-200)#ripng 100 enable
SwitchA(config-vlanif-200)#quit
```

Configure Switch B.

```
SwitchA#configure
SwitchA(config)#ripng 100
SwitchA(config-ripng-100)#quit
SwitchA(config)#ripng 200
SwitchA(config-ripng-200)#quit
SwitchA(config)#interface vlan 100
SIM-MPU(config-vlanif-100)#ripng 100 enable
SwitchA(config-vlanif-100)#quit
SwitchA(config)#interface vlan 300
SIM-MPU(config-vlanif-300)#ripng 200 enable
SwitchA(config-vlanif-300)#quit
```

Configure Switch C.

```
SwitchA#configure
SwitchA(config)#ripng 200
SwitchA(config-ripng-200)#quit
SwitchA(config)#interface vlan 300
SIM-MPU(config-vlanif-300)#ripng 200 enable
SwitchA(config-vlanif-300)#quit
SwitchA(config)#interface vlan 400
SIM-MPU(config-vlanif-400)#ripng 200 enable
SwitchA(config-vlanif-400)#quit
```

Check configuration results.

Use the following command to show information about the RIPng database on Switch C.

```
SwitchC#show ripng database
```

Process	Prefix/Prefixlen	Nexthop	Metric	Age
State	Protocol	Tag		
200	3::/64	fe80::f2f1:f2ff:fef3:301	0	0
Active	ripng	0		
200	4::/64	fe80::f2f1:f2ff:fef3:301	0	0
Active	ripng	0		

```
Total : 3
```

Step 3 Configure devices to redistribute routes.

Configure RIPng process 200 of Switch B to redistribute routes of RIPng process 100.

```
SwitchB#configure
SwitchB(config)#ripng 200
SwitchB(config-ripng-200)#import-route ripng 100
SwitchB(config-ripng-200)#quit
```

Check configuration results.

Use the following command to show information about the RIPng database on Switch C.

```
SwitchC#show ripng database
```

Process	Prefix/Prefixlen	Nexthop	Metric	Age
State	Protocol	Tag		
200	1::/64	fe80::f2f1:f2ff:fe3:201	2	22
Active	ripng	0		
200	2::/64	fe80::f2f1:f2ff:fe3:201	2	22
Active	ripng	0		
200	3::/64	fe80::f2f1:f2ff:fe3:301	0	0
Active	ripng	0		
200	4::/64	fe80::f2f1:f2ff:fe3:301	0	0
Active	ripng	0		
Total : 4				

3.14 Routing policy

3.14.1 Introduction

Functions

On today's high-performance networks, network organizers need a domain that can forward and route packets based on their own defined routing policies. On the basis of routing policies, the administrator can allocate network traffic through specified paths.

The routing policy implements such functions as route filtering and route attribute configuration. It changes the path through which network traffic passes by changing route attributes (including accessibility). When advertising, receiving, and redistributing routing information, routing protocols implement some policies based on actual network requirements to filter and change the properties of routing information, such as:

- Control the receiving and advertising of routes. Receive and advertise necessary and legal routing information to control the capacity of routing tables and improve network security.
- Control the redistribution of routes. When one routing protocol redistributes the routing information discovered by other routing protocols to enrich its routing information, it redistributes only a portion of the routing information that meets conditions.
- Configure the properties of specific routes. Modify the properties of routes filtered through routing policies to meet own needs.

Implementing the routing policy

The routing policy is implemented in the following steps:

- Step 1 Define a group of matching rules which are different properties in the routing information.
- Step 2 Apply the matching rules to the routing policies in the processes of advertising, receiving, and redistributing.

Common routing policies

- Access Control List (ACL): it is for IP packets. When defining an ACL, you can specify an IP address and subnet range to match the destination network segment address or next hop address of routing information.
- Address prefix list: its functions are similar to ACL functions, but it is more flexible and easier for users to understand. When using an address prefix list to filter routing information, its matching object is the destination address information domain of the routing information. In addition, you can specify router options to indicate that they only receive routing information advertised by certain routers.
- AS path access list (AS-path): the AS path is only used for BGP. The routing information of BGP includes the AS path domain. The AS path specifies matching conditions for the path domain of ASs.
- Community list: it is used for BGP only. The BGP packet of routing information contains the community attribute field to identify a community. The community list specifies matching conditions for the community attribute domain.

ACL

The ACL is a collection of filtering rules. In each set, all filtering rules have a sequential order. When defining filtering rules, describe the filtering rules based on attributes, such as the ingress interface, source or destination address, protocol type, source or destination port number of the packet, and specify whether to deny or receive the packet. Afterwards, the system classifies the packets arriving at the router based on filtering rules and determines whether to deny or receive the packets.

The ACL itself is just a set of rules that classify packets through filtering rules, so it needs to be used with routing policies to filter packets.

Deploy the ACL on network devices (such as access devices and core devices) to ensure the security and stability of the network. For example:

- Prevent attacks on networks, such as IP packets, TCP packets, and Internet Control Message Protocol (ICMP) packets.

- Control network access behaviors, such as controlling communication between internal and external networks on the enterprise network, allowing users to access specific network resources, and allowing access to the network during specific time periods.
- Restrict network traffic and improve network performance. For example, limit the bandwidth of network uplink and downlink traffic, charge users for bandwidth applications, and ensure the full utilization of high bandwidth network resources.

Address prefix list

The address prefix list is a filter that contains a set of rules for filtering routing information, and provides an ordered set of filtering rules based on the routing address domain (IP address, address prefix length range, and application rules). The address prefix list can be applied to various dynamic routing protocols to filter the routing information advertised and received by the routing protocol.

Compared with the ACL, the address prefix list has simple configuration and flexible application. However, when the number of routes to be filtered is large and there are no identical prefixes, configuring the address prefix list can be cumbersome.

The address prefix list includes the IPv4 address prefix list for IPv4 routes and the IPv6 address prefix list for IPv6 routes. The implementation of the IPv6 address prefix list is the same as that of the IPv4 address prefix list. There are two criteria for matching the address prefix list: mask length and mask range.

- Mask length: the object that matches the address prefix list is the IP address prefix, which is defined by both the IP address and the mask length. For example, for route 10.1.1.1/16, the mask length is 16, and the valid prefix for this address is 16 bits, which is 10.1.0.0.
- Mask range: for routes with the same prefix but different masks, specify the length range of the prefix mask to be matched to implement precise matching or matching within a certain mask length range.

During the matching process, check each entry identified by the index in ascending order. As long as an entry meets the conditions, this means that the matching process ends and the matching of the next entry will not proceed. Therefore, incorrect logical sequence in configuration can lead to matching anomalies, and operators need to ensure correctness during configuration.

AS path access list

The AS path access list is a set of rules that filter the AS-Path attribute of BGP routes. In the routing information of BGP, there is an AS-Path attribute, which records all the AS IDs that the BGP route needs to pass through from the local to the destination address in vector order. Therefore, based on the AS-Path attribute, some filtering rules can be defined to filter the BGP routing information.

Route-Policy

The Route-Policy is a complex filter that can not only match certain properties of given routing information but also change the properties of the routing information when the conditions are met. The Route-Policy can use the previous filters to define its own matching rules.

A Route-Policy can be composed of multiple nodes, each of which is a unit for matching check. During the matching process, the system checks each node in ascending order of node

number. Each node can be composed of a set of match and apply clauses. The match clause defines matching rules, and the matching objects are some attributes of routing information. Different match clauses within the same node have an AND relationship, and only by meeting the matching conditions specified by all match clauses within the node can the node pass the matching test. The apply clause specifies an action, which configures some properties of routing information after matching through nodes. There is an OR relationship between different nodes in a Route-Policy. If one of the nodes is passed, this means that matching tests will not be performed on other nodes through the route mapping.

3.14.2 Preparing for configurations

Scenario

After the routing policy is configured, it can be applied when different routing protocols advertise, receive, or redistribute routes, thus filtering routes and configuring properties.

Prerequisites

Configuring the routing protocol

3.14.3 Default configurations

Default configurations of the routing policy are as below.

Function	Default value
Routing policy	Disable

3.14.4 Configuring basic functions of the routing policy

Configure basic functions of the routing policy for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#route-policy <i>name { permit deny } node node</i>	Create a routing policy. Enter the routing policy view.
3	Raisecom(config-route-policy-a-1)# match { destination next-hop route-source } acl-ipv4 <i>acl-number</i>	(Optional) configure the match subclause to match the IPv4 route with ACL.
4	Raisecom(config-route-policy-a-1)# match { destination next-hop route-source } acl-ipv6 <i>acl-number</i>	(Optional) configure the match subclause to match the IPv6 route with ACL.
5	Raisecom(config-route-policy-a-1)# match { destination next-hop route-source } ip-prefix-list <i>prefixname</i>	(Optional) configure the match subclause to match the IPv4 route with the address prefix list.

Step	Command	Description
6	Raisecom(config-route-policy-a-1)# match { destination next-hop route-source } ipv6-prefix-list <i>prefixname</i>	(Optional) configure the match subclause to match the IPv6 route with the address prefix list.
7	Raisecom(config-route-policy-a-1)# match as-path-filter <i>name</i>	(Optional) configure the match subclause to match the BGP route with the AS-PATH attribute filter.
8	Raisecom(config-route-policy-a-1)# match community-filter <i>filter-number</i>	(Optional) configure the match subclause to match the BGP route with the community attribute filter.
9	Raisecom(config-route-policy-a-1)# match extcommunity-filter <i>filter-number</i>	(Optional) configure the match subclause to match the BGP route with the extended community attribute filter.
10	Raisecom(config-route-policy-a-1)# match cost <i>cost</i>	(Optional) configure the match subclause to match the route cost.
11	Raisecom(config-route-policy-a-1)# match process <i>process-id</i>	(Optional) configure the match subclause to match the route instance ID.
12	Raisecom(config-route-policy-a-1)# match route-type { internal external-type1 external-type2 external-type1or2 nssa-external-type1 nssa-external-type2 nssa-external-type1or2 }	(Optional) configure the match subclause to match the route type.
13	Raisecom(config-route-policy-a-1)# match tag <i>tag</i>	(Optional) configure the match subclause to match the route tag filed.
14	Raisecom(config-route-policy-a-1)# apply as-path { additive replace delete } { x.y-format <i>x.y-format</i> 4bytes-format <i>4bytes-format</i> }*	(Optional) configure the apply subclause to configure the AS-PATH attribute of BGP routes.
15	Raisecom(config-route-policy-a-1)# apply community { replace additive } { aann-format <i>aann-format</i> 4bytes-format <i>4bytes-format</i> internet no-advertise no-export no-export-subconfed }	(Optional) configure the apply subclause to configure the attribute of BGP routes.
16	Raisecom(config-route-policy-a-1)# apply extcommunity rt { replace additive } { 2bytes-aann-format <i>2bytes-aann-format</i> 4bytes-aann-format <i>4bytes-aann-format</i> ip-format <i>ip-format</i> }	(Optional) configure the apply subclause to configure the extended attribute of BGP routes.
17	Raisecom(config-route-policy-a-1)# apply cost <i>cost</i>	(Optional) configure the apply subclause to configure the route cost.

Step	Command	Description
18	<code>Raisecom(config-route-policy-a-1)# apply cost-type { type-1 type-2 }</code>	(Optional) configure the apply subclause to configure the route cost type.
19	<code>Raisecom(config-route-policy-a-1)# apply isis { level-1 level-2 level-1-2 }</code>	(Optional) configure the apply subclause to configure the priority level of ISIS routes.
20	<code>Raisecom(config-route-policy-a-1)# apply tag <i>tag-value</i></code>	(Optional) configure the apply subclause to configure the route tag field.

3.14.5 Configuring the filter

Configure the filter for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip prefix-list <i>list-name</i> { deny permit } <i>A.B.C.D/M</i> {greater-equal <i>greater-equal</i> less-equal <i>less-equal</i>}</code>	Create an IPv4 prefix list entry. If the greater-equal or less-equal parameter is not configured, the mask will be matched exactly.
3	<code>Raisecom(config)#ipv6 prefix-list <i>list-name</i> { deny permit } <i>X:X::X:X/M</i> {greater-equal <i>greater-equal</i> less-equal <i>less-equal</i>}</code>	Create an IPv6 prefix list entry. If the greater-equal or less-equal parameter is not configured, the mask will be matched exactly.
4	<code>Raisecom(config)#as-path-filter <i>list-name</i> { deny permit } <i>EXPRESSION</i></code>	Create an AS path filtering list.
5	<code>Raisecom(config)#ip community-filter <i>filter-number</i> { permit deny } {aann-format <i>aann-format</i> 4bytes-format <i>4bytes-format</i> internet no-advertise no-export no-export-subconfed}</code>	Create a community property filter.
6	<code>Raisecom(config)#ip extcommunity-filter <i>filter-number</i> { permit deny } rt {2bytes-aann-format <i>2bytes-aann-format</i> 4bytes-aann-format <i>4bytes-aann-format</i> ip-format <i>ip-format</i>}</code>	Create an extended community property filter.

3.14.6 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom# show route-policy [<i>list-name</i>]	Show the rule information about the routing policy.
2	Raisecom# show route-policy information	Show the resource information about the routing policy.
3	Raisecom# show route-policy config	Show configurations of the routing policy.
4	Raisecom# show prefix-list	Show the rule information about the prefix list.
5	Raisecom# show prefix-list config	Show configurations of the prefix list.
6	Raisecom# show prefix-list information	Show the resource information about the prefix list.
7	Raisecom# show as-path-filter	Show the rule information about the AS path filter.
8	Raisecom# show as-path-filter config	Show configurations of the AS path filter.
9	Raisecom# show as-path-filter information	Show the resource information about the AS path filter.

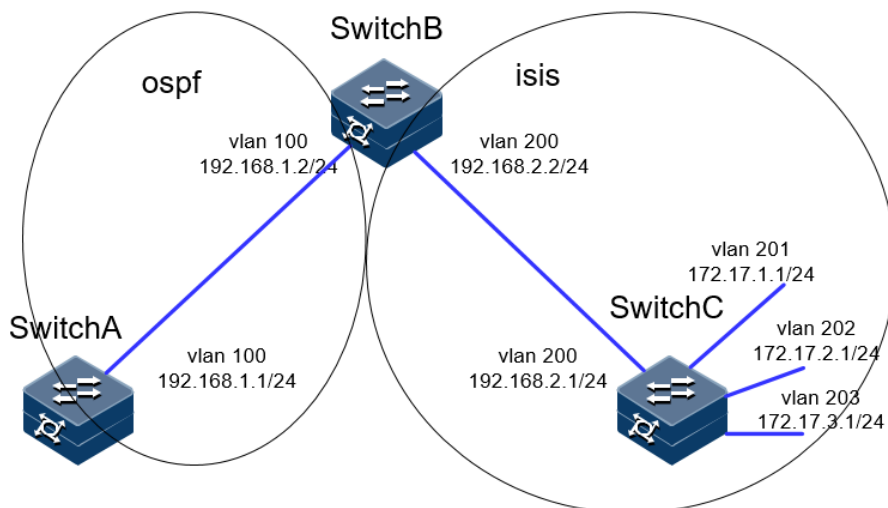
3.14.7 Example for applying the routing policy to IPv4 routes

Networking requirements

As shown below, Switch B and Switch A exchange routing information through OSPF, and Switch B and Switch C exchange routing information through IS-IS.

Configure route redistribution on Switch B to redistribute IS-IS routes to OSPF. Configure routing properties through the routing policy. Among them, configure the cost of the route 172.17.1.0/24 to 100, and configure the Tag of the route 172.17.2.0/24 to 20.

Figure 3-54 Networking with the routing policy in IPv4 route redistribution



Configuration steps

Step 1 Configure IPv4 addresses of interfaces.

Step 2 Configure ISIS.

Switch C:

```
Raisecom-C#configure
Raisecom-C(config)#isis 1
Raisecom-C(config-isis-1)#network-entity 10.0000.0000.0001.00
Raisecom-C(config-isis-1)#exit
Raisecom-C(config)#interface vlan 200
Raisecom-C(config-vlanif-200)#ip address 192.168.2.1/24
Raisecom-C(config-vlanif-200)#isis enable 1
Raisecom-C(config-vlanif-200)#exit
Raisecom-C(config)#interface vlan 201
Raisecom-C(config-vlanif-201)#ip address 172.1.1.1/24
Raisecom-C(config-vlanif-201)#isis enable 1
Raisecom-C(config-vlanif-201)#exit
Raisecom-C(config)#interface vlan 202
Raisecom-C(config-vlanif-202)#ip address 172.1.1.1/24
Raisecom-C(config-vlanif-202)#isis enable 1
Raisecom-C(config-vlanif-202)#exit
Raisecom-C(config)#interface vlan 203
Raisecom-C(config-vlanif-203)#ip address 172.1.1.1/24
Raisecom-C(config-vlanif-203)#isis enable 1
Raisecom-C(config-vlanif-203)#exit
```

Switch B:

```
Raisecom-B#configure
```

```
Raisecom-B(config)#isis 1
Raisecom-B(config-isis-1)#network-entity 10.0000.0000.0002.00
Raisecom-B(config-isis-1)#exit
Raisecom-B(config)#interface vlan 200
Raisecom-B(config-vlanif-200)# ip address 192.168.2.2/24
Raisecom-B(config-vlanif-200)#isis enable 1
Raisecom-B(config-vlanif-200)#exit
```

Step 3 Configure OSPF and route redistribution.

Switch A:

```
Raisecom-A#configure
Raisecom-A(config)#ospf 1
Raisecom-A(config-ospf-1)#router-id 1.1.1.1
Raisecom-A(config-ospf-1)#network 192.168.1.0 255.255.255.0 area 0
Raisecom-A(config-ospf-1)#exit
Raisecom-A(config)#
```

Switch B:

```
Raisecom-B#configure
Raisecom-B(config)#ospf 1
Raisecom-B(config-ospf-1)#router-id 2.2.2.2
Raisecom-B(config-ospf-1)#network 192.168.1.0 255.255.255.0 area 0
Raisecom-B(config-ospf-1)#import-route isis 1
Raisecom-B(config-ospf-1)#exit
Raisecom-B(config)#
```

Step 4 Check configuration results.

Use the **show ospf route** command to show redistributed routes.

```
Raisecom-A(config)#show ospf route
```

OSPF Process 1				PathType	Cost	Cost2	NextHop
RoutType	Prefix	AreaId	Time				
BackupNextHop							
ASBR	2.2.2.2/32			INTRA	1	0	192.168.1.2
0.0.0.0	0	0:00:05					
Network	172.17.1.0/24			ASE2	1	1	192.168.1.2
0.0.0.0	N/A	0:00:05					
Network	172.17.2.0/24			ASE2	1	1	192.168.1.2
0.0.0.0	N/A	0:00:18					
Network	172.17.3.0/24			ASE2	1	1	192.168.1.2
0.0.0.0	N/A	0:02:22					
Network	192.168.1.0/24			INTRA	1	0	192.168.1.1
0.0.0.0	N/A	0:24:26					

```

Network 192.168.2.0/24 ASE2 1 1 192.168.1.2
0.0.0.0 N/A 0:02:22
Route :
ABR ASBR Network Intra Inter External
0 1 5 1 0 4

Path :
ABR ASBR Network Intra Inter External
0 1 5 1 0 4

```

Step 5 Configure the filtering list.

Configure ACL 1002 to allow route 172.17.2.0/24 to pass.

```

Raisecom-B(config)#acl-ipv4 1002
Raisecom-B(configure-acl-ipv4-1002)#rule 1 ip src-ip 172.17.2.0/24 dst-ip
any
Raisecom-B(configure-acl-ipv4-1002)#rule 1 action permit
Raisecom-B(configure-acl-ipv4-1002)#exit

```

Configure the address prefix list named prefix to allow route 172.17.1.0/24 to pass.

```

Raisecom-B(config)#ip prefix-list prefix permit 172.17.1.0/24

```

Step 6 Configure the routing policy.

```

Raisecom-B(config)#route-policy isis2ospf permit node 1
Raisecom-B(config-route-policy-isis2ospf-1)#match destination ip-prefix-
list prefix
Raisecom-B(config-route-policy-isis2ospf-1)#apply cost 100
Raisecom-B(config-route-policy-isis2ospf-1)#exit
Raisecom-B(config)#route-policy isis2ospf permit node 2
Raisecom-B(config-route-policy-isis2ospf-2)#match destination acl-ipv4
1002
Raisecom-B(config-route-policy-isis2ospf-2)#apply tag 20
Raisecom-B(config-route-policy-isis2ospf-2)#exit
Raisecom-B(config)#route-policy isis2ospf permit node 3
Raisecom-B(config-route-policy-isis2ospf-3)#exit
Raisecom-B(config)#

```

Apply the routing policy in OSPF route redistribution.

```

Raisecom-B(config)#ospf 1
Raisecom-B(config-ospf-1)#import-route isis 1 route-policy isis2ospf

```

Check configuration results.

The cost of the route 172.17.1.0/24 is 200. The Tag value of the route 172.17.2.0/24 is 20 (0x14)

Raisecom-A (config)#show ospf route

```

OSPF Process 1
RoutType Prefix          PathType Cost  Cost2  NextHop
BackupNextHop AreaId Time
ASBR 2.2.2.2/32 INTRA 1 0 192.168.1.2
0.0.0.0 0 0:00:26
Network 172.17.1.0/24 ASE2 1 100 192.168.1.2
0.0.0.0 N/A 0:02:52
Network 172.17.2.0/24 ASE2 1 1 192.168.1.2
0.0.0.0 N/A 0:01:56
Network 172.17.3.0/24 ASE2 1 1 192.168.1.2
0.0.0.0 N/A 0:00:26
Network 192.168.1.0/24 INTRA 1 0 192.168.1.1
0.0.0.0 N/A 0:39:56
Network 192.168.2.0/24 ASE2 1 1 192.168.1.2
0.0.0.0 N/A 0:00:26
Route :
ABR ASBR Network Intra Inter External
0 1 5 1 0 4

Path :
ABR ASBR Network Intra Inter External
0 1 5 1 0 4

```

Raisecom-A(config)#show ospf database ls-type as-external-lsa link-id
172.17.2.0 adv-router 2.2.2.2

Database of OSPF Process 1

Detailed LSA Information

```

Buffer: 00 b7 02 05 ac 11 02 00 02 02 02 02 80 00 00 01
Buffer: 72 83 00 24 ff ff ff 00 80 00 00 01 00 00 00 00
Buffer: 00 00 00 14
Lsa Type:(5)AS-External Lsa
Lsa Age :183
Options : (0b 00(DC)(EA)(N/P)(MC)(E)0)0x2
Link State Id :172.17.2.0(Destination network)
Advertising Router :2.2.2.2
Sequence Number :0x80000001
Checksum:0x7283
Length :36
Network Mask:255.255.255.0
E-bit:Set
Metric:1
Forwarding Address:0.0.0.0
External Route Tag:0x14

```

3.14.8 Example for applying the routing policy to IPv6 routes

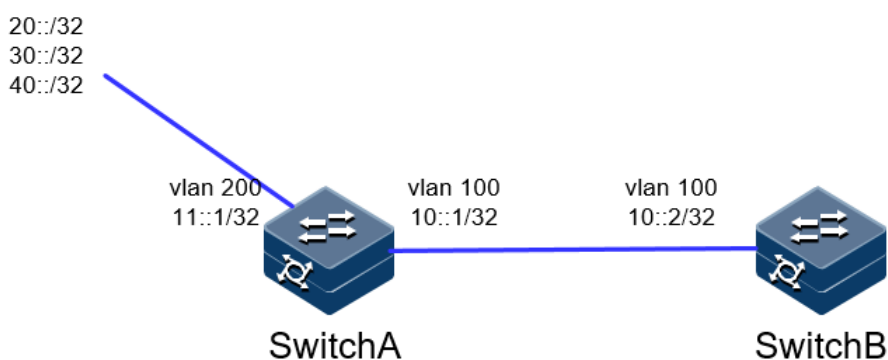
Networking requirements

Enable RIPng on Switch A and Switch B.

Configure three static routes on Switch A and apply the routing policy in redistributing static routes so that the three static routes are partially redistributed and partially masked: the routes in the 20::/32 and 40::/32 network segments are visible while the routes in the 30::/32 network segment are masked.

Check whether the routing policy is effective by viewing the RIPng routing table on Switch B.

Figure 3-55 Networking with the routing policy in IPv6 route redistribution



Configuration steps

Step 1 Configure IPv6 addresses of interfaces.

Step 2 Configure RIPng.

Switch A:

```
Raisecom-A#configure
Raisecom-A(config)#ripng 1
Raisecom-A(config-ripng-1)#exit
Raisecom-A(config)#interface vlan 100
Raisecom-A(config-vlanif-100)#ripng 1 enable
Raisecom-A(config-vlanif-100)#exit
```

Switch B:

```
Raisecom-B#configure
Raisecom-B(config)#ripng 1
Raisecom-B(config-ripng-1)#exit
Raisecom-B(config)#interface vlan 100
Raisecom-B(config-vlanif-100)#ripng 1 enable
Raisecom-B(config-vlanif-100)#exit
```


Raisecom-B(config)#

Step 3 Configure the static route.

```
Raisecom-A(config)#ipv6 route-static 20:: 32 11::2
Raisecom-A(config)#ipv6 route-static 30:: 32 11::2
Raisecom-A(config)#ipv6 route-static 40:: 32 11::2
```

Check the routing policy, and apply it.

```
Raisecom-A(config)#ipv6 prefix-list a permit 30::/32
Raisecom-A(config)#route-policy sta2ripng deny node 0
Raisecom-A(config-route-policy-sta2ripng-0)#match destination ipv6-
prefix-list a
Raisecom-A(config-route-policy-sta2ripng-0)#exit
Raisecom-A(config)#route-policy sta2ripng permit node 10
Raisecom-A(config-route-policy-sta2ripng-10)#exit
Raisecom-A(config)#ripng 1
Raisecom-A(config-ripng-1)#import-route static route-policy sta2ripng
```

Step 4 Check configuration results.

Check the routing table of switch B.

```
Raisecom-B(config)#show ripng route
```

Process	Prefix/Prefixlen	Nexthop	Metric	Age
State	Protocol	Tag		
1	10::/32	fe80::f2f1:f2ff:fef3:101	0	0
Active	ripng	0		
1	20::/32	fe80::f2f1:f2ff:fef3:201	2	25
Active	ripng	0		
1	40::/32	fe80::f2f1:f2ff:fef3:201	2	25
Active	ripng	0		
Total : 3				

3.15 ECMP

3.15.1 Introduction

Equal-cost Multi-path (ECMP) is applied in network environments where multiple different links reach the same destination address. If traditional routing techniques are used, packets sent to the destination address can utilize only one link, while the other links are in a backup or invalid status, and switching between them in a dynamic routing environment takes a certain amount of time. ECMP can use multiple links simultaneously in this network environment, not only increasing transmission bandwidth, but also backing up data transmission of failed links without delay or packet loss.

When there are multiple routes discovered by the same routing protocol to the same destination, and the cost values of these routes are also the same, then the load balancing conditions are met. ECMP provides a common algorithm configuration method and an enhanced template configuration method. The common ECMP load balancing method is based on source IP address, destination IP address, and source port number and destination port number at the transport layer. The enhanced ECMP load sharing method provides more templates for load balancing methods.

3.15.2 Preparing for configurations

Scenario

N/A

Prerequisites

N/A

3.15.3 Default configurations

Function	Default value
ECMP algorithm	Disable
ECMP profile	The default profile is enabled.

3.15.4 Configuring the ECMP load balancing algorithm

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)# ecmp load-balance { src-ip default }	Configure the ECMP load balancing algorithm. • src-ip: load balancing based on source IP address • default: the default algorithm is load balancing based on source IP address and destination IP address.

3.15.5 Configuring the ECMP profile

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#ecmp-profile default	Configure the ECMP load balancing profile.
3	Raisecom(config-ecmp-profile-default)# l3 field { src-ip dst-ip src-mac dst-mac src-port vlan l4-srcport l4-dstport protocol all default }	Configure the load balancing mode for L3 packets in the ECMP load balancing profile. • src-ip: load balancing based on source IP address • dst-ip: load balancing based on destination IP address • src-mac: load balancing based on source MAC address • dst-mac: load balancing based on destination MAC address • src-port: load balancing based on source port • vlan: load balancing based on VLAN • l4-srcport: load balancing based on source port at the transport layer • l4-dstport: load balancing based on destination port at the transport layer • protocol: load balancing based on protocol • all: load balancing based on all previous items • default: the default mode is load balancing based on source IP address and destination IP address. By default, the default mode of IPv4 load balancing is src-ip, dst-ip, l4-srcport, l4-dstport, and protocol
4	Raisecom(config-route-policy-a-1)#ecmp-profile default	Apply the ECMP load balancing profile.

3.15.6 Checking configurations

Step	Command	Description
1	Raisecom#show ecmp-profile	Show configurations of the ECMP load balancing profile.
2	Raisecom# show ecmp load-balance	Show the binding information about the ECMP load balancing profile.

4 DHCP

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

- DHCP Client
- DHCP Server
- DHCP Relay

4.1 DHCP Client

4.1.1 Introduction

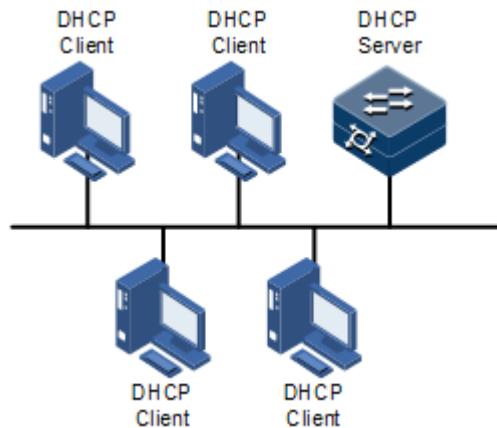
Dynamic Host Configuration Protocol (DHCP) refers to the protocol which assigns configurations, such as the IP address, to users on the TCP/IP network. Based on BOOTP (Bootstrap Protocol) protocol, it has additional features, such as automatically assigning available network addresses, reusing network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

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

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

Typical applications of DHCP usually include a set of DHCP server and multiple clients (such as the PC or laptop), as shown in Figure 4-1.

Figure 4-1 DHCP typical networking



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

Figure 4-2 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 4-2 Structure of a DHCP packet

0	7	15	23	31
OP	Hardware type	Hardware length	Hops	
Transaction ID				
Seconds		Flags		
Client IP address				
Your(client) IP address				
Server IP address				
Relay agent IP address				
Client hardware address				
Server host name				
File				
Options				

Table 4-1 describes fields of DHCP packets.

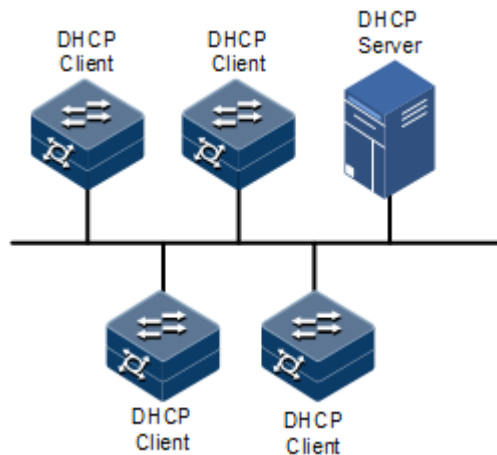
Table 4-1 Fields of a DHCP packet

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 4-3.

Figure 4-3 DHCP Client networking



4.1.2 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.

4.1.3 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

4.1.4 Configuring DHCP Client

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

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.

4.1.5 Checking configurations

Use the following commands to check configuration results.

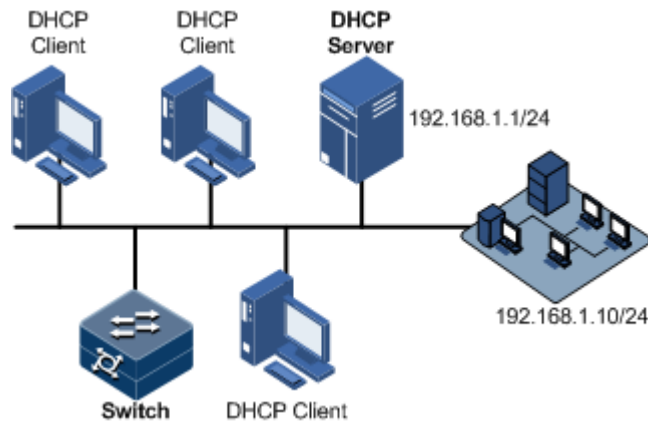
No.	Command	Description
1	Raisecom#show dhcp client [<i>interface-type interface-number</i> <i>vlan vlan-id</i>]	Show configurations of DHCP Client.

4.1.6 Example for configuring DHCP Client

Networking requirements

As shown in Figure 4-4, the Switch is used as a DHCP client, and the host name is raisecom. The Switch is connected to the DHCP server and NMS. The DHCP server should assign IP addresses to the SNMP interface on the Switch and make NMS manage the Switch.

Figure 4-4 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: 0 days 23 hours 59 minutes 49 seconds.
```

4.2 DHCP Server

4.2.1 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:

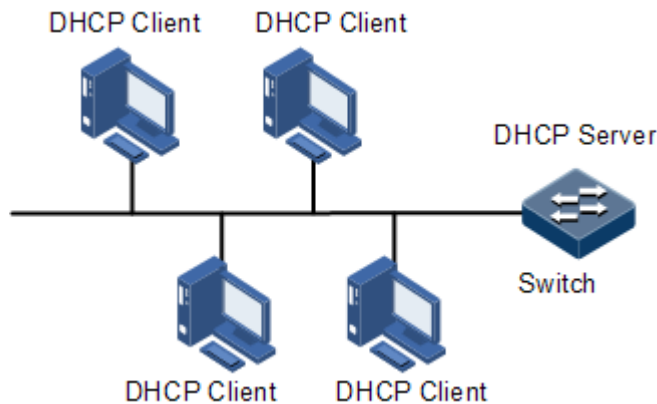
- The network scale is large. It requires much workload for manual configurations, and is difficult to manage the entire network intensively.
- The number of hosts on the network is greater than that of IP addresses, which makes it unable to assign a fixed IP address for each host and restricts the number 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 4-5.

Figure 4-5 DHCP Server and Client networking



DHCP packets

Figure 4-6 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 4-6 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

4.2.2 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.

4.2.3 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 server pool pool-name	Create an IPv4 address pool, and enter address pool configuration mode.
4	Raisecom(config-dhcp-pool-*)#ip range start-ip-address end-ip-address mask mask	Configure the range of IP addresses in the IPv4 address pool.
5	Raisecom(config-dhcp-pool-*)#dhcp server exclude-ip start-ip-address [end-ip-address]	Configure the range of excluded IP addresses in the IPv4 address pool.
6	Raisecom(config-dhcp-pool-*)#lease-time { hour day day hour hour minute minute unlimited default }	Configure the lease period for the IPv4 address pool.
7	Raisecom(config-dhcp-pool-*)#dns ip-address [backup]	Configure the DNS server address of the IPv4 address pool.
8	Raisecom(config-dhcp-pool-*)#gateway ip-address	Configure the default gateway of the IPv4 address pool.
9	Raisecom(config-pool)#option 43 [sub-option option-code] { ascii ascii-string hex hex-string }	Configure information carried by the option.
10	Raisecom(config)#dhcp server static-bind ip-address mac-address	Bind the IP address in the IPv4 address pool with the MAC address of the user device.

4.2.4 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 vlan-id	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 enable server	Enable DHCP Server on the interface.

4.2.5 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 server pool <i>pool-name</i>	Recycle the IP address pool.
3	Raisecom(config)#no dhcp server user-bind	Recycle the address binding table of the DHCPv4 server.
4	Raisecom(config)#no dhcp server dynamic-bind <i>ip-address</i>	Recycle the IP addresses bound with MAC addresses of the user devices.

4.2.6 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 server 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.

4.2.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show dhcp server 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.

4.2.8 Maintenance

Maintain the device as below.

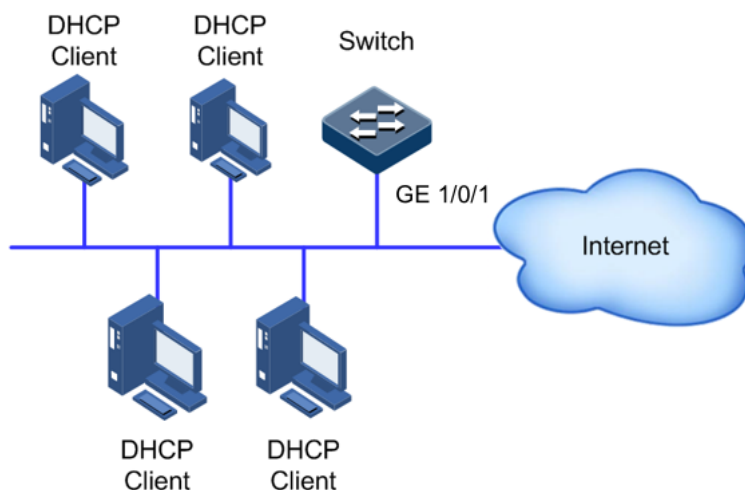
Command	Description
Raisecom(config)#reset dhcp server statistics	Clear statistics on DHCP Server.

4.2.9 Example for configuring DHCPv4 Server

Networking requirements

As shown in Figure 4-7, 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 4-7 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 server 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)#dhcp enable server
```

Checking results

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

```
Raisecom#show dhcp server config
!
dhcp start
dhcp server 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
dhcp enable 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
-----
```

4.3 DHCP Relay

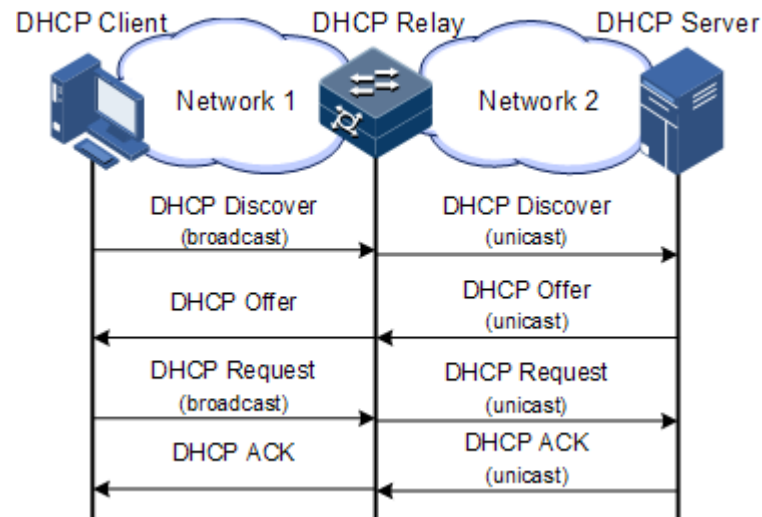
4.3.1 Introduction

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 4-8 shows typical application of DHCP Relay.

Figure 4-8 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.

4.3.2 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

4.3.3 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

Function	Default value
Interface DHCPv6 Relay	Disable

4.3.4 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 <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.
4	Raisecom(config-vlanif-*)#dhcp enable relay	Enable interface DHCP Relay.
5	Raisecom(config-vlanif-*)#dhcp relay server-ip <i>ip-address</i>	Configure the IP address of the DHCP server.

4.3.5 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 <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.
4	Raisecom(config-vlanif-*)#dhcpv6 enable relay	Enable interface DHCPv6 Relay.
5	Raisecom(config-vlanif-*)#dhcpv6 relay destination <i>ipv6-address</i>	Configure the IPv6 address of the DHCPv6 server.

4.3.6 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.
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 format { default 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 format { default user- defined <i>format-string</i> }	Configure contents of the Remote ID of DHCP Relay Option 82.

4.3.7 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 relay 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 relay 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.

4.3.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show dhcp relay 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.

4.3.9 Maintenance

Maintain the device as below.

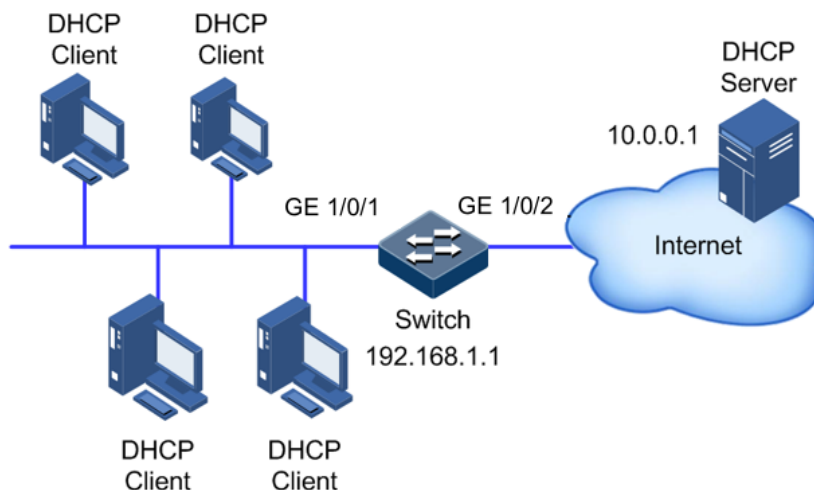
Command	Description
Raisecom(config)#reset dhcp relay statistics	Clear statistics on DHCP Relay.
Raisecom(config)#reset dhcpv6 statistics	Clear statistics on DHCPv6 Relay.

4.3.10 Example for configuring DHCPv4 Relay

Networking requirements

As shown in Figure 4-9, 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 4-9 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)#dhcp enable relay
Raisecom(config-vlanif-1)#dhcp relay server-ip 10.0.0.1
Raisecom(config-vlanif-1)#exit
```

Checking results

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

```
Raisecom#show dhcp relay config
!
dhcp start

interface vlan 1
dhcp enable 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
- ACL-based simplified traffic policy

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:

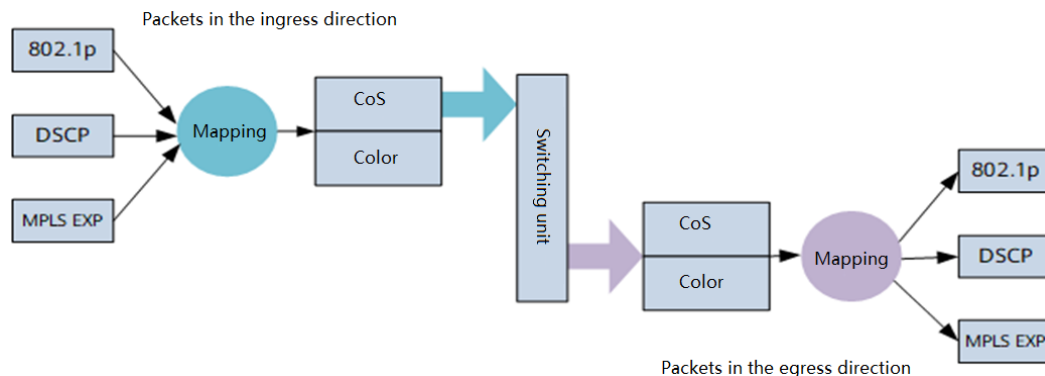
- Committed Access Rate (CAR): CAR refers to classifying the packets according to the preconfigured packet matching rules, such as IP packets priority, the packet source address or destination address. The system continues to send the packets if the flow complies with the rules of token bucket. Otherwise, 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.
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

PHB	Color	IEEE 802.1p priority
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
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

DHCP	PHB	Color	DHCP	PHB	Color
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
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

PHB	Color	DSCP
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
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</i> <i>interface-number</i>	Enter Layer 2 physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.

Step	Command	Description
3	<code>Raisecom(config-ge-1/0/*)#trust [dot1p { inner outer } dscp]</code>	Configure types of priorities trusted by the interface. • dot1p inner: inner priority of VLAN packets • dot1p outer: outer priority of VLAN packets • dscp: precedence of IP packets

5.2.5 Configuring the diffserv profile

Configure the diffserv profile for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#diffserv domain default</code>	Create a diffserv domain profile, or enter the default profile. • default: default profile • ds-domain-name: name of the profile to be created
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 mapping between the IEEE 802.1p priority and PHB of VLAN packets in the ingress direction in the DiffServ domain, and configure the color of packets. • 8021p-value: IEEE 802.1p priority • BE AF1 AF2 AF3 AF4 EF CS6 CS7: queue • 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 mapping between the IEEE 802.1p priority and PHB behavior/color of VLAN packets in the egress direction in the DiffServ domain. • 8021p-value: IEEE 802.1p priority • BE AF1 AF2 AF3 AF4 EF CS6 CS7: queue • 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 mapping between the DSCP priority and PHB of IP packets in the ingress direction in the DiffServ domain, and configure the color of packets. • dscp-value: DSCP priority • BE AF1 AF2 AF3 AF4 EF CS6 CS7: queue • green yellow red: color

Step	Command	Description
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 mapping between the DSCP priority and PHB behavior/color of IP packets in the egress direction in the DiffServ domain. - dscp-value: DSCP priority - BE AF1 AF2 AF3 AF4 EF CS6 CS7: queue - green yellow red: color

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

Configure IEEE 802.1p/DSCP remarking for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i></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-1/0/*)#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.
2	<code>Raisecom#show differv interface <i>interface-type</i> <i>interface-number</i></code>	Show configurations of the interface in the diffserv domain profile.

5.3 Queue scheduling

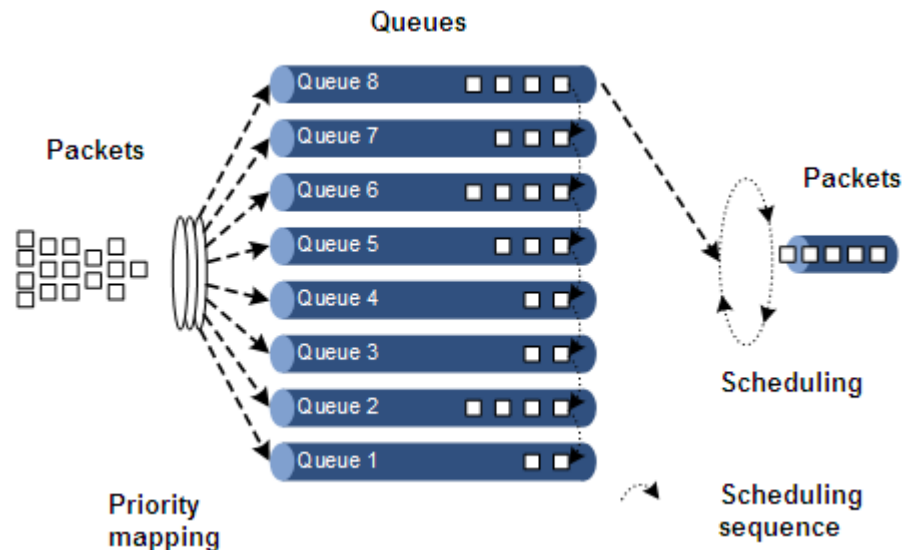
5.3.1 Introduction

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 (WFQ), 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.

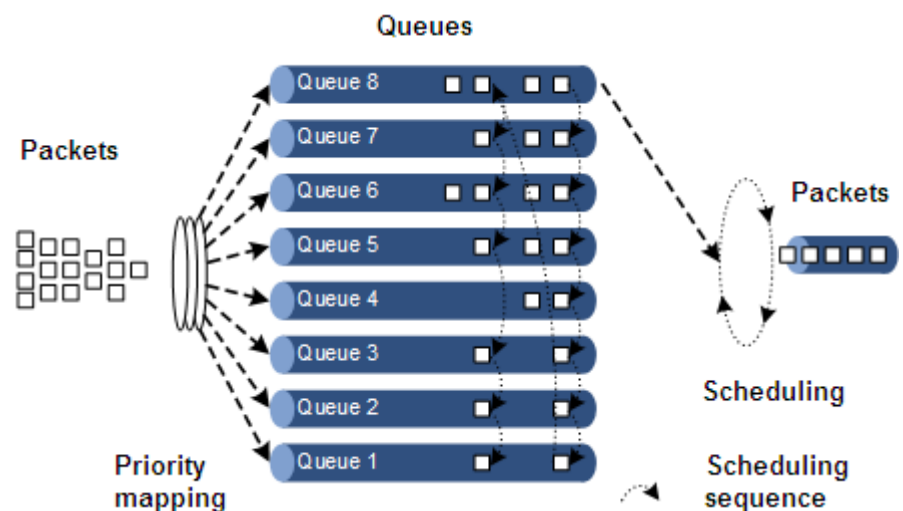
- SP: the device strictly schedules packets in a descending order of priority. Packets with lower priority cannot be scheduled until packets with higher priority are scheduled, as shown in Figure 5-1.

Figure 5-1 SP scheduling



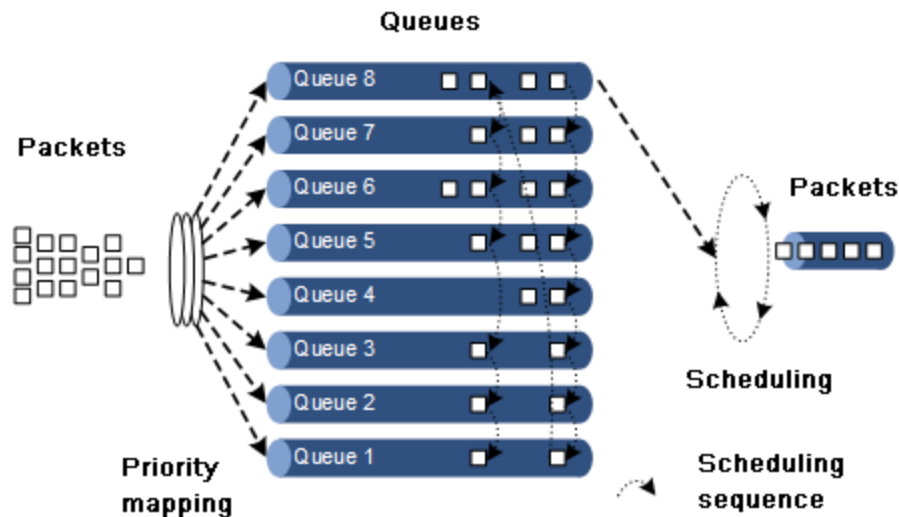
- WRR: on the basis of scheduling packets cyclically according to the priority, the device schedules packets by the weight of each queue in units of bit, as shown in Figure 5-2.

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 queue scheduling

Default configurations of queue scheduling are as below.

Function	Default value
Queue scheduling mode	SP
Queue weight	• WRR weight for scheduling 8 queues is 1. • WFR 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-1/0/*)#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.
3	Raisecom(config-ge-1/0/*)#queue scheduling wrr	Configure the queue scheduling mode to WRR on the interface.
4	Raisecom(config-ge-1/0/*)#queue <i>queue-id</i> weight <i>weight-value</i>	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	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/*)#queue scheduling wfq	Configure the queue scheduling mode to WFQ on the interface.

Step	Command	Description
4	<code>Raisecom(config-ge-1/0/*)#queue <i>queue-id</i> weight <i>weight-value</i></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 <i>interface-type interface-number</i></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-1/0/1)# queue <i>queue-id</i> min-bandwidth { kbps mbps gbps } <i>bandwidth</i></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	<code>Raisecom#show queue interface</code>	Show the queue on the interface
2	<code>Raisecom#show queue statistics interface <i>interface-type interface-number</i></code>	Show statistics about queues on the interface.

5.3.9 Maintenance

Maintain the device as below.

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

5.3.10 Example for configuring queue scheduling

Networking requirements

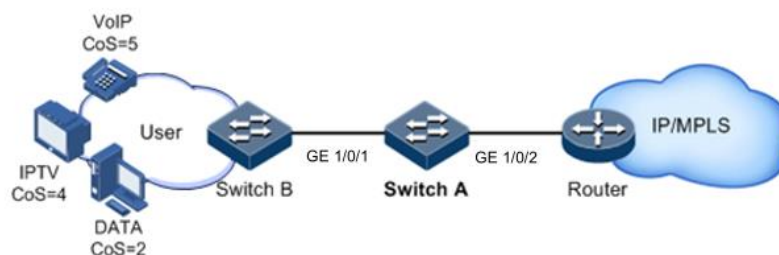
As shown in Figure 5-4, the user uses voice, video and data services.

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 1/0/2
SwitchA(config-ge-1/0/2)#trust 8021p outer
```

Step 2 Conduct SP+WRR queue scheduling in the egress direction of GE 1/0/2.

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#queue scheduling sp+wrr queue 5
SwitchA(config-ge-1/0/2)#queue 4 weight 50
SwitchA(config-ge-1/0/2)#queue 2 weight 20
SwitchA(config-ge-1/0/2)#quit
```

Checking results

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

```
Raisecom#show queue interface ge 1/0/2
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-1/0/2	0	0M	0M	1
ge-1/0/2	1	0M	0M	1
ge-1/0/2	2	0M	0M	20
ge-1/0/2	3	0M	0M	1
ge-1/0/2	4	0M	0M	50
ge-1/0/2	5	0M	0M	--
ge-1/0/2	6	0M	0M	1
ge-1/0/2	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.
2	Raisecom(config)#drop-profile drop-profile-name	Create a WRED profile, and enter WRED configuration mode.

Step	Command	Description
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: low threshold percentage of WRED discarding, namely, percentage of low-threshold packets discarded by WRED to the queue length • high-limit-percentage: high threshold percentage of WRED discarding, namely, percentage of high-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-ge-1/0/*)#qos wred drop-profile-name</code>	Apply the WRED profile to the interface.
6	<code>Raisecom(config-ge-1/0/*)#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 { all name drop-profile-name }</code>	Show information about the WRED profile.

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 interface-type interface-number	Enter physical interface configuration mode.
3	Raisecom(config-gigaethernet1/1/*)#rate-limit { ingress egress } cir cir-value	Configure rate limiting based on interface in the ingress or egress direction.
4	Raisecom(config-ge-1/0/*)#rate-limit { ingress egress } cir cir-value cbs cbs-value	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> vlan <i>vlan-id</i> } [ingress egress]]	Show configurations of rate limiting based on interface.
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

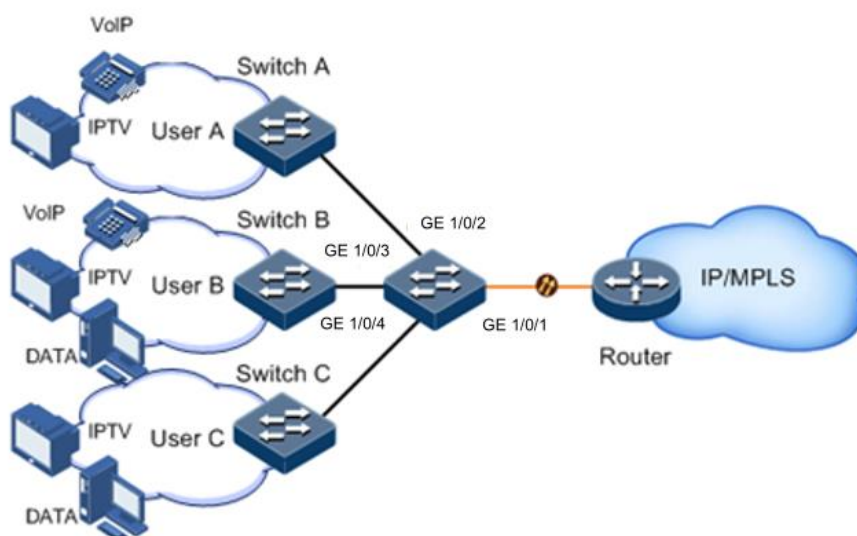
As shown in Figure 5-5, User A, User B, and User C are respectively connected to the device by Switch A, Switch B, and Switch C.

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 ge 1/0/1
Raisecom(config-ge-1/0/1)#rate-limit ingress cir 25000 cbs 100
Raisecom(config-ge-1/0/1)#exit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#rate-limit ingress cir 35000 cbs 100
Raisecom(config-ge-1/0/2)#exit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#rate-limit ingress cir 30000 cbs 100
Raisecom(config-ge-1/0/3)#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)	CirOper(kbps)	CbsOper(kb)
ge-1/0/1	ingress	25000	100	25024	101
ge-1/0/2	ingress	35000	100	30016	101
ge-1/0/3	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.
2	Raisecom(config)#bandwidth-profile <i>bwp-profile-id</i> cir <i>cir</i> cbs <i>cbs</i> [color-aware]	Create a bandwidth guarantee profile.
3	Raisecom(config)#bandwidth-profile <i>bwp-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-ge-1/0/*)#bandwidth ingress <i>bwp-profile-id</i>	Apply the bandwidth guarantee profile in the ingress direction of the Layer 2 interface.
	Raisecom(config-ge-1/0/*)#bandwidth egress <i>bwp-profile-id</i>	Apply the bandwidth guarantee profile in the egress direction of the Layer 2 interface.
6	Raisecom(config-ge-1/0/*)#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-ge-1/0/*)#exit Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
8	Raisecom(config-vlan*)#bandwidth ingress <i>bwp-profile-id</i>	Apply the bandwidth guarantee profile in the ingress direction of the VLAN interface.
	Raisecom(config-vlan*)#bandwidth egress <i>bwp-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>bwp-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>bwp-profile-id cir cir cbs cbs</i> [color-aware]	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-ge-1/0/*)#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-ge-1/0/*)#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-ge-1/0/*)#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</i> [color-aware]	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-ge-1/0/*)#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-ge-1/0/*)#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-ge-1/0/*)#exit Raisecom(config)#interface port-channel <i>port-channel-id</i>	Enter aggregation group configuration mode.

Step	Command	Description
6	<code>Raisecom(config-port-channel*)#bandwidth ingress coslist cos-value-list bwp-profile-id</code>	Apply the bandwidth guarantee profile in the ingress direction of the interface+CoS.
7	<code>Raisecom(config-port-channel*)#exit</code> <code>Raisecom(config)#interface vlan vlan-id</code>	Enter VLAN interface configuration mode.
8	<code>Raisecom(config-vlan*)#bandwidth ingress coslist cos-value-list bwp-profile-id</code>	Apply the bandwidth guarantee profile in the ingress direction of the interface+CoS.
	<code>Raisecom(config-vlan*)#bandwidth egress coslist cos-value-list bwp-profile-id</code>	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	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#bandwidth-profile bwp-profile-id cir cir cbs cbs [color-aware]</code>	Create a bandwidth guarantee profile.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter Layer 2 physical interface configuration mode.
4	<code>Raisecom(config-ge-1/0/*)#bandwidth ingress vlan vlan-id coslist cos-value-list bwp-profile-id</code>	Apply the bandwidth guarantee profile in the ingress direction of the interface+VLAN+CoS.
	<code>Raisecom(config-ge-1/0/*)#bandwidth egress vlan vlan-id coslist cos-value-list bwp-profile-id</code>	Apply the bandwidth guarantee profile in the egress direction of the interface+VLAN+CoS.
5	<code>Raisecom(config-ge-1/0/*)#exit</code> <code>Raisecom(config)#interface port-channel port-channel-id</code>	Enter aggregation group configuration mode.
6	<code>Raisecom(config-port-channel*)#bandwidth ingress vlan vlan-id coslist cos-value-list bwp-profile-id</code>	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>bwp-profile-id</i>]	Show information about the bandwidth guarantee profile.
2	Raisecom#show bandwidth interface <i>interface-type</i> <i>interface-number</i>	Show information about the bandwidth guarantee profile on the interface.

5.7 ACL-based simplified traffic policy

5.7.1 Introduction

The ACL-based simplified traffic policy refers to matching packet information with ACL rules, providing the same QoS services for packets that comply with the same ACL rules, and providing differential services for different types of services.

When you wish to control the traffic entering the network, you can configure ACL rules to match packets based on their source IP addresses, fragmentation tag, destination IP address, source port number, source MAC address, and other information. Then, you can configure the ACL-based simplified traffic policy to implement packet filtering, traffic policing, traffic mirroring, redirection, re-marking, or traffic statistics on packets that match ACL rules.

Compared with the traffic policy, the ACL-based simplified traffic policy does not require the creation of traffic classifications, traffic behaviors, or traffic policies, and have simpler configurations; however, due to only matching packets based on ACL rules, the matching rules are not as rich as those of traffic policies.

5.7.2 Preparing for configurations

Scenario

N/A

Prerequisite

N/A

5.7.3 Configuring ACL-based packet filtering

Configure ACL-based packet filtering for the device as below.

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

Step	Command	Description
2	<code>Raisecom(config)#acl-ipv4 <i>acl-id</i></code>	Configure the ACL and rule for filtering some IP addresses. For the command update, see commands in the ACL module.
3	<code>Raisecom(config)# traffic-policy filter global { inbound outbound } { acl-12 acl-ipv4 acl-hybrid acl-ipv6 acl-mpls acl-userdefined } <i>list-id</i> [rule <i>rule-id</i>] [time-range <i>tr-id</i>]</code>	Apply a configured ACL rule globally. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID
4	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical interface configuration mode.
5	<code>Raisecom(config-ge-1/0/1)# traffic-policy filter { inbound outbound } { acl-12 acl-ipv4 acl-hybrid acl-ipv6 acl-mpls acl-userdefined } <i>list-id</i> [rule <i>rule-id</i>] [time-range <i>tr-id</i>]</code>	Apply a configured ACL rule on the interface. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID

5.7.4 Configuring ACL-based traffic policing

Configure ACL-based traffic policing for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#acl-ipv4 <i>acl-id</i></code>	Configure the ACL and rule for filtering some IP addresses. For the command update, see commands in the ACL module.
3	<code>Raisecom(config)#meter <i>meter-id</i></code>	Configure the meter, and configure the rate limiting rule. For the command update, see commands in the ACL module.

Step	Command	Description
4	<code>Raisecom(config)#traffic-policy limit global { inbound outbound } { acl-12 acl-ipv4 acl-hybrid acl-ipv6 acl-mps acl-userdefined } acl-id [rule rule-id] meter meter-id [time-range tr-id red (drop pass) red-remark-dscp dscp-value red-remark-8021p 8021p-value red-remark-cfi cfi-value yellow (drop pass) yellow-remark-dscp dscp-value yellow-remark-8021p 8021p-value yellow-remark-cfi cfi-value]</code>	Apply a configured ACL rule globally. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • meter-id: meter rule ID • drop: discard packets. • Pass: allow packets. • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID • (Optional) dscp-value: specify the DSCP priority after re-marking. • (Optional) 8021p-value: specify the 8021p priority after re-marking. • (Optional) cfi-value: specify the cfi priority after re-marking.
5	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical interface configuration mode.
6	<code>Raisecom(config-ge-1/0/1)#traffic-policy limit { inbound outbound } { acl-12 acl-ipv4 acl-hybrid acl-ipv6 acl-mps acl-userdefined } acl-id [rule rule-id] meter meter-id [time-range tr-id red (drop pass) red-remark-dscp dscp-value red-remark-8021p 8021p-value red-remark-cfi cfi-value yellow (drop pass) yellow-remark-dscp dscp-value yellow-remark-8021p 8021p-value yellow-remark-cfi cfi-value]</code>	Apply a configured ACL rule globally. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • meter-id: meter rule ID • drop: discard packets. • Pass: allow packets. • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID • (Optional) dscp-value: specify the DSCP priority after re-marking. • (Optional) 8021p-value: specify the 8021p priority after re-marking. • (Optional) cfi-value: specify the cfi priority after re-marking.

5.7.5 Configuring ACL-based traffic redirection

Configure ACL-based **traffic redirection** for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#acl-ipv4 acl-id</code>	Configure the ACL and rule for filtering some IP addresses. For the command update, see commands in the ACL module.

Step	Command	Description
3	<pre>Raisecom(config)# traffic-policy redirect global { inbound outbound } { acl-l2 acl-ipv4 acl-hybrid acl-ipv6 acl-mpls acl- userdefined } acl-id [rule rule-id] { cpu interface interface-type interface-number ip- nexthop1 ip-nexthop [vpn-instance vpn- instance-name] ipv6- nexthop1 ipv6-nexthop [vpn-instance vpn- instance-name] } [time- range tr-id]</pre>	Apply a configured ACL rule globally. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID • cpu: redirect packets to the CPU. • interface <i>interface-type interface-number</i>: redirect packets to the specified interface. • (Optional) <i>vpn-instance-name</i>: redirect packets to the specified VPN. • <i>ip-nexthop</i>: redirect packets to the next IPv4 address. • <i>ipv6-nexthop</i>: redirect packets to the next IPv6 address.
4	<pre>Raisecom(config)#interface interface-type interface- number</pre>	Enter physical interface configuration mode.
5	<pre>Raisecom(config-ge-1/0/1)# traffic-policy redirect { inbound outbound } { acl-l2 acl-ipv4 acl-hybrid acl-ipv6 acl-mpls acl- userdefined } acl-id [rule rule-id] { cpu interface interface-type interface-number ip- nexthop1 ip-nexthop [vpn-instance vpn- instance-name] ipv6- nexthop1 ipv6-nexthop [vpn-instance vpn- instance-name] } [time- range tr-id]</pre>	Apply a configured ACL rule on the interface. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID • cpu: redirect packets to the CPU. • interface <i>interface-type interface-number</i>: redirect packets to the specified interface. • (Optional) <i>vpn-instance-name</i>: redirect packets to the specified VPN. • <i>ip-nexthop</i>: redirect packets to the next IPv4 address. • <i>ipv6-nexthop</i>: redirect packets to the next IPv6 address.

5.7.6 Configuring ACL-based traffic re-marking

Configure ACL-based traffic re-marking for the device as below.

Step	Command	Description
1	<pre>Raisecom#configure</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#acl 1-ipv4 acl-id</pre>	Configure the ACL and rule for filtering some IP addresses. For the command update, see commands in the ACL module.

Step	Command	Description
3	<pre> Raisecom(config)#tr affic-policy remark global inbound acl acl-id [rule rule- id] { 8021p-inner 8021p-value destination-mac mac-address dscp dscp-value precedence precedence-value vlan-id vlan-id } [time-range tr- id] Raisecom(config)#tr affic-policy remark global outbound acl acl-id [rule rule- id] { 8021p-outer 8021p-value cvlan-id cvlan-id dscp dscp-value vlan-id vlan-id } [time-range tr- id] </pre>	Apply a configured ACL rule globally. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID • 8021p-value: re-mark the 8021p priority. • mac-address: re-mark the destination MAC address. • dscp-value: re-mark the following DSCP service types: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1–cs7, default, and ef. • ip-precedence-value: re-mark the IP precedence. • local-precedence-value: re-mark the local priority. • vlan-id: re-mark the VLAN index. • cvlan-id: re-mark the inner VLAN index of QinQ packets. The properties of packets that can be re-marked in the ingress direction include: 802.1p priority, destination MAC address, DSCP service type, local priority, IP precedence, and VLAN ID. The properties of packets that can be re-marked in the egress direction include: 802.1p priority, inner VLAN tag of QinQ packets, DSCP service type, and VLAN ID.
4	<pre> Raisecom(config)#in terface interface- type interface- number </pre>	Enter physical interface configuration mode.

Step	Command	Description
5	<pre> Raisecom(config-ge-1/0/1)#traffic- policy remark inbound acl acl-id [rule rule-id] { 8021p-inner 8021p-value destination-mac mac-address dscp dscp-value precedence precedence-value vlan-id vlan-id } [time-range tr- id] Raisecom(config-ge-1/0/1)#traffic- policy remark outbound acl acl-id [rule rule-id] { 8021p-outer 8021p-value cvlan-id cvlan-id dscp dscp-value vlan-id vlan-id } [time-range tr- id] </pre>	Apply a configured ACL rule on the interface. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID • 8021p-value: re-mark the 8021p priority. • mac-address: re-mark the destination MAC address. • dscp-value: re-mark the following DSCP service types: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1–cs7, default, and ef. • ip-precedence-value: re-mark the IP precedence. • local-precedence-value: re-mark the local priority. • vlan-id: re-mark the VLAN index. • cvlan-id: re-mark the inner VLAN tag of QinQ packets. The properties of packets that can be re-marked in the ingress direction include: 802.1p priority, destination MAC address, DSCP service type, local priority, IP precedence, and VLAN ID. The properties of packets that can be re-marked in the egress direction include: 802.1p priority, inner VLAN tag of QinQ packets, DSCP service type, and VLAN ID.

5.7.7 Configuring ACL-based traffic statistics

Configure ACL-based traffic statistics for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#acl-ipv4 acl-id	Configure the ACL and rule for filtering some IP addresses. For the command update, see commands in the ACL module.

Step	Command	Description
3	<code>Raisecom(config)# traffic-policy statistic global { inbound outbound } { acl-l2 acl-ipv4 acl-hybrid acl-ipv6 acl-mps acl-userdefined } acl-id rule rule-id [time-range tr-id by-bytes]</code>	Apply a configured ACL rule globally. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID • (Optional) by-bytes: gather statistics by bytes. • By default, the device gathers statistics by packets.
4	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical interface configuration mode.
5	<code>Raisecom(config-ge-1/0/1)# traffic-policy statistic { inbound outbound } { acl-l2 acl-ipv4 acl-hybrid acl-ipv6 acl-mps acl-userdefined } acl-id rule rule-id [time-range tr-id by-bytes]</code>	Apply a configured ACL rule on the interface. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID • (Optional) by-bytes: gather statistics by bytes. • By default, the device gathers statistics by packets.
6	<code>Raisecom(config-ge-1/0/1)#show traffic-policy statistic interface interface-type interface-number { inbound outbound }</code>	Show interface statistics. • inbound: ingress direction • outbound: egress direction
7	<code>Raisecom(config-ge-1/0/1)# show traffic-policy statistic global { inbound outbound }</code>	Show global statistics. • inbound: ingress direction • outbound: egress direction

Configuring ACL-based traffic mirroring

Configure ACL-based traffic mirroring for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#acl-ipv4 acl-id</code>	Configure the ACL and rule for filtering some IP addresses. For the command update, see commands in the ACL module.

Step	Command	Description
3	<code>Raisecom(config)# traffic-policy mirror global { inbound outbound } { acl-12 acl-ipv4 acl-hybrid acl-ipv6 acl-mps acl-userdefined } acl-id rule rule-id to mirror-group group-id { time-range tr-id }</code>	Apply a configured ACL rule globally. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID • group-id: mirroring group ID
4	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical interface configuration mode.
5	<code>Raisecom(config-ge-1/0/1)# traffic-policy mirror { inbound outbound } { acl-12 acl-ipv4 acl-hybrid acl-ipv6 acl-mps acl-userdefined } acl-id rule rule-id to mirror-group group-id { time-range tr-id }</code>	Apply a configured ACL rule on the interface. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID • group-id: mirroring group ID

Configuring ACL-based traffic loopback

Configure ACL-based traffic loopback for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#acl-ipv4 acl-id</code>	Configure the ACL and rule for filtering some IP addresses. For the command update, see commands in the ACL module.
3	<code>Raisecom(config)# traffic-policy loopback global { inbound outbound } { acl-12 acl-ipv4 acl-hybrid acl-ipv6 acl-mps acl-userdefined } acl-id rule rule-id [swap-mac (enable disable) new-source-mac src-mac new-dest-mac dst-mac time-range tr-id]</code>	Apply a configured ACL rule globally. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID • (Optional) swap-mac: configure whether to swap the source MAC address with the destination MAC address. • (Optional) src-mac: specify the new source MAC address. • (Optional) des-mac: specify the new destination MAC address.

Step	Command	Description
4	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
5	Raisecom(config-ge-1/0/1)# traffic-policy loopback { inbound outbound } { acl-12 acl-ipv4 acl-hybrid acl-ipv6 acl-mpls acl- userdefined } acl-id rule <i>rule-id</i> [swap-mac (enable disable) new- source-mac src-mac new- dest-mac dst-mac time- range tr-id]	Apply a configured ACL rule on the interface. • inbound: ingress direction • outbound: egress direction • acl-id: ACL template ID • (Optional) rule-id: ACL rule ID • (Optional) tr-id: timerange rule ID • (Optional) swap-mac: configure whether to swap the source MAC address with the destination MAC address. • (Optional) src-mac: specify the new source MAC address. • (Optional) des-mac: specify the new destination MAC address.

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
- IGMP
- PIM
- MLD
- PIMv6

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

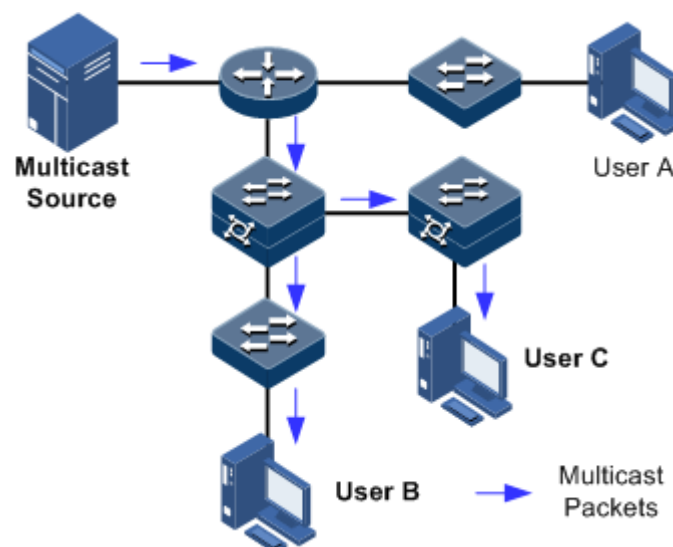
Multicast is a kind of packets transmission method which is parallel with unicast and broadcast.

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

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

Advantages and application of multicast

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

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

The multicast technology is used in the following aspects:

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

- Training, cooperative operations communications, such as: distance education, telemedicine
- Data warehousing and financial applications (stock)
- Any other point-to-multipoint applications

Basic concepts in multicast

- Multicast group

A multicast group refers to the recipient set using the same IP multicast address identification. Any user host (or other receiving device) will become a member of the group after joining the multicast group. They can identify and receive multicast data with the destination address as IP multicast address.

- Multicast group members

Each host joining a multicast group will become a member of the multicast group. Multicast group members are dynamic, and hosts can join or leave multicast group at any time. Group members may be widely distributed in any part of the network.

- Multicast source

A multicast source refers to a server which regards multicast group address as the destination address to send IP packet. A multicast source can send data to multiple multicast groups; multiple multicast sources can send to a multicast group.

- Multicast router

A multicast router is a router that supports Layer 3 multicast. The multicast router can achieve multicast routing and guide multicast packet forwarding, and provide multicast group member management to distal segment connecting with users.

- Routed interface

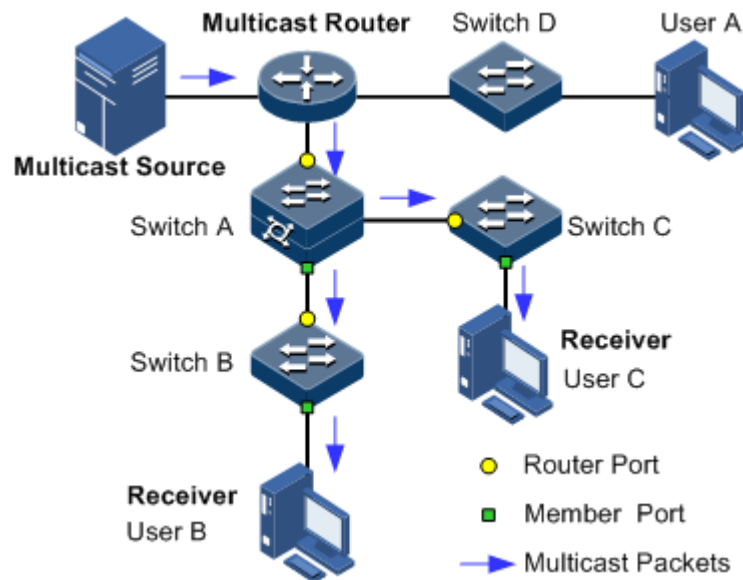
A routed interface refers to the interface towards the multicast router between a multicast router and a host. The device receives multicast packets from this interface.

- 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

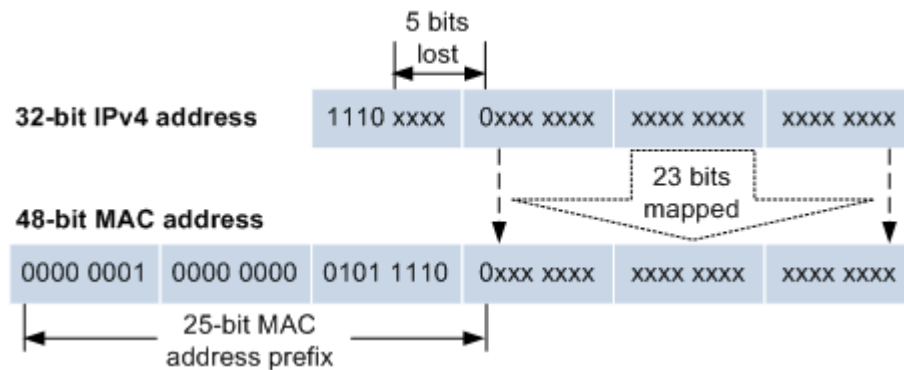
When the Ethernet transmits unicast IP packets, it uses the MAC address of the receiver as the destination MAC address. However, when multicast packets are transmitted, the destination is no longer a specific receiver, but a group with an uncertain number of members, so the Ethernet needs to use the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

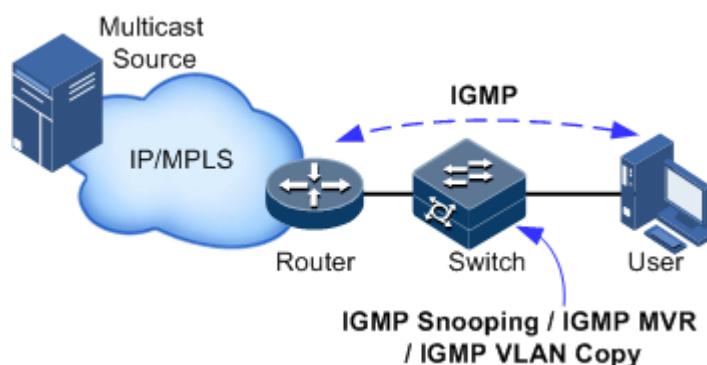
Basis of multicast protocol

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.

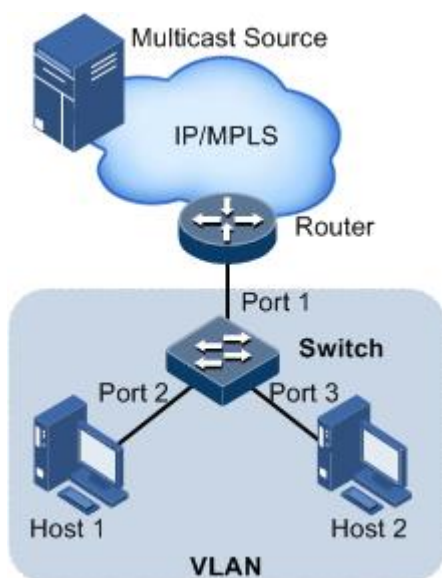
IGMP Snooping establishes a Layer 2 multicast forwarding table, of which entries can be learnt dynamically or configured manually.

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
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 stop }	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-*)#igmp-snooping enable	Enable IGMP Snooping on all VLANs.
6	Raisecom(config-vlan-*)#igmp-snooping version { v1 v2 v3 }	(Optional) configure the protocol version.
7	Raisecom(config-vlan-*)#igmp-snooping forwarding-mode { ip mac }	(Optional) configure the forwarding mode of multicast entries to IP or MAC.
8	Raisecom(config-vlan-*)#igmp-snooping require-router-alert { enable disable }	(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/*)#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-*)#igmp-snooping querier { enable disable }	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-*)#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-*)#igmp-snooping max-response-time <i>response-time</i>	(Optional) configure the maximum response time for query packets.

8	Raisecom(config-vlan-*)#igmp-snooping lastmember-query-interval <i>interval</i>	(Optional) configure the interval for sending specific group query packets.
9	Raisecom(config-vlan-*)#igmp-snooping lastmember-query-number <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-*)#igmp-snooping report-suppress { enable disable }	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-*)#igmp-snooping forwarding-mode <i>ip</i>	Configure the forwarding mode to IP.
4	Raisecom(config-vlan-*)#igmp-snooping multicast-duplicate { enable disable }	Enable multicast copy.
5	Raisecom(config-vlan-*)#igmp-snooping multicast user-vlan <i>vlan-list</i>	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 <i>interface-type interface-number</i>	Enter physical interface configuration mode.

3	Raisecom(config-ge-1/0/*)#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-*)#igmp-snooping workmode igmp-proxy	Configure the working mode to Proxy.
4	Raisecom(config-vlan-*)#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-*)#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 interface-type interface-number	Enter physical interface configuration mode.
3	Raisecom(config-ge-1/0/*)#igmp-snooping group-limit number [action { delay replace }]	Configure the limit on the number of 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 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)#interface interface-type interface-number	Enter physical interface configuration mode.
4	Raisecom(config-ge-1/0/*)#igmp-snooping group-policy acl-ipv4 list-id	Bind the interface multicast policy with the ACL profile.
5	Raisecom(config)#vlan vlan-id	Enter VLAN configuration mode.
6	Raisecom(config-vlan-*)#igmp-snooping group-policy acl-ipv4 list-id	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 the static router interface

Configure the static router interface 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 router-port interface-type interface-number	Configure the static router interface.
4	Raisecom(config-vlan-10)#igmp-snooping router-port drop-report { enable disable }	Configure the static router interface to discard Report packets.
5	Raisecom(config-vlan-10)#igmp-snooping router-port-limit { default value }	Configure the maximum number of static router interfaces.

6.2.13 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- *)#igmp-snooping forwarding- mode ip	Configure the forwarding mode to IP.
5	Raisecom(config-vlan- *)#igmp-snooping version v3	Configure the protocol version to v3.
6	Raisecom(config-vlan- *)#igmp-snooping ssm-mapping { enable disable }	Enable SSM Mapping.
7	Raisecom(config-vlan- *)#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.

6.2.14 Configuring IGMP Snooping multicast MVR

Configure IGMP Snooping multicast MVR 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 mvr enable	Enable multicast MVR. Multicast MVR and multicast VLAN copy cannot be concurrently enabled.
4	Raisecom(config-vlan-10)# igmp- snooping channel group-address group-address-start to group- address-end	Configure the range of multicast channels used by multicast MVR.



Note

Multicast MVR and multicast VLAN copy cannot be concurrently enabled.

6.2.15 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.

6.2.16 Maintenance

Maintain the device as below.

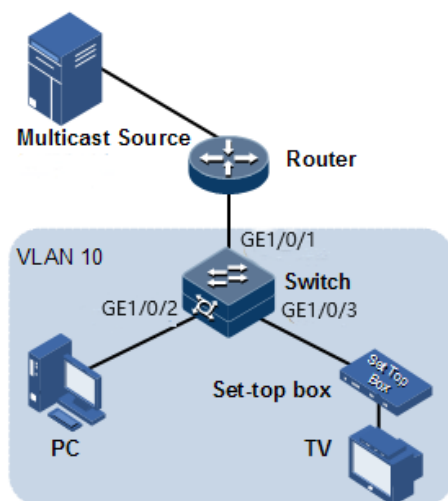
Command	Description
Raisecom(config)#reset igmp-snooping forwarding-table	Clear dynamically learnt multicast entries.
Raisecom(config)#reset igmp-snooping statistics	Clear statistics on IGMP Snooping packets.

6.2.17 Example for configuring basic functions of IGMP Snooping

Networking requirements

As shown below, switch interface GE 1/0/1 is connected to the multicast router. Switch interfaces GE 1/0/2 and GE 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
```

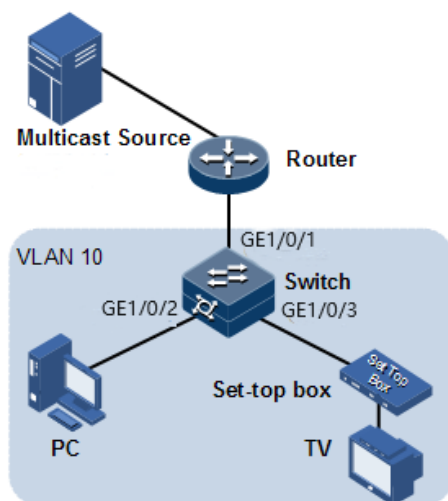
6.2.18 Example for configuring the static member of IGMP Snooping

Networking requirements

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

The user under interface GE 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
```

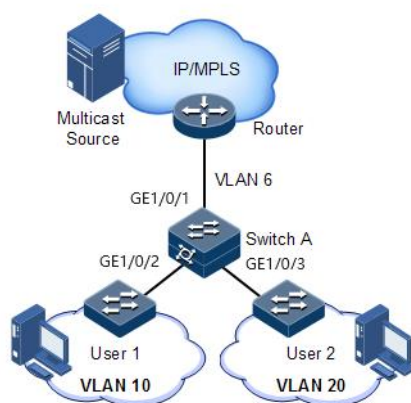
6.2.19 Example for configuring IGMP Snooping multicast copy

Networking requirements

As shown below, switch interface GE 1/0/1 is connected to the multicast router. Switch interfaces GE 1/0/2 and GE 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 GE 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



```
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
```

6.2.20 Example for configuring IGMP Snooping Proxy

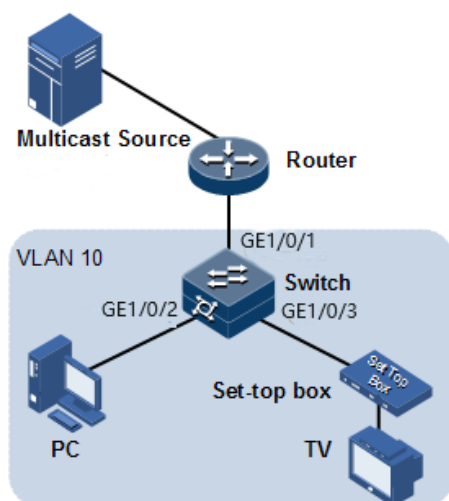
Networking requirements

As shown below, switch interface GE 1/0/1 is connected to the multicast router. Switch interfaces GE 1/0/2 and GE 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
```

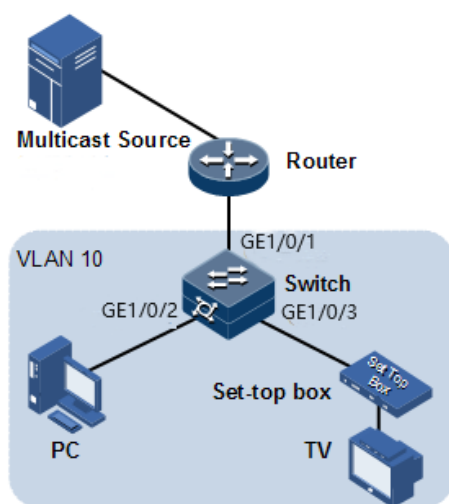
6.2.21 Example for configuring the multicast policy of IGMP Snooping

Networking requirements

As shown below, switch interface GE 1/0/1 is connected to the multicast router. Switch interfaces GE 1/0/2 and GE 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 GE 1/0/2 to join 225.1.1.1 to 225.1.1.3 and the user under interface GE 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 1/0/2
Raisecom(config-ge-1/0/2)#igmp-snooping group-policy acl-ipv4 1001
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#igmp-snooping group-policy acl-ipv4 1002
Raisecom(config-ge-1/0/3)#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 1/0/2
  igmp-snooping enable
  igmp-snooping group-policy acl-ipv4 1001 version 1-3
!
interface ge 1/0/3
  igmp-snooping enable
  igmp-snooping group-policy acl-ipv4 1002 version 1-3
```

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

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

6.3 MLD Snooping

6.3.1 Introduction

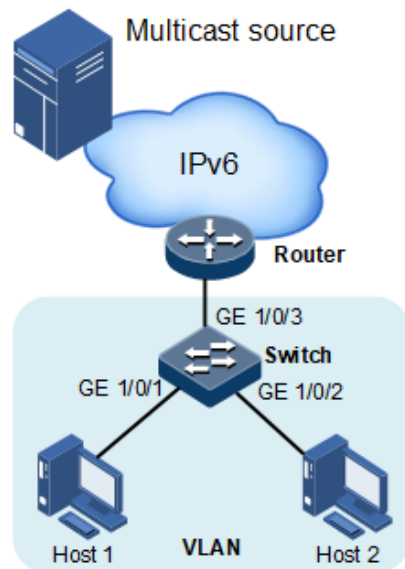
MLD Snooping is an IPv6 Layer 2 multicast protocol, which listens to multicast protocol packets sent between Layer 3 multicast devices and user hosts, maintains the information about the egress interface of the group broadcast packet, and then manage and control the forwarding of multicast data packets.

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
Maximum response time for sending Query packets	10s
Aging time of the router interface	180s

Function	Default value
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 stop }	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-*)#mld-snooping { enable disable }	Enable MLD Snooping on all VLANs.
6	Raisecom(config-vlan-*)#mld-snooping version { v1 v2 }	(Optional) configure the protocol version.
7	Raisecom(config-vlan-*)#mld-snooping forwarding-mode { ip mac }	(Optional) configure the forwarding mode of multicast entries to IP or MAC.
8	Raisecom(config-vlan-*)#mld-snooping require-router-alert { enable disable }	(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/*)#mld-snooping { enable disable }	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-*)#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-*)#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-*)#mld-snooping max-response-time <i>response-time</i>	(Optional) configure the maximum response time for query packets.
8	Raisecom(config-vlan-*)#mld-snooping lastmember-query-interval <i>interval</i>	(Optional) configure the interval for sending specific group query packets.
9	Raisecom(config-vlan-*)#mld-snooping lastmember-query-number <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-*)#mld-snooping report-suppress { enable disable }	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-*)#mld-snooping forwarding-mode ip	Configure the forwarding mode to IP.
4	Raisecom(config-vlan-*)#mld-snooping multicast-duplicate { enable disable }	Enable multicast copy.
5	Raisecom(config-vlan-*)#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/*)#mld-snooping static-group group-address group-address 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-*)#mld-snooping workmode mld-proxy	Configure the working mode to Proxy.
4	Raisecom(config-vlan-*)#mld-snooping querier { enable disable }	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 { <i>delay</i> <i>replace</i> }]	Configure the limit on the number of interface multicast groups of MLD Snooping.

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-*)#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 <i>vlan-id</i>	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-*)#mld-snooping ssm-mapping { enable disable }	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 Configuring MLD Snooping multicast MVR

Configure MLD Snooping multicast MVR 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)# mld-snooping mvr enable	Enable multicast MVR. Multicast MVR and multicast VLAN copy cannot be concurrently enabled.
4	Raisecom(config-vlan-10)# mld-snooping channel group-address group-address-start to group-address-end	Configure the range of multicast channels used by multicast MVR.



Note

Multicast MVR and multicast VLAN copy cannot be concurrently enabled.

6.3.14 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.

No.	Command	Description
4	Raisecom#show mld-snooping forwarding-table	Show multicast entries of MLD Snooping.

6.3.15 Maintenance

Maintain the device as below.

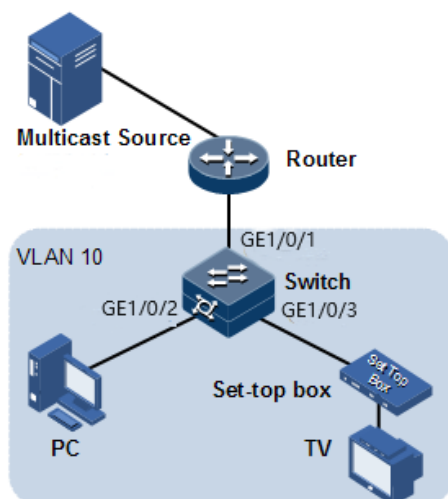
Command	Description
Raisecom(config)#reset mld-snooping forwarding-table	Clear dynamically learnt multicast entries.

6.3.16 Example for configuring basic functions of MLD Snooping

Networking requirements

As shown below, switch interface GE 1/0/1 is connected to the multicast router. Switch interfaces GE 1/0/2 and GE 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
```

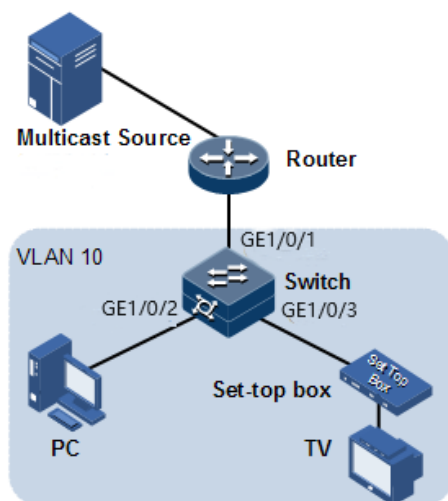

6.3.17 Example for configuring the static member of MLD Snooping

Networking requirements

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

The user under interface GE 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
```

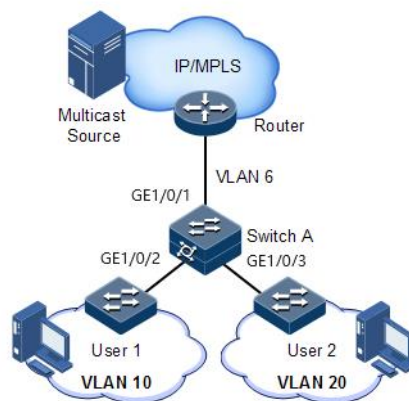
6.3.18 Example for configuring MLD Snooping multicast copy

Networking requirements

As shown below, switch interface GE 1/0/1 is connected to the multicast router. Switch interfaces GE 1/0/2 and GE 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 GE 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
```

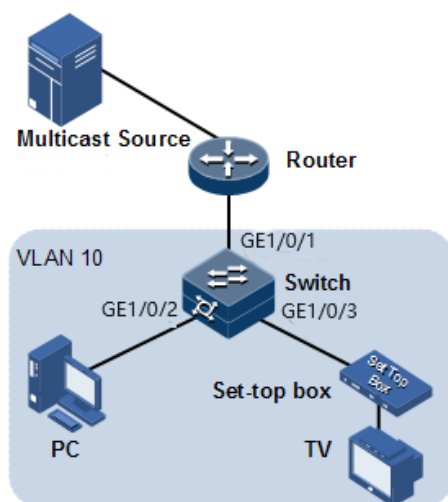
6.3.19 Example for configuring MLD Snooping Proxy

Networking requirements

As shown below, switch GE interface 1/0/1 is connected to the multicast router. Switch GE interfaces 1/0/2 and 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
```

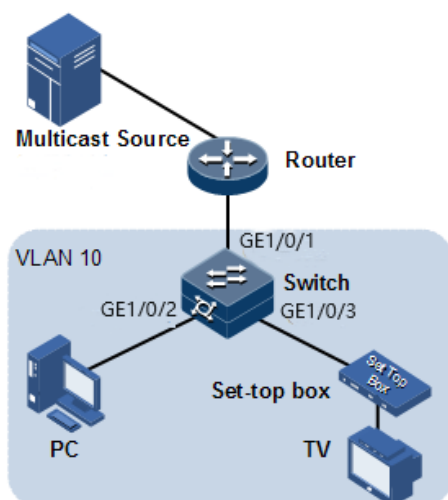
6.3.20 Example for configuring the multicast policy of MLD Snooping

Networking requirements

As shown below, switch interface GE 1/0/1 is connected to the multicast router. Switch interfaces GE 1/0/2 and GE 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 GE 1/0/2 to join ff1e::1 to ff1e::3 and the user under interface GE 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 1/0/2
```



```
Raisecom(config-ge-1/0/2)#mld-snooping group-policy acl-ipv6 3001
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#mld-snooping group-policy acl-ipv6 3002
Raisecom(config-ge-1/0/3)#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 1/0/2
  mld-snooping enable
  mld-snooping group-policy acl-ipv6 3001 version 1-2
!
interface ge 1/0/3
  mld-snooping enable
  mld-snooping group-policy acl-ipv6 3002 version 1-2
!
```

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
```

6.4 IGMP

6.4.1 Introduction

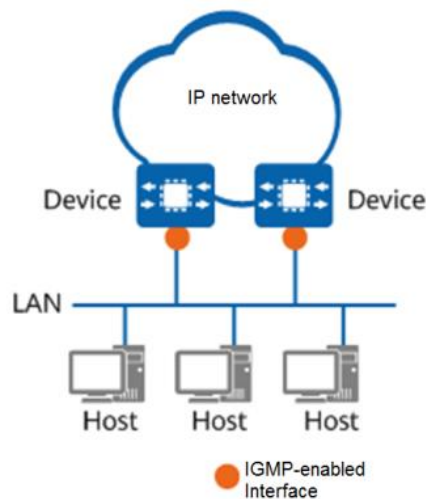
IP multicast communication is that packets are sent from a source and forwarded to a specific group of receivers, but in multicast communication models, the sender does not pay attention to the receiver location. To enable multicast packets to ultimately reach the receiver host, a mechanism is needed to enable the multicast device connected to the receiver network segment to learn multicast receivers existing in that network segment, and to ensure that the receivers can join the corresponding multicast groups. IGMP is a protocol used to establish and maintain multicast group membership between the receiver host and multicast devices directly adjacent to its network segment.

6.4.2 Preparing for configurations

Scenario

As shown below, multiple hosts receive data from the multicast source.

Figure 6-17 Location of IGMP on the multicast network



Prerequisites

Enable PIM on the IGMP-enabled interface.

6.4.3 Default configurations of IGMP

Default configurations of IGMP are as below.

Function	Default value
Global IGMP status	Disable
Interface IGMP status	Disable
IGMP version	v2

Function	Default value
General querying interval	125s
Robustness factor	2
Maximum response time	10s
Keepalive time of other queriers	255s

6.4.4 Enabling IGMP

Enable IGMP for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#pim { vpn-instance vpn-name }	Create a PIM instance.  Note IGMP relies on PIM.
3	Raisecom(config)#igmp { vpn-instance vpn-name }	Create an IGMP instance.
4	Raisecom(config)#interface vlan vlan-id	Enter the VLANIF configuration view.
5	Raisecom(config-vlanif-10)#pim enable { sm dm }	Enable PIM.
6	Raisecom(config-vlanif-10)#igmp enable	Enable IGMP.
7	Raisecom(config-vlanif-10)#igmp version { v1 v2 v3 }	(Optional) configure the IGMP version.

6.4.5 Configuring parameters of the IGMP querier

Configure parameters of the IGMP querier for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface vlan vlan-id	Enter the VLANIF configuration view.
3	Raisecom(config-vlanif-10)#igmp timer query interval	Configure the querying interval, in units of second.
4	Raisecom(config-vlanif-10)#igmp robust-count robust-value	Configure the robust factor of the querier.

5	Raisecom(config-vlanif-10)#igmp timer other-querier-present interval	Configure the Keepalive time of other IGMP queriers.

6.4.6 Configuring IGMP immediate leave

Configure IGMP immediate leave 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 the VLANIF configuration view.
3	Raisecom(config-vlanif-10)#igmp fast-leave enable	Enable immediate leave.  Note Immediate leave takes effect on IGMPv2 only.

6.4.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show igmp config	Show IGMP configurations.

6.4.8 Maintenance

Maintain the device as below.

Command	Description
Raisecom#show igmp interface	Show information about the IGMP interface.
Raisecom#show igmp routing-table	Show information about the IGMP multicast table.
Raisecom#show igmp { public-net vpn-instance <i>vpn-name</i> }	Show information about the IGMP instance.

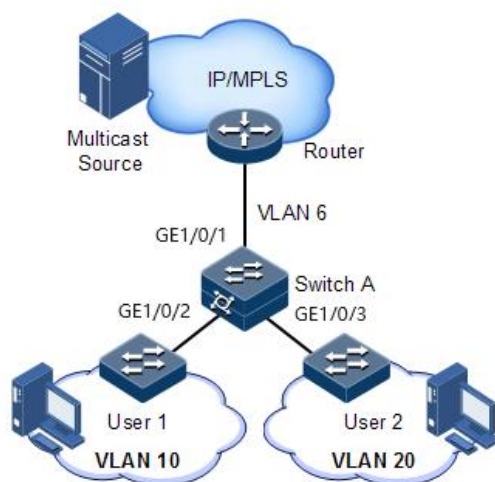
6.4.9 Example for configuring basic functions of IGMP

Networking requirements

As shown below, interface Gig Ethernet 1/0/1 on the switch is connected to the multicast router, while interfaces Gig Ethernet 1/0/2 and Gig Ethernet 1/0/3 are connected to the user. The multicast VLAN and user VLAN are different, and IGMP basic functions are configured.

- GE 1/0/1 joins VLAN 6, user 1 joins VLAN 10, and user 2 joins VLAN 20.
- Multicast router interface IP address 203.6.1.1/24
- IP address of the interface of user 1: 10.1.1.1/24
- IP address of the interface of user 2: 20.1.1.1/24

Figure 6-18 Networking with basic functions of IGMP



Configuration steps

Step 1 Create VLANs, and add interfaces to VLANs.

```
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 Configure IP addresses of interfaces.

```
Raisecom(config)#interface vlan 6
Raisecom(config-vlanif-6)#ip address 203.6.1.1/24
Raisecom(config-vlanif-6)#quit
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#ip address 10.1.1.1/24
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#ip address 20.1.1.1/24
Raisecom(config-vlanif-20)#quit
```

Step 3 Configure basic functions of PIM-SM and IGMP.

```
Raisecom(config)#pim
Raisecom(config-pim)#quit
Raisecom(config)#igmp
Raisecom(config-igmp)#quit
Raisecom(config)#interface vlan 6
Raisecom(config-vlanif-6)#pim enable sm
Raisecom(config-vlanif-6)#igmp enable
Raisecom(config-vlanif-6)#quit
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#pim enable sm
Raisecom(config-vlanif-10)#igmp enable
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#pim enable sm
Raisecom(config-vlanif-20)#igmp enable
Raisecom(config-vlanif-20)#quit
```

Checking results

Use the following command to check IGMP configurations.

```
Raisecom#show igmp config
!
igmp
!
interface vlan 6
igmp enable
!
interface vlan 10
igmp enable
!
interface vlan 20
igmp enable
```

Use the following command to check PIM configurations.

```
Raisecom#show pim config
!
pim
!
interface vlan 6
  pim enable sm
!
interface vlan 10
  pim enable sm
!
interface vlan 20
  pim enable sm
```

6.5 PIM

6.5.1 Introduction

Protocol Independent Multicast (PIM) is an intra-domain multicast routing protocol that utilizes unicast routing information to perform RPF checks on multicast packets and create multicast routing entries. The protocol that provides routing information for IP multicast can be any unicast routing protocol, such as the static routing, RIP, OSPF, IS-IS, and BGP. Multicast routes are not related to unicast routing protocols, but generates corresponding multicast routing entries through unicast routing tables.

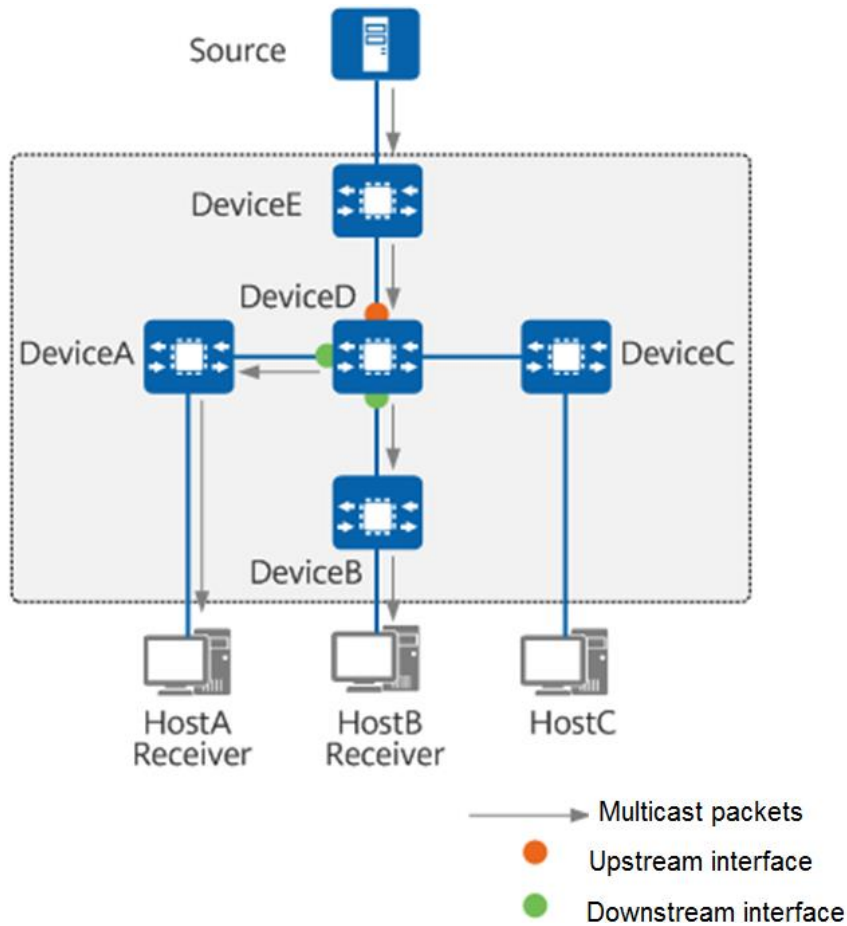
On the network, multicast data needs to be replicated and forwarded through a multicast network from the multicast source to the receiver. To build a multicast network, configure multicast protocols on the network. PIM is currently the most widely used domain multicast protocol. The multicast spanning tree constructed through PIM can be used to guide multicast data forwarding on the network.

PIM can implement on-demand creation of multicast routes, dynamic response to network topology changes, and forwarding packets according to routing entries.

6.5.2 Preparing for configurations

Scenario

Figure 6-19 Location of PIM on the multicast network



Prerequisites

N/A

6.5.3 Default configurations of PIM

Default configurations of PIM are as below.

Function	Default value
Global PIM status	Disable
Interface PIM status	Disable
DR priority	1
Interval for sending Hello packets	30s

Function	Default value
SPT switching condition	Switch STP when the RP or the DR of the group member receives the first multicast data packet.
BFD	Disable
PIM Silent	Disable

6.5.4 Configuring PIM-DM

Configure PIM-DM for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#pim { vpn-instance <i>vpn-name</i> }	Create a PIM instance.
3	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter the VLANIF configuration view.
4	Raisecom(config-vlanif-10)#pim enable dm	Enable PIM-DM.

6.5.5 Configuring PIM-SM

Configure PIM-SM for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#pim { vpn-instance <i>vpn-name</i> }	Create a PIM instance.
3	Raisecom(config-pim)#rp-address <i>ip-address</i> group all-multicast	(Optional) configure the static RP.
4	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter the VLANIF configuration view.
5	Raisecom(config-vlanif-10)#pim enable sm	Enable PIM-SM.
6	Raisecom(config-vlanif-10)#pim c-rp group all-multicast	(Optional) configure the candidate RP.
7	Raisecom(config-vlanif-10)#pim c-bsr group all-multicast	(Optional) configure the candidate BSR.

6.5.6 Configuring the BSR management domain of PIM-SM

Configure the BSR management domain of PIM-SM for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#pim { vpn-instance <i>vpn-name</i> }	Create a PIM instance.
3	Raisecom(config-pim)#c-bsr admin-scope enable	Enable the BSR management domain of PIM-SM.
4	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter the VLANIF configuration view.
5	Raisecom(config-vlanif-10)#pim enable sm	Enable PIM-SM.
6	Raisecom(config-vlanif-10)#pim c-rp group <i>group-address/group-mask len</i>	(Optional) configure the group address range of the candidate RP service of the management domain.
7	Raisecom(config-vlanif-10)#pim c-bsr group <i>group-address/group-mask len</i>	(Optional) configure the group address range of the candidate BSR service of the management domain.
8	Raisecom(config-vlanif-10)#pim bsr-boundary group <i>group-address/group-mask len</i>	(Optional) configure the boundary of the BSR management domain.

6.5.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show pim config	Show PIM configurations.

6.5.8 Maintenance

Maintain the device as below.

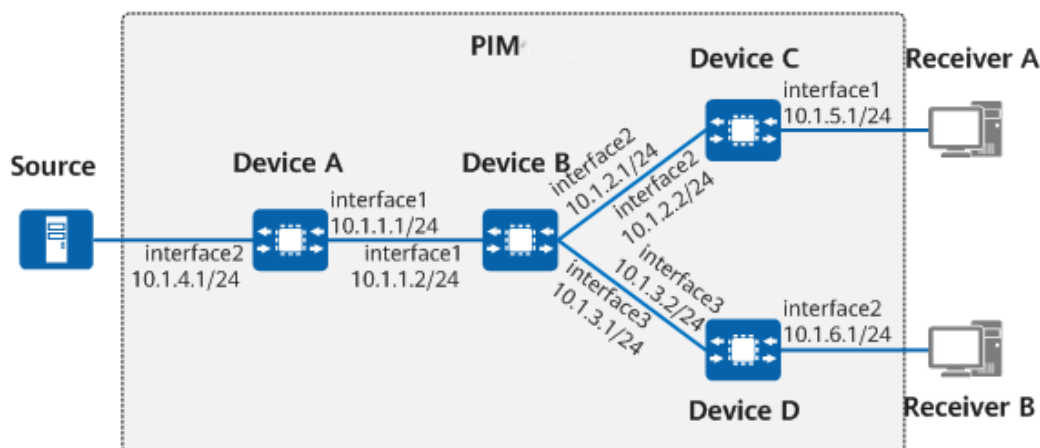
Command	Description
Raisecom#show pim interface	Show information about the PIM interface.
Raisecom#show pim routing-table	Show information about the PIM multicast table.
Raisecom#show pim { public-net vpn-instance <i>vpn-name</i> }	Show information about the PIM instance.

6.5.9 Example for configuring PIM-DM

Networking requirements

Deploy multicast on the devices so that the user host (receiver) can receive Video on Demand (VoD) information through multicast.

Figure 6-20 PIM-DM networking



Configuration steps

Step 1 Create VLANs, and add interfaces to VLANs.

Device A

```
Raisecom#configure
Raisecom(config)#vlan 10,20
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port hybrid vlan 10 untagged
Raisecom(config-ge-1/0/1)#port hybrid pvid 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port hybrid vlan 20 untagged
Raisecom(config-ge-1/0/2)#port hybrid pvid 20
Raisecom(config-ge-1/0/2)#quit
```

Device B

```
Raisecom#configure
Raisecom(config)#vlan 10,20,30
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port hybrid vlan 10 untagged
Raisecom(config-ge-1/0/1)#port hybrid pvid 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port hybrid vlan 20 untagged
```

```
Raisecom(config-ge-1/0/2)#port hybrid pvid 20
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port hybrid vlan 30 untagged
Raisecom(config-ge-1/0/3)#port hybrid pvid 30
Raisecom(config-ge-1/0/3)#quit
```

Device C

```
Raisecom#configure
Raisecom(config)#vlan 10,20
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port hybrid vlan 10 untagged
Raisecom(config-ge-1/0/1)#port hybrid pvid 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port hybrid vlan 20 untagged
Raisecom(config-ge-1/0/2)#port hybrid pvid 20
Raisecom(config-ge-1/0/2)#quit
```

Device D

```
Raisecom#configure
Raisecom(config)#vlan 20,30
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port hybrid vlan 20 untagged
Raisecom(config-ge-1/0/2)#port hybrid pvid 20
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port hybrid vlan 30 untagged
Raisecom(config-ge-1/0/3)#port hybrid pvid 30
Raisecom(config-ge-1/0/3)#quit
```

Step 2 Configure IP addresses of interfaces.

Device A

```
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#ip address 10.1.1.1/24
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#ip address 10.1.4.1/24
Raisecom(config-vlanif-20)#quit
```

Device B

```
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#ip address 10.1.1.2/24
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#ip address 10.1.2.1/24
Raisecom(config-vlanif-20)#quit
Raisecom(config)#interface vlan 30
Raisecom(config-vlanif-30)#ip address 10.1.3.1/24
Raisecom(config-vlanif-30)#quit
```

Device C

```
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#ip address 10.1.5.1/24
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#ip address 10.1.2.2/24
Raisecom(config-vlanif-20)#quit
```

Device D

```
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#ip address 10.1.6.1/24
Raisecom(config-vlanif-20)#quit
Raisecom(config)#interface vlan 30
Raisecom(config-vlanif-30)#ip address 10.1.3.2/24
Raisecom(config-vlanif-30)#quit
```

Step 3 Configure OSPF unicast routes.

Device A

```
Raisecom(config)#ospf 1
Raisecom(config-ospf-1)#router-id 1.1.1.1
Raisecom(config-ospf-1)#network 10.0.0.0 255.0.0.0 area 0
```

Device B

```
Raisecom(config)#ospf 1
Raisecom(config-ospf-1)#router-id 2.2.2.2
Raisecom(config-ospf-1)#network 10.0.0.0 255.0.0.0 area 0
```

Device C

```
Raisecom(config)#ospf 1
Raisecom(config-ospf-1)#router-id 3.3.3.3
Raisecom(config-ospf-1)#network 10.0.0.0 255.0.0.0 area 0
```

Device D

```
Raisecom(config)#ospf 1
Raisecom(config-ospf-1)#router-id 4.4.4.4
Raisecom(config-ospf-1)#network 10.0.0.0 255.0.0.0 area 0
```

Step 4 Configure PIM-DM and IGMP.

Device A

```
Raisecom(config)#pim
Raisecom(config-pim)#quit
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#pim enable dm
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#pim enable dm
Raisecom(config-vlanif-20)#quit
```

Device B

```
Raisecom(config)#pim
Raisecom(config-pim)#quit
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#pim enable dm
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#pim enable dm
Raisecom(config-vlanif-20)#quit
Raisecom(config)#interface vlan 30
Raisecom(config-vlanif-30)#pim enable dm
Raisecom(config-vlanif-30)#quit
```

Device C

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

```
Raisecom(config-pim)#quit
Raisecom(config)#igmp
Raisecom(config-igmp)#quit
Raisecom(config-pim)#quit
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#pim enable dm
Raisecom(config-vlanif-10)#igmp enable
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#pim enable dm
Raisecom(config-vlanif-20)#quit
```

Device D

```
Raisecom(config)#pim
Raisecom(config-pim)#quit
Raisecom(config)#igmp
Raisecom(config-igmp)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#pim enable dm
Raisecom(config-vlanif-20)#igmp enable
Raisecom(config-vlanif-20)#quit
Raisecom(config)#interface vlan 30
Raisecom(config-vlanif-30)#pim enable dm
Raisecom(config-vlanif-30)#quit
```

Checking results

Use the following command to check PIM configurations.

Device A:

```
Raisecom#show pim config
!
pim
!
interface vlan 10
  pim enable dm
!
interface vlan 20
  pim enable dm
```

Device B:

```
Raisecom#show pim config
!
pim
```

```
!  
interface vlan 10  
  pim enable dm  
!  
interface vlan 20  
  pim enable dm  
!  
interface vlan 30  
  pim enable dm
```

Device C:

```
Raisecom#show pim config  
!  
pim  
!  
interface vlan 10  
  pim enable dm  
!  
interface vlan 20  
  pim enable dm
```

Device D:

```
Raisecom#show pim config  
!  
pim  
!  
interface vlan 20  
  pim enable dm  
!  
interface vlan 30  
  pim enable dm
```

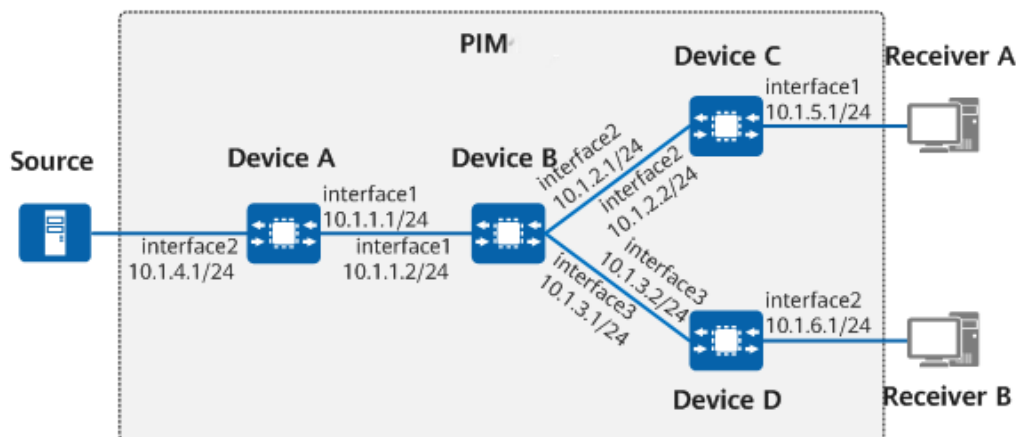
6.5.10 Example for configuring PIM-SM

Networking requirements

Deploy multicast on the devices so that the user host (receiver) can receive Video on Demand (VoD) information through multicast.

Configure the candidate RP and candidate BSR on Device A and Device B.

Figure 6-21 PIM-SM networking



Configuration steps

Step 1 Create VLANs, and add interfaces to VLANs.

Device A

```
Raisecom#configure
Raisecom (config)#vlan 10,20
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port hybrid vlan 10 untagged
Raisecom(config-ge-1/0/1)#port hybrid pvid 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port hybrid vlan 20 untagged
Raisecom(config-ge-1/0/2)#port hybrid pvid 20
Raisecom(config-ge-1/0/2)#quit
```

Device B

```
Raisecom#configure
Raisecom(config)#vlan 10,20,30
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port hybrid vlan 10 untagged
Raisecom(config-ge-1/0/1)#port hybrid pvid 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port hybrid vlan 20 untagged
Raisecom(config-ge-1/0/2)#port hybrid pvid 20
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port hybrid vlan 30 untagged
Raisecom(config-ge-1/0/3)#port hybrid pvid 30
Raisecom(config-ge-1/0/3)#quit
```

Device C

```
Raisecom#configure
Raisecom(config)#vlan 10,20
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port hybrid vlan 10 untagged
Raisecom(config-ge-1/0/1)#port hybrid pvid 10
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port hybrid vlan 20 untagged
Raisecom(config-ge-1/0/2)#port hybrid pvid 20
Raisecom(config-ge-1/0/2)#quit
```

Device D

```
Raisecom#configure
Raisecom(config)#vlan 20,30
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port hybrid vlan 20 untagged
Raisecom(config-ge-1/0/2)#port hybrid pvid 20
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#port hybrid vlan 30 untagged
Raisecom(config-ge-1/0/3)#port hybrid pvid 30
Raisecom(config-ge-1/0/3)#quit
```

Step 2 Configure IP addresses of interfaces.

Device A

```
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#ip address 10.1.1.1/24
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#ip address 10.1.4.1/24
Raisecom(config-vlanif-20)#quit
```

Device B

```
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#ip address 10.1.1.2/24
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#ip address 10.1.2.1/24
Raisecom(config-vlanif-20)#quit
Raisecom(config)#interface vlan 30
```

```
Raisecom(config-vlanif-30)#ip address 10.1.3.1/24
Raisecom(config-vlanif-30)#quit
```

Device C

```
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#ip address 10.1.5.1/24
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#ip address 10.1.2.2/24
Raisecom(config-vlanif-20)#quit
```

Device D

```
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#ip address 10.1.6.1/24
Raisecom(config-vlanif-20)#quit
Raisecom(config)#interface vlan 30
Raisecom(config-vlanif-30)#ip address 10.1.3.2/24
Raisecom(config-vlanif-30)#quit
```

Step 3 Configure OSPF unicast routes.

Device A

```
Raisecom(config)#ospf 1
Raisecom(config-ospf-1)#router-id 1.1.1.1
Raisecom(config-ospf-1)#network 10.0.0.0 255.0.0.0 area 0
```

Device B

```
Raisecom(config)#ospf 1
Raisecom(config-ospf-1)#router-id 2.2.2.2
Raisecom(config-ospf-1)#network 10.0.0.0 255.0.0.0 area 0
```

Device C

```
Raisecom(config)#ospf 1
Raisecom(config-ospf-1)#router-id 3.3.3.3
Raisecom(config-ospf-1)#network 10.0.0.0 255.0.0.0 area 0
```

Device D

```
Raisecom(config)#ospf 1
Raisecom(config-ospf-1)#router-id 4.4.4.4
Raisecom(config-ospf-1)#network 10.0.0.0 255.0.0.0 area 0
```

Step 4 Configure PIM-SM and IGMP.

Device A

```
Raisecom(config)#pim
Raisecom(config-pim)#quit
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#pim enable sm
Raisecom(config-vlanif-10)#pim c-rp group all-multicast
Raisecom(config-vlanif-10)#pim c-bsr group all-multicast
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#pim enable sm
Raisecom(config-vlanif-20)#quit
```

Device B

```
Raisecom(config)#pim
Raisecom(config-pim)#quit
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#pim enable sm
Raisecom(config-vlanif-10)#pim c-rp group all-multicast
Raisecom(config-vlanif-10)#pim c-bsr group all-multicast
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#pim enable sm
Raisecom(config-vlanif-20)#quit
Raisecom(config)#interface vlan 30
Raisecom(config-vlanif-30)#pim enable sm
Raisecom(config-vlanif-30)#quit
```

Device C

```
Raisecom(config)#pim
Raisecom(config-pim)#quit
Raisecom(config)#igmp
Raisecom(config-igmp)#quit
Raisecom(config-pim)#quit
Raisecom(config)#interface vlan 10
Raisecom(config-vlanif-10)#pim enable sm
Raisecom(config-vlanif-10)#igmp enable
Raisecom(config-vlanif-10)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#pim enable sm
```

```
Raisecom(config-vlanif-20)#quit
```

Device D

```
Raisecom(config)#pim
Raisecom(config-pim)#quit
Raisecom(config)#igmp
Raisecom(config-igmp)#quit
Raisecom(config)#interface vlan 20
Raisecom(config-vlanif-20)#pim enable sm
Raisecom(config-vlanif-20)#igmp enable
Raisecom(config-vlanif-20)#quit
Raisecom(config)#interface vlan 30
Raisecom(config-vlanif-30)#pim enable sm
Raisecom(config-vlanif-30)#quit
```

Checking results

Use the following commands to check PIM configurations.

Device A:

```
Raisecom#show pim config
!
pim
!
interface vlan 10
  pim enable sm
  pim c-bsr group all-multicast
  pim c-rp group all-multicast
!
interface vlan 20
  pim enable sm
```

Device B:

```
Raisecom#show pim config
!
pim
!
interface vlan 10
  pim enable sm
  pim c-bsr group all-multicast
  pim c-rp group all-multicast
!
interface vlan 20
  pim enable sm
```

```
!  
interface vlan 30  
  pim enable sm
```

Device C:

```
Raisecom#show pim config  
!  
pim  
!  
interface vlan 10  
  pim enable sm  
!  
interface vlan 20  
  pim enable sm
```

Device D:

```
Raisecom#show pim config  
!  
pim  
!  
interface vlan 20  
  pim enable sm  
!  
interface vlan 30  
  pim enable sm
```

6.6 MLD

6.6.1 Introduction

IP multicast communication is that packets are sent from a source and forwarded to a specific group of receivers, but in multicast communication models, the sender does not pay attention to the receiver location. To enable multicast packets to ultimately reach the receiver host, a mechanism is needed to enable the multicast device connected to the receiver network segment to learn multicast receivers existing in that network segment, and to ensure that the receivers can join the corresponding multicast groups. Multicast Listener Discovery (MLD) is a protocol used to establish and maintain multicast group membership between the receiver host and multicast devices directly adjacent to its network segment.

6.6.2 Preparing for configurations

Scenario

See the IGMP test scenario.

Prerequisites

Configure PIM-IPv6 on the MLD-enabled interface.

6.6.3 Default configurations of MLD

Default configurations of MLD are as below.

Function	Default value
Global MLD status	Disable
Interface MLD status	Disable
MLD version	v2
General querying interval	125s
Robustness factor	2
Maximum response time	10s
Keepalive time of other queriers	255s

6.6.4 Enabling MLD

Enable MLD for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#pim-ipv6 { vpn-instance vpn-name }	Create a PIM IPv6 instance.  Note MLD relies on PIM IPv6.
3	Raisecom(config)#mld { vpn- instance vpn-name }	Create an MLD instance.
4	Raisecom(config)#interface vlan vlan-id	Enter the VLANIF configuration view.
5	Raisecom(config-vlanif- 10)#ipv6 enable	Enable IPv6.
6	Raisecom(config-vlanif- 10)#pim-ipv6 enable { sm dm }	Enable PIM.
7	Raisecom(config-vlanif-10)#mld enable	Enable MLD.

8	Raisecom(config-vlanif-10)#mld version { v1 v2 }	(Optional) configure the MLD version.

6.6.5 Configuring parameters of the MLD querier

Configure parameters of the MLD querier for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter the VLANIF configuration view.
3	Raisecom(config-vlanif-10)#mld timer query <i>interval</i>	Configure the querying interval, in units of second.
4	Raisecom(config-vlanif-10)#mld robust-count <i>robust-value</i>	Configure the robust factor of the querier.
5	Raisecom(config-vlanif-10)#mld timer other-querier-present <i>interval</i>	Configure the Keepalive time of other IGMP queriers.

6.6.6 Configuring MLD immediate leave

Configure immediate leave for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter the VLANIF configuration view.
3	Raisecom(config-vlanif-10)#mld fast-leave enable	Enable immediate leave.  Note Immediate leave takes effect on MLD v1 only.

6.6.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show mld config	Show MLD configurations.

6.6.8 Maintenance

Maintain the device as below.

Command	Description
Raisecom#show mld interface	Show information about the MLD interface.
Raisecom#show mld routing-table	Show information about the MLD multicast table.
Raisecom#show mld { public-net vpn-instance <i>vpn-name</i> }	Show information about the MLD instance.

6.6.9 Example for configuring basic functions of MLD

See the example for configuring basic functions of IGMP.

6.7 PIMv6

6.7.1 Introduction

See the introduction to PIM.

6.7.2 Preparing for configurations

Scenario

See the scenario of PIM.

Prerequisites

N/A

6.7.3 Default configurations of PIMv6

Default configurations of PIMv6 are as below.

Function	Default value
Global PIMv6 status	Disable
Interface PIMv6 status	Disable
DR priority	1
Interval for sending Hello packets	30 s
SPT switching condition	Switch STP when the RP or the DR of the group member receives the first multicast data packet.
BFD	Disable

6.7.4 Configuring PIMv6-DM

Configure PIMv6-DM for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#pim-ipv6 { vpn-instance vpn-name }	Create a PIM IPv6 instance.
3	Raisecom(config)#interface vlan vlan-id	Enter the VLANIF configuration view.
4	Raisecom(config-vlanif-10)#ipv6 enable	Enable IPv6.
5	Raisecom(config-vlanif-10)#pim-ipv6 enable dm	Enable PIMv6-DM.

6.7.5 Configuring PIM-SM

Configure PIM-SM for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#pim-ipv6 { vpn-instance vpn-name }	Create a PIM IPv6 instance.
3	Raisecom(config-pim6)#rp-address ipv6-address group all-multicast	(Optional) configure the static RP.
4	Raisecom(config)#interface vlan vlan-id	Enter the VLANIF configuration view.
5	Raisecom(config-vlanif-10)#ipv6 enable	Enable IPv6.
6	Raisecom(config-vlanif-10)#pim-ipv6 enable sm	Enable PIMv6-SM.
7	Raisecom(config-vlanif-10)#pim-ipv6 c-rp group all-multicast	(Optional) configure the candidate RP.
8	Raisecom(config-vlanif-10)#pim-ipv6 c-bsr group all-multicast	(Optional) configure the candidate BSR.

6.7.6 Configuring the BSR management domain of PIM-SM

Configure the BSR management domain of PIM-SM for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#pim-ipv6 { vpn-instance vpn-name }	Create a PIM IPv6 instance.

3	Raisecom(config-pim6)#c-bsr admin-scope enable	Enable the BSR management domain of PIM-SM.
4	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter the VLANIF configuration view.
5	Raisecom(config-vlanif-10)#ipv6 enable	Enable IPv6.
6	Raisecom(config-vlanif-10)#pim-ipv6 enable sm	Enable PIMv6-SM.
7	Raisecom(config-vlanif-10)#pim-ipv6 c-rp group <i>group-address/group-mask len</i>	(Optional) configure the group address range of the candidate RP service of the management domain.
8	Raisecom(config-vlanif-10)#pim-ipv6 c-bsr group <i>group-address/group-mask len</i>	(Optional) configure the group address range of the candidate BSR service of the management domain.
9	Raisecom(config-vlanif-10)#pim-ipv6 bsr-boundary group <i>group-address/group-mask len</i>	(Optional) configure the boundary of the BSR management domain.

6.7.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show pim-ipv6 config	Show PIMv6 configurations.

6.7.8 Maintenance

Maintain the device as below.

Command	Description
Raisecom#show pim-ipv6 interface	Show information about the PIMv6 interface.
Raisecom#show pim-ipv6 routing-table	Show information about the PIMv6 multicast table.
Raisecom#show pim-ipv6 { public-net vpn-instance <i>vpn-name</i> }	Show information about the PIMv6 instance.

6.7.9 Example for configuring PIMv6-DM

See the example for configuring PIM-DM.

6.7.10 Example for configuring PIMv6-SM

See the example for configuring PIMv6-SM.

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.

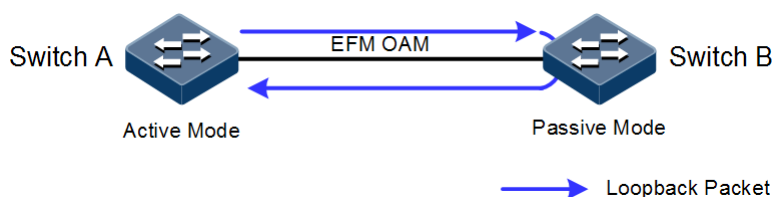
Remote loopback

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 ge 1/0/1	Enter physical interface configuration mode. • <i>interface-type</i>: interface type • <i>interface-number</i>: interface ID
3	Raisecom(config-ge-1/0/*)#efm max-rate value Example: Raisecom(config-ge-1/0/1)#efm max-rate max-rate	(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. • <i>value</i>: number of sent PDUs per unit time
4	Raisecom(config-ge-1/0/*)#efm min-rate min-rate Example: Raisecom(config-ge-1/0/1)#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. • <i>value</i>: timeout time
5	Raisecom(config-ge-1/0/*)#efm mode { active passive } Raisecom(config-ge-1/0/1)#exit Example: Raisecom(config-ge-1/0/1)#efm active	Configure the working mode of EFM OAM. At least one end is in active mode before configuration; otherwise, link detection cannot proceed. • <i>active</i>: in the active mode, the interface actively sends OAM PDUs to initiate end-to-end discovery or remote loopback processes. • <i>passive</i>: in the passive mode, the interface passively waits for the OAM PDU sent by the peer end.
6	Raisecom(config-ge-1/0/*)#exit	Enter global configuration mode.
7	Raisecom(config-ge-1/0/*)#efm { enable disable } Example: Raisecom(config-ge-1/0/1)#efm enable	Enable interface EFM OAM. • <i>Enable</i>: enable interface EFM OAM. • <i>Disable</i>: 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-ge-1/0/*)#efm remote-loopback timeout value Example: Raisecom(config-ge-1/0/1)#efm remote-loopback timeout 5	(Optional) configure the local waiting time for response, which is the response timeout time. 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-ge-1/0/*)#efm remote-loopback { supported unsupported } Example: Raisecom(config-ge-1/0/*)#efm min-rate 5	Configure remote loopback to be supported or unsupported. - Supported: supported - Unsupported: unsupported
6	Raisecom(config-ge-1/0/*)#efm remote-loopback start holdtime { <0-1000> default } Example: Raisecom(config-ge-1/0/1)#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. When this time expires, the remote loopback is automatically cancelled.
7	Raisecom(config-ge-1/0/*)#efm mode remote-loopback stop Example: Raisecom(config-ge-1/0/1)#efm mode remote-loopback stop	Stop remote loopback.

7.2.6 Configuring EFM link performance monitoring

Configure OAM link performance monitoring 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.
3	Raisecom(config-ge-1/0/*)#efm link-monitor { supported unsupported } Example: Raisecom(config-ge-1/0/*)#efm link-monitor supported	Enable EFM link performance monitoring on the interface. After an interface is enabled with EFM, it supports link performance monitoring and collects data every 100ms by default. The device with limited CPU performance covers all dot3ah-enabled interfaces and collects data for a round. - Supported: supported - Unsupported: unsupported
4	Raisecom(config-ge-1/0/*)#efm link-monitor error-frame threshold <i>hold-value</i> window <i>window-value</i>	Configure the monitor window and threshold of errored frames. - Frame: by default, error frame detection is enabled, the window size is 10s (100 multiples of 100ms), and the threshold is 1 error frame; in other words, when 1 error frame is detected every 10s, the link error of the error frame is detected. - Hold-value: error frame event threshold, ranging from 1 to 65535, an integer, in units of frame - Window-size: error frame event monitoring window, ranging from 10 to 600, an integer, being 100 by default, in units of multiples of 100ms
5	Raisecom(config-ge-1/0/*)#efm link-monitor error-frame-period threshold <i>hold-value</i> window <i>window-value</i>	Configure the monitor window and threshold of errored frame period events. - Hold-value: error frame period event threshold, ranging from 1 to 65535, an integer, in units of frame - Window-size: error frame period event monitoring window, ranging from 1 to 65535, an integer, being 1 by default, in units of multiples of 10000 frames
6	Raisecom(config-ge-1/0/*)#efm link-monitor error-frame-second threshold <i>hold-value</i> window <i>window-value</i>	Configure the window and threshold of link errored frame seconds. - Hold-value: error frame second threshold, ranging from 1 to 65535, an integer, in units of frame - Window-size: error frame second event monitoring window, ranging from 1 to 65535, an integer, being 100 by default, in units of multiples of 100ms

Step	Command	Description
7	<code>Raisecom(config-ge-1/0/*)#efm link-monitor trigger { error-down trap all }</code>	When four types of link performance errors or two types of emergency link failures (Link Fault and Critical Event) occur locally, or when the same fault messages are received from a remote end, an alarm Trap can be sent to the server locally through the NMS or the interface can be directly shut down (not supported for emergency events), or the above operations can be performed simultaneously, or no operation can 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	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code> Example: <code>Raisecom(config)#interface ge 1/0/1</code>	Enter physical interface configuration mode. • <i>interface-type</i> : interface type • <i>interface-number</i> : interface ID
3	<code>Raisecom(config-ge-1/0/*)#efm critical-event { supported unsupported }</code> Example: <code>Raisecom(config-ge-1/0/1)#efm critical-event supported</code>	Configure EFM emergency event detection. • supported: supported • unsupported: not supported
4	<code>Raisecom(config-ge-1/0/1)#efm link-monitor trigger { error-down trap all }</code>	Configure the action to be taken after receiving an emergent event. • error-down: shut down the interface. • trap: trigger a Trap. • All: do them all.

7.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show efm session { interface interface-type interface-number }</code>	Show information about EFM sessions at both ends.
2	<code>Raisecom#show efm interface interface-type interface-number</code>	Show EFM statistics on the interface.

No.	Command	Description
3	Raisecom#show efm fault-logs interface <i>interface-type</i> <i>interface-number</i>	Show information about EFM error logs at both ends.

7.2.9 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config-ge-1/0/*)#efm fault-logs clear all	Show information about the MLD interface.

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. In this way, the active link can be switched to the standby link to minimize traffic loss.

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.
- On the global node, 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 <i>group-number</i>	Show configurations and status of the link-state group.

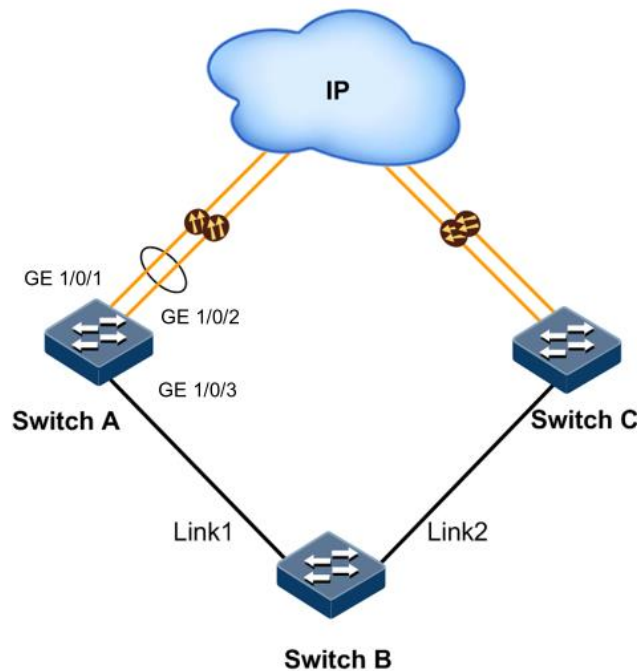
7.3.6 Example for configuring link-state tracking

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 1/0/1 and GE 1/0/2 to the LAG.

```

Raisecom#configure
Raisecom(config)#int eth-trunk 1
Raisecom(config-eth-trunk-1)#add interface ge 1/0/1

```

```
Raisecom(config-eth-trunk-1)#add interface ge 1/0/2
```

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 1/0/3 to the link-state group.

```
Raisecom(config-monitorlink-1)#add interface ge 1/0/3 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-1/0/3           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-1/0/3           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.

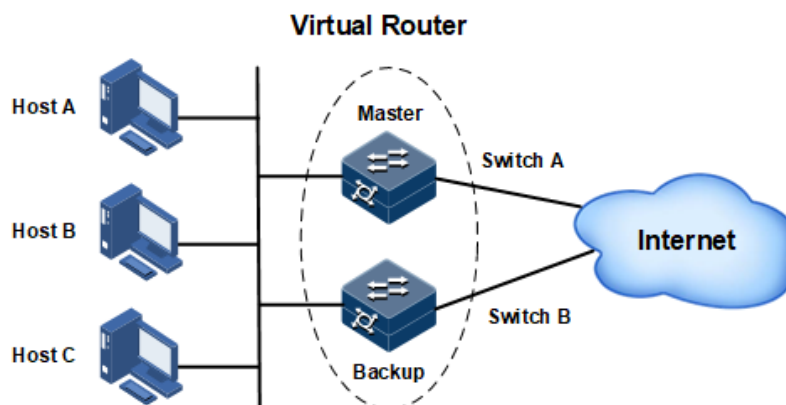
VRRP backup group

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 and Switch B 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 and Switch B is the master device, which carries out the gateway functions, while the other device is the backup device.

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:

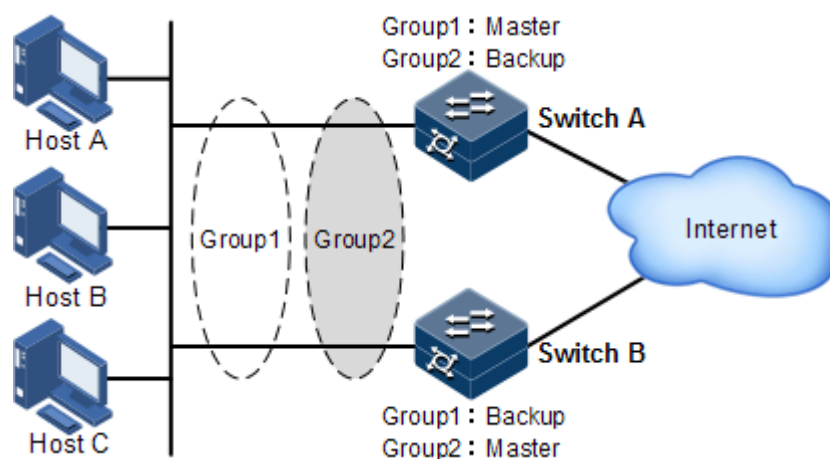
- Step 1 After being enabled with VRRP the device determines its role in the VRRP backup group based on priority. The device with the highest priority is the master while the device with lower priority is the backup. The master device regularly sends VRRP notification packets to notify other devices 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 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 group-id <i>virtual-ip</i> <i>ipv4-address</i>	Configure the virtual IPv4 address of the VRRP backup group.
4	Raisecom(config-vlan*)#vrrp group-id <i>advertise-interval</i> { <i>interval</i> default }	(Optional) configure the interval for sending VRRP packets. • group-id: VRRP instance ID • {interval default}: interval for sending VRRP packets, in units of second, ranging from 1 to 4000, being 1 by default

Step	Command	Description
5	<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.
6	<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
7	<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.
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

Step	Command	Description
14	<code>Raisecom(config-vlan*)# vrrp member-group-id track admin-vrrp interface vlan vlan-id vrid group-id</code>	(Optional) configure VRRP role management. • group-id: VRRP instance ID • vlan-id: management VLAN interface ID • member-group-id: associated VRRP instance ID

7.4.5 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 virtual-ip ipv6-address</code>	Configure the virtual IPv6 address of the VRRP6 backup group.
4	<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 100 by default
5	<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.
6	<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
7	<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.
8	<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: bound VLAN ID

Step	Command	Description
9	<code>Raisecom(config-vlan*)#vrrp-ipv6 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 • VRRP-id: management VRRP6 instance ID
10	<code>Raisecom(config-vlan*)#vrrp-ipv6 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*)#vrrp6vrrp-ipv6 group-id role admin</code>	(Optional) configure VRRP6 role management. • group-id: VRRP6 instance ID
12	<code>Raisecom(config-vlan*)#vrrp-ipv6 admin-vrrp admin- group-id associate- vrrp interface vlan vlan-id member-group- id</code>	(Optional) configure VRRP role management. • group-id: VRRP instance ID • vlan-id: management VLAN interface ID • member-group-id: associated VRRP instance ID

7.4.6 Configuring VRRP Trap

Configure VRRP Trap for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#vrrp snmp- trap { enable disable }</code>	Enable or disable VRRP Trap. By default, it is enabled.

7.4.7 Configuring the VRRP monitoring interface

Configure the VRRP monitoring interface 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-vlanif-*)#vrrp group-id track { interface-type interface-number vlan vlan-id } [{ increased reduced } { value default }]</code>	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.

7.4.8 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-vlanif-*)# vrrp <i>group-id track bfd 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.

7.4.9 Configuring NQA for VRRP

Configure NQA 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.

Step	Command	Description
3	<code>Raisecom(config-vlan*)# vrrp group-id track nqa ADMINNAME OPERATETAG { reduced (value default) }</code>	Configure the VRRP backup group to monitor the NQA session to implement expedited switching.



Note

- **increased priority:** it is the increased priority when the monitored NQA session changes to unreachable status, an integer, ranging from 1 to 255. The range of priority after increment is 1–254. When the monitored NQA session changes from the unreachable status to reachable 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 NQA session changes to unreachable status, an integer, ranging from 1 to 255. The range of priority after reduction is 1–254. When the monitored NQA session changes from the unreachable status to reachable 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	<code>Raisecom#show vrrp session { role { admin member normal } }</code>	Show the basic status of VRRP.
2	<code>Raisecom#show vrrp admin-vrrp</code>	Show information about management VRRP.
3	<code>Raisecom#show vrrp statistics</code>	Show VRRP statistics.
4	<code>Raisecom#show vrrp interface vlan vlan-id</code>	Show VRRP information about the VLAN interface.
5	<code>Raisecom#show vrrp associate interface vlan vlan-id group-id</code>	Show VRRP information about the specified group on the interface.
6	<code>Raisecom#show vrrp binding { admin-vrrp interface vlan vlan-id group-id }</code>	Show binding information about the VRRP management group.

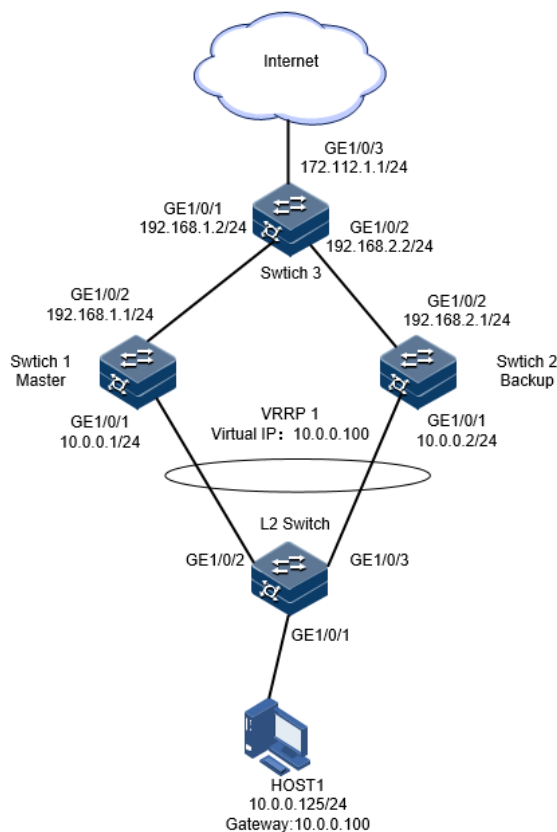
7.4.11 Example for configuring VRRP master/backup

Networking requirements

As shown in Figure 7-5, host 1 is dual-homed to switch 1 and switch 2 through the switch. To ensure sustainable transmission of various services of the user on the network, configure VRRP master/backup backup.

Under normal conditions, host 1 accesses the Internet through switch 1 as the default gateway. When switch 1 fails, switch 2 replaces switch 1, thus implementing gateway backup.

Figure 7-5 Configuring VRRP master/backup



Configuration steps

Step 1 Configure Layer 2 forwarding on the L2 Switch.

```
L2switch(config)#vlan 100
L2switch(config)#interface ge 1/0/2
L2switch(config-ge-1/0/2)#port hybrid pvid 100
L2switch(config-ge-1/0/2)#port hybrid vlan 100 untagged
L2switch(config)#vlan 100
L2switch(config)#interface ge 1/0/3
L2switch(config-ge-1/0/3)#port hybrid pvid 100
L2switch(config-ge-1/0/3)#port hybrid vlan 100 untagged
```

Step 2 Configure Switch 1.

```
switch1(config)#vlan 100
switch1(config)#interface vlan 100
switch1(config-vlanif-100)#ip address 10.0.0.1/24
```

```
switch1(config)#vlan 300
switch1(config)#interface vlan 300
switch1(config-vlanif-300)#ip address 192.168.1.1/24
switch1 (config)#interface ge 1/0/1
switch1(config-ge-1/0/1)#port hybrid pvid 100
switch1(config-ge-1/0/1)#port hybrid vlan 100 untagged
switch1 (config)#interface ge 1/0/2
switch1(config-ge-1/0/2)#port hybrid pvid 300
switch1(config-ge-1/0/2)#port hybrid vlan 300 untagged
switch1(config)#interface vlan 100
switch1(config-vlanif-100)#vrrp 1 virtual-ip 10.0.0.100
switch1(config-vlanif-100)#vrrp 1 priority 120
```

Step 3 Configure Switch 2.

```
switch2(config)#vlan 100
switch2(config)#interface vlan 100
switch2(config-vlanif-100)#ip address 10.0.0.1/24
switch2(config)#vlan 500
switch2(config)#interface vlan 500
switch2(config-vlanif-500)#ip address 192.168.2.1/24
switch2(config)#interface ge 1/0/1
switch2(config-ge-1/0/1)#port hybrid pvid 100
switch2(config-ge-1/0/1)#port hybrid vlan 100 untagged
switch2 (config)#interface ge 1/0/2
switch2(config-ge-1/0/2)#port hybrid pvid 500
switch2(config-ge-1/0/2)#port hybrid vlan 500 untagged
switch2(config)#interface vlan 100
switch2(config-vlanif-100)#vrrp 1 virtual-ip 10.0.0.100
```

Checking results

switch1#show vrrp session

Interface	VRID	Role	Version	VR-State	Pri	IP-Count	State
vlan-100	1	normal	2	Master	120	1	Active
Auth-Mode	Auth-Key						
none	N/A						

switch2#show vrrp session

Interface	VRID	Role	Version	VR-State	Pri	IP-Count	State
vlan-100	1	normal	2	Backup	100	1	Active
Auth-Mode	Auth-Key						
none	N/A						

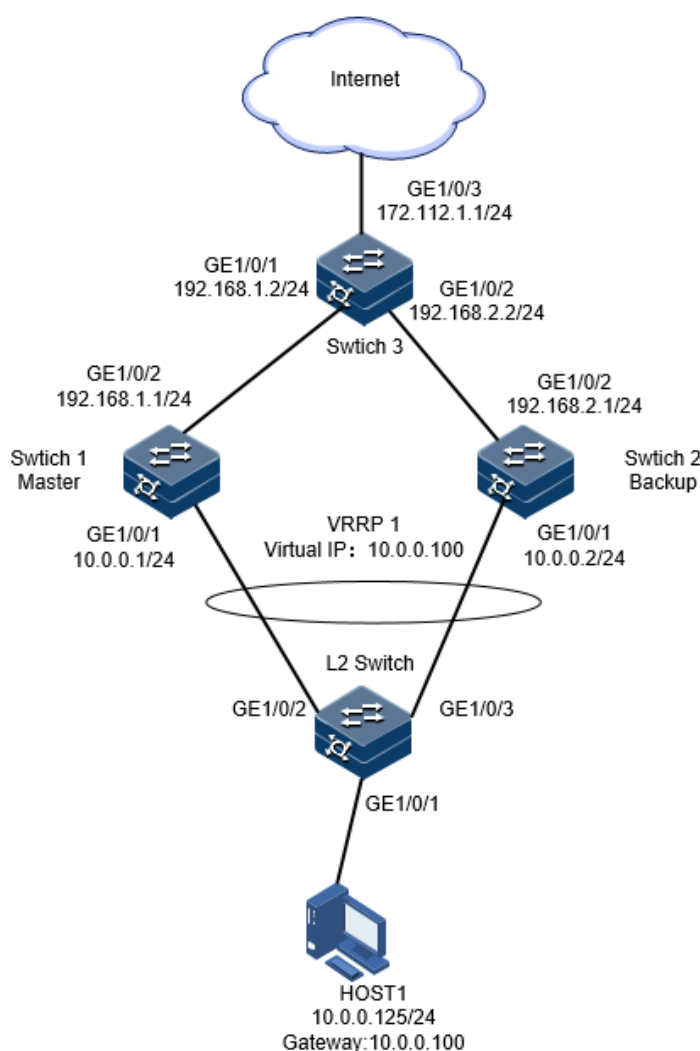
7.4.12 Example for configuring the VRRP monitoring interface

Networking requirements

As shown in Figure 7-6, host 1 is dual-homed to switch 1 and switch 2 through the switch. To ensure sustainable transmission of various services of the user on the network, configure VRRP master/backup backup.

Switch 1 monitors VLANIF interface 300. If GE 1/0/2 on switch 1 becomes Down, the VRRP priority of Switch 1 is decreased according to configuration, so the master needs to be elected again.

Figure 7-6 Configuring the VRRP monitoring interface



Configuration steps

Step 1 Configure Layer 2 forwarding on the L2 switch.

```
L2switch(config)#vlan 100
```

```
L2switch(config)#interface ge 1/0/2
L2switch(config-ge-1/0/2)#port hybrid pvid 100
L2switch(config-ge-1/0/2)#port hybrid vlan 100 untagged
L2switch(config)#vlan 100
L2switch(config)#interface ge 1/0/3
L2switch(config-ge-1/0/3)#port hybrid pvid 100
L2switch(config-ge-1/0/3)#port hybrid vlan 100 untagged
```

Step 2 Configure Switch 1.

```
switch1(config)#vlan 100
switch1(config)#interface vlan 100
switch1(config-vlanif-100)#ip address 10.0.0.1/24
switch1(config)#vlan 300
switch1(config)#interface vlan 300
switch1(config-vlanif-300)#ip address 192.168.1.1/24
switch1 (config)#interface ge 1/0/1
switch1(config-ge-1/0/1)#port hybrid pvid 100
switch1(config-ge-1/0/1)#port hybrid vlan 100 untagged
switch1 (config)#interface ge 1/0/2
switch1(config-ge-1/0/2)#port hybrid pvid 300
switch1(config-ge-1/0/2)#port hybrid vlan 300 untagged
switch1(config)#interface vlan 100
switch1(config-vlanif-100)#vrrp 1 virtual-ip 10.0.0.100
switch1(config-vlanif-100)#vrrp 1 priority 120
switch1(config-vlanif-100)#vrrp 1 track interface vlan 300 reduce 30
```

Step 3 Configure Switch 2.

```
switch2(config)#vlan 100
switch2(config)#interface vlan 100
switch2(config-vlanif-100)#ip address 10.0.0.1/24
switch2(config)#vlan 500
switch2(config)#interface vlan 500
switch2(config-vlanif-500)#ip address 192.168.2.1/24
switch2(config)#interface ge 1/0/1
switch2(config-ge-1/0/1)#port hybrid pvid 100
switch2(config-ge-1/0/1)#port hybrid vlan 100 untagged
switch2 (config)#interface ge 1/0/2
switch2(config-ge-1/0/2)#port hybrid pvid 500
switch2(config-ge-1/0/2)#port hybrid vlan 500 untagged
switch2(config)#interface vlan 100
switch2(config-vlanif-100)#vrrp 1 virtual-ip 10.0.0.100
```

Step 4 Show the configuration of the VRRP monitoring interface on Switch 1.

```
switch1 (config)# show vrrp associate interface
```

LocalIf	VrId	PeerIf
-		

vlan-100	1	vlan-300

Step 5 Shut down GE 1/0/2 on Switch 1.

```
switch1 (config)#interface ge 1/0/2
switch1(config-ge-1/0/2)#shutdown
```

Checking results

Use the following commands to check whether the VRRP priority of Switch 1 is 90 and the status of Switch 2 is changed from Backup to Master.

```
switch1#show vrrp session
```

Interface	VRID	Role	Version	VR-State	Pri	IP-Count	State
Auth-Mode	Auth-Key						

vlan-100	1	normal	2	Master	120	1	Active
none	N/A						

```
switch2#show vrrp session
```

Interface	VRID	Role	Version	VR-State	Pri	IP-Count	State
Auth-Mode	Auth-Key						

vlan-100	1	normal	2	Backup	100	1	Active
none	N/A						

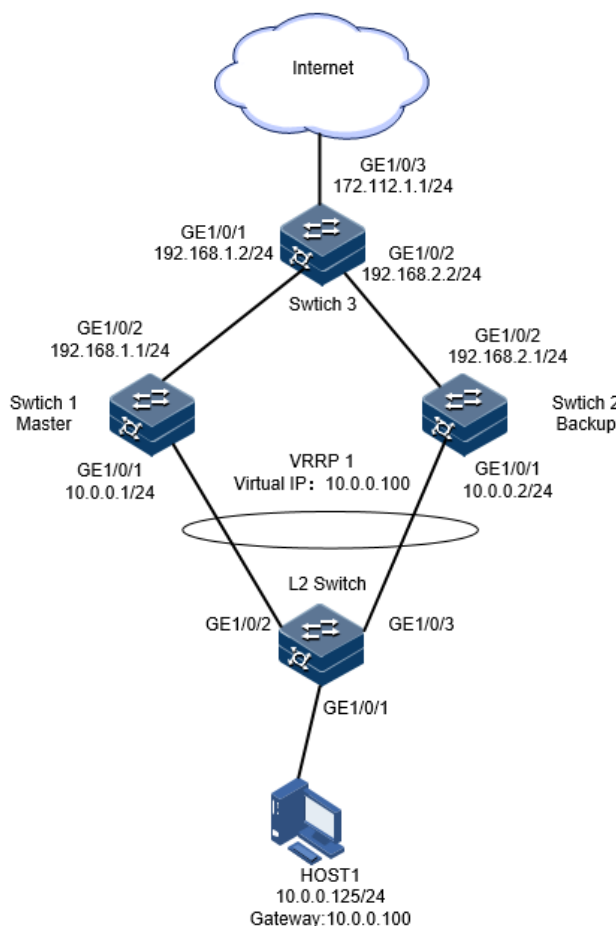
7.4.13 Example for configuring VRRP to monitor the BFD status

Networking requirements

As shown in Figure 7-7, host 1 is dual-homed to switch 1 and switch 2 through the L2 switch. To ensure sustainable transmission of various services of the user on the network, configure VRRP master/backup backup.

Create BFD link detection between GE 1/0/2 on Switch 1 and GE 1/0/1 on Switch 3. Configure VRRP to monitor the BFD status on Switch 1. If BFD becomes Down, the VRRP priority of Switch 1 is decreased according to configuration, so the master needs to be elected again.

Figure 7-7 Configuring the VRRP to monitor the BFD status



Configuration steps

Step 1 Configure Layer 2 forwarding on the L2 switch.

```
L2switch(config)#vlan 100
L2switch(config)#interface ge 1/0/2
L2switch(config-ge-1/0/2)#port hybrid pvid 100
L2switch(config-ge-1/0/2)#port hybrid vlan 100 untagged
L2switch(config)#vlan 100
L2switch(config)#interface ge 1/0/3
L2switch(config-ge-1/0/3)#port hybrid pvid 100
L2switch(config-ge-1/0/3)#port hybrid vlan 100 untagged
```

Step 2 Configure the BFD session on Switch 3.

```
Switch3(config)#bfd start
Switch3(config)#bfd track 1 remote-ip 192.168.1.1 local-ip 192.168.1.2
```

Step 3 Configure Switch 1.

```
switch1(config)#vlan 100
switch1(config)#interface vlan 100
switch1(config-vlanif-100)#ip address 10.0.0.1/24
switch1(config)#vlan 300
switch1(config)#interface vlan 300
switch1(config-vlanif-300)#ip address 192.168.1.1/24
switch1 (config)#interface ge 1/0/1
switch1(config-ge-1/0/1)#port hybrid pvid 100
switch1(config-ge-1/0/1)#port hybrid vlan 100 untagged
switch1 (config)#interface ge 1/0/2
switch1(config-ge-1/0/2)#port hybrid pvid 300
switch1(config-ge-1/0/2)#port hybrid vlan 300 untagged
switch1(config)#bfd start
switch1(config)#bfd track 1 remote-ip 192.168.1.2 local-ip 192.168.1.1
switch1(config)#interface vlan 100
switch1(config-vlanif-100)#vrrp 1 virtual-ip 10.0.0.100
switch1(config-vlanif-100)#vrrp 1 priority 120
switch1(config-vlanif-100)#vrrp 1 track bfd 1 reduce 30
```

Step 4 Configure Switch 2.

```
switch2(config)#vlan 100
switch2(config)#interface vlan 100
switch2(config-vlanif-100)#ip address 10.0.0.1/24
switch2(config)#vlan 500
switch2(config)#interface vlan 500
switch2(config-vlanif-500)#ip address 192.168.2.1/24
switch2(config)#interface ge 1/0/1
switch2(config-ge-1/0/1)#port hybrid pvid 100
switch2(config-ge-1/0/1)#port hybrid vlan 100 untagged
switch2 (config)#interface ge 1/0/2
switch2(config-ge-1/0/2)#port hybrid pvid 500
switch2(config-ge-1/0/2)#port hybrid vlan 500 untagged
switch2(config)#interface vlan 100
switch2(config-vlanif-100)#vrrp 1 virtual-ip 10.0.0.100
```

Step 5 Shut down GE 1/0/2 on Switch 1.

```
switch1 (config)#interface ge 1/0/2
switch1(config-ge-1/0/2)#shutdown
```

Checking results

Use the following commands to check whether the VRRP priority of Switch 1 is 90 and the status of Switch 2 is changed from Backup to Master.

```
switch1#show vrrp session
  Interface          VRID Role   Version VR-State Pri IP-Count State
Auth-Mode  Auth-Key
-----
vlan-100      1   normal 2      Backup  90 1      Active
none          N/A

switch2#show vrrp session
  Interface          VRID Role   Version VR-State Pri IP-Count State
Auth-Mode  Auth-Key
-----
vlan-100      1   normal 2      Master  100 1      Active
none          N/A
-----
```

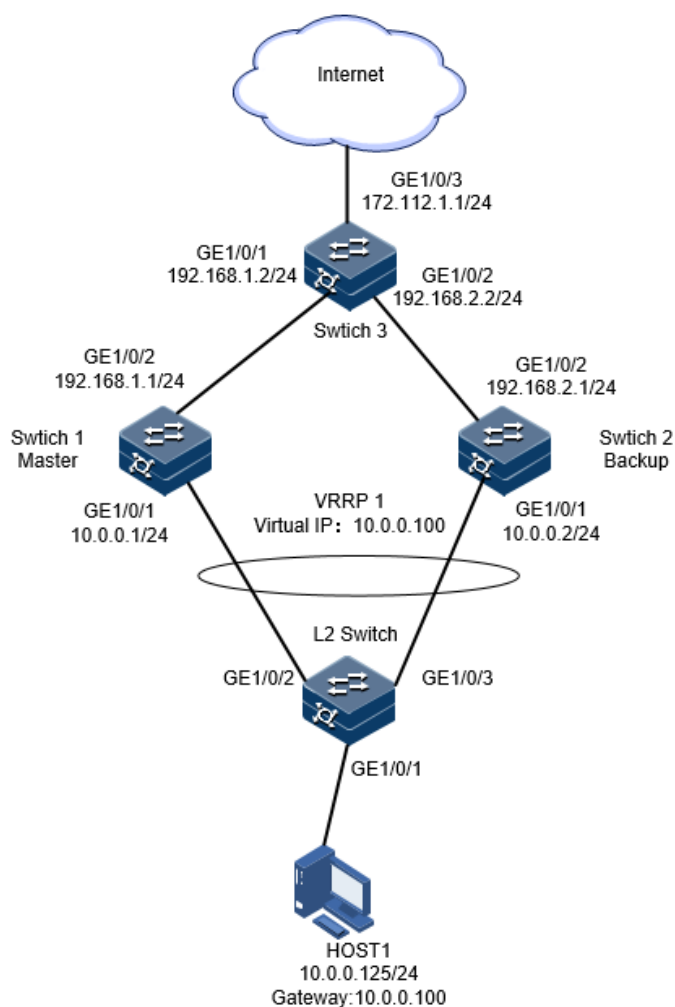
7.4.14 Example for configuring VRRP to monitor the NQA status

Networking requirements

As shown in Figure 7-8, host 1 is dual-homed to switch 1 and switch 2 through the L2 switch. To ensure sustainable transmission of various services of the user on the network, configure VRRP master/backup backup.

Create NQA link detection between Switch 1 and Switch 3. Configure VRRP to monitor the NQA status on Switch 1. If NQA becomes unreachable, the VRRP priority of Switch 1 is decreased according to configuration, so the master needs to be elected again.

Figure 7-8 Configuring the VRRP to monitor the NQA status



Configuration steps

Step 1 Configure Layer 2 forwarding on the L2 switch.

```
L2switch(config)#vlan 100
L2switch(config)#interface ge 1/0/2
L2switch(config-ge-1/0/2)#port hybrid pvid 100
L2switch(config-ge-1/0/2)#port hybrid vlan 100 untagged
L2switch(config)#vlan 100
L2switch(config)#interface ge 1/0/3
L2switch(config-ge-1/0/3)#port hybrid pvid 100
L2switch(config-ge-1/0/3)#port hybrid vlan 100 untagged
```

Step 2 Configure NQA detection on Switch 1.

```
Switch1(config)#nqa test-instance 123 456 type icmp-echo
```

```
Switch1(nqa-123-456-icmp-echo)#frequency 30000
Switch1(nqa-123-456-icmp-echo)#reaction trap test-complete
Switch1(nqa-123-456-icmp-echo)#reaction trap test-failure 1
Switch1(nqa-123-456-icmp-echo)#destination ip 198.168.1.2
```

Step 3 Configure Switch 1.

```
switch1(config)#vlan 100
switch1(config)#interface vlan 100
switch1(config-vlanif-100)#ip address 10.0.0.1/24
switch1(config)#vlan 300
switch1(config)#interface vlan 300
switch1(config-vlanif-300)#ip address 192.168.1.1/24
switch1(config)#interface ge 1/0/1
switch1(config-ge-1/0/1)#port hybrid pvid 100
switch1(config-ge-1/0/1)#port hybrid vlan 100 untagged
switch1(config)#interface ge 1/0/2
switch1(config-ge-1/0/2)#port hybrid pvid 300
switch1(config-ge-1/0/2)#port hybrid vlan 300 untagged
switch1(config)#bfd start
switch1(config)#bfd track 1 remote-ip 192.168.1.2 local-ip 192.168.1.1
switch1(config)#interface vlan 100
switch1(config-vlanif-100)#vrrp 1 virtual-ip 10.0.0.100
switch1(config-vlanif-100)#vrrp 1 priority 120
switch1(config-vlanif-100)#vrrp 1 track nqa 123 456 reduce 30
```

Step 4 Configure Switch 2.

```
switch2(config)#vlan 100
switch2(config)#interface vlan 100
switch2(config-vlanif-100)#ip address 10.0.0.1/24
switch2(config)#vlan 500
switch2(config)#interface vlan 500
switch2(config-vlanif-500)#ip address 192.168.2.1/24
switch2(config)#interface ge 1/0/1
switch2(config-ge-1/0/1)#port hybrid pvid 100
switch2(config-ge-1/0/1)#port hybrid vlan 100 untagged
switch2(config)#interface ge 1/0/2
switch2(config-ge-1/0/2)#port hybrid pvid 500
switch2(config-ge-1/0/2)#port hybrid vlan 500 untagged
switch2(config)#interface vlan 100
switch2(config-vlanif-100)#vrrp 1 virtual-ip 10.0.0.100
```

Step 5 Shut down GE 1/0/2 on Switch 1.

```
switch1 (config)#interface ge 1/0/2
switch1(config-ge-1/0/2)#shutdown
```

Checking results

Use the following commands to check whether the VRRP priority of Switch 1 is 90 and the status of Switch 2 is changed from Backup to Master.

```
switch1#show vrrp session
```

Interface	VRID	Role	Version	VR-State	Pri	IP-Count	State
vlan-100	1	normal	2	Backup	90	1	Active

```
switch2#show vrrp session
```

Interface	VRID	Role	Version	VR-State	Pri	IP-Count	State
vlan-100	1	normal	2	Master	100	1	Active

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

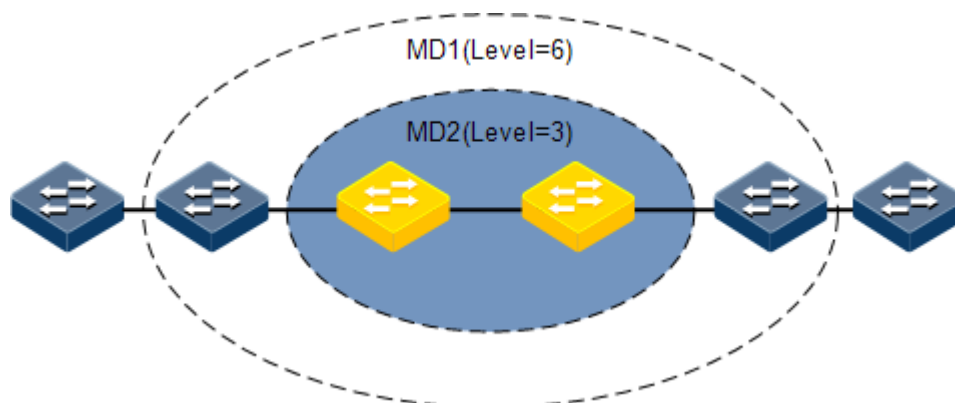
- MD

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 7-9, 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 7-9 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.

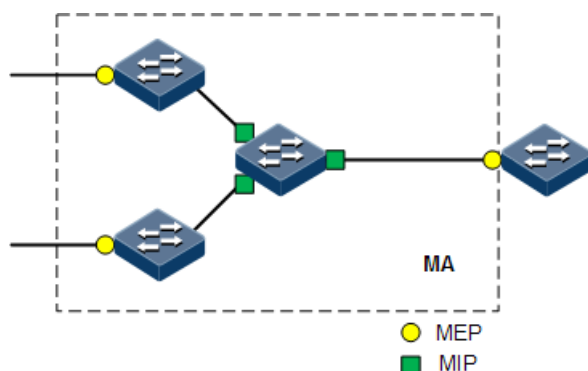
- MEP

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 7-10 MEP and MIP



- MIP

As shown in Figure 7-10, 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.

- 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
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.

Step	Command	Description
3	<pre>Raisecom(config)#c fm md md-name level level format { dns dns-format- string mac mac- format-string string string none } Raisecom(config)#c fm md md-name [level level]</pre>	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	<pre>Raisecom(config- cfm-md-*)#mip create-type { default explicit none }</pre>	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 a lower-level MEP has been configured on the interface. • None: the MIP is not automatically created.
5	<pre>Raisecom(config- cfm-md-*)#ma ma- name format { string icc } format-string</pre>	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.
6	<pre>Raisecom(config- cfm-md-* -ma-*)#map vlan vlan-id</pre>	Configure the VLAN associated with the MA.
7	<pre>Raisecom(config- cfm-md-* -ma-*)#mep mep-id mep-id interface interface-type interface-number { inward outward }</pre>	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 <i>interface-type</i> MEP can be created, and multiple inward <i>interface-type</i> MEPs can be created, but only one inward <i>interface-type</i> 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 md-name	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-* -ma-*)#ccm interval { 3.3ms 10ms 100ms 1s 10s 1min 10min default }</code>	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	<code>Raisecom(config-cfm-md-* -ma-*)#ccm send [mep-id mep-id] enable</code>	Enable MEPs to send CCMs.
6	<code>Raisecom(config-cfm-md-* -ma-*)#rmep mep-id mep-id mac mac- address</code>	Configure the static RMEP. This function is used with the CCM packet detection.
7	<code>Raisecom(config-cfm-md-* -ma-*)#ccm send [mep-id mep-id] priority { priority default }</code>	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	<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-* -ma-*)#ping mep-id mep-id rmep-id mep-id [count count tlv- type { null null-crc prbs prbs-crc } tlv-len len priority priority] * Raisecom(config-cfm-md-* -ma-*)#ping mep-id mep-id mac mac-address [count count tlv- type { null null-crc prbs prbs-crc } tlv-len len priority priority] * Raisecom(config-cfm-md-* -ma-*)#ping mep-id mep-id mac multicast [count count tlv- type { null null-crc prbs prbs-crc } tlv-len len priority priority] *</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	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>)#trace mep-id <i>mep-id</i> mac <i>mac-address</i> [<i>ttl</i> <i>ttl</i> <i>fdb</i> <0-1>] * Raisecom(config-cfm-md-*<i>-ma-*</i>)# trace mep-id <i>mep-id</i> rmep-id <i>mep-id</i> [<i>ttl</i> <i>ttl</i> <i>fdb</i> <0-1>] *	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	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>)#ais [mep <i>mep-id</i>] interval { <i>1s</i> <i>1min</i> <i>default</i> }	Configure the interval for the MEP in the current MA to send AIS packets to the MEP in the higher-level MA.
5	Raisecom(config-cfm-md-*<i>-ma-*</i>)#ais [mep <i>mep-id</i>] md-level { <i>level</i> <i>default</i> }	Configure the level of the AIS packets to be sent by the MEP in the current MA.
6	Raisecom(config-cfm-md-*<i>-ma-*</i>)#ais [mep <i>mep-id</i>] priority { <i>priority</i> <i>default</i> }	Configure the priority of the AIS packets to be sent by the MEP in the current MA.
7	Raisecom(config-cfm-md-*<i>-ma-*</i>)#ais [mep <i>mep-id</i>] enable	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	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.

Step	Command	Description
4	<pre>Raisecom(config-cfm-md-*<i>-ma</i>-*)#loss-measure mep-id mep-id rmep-id mep-id [interval { 100ms 1s } priority priority count <1-100>] * Raisecom(config-cfm-md-*<i>-ma</i>-*)#loss-measure mep-id mep-id mac mac-address [interval { 100ms 1s } priority priority count <1-100>] *</pre>	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	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	<pre>Raisecom(config-cfm-md-*<i>-ma</i>-*)#delay-measure mep-id mep-id rmep-id mep-id [interval { 100ms 1s } priority priority frame- len len count count] * Raisecom(config-cfm-md-*<i>-ma</i>-*)#delay-measure mep-id mep-id mac mac-address [interval { 100ms 1s } priority priority frame- len len count count] *</pre>	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	Show configurations of CFM MDs.
3	Raisecom#show cfm ma	Show configurations of CFM MAs.
4	Raisecom#show cfm mep	Show configurations of CFM MEPs.
5	Raisecom#show cfm rmep	Show configurations of CFM RMEPs.
6	Raisecom#show cfm mip	Show configurations of CFM MIPs.

7.5.12 Example for configuring CFM

Networking requirements

As shown in Figure 7-11:

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.

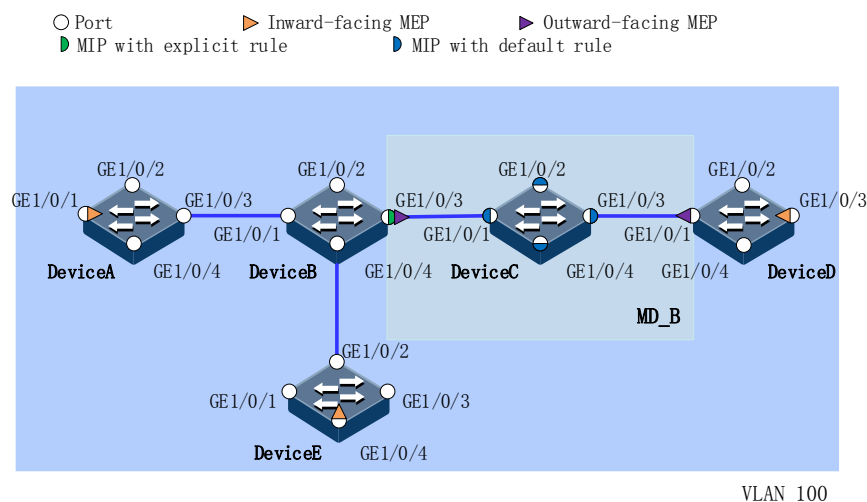
Plan the MIP for MD_A on Device B. This is only configured when there is a low-level MEP on the interface. According to this plan, due to the configuration of the MIP of MD_B on GE1/0/3 on Device B, therefore use the explicit rule to create the MIPs of MD_A on Device B, and use the none rule on other 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 7-11 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 level 5 format none
DeviceA(config-cfm-md-MD_A)#mip create-type none
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)#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 level 5 format none
DeviceB(config-cfm-md-MD_A)#mip create-type explicit
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)#end
DeviceB#configure
DeviceB(config)#cfm md MD_B level 3 format none
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 level 3 format none
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 level 5 format none
DeviceD(config-cfm-md-MD_A)#mip create-type none
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)#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 level 3 format none
DeviceD(config-cfm-md-MD_B)#mip create-type none
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)#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 level 5 format none
DeviceE(config-cfm-md-MD_A)#mip create-type none
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)#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 level 5 format none
  mip create-type none
  ma 1 format icc 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
- MAC address authentication
- URPF
- Time range
- DOS attack prevention

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-mp1s <i>acl-number</i> [name <i>acl-name</i>] Raisecom(config)#acl-userdefined <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 IPv6 ACL configuration mode. • When the ACL number is 5001–6000, this configuration enters user defined ACL configuration mode.
3	<pre> Raisecom(configure-acl-ipv4-*)#rule <i>rule-id</i> ip <i>src-ip ip-address</i> <i>dst-ip ip-address</i> Raisecom(configure-acl-ipv4-*)#rule <i>rule-id</i> icmp <i>src-ip ip-address</i> <i>dst-ip ip-address</i> <i>icmp-type icmp-type</i> <i>icmp-code icmp-code</i> [fragment] Raisecom(configure-acl-ipv4-*)#rule <i>rule-id</i> tcp <i>src-ip ip-address</i> <i>src-port port</i> <i>dst-ip ip-address</i> <i>dst-port port</i> { syn synack ack fin } [fragment] Raisecom(configure-acl-ipv4-*)#rule <i>rule-id</i> igmp <i>src-ip ip-address</i> <i>dst-ip ip-address</i> [fragment] Raisecom(configure-acl-ipv4-*)#rule <i>rule-id</i> udp <i>src-ip ip-address</i> <i>src-port port</i> <i>dst-ip ip-address</i> <i>dst-port port</i> [fragment] </pre>	Configure the matching rules for IP ACL.

Step	Command	Description
4	<pre>Raisecom(configure-acl-l2-*)#rule rule-id ethernet src-mac mac-address dst-mac mac- address Raisecom(configure-acl-l2-*)#rule rule-id src-mac ethernet mac-address dst-mac mac- address eth-type { ip arp ethtype } Raisecom(configure-acl-l2-*)#rule rule-id src-mac ethernet 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 ip 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-ipv6-*)#rule rule- id field1 data/mask/offset { field2 data/mask/offset field3 data/mask/offset field4 data/mask/offset }*</pre>	Configure the matching rule for user defined ACL. • Data: information to be matched • Mask: perform the mask operation on the data • Offset: number of bytes from the matching information to the packet header, mandatorily divisible by 4
7	<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.

Step	Command	Description
2	<code>Raisecom(config)#interface interface-type interface- number</code>	Enter physical interface configuration mode, or VLAN configuration mode. Take physical interface configuration mode for example.
3	<code>Raisecom(config-ge-1/0/*)#acl- 12 in acl-num</code>	Apply ACL to the interface.
	<code>Raisecom(config-ge-1/0/*)#acl- 12 in name</code>	Apply ACL to the interface.
4	<code>Raisecom(config-ge-1/0/*)#exit</code>	Return to global configuration mode.

8.1.5 Configuring statistics

Configure statistics for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#counter counter- id { packet byte all } sort { green red greenred greenyellow redyellow total }</code>	Create a statistic rule.
3	<code>Raisecom(configure-acl-12-*)#rule rule-id action counter counter-id</code>	Apply the statistic rule to the ACL.

8.1.6 Configuring rate limiting

Configure rate limiting for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#meter meter-id pps pps-value color { aware blind }</code>	Create a rate limiting profile based on the number of packets.
3	<code>Raisecom(config)#meter meter-id cir { kbps mbps gbps } cir- value cbs { bytes kbytes mbytes } cbs-value ebs { bytes kbytes mbytes } ebs-value color { aware blind }</code>	Create a single-rate three-color rate limiting profile.
4	<code>Raisecom(config)#meter meter-id cir { kbps mbps gbps } cir- value cbs { bytes kbytes mbytes } cbs-value pir { kbps mbps gbps } pir-value pbs { bytes kbytes mbytes } pbs-value color { aware blind }</code>	Create a dual-rate three-color rate limiting profile.

Step	Command	Description
5	Raisecom(configure-acl-12-*)#rule <i>rule-id</i> meter <i>meter-id</i> outaction { red-drop yellow-drop }	Apply the rate limiting profile to the ACL.

8.1.7 Configuring the time range

Configure the time range for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#acl-12 <i>acl-id</i>	Enter the ACL list view.
3	Raisecom(configure-acl-12-*)#rule <i>rule-id</i> time-range <i>timerange-list-id</i>	Apply the time range to the ACL.

8.1.8 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.

8.1.9 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)#reset acl statistics [acl <i>acl-id</i> rule <i>rule-id</i> direction { in out }]	Clear statistics on global ACL.
Raisecom(config)#reset acl statistics interface <i>interface-type</i> <i>interface-number</i> [acl <i>acl-id</i> rule <i>rule-id</i> direction { in out }]	Clear statistics on interface ACL.

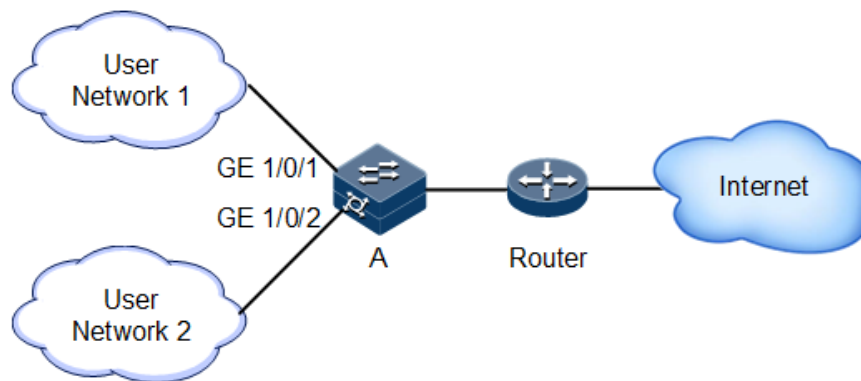
8.1.10 Example for configuring ACL

Networking requirements

As shown below, the network requirements are as below:

- Deny the Internet access from switch A between 00:00 and 08:00 every day.
- Limit the rate for accessing the Internet from switch A between 08:00 and 12:00 every day to 10000 pps.

Figure 8-1 ACL networking



Configuration steps

Step 1 Configure the time range.

```
Raisecom#configure
Raisecom(config)#timerange list 1
Raisecom(config-timerange-1)#time-range 1 everyday 00:00:00 to 08:00:00
Raisecom(config-timerange-1)#configure
Raisecom(config)#timerange list 2
Raisecom(config-timerange-1)#time-range 1 everyday 08:00:00 to 12:00:00
```

Step 2 Configure the meter.

```
Raisecom#configure
Raisecom(config)#meter 1 pps 10000 color blind
```

Step 3 Configure the ACL rule and action.

```
Raisecom#configure
Raisecom(config)#acl-12 1 name test
Raisecom(configure-acl-12-1)#rule 1 src-mac any dst-mac any
Raisecom(configure-acl-12-1)#rule 1 time-range 1
Raisecom(configure-acl-12-1)#rule 1 action deny
```

```
Raisecom(configure-acl-12-1)#rule 2 src-mac any dst-mac any
Raisecom(configure-acl-12-1)#rule 2 time-range 2
Raisecom(configure-acl-12-1)#rule 2 meter 1 outaction red-drop yellow-drop
```

Step 4 Apply the ACL to the interface.

```
Raisecom#configure
Raisecom(config)#interface ge 1/0/1 to ge 1/0/2
Raisecom(config-ge-1/0/1->ge-1/0/2)#acl-12 in 1
```

Checking results

```
Raisecom#show acl config
!
acl-12 1 name test
rule 1 src-mac any dst-mac any
rule 1 time-range 1
rule 1 action deny
rule 2 src-mac any dst-mac any
rule 2 time-range 2
rule 2 meter 1 outaction red-drop yellow-drop
!
interface ge 1/0/1
acl-12 in name test
!
interface ge 1/0/2
acl-12 in name test
```

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
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 { count default }	Configure the times for retransmitting RADIUS packets, being 3 by default.
5	Raisecom(config-aaa)#radius-server retransmit-interval { interval default }	Configure the global interval for retransmitting RADIUS packets, being 2s by default.

Step	Command	Description
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 { count default } retransmit-interval { interval 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 { count default } retransmit-interval { interval 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 300 by default.
4	Raisecom(config-aaa)#tacacs-server timeout { second default }	Configure the TCP connection timeout time and packet receiving timeout time of the TACACS+ authentication server, being 2s by default.

Step	Command	Description
5	<code>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 { second default } source-ip ip-address [source-vpn-instance vpn-name] vpn-instance vpn-name]*</code>	Create an IPv4 TACACS+ server.
6	<code>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 { second default } source-ip6 ipv6-address [source-vpn-instance vpn-name] vpn-instance vpn-name]*</code>	Create an IPv6 TACACS+ server.

8.2.6 Configuring the AAA server group

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#aaa</code>	Enter AAA configuration mode.
3	<code>Raisecom(config-aaa)#server-group group-name { radius-server tacacs-server } server-name</code>	Create an AAA server group, or add servers to the AAA server group.

8.2.7 Configuring the AAA mode

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#aaa</code>	Enter AAA configuration mode.
3	<code>Raisecom(config-aaa)#aaa authentication { dot1x login mac-authen enable } method method-name first { group-name local } second { group-name local none } third { group-name local none }</code>	Configure the AAA authentication modes.  Note Up to 2 modes can be configured for an AAA server group.

Step	Command	Description
4	<pre>Raisecom(config-aaa)#aaa authorization { login cmd } method method-name first { group-name local } second { group-name local none } third { group-name local none }</pre>	Configure the AAA authorization modes.  Note Up to 2 modes can be configured for an AAA server group.
5	<pre>Raisecom(config-aaa)#aaa accounting { dot1x login mac-authen } method method- name first { group-name local } second { group-name local none } third { group- name local none }</pre>	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	<pre>Raisecom#show aaa config</pre>	Show AAA configurations.
2	<pre>Raisecom#show aaa information</pre>	Show global information about AAA.
3	<pre>Raisecom#show aaa server</pre>	Show information about AAA servers.
4	<pre>Raisecom#show aaa server-group</pre>	Show information about AAA server groups.
5	<pre>Raisecom#show aaa method</pre>	Show information about AAA modes.

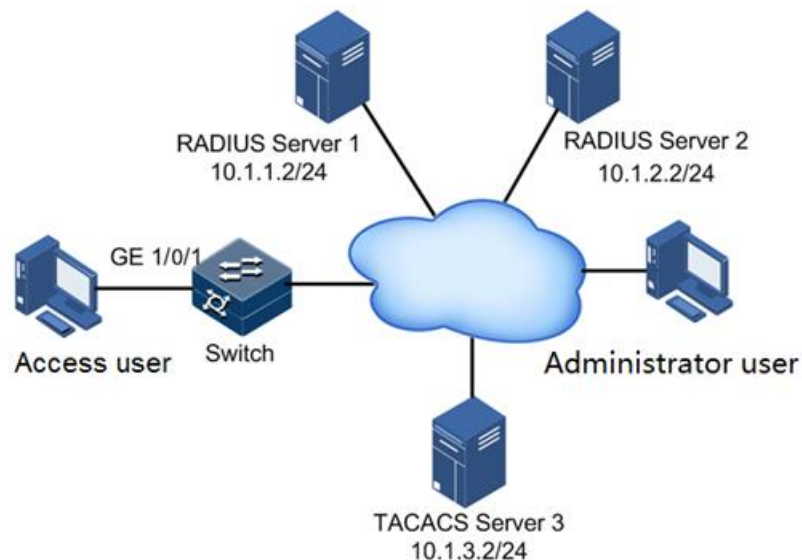
8.2.9 Example for configuring AAA

Networking requirement

As shown in Figure 8-2, 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 8-2 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
Raisecom(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 1/0/1
Raisecom(config-ge-1/0/1)#dot1x enable
Raisecom(config-ge-1/0/1)#dot1x aaa-authentication Method4
Raisecom(config-ge-1/0/1)#dot1x aaa-accounting Method5
Raisecom(config-ge-1/0/1)#exit
```

Checking results

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.

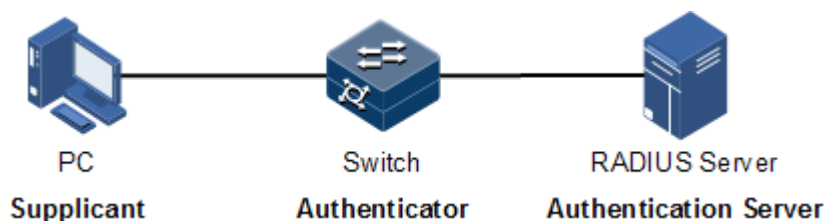
It is used to authenticate and control access devices at the physical layer of the network device. It defines a point-to-point connection mode between the device interface and user devices. User devices, connected to the interface, can access resources in the LAN if they are authenticated. Otherwise, they cannot access resources in the LAN through the switch.

802.1x structure

As shown in Figure 8-3, 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 8-3 802.1x 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 authentication.
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.

Step	Command	Description
9	<code>Raisecom(config-ge-1/0/*)#dot1x max-user user-number</code>	Configure the maximum number of users allowed to be authenticated by the 802.1x interface.
10	<code>Raisecom(config-ge-1/0/*)#nac guest-vlan vlan-id</code>	Configure the Guest VLAN of the specified interface, which takes effect on both 802.1x and MAC authentication.
11	<code>Raisecom(config-ge-1/0/*)#dot1x critical-vlan vlan-id</code>	Configure the critical VLAN of 802.1x on the specified interface.
12	<code>Raisecom(config-ge-1/0/*)#dot1x restrict-vlan vlan-id</code>	Configure the restrict VLAN of 802.1x on the specified interface.
13	<code>Raisecom(config-ge-1/0/*)#dot1x reauthenticate all user</code>	Manually trigger reauthentication of 802.1x users on the specified interface.
14	<code>Raisecom(config-ge-1/0/*)#dot1x delete all user</code>	Force 802.1x users on the interface to be offline.
15	<code>Raisecom(config-ge-1/0/*)#dot1x quiet { disable enable }</code>	Enable or disable silence of 802.1x users on the interface.
16	<code>Raisecom(config-ge-1/0/*)#dot1x quiet-times times</code>	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	<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.
3	<code>Raisecom(config-ge-1/0/*)#dot1x reauthenticate { enable disable }</code>	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 <i>time</i>	Configure the time of the re-authentication timer.
4	Raisecom(config-ge-1/0/*)#dot1x timer quiet-period <i>time</i>	Configure the time of the quiet timer.
5	Raisecom(config-ge-1/0/*)#dot1x supp period <i>time</i>	Configure the Request/MD5 Challenge request packet timeout timer.
6	Raisecom(config-ge-1/0/*)#dot1x server-timeout period <i>time</i>	Configure the authentication server timeout timer.
7	Raisecom(config-ge-1/0/*)#dot1x tx period <i>time</i>	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.
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

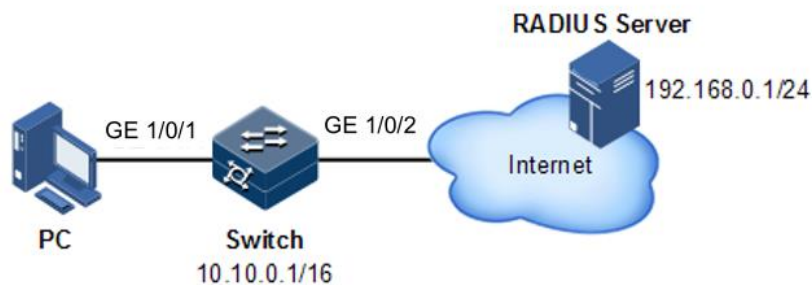
Networking requirements

As shown in Figure 8-4, 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 8-4 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.

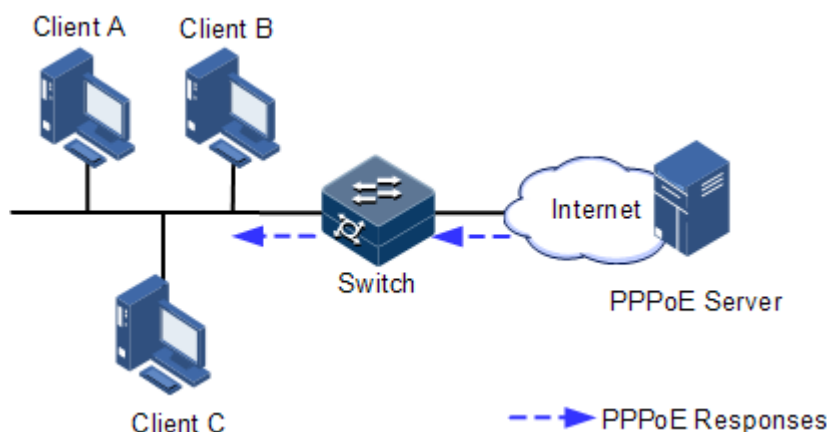
In PPPoE dial-up mode, you can access the network through various interfaces on the device as long as authentication by the authentication server is successful.

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 8-5. 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 8-5 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 2 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 3 After receiving the PADI packet, the authentication server replies a unicast packet PPPoE Active Discovery Offer (PADO).
- Step 4 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 5 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
Global policy for processing received PPPoE+ Tag packets	replace
Padding mode of Circuit ID	SwitchCommon
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
Global policy for processing received PPPoE+ Tag packets	replace



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#config	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 reduce the CPU utilization. The packets received by the trusted interface are not sent to the CPU for processing, but directly forwarded by the switching chip. The PPPoE trusted interface is configured on the interface connected to the PPPoE server.

Configure the PPPoE trusted interface for the device as below.

Step	Command	Description
1	Raisecom#config	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: is padded with the ID of the interface receiving client request packets, VLAN IDs (outer VLAN ID and inner VLAN ID).
- Remote ID: is padded with the MAC address of the interface receiving client request packets.

Configuring the Circuit ID

The Circuit ID has 3 padding modes:

- ascii: pad the Circuit ID with the character string configured by the command.
- default: pad the Circuit ID with the default value.
- User-define: pad the Circuit ID with the user-defined format.

Configure the Circuit ID for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#pppoeplus default circuit-id format { ascii default user-define } string	Configure the Circuit ID of the switch (no string needs to be configured in the default mode).
3	Raisecom(config)#interface interface-type interface-number	Enter physical interface configuration mode.
4	Raisecom(config-ge-1/0/1)#pppoeplus circuit-id format { ascii default user-define } string	Configure the Circuit ID on the interface (no string needs to be configured in the default mode; if both the interface Circuit ID and global Circuit ID are configured, the configuration of the interface Circuit-ID prevails).

Configuring the Remote ID

The Remote ID has 3 padding modes:

- **ascii**: pad the Remote ID with the character string configured by the command.
- **default**: pad the Remote ID with the default value.
- **User-define**: pad the Remote ID with the user-defined format.

Configure the Remote ID for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#pppoeplus default remote-id format { ascii default user-define } string	Configure the Remote ID of the switch (no string needs to be configured in the default mode).
3	Raisecom(config)#interface interface-type interface-number	Enter Layer 2 physical interface configuration mode.
4	Raisecom(config-ge-1/0/1)#pppoeplus remote-id format { ascii default user-define } string	Configure the Remote ID on the interface (no string needs to be configured in the default mode; if both the interface Remote ID and global Remote ID are configured, the configuration of the interface Circuit-ID prevails).

Configuring the policy for processing PPPoE+ Tag

Tags of some fields may be forged by the client because of some reasons, thus replacing the original Tags in the message is required.

- If the policy for processing received PPPoE+ Tag packets to replace, and the PPPoE packet already carries the information field Tag, the Tag will be replaced.
- If the policy for processing received PPPoE+ Tag packets to keep, and the PPPoE packet already carries the information field Tag, the original tag will be retained.
- If the policy for processing received PPPoE+ Tag packets is configured to drop, and the PPPoE packet already carries the information field Tag, the original tag will be discarded.

Configure Tag overriding for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#pppoeplus default policy { drop keep replace }	Configure the global policy for processing received PPPoE+ Tag packets.
3	Raisecom(config-ge-1/0/1)# pppoeplus policy { drop keep replace }	Configure the interface policy for processing received PPPoE+ Tag packets. If both the global policy and interface policy are configured, the interface policy prevails.

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 information	Show current global PPPoE+ configurations, including default configurations.

8.4.7 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)#reset pppoeplus statistic [interface interface-type interface-number]	Clear PPPoE+ statistics. The device supports clearing PPPoE+ statistics on the specified interface.
Raisecom#show pppoeplus interface [interface-type interface-number]	Show configurations and statistics on the PPPoE+ interface.

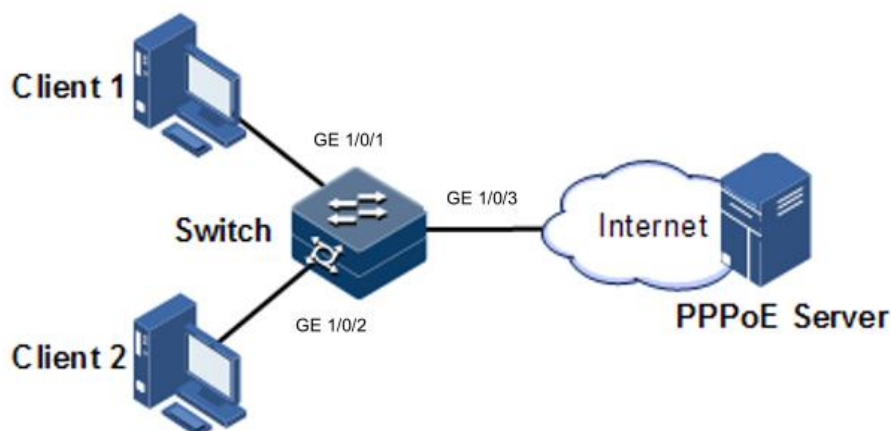
8.4.8 Example for configuring PPPoE+

Networking requirements

As shown in Figure 8-6, to prevent illegal clients from accessing and managing legal users, you can configure PPPoE+ on the Switch.

- GE 1/0/1 and GE 1/0/2 are connected to Client 1 and Client 2 respectively. GE 1/0/3 is connected to the PPPoE server.
- Enable global PPPoE+, and PPPoE on GE 1/0/1, GE 1/0/2, and GE 1/0/3. Configure GE 1/0/3 as the trusted interface.
- Configure the Circuit ID mode to user-defined, and configure the format is the interface name + outer VLAN ID + device name + inner VLAN ID + interface ID + interface MAC address. Configure the Remote ID to ascii, and configure the content to 01:02:03:04:05:06.
- Configure the policy for processing received PPPoE+ packets on GE 1/0/1 and GE 1/0/2.

Figure 8-6 PPPoE+ networking



Configuration steps

Step 1 Enable global PPPoE+. Enable PPPoE+ on GE 1/0/1, GE 1/0/2, and GE 1/0/3.

```
Raisecom(config)#pppoeplus start
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#pppoeplus enable
Raisecom(config-ge-1/0/1)#exit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#pppoeplus enable
Raisecom(config-ge-1/0/2)#exit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#pppoeplus enable
Raisecom(config-ge-1/0/3)#exit
```

Step 2 Configure GE 1/0/3 as the trusted interface.

```
Raisecom#configure
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#pppoeplus trust
Raisecom(config-ge-1/0/3)#exit
```

Step 3 Configure the format of the Circuit ID and Remote ID.

```
Raisecom(config)#pppoeplus default circuit-id format user-
defined %portname:%svlan:%devicename:%portNo:%portmac
Raisecom(config)#pppoeplus default remote-id format ascii
01:02:03:04:05:06
```

Step 4 Configure the policy for processing received PPPoE+ Tag packets on GE 1/0/1 and GE 1/0/2.

```
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#pppoeplus policy keep
Raisecom(config-ge-1/0/1)#exit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#pppoeplus policy drop
Raisecom(config-ge-1/0/2)#exit
```

Checking results

Use the **show pppoeplus config** command to show PPPoE+ configurations.

```
Raisecom#show pppoeplus config
!
pppoeplus start
pppoeplus default remote-id format ascii 01:02:03:04:05:06
pppoeplus default circuit-id format user-
defined %portname:%svlan:%devicename:%portNo:%portmac
!
interface ge 1/0/1
  pppoeplus enable
  pppoeplus policy keep
!
interface ge 1/0/2
  pppoeplus enable
  pppoeplus policy drop
!
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/*)#port-security enable	Enable port security MAC.
4	Raisecom(config-ge-1/0/*)#port-security maximum <i>maximum</i>	Configure the maximum number of secure MAC addresses.
5	Raisecom(config-ge-1/0/*)#port-security protect-action { protect restrict shutdown }	Configure the secure MAC violation mode.
6	Raisecom(config-ge-1/0/*)#shutdown Raisecom(config-ge-1/0/*)#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/*)#port-security { enable disable }	Enable port security MAC.

Step	Command	Description
4	<code>Raisecom(config-ge-1/0/*)#port-security mac-address sticky { enable disable }</code>	Enable sticky secure MAC learning.
5	<code>Raisecom(config-ge-1/0/*)#port-security mac-address sticky vlan <i>vlan-id</i> mac <i>mac-address</i></code>	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	<code>Raisecom#show mac-address config</code>	Show configurations of port security MAC.
2	<code>Raisecom#show mac-address { security sticky }</code>	Show information about entries of secure MAC addresses.

8.5.7 Maintenance

Maintain the device as below.

Command	Description
<code>Raisecom(config)#no mac-address { security sticky } [<i>interface-type interface-number</i>]</code>	Clear the specified type of secure MAC addresses.

8.5.8 Example for configuring port security MAC

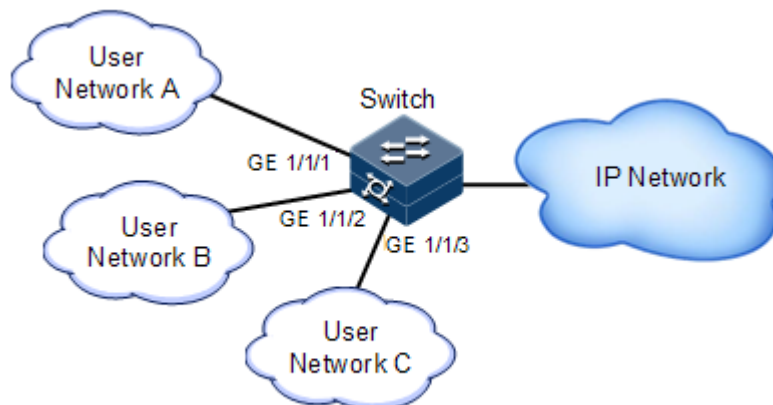
Networking requirements

As shown in Figure 8-7, 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 8-7 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 1/0/2.

```
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 1/0/3.

```
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-ge-1/0/1)#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-ge-1/0/*)#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-ge-1/0/1)#storm-suppression action { block error-down none }	Configure the action for storm suppression on the interface.
5	Raisecom(config-ge-1/0/1)#storm-suppression interval <i>interval</i>	Configure the restoration period of the shutdown interface.
6	Raisecom(config-ge-1/0/1)#storm-suppression snmp-trap enable	Enable or disable storm suppression Trap.
7	Raisecom(config-ge-1/0/1)#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.

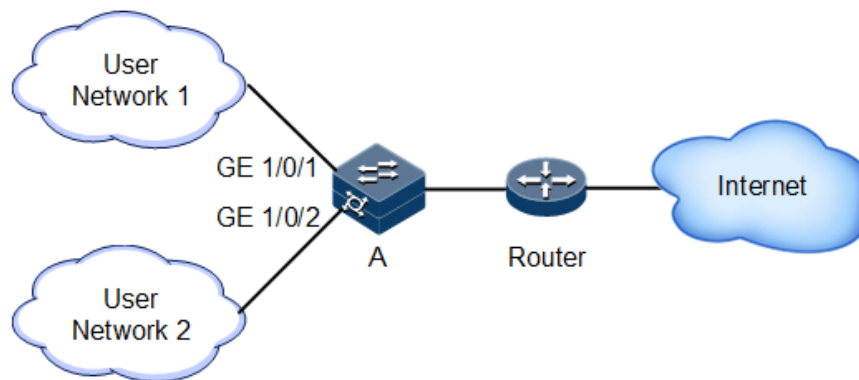
8.6.6 Example for configuring storm suppression

Networking requirements

As shown in Figure 8-8, when GE 1/0/1 and GE 1/0/2 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 8-8 Storm suppression networking



Configuration steps

Enable storm suppression, and configure the threshold for storm suppression.

```

Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#storm-suppression broadcast min-rate kbps 320
max-rate kbps 640
Raisecom(config-ge-1/0/1)#storm-suppression action error-down
Raisecom(config-ge-1/0/1)#exit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#storm-suppression broadcast min-rate kbps 320
max-rate kbps 640
Raisecom(config-ge-1/0/2)#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-1/0/1	UNC	disable bps	n/a	none/normal
5				
	UNMC	disable bps	n/a	none/normal
5				
	BC	enable bps	320/640 (kbit/s)	none/error-down
5				
ge-1/0/2		UNC	disable bps	n/a
none/normal	5			
	UNMC	disable bps	n/a	none/normal
5				

```

          BC      enable bps      320/640      (kbit/s)
none/error      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-ge-1/0/*)# storm-control { unknown-unicast unknown-multicast broadcast unicast multicast } cir { kbps 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-ge-1/0/*)# 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-ge-1/0/*)# 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</i> <i>interface-number</i>]	Show configurations of storm control on the interface.

8.6.9 Example for configuring storm control

Networking requirements

When GE 1/0/1 and GE 1/0/2 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 1/0/1
Raisecom(config-ge-1/0/1)#storm-control broadcast cir kbps 640 cbs kbytes
6400
Raisecom(config-ge-1/0/1)#exit
Raisecom(config)#interface ge 1/0/2
```

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-1/0/1           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-1/0/2           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
```

8.7 ARP attack protection

8.7.1 Introduction

ARP attack protection is a security feature against ARP attacks. It guarantees the security of network devices through a series of actions, such as learning ARP entries, restricting and checking ARP packet processing.

8.7.2 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

8.7.3 Default configurations of ARP attack protection

N/A

8.7.4 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 disable }	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 disable }	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 disable }	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 disable }	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 disable }	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 and the device receives an ARP packet, the device compares the information about the packet, such as the source IP address, source MAC address, the receiving interface, and VLAN of the packet with the information in the DHCP Snooping binding table. If the information matches, the device determines that the user is legal and allows the ARP packet to pass; otherwise, the device determines that the ARP packet is an attack packet and discards the ARP packet. This function is application to the DHCP Snooping scenario only.

Step	Command	Description
8	<pre> Raisecom(config- vlan*)#arp- antiattack check user-bind check-item { interface ip- address mac- address } 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.

8.7.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show arp-antiattack config	Show configurations of ARP attack protection.
2	Raisecom#show arp-antiattack interface	Show dynamic ARP entries.
3	Raisecom#show arp-antiattack information	Show information about global ARP attack protection.

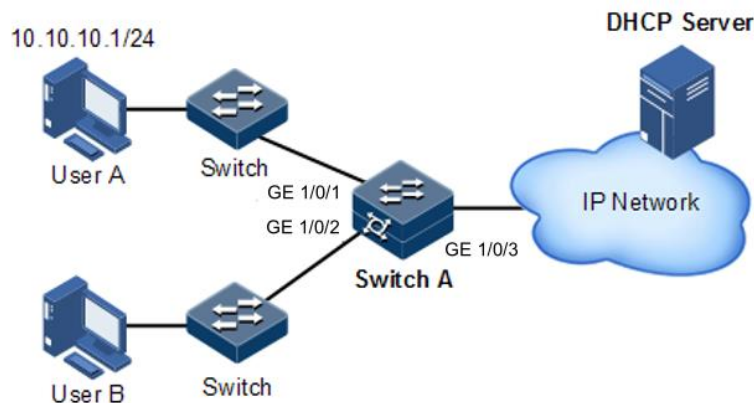
8.7.6 Example for configuring ARP attack protection

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 1/0/2.

Figure 8-9 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 1/0/2
Raisecom(config-ge-1/0/2)#arp-antiattack check user-bind enable
Raisecom(config-ge-1/0/2)#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 1/0/2
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	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter Layer 2 physical interface configuration mode or VLAN interface configuration mode.
4	<code>Raisecom(config-ge-1/0/*)#nd-snooping { enable disable }</code>	Enable ND Snooping on the interface that is connected to the gateway.
5	<code>Raisecom(config-ge-1/0/*)#nd-snooping trust</code>	Configure the interface that is connected to the gateway as a trusted interface.
6	<code>Raisecom(config)#nd-snooping check { na ns rs } { enable disable }</code>	Enable validity check on NS/NA/RS packets by ND Snooping.

8.8.5 Checking configurations

Use the following commands to check configuration results.

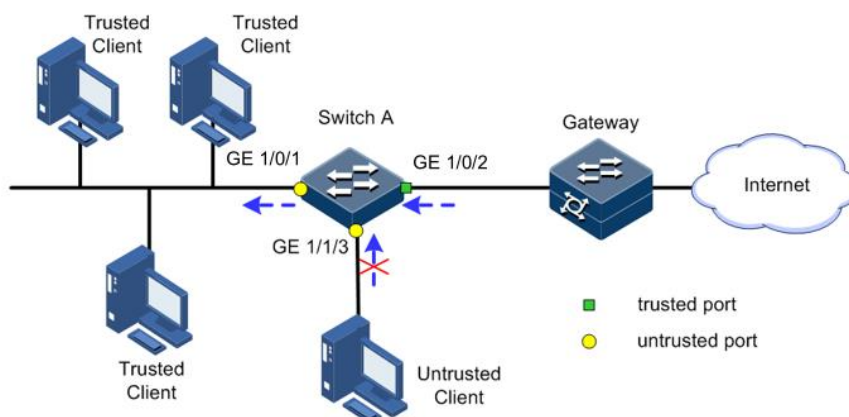
No.	Command	Description
1	<code>Raisecom#show nd-snooping config</code>	Show configurations of ND Snooping.
2	<code>Raisecom#show nd-snooping user-bind</code>	Show the user binding table of ND Snooping.
3	<code>Raisecom#show nd-snooping prefix</code>	Show the prefix table of ND Snooping.

8.8.6 Example for configuring ND Snooping

Networking requirements

As shown in Figure 8-10, 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 8-10 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 1/0/2 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 1/0/2
SwitchA(config-ge-1/0/2)#port link-type access
SwitchA(config-ge-1/0/2)#port default vlan 10
SwitchA(config-ge-1/0/2)#exit
SwitchA(config)#interface ge 1/1/0
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan 10
SwitchB(config-ge-1/0/1)#exit
```

- Step 3 Enable global ND Snooping and enable ND Snooping in VLAN 10. Configure GE 1/0/1 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 1/0/1
SwitchA(config-ge-1/0/1)#nd-snooping enable
SwitchA(config-ge-1/0/1)#nd-snooping trust
```

```
SwitchA(config-ge-1/0/1)#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 1/0/1  
nd-snooping enable  
nd-snooping trust
```

8.9 DHCP Snooping

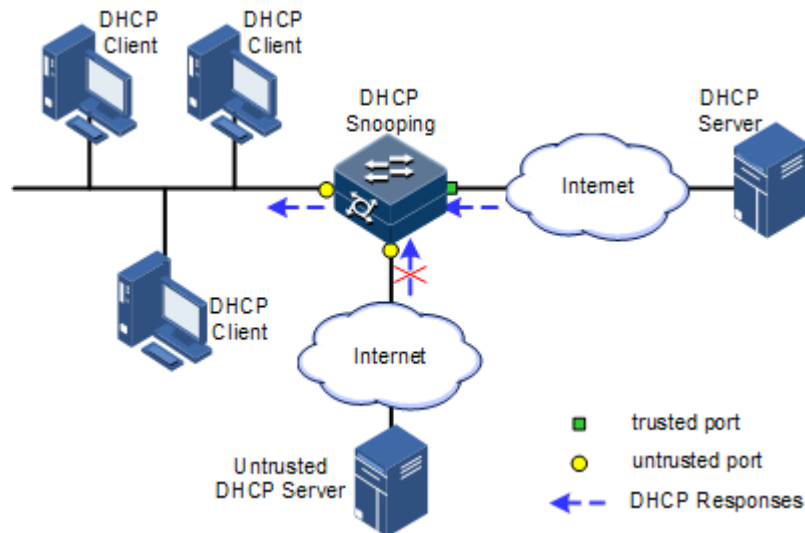
8.9.1 Introduction

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 8-11, 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 8-11 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 stop }	Enable global DHCP Snooping.
3	Raisecom(config)#interface <i>interface-type interface-number</i> Raisecom(config)#vlan <i>vlan-id</i>	Enter physical interface configuration mode or VLAN interface configuration mode.
4	Raisecom(config-ge-1/0/*)#dhcp-snooping { enable disable }	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. This configuration takes effect in the physical interface configuration mode only.

Step	Command	Description
6	Raisecom(config-vlan-*)# dhcp-snooping trust interface <i>interface-type interface-number</i>	Configure the trusted interface of DHCP Snooping. This configuration takes effect in the VLAN interface configuration mode only.
7	Raisecom(config-ge-1/0/*)# dhcp-snooping max-user-number { <i>number</i> default }	Configure the number of entries in the DHCP Snooping binding table.
8	Raisecom(config-ge-1/0/*)# dhcp-snooping server-filter { enable disable }	Configure DHCP Snooping to trust server configurations.
9	Raisecom(config-ge-1/0/*)# dhcp-snooping check user-bind { enable disable }	Configure matching detection between DHCP packets and binding table.
10	Raisecom(config-ge-1/0/*)# dhcp-snooping check mac-address { enable disable }	Check whether the MAC address in the header of request packets sent by DHCP users.
11	Raisecom(config-ge-1/0/*)# dhcp-snooping option82 { enable disable }	Configure DHCP Snooping to support Option 82.
12	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 stop }	Enable global DHCP Snooping.
3	Raisecom(config)# interface <i>interface-type interface-number</i> Raisecom(config)# vlan <i>vlan-id</i>	Enter physical interface configuration mode or VLAN interface configuration mode.
4	Raisecom(config-ge-1/0/*)# dhcp-snooping { enable disable }	Enable interface DHCP Snooping.
5	Raisecom(config-ge-1/0/*)# dhcp-snooping option82 { enable disable }	Configure global DHCP Snooping to support Option 82.
6	Raisecom(config-ge-1/0/*)# dhcp-snooping option82 circuit-id format { default user-defined <i>format-string</i> }	Configure the content of the Circuit ID of DHCP Snooping Option 82.

Step	Command	Description
7	Raisecom(config-ge-1/0/*)#dhcp-snooping option82 remote-id format { default user-defined format-string }	Configure the content of the Circuit ID of DHCP Snooping Option 82.
8	Raisecom(config-ge-1/0/*)#dhcp-snooping option82 { drop keep append }	Configure the policy for processing DHCP request packets with Option 82 by DHCP Snooping.
9	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 stop }	Enable global DHCPv6 Snooping.
3	Raisecom(config)#interface interface-type interface-number Raisecom(config)#vlan vlan-id	Enter physical interface configuration mode or VLAN interface configuration mode.
4	Raisecom(config-ge-1/0/*)#dhcpv6-snooping { enable disable }	Enable interface DHCPv6 Snooping.
5	Raisecom(config-ge-1/0/*)#dhcpv6-snooping trust	Configure the trusted interface of DHCPv6 Snooping. This configuration takes effect in the physical interface configuration mode only.
6	Raisecom(config-vlan-*)#dhcpv6-snooping trust interface interface-type interface-number	Configure the trusted interface of DHCPv6 Snooping. This configuration takes effect in the VLAN interface configuration mode only.
7	Raisecom(config-ge-1/0/*)#dhcpv6-snooping max-user-number { number default }	Configure the number of entries in the DHCPv6 Snooping binding table.
8	Raisecom(config-ge-1/0/*)#dhcpv6-snooping option18 { enable disable }	Enable DHCP Snooping to support Option 18.
9	Raisecom(config-ge-1/0/*)#dhcpv6-snooping option18 format { default user-defined format-string }	Configure the content of DHCP Snooping Option 18.
10	Raisecom(config-ge-1/0/*)#dhcpv6-snooping option37 { enable disable }	Configure DHCPv6 Snooping to support Option 37.

Step	Command	Description
11	Raisecom(config-ge-1/0/*)#dhcpv6-snooping option37 format { default user-defined format-string }	Configure the content of DHCP Snooping 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 dhcp-snooping vlan	Show VLAN configurations of DHCP Snooping.
6	Raisecom#show dhcpv6-snooping config	Show configurations of DHCPv6 Snooping.
7	Raisecom#show dhcpv6-snooping user-bind	Show configurations of the DHCPv6 Snooping binding table.
8	Raisecom#show dhcpv6-snooping statistics	Show statistics on DHCPv6 Snooping statistics.
9	Raisecom#show dhcpv6-snooping interface	Show configurations of DHCPv6 Snooping interfaces.
10	Raisecom#show dhcpv6-snooping vlan	Show VLAN configurations of DHCPv6 Snooping.

8.9.8 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)#reset dhcp-snooping user-bind	Clear information about the DHCP Snooping IPv4 binding table of the user.
Raisecom(config)#reset dhcpv6-snooping user-bind	Clear information about the DHCP Snooping IPv6 binding table of the user.
Raisecom(config)#reset dhcp-snooping statistics	Clear statistics on configurations of DHCPv4 Snooping user interfaces.

Command	Description
<code>Raisecom(config)#reset dhcpv6-snooping statistics</code>	Clear statistics on configurations of DHCPv6 Snooping user interfaces.

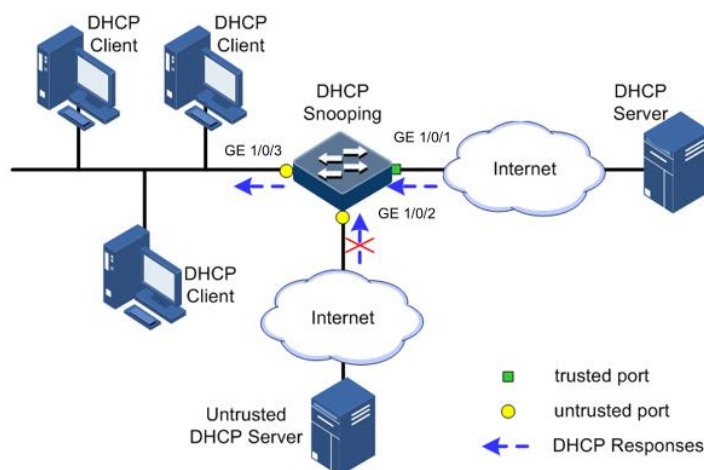
8.9.9 Example for configuring DHCP Snooping

Networking requirements

As shown in Figure 8-12, 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. Configure GE 1/0/3 as below:

- Configure the Remote-ID of DHCP packets to self-defined format. Configure the encapsulation format to hexadecimal. The encapsulation content is the system ID + slot ID + port number (8 bits) + MAC address.
- Configure the Circuit-ID of DHCP packets to self-defined format. Configure the encapsulation format to ASCII. The encapsulation content is the interface name: outer VLAN ID (4 bits) + inner VLAN ID + device name + system ID.

Figure 8-12 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 1/0/1
Raisecom(config-ge-1/0/1)#dhcp-snooping enable
Raisecom(config-ge-1/0/1)#dhcp-snooping trust
Raisecom(config-ge-1/0/1)#exit
```

Step 3 Configure DHCP Relay to support Option 82 field and configure Option 82 field.

```
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#dhcp-snooping enable
Raisecom(config-ge-1/0/3)#dhcp-snooping option82 enable
Raisecom(config-ge-1/0/3)#dhcp-snooping option82 remote-id format user-
defined %sys %slot %8port %mac
Raisecom(config-ge-1/0/3)#dhcp-snooping option82 circuit-id format user-
defined 'raisecom' '%portname:%4svlan,%cvlan,%devicename,%sys'
Raisecom(config-ge-1/0/3)#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 1/0/1
  dhcp-snooping enable
  dhcp-snooping trust
!
interface ge 1/0/3
  dhcp-snooping enable
  dhcp-snooping option82 enable
  dhcp-snooping option82 remote-id format user-
defined %sys %slot %8port %mac
  dhcp-snooping option82 circuit-id format user-defined
'%portname:%4svlan,%cvlan,%devicename,%sys'
...
```

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 features (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:

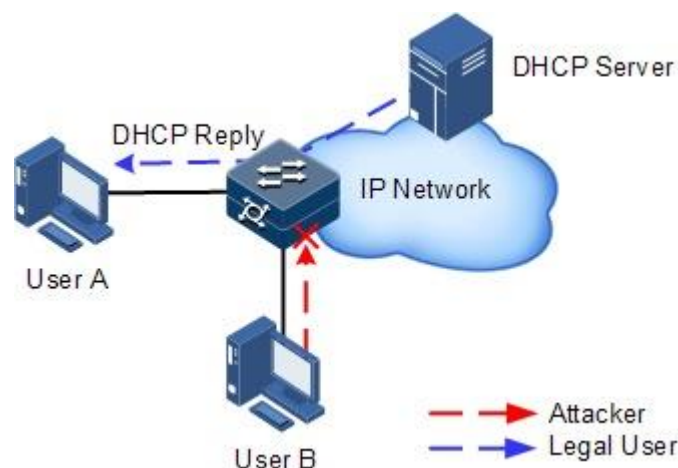
- Static binding: configure binding information manually and generate binding entry to complete the interface control, which fits for the case where the number of hosts is small or where you need to perform separate binding on a single host.
- Dynamic binding: obtain binding information automatically 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 8-13 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 8-13 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 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 interface-type interface-number] vlan vlan-id/any	Configure static binding.
	Raisecom(config)#user-bind static ipv6 ipv6-address/any mac mac-address/any interface interface-type interface-number 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 ip source check config	Show configurations of IP Source Guard.
2	Raisecom#show ip source check interface	Show information about the interface enabled with IP Source Guard.

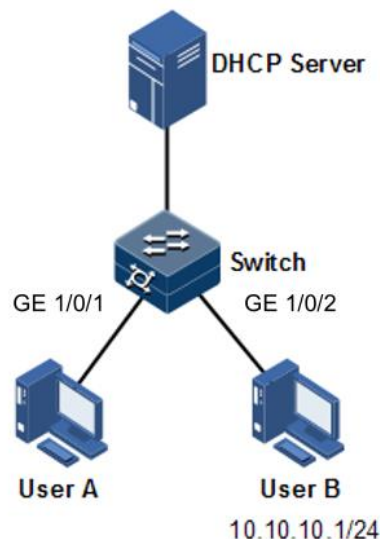
8.10.7 Example for configuring IP Source Guard

Networking requirements

As shown in Figure 8-14, to prevent IP address embezzlement, you need to configure IP Source Guard on the Switch.

- The Switch permits all IP packets on GE 1/0/1 to pass.
- GE 1/0/2 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 8-14 Configuring IP Source Guard



Configuration steps

Step 1 Configure IP Source Guard.

```
Raisecom#configure
Raisecom(config)#int ge 1/0/2
Raisecom(config-ge-1/0/2)#ip source check user-bind enable
Raisecom(config-ge-1/0/2)#exit
Raisecom(config)#int ge 1/0/1
Raisecom(config-ge-1/0/1)#ip source check user-bind enable
Raisecom(config-ge-1/0/1)#exit
```

Step 2 Configure static binding entries.

```
Raisecom(config)#user-bind static ip 10.10.10.1 mac any interface ge
1/0/2 vlan any
```

Step 3 Configure DHCP Snooping on interface GE 1/0/2 and other interfaces.

Checking results

Use the **show ip source check config** command to show configurations of IP Source Guard.

```
Raisecom#show ip source check config
!
user-bind static ip 10.10.10.1 mac any interface ge 1/0/2 vlan any
!
interface ge 1/0/2
```

```
ip source check user-bind enable
!
interface ge 1/0/1
ip source check user-bind enable
```

Use the **show ip source check interface** command to show information about the interface enabled with IP Source Guard.

```
Raisecom#show ip source check interface
Interface          Check-Item          Alarm    Limit    DropPkts
-----
ge-1/0/2           ip,mac,vlan         disable  100      0
ge-1/0/1           ip,mac,vlan         disable  100      0
-----
```

8.11 CPU attack protection

8.11.1 Introduction

On the network, there are a large number of malicious attacks on the Central Processing Unit (CPU) and all kinds of packets that need to be sent to the CPU normally. The malicious attack packets on the CPU cause the CPU to be busy processing attack packets for a long time and interrupt other services and even the system. A large number of normal packets also lead to high CPU utilization and performance degradation, thus affecting normal services.

To protect the CPU and ensure the processing and response of the CPU for normal services, the device provides the CPU attack protection function. CPU attack protection aims at the packets sent to the CPU, protects the security of the device itself, ensures the normal operation of the existing services in the event of an attack, and prevent various services from affecting each other when the device is attacked.

8.11.2 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

8.11.3 Configuring rate limiting for 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.
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 lacp lldp 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-cpudefend-policy-test)# packet-type { arp bfd dhcpreply dhcprequest igmp lacp lldp mld stp-customer telnet priority } priority-value	Configure the priority of the specified protocol packet type in the policy. The protocol packet types supported by the device depend on the protocols supported by the device.
5	Raisecom(config-cpudefend-policy-test)# deny packet-type { arp bfd dhcpreply dhcprequest igmp lacp lldp mld stp-customer telnet ... }	Configure the type of the specified protocol packet to be discarded in the policy. The protocol packet types supported by the device depend on the protocols supported by the device.
6	Raisecom(config-cpudefend-policy-test)# session-car packet-type { bgp ftp http isis ospf ospfv3 ssh telnet tftp ... } pps pps-value	Configure the rate limit of the protocol session of dynamic link protection for the specified protocol packet type in the policy.
7	Raisecom(config-cpudefend-policy-test)# filter <1-8> { acl-ipv4 acl-listid acl-ipv6 acl-listid }	Configure the filter in the policy.
8	Raisecom(config)# cpu-defend bind-policy test	Configure the binding policy for CPU attack protection. The bound policy cannot be modified. To modify it, unbind the policy. This command is read only in the dynamic adjustment mode based on CPU utilization.

Step	Command	Description
9	Raisecom(config)# cpu-defend mode { cpuratio-control fixed }	Configure the mode of the binding policy for CPU attack protection, including the dynamic adjustment mode based on CPU utilization and fixed. By default, it is fixed.
10	Raisecom(config)# cpu-defend { level1-policy policy-name level2-policy policy-name level3-policy policy-name }	Configure the policy for each level in the dynamic adjustment mode based on CPU utilization for the binding policy.
11	Raisecom(config)# cpu-defend { level1-cpuratio <1-100> level2-cpuratio <1-100> }	Configure the maximum CPU utilization in level 1 or level 2 in the dynamic adjustment mode based on CPU utilization for the binding policy.

8.11.4 Configuring attack traceability for CPU attack protection

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
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)# auto-defend enable	Configure attack traceability of the policy for CPU attack protection. By default, it is enabled.
4	Raisecom(config-cpudefend-policy-test)# auto-defend threshold threshold-value	Configure the attack traceability threshold of the policy for CPU attack protection. By default, it is 128 pps.
5	Raisecom(config-cpudefend-policy-test)# auto-defend attack-packet sample sample-value	Configure the attack traceability sampling value of the policy for CPU attack protection. By default, it is 8.
6	Raisecom(config-cpudefend-policy-test)# auto-defend alarm enable	Enable attack traceability alarm of the policy for CPU attack protection. By default, it is disabled.
7	Raisecom(config-cpudefend-policy-test)# auto-defend alarm threshold threshold-value	Enable the attack traceability alarm threshold of the policy for CPU attack protection. By default, it is 128.

Step	Command	Description
8	Raisecom(config-cpudefend-policy-test)# auto-defend action { deny error-down }	Configure the penalty action for attack traceability of the policy for CPU attack protection. By default, there is no action.
9	Raisecom(config)# cpu-defend bind-policy test	Configure the application for CPU attack protection. The bound policy cannot be modified. To modify it, unbind it.

8.11.5 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.
3	Raisecom#show auto-defend attack-source	Show configurations of attack traceability for CPU attack protection.

8.11.6 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)#reset cpu-defend statistics	Clear global statistics on CPU attack protection.

8.11.7 Example for configuring CPU attack protection

Networking requirements

Rate limiting for CPU attack protection is targeted at packets received by the CPU, so no networking chart is needed.

Configuration steps

Configure the device as below:

```
Raisecom(config)#cpu-defend policy test
Raisecom(config-cpudefend-policy-test)#car packet-type arp pps 120
Raisecom(config-cpudefend-policy-test)#quit
```

Raisecom(config)#**cpu-defend bind-policy test**

Checking results

Use the **show cpu-defend policy name** command to show information about CPU attack protection.

Raisecom(config)# **show cpu-defend policy name test**
Cpu-defend policy test information:

```
-----
Policy name      :test
Description      :
Status           :active/binding

Attack source trace information:
Status           :enable
Threshold        :128
Alarm status     :disable
Alarm Threshold  :128

Auto port defend information:
Auto port defend aging time:300
```

Car packet information:

PacketType	Priority	Action	RateMode	RateValue

total	0	no-deny	pps	1024(packets/s)
dot1x	3	no-deny	pps	128(packets/s)
arp	4	no-deny	pps	120(packets/s)
telnet	4	no-deny	pps	512(packets/s)
ftp	5	no-deny	pps	512(packets/s)
icmp	2	no-deny	pps	128(packets/s)
icmp-ipv6	2	no-deny	pps	128(packets/s)
igmp	4	no-deny	pps	256(packets/s)
snmp	2	no-deny	pps	256(packets/s)
ntp	4	no-deny	pps	64(packets/s)
ospf	5	no-deny	pps	512(packets/s)
ospfv3	5	no-deny	pps	512(packets/s)
dhcpreply	4	no-deny	pps	256(packets/s)
dhcprequest	4	no-deny	pps	256(packets/s)
dhcpv6reply	4	no-deny	pps	256(packets/s)
dhcpv6request	4	no-deny	pps	256(packets/s)
rip	5	no-deny	pps	512(packets/s)
ripng	5	no-deny	pps	512(packets/s)
bfd	6	no-deny	pps	256(packets/s)
bgp	5	no-deny	pps	512(packets/s)
pim	5	no-deny	pps	256(packets/s)
pim-ipv6	5	no-deny	pps	256(packets/s)

vrrp	2	no-deny	pps	256(packets/s)
stp-customer	6	no-deny	pps	64(packets/s)
isis	4	no-deny	pps	512(packets/s)
loopback-detect	4	no-deny	pps	256(packets/s)
udld	5	no-deny	pps	64(packets/s)
efm	3	no-deny	pps	64(packets/s)
protect-link	6	no-deny	pps	128(packets/s)
lldp	3	no-deny	pps	256(packets/s)
pppoe	3	no-deny	pps	128(packets/s)
flush	3	no-deny	pps	64(packets/s)
hvs	7	no-deny	pps	32(packets/s)
sync	3	no-deny	pps	512(packets/s)
fibhit	2	no-deny	pps	768(packets/s)
ssh	4	no-deny	pps	512(packets/s)
lACP	6	no-deny	pps	256(packets/s)
mvrp	2	no-deny	pps	64(packets/s)
g8031	6	no-deny	pps	64(packets/s)
g8032	6	no-deny	pps	64(packets/s)
mad	5	no-deny	pps	128(packets/s)
http	4	no-deny	pps	256(packets/s)
mld	4	no-deny	pps	256(packets/s)
nd	4	no-deny	pps	256(packets/s)
tftp	2	no-deny	pps	512(packets/s)
arp-miss	0	no-deny	pps	256(packets/s)
bpdu	2	no-deny	pps	128(packets/s)
12-unknownprotocol	1	no-deny	pps	128(packets/s)
nd-miss	0	no-deny	pps	256(packets/s)
cfm	4	no-deny	pps	128(packets/s)

Session-car packet information:

PacketType	RateMode	RateValue

telnet	pps	1024(packets/s)
ftp	pps	1024(packets/s)
ospf	pps	1024(packets/s)
ospfv3	pps	1024(packets/s)
bgp	pps	1024(packets/s)
isis	pps	1024(packets/s)
ssh	pps	1024(packets/s)
http	pps	1024(packets/s)
tftp	pps	1024(packets/s)

8.12 MAC address authentication

8.12.1 Introduction

MAC address authentication is an authentication mode that controls the network access permissions of users based on interface and MAC address, without the need to install client software. After the device detects the user's MAC address for the first time on the interface enabled with MAC address authentication, it initiates the authentication operation for the user. During the authentication process, the user does not need to manually enter the user name and password. If the user authentication is successful, he/she is allowed to access network resources through the interface; otherwise, the MAC address is configured as the silent MAC address. During the silence period, when user packets from this MAC address arrive, the device directly discards them to prevent the illegal MAC address from repeated authentication in a short period.

- Format of the user name for MAC address authentication
 - MAC address user account: the device uses the source MAC address as the user name and password for user authentication, or uses the MAC address as the user name and configures the password.
 - Fixed user name account: all MAC address authentication users use a fixed user name and password specified on the device to replace the user's MAC address as identity for authentication.
- Authentication mode
 - RADIUS server authentication for MAC address authentication: when using the radius server authentication for MAC address authentication, the device works as a RADIUS client and cooperates with the RADIUS server to implement MAC address authentication.
 - Local authentication for MAC address authentication: when using local authentication MAC address authentication, the device directly authenticates the user on the device. Configure the local user name and password on the device.
- Re-authentication

MAC address re-authentication refers to the periodic authentication of MAC address authentication users on the interface by the device, to detect changes in the user's connection status and ensure their normal online status.

8.12.2 Default configurations

Default configurations of MAC address authentication are as below.

Function	Default value
Global MAC address authentication status	Disable
Interface MAC address authentication status	Disable
Global authentication mode	pap
802.1x re-authentication status	Permit
802.1x re-authentication timer time	1800s
MAC address authentication silence timer time	60s

Function	Default value
Maximum number of users	256

8.12.3 Configuring MAC address authentication

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#mac-authen { start stop }	Enable or disable global MAC address authentication.
3	Raisecom(config)#mac-authen aaa authentication method <i>method-name</i>	Configure the AAA mode name for global MAC address authentication.
4	Raisecom(config)#mac-authen max-user <i>user-number</i>	Configure the maximum number of users for global MAC address authentication.
5	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter layer 2 physical interface configuration mode.
6	Raisecom(config-ge-1/0/*)#mac-authen enable	Enable interface MAC address authentication.
7	Raisecom(config-ge-1/0/*)#mac-authen max-user <i>user-number</i>	Configure the maximum number of users allowed by the interface for MAC address authentication.
8	Raisecom(config-ge-1/0/*)#authentication guest-vlan <i>vlan-id</i>	Configure the guest VLAN of the specified interface. It takes effect on both 802.1x and MAC address authentication.
9	Raisecom(config-ge-1/0/*)#mac-authen critical-vlan <i>vlan-id</i>	Configure the critical VLAN of the specified interface for MAC address authentication.
10	Raisecom(config-ge-1/0/*)#mac-authen restrict-vlan <i>vlan-id</i>	Configure the restrict VLAN of the specified interface for MAC address authentication, an integer, ranging from 1 to 4094.
11	Raisecom(config-ge-1/0/*)#mac-authen reauthenticate all user	Manually re-authenticate the 802.1x user of the specified interface.
12	Raisecom(config-ge-1/0/*)#mac-authen delete all user	Force the MAC address authentication user to be offline on the interface.
13	Raisecom(config-ge-1/0/*)#mac-authen quiet { disable enable }	Enable or disable the silence function of the MAC address authentication user on the interface.

Step	Command	Description
14	Raisecom(config-ge-1/0/*)#mac-authen quiet-times { times default }	Configure the times of authentication failure for triggering the silence function for the MAC address authentication user on the interface.
15	Raisecom(config-ge-1/0/*)#mac-authen critical-vlan user aging { disable enable }	Enable or disable the aging of aged users of MAC address authentication on the interface.
16	Raisecom(config-ge-1/0/*)#mac-authen critical-vlan user reauthenticate { disable enable }	Enable or disable re-authentication of aged users of MAC address authentication on the interface.
17	Raisecom(config-ge-1/0/*)#mac-authen restrict-vlan user aging { disable enable }	Enable or disable re-authentication of failing users by MAC address authentication on the interface.
18	Raisecom(config-ge-1/0/*)#mac-authen restrict-vlan user reauthenticate { disable enable }	Enable or disable re-authentication of failing users by MAC address authentication on the interface.
19	Raisecom(config)#show mac-authen config	Show configurations of MAC address authentication.
20	Raisecom(config)#show mac-authen information	Show global information about MAC address authentication.
21	Raisecom(config)#show mac-authen interface-type interface-number	Show information about MAC address authentication on the specified interface.
22	Raisecom(config)#show mac-authen user	Show the current user for MAC address authentication.

8.12.4 Example for configuring MAC address authentication

Networking requirements

As shown below, the user needs to be authentication through MAC address authentication. The user is directed connected to the device which can access the authentication server.

Figure 8-15 MAC address authentication networking



Configuration steps

Step 1 Configure the device as below.

```
Raisecom(config)#aaa
Raisecom(config-aaa)#radius-server host server1 ip-address 192.168.5.66
key 12345
Raisecom(config-aaa)#server-group grp1 radius-server server1
Raisecom(config-aaa)#aaa authentication mac-authen method m1 first grp1
Raisecom(config-aaa)#quit
Raisecom(config)#mac-authen start
Raisecom(config)#mac-authen aaa authentication method m1
Raisecom(config)#mac-authen mode fixed-user username wwf password plain
12345
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#mac-authen enable
```

- Step 2 Use the **show mac-authen information** command to show information about MAC address authentication.

```
Raisecom(config)#show mac-authen information
Max User Number           : 256
  Default Max User Number   : 256
  Current User Number       : 0
  Auth Success User Number  : 0
  Auth Fail User Number     : 0
  Auth Timeout User Number  : 0
  UserName Password Format   : Fixed
  MacAddress UpperCase      : Disable
  MacAddress With Hyphen    : Disable
  Mac Auth Method           : Pap
  AAA Authentication Method  : m1
  AAA Accounting Method     : n/a
  Fixed User Name           : wwf
  Fixed Password            : 12345
```

Checking results

Use the **show mac-authen user** command to show the current user for MAC address authentication.

```
Raisecom(config)# show mac-authen user
S:Success, F:Fail, T:Timeout, J:Join, A:Authenticate, O:Origin, C:Current,
L:Last
Interface  Mac-Address  AuthNum(S/F/T)  Vlan(J/A/O)  Result(C/L)
ge 1/0/1   0010:9400:0001  1/0/0           11/0/11      Success/None
```

8.13 URPF

8.13.1 Introduction

Usually, after receiving a data packet, the router obtains the destination IP address in the packet and looks up the local routing table for the destination IP address. If there is a corresponding entry, the router forwards the data packet; otherwise, it discards the packet. From this perspective, when the router forwards packets, it does not care about the source IP address of the packet. This provides an opportunity for source address spoofing attacks.

Source address spoofing attacks involve intruders to forge a series of packets with forged source addresses, frequently accessing the device or host where the destination address is located; even if the response packet cannot reach the attacker, it will cause a certain degree of damage to the attacked object.

Unicast Reverse Path Forwarding (URPF) is used to prevent network attack behavior based on source address spoofing. Once the router interface is enabled with URPF, when it receives a data packet, it first checks the legitimacy of the source address of the data packet. If the packet pass the legitimacy check of the source address, the router will further search for forwarding entries to the destination address and enter the packet forwarding process; Otherwise, the packet will be discarded.

Strict URPF

Strict URPF not only requires the router to have a route to the packet source address in the forwarding table, but also requires the ingress interface of the packet to be consistent with the egress interface of the route to the source address in the forwarding table. Only the packets that meet both above conditions are considered legal packets. In some special cases (such as the presence of asymmetric paths), strict URPF may erroneously discard non-attack packets.

Loose URPF

Loose URPF requires a source address route to the packet to exist in the forwarding table of the router, without checking whether the ingress interface of the packet is consistent with the outgoing interface of the route to the source address in the forwarding table. When there are asymmetric paths on the user network that cannot guarantee consistency between the ingress interface of packets and the egress interface of the device route to the source address, loose URPF check can be configured.

Attacks, such as TCP Syn Flood, UDP Flood, and ICMP Flood, can attack target devices or hosts through source address spoofing, causing severe performance degradation and even system crashes for the victim. URPF is a commonly used technology used by network devices to prevent such attacks.

8.13.2 Preparing for configurations

Scenario

The switch is connected to the Internet Service Provider (ISP) router through an uplink interface, while the downlink interface is connects to the user's network. The administrator wants that the switch prevents source IP address spoofing attacks on the downstream interface and prevents illegal users from forging source IP addresses to attack legal users.

Prerequisite

N/A

Default configurations of URPF

Default configurations of URPF are as below.

Function	Default value
Interface URPF status	Disable

8.13.3 Configuring global URPF

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interface interface-type interface-number	Enter interface configuration mode.
3	Raisecom(config-ge-1/0/1)# urpf { loose strict } { allow- default-route }	Enable URPF. • Loose: loose mode • Strict: strict mode • (Optional) allow-default-route: allow to match the default route

8.13.4 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom#show urpf interface { interface-type interface-number }	Show the URPF mode of the interface.

8.14 Time range

8.14.1 Introduction

Some functions need to be started on a scheduled basis or within certain periods, and they can be restricted through the timerange command. When the function (such as ACL, POE, and NQA) that can be paired with timerange is configured, this time range can be quoted through a time period index.

8.14.2 Preparing for configurations

Scenario

When the device needs to execute different security policies in different time ranges, you can configure the time range.

Prerequisite

N/A

Default configurations of time range

Default configurations of time range are as below.

Function	Default value
time range status	Disable

8.14.3 Configuring time range

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#time-range list <i>id</i>	Create a time range list.

Step	Command	Description
3	<pre>Raisecom(config-timerange-*)#time- range timerange-id absolute from hour:minute:second year/month/monthday to hour:minute:second year/month/monthday Raisecom(config-timerange-*)#time- range timerange-id everyhour minute:second to minute:second Raisecom(config-timerange-*)#time- range timerange-id everyday hour:minute:second to hour:minute:second Raisecom(config-timerange-*)#time- range timerange-id everyweek hour:minute:second { mon tue wed thu fri sat sun } to { mon tue wed thu fri sat sun } Raisecom(config-timerange-*)#time- range timerange-id everymonth hour:minute:second monthday to hour:minute:second monthday Raisecom(config-timerange-*)#time- range timerange-id everyweekend hour:minute:second to hour:minute:second Raisecom(config-timerange-*)#time- range timerange-id everyyear hour:minute:second month/monthday to hour:minute:second month/monthday</pre>	Create a time range that can be applied to ACL rules. - Relative time range (periodic time range): periodic time range of one week described by the everyxxx parameter. It can be indicated by an absolute time range to indicate the effective date of the time range. - Absolute time range: a specific time range specified by the absolute parameter. You can limit the relative time range (periodic time range) to take effect within a specific time range specified by the absolute time range. If multiple effective times are configured for this time range, the effective principle is to perform OR between periodic time ranges, and to perform AND between the periodic time range and absolute time range.
4	<pre>Raisecom(configure-acl-12-*)#rule rule-id time-range timerange-list-id</pre>	Apply the time range to the ACL.
5	<pre>Raisecom(config)#nqa schedule admin- name operate-tag time-range time- range-list</pre>	Apply the time range to the NQA.

8.14.4 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	<pre>Raisecom#show timerange list</pre>	Show all time ranges.

8.15 DOS attack prevention

8.15.1 Introduction

Abnormal packet attack prevention

Abnormal packet attack is the process of sending defective IP packets to the target device, causing errors and crashes in processing such IP packets, resulting in losses to the target device. Abnormal packet attack prevention refers to the realtime detection and discarding of abnormal packets by the device, in order to protect the device.

Fragmented packet attack prevention

Fragmented packet attack is a method of sending errored fragmentation packets to the target device, causing it to crash or restart or consuming a large amount of CPU resources while processing the errored fragmentation packets, resulting in losses to the target device. Fragmented packet attack prevention refers to the realtime detection of fragmented packets by devices and discarding or rate limiting of packets, in order to protect the device.

Flood attack prevention

Flood attack refers to the attacker sending a large number of false packets to the target device in a short period, causing the target device to be busy processing useless packets and unable to provide normal services to users.

Flood attack prevention refers to the realtime detection of flood packets by devices and the discarding or rate limiting of packets, in order to protect the device.

Flood attacks are divided into TCP SYN flood attacks, UDP flood attacks, and ICMP flood attacks.

- TCP SYN flood attack

The TCP SYN attack exploits a vulnerability in the TCP three-way handshake. During the three-way handshake in TCP, when the receiving end receives the initial SYN packet from the sending end, it returns a SYN+ACK packet to the sending end. The connection remains in a semi-connected status while the receiving end is waiting for the final ACK packet from the sending end. If the receiving end finally does not receive the ACK packet, then it resends a SYN+ACK packet to the sending end. If the sender does not return an ACK packet after multiple retries, the receiver will close the session and refresh it from memory. It takes approximately 30 seconds from transmitting the first SYN+ACK to closing the session.

During this period, the attacker may send hundreds of thousands of SYN packets to open ports without responding to SYN+ACK packets from the receiving end. The memory of the receiving end will soon exceed its load and it will no longer be able to accept any new connections, and the existing connections will be disconnected.

The method for handling TCP SYN attacks by the device is to limit the rate of TCP SYN packets after enabling TCP SYN flood attack prevention, ensuring that device resources are not exhausted under attack.

- UDP flood attack

The UDP flood attack refers to the attacker sending a large number of UDP packets to the target device in a short period, causing the target device to be overloaded and unable to process normal services. UDP flood attacks can be divided into the following two categories:

- Fraggle attack

The principle of fraggle attack is that the attacker sends UDP packets with the source address being the target host address, the destination address being the broadcast address, and the destination port number being 7. If many hosts in the broadcast network have been activated with UDP response request service, the destination host will receive excessive response packets, causing the system to be busy. In this way, the attack effect is implemented.

After flood attack prevention is enabled, the device takes packets with the UDP port number of 7 as attack packets and discards them directly.

- UDP diagnostic port attack

The attacker sends packets to diagnostic UDP ports (such as 7-echo, 13 day time, and 19 Charge). If a large number of packets are sent simultaneously, they can cause flood and potentially affect the normal operation of network devices.

After flood attack prevention is enabled, the device takes packets with UDP ports of 7, 13, and 19 as attack packets and discards them directly.

- ICMP flood attack

Usually, the network administrator uses the Ping program to monitor and troubleshoot the network. The general process is as follows:

1. The source device sends an ICMP response request packet to the receiving device.
2. After receiving the ICMP response request packet, the receiving device will respond with an ICMP reply packet to the source device.

If the attacker sends a large number of ICMP response request packets to the target device, the target device will be busy processing these requests and unable to continue to process other data packets, causing an impact on normal services.

The device implements Committed Access Rate (CAR) rate limiting against ICMP flood attacks to ensure that the CPU is not attacked and to ensure the normal operation of the network.

8.15.2 Preparing for configurations

Scenario

Devices are often subjected to different types of network attacks, which can lead to high resource utilization and affect network services. To ensure the provision of secure network services to users, deploy attack prevention on devices to prevent the following types of attacks:

- Abnormal packet attack prevention: prevent abnormal packet attacks.
- Fragmented packet attack prevention: limit the rate of fragmented packets, preventing them from attacking the CPU and occupying too much CPU and device resources.
- Flood attack prevention includes the following three types:
 - TCP SYN flood attack: limit the rate of TCP SYN packets, and preventing the CPU from processing TCP SYN packets to consume too many resources.
 - UDP flood attack prevention: directly discard UDP packets sent on specific ports.
 - ICMP flood attack prevention: limit the uploading rate of ICMP flood attack packets to prevent the CPU from processing ICMP flood attack packets and occupying too many resources.

Prerequisites

N/A

8.15.3 Default configurations of DOS attack prevention

Default configurations of DOS attack prevention are as below.

Function	Default value
Global DOS attack prevention status	Disable
Abnormal packet attack prevention	Disable
Fragmented packet attack prevention	Disable
Rate for sending fragmented packets	155000000 bit/s
TCP Syn attack prevention	Disable
Rate for sending TCP Syn flood packets	155000000 bit/s
UDP flood attack prevention	Disable
ICMP flood attack prevention	Disable
Rate for sending ICMP flood packets	155000000 bit/s

8.15.4 Configuring abnormal packet attack prevention

Configure abnormal packet attack prevention for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#dos-antiattack pkt-limit abnormal enable	Enable abnormal packet attack prevention.

8.15.5 Configuring fragmented packet attack prevention

Configure fragmented packet attack prevention for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#dos-antiattack pkt-limit fragment enable	Enable fragmented packet attack prevention.
3	Raisecom(config)#dos-antiattack pkt-limit fragment cir { kbps mbps gbps } cir-number Raisecom(config)#dos-antiattack pkt-limit fragment pps pps-number	Configure the rate for receiving fragmented packets.

8.15.6 Configuring TCP SYN flood attack prevention

Configure TCP SYN flood attack prevention for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#dos-antiattack pkt-limit tcp-syn enable	Enable TCP SYN flood attack prevention.
3	Raisecom(config)#dos-antiattack pkt-limit tcp-syn cir { kbps mbps gbps } cir-number Raisecom(config)#dos-antiattack pkt-limit tcp-syn pps pps-number	Configure the rate for receiving TCP SYN packets.

8.15.7 Configuring UDP flood attack prevention

Configure UDP flood attack prevention for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#dos-antiattack pkt-limit udp-flood enable	Enable UDP flood attack prevention.

8.15.8 Configuring ICMP flood attack prevention

Configure ICMP flood attack prevention for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#dos-antiattack pkt-limit icmp-flood enable	Enable ICMP flood attack prevention.
3	Raisecom(config)#dos-antiattack pkt-limit icmp-flood cir { kbps mbps gbps } cir-number Raisecom(config)#dos-antiattack pkt-limit icmp-flood pps pps-number	Configure the rate for receiving ICMP packets.

8.15.9 Checking configurations

Use the following commands to check configuration results.

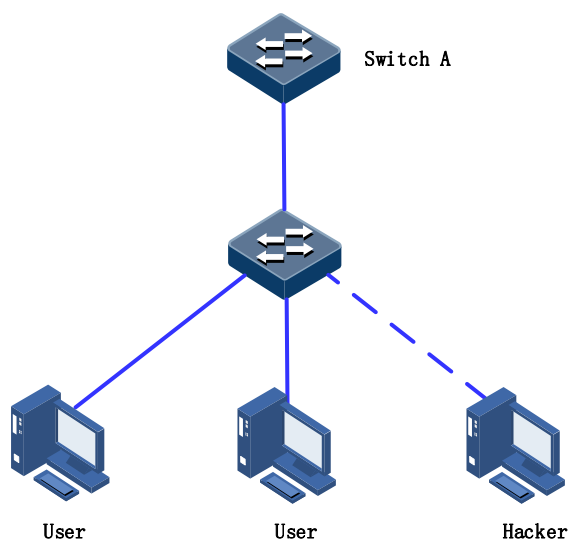
No.	Command	Description
1	Raisecom#show dos- antiattack config	Show configurations of DOS attack prevention.
2	Raisecom#show dos- antiattack statistics	Show statistics of DOS attack prevention.

8.15.10 Example for configuring DOS attack prevention

Networking requirements

If hackers launch abnormal packet attacks, fragmented packet attacks, and flood attacks on Switch A within the LAN, this will cause Switch A to crash. To prevent this situation, the administrator hopes to deploy various attack prevention measures on Switch A to provide users with a secure network environment and ensure normal network services.

Figure 8-16 DOS attack prevention



Configuration steps

Step 1 Configure DOS attack prevention.

```
Raisecom#configure
Raisecom(config)#dos-antiattack pkt-limit enable
```

Step 2 Configure abnormal packet attack prevention.

```
Raisecom(config)#dos-antiattack pkt-limit abnormal enable
```


- Step 3 Configure fragmented packet attack prevention. Configure the rate for receiving fragmented packets to 15 kbit/s.

```
Raisecom(config)#dos-antiattack pkt-limit fragment enable
Raisecom(config)#dos-antiattack pkt-limit fragment cir kbps 15
```

- Step 4 Configure TCP SYN attack prevention. Configure the rate for receiving TCP SYN packets to 15 kbit/s.

```
Raisecom(config)#dos-antiattack pkt-limit tcp-syn enable
Raisecom(config)#dos-antiattack pkt-limit tcp-syn cir kbps 15
```

- Step 5 Configure UDP flood attack prevention.

```
Raisecom(config)#dos-antiattack pkt-limit udp-flood enable
```

- Step 6 Configure ICMP flood attack prevention. Configure the rate for receiving ICMP flood packets to 15 kbit/s.

```
Raisecom(config)#dos-antiattack pkt-limit icmp-flood enable
Raisecom(config)#dos-antiattack pkt-limit icmp-flood cir kbps 15
```

Checking results

Use the **show dos-antiattack config** command to show configurations of DOS attack prevention.

```
Raisecom#show dos-antiattack config
!
!
dos-antiattack pkt-limit enable
!
dos-antiattack pkt-limit abnormal enable
dos-antiattack pkt-limit fragment enable
dos-antiattack pkt-limit fragment cir kbps 15
dos-antiattack pkt-limit tcp-syn enable
dos-antiattack pkt-limit tcp-syn cir kbps 15
dos-antiattack pkt-limit udp-flood enable
dos-antiattack pkt-limit icmp-flood enable
dos-antiattack pkt-limit icmp-flood cir kbps 15
```

9 Reliability

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

- Link aggregation
- G.8031
- G.8032
- STP/RSTP
- MSTP
- Loop detection
- Interface backup
- Interface isolation
- L2CP
- BFD
- Link flap protection
- Interface loopback

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

Function	Default value
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)#interface eth-trunk <i>trunk-number</i>	Enter aggregation group configuration mode.

Step	Command	Description
4	<code>Raisecom(config-eth-trunk-*)#mode lacp-static</code>	Configure the working mode of the LAG to static LACP LAG.
5	<code>Raisecom(config-eth-trunk-*)#lacp timeout { fast slow }</code>	Configure the LACP timeout mode. By default, it is slow.
6	<code>Raisecom(config-eth-trunk-*)#active-linknumber { max min } { number 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-1/0/*)#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-1/0/*)#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.

Step	Command	Description
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.
4	<code>Raisecom(config-eth-trunk-*)#add primary interface interface-type interface-number</code>	Configure the master interface of the LAG.
5	<code>Raisecom(config-eth-trunk-*)#add secondary interface interface-type interface-number</code>	Configure the slave interface of the LAG.
6	<code>Raisecom(config-eth-trunk-*)#revert enable</code> <code>Raisecom(config-eth-trunk-*)#wait-to-store time</code>	Configure the revertive mode and WTR time of the LAG. By default, the mode is non-revertive.
7	<code>Raisecom(config-eth-trunk-*)#exit</code>	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	<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-*)#load-balance { src-mac dst-mac srcdst-mac src-ip dst-ip srcdst-ip default }</code>	Configure the load balancing algorithm for the LAG globally. By default, the system adopts the src-dst-mac mode; in other words, the system selects the forwarding interface according to the OR operation of the source MAC address and destination MAC address.

9.1.8 Checking configurations

Use the following commands to check configuration results.

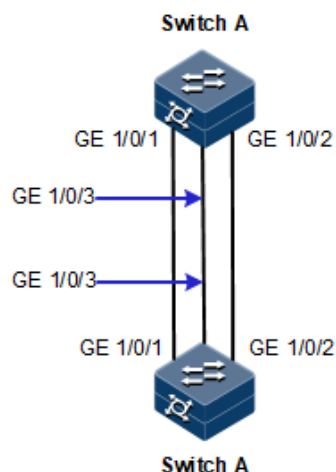
No.	Command	Description
1	Raisecom#show lacp eth-trunk trunk-number	Show the local system LACP interface status, flag, interface priority, administration key, operation key, and interface status machine status. The information about LACP neighbors include the tag, interface priority, device ID, Age, 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 1/0/1, GE 1/0/2, and GE 1/0/3 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)#lACP system-priority 1000
SwitchA(config)#int eth-trunk 1
SwitchA(config-eth-trunk-1)#mode lACP-static
SwitchA(config-eth-trunk-1)#add interface ge 1/0/1
SwitchA(config-eth-trunk-1)#add interface ge 1/0/2
SwitchA(config-eth-trunk-1)#add interface ge 1/0/3
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 lACP-static
SwitchB(config-eth-trunk-1)#add interface ge 1/0/1
SwitchB(config-eth-trunk-1)#add interface ge 1/0/2
SwitchB(config-eth-trunk-1)#add interface ge 1/0/3
SwitchB(config-eth-trunk-1)#exit
```

Checking results

Use the **show lACP eth-trunk 1** command to show global configurations of the static LACP link aggregation on Switch A.

```
SwitchA#show lACP 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-1/0/1 :
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-1/0/2 :
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-1/0/3 :
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.8031

9.2.1 Introduction

G.8031 is a linear protection switching standard defined by ITU-T based on VLAN Ethernet technologies. In the protection switching mechanism, corresponding protection resources are allocated to all work resources, such as paths and bandwidth. Compared with the spanning tree protection technology defined by IEEE, the protection technology defined by G.8031 is simple and fast, implementing network resource switching in a predictable way, making it easier for carriers to effectively plan the network and understand the network's activity status and to achieve carrier-grade operations.

G.8031 defines two protection structures, 1+1 and 1:1. In the 1+1 structure, each protection resource corresponds to a working resource. In the protection domain, the 1+1 structure adopts the double-transmitting single-receiving protection mechanism. The 1:1 structure adopts a mechanism of switching between protecting resources and working resources.

- Fault detection mechanism

G.8031 uses Continuity Check (CC) defined in Y.1731 or IEEE 802.1ag for bidirectional link forwarding detection, which can locate the fault point and detect whether the fault is unidirectional or bidirectional. In protection conversion, the default transmission period of CC messages is 3.33ms (in other words, the transmission rate is 300 frames per second).

Two adjacent nodes periodically send CC messages from the physical interface to detect faults. When a node detects the loss of CC messages within a specific period, it regards this as a fault.

The node sends a Remote Defect Indication (RDI) frame from the interface where the fault is detected. If it is a unidirectional fault, the downstream node of the link will detect the RDI frame.

- 1+1 protection structure

In the 1+1 structure, the protection line is dedicated to each working line, and the working line and protection line are bridged at the source end of the protection domain. The services are simultaneously sent to the host of the protection domain on both the working line and protection line. At the host, the selector selects to receive the business from the work or protection line based on defect indications.

The switching types of 1+1 Ethernet linear protection include unidirectional switching and bidirectional switching. For unidirectional switching, only the affected line direction is switched to the protection line, and the selectors at both ends are independent and do not require APS signaling support. The mechanism of bidirectional switching is similar to unidirectional, usually requiring APS signaling to be coordinated at both ends. Unidirectional protection can prevent unidirectional faults in two independent directions.

The operation types of 1+1 Ethernet linear protection can be either non-revertive or revertive. In revertive mode, when the faulty link is restored, the WTR timer is started. After the WTR times out, the selector switches services to the working line. In non-revertive mode, even if the faulty link is restored, the selector is still connected to the protection line.

- 1:1 protection structure

In a 1:1 structure, the protected line is dedicated to each working line, and the protected work services are transmitted by either the working line or protection line. The method for selecting the work line and protection line is based on defect indication mechanism.

The switching types of 1:1 Ethernet linear protection also include unidirectional switching and bidirectional switching. The operation types can be revertive or non-revertive. During bidirectional switching, both the affected line direction and unaffected line direction are switched to the protected line, but unidirectional switching only switches the affected line direction to the protection line. In switching, the source connector and destination connector need to switch to the same line, so Automatic Protection Switching (APS) is required to coordinate both ends of the line.

In 1:1 protection switching mode, based on local or nearby information and APS protocol information from the other end or remote end, protection switching is implemented by the source selector bridge and the destination selector of the protection domain together.

The CC message is used to detect faults in the working line and protection line. When the working is faulty, the selector at the detected end switches services to the protection line and sends APS notification to the other end. The source end receives APS notification and synchronizes switching.

9.2.2 Preparing for configurations

Scenario

N/A

Prerequisite

- Connect the interface, configure its physical parameters, and make it Up at the physical layer.

- Create VLANs.
- Add the interface to VLANs.

9.2.3 Default configurations of G.8031

Default configurations of G.8031 are as below.

Function	Default value
G.8031 mode	Revertive
WTR timer	5min
Hold-off timer	0

9.2.4 Creating a G.8031 protection group

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#g8031 instance <i>instance-id</i>	Create a G.8031 instance, and enter the configuration node.
3	Raisecom(config-g8031-instance-*)#control-vlan <i>vlan-id</i>	Specify the control VLAN. The protection group is in non-revertive mode if you configure the revertive disable parameter. • In revertive mode, when the working line recovers from a fault, traffic is switched from the protection line to the working line. • In non-revertive mode, when the working line recovers from a fault, traffic is not switched from the protection line to the working line.
4	Raisecom(config-g8031-instance-*)#data-vlan <i>vlan-id</i>	Specify the data VLAN.
5	Raisecom(config-g8031-instance-*)#working-port interface <i>interface-type interface-number</i>	Configure the interface, and specify it as the working interface.
6	Raisecom(config-g8031-instance-*)#protection-port interface <i>interface-type interface-number</i>	Configure the interface, and specify it as the protection interface.
7	Raisecom(config-g8031-instance-*)#wtr-timer <i>wtr-time</i>	Configure the 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
8	<code>Raisecom(config-g8031-instance-*)#holdoff-timer holdoff-time</code>	Configure the Hold-off timer. When the working line is faulty, the system delays the fault reporting and thus switches services to the protection line after a period. This prevents frequent switching of lines due to the flapping of the working line.  Note If the Hold-off timer value is over great, it may influence 50ms switching performance. Therefore, we recommend configuring the Hold-off timer value to 0.

9.2.5 (Optional) configuring G.8031 switching control

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config-g8031-instance-*)#protection-switch force-switch</code>	Configure forcible switch (FS) of the traffic from the working line to the protection line. FS can be configured on multiple interfaces on multiple ring nodes.
3	<code>Raisecom(config-g8031-instance-*)#protection-switch manual-switch</code>	Configure manual switch (MS) of the traffic from the working line to the protection line. Its priority is lower than that of FS and APS. FS can be configured on only one interface on only one ring node.
4	<code>Raisecom(config-g8031-instance-*)#protection-switch clear</code>	Configure traffic switching clearing.

9.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show g8031 interface</code>	Show the status of the G.8031 interface.
2	<code>Raisecom#show g8031 instance [instance-id]</code>	Show the status of G.8031

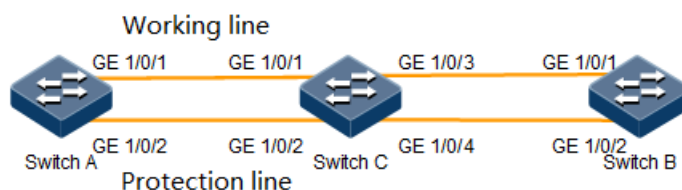
9.2.7 Example for configuring G.8031

Networking requirements

As shown below, to improve Ethernet reliability, switches A, B, and C form G.8031 protection lines.

The protocol control VLAN is VLAN 2. The blocked VLANs are the default ones: VLANs 2–10.

Figure 9-2 G.8031 networking



Configuration steps

Step 1 Add interfaces to VLANs 2–10.

Configure switch A.

```
Raisecom#hostname SwitchA
SwitchA#configure
SwitchA(config)#interface ge 1/0/1 to ge 1/0/2
SwitchA(config-ge-1/0/1->ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/1->ge-1/0/2)#port trunk allow-pass vlan 2-10
SwitchA(config-ge-1/0/1->ge-1/0/2)#exit
```

Configure switch B with the same configurations of switch A.

Configure switch C.

```
Raisecom#hostname SwitchC
SwitchC#configure
SwitchC(config)#interface ge 1/0/1 to ge 1/0/4
SwitchC(config-ge-1/0/1->ge-1/0/4)#port link-type trunk
SwitchC(config-ge-1/0/1->ge-1/0/4)#port trunk allow-pass vlan 2-10
SwitchC(config-ge-1/0/1->ge-1/0/4)#exit
```

Step 2 Create a protection group.

Configure switch A.

```
SwitchA(config)#g8031 instance 1
SwitchA(config-g8031-instance-1)#control-vlan 2
```

```
SwitchA(config-g8031-instance-1)#data-vlan 2-10
SwitchA(config-g8031-instance-1)#working-port interface ge 1/0/1
SwitchA(config-g8031-instance-1)#protection-port interface ge 1/0/2
```

Configure switch B.

```
SwitchC(config)#g8031 instance 1
SwitchC(config-g8031-instance-1)#control-vlan 2
SwitchC(config-g8031-instance-1)#data-vlan 2-10
SwitchC(config-g8031-instance-1)#working-port interface ge 1/0/1
SwitchC(config-g8031-instance-1)#protection-port interface ge 1/0/2
```

Checking results

Use the **show g8031 interface** command on the device to check whether G.8031 protection has taken effect.

Take switch A for example. The status information is as below:

```
SwitchA#show g8031 interface
Instance Interface      Role      Active Operate Forward  RxCount
TxCount
-----
1      ge-1/0/1      working  active working forwarding 0      0
1      ge-1/0/2      protection standby working blocking 0      6
-----
```

Manually disconnect the link to emulate a fault. Use the command on switch A again to check the G.8031 protection status.

```
SwitchA#show g8031 interface
Instance Interface      Role      Active Operate Forward  RxCount
TxCount
-----
1      ge-1/0/1      working  standby failed blocking 0      0
1      ge-1/0/2      protection active working forwarding 0      6
-----
```

9.3 G.8032

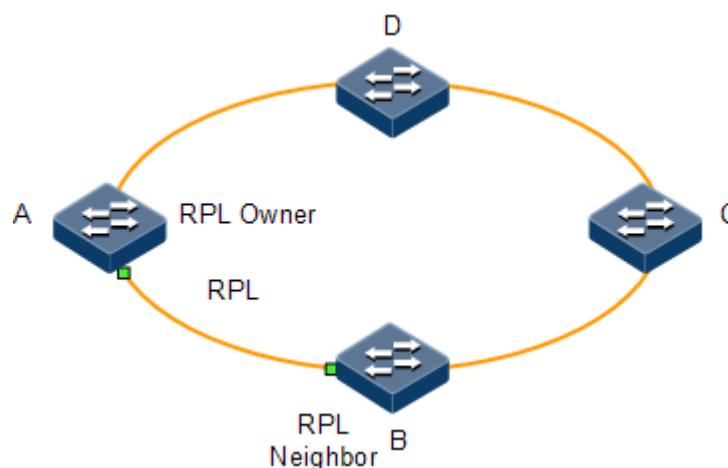
9.3.1 Introduction

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 9-3 G.8032 ring networking



The basic concepts of G.8032 Ethernet Ring Protection Switching as shown in Figure 9-3 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.

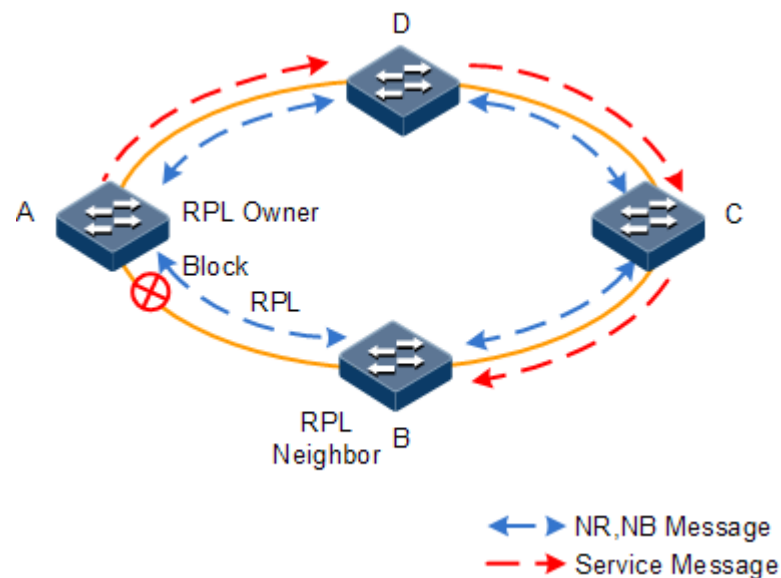
Ring states

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 9-4.

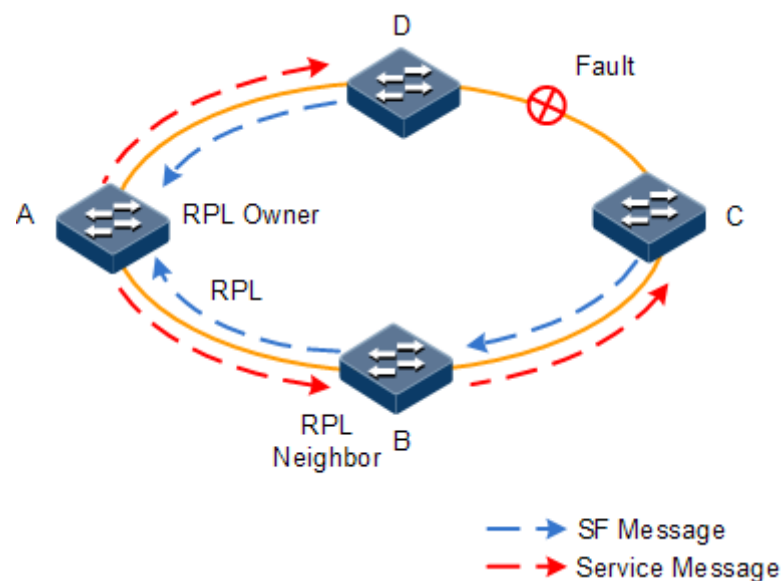
Figure 9-4 Idle state



As shown in Figure 9-4, 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 9-5 Protecting state



As shown in Figure 9-5, 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 9-5, 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.

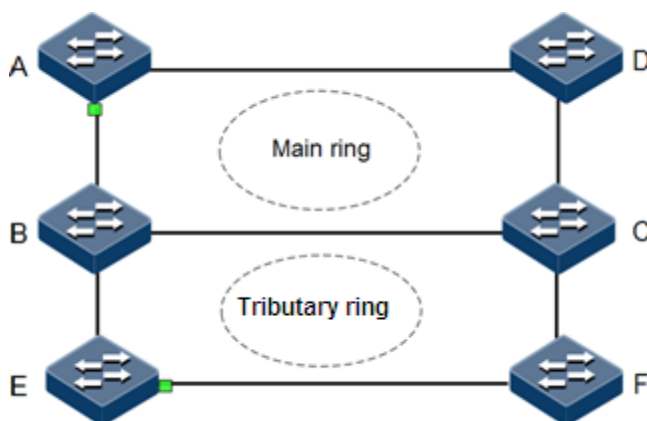
When the faults are recovered, the link is switched to faults recovery.

- 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 9-6 Tributary ring



As shown in Figure 9-6, 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.

9.3.2 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.

9.3.3 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
Tributary ring virtual channel mode in intersecting node	With
Ring Propagate switch in crossing node	Disable

9.3.4 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 9.3.5 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 instance <i>instance-id</i>	Create a G.8032 instance, and enter the G.8032 node.
3	Raisecom(config-g8032-instance-*)#control-vlan <i>vlan-id</i>	Specify the control 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.
4	Raisecom(config-g8032-instance-*)#data-vlan <i>vlan-id</i>	Specify the data VLAN.

Step	Command	Description
5	<code>Raisecom(config-g8032-instance-*)# add interface interface-type interface-number [rpl { owner neighbor }]</code>	Configure the RPL interface and RPL role.
6	<code>Raisecom(config-g8032-instance-*)#version { v1 v2 }</code>	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.
7	<code>Raisecom(config-g8032-instance-*)#guard-timer guard-time</code>	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.
8	<code>Raisecom(config-g8032-instance-*)#wtr-timer wtr- time</code>	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.
9	<code>Raisecom(config-g8032-instance-*)#holdoff-timer holdoff-time</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.

9.3.5 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 9.3.4 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 9.3.4 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	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)# g8032 instance instance-id	Create an instance.
3	Raisecom(config-g8032-instance-*)#control-vlan vlan-id	Specify the control 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.
4	Raisecom(config-g8032-instance-*)#data-vlan vlan-id	Specify the data VLAN.
5	Raisecom(config-g8032-instance-*)#virtual-control-vlan vlan-id	Specify the virtual channel VLAN.
6	Raisecom(config-g8032-instance-*)# add interface interface-type interface-number [rpl { owner neighbor }]	Configure the RPL interface and RPL role.
7	Raisecom(config-g8032-instance-*)# add interface interface-type interface-number vc-mep	Configure the RPL interface, and specify it as the VC MEP.

9.3.6 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-instance-*)#force-switch <i>interface-type</i> <i>interface-number</i>	Configure FS of the traffic on the protection ring. FS can be configured on multiple interfaces of multiple ring nodes.
3	Raisecom(config-g8032-instance-*)#manual-switch <i>interface-type</i> <i>interface-number</i>	Configure MS of the traffic on the protection ring to the interface 1 or 2. Its priority is lower than the one of FS and APS. MS can be configured on only one interface one only one ring node.



Note

By default, traffic is automatically switched to the other line when the current line fails to forward traffic.

9.3.7 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.

9.3.8 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)#g8032 instance <i>instance-id</i> Raisecom(config-g8032-instance-*)#clear	Clear the effect of the ring protection control command (force-switch, manual-switch, WTR timer timeout, and WTB timer timeout).

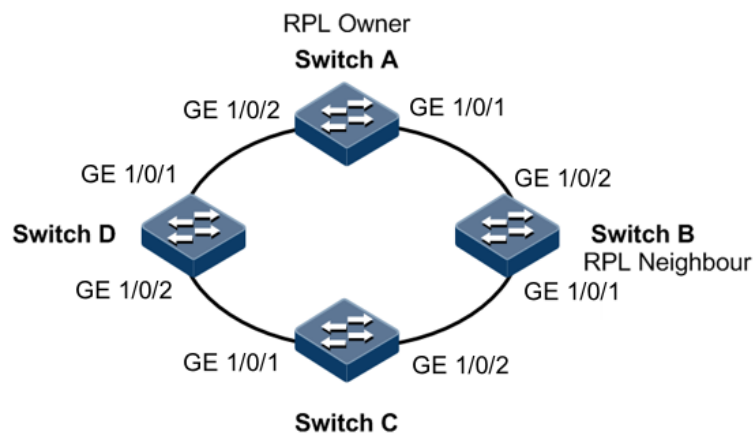
9.3.9 Example for configuring single ring G.8032

Networking requirements

As show in Figure 9-7, 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 9-7 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 instance 1
SwitchA(config-g8032-instance-1)#control-vlan 1
SwitchA(config-g8032-instance-1)#data-vlan 2-10
```



```
SwitchA(config-g8032-instance-1)#add interface ge 1/0/1 rpl owner
SwitchA(config-g8032-instance-1)#add interface ge 1/0/2
```

Configure Switch B.

```
SwitchB(config)#g8032 instance 1
SwitchB(config-g8032-instance-1)#control-vlan 1
SwitchB(config-g8032-instance-1)#data-vlan 2-10
SwitchA(config-g8032-instance-1)#add interface ge 1/0/1 rpl neighbor
SwitchA(config-g8032-instance-1)#add interface ge 1/0/2
```

Configure Switch C.

```
SwitchC(config)#g8032 instance 1
SwitchC(config-g8032-instance-1)#control-vlan 1
SwitchC(config-g8032-instance-1)#data-vlan 2-10
SwitchC(config-g8032-instance-1)#add interface ge 1/0/1
SwitchC(config-g8032-instance-1)#add interface ge 1/0/2
```

Configure Switch D.

```
SwitchD(config)#g8032 instance 1
SwitchD(config-g8032-instance-1)#control-vlan 1
SwitchD(config-g8032-instance-1)#data-vlan 2-10
SwitchD(config-g8032-instance-1)#add interface ge 1/0/1
SwitchD(config-g8032-instance-1)#add interface ge 1/0/2
```

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
```

Count	Instance Tx-Count	Interface	Role	Type	Operate	Forward	Rx-
1		ge 1/0/1	port1	rpl	working	blocking	0 15

```
1      ge 1/0/2      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 1/0/1	port1	rpl	working	forwarding	16	41
1		ge 1/0/2	port2	normal	failed	blocking	18	42

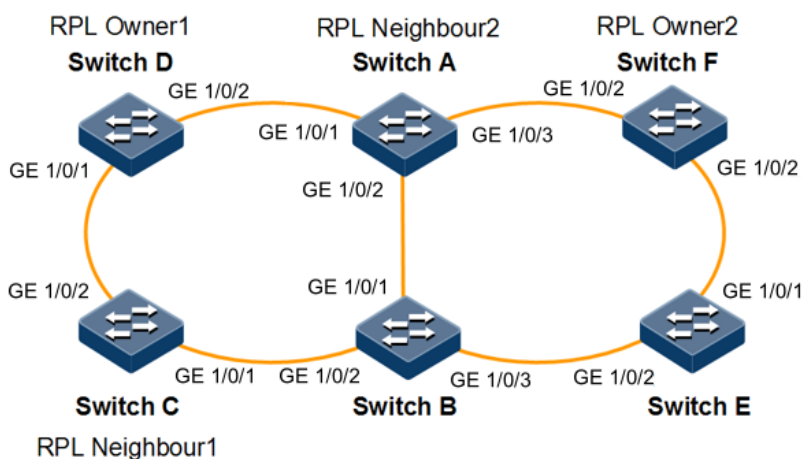
9.3.10 Example for configuring intersecting G.8032

Networking requirements

As shown in Figure 9-8, 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 GE 1/0/1 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 GE 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 9-8 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 1/0/1 to ge 1/0/3
Switch(config-ge-1/0/1->ge-1/0/3)#port link-type trunk
Switch(config-ge-1/0/1->ge-1/0/3)#port trunk allow-pass vlan all
Switch(config-ge-1/0/1->ge-1/0/3)#exit
```

Configure Switches C, D, E, and F.

```
Switch#configure
Switch(config)#vlan 1-4094
Switch(config)#interface ge 1/0/1 to ge 1/0/2
Switch(config-ge-1/0/1->ge-1/0/2)#port link-type trunk
Switch(config-ge-1/0/1->ge-1/0/2)#port trunk allow-pass vlan all
Switch(config-ge-1/0/1->ge-1/0/2)#exit
```

Step 2 Create a main ring for G.8032 protection ring.

Configure Switches A and B.

```
Switch(config)#g8032 instance 1
Switch(config-g8032-instance-1)#control-vlan 1
Switch(config-g8032-instance-1)#data-vlan 1-4094
Switch(config-g8032-instance-1)#add interface ge 1/0/1
```

```
Switch(config-g8032-instance-1)#add interface ge 1/0/2
```

```
Switch(config)#g8032 instance 1
Switch(config-g8032-instance-1)#control-vlan 1
Switch(config-g8032-instance-1)#data-vlan 1-4094
Switch(config-g8032-instance-1)#add interface ge 1/0/1
Switch(config-g8032-instance-1)#add interface ge 1/0/2 rpl neighbour
```

Configure Switch D.

```
Switch(config)#g8032 instance 1
Switch(config-g8032-instance-1)#control-vlan 1
Switch(config-g8032-instance-1)#data-vlan 1-4094
Switch(config-g8032-instance-1)#add interface ge 1/0/1 rpl owner
Switch(config-g8032-instance-1)#add interface ge 1/0/2
```

Step 3 Configure a tributary ring for G.8032.

Configure Switch A.

```
Switch(config)#g8032 instance 2
Switch(config-g8032-instance-2)#control-vlan 4094
Switch(config-g8032-instance-2)#data-vlan 1-4094
Switch(config-g8032-instance-2)#add interface ge 1/0/3 rpl owner
Switch(config-g8032-instance-2)#virtual-control-vlan 3
```

Configure Switch B.

```
Switch(config)#g8032 instance 2
Switch(config-g8032-instance-2)#control-vlan 4094
Switch(config-g8032-instance-2)#data-vlan 1-4094
Switch(config-g8032-instance-2)#add interface ge 1/0/3
Switch(config-g8032-instance-2)#virtual-control-vlan 3
```

Configure Switch E.

```
Switch(config)#g8032 instance 2
Switch(config-g8032-instance-2)#control-vlan 4094
Switch(config-g8032-instance-2)#data-vlan 1-4094
Switch(config-g8032-instance-2)#add interface ge 1/0/1
Switch(config-g8032-instance-2)#add interface ge 1/0/2
```

Configure Switch F.

```
Switch(config)#g8032 instance 2
Switch(config-g8032-instance-2)#control-vlan 4094
Switch(config-g8032-instance-2)#data-vlan 1-4094
Switch(config-g8032-instance-2)#add interface ge 1/0/1 rp1 neighbour
Switch(config-g8032-instance-2)#add interface ge 1/0/2
```

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

	Instance	Interface	Role	Type	Operate	Forward	Rx-
Count	Tx-Count						

1		ge 1/0/1	port1	rp1	working	blocking	0 :::
15							
	1	ge 1/0/2	port2	normal	working	forwarding	
0 :::			11				

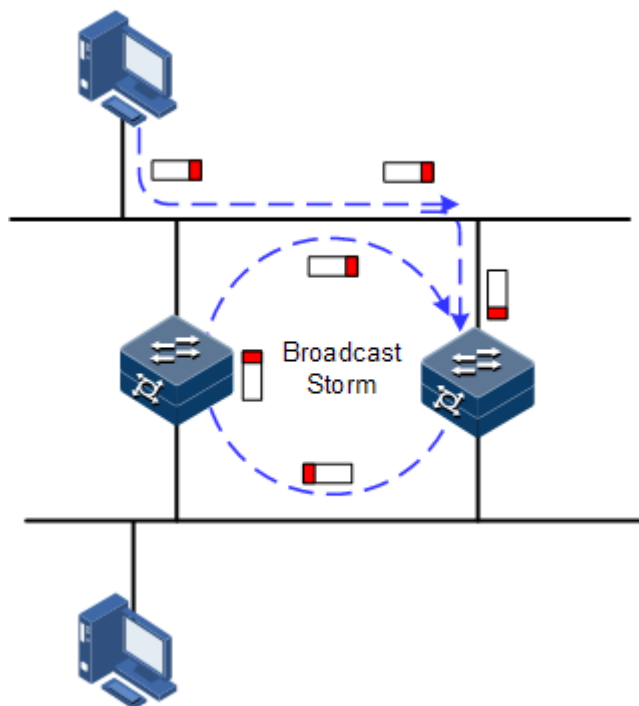
9.4 STP/RSTP

9.4.1 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 9-9.

Figure 9-9 Network storm due to loopback

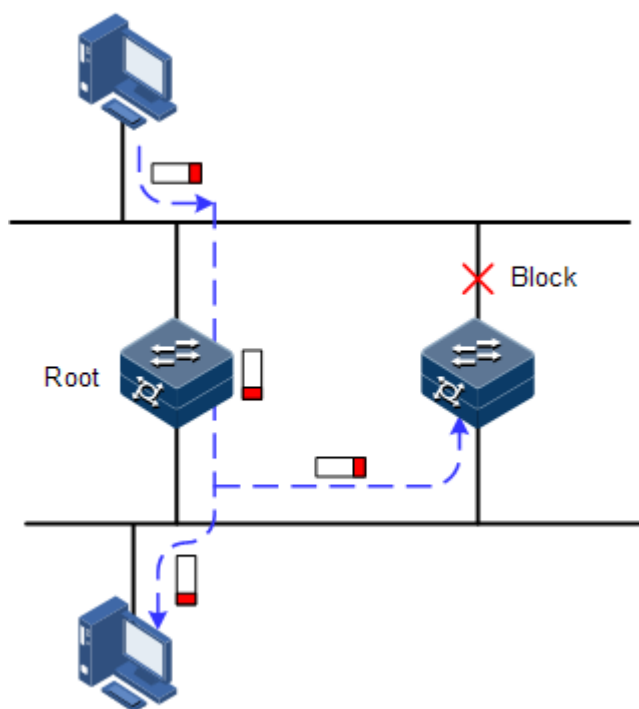


Spanning Tree Protocol (STP) is compliant to IEEE 802.1d standard and used to remove data physical loop in data link layer in the LAN.

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 9-10 shows loop networking with STP.

Figure 9-10 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

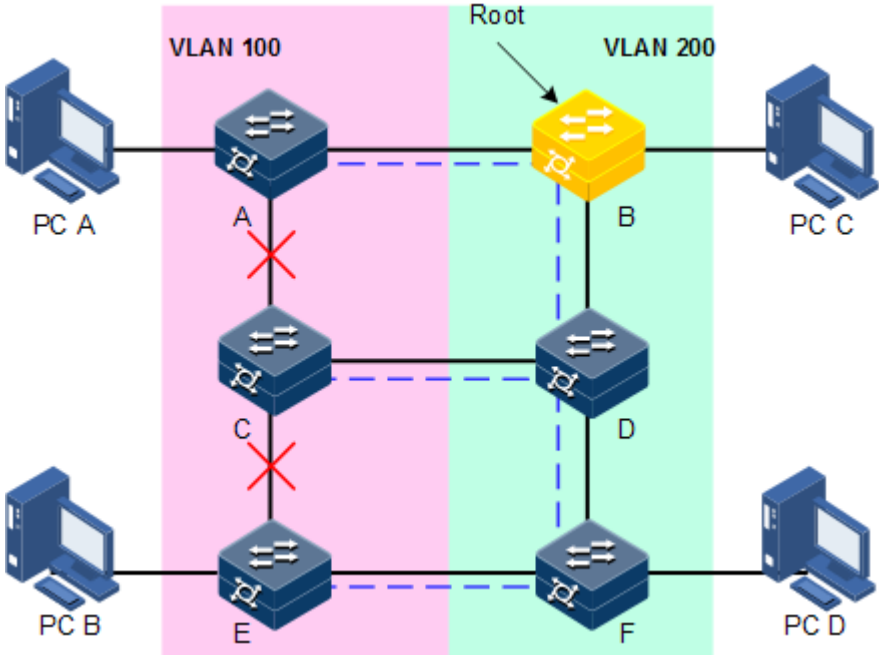
For improving the slow convergent speed of STP, IEEE 802.1w establishes Rapid Spanning Tree Protocol (RSTP), which increases the mechanism to change interface blocking state to forwarding state, speed up the topology convergence rate.

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 9-11, 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 9-11 Failure in forwarding VLAN packets due to RSTP



9.4.2 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

9.4.3 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

9.4.4 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- 1/0/*)#stp { enable disable }	Enable interface STP.

9.4.5 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-1/0/*)#stp priority <i>priority-value</i>	Configure interface priorities on the device.
4	Raisecom(config-ge-1/0/*)#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.

9.4.6 Configuring the root/backup bridge

Two methods for STP/RSTP root selection are as below:

- After the device priority is configured, it is calculated by the spanning tree. Then, the root bridge or backup bridge is determined.
- Assign the root bridge 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, STP/RSTP 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)#stp root { primary secondary default }	Configure the device as the root bridge or backup bridge for a spanning tree instance.

9.4.7 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 interface-type interface- number	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.

Step	Command	Description
3	<code>Raisecom(config-ge-1/0/*)#stp edge-port { enable disable }</code>	Configure attributes of the RSTP edge interface.

9.4.8 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	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<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.
3	<code>Raisecom(config-ge-1/0/*)#stp point-to-point { force-true force-false auto }</code>	Configure the link type for interface.

9.4.9 Checking configurations

Use the following commands to check configuration results.

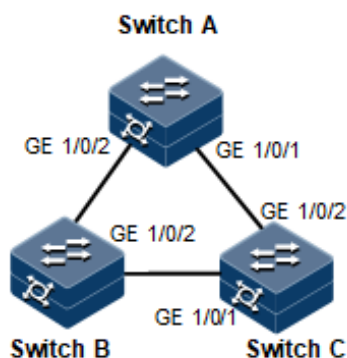
No.	Command	Description
1	<code>Raisecom#show stp information</code>	Show basic configurations of STP.
2	<code>Raisecom#show stp interface</code>	Show configurations of the spanning tree on the interface.
3	<code>Raisecom#show stp bridge</code>	Show information about the root bridge of STP.

9.4.10 Example for configuring STP

Networking requirements

As shown in Figure 9-12, 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 9-12 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 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#stp enable
SwitchA(config-ge-1/0/1)#exit
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/2)#stp enable
SwitchA(config-ge-1/0/2)#exit
```

Configure Switch B.

```
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#port link-type trunk
SwitchB(config-ge-1/0/1)#stp enable
SwitchB(config-ge-1/0/1)#exit
SwitchB(config)#interface ge 1/0/2
SwitchB(config-ge-1/0/2)#port link-type trunk
SwitchB(config-ge-1/0/2)#stp enable
SwitchB(config-ge-1/0/2)#exit
```

Configure Switch C.

```
SwitchC(config)#interface ge 1/0/1
SwitchC(config-ge-1/0/1)#port link-type trunk
SwitchC(config-ge-1/0/1)#stp enable
SwitchC(config-ge-1/0/1)#exit
SwitchC(config)#interface ge 1/0/2
SwitchC(config-ge-1/0/2)#port link-type trunk
SwitchC(config-ge-1/0/2)#stp enable
SwitchC(config-ge-1/0/2)#exit
```

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

Configure Switch A.

```
SwitchA(config)#stp priority 0
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#stp path-cost 10
```

Configure Switch B.

```
SwitchB(config)#interface ge 1/0/1
```

```
SwitchB(config-ge-1/0/1)#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-1/0/1				designated
forward	--	different			
			0	ge-1/0/2	designated
forward	--	different			

9.5 MSTP

9.5.1 Introduction

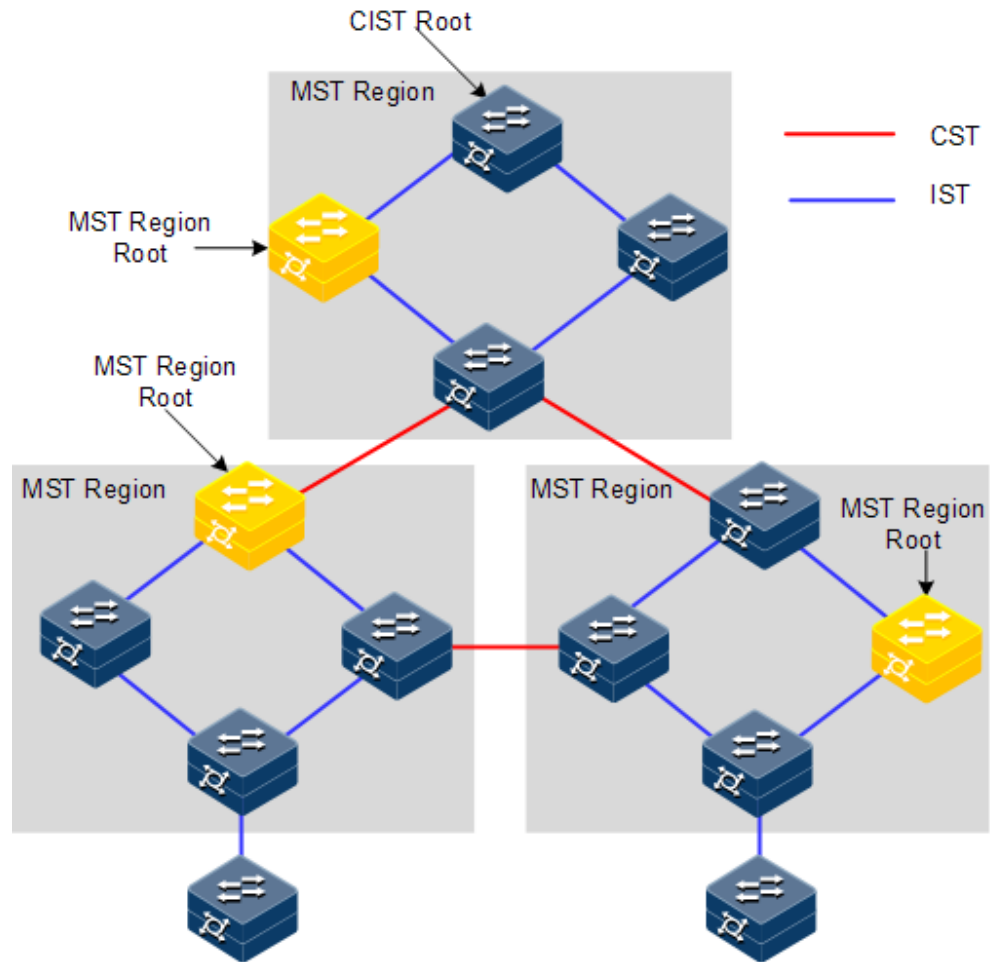
Multiple Spanning Tree Protocol (MSTP) is defined by IEEE 802.1s. Recovering the disadvantages of STP and RSTP, the MSTP implements fast convergence and distributes different VLAN flow following its own path to provide an excellent load balancing mechanism.

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.

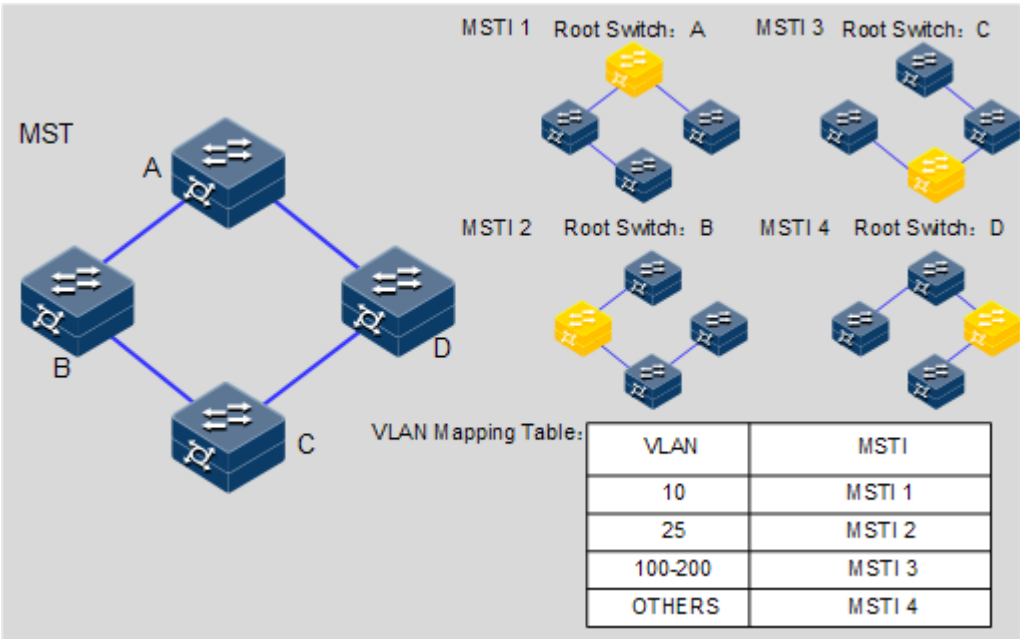
Compared with STP and RSTP, MSTP also introduces total root (CIST Root) and region root (MST Region Root) concepts. The total root is a global concept; all switches running STP/RSTP/MSTP can have only one total root, which is the CIST Root. The region root is a local concept, which is relative to an instance in a region. As shown in Figure 9-13, 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 9-13 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 9-14.

Figure 9-14 MSTI concepts

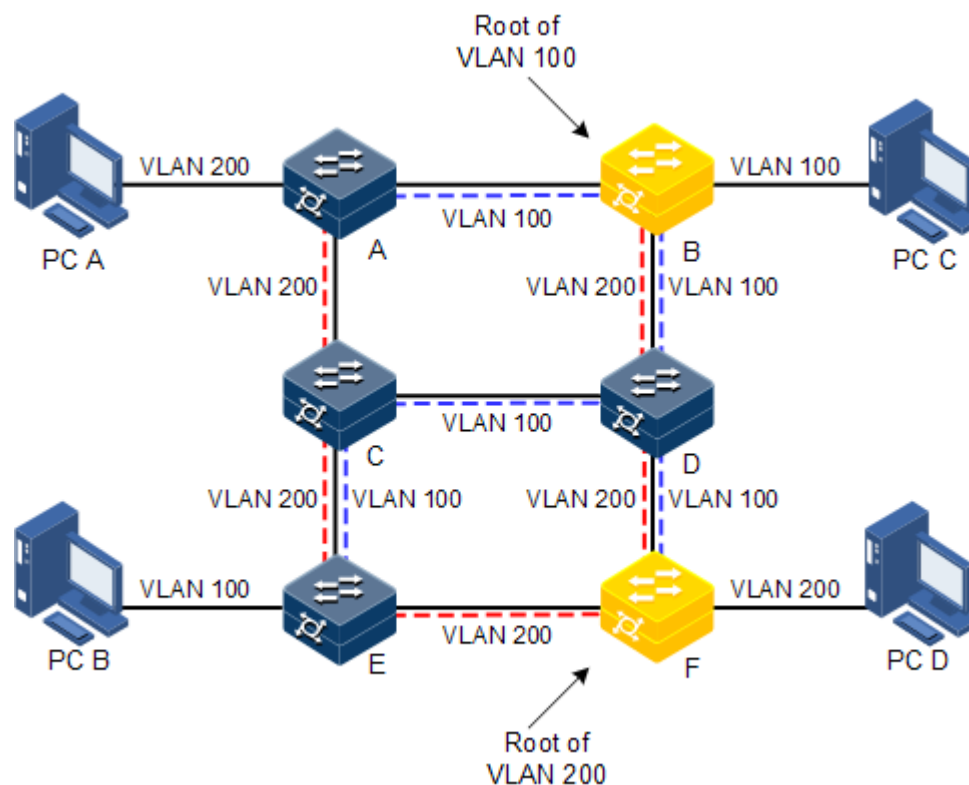


Note

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 9-15 Networking with multiple spanning trees instances in MST region



Apply MSTP to the network as shown in Figure 9-15. 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.

9.5.2 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

9.5.3 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

9.5.4 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-1/0/*)#stp { enable disable }	Enable interface STP.

9.5.5 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</i> vlan <i>vlan-list</i>	Configure mapping from the MST region VLAN to instance.
3	Raisecom(config)#stp config-name <i>name</i>	Configure the MST region name.
4	Raisecom(config)#stp revision-level <i>level-value</i>	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.

9.5.6 Configuring the root/backup bridge

Two methods for MSTP root selection are as below:

- After the device priority is configured, it is calculated by the spanning tree. Then, the root bridge or backup bridge is determined.
- Assign the root bridge 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 <i>instance-id</i>] 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 the 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.

9.5.7 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-1/0/*)#stp [instance <i>instance-id</i>] priority <i>priority-value</i> Raisecom(config-ge-1/0/*)#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.

9.5.8 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-1/0/*)#stp [instance <i>instance-id</i>] path- cost <i>cost-value</i>	Configure the path cost of the interface.

9.5.9 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.

9.5.10 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.

9.5.11 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.

9.5.12 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-1/0/*)#stp bpdu-filter { enable disable }	Configure BPDU filtering on the edge interface.

9.5.13 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.

Step	Command	Description
2	<code>Raisecom(config)#stp bpduprotection { enable disable }</code>	Configure BPDU Guard.
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-1/0/*)#stp bpduprotection 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.

9.5.14 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-1/0/*)#stp mcheck</code>	(Optional) forcibly configure the interface to MSTP mode.

9.5.15 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-1/0/*)#stp point-to-point { force-true force-false auto }	Configure the link type of the interface.

9.5.16 Configuring root interface protection

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 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.
3	Raisecom(config-ge-1/0/*)#stp root-protection { enable disable }	Enable/Disable root interface protection.

9.5.17 Configuring interface loop guard

The spanning tree has two functions: loop guard and link backup. Loop guard 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.

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



Note

Loop guard and link backup are mutually exclusive; in other words, loop guard is implemented on the cost of disabling link backup.

Configure interface loop 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 or aggregation group configuration mode. Take physical interface configuration mode for example.
3	Raisecom(config-ge-1/0/*)#stp loop-guard { enable disable }	Configure interface loop guard.

9.5.18 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.

Step	Command	Description
3	Raisecom(config-ge-1/0/*)#stp tc-restriction { enable disable }	Configure TC packet suppression.

9.5.19 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 disable }	Configure TC protection.

9.5.20 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.

9.5.21 Maintenance

Maintain the device as below.

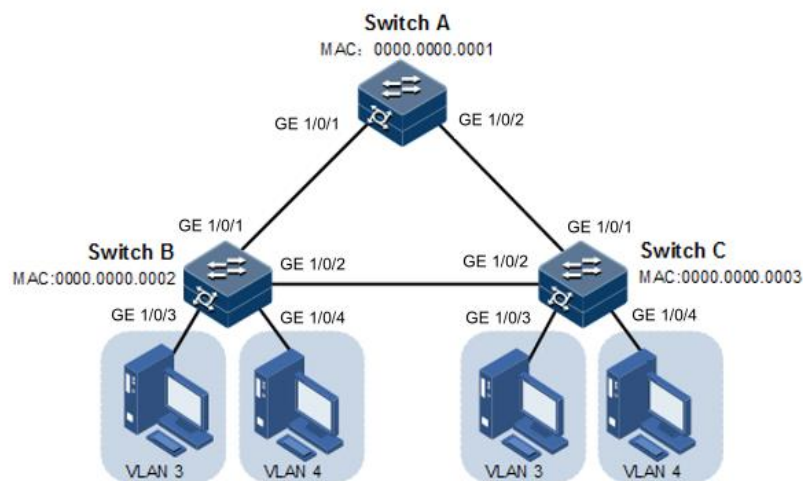
Command	Description
<code>Raisecom(config-ge-1/0/*)#reset stp statistics</code>	Clear statistics about spanning tree on the interface.

9.5.22 Example for configuring MSTP

Networking requirements

As shown in Figure 9-16, 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. Instance 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 9-16 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 1/0/1 and GE 1/0/2 on Switch A to allow packets of all VLAN to pass in Trunk mode. Configure GE 1/0/1 and GE 1/0/2 on Switch B to allow packets of all VLANs to pass in Trunk mode. Configure GE 1/0/1 and GE 1/0/2 on Switch C to allow packets of all VLANs to pass in Trunk mode. Configure GE 1/0/3 and GE 1/0/4 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 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan all
SwitchA(config-ge-1/0/1)#exit
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type trunk
SwitchA(config-ge-1/0/2)#port trunk allow-pass vlan all
SwitchA(config-ge-1/0/2)#exit
```

Configure Switch B.

```
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 all
SwitchB(config-ge-1/0/1)#exit
SwitchB(config)#interface ge 1/0/2
SwitchB(config-ge-1/0/2)#switchport mode trunk
SwitchB(config-ge-1/0/2)#port trunk allow-pass vlan all
SwitchB(config-ge-1/0/2)#exit
SwitchB(config)#interface ge 1/0/3
SwitchB(config-ge-1/0/3)#switchport access vlan 3
SwitchB(config-ge-1/0/3)#exit
SwitchB(config)#interface ge 1/0/4
SwitchB(config-ge-1/0/4)#switchport access vlan 4
SwitchB(config-ge-1/0/4)#exit
```

Configure Switch C.

```
SwitchC(config)#interface ge 1/0/1
SwitchC(config-ge-1/0/1)#port link-type trunk
SwitchC(config-ge-1/0/1)#port trunk allow-pass vlan all
SwitchC(config-ge-1/0/1)#exit
SwitchC(config)#interface ge 1/0/2
SwitchC(config-ge-1/0/2)#switchport mode trunk
SwitchC(config-ge-1/0/2)#port trunk allow-pass vlan all
SwitchC(config-ge-1/0/2)#exit
SwitchC(config)#interface ge 1/0/3
SwitchC(config-ge-1/0/3)#switchport access vlan 3
SwitchC(config-ge-1/0/3)#exit
SwitchC(config)#interface ge 1/0/4
SwitchC(config-ge-1/0/4)#switchport access vlan 4
SwitchC(config-ge-1/0/4)#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 1/0/1
SwitchA(config-ge-1/0/1)#stp enable
SwitchA(config-ge-1/0/1)#exit
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#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 1/0/1
SwitchB(config-ge-1/0/1)#stp enable
SwitchB(config-ge-1/0/1)#exit
SwitchB(config)#interface ge 1/0/2
SwitchB(config-ge-1/0/2)#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 1/0/1
SwitchC(config-ge-1/0/1)#stp enable
SwitchC(config-ge-1/0/1)#exit
SwitchC(config)#interface ge 1/0/2
SwitchC(config-ge-1/0/2)#stp enable
```

Step 4 Configure the internal path cost of GE 1/0/1 of spanning tree instance 3 to 500000 on Switch B.

```
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#stp instance 3 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-1/0/1	root	forward	--	same
0	ge-1/0/2	alternate	discarding	--	same
3	ge-1/0/1	root	forward	--	same
3	ge-1/0/2	alternate	discarding	--	same
4	ge-1/0/1	alternate	discarding	--	same
4	ge-1/0/2	root	forward	--	same

9.6 Loop detection

9.6.1 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.

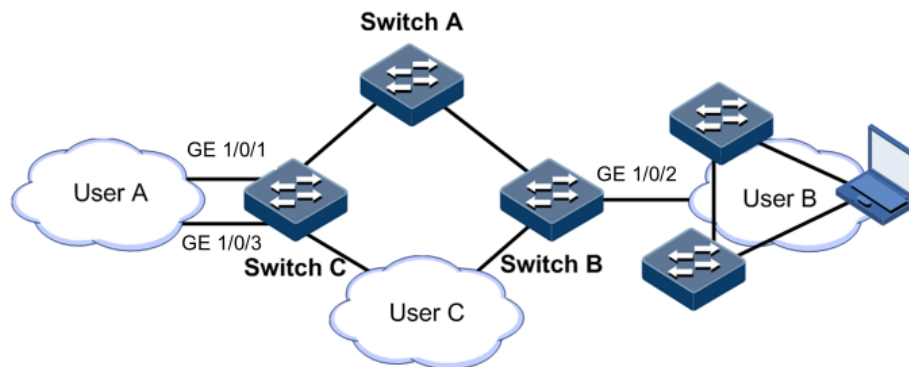
Loop types

Common loop types include self-loop and inner loop.

As shown in Figure 9-17, 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 1/0/2 on Switch B.
- Inner loop: a loop forming on different Ethernet interfaces of the same device. GE 1/0/1 and GE 1/0/3 on Switch C forms an inner loop with the user network A.

Figure 9-17 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 9-17, 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 1/0/2.
- 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 1/0/1.

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.

9.6.2 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.

9.6.3 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	30s
Mode for processing detected loops	Block
Loop detection period	5s
Loop detection mode	vlan mode

9.6.4 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-1/0/*)#loopback-detect mode vlan	Configure loop detection based on VLAN.
4	Raisecom(config-ge-1/0/*)#loopback-detect vlan <i>vlan-list</i>	Configure the VLAN for sending packets.
5	Raisecom(config-ge-1/0/*)#loopback-detect action <i>block</i>	Configure the action taken for loops.
6	Raisecom(config)#loopback-detect interval <i>interval</i>	Configure the interval for sending packets, in units of second.
7	Raisecom(config)#loopback-detect recovery-interval <i>interval</i>	Configure the interval for recovery, in units of second.

9.6.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show loopback-detect interface	Show configurations of loop detection on the interface.

9.6.6 Example for configuring inner loop detection

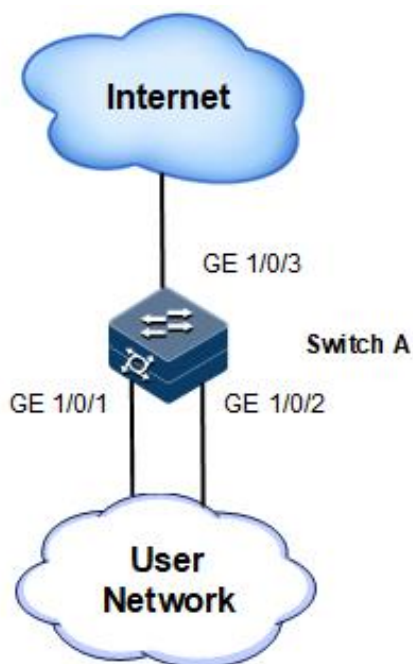
Networking requirements

As shown in Figure 9-18, GE 1/0/2 and GE 1/0/3 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 1/0/2 and GE 1/0/3.
- 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 9-18 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 1/0/1
Raisecom(config-ge-1/0/1)#port link-type hybrid
Raisecom(config-ge-1/0/1)#port hybrid vlan 3 untagged
Raisecom(config-ge-1/0/1)#exit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/1)#port link-type hybrid
Raisecom(config-ge-1/0/2)#port hybrid vlan 3 untagged
Raisecom(config-ge-1/0/2)#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 1/0/1
Raisecom(config-ge-1/0/1)#loopback-detect enable
Raisecom(config-ge-1/0/1)#loopback-detect action block
Raisecom(config-ge-1/0/1)#loopback-detect vlan 3
Raisecom(config-ge-1/0/1)#loopback-detect interval 3
```

```
Raisecom(config-ge-1/0/1)#exit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#loopback-detect enable
Raisecom(config-ge-1/0/2)#loopback-detect action block
Raisecom(config-ge-1/0/2)#loopback-detect vlan 3
Raisecom(config-ge-1/0/2)#loopback-detect interval 3
```

Checking results

Use the **show loopback-detection interface** command to show loop detection status.

```
Raisecom#show loopback-detect interface
```

Status	Interface	Enable	Action	Loop-

ge-1/0		/1	enable	block
none-loop				
ge-1/0/2	enable	block		none-loop

9.7 Interface backup

9.7.1 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.

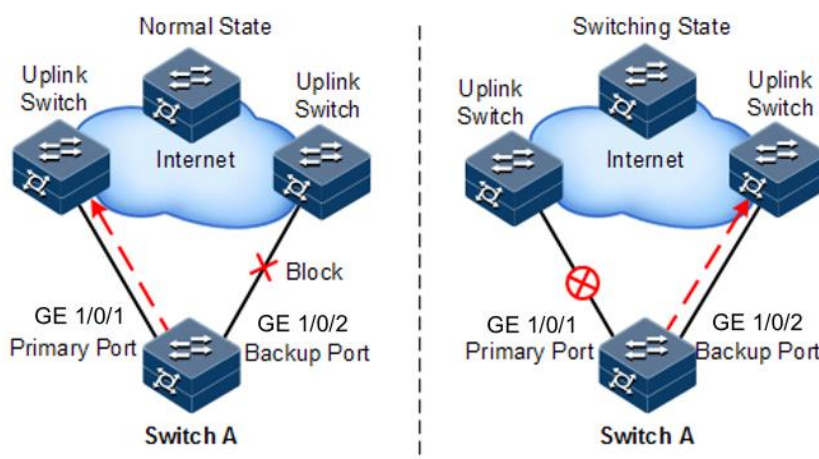
When the primary link fails, traffic is switched to the backup link. In this way, not only 50ms fast switching is ensured, but also configurations are simplified.

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 9-19 Principles of interface backup



As shown in Figure 9-19, GE 1/0/1 and GE 1/0/2 on Switch A are connected to their uplink devices respectively. The interface forwarding states are shown as below:

- Under normal conditions, GE 1/0/1 is the primary interface while GE 1/0/2 is the backup interface. GE 1/0/1 and the uplink device forward packet while GE 1/0/2 and the uplink device do not forward packets.
- When the link between GE 1/0/1 and its uplink device fails, the backup GE 1/0/2 and its uplink device forward packets.
- When GE 1/0/1 restores normally and keeps Up for a period (restore-delay), GE 1/0/1 restores to forward packets and GE 1/0/2 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 9-20.

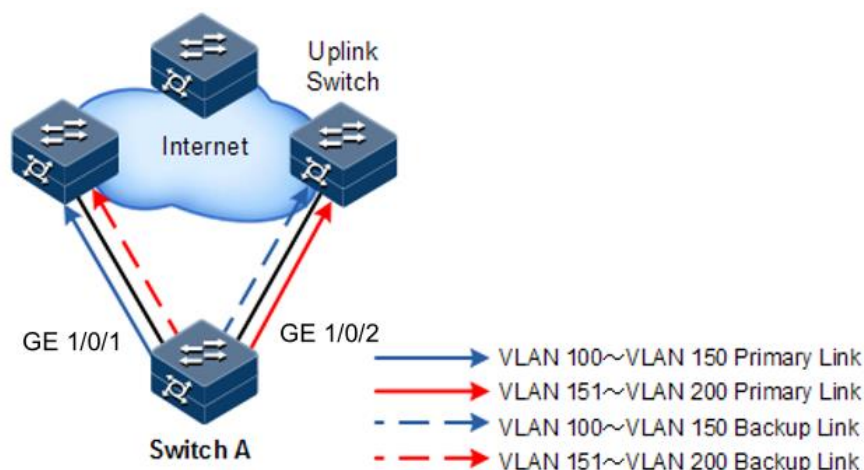


Figure 9-20 Networking with interface backup in different VLANs

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 1/0/1 is the primary interface and GE 1/0/2 is the backup interface.
- In VLANs 151–200, GE 1/0/2 is the primary interface and GE 1/0/1 is the backup interface.
- GE 1/0/1 forwards traffic of VLANs 100–150, and GE 1/0/2 forwards traffic of VLANs 151–200.
- When GE 1/0/1 fails, GE 1/0/2 forwards traffic of VLANs 100–200.
- When GE 1/0/1 restores normally and keeps Forward for a period (restore-delay), GE 1/0/1 forwards traffic of VLANs 100–150, and GE 1/0/2 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.

9.7.2 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

9.7.3 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

9.7.4 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 llbp	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.

9.7.5 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.

9.7.6 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.

9.7.7 Example for configuring interface backup

Networking requirements

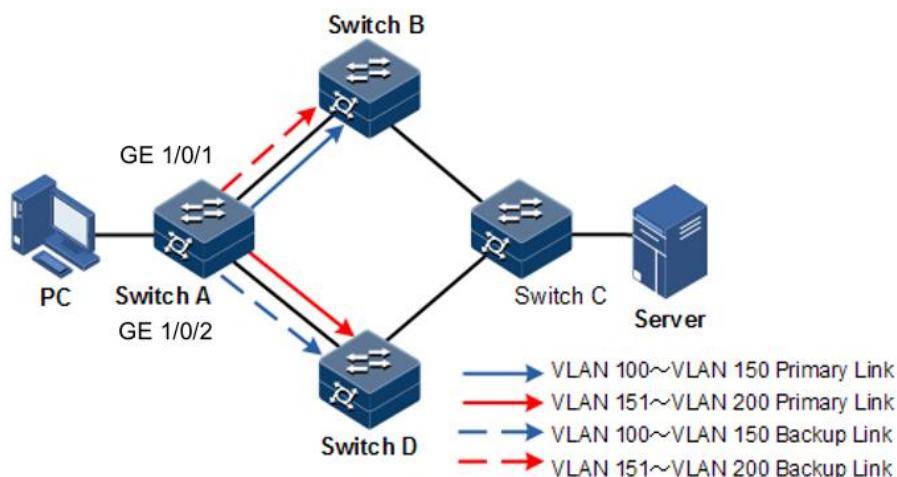
As shown in Figure 9-21, the PC accesses the server through the Switch. To implement a reliable remote access from the PC to the server, configure an interface backup group on Switch A and specify the VLAN list so that the two interfaces concurrently forward services in different VLANs and balance load. Configure Switch A as below:

- Add GE 1/0/1 to VLANs 100–150 as the primary interface and GE 1/0/2 as the backup interface.
- Add GE 1/0/2 to VLANs 151–200 as the primary interface and GE 1/0/1 as the backup interface.

When GE 1/0/1 or its link fails, the system switches traffic to the backup interface GE 1/0/2 to resume the link.

Switch A is required to support interface backup while other switches are not.

Figure 9-21 Interface backup networking



Configuration steps

Step 1 Create VLANs 100–400, and add GE 1/0/1 and GE 1/0/2 to these VLANs.

```
Raisecom#configure
Raisecom(config)#vlan 100-200
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 100-200
Raisecom(config-ge-1/0/1)#exit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port link-type trunk
Raisecom(config-ge-1/0/2)#port trunk allow-pass vlan 100-200
Raisecom(config-ge-1/0/2)#exit
```

Step 2 Configure GE 1/0/1 as the primary interface of VLANs 100–150 and GE 1/0/2 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 1/0/1 role master
Raisecom(config-protectlink-1)#add interface ge 1/0/2 role slave
```

Step 3 Configure GE 1/0/2 as the primary interface of VLANs 151–200 and GE 1/0/1 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 1/0/2 role master
```

```
Raisecom(config-protectlink-1)#add interface ge 1/0/1 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 1/0/1 and GE 1/0/2 are Forward, GE 1/0/1 forwards traffic of VLANs 100–150, and GE 1/0/2 forwards traffic of VLANs 151–200.

```
Raisecom#show protect-link interface
```

Interface	Group	Role	State	Status	Linkstate

ge-1/0/1	1	master	forward	active	up/up
ge-1/0/2	1	slave	block	active	up/up
ge-1/0/1	2	slave	block	active	up/up
ge-1/0/2	2	master	forward	active	up/up

Manually disconnect the link between Switch A and Switch B to emulate a fault. Then, GE 1/0/1 becomes Down, and GE 1/0/2 forwards traffic of VLANs 100–200.

```
Raisecom#show protect-link interface
```

Interface	Group	Role	State	Status	Linkstate

ge-1/0/1	1	master	block	active	up/down
ge-1/0/2	1	slave	forward	active	up/up
ge-1/0/1	2	slave	block	active	up/down
ge-1/0/2	2	master	forward	active	up/up

9.8 Interface isolation

9.8.1 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.

9.8.2 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

9.8.3 Default configurations of interface isolation

Default configurations of interface isolation are as below.

Function	Default value
Interface isolation status of each interface	Disable

9.8.4 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.

9.8.5 Checking configurations

Use the following commands to check configuration results.

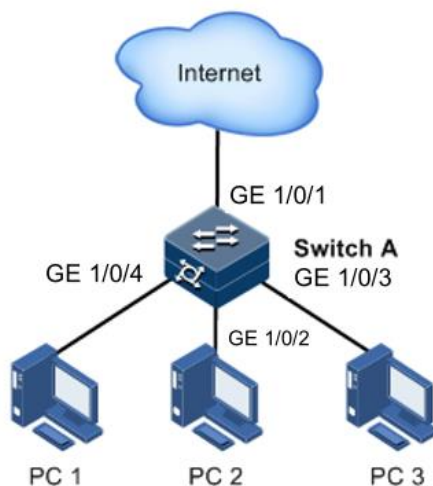
No.	Command	Description
1	Raisecom# show port-isolate information	Show configurations of interface isolation.
2	Raisecom# show port-isolate group	Show configurations of the interface isolation group.

9.8.6 Example for configuring interface isolation

Networking requirements

As shown in Figure 9-22, 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 1/0/4 and GE 1/0/2 on Switch A.

Figure 9-22 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 1/0/4
Raisecom(config-isolate-group-1)#add interface ge 1/0/2
```

Checking results

Use the **show port-isolate group** command to show configurations of interface isolation.

```
Raisecom#show port-isolate group
      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.

9.9 L2CP

9.9.1 Introduction

Metro Ethernet Forum (MEF) introduces the concept of services, including six types of services, such as EPL, EVPL, EP-LAN, and EVP-LAN. Each type of services processes Layer 2 Control Protocol (L2CP) packets differently.

MEF6.1 defines the processing methods for L2CP packets, which are:

- Discard: discard packets.
- Peer: submit packets to the CPU.
- Tunnel: transmit packets to the Metropolitan Area Network (MAN). The processing configuration is more complex than that of the discard and peer. The matching rules of the user network-side interface and the carrier-side interface tunnel terminal are used together to enable the packets to pass through the carrier network.

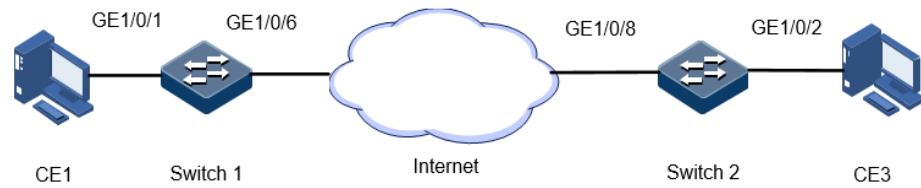
9.9.2 Preparing for configurations

Scenario

As shown below, switch 1 and switch 2 work as the carrier network access devices, and CE 1 and CE 3 work as the user network access devices. CE 1 and CE 3 are connected with GE 1/0/1 on switch 1 and GE 1/0/2 on switch 2 respectively.

Through transparent transmission of L2 protocol packets of different user networks, the devices on the user networks can jointly implement functions of the spanning tree.

Figure 9-23 BPDU Tunnel topology



Prerequisites

N/A

9.9.3 Default configurations

Default configurations of BPDU Tunnel are as below.

Function	Default value
L2CP	Disable

9.9.4 Configuring L2CP

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-1/0/1)#l2cp { uni nni disable }	Enable L2CP. • Uni: user-side interface • Nni: network-side interface • Disable: disable the interface role. By default, there is no role.
4	Raisecom(config-ge-1/0/1)#l2cp known-protocol { cdp eoam3ah gmrp gvrp hgmpp lacp lldp pagp stp udld vtp lamp eismc dot1x elmi pvst } [vlan vlan-id] action tunnel group-mac mac-address	Configure the swapping rule on the UNI. • known-protocol: matching protocol • mac-address: swapped multicast MAC address
5	Raisecom(config-ge-1/0/*)#l2cp protocol-mac dst-mac-address [vlan vlan-id] action tunnel group-mac mac-address	Configure the swapping rule on the UNI. • dst-mac-address: matching destination MAC address • mac-address: swapped multicast MAC address • vlan-id: matching the VLAN ID

Step	Command	Description
6	<code>Raisecom(config-ge-1/0/1)# l2cp known-protocol { cdp eoam3ah gmrp gvrp h gmp lacp lldp pagp stp udld vtp lamp e smc dot1x elmi pvst } action { peer discard }</code>	Configure the sending or discarding rule on the UNI. • known-protocol: matching protocol • peer: sending to the CPU • discard: discarding
7	<code>Raisecom(config-ge-1/0/1)# l2cp protocol-mac dst-mac- address action { peer di scard }</code>	Configure the sending or discarding rule on the UNI. • dst-mac-address: matching destination MAC address • peer: sending to the CPU • discard: discarding

9.9.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show l2cp</code>	Show global information about BPDU Tunnel.
2	<code>Raisecom#show l2cp config</code>	Show L2CP configurations.
3	<code>Raisecom#show protocol statistics rx with-value</code>	Show statistics on packets sent to the CPU by L2CP.

9.9.6 Example for configuring L2CP

Configuration steps

Step 1 Configure CE 1.

```
Raisecom(config)#stp enable
```

Step 2 Configure CE 3.

```
Raisecom(config)#stp enable
```

Step 3 Configure switch 1.

```
Raisecom(config-ge-1/0/1)#l2cp uni
```



```
Raisecom(config-ge-1/0/1)#12cp known-protocol stp action tunnel group-mac  
01:00:0c:cd:cd:d0  
Raisecom(config-ge-1/0/6)#12cp nni
```

Step 4 Configure switch 2.

```
Raisecom(config-ge-1/0/2)#12cp uni  
Raisecom(config-ge-1/0/2)#12cp known-protocol stp action tunnel group-mac  
01:00:0c:cd:cd:d0  
Raisecom(config-ge-1/0/8)#12cp nni
```

Checking results

On CE 1 and CE 3, you can see information about the peer spanning tree.

9.10 BFD

9.10.1 Introduction

Bidirectional Forwarding Detection (BFD) is a unified network-wide detection mechanism used to quickly detect and monitor the forwarding connectivity status of links or IP routers on a network.

9.10.2 Preparing for configurations

Scenario

BFD establishes a session on two network devices to detect bidirectional forwarding paths between network devices and serve upper-layer applications. BFD does not have a neighbor discovery mechanism, but relies on the upper layer application being served to notify its neighbor information to establish a session. After the session is established, it will periodically and quickly send BFD packets. If the BFD packet is not received within the detection time, it judges that the bidirectional forwarding path has failed, and the upper layer application being served is notified to take corresponding actions.

Prerequisite

N/A

9.10.3 Default configurations

Default configurations of BFD are as below.

Function	Default value
Global BFD	Disable

Function	Default value
Sending interval	1000ms
Receiving interval	1000ms
Local detection multiples	3

9.10.4 Configuring BFD static session detection

Configure BFD static session detection for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#bfd start	Enable global BFD.
3	Raisecom(config)#bfd track 1 remote-ip 10.0.0.2 local-ip 10.0.0.1 interface vlan 1	Configure the track to generate a BFD static session.
4	Raisecom(config)#bfd track 1 remote-ip6 2001::2 local-ip6 2001::1 interface vlan 1	Configure the track to generate an IPv6 BFD static session.

9.10.5 Configuring one-arm echo for BFD

Configure one-arm echo for BFD for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#bfd start	Enable global BFD.
3	Raisecom(config)#bfd track track-id remote-ip remote-ip local-ip local-ip interface vlan vlan-id one-arm-echo	Configure the BFD session of one-arm echo.
4	Raisecom(config)#bfd track 1 remote-ip6 remote-ip6 local-ip6 local-ip6 interface vlan vlan-id one-arm-echo	Configure session parameters.

9.10.6 Configuring BFD to detection layer 3 eth-trunk

Configure BFD to detection layer 3 eth-trunk for BFD for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#bfd start	Enable global BFD.
3	Raisecom(config)#bfd track 1 link-bundle remote-ip 10.0.0.2 local-ip 10.0.0.1 interface eth-trunk 1	Configure track to be bound with the LAG interface, and generate the main session and sub-session.
4	Raisecom(config)#bfd track 1 link-bundle remote-ip6 2001::2 local-ip 2001::1 interface eth-trunk 1	Configure track to be bound with the LAG interface, and generate the main session and sub-session.

9.10.7 Configuring parameters of the BFD session

Configure parameters of the BFD session for BFD for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#bfd start	Enable global BFD.
3	Raisecom(config)#bfd track 1 remote-ip 10.0.0.2 local-ip 10.0.0.1	Create a BFD session.
4	Raisecom(config)#bfd track 1 min-tx 1000 min-rx 1000 multiplier 3	Configure parameters of the BFD session.

9.10.8 Checking configurations

Use the following commands to check configuration results.

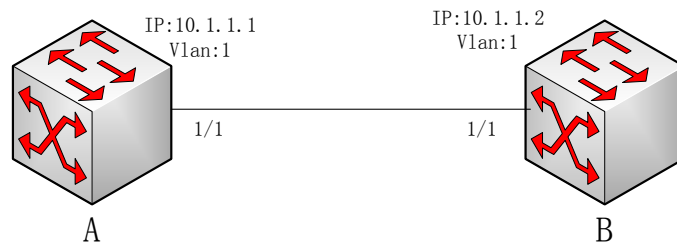
No.	Command	Description
1	Raisecom#show bfd session	Show the BFD session.
2	Raisecom#show bfd track	Show the BFD track.
3	Raisecom#show bfd link-bundle session	Show the BFD link-bundle session.

9.10.9 Example for configuring single-hop BFD

Networking requirements

As shown below, configure the BFD single-hop session to detect the link status between device A and device B.

Figure 9-24 Single-hop BFD networking



Configuration steps

Step 1 Configure the IP address and session parameters on device A.

```
Raisecom#configure
Raisecom(config)#interface vlan 1
Raisecom(config)#ip address 10.1.1.1/24
Raisecom(config)#bfd track 1 remote-ip 10.1.1.2 local-ip 10.1.1.1
interface vlan 1
Raisecom(config)#bfd track 1 min-tx 500 min-rx 600 multiplier 3
```

Step 2 Configure the IP address and session parameters on device B

```
Raisecom#configure
Raisecom(config)#interface vlan 1
Raisecom(config)#ip address 10.1.1.2/24
Raisecom(config)#bfd track 1 remote-ip 10.1.1.1 local-ip 10.1.1.2
interface vlan 1
Raisecom(config)#bfd track 1 min-tx 500 min-rx 600 multiplier 4
```

Checking results

Use the **show bfd session** command to show the session status.

```
Raisecom#show bfd session
  Interface      State Local-Discr Remote-Discr local-addr      remote-
addr
-----
vlan-1          up    1           1           10.1.1.1         10.1.1.2
-----
```

9.11 Link flap protection

9.11.1 Introduction

Link flap protection is a function which shuts down the interface frequently being UP and Down, makes the interface Down, and prevents network topology from changing rapidly.

9.11.2 Preparing for configurations

Scenario

Network jitter or link line failures can cause frequent up/down changes in the physical status of local device interfaces, leading to link flaps and frequent changes in network topology, which can affect user communication. To solve the above problems, you can configure link flap protection by shutting down interfaces with frequent up/down physical status, making them in a down status, and stopping frequent changes in the network topology structure.

Link flap times: the interface status switches between up and down once, which is recorded as one flap.

Interval for detecting link flaps: the system needs to count the number of link flaps within a specified interval.

If the number of link flaps reaches the threshold during the interval for detecting link flaps, the interface will be shut down.

Prerequisites

N/A

9.11.3 Default configurations of link flap protection

Default configurations of link flap protection are as below.

Function	Default value
Link flap protection status	Disable
Interval for detecting link flaps	10s
Link flap times	5

9.11.4 Configuring link flap protection

Configure link flap 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.

Step	Command	Description
3	Raisecom(config-ge-1/0/*)#port link-flap protection { enable disable }	Enable or disable link flap protection.
4	Raisecom(config)#port link-flap interval { 60 default }	Configure the interval for detecting link flaps.
5	Raisecom(config)#port link-flap threshold { 7 default }	Configure the link flap threshold.

9.11.5 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom#show link-flap config	Show configurations of link flap protection.
2	Raisecom#show link-flap interface	Show information about interfaces of link flap protection.

9.11.6 Example for configuring link flap protection

Configuration steps

Configure related parameters of link flap protection on device A.

```
Raisecom#configure
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port link-flap protection enable
Raisecom(config-ge-1/0/1)#port link-flap interval 60
Raisecom(config-ge-1/0/1)#port link-flap threshold 7
```

Checking results

Use the **show link-flap interface** command to show configurations of link flap protection.

```
Raisecom#show link-flap interface
Error-down recovery interval : 0
Interface      Status      Interval    Threshold
-----
ge-1/0/1      enable      60          7
-----
```

9.12 Interface loopback

9.12.1 Introduction

Before the network fails or a device provides services, the connectivity and network quality between the device and other devices can be detected through the interface loopback command on the device.

9.12.2 Preparing for configurations

Scenario

Before the device provides services, to ensure the connectivity of the link, you can configure interface loopback on the device. Test packets can be sent from the testing instrument to the testing interface on the device, and the device swaps the source MAC address and destination MAC in the test packets, loop back the test packets from the interface to the testing instrument, and then obtain network connectivity and network quality information between the device and the testing device.

Prerequisite

N/A

9.12.3 Default configurations of interface loopback

Default configurations of interface loopback are as below.

Function	Default value
Interface loopback	Disable
Interface loopback period	N/A

9.12.4 Configuring interface loopback

Configure interface loopback 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/*)# loopback-mode { none remote } [interval <i>interval</i>]	Configure the interface loopback mode and test duration.

9.12.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show interface loop-status	Show configurations and the status of interface loopback.

9.12.6 Example for configuring interface loopback

Configuration steps

Configure interface loopback.

```
Raisecom#configure
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#loopback-mode remote
```

Checking results

Use the **show interface loop-status** command to show information about interface loopback.

```
Raisecom(config-ge-1/0/1)#show interface loop-status
Interface           Mode           HoldTime(min)
-----
ge-1/0/1             remote         forever
ge-1/0/2             none           forever
ge-1/0/3             none           forever
ge-1/0/4             none           forever
ge-1/0/5             none           forever
ge-1/0/6             none           forever
ge-1/0/7             none           forever
ge-1/0/8             none           forever
ge-1/0/9             none           forever
ge-1/0/10            none           forever
ge-1/0/11            none           forever
ge-1/0/12            none           forever
-----
```


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
- ISF
- MAD
- NQA
- POE
- Patching
- Periodically backing up configurations

10.1 SNMP

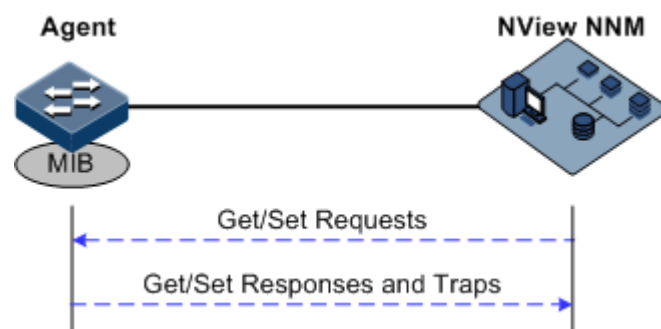
10.1.1 Introduction

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
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 stop }	Start SNMP Server.
3	Raisecom(config)#snmp mib-view view-name { included excluded } oid-tree { mask subtree-mask }	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.

Step	Command	Description
4	<code>Raisecom(config)#snmp community { read write } { cipher plain } community- name { mib-view view-name acl-ipv4 acl-ipv4-number acl-ipv6 acl-ipv6-number }</code>	Create a community name, and configure the corresponding view and authority. Use default view internet if mib view view-name option is empty.

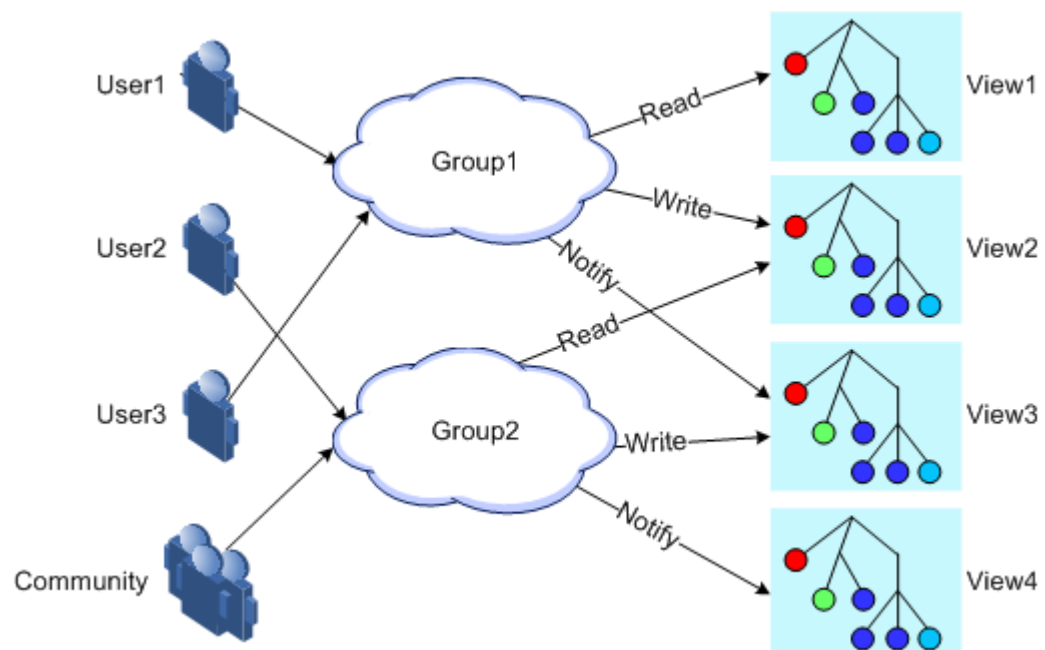
10.1.5 Configuring basic functions of SNMPv3

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	<code>Raisecom#configure</code>	Enter global configuration mode.

Step	Command	Description
2	<code>Raisecom(config)#snmp mib-view view-name { included excluded } oid-tree { mask subtree-mask }</code>	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	<code>Raisecom(config)#snmp group group-name { authentication privacy noauthentication } { read-view read-view-name write-view write-view-name notify-view notify-view-name }</code>	Configure the access group.
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.

Step	Command	Description
7	Raisecom(config)#snmp reauth-interval <i>reauth-interval-value</i>	Configure the SNMP re-authentication time.
8	Raisecom(config)#snmp packet max-size { <i>size-value</i> default }	Configure the maximum length of received and sent SNMP packets.
9	Raisecom(config)#snmp reply-source-ip { enable disable }	Configure the IP address to be input as the source IP address of the response packet.
10	Raisecom(config)#snmp udp-port { <i>port-number</i> default }	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</i> { v1 v2 } [port <i>port-id</i> securityname <i>security-name</i> vpn-instance <i>vpn-name</i>]*	Configure the SNMPv1 or SNMPv2c Trap target host (IPv4).
4	Raisecom(config)#snmp-ipv6 trap-host <i>ipv6-address</i> { v1 v2 } [port <i>port-id</i> securityname <i>security-name</i> vpn-instance <i>vpn-name</i>]*	Configure the SNMPv1 or SNMPv2c Trap target host (IPv6).
5	Raisecom(config)#snmp trap-host <i>ip-address</i> v3 { authentication privacy } securityname <i>security-name</i> [port <i>port-id</i> vpn-instance <i>vpn-name</i>]	Configure the SNMPv3 Trap target host (IPv4).

Step	Command	Description
6	Raisecom(config)#snmp-ipv6 trap-host <i>ipv6-address</i> v3 { authentication privacy } securityname <i>security-name</i> [port <i>port-id</i> vpn-instance <i>vpn-name</i>]*	Configure the SNMPv3 Trap target host (IPv6).

10.1.8 Checking configurations

Use the following commands to check configuration results.

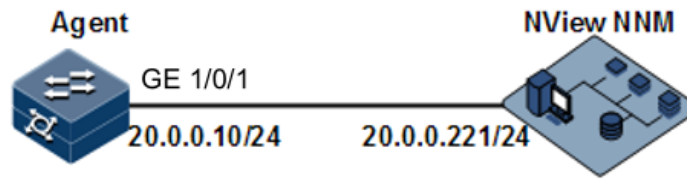
No.	Command	Description
1	Raisecom#show snmp information	Show SNMP basic configurations, including the local SNMP engine ID, logo and contact method of the administrator, physical location of the device, Trap status, SNMP service status, and SNMP service port number.
2	Raisecom#show snmp group	Show configurations of the SNMP access group.
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
-----
-----
```

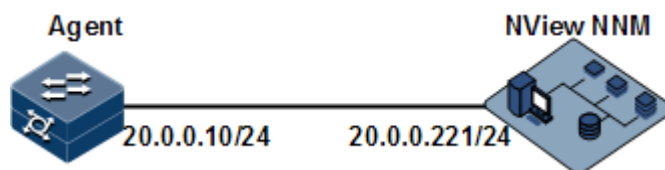
10.1.10 Example for configuring SNMPv3 and Trap

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
!
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
ACS87nMCx4RbzvVP51o3zDtbzu5xyzSZaDGMH0uqsc0
Software Version:  SNMP_VL3.00.00.00
```

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.

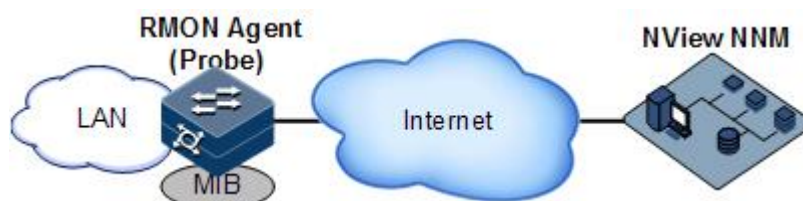
The RMON Agent is commonly referred to as the probe program. The RMON Probe can take the communication subnet statistics and performance analysis. Whenever it finds network failure, RMON Probe can report the NView NNM system, and describes the capture information under unusual circumstances so that the 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 index-number bucket buckets- number interval sampling-interval [owner owner-name]	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.

Step	Command	Description
2	<code>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> }</code>	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	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#rmon event <i>event-id</i> { log trap both } { description <i>string</i> owner <i>owner-name</i> }</code>	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	<code>Raisecom#show rmon config</code>	Show RMON configurations.
2	<code>Raisecom#show rmon alarm</code>	Show information about RMON alarm groups.
3	<code>Raisecom#show rmon event</code>	Show information about RMON event groups.
4	<code>Raisecom#show rmon statistics</code>	Show information about RMON statistics groups.
5	<code>Raisecom#show rmon history</code>	Show information about RMON history statistics groups.
6	<code>Raisecom#show rmon history <i>index-number</i></code>	Show information about the specified RMON history statistics group.
7	<code>Raisecom#show rmon history statistics</code>	Show statistics on the specified RMON history statistics group.
8	<code>Raisecom#show rmon log</code>	Show log information about the RMON event group.

10.2.9 Maintenance

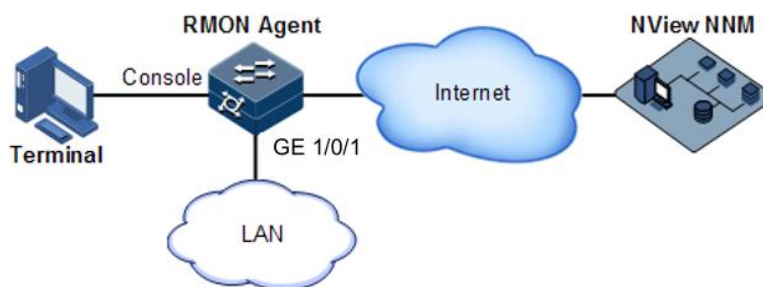
N/A

10.2.10 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.

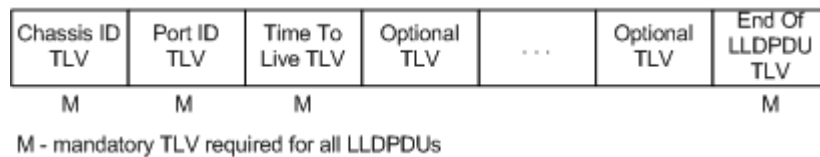
LLDP packet

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



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

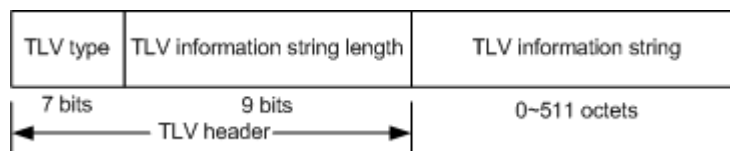


Table 10-1 lists TLV types. At present only types 0-8 are used.

Table 10-1 TLV types

TLV type	Description	Optional/Required
0	End Of LLDPDU	Required

TLV type	Description	Optional/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 0 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
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

Function	Default value
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.
3	Raisecom(config-ge-1/0/*)#lldp admin-status { tx-only rx-only rx-tx disable } Example: Raisecom(config-ge-1/0/*)#lldp admin-status tx-only	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	Raisecom(config)#lldp tx-interval { interval default } Example: Raisecom(config)#lldp tx-interval 10	(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)#lldp tx-delay { tx-delay default } Example: Raisecom(config)#lldp tx-delay 5	(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	Raisecom(config)#lldp reinit-delay { delay default } Example: Raisecom(config)#lldp reinit-delay 5	(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	Raisecom(config)#lldp tx-hold { multiple default } Example: Raisecom(config)#lldp tx-hold 2	(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.

Step	Command	Description
2	Raisecom(config)# interface <i>interface-type interface-number</i> Example: Raisecom(config)# interface ge 1/0/1	Enter physical interface configuration mode.
3	Raisecom(config-ge-1/0/*)# lldp management-address <i>ip-address</i> { 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 trap- 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
3	Raisecom(config)# interface <i>interface-type interface-number</i> Example: Raisecom(config)# interface ge - 1/0/1	Enter physical interface configuration mode.
4	Raisecom(config-ge-1/0/1)# lldp trap { enable disable }	Enable LLDP Trap.

10.3.9 Configuring TLV

Configure TLV for the device as below.

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

Step	Command	Description
3	<code>Raisecom(config-ge-1/0/*)#lldp basic-tlv-tx { port-description system-name system-description system-capability all } { enable disable }</code>	(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	<code>Raisecom(config-ge-1/0/*)#lldp dot1-tlv-tx port-vid { enable disable }</code> <code>Raisecom(config-ge-1/0/1)#lldp dot1-tlv-tx protocol-vid <i>vlan-list</i> { enable disable }</code> <code>Raisecom(config-ge-1/0/*)#lldp dot1-tlv-tx vlan-name <i>vlan-list</i> { enable disable }</code>	(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	<code>Raisecom(config-ge-1/0/*)#lldp dot3-tlv-tx { mac-phy power link-aggregation max-frame-size all } { enable disable }</code>	(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	<code>Raisecom(config-ge-1/0/1)#lldp med-tlv-tx { capabilities network-policy location extended-pse extended-pd inventory all } { enable disable }</code>	(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
7	<code>Raisecom(config-ge-1/0/1)#lldp voice-vlan { untagged vlan <i>vlan-id</i> [cos { <i>cos-value</i> default } dscp { <i>dscp-value</i> default }] }</code>	(Optional) configure the voice VLAN encapsulated by the network-policy TLV on the interface. • Untagged: remove the VLAN ID tag when the terminal sends voice traffic. • Vlan-id: voice VLAN ID • Cos-value: CoS priority, being 5 by default • Dscp-value: DSCP priority, being 6 by default

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 information	Show information about the LLDP local system.
3	Raisecom# show lldp remote [<i>interface-type interface-number</i>]	Show information about the LLDP neighbor.
4	Raisecom# show lldp statistics	Show statistics about LLDP.
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.

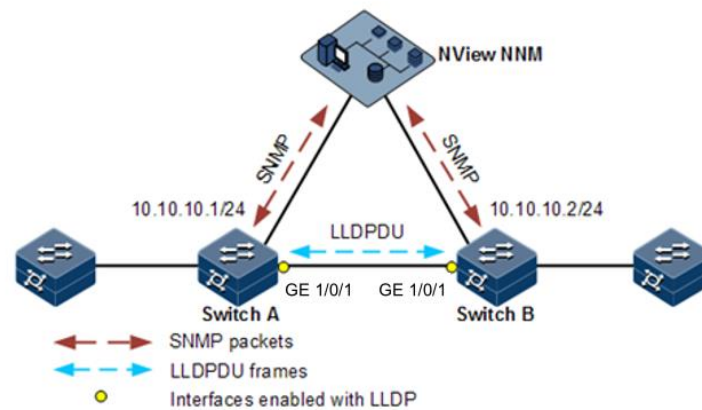
Command	Description
Raisecom(config-ge-1/0/*)# lldp port statistics counter	Clear LLDP statistics on the interface.

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 ge 1/0/1
SwitchA(config-ge-1/0/1)#port hybrid vlan 10 tagged
SwitchA(config-ge-1/0/1)#port hybrid pvid 10
SwitchA(config-ge-1/0/1)#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 ge 1/0/1
SwitchB (config-ge-1/0/1)#port hybrid vlan 10 tagged
SwitchB (config-ge-1/0/1)#port hybrid pvid 10
SwitchB (config-ge-1/0/1)#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 config
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

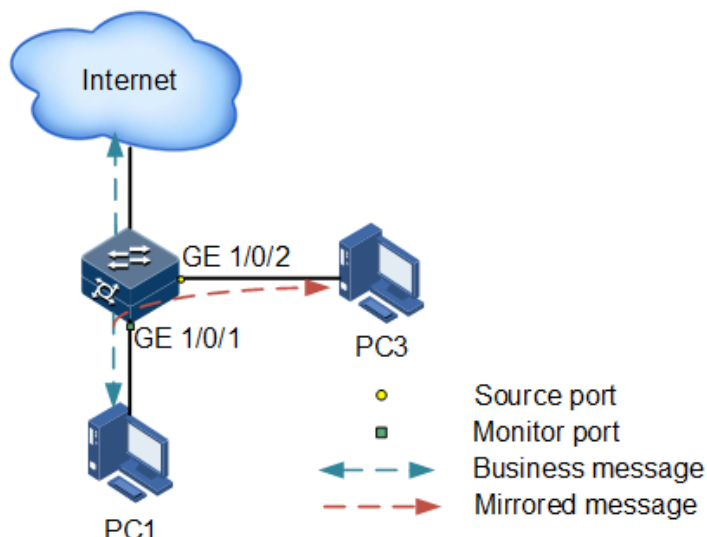


Figure 10-10 shows principles of port mirroring. PC 1 is connected to the external network by the GE 1/0/1; PC 3 is the monitor PC, connecting the external network by GE 1/0/2.

When monitoring packets from the PC 1, you need to assign GE 1/0/1 to connect to PC 1 as the mirror source port, enable port mirroring on the ingress port and assign GE 1/0/2 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 1/0/2). 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 interface-type interface-number { rspan vlan-id 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 interface-type interface-number	Enter physical interface configuration mode.
4	Raisecom(config-ge-1/0/1)#mirror { inbound outbound both } group group-number	Configure the port mirroring rule. • { inband outband both } : ingress, egress, or both directions of the mirroring • Group-number: mirroring group ID, ranging from 1 to 4

10.4.5 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.

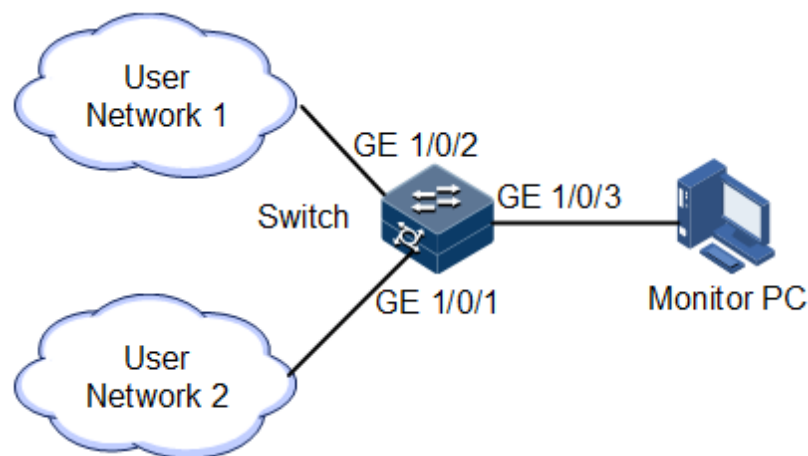
10.4.6 Example for configuring port mirroring

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 1/0/1, user network 2 accesses the device through GE 1/0/2, and the data monitor device is connected to GE 1/0/3.

Figure 10-11 Port mirroring networking



Configuration steps

Enable port mirroring on the Switch.

```
Raisecom#configure
Raisecom(config)#mirror group 1 interface ge 1/0/3
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#mirror ingress group 1
```

Checking results

Use the **show mirror** command to show configurations of port mirroring.

```
Raisecom#show mirror group
```

```
mirror-----
---
1          ge-1/0/3      n/a
-----
```

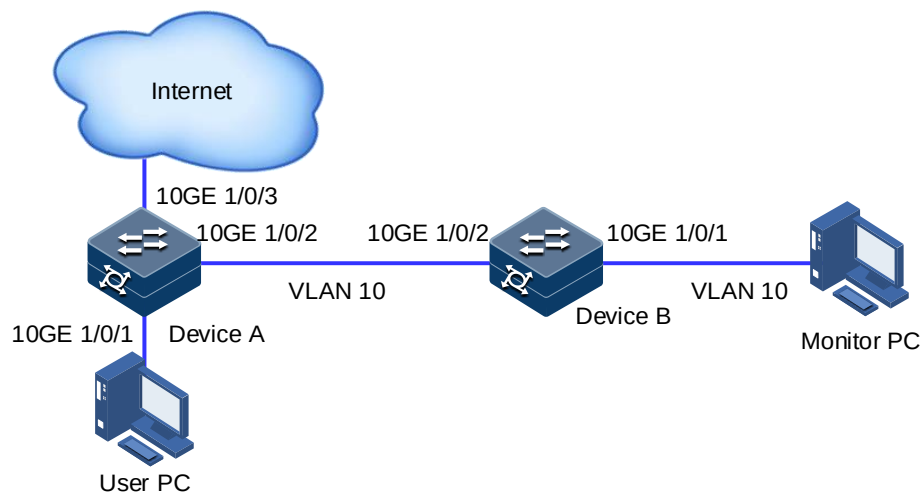

10.4.7 Example for configuring remote port mirroring

Networking requirements

As shown in Figure 10-12, the network administrator wants to monitor the user PC through the remote 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. The user PC accesses switch A through GE 1/0/1, and the data monitor device is connected to GE 1/0/1 on switch B.

Figure 10-12 Remote port mirroring networking



Configuration steps

Step 1 Enable port mirroring on switch A.

```
Raisecom#configure
Raisecom(config)#mirror group 1 ge 1/0/2 rspan 10 tpid 0x8100
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#mirror inbound group 1
```

Step 2 Configure VLAN forwarding on switch B.

```
Raisecom#configure
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#port trunk allow-pass vlan 10
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#port trunk allow-pass vlan 10
```

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	<code>Raisecom(config)#virtual-cable-test force-detect</code>	Enable global cable diagnosis. This command conducts cable diagnosis on all supportive interfaces.
2	<code>Raisecom(config-ge-1/0/*)#virtual-cable-test</code>	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(config)#show virtual-cable-test config	Show configurations of cable diagnosis.
2	Raisecom(config)#show virtual-cable-test	Show results of cable diagnosis on all interfaces.
3	Raisecom(config)#show virtual-cable-test interface <i>interface-type primary-interface-number</i>	Show results of cable diagnosis on the specified interface.
4	Raisecom(config)#show virtual-cable-test link-down	Show results of cable diagnosis on all Down interfaces.

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 (DLD PDU) 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 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.
12	Raisecom(config-ge-1/0/*)#udld rx-mode { normal rxloss }	Configure whether to perform the error-down or Up action by focusing the RXLOS and other messages of the optical module.
13	Raisecom(config-ge-1/0/*)#udld up-delay time	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	Raisecom#show udld config	Show UDLD configurations.
2	Raisecom#show udld interface	Show the protocol status of all interface enabled with UDLD.
3	Raisecom#show udld local	Show local information about UDLD.
4	Raisecom#show udld peer	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 config</code>	Show configurations of the current optical module.
2	<code>Raisecom#show transceiver interface</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 interface-type <i>primary-interface-number</i></code>	Show configurations of the current optical module on the specified interface.
4	<code>Raisecom#show transceiver interface-type <i>primary-interface-number</i> [threshold]</code>	Show the threshold of the optical module on the specified interface.

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 { start stop }	Enable system logs.
3	Raisecom(config)#logging file max-number { max-num default }	Configure the maximum number of log files of the system logs.
4	Raisecom(config)#logging file size kbytes { size-value default }	Configure the size of the system logs.
5	Raisecom(config)#logging origin-id STRING	Configure the origin ID of the system log.

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.

Step	Command	Description
2	<code>Raisecom(config)#logging module <i>module-name</i> action { console monitor logfile buffer trap trapbuffer syslog smtp } { log debug trap } [state { enable disable default } level { emergencies alert critical error warning notification information debugging default }]</code>	Configure the output direction of module logs, output enabling status, and output level.

10.8.6 Configuring system log output to Telnet/SSH terminals

Configure system log output to Telnet/SSH terminals for the device as below.

Step	Command	Description
1	<code>Raisecom#terminal monitor</code> <code>Raisecom#no terminal monitor</code>	Enable or disable information output to Telnet/SSH terminals.
2	<code>Raisecom#terminal log</code> <code>Raisecom#no terminal log</code>	Enable or disable log output to Telnet/SSH terminals. By default, it is enabled.
3	<code>Raisecom#terminal trap</code> <code>Raisecom#no terminal trap</code>	Enable or disable Trap output to Telnet/SSH terminals. By default, it is enabled.
4	<code>Raisecom#terminal debug</code> <code>Raisecom#no terminal debug</code>	Enable or disable debugging information output to Telnet/SSH terminals. By default, it is disabled.

10.8.7 Configuring system log output to the syslog server

Configure system log output to the syslog server for the device as below.

Step	Command	Description
1	<code>Raisecom(config)#syslog server <i>ip-address</i> [port <i>port-num</i> facility { kernel user mail system-daemons security-authorization1 syslogd line-printer network-news uucp clock-daemon security-authorization2 ftp ntp log-audit log-alert note2 local0 local1 local2 local3 local4 local5 local6 local7 default }]*</code> <code>Raisecom(config)#</code>	Configure the sent log to contain the destination IP address, destination port number, and facility of the IPv4 syslog server.

Step	Command	Description
2	Raisecom(config)# syslog-ipv6 server <i>ipv6-address</i> [port <i>port-num</i> facility { kernel user mail system-daemons security- authorization1 syslogd line- printer network-news uucp clock- daemon security-authorization2 ftp ntp log-audit log-alert note2 local0 local1 local2 local3 local4 local5 local6 local7 default }]* Raisecom(config)#	Configure the sent log to contain the destination IP address, destination port number, and facility of the IPv6 syslog server.
3	Raisecom# show syslog server	Check configurations of the syslog server.

10.8.8 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.

No.	Command	Description
11	Raisecom#show logging event	Show event information for all module logs.
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.

10.8.9 Maintenance

Maintain the device as below.

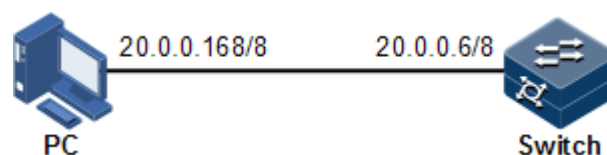
Command	Description
Raisecom(config)#clear logging { buffer trap }	Clear log information in the log or trap buffer.
Raisecom(config)#clear logging statistics	Clear log statistics.
Raisecom(config)#clear logging file all	Clear all log files.
Raisecom(config)#clear logging module <i>module-name</i>	Clear log statistics of the specified module.

10.8.10 Example for configuring outputting system logs to the log host

Networking requirements

As shown in Figure 10-13, configure the system log, and output device log information to the log host for users to check.

Figure 10-13 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
```

Step 3 Configure the debugging information to be output to the terminal.

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

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 Introduction

An alarm refers to the information that the system can produce according to different fault types and different alarm sources when the device fails or some working status changes.

The alarm is used to report some urgent and important events, notify network administrators in time, and provide strong support for monitoring device operation and fault diagnosis.

The alarm is stored in the alarm buffer of the device, and its log is generated at the same time. If the NMS is configured, the alarm is sent to it through SNMP. The information sent to the NMS is called Trap.

10.9.2 Preparing for configurations

Scenario

When the device fails, alarm management module will collect fault information and output alarm occurrence time, alarm name and description information in log format to help users locate problem quickly.

If the device is configured with the NMS, alarm can be reported directly to the NMS, providing possible alarm causes and treatment recommendations to help users deal with fault.

If the device is configured with hardware monitoring, it will record the hardware monitoring alarm table, generated Syslog, and sent Trap when the operation environment of the device becomes abnormal, and notify the user of taking actions accordingly and prevent faults.

Alarm management facilitates alarm suppression, alarm auto-reporting, alarm monitoring, alarm reverse, alarm delay, alarm memory mode, alarm clear and alarm view directly on the device.

Prerequisite

Hardware environment monitoring alarm output:

- 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.

10.9.3 Configuring basic functions of alarm management

N/A

10.9.4 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).

No.	Command	Description
4	Raisecom#show alarm { active history all } [object <i>object-name</i>]	Show information about the specified alarm (active alarm, history alarm, and all alarms).
6	Raisecom#show alarm object	Show information about the alarm object.
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 <i>object-name</i>]	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 the occupied time and unitization of the CPU in each period (5s, 1min, 10min, and 2h) in a static mode or dynamic mode (total CPU utilization in each period).

It can be used to view the operational status of all tasks and detailed operational status of the specified task.

It can be used to show the history CPU utilization in each period.

It can be used to show 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, 1min, and 10min) 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 high-threshold-value	Configure the rising threshold of all CPU entries or the specified CPU entry.
3	Raisecom(config)#cpu { all cpu-index } description description-string	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 interval-value	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 Introduction

Memory monitoring can monitor the memory utilization of the system in real time, provide memory utilization threshold alarms, facilitate troubleshooting, and help network administrators locate faults.

10.11.2 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.

10.11.3 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 <i>memory-index</i> } high-threshold <i>high-threshold-value</i>	Configure the memory monitoring alarm threshold of all memory entries or the specified memory entry.
3	Raisecom(config)#memory { all <i>memory-index</i> } description <i>description-string</i>	Configure the description of all memory entries or the specified memory entry.
4	Raisecom(config)#memory { all <i>memory-index</i> } snmp-trap { disable enable }	Enable or disable Trap sending for all memory entries or the specified memory entry.
5	Raisecom(config)#memory monitor interval <i>interval-value</i>	Configure the interval for sampling memory utilization.
6	Raisecom(config)#memory monitor { disable enable }	Enable or disable memory utilization monitoring.

10.11.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	<code>Raisecom#show memory</code>	Show memory utilization.
2	<code>Raisecom#show memory verbose</code>	Show detailed memory utilization.
3	<code>Raisecom#show memory task</code>	Show memory utilization of each process.

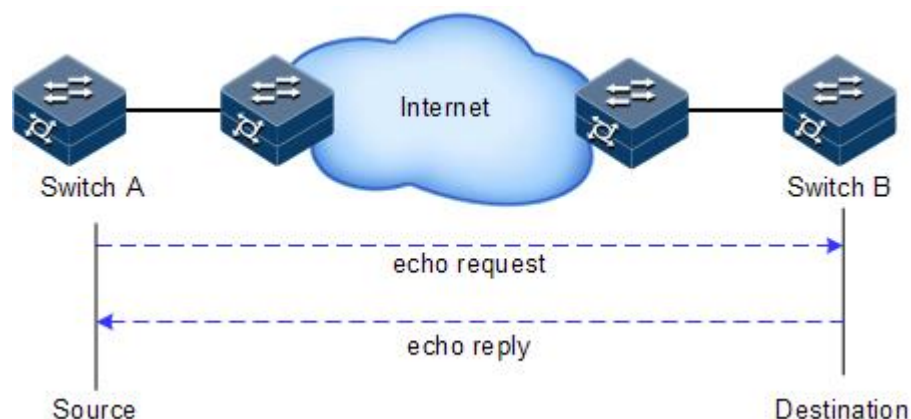
10.12 PING

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 10-14 shows principles of PING.

Figure 10-14 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:

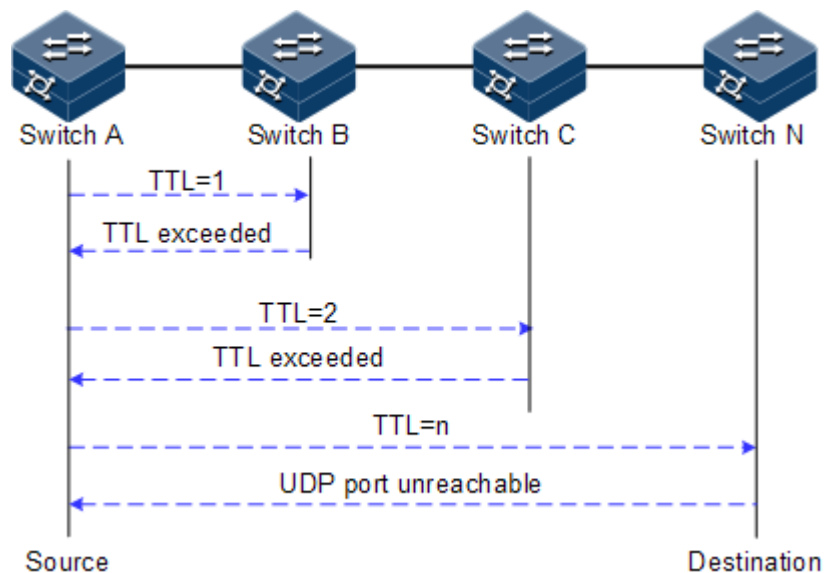
- Step 1 Send a piece of TTL1 sniffer packet (where the UDP port number of the packet is unavailable to any application programs in destination side).
- Step 2 TTL deducts 1 when reaching the first hop. Because the TTL value is 0, in the first hop the device returns an ICMP timeout packet, indicating 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 10-15 shows principles of traceroute.

Figure 10-15 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	<code>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]</code>	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	<code>Raisecom(config)#temperature { all <i>temperature-index</i> } low-threshold <i>low-threshold-value</i> high-threshold <i>high-threshold-value</i></code>	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	<code>Raisecom(config)#temperature { all <i>temperature-index</i> } snmp-trap { disable enable }</code>	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	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#power monitor { disable enable }</code>	Enable or disable power supply monitoring.
3	<code>Raisecom(config)#power monitor interval <i>interval-value</i></code>	Configure the period of power supply monitoring. By default, it is 25s.
4	<code>Raisecom(config)#power { all <i>power-index</i> } description <i>description-string</i></code>	Configure the description of all or specified power supply entry.
5	<code>Raisecom(config)#power { all <i>power-index</i> } snmp-trap { disable enable }</code>	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	<code>Raisecom#show temperature config</code>	Show configurations of temperature monitoring.
2	<code>Raisecom#show power config</code>	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	<code>Raisecom(config)#fan { all fan-index } description description- string</code>	Configure the description of all fans or specified fan.
6	<code>Raisecom(config)#fan { all fan-index } level level-value</code>	Configure the speed level of all fans or specified fan.
7	<code>Raisecom(config)#fan { all fan-index } snmp- trap { disable enable }</code>	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	<code>Raisecom#show fan</code>	Show information fan monitoring, including the current speed and speed level.
2	<code>Raisecom#show fan verbose</code>	Show basic information about the fan.
3	<code>Raisecom#show fan config</code>	Show configurations of fan monitoring.

10.16 ISF

10.16.1 Introduction

Intelligent Stacking Frame (ISF) refers to the combination of two or more switches that support stacking to logically form one switch. This virtualization technology can integrate the hardware resource capabilities and software processing capabilities of multiple devices, and implement collaborative work, unified management, and uninterrupted maintenance of multiple devices.

Basic concepts

- Operating modes

An ISF device supports two operating modes:

- Default mode: it cannot form an ISF with other devices.
- ISF mode: it can be configured with stacking and form an ISF device with other devices.

When the ISF device switches between these two modes, it will be restarted.

- Roles of member devices

Each ISF device in the ISF is a member device, which may be in different roles according to the negotiation result.

- Master: it manages and controls the entire ISF.
- Slave: it processes services and forwards packets; meanwhile it works as a backup for the master device. In other words, when the master device fails, the ISF will automatically elect a new master device from all slave devices to replace the original master device.

- Member device ID

The ISF uses the member device ID to identify and manage member devices. When configuring the ISF, you must ensure that the member device IDs are unique. If the member device IDs of two devices are the same, negotiation will fail, and establishing the ISF will fail.

- Member priority

The member priority is an attribute of a member device. By default, the member priority of the device is 1. In the process of stacking negotiation, the member priority will affect whether the member device can be elected as the master device. To make a device be elected as the master device of the ISF, you can configure the member priority to a greater value.

- ISF interface

An ISF interface is a logical interface specifically used for connecting stacked member devices. Each member device can be configured with two ISF interfaces, which need to be bound to the physical interface before they can take effect.

- ISF domain

The ISF domain is a logical concept. An ISF system corresponds with an ISF domain. Only member devices with the same ISF domain ID can establish an ISF. The member devices in different ISF domains cannot establish an ISF even if they can receive ISF packets from the peer device.

ISF topology

Two switches in this series support forming an ISF in the chain or ring topology.

Figure 10-16 Chain topology with 2 member devices

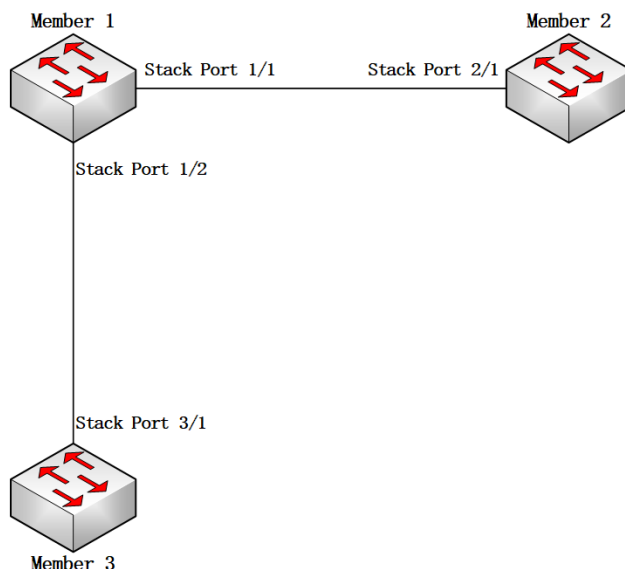
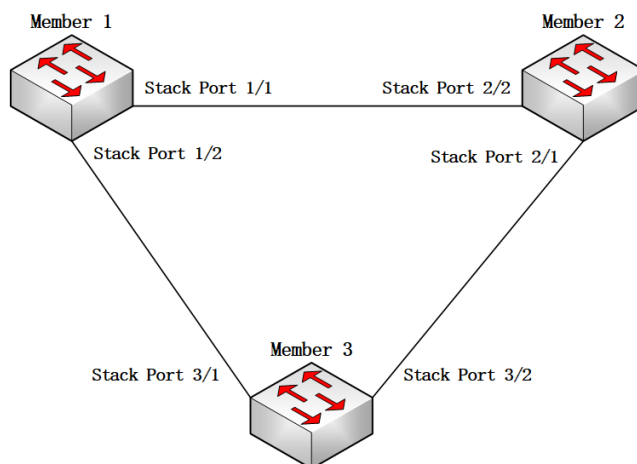


Figure 10-17 Ring topology with 2 member devices



Caution

- When member devices form a ring topology, the ISF interface IDs of adjacent stacked member devices are different. As shown in Figure 10-16, ISF interface 1/1 on ISF member device 1 is connected to ISF interface 2/2 on ISF member device 2. If two connected devices have the same ISF IDs, the ISF will fail to synchronize during switching between the master device and slave device.
- To configure the ISF, plan the ISF topology in the common mode, configure the corresponding ISF interfaces according to the ISF topology, and configure the ISF mode; otherwise, the devices fail to save configurations of ISF interfaces, and they fail to perform ISF negotiation due to no ISF interfaces after the devices are restarted.

Role election

Role election occurs when the ISF changes as below:

- The ISF is established.
- The ISF is split; in other words, the stacking link is disconnected.
- Two independent ISFs are merged.

Roles are elected in the following roles in descending order:

3. The current master device prevails. If two independent ISFs are merged, the new master device is elected between the master devices of these two independent ISFs.
4. The device that has been forcibly configured as the master device.
5. The device running for a long time (the device with the longest time prevails if multiple devices has been running for over 1min)
6. The device with a lowest bridge MAC address

The optimal device elected according to previous rules is the master device while other devices are slave devices.

10.16.2 Default configurations

Default configurations of ISF are as below.

Function	Default value
Stacking	Disable
ISF member priority	1
ISF member ID	1
ISF member domain ID	1
Interval for sending ISF packets by the ISF member	3s

10.16.3 Configuring ISF

Configure the ISF for the device as below.

Step	Command	Description
1	<code>Raisecom(config)#interface stack-port <i>number</i></code>	Create an ISF interface.
2	<code>Raisecom(config-stack-port-<i>number</i>)#add interface <i>interface-type interface-number</i></code>	Add a physical interface to the ISF interface.
3	<code>Raisecom(config)#hvs hello-interval { <i>hello-time</i> default }</code>	Configure the interval for sending ISF packets, in units of second.
4	<code>Raisecom(config)#hvs master</code>	Forcibly configure the ISF member as the master device in stacking negotiation.
5	<code>Raisecom(config)#hvs member-id <i>id</i></code>	Configure the ISF member ID.

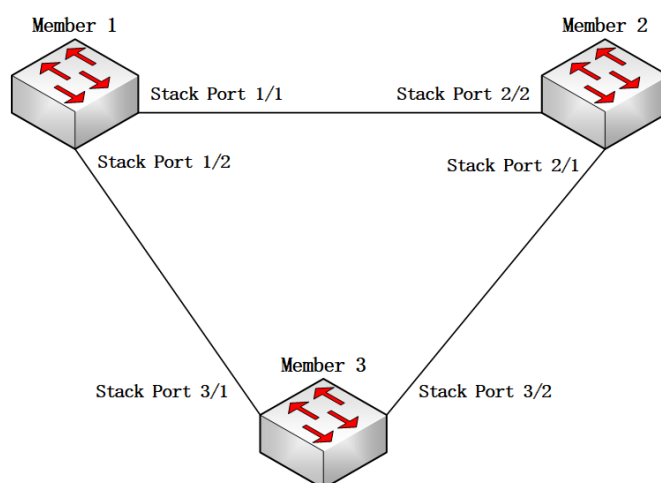
Step	Command	Description
6	<code>Raisecom(config)#hvs priority <i>value</i></code>	Configure the priority of the ISF member.
7	<code>Raisecom(config)#hvs switch-master member { <i>myself</i> <i>id</i> }</code>	Configure the ISF to switch between the master device and a slave device.
8	<code>Raisecom(config)#hvs mode { <i>normal</i> <i>stack</i> }</code>	Configure the ISF member device to switch its mode. Then, it will be automatically restarted.
9	<code>Raisecom(config)#show hvs member</code>	Show the members and roles in the current ISF.
10	<code>Raisecom(config)#show hvs topo</code>	Show topology information about the ISF.
11	<code>Raisecom(config)#show hvs interface</code>	Show information about ISF interfaces on the local device.
12	<code>Raisecom(config)#show hvs config</code>	Show stacking configurations of the local device.

10.16.4 Example for configuring ISF

Networking requirements

As shown below, to configure 2 devices to form an ISF in chain topology, configure them as below.

Figure 10-18 Chain topology with 2 devices for ISF



Configuration steps

Step 1 Configure member 1.

```
Raisecom(config)#interface stack-port 1
```

```
Raisecom(config-stack-port-1)#add interface ge 1/0/1
Raisecom(config-stack-port-1)#add interface ge 1/0/2
Raisecom(config-stack-port-1)#quit
Raisecom(config)#interface stack-port 2
Raisecom(config-stack-port-2)#add interface ge 1/0/3
Raisecom(config-stack-port-2)#quit
Raisecom(config)#hvs member-id 1
Raisecom(config)#hvs mode stack
```

Step 2 Configure member 2.

```
Raisecom(config)#interface stack-port 1
Raisecom(config-stack-port-1)#add interface ge 1/0/3
Raisecom(config-stack-port-1)#quit
Raisecom(config)#interface stack-port 2
Raisecom(config-stack-port-2)#add interface ge 1/0/1
Raisecom(config-stack-port-2)#add interface ge 1/0/2
Raisecom(config-stack-port-2)#quit
Raisecom(config)#hvs member-id 2
Raisecom(config)#hvs mode stack
```

Step 3 Configure member 3.

```
Raisecom(config)#interface stack-port 1
Raisecom(config-stack-port-1)#add interface ge 1/0/1
Raisecom(config-stack-port-1)#quit
Raisecom(config)#interface stack-port 2
Raisecom(config-stack-port-2)#add interface ge 1/0/2
Raisecom(config-stack-port-2)#quit
Raisecom(config)#hvs member-id 3
Raisecom(config)#hvs mode stack
```

Step 4 After 3 member devices are restarted, they start to negotiate. You can then check whether the ISF is established by the command.

Checking results

Use the **show hvs member** command on member 2 to check the result.

```
Raisecom(config)#show hvs member
```

SysId	Role/ConfRole	State/Pri	Mac	Port0	Port0Mac
Port1	Port1Mac	Uptime			
1	master/no	done/1	f0f1:f2f3:0101	up	f0f1:f2f3:0101
up	f0f1:f2f3:0101	05h:37m:34s			
2	slave/no	done/1	f0f1:f2f3:0201	up	f0f1:f2f3:0201
up	f0f1:f2f3:0201	05h:37m:34s			

```
* 3      slave/no      done/1      f0f1:f2f3:0301      up      f0f1:f2f3:0301
up      f0f1:f2f3:0301      05h:37m:34s
```

Use the **show hvs topo** command. The result is as below.

```
Raisecom(config)#show hvs topo
Interface: stack-port-3/1, State: up, MAC: f0:f1:f2:f3:03:01
Hop  SysId  Port0 State  MAC              Port1 State  MAC
0    3      1    up    f0:f1:f2:f3:03:01 2    up
f0:f1:f2:f3:03:01
1    1      1    up    f0:f1:f2:f3:01:01 2    up
f0:f1:f2:f3:01:01
2    2      1    up    f0:f1:f2:f3:02:01 2    up
f0:f1:f2:f3:02:01
Interface: stack-port-3/2, State: up, MAC: f0:f1:f2:f3:03:01
Hop  SysId  Port0 State  MAC              Port1 State  MAC
0    3      1    up    f0:f1:f2:f3:03:01 2    up
f0:f1:f2:f3:03:01
1    2      1    up    f0:f1:f2:f3:02:01 2    up
f0:f1:f2:f3:02:01
2    1      1    up    f0:f1:f2:f3:01:01 2    up
f0:f1:f2:f3:01:01
```

10.17 MAD

10.17.1 Introduction

When the link between member devices in an ISF is disconnected, this may cause the ISF to split into multiple new ISFs with the same Layer 3 configurations, such as the IP address. As a result, the IP addresses may conflict and the network may fail. The Multi-Active Detection (MAD) protocol is used for stacking splitting detection, conflict processing, and fault clearance to improve system availability.

There are several working modes for detecting conflicts in MAD.

- Direct connection mode

In direct connection mode, an additional physical interface needs to be allocated between the stacked member devices to be configured with MAD and to receive MAD packets. The topology can be established as shown in Figure 10-18.

- Proxy mode

In proxy mode, another device needs to be enabled with MAD. Establish a cross-device aggregation link between the device and the stacked member devices. Then, enable MAD on the aggregation interface to establish a topology, as shown in Figure 10-19.

- Out-of-band interface detection mode

In this mode, enable MAD on the out-of-band interface, and connect the out-of-band interface on all stacked member devices to the same switch, and ensure normal communication between all out-of-band interfaces.

Figure 10-19 Direction connection mode of MAD

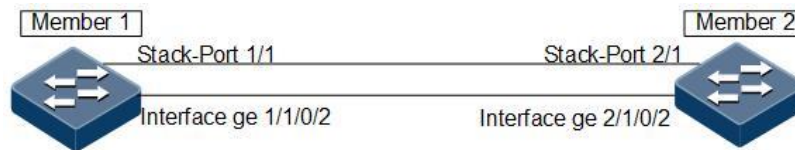
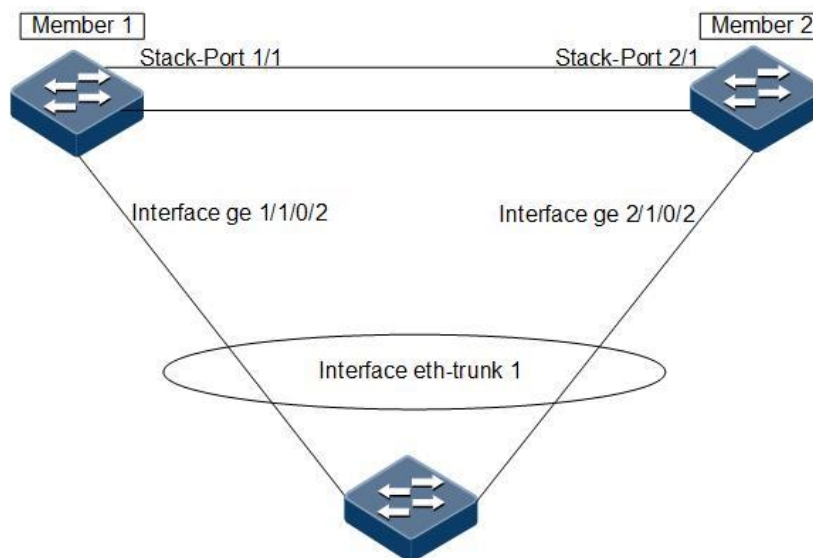


Figure 10-20 Proxy mode of MAD



10.17.2 Preparing for configurations

Scenario

- Backup management IP address

In addition to configuring the working mode of interfaces, MAD can also configure a backup IP address for each stack member. When MAD detects multiple devices, it automatically configures the backup IP address as the IP address of the out-of-band interface.

- Reserved interface

When MAD detects multiple devices, it compares them. If it finds that a device is not the preferred device, it will shut down device's own interface. If you do not want the interface to be shut down when MAD detects multiple hosts, you can configure the interface as a reserved interface.

Prerequisites

N/A

10.17.3 Configuring MAD

Configure MAC for the device as below.

Step	Command	Description
1	Raisecom(config)#multi-active-detect backup ip address <i>ip-address</i> member { all <i>member-id</i> }	Configure the backup management IPv4 address for the specified ISF member device.
2	Raisecom(config)#multi-active-detect backup ipv6 address <i>ipv6-address</i> member { all <i>member-id</i> }	Configure the backup management IPv6 address for the specified ISF member device.
3	Raisecom(config)#interface ge 1/0/0/* Raisecom(config-ge-1/1/0/*)#multi-active-detect mode direct	Configure the working mode of MAD on the interface.
4	Raisecom(config)#interface eth-trunk 1 Raisecom(config-eth-trunk-1)#multi-active-detect mode relay	Configure the working mode of MAD on the LAG interface.
5	Raisecom(config)#interface meth 0/0/0 Raisecom(config-meth-0/0/0)#multi-active-detect { disable enable } Raisecom(config)#interface ge 1/0/0/* Raisecom(config-ge-1/1/0/*)#multi-active-detect { disable enable }	Enable or disable MAD on the interface.
6	Raisecom(config-meth-0/0/0)#multi-active-exclude { disable enable }	Enable the reserved interface of MAD on the interface.
7	Raisecom(config)#show multi-active-detect config	Show MAD configurations on the current device.
8	Raisecom(config)#show multi-active-detect information	Show MAD information about the current device.

10.17.4 Example for configuring MAD

Networking requirements

Configure the ISF to make two devices form an ISF. Then, configure MAD.

Configuration steps

Step 1 Configure member 1.

```
Raisecom(config)#interface stack-port 1
Raisecom(config-stack-port-1)#add interface ge 1/0/1
Raisecom(config-stack-port-1)#quit
Raisecom(config)#hvs member-id 1
Raisecom(config)#hvs mode stack
```

Step 2 Configure member 2.

```
Raisecom(config)#interface stack-port 1
Raisecom(config-stack-port-1)#add interface ge 1/0/1
Raisecom(config-stack-port-1)#quit
Raisecom(config)#hvs member-id 2
Raisecom(config)#hvs mode stack
```

Step 3 After two member devices form an ISF, configure MAD.

```
Raisecom(config)#interface GE 1/0/0/2
Raisecom(config-ge-1/1/0/2)#stp disable
Raisecom(config-ge-1/1/0/2)#multi-active-detect mode direct
Raisecom(config-ge-1/1/0/2)#quit
Raisecom(config)#interface ge 2/1/0/2
Raisecom(config-ge-1/1/0/2)#stp disable
Raisecom(config-ge-2/1/0/2)#multi-active-detect mode direct
```

Checking results

Use the **show multi-active-detect information** command to show the MAD status.

Status of member 1:

```
Raisecom(config)#show multi-active-detect information
Current status : normal
Direct detect information:
  ge-1/1/0/2      up
Excluded ports(configurable):
  ge-1/1/0/5
Excluded ports(can not be configured):
  ge-1/1/0/1
```

Status of member 2:

```
Raisecom(config)#show multi-active-detect information
Current status : conflict
Direct detect information:
```

```
ge-2/1/0/2      up
Excluded ports(configurable):
ge-2/1/0/5
Excluded ports(can not be configured):
ge-2/1/0/1
```

10.18 NQA

10.18.1 Introduction

Network Quality Analysis (NQA) is a realtime network performance detection and statistical technology that can gather statistics about network information, such as response time, network jitter, and packet loss rate. NQA can monitor network QoS in real time and provide effective fault diagnosis and localization in the event of network failures.

10.18.2 Preparing for configurations

Scenario

To make the network QoS visible, you can check whether the network QoS meets the requirements. In this case, you need to deploy probe devices on the network to monitor the network QoS.

When the device provides NQA, there is no need to deploy specialized probe devices, which can effectively save costs. NQA can implement accurate testing of network operation status and output statistics.

NQA monitors the performance of various protocols running on the network, enabling users to collect realtime network performance indicators, such as the total HTTP delay, TCP connection delay, DNS resolution delay, file transmission rate, FTP connection delay, and DNS resolution error rate.

Prerequisites

N/A

10.18.3 Default configurations

Default configurations of NQS are as below.

Function	Default value
NQS	Disable

10.18.4 Configure the ICMP-echo test

Configure the ICMP-echo test for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#nqa test-instance <i>admin-name</i> <i>operate-tag</i> type icmp-echo	Configure the test instance to icmp-echo.
3	Raisecom(nqa-admin-test-icmp-echo)#destination ip <i>ip-address</i>	Configure the destination IP address.
4	Raisecom(nqa-admin-test-icmp-echo)#frequency <i>freq-ms</i>	Configure the test frequency, in units of millisecond.
5	Raisecom(nqa-admin-test-icmp-echo)#probe count <i>count</i>	Configure the count of probes in each test.
6	Raisecom(nqa-admin-test-icmp-echo)#probe timeout <i>timeout-time-ms</i>	Configure the waiting time for each test, in units of millisecond.
7	Raisecom(config)#nqa schedule <i>admin-name</i> <i>operate-tag</i> start-time now life-time forever	Configure the scheduling policy is immediate start with permanent cycling. Select one of this configuration and binding the time range.
8	Raisecom(config)#nqa schedule <i>admin-name</i> <i>operate-tag</i> time-range <i>timer-range-list</i>	Configure the scheduling policy to be bound with the time range. Select one of this configuration and starting policy.

10.18.5 Configuring the UDP-echo test

Configure the UDP-echo test for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#nqa server enable	Enable NQA Server.
3	Raisecom(config)#nqa server udp-connect <i>ip-address</i> <i>udp-port</i>	Configure UDP Server.

Configure the client as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#nqa test-instance <i>admin-name</i> <i>operate-tag</i> type udp-echo	Configure the test instance to udp-echo.

Step	Command	Description
3	Raisecom(nqa-admin-test-udp-echo)# destination ip <i>ip-address</i>	Configure the destination IP address.
4	Raisecom(nqa-admin-test-udp-echo)# destination port <i>udp-port</i>	Configure the destination UDP port number.
5	Raisecom(nqa-admin-test-udp-echo)# frequency <i>freq-ms</i>	Configure the test frequency, in units of millisecond.
6	Raisecom(nqa-admin-test-udp-echo)# probe count <i>count</i>	Configure the count of probes in each test.
7	Raisecom(nqa-admin-test-udp-echo)# probe timeout <i>timeout-time-ms</i>	Configure the waiting time for each test, in units of millisecond.
8	Raisecom(config)# nqa schedule <i>admin-name operate-tag start-time now life-time forever</i>	Configure the scheduling policy is immediate start with permanent cycling. Select one of this configuration and binding the time range.
9	Raisecom(config)# nqa schedule <i>admin-name operate-tag time-range timer-ange-list</i>	Configure the scheduling policy to be bound with the time range. Select one of this configuration and starting policy.

10.18.6 Configuring the TCP test

Configure the server as below.

Step	Command	Description
1	Raisecom# configure	Enter global configuration mode.
2	Raisecom(config)# nqa server enable	Enable NQA Server.
3	Raisecom(config)# nqa server tcp-connect <i>ip-address tcp-port</i>	Configure TCP Server.

Configure the client as below.

Step	Command	Description
1	Raisecom# configure	Enter global configuration mode.
2	Raisecom(config)# nqa test-instance <i>admin-name operate-tag type tcp</i>	Configure the test instance to tcp.
3	Raisecom(nqa-admin-test-tcp)# destination ip <i>ip-address</i>	Configure the destination IP address.

Step	Command	Description
4	<code>Raisecom(nqa-admin-test-tcp)#destination port tcp-port</code>	Configure the destination TCP port number.
5	<code>Raisecom(nqa-admin-test-tcp)#frequency freq-ms</code>	Configure the test frequency, in units of millisecond.
6	<code>Raisecom(nqa-admin-test-tcp)#probe count count</code>	Configure the count of probes in each test.
7	<code>Raisecom(nqa-admin-test-tcp)#probe timeout timeout-time-ms</code>	Configure the waiting time for each test, in units of millisecond.
8	<code>Raisecom(config)#nqa schedule admin-name operate-tag start-time now life-time forever</code>	Configure the scheduling policy is immediate start with permanent cycling. Select one of this configuration and binding the time range.
9	<code>Raisecom(config)#nqa schedule admin-name operate-tag time-range timer-ange-list</code>	Configure the scheduling policy to be bound with the time range. Select one of this configuration and starting policy.

10.18.7 Configuring the DNS test

Configure the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#nqa test-instance admin-name operate-tag type dns</code>	Configure the test instance to dns.
3	<code>Raisecom(nqa-admin-test-dns)#destination ip ip-address</code>	Configure the IP address of the DNS server.
4	<code>Raisecom(nqa-admin-test-dns)#resolve-target domain-name</code>	Configure the name of the domain to be resolved.
5	<code>Raisecom(nqa-admin-test-tcp)#frequency freq-ms</code>	Configure the test frequency, in units of millisecond.
6	<code>Raisecom(nqa-admin-test-tcp)#probe count count</code>	Configure the count of probes in each test.
7	<code>Raisecom(nqa-admin-test-tcp)#probe timeout timeout-time-ms</code>	Configure the waiting time for each test, in units of millisecond.

Step	Command	Description
8	Raisecom(config)#nqa schedule admin-name operate-tag start- time now life-time forever	Configure the scheduling policy is immediate start with permanent cycling. Select one of this configuration and binding the time range.
9	Raisecom(config)#nqa schedule admin-name operate-tag time- range timer-ange-list	Configure the scheduling policy to be bound with the time range. Select one of this configuration and starting policy.

10.18.8 Configuring the HTTP test

Configure the HTTP test for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#nqa test- instance admin-name operate- tag type http	Configure the test instance to http.
3	Raisecom(nqa-admin-test- http)#destination ip ip- address	Configure the IP address of the HTTP server.
4	Raisecom(nqa-admin-test- http)#url url-path	Configure the probe URL.
5	Raisecom(nqa-admin-test- http)#frequency freq-ms	Configure the test frequency, in units of millisecond.
6	Raisecom(nqa-admin-test- http)#probe count count	Configure the count of probes in each test.
7	Raisecom(nqa-admin-test- http)#probe timeout timeout- time-ms	Configure the waiting time for each test, in units of millisecond.
8	Raisecom(config)#nqa schedule admin-name operate-tag start- time now life-time forever	Configure the scheduling policy is immediate start with permanent cycling. Select one of this configuration and binding the time range.
9	Raisecom(config)#nqa schedule admin-name operate-tag time- range timer-ange-list	Configure the scheduling policy to be bound with the time range. Select one of this configuration and starting policy.

10.18.9 Configuring the FTP test

Configure the FTP test for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#nqa test-instance admin-name operate-tag type ftp	Configure the test instance to http.
3	Raisecom(nqa-admin-test-ftp)#destination ip ip-address	Configure the IP address of the FTP server.
4	Raisecom(nqa-admin-test-ftp)#username ftp-username	Configure the FTP user name.
5	Raisecom(nqa-admin-test-ftp)#password ftp-password	Configure the FTP password.
6	Raisecom(nqa-admin-test-ftp)#filename ftp-filename	Configure the name of the file for probe.
7	Raisecom(nqa-admin-test-ftp)#operation { get put }	(Optional) configure the FTP operation. By default, it is get.
8	Raisecom(nqa-admin-test-ftp)#frequency freq-ms	Configure the test frequency, in units of millisecond.
9	Raisecom(nqa-admin-test-ftp)#probe count count	Configure the count of probes in each test.
10	Raisecom(nqa-admin-test-ftp)#probe timeout timeout-time-ms	Configure the waiting time for each test, in units of millisecond.
11	Raisecom(config)#nqa schedule admin-name operate-tag start-time now life-time forever	Configure the scheduling policy is immediate start with permanent cycling. Select one of this configuration and binding the time range.
12	Raisecom(config)#nqa schedule admin-name operate-tag time-range timer-ange-list	Configure the scheduling policy to be bound with the time range. Select one of this configuration and starting policy.

10.18.10 Configuring the SNMP test

Configure the SNMP test for the device as below.

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

Step	Command	Description
2	Raisecom(config)#nqa test-instance <i>admin-name operate-tag type snmp</i>	Configure the test instance to snmp.
3	Raisecom(nqa-admin-test-snmp)#destination ip <i>ip-address</i>	Configure the IP address of the SNMP server.
4	Raisecom(nqa-admin-test-snmp)#frequency <i>freq-ms</i>	Configure the test frequency, in units of millisecond.
5	Raisecom(nqa-admin-test-snmp)#probe count <i>count</i>	Configure the count of probes in each test.
6	Raisecom(nqa-admin-test-snmp)#probe timeout <i>timeout-time-ms</i>	Configure the waiting time for each test, in units of millisecond.
7	Raisecom(config)#nqa schedule <i>admin-name operate-tag start-time now life-time forever</i>	Configure the scheduling policy is immediate start with permanent cycling. Select one of this configuration and binding the time range.
8	Raisecom(config)#nqa schedule <i>admin-name operate-tag time-range timer-ange-list</i>	Configure the scheduling policy to be bound with the time range. Select one of this configuration and starting policy.

10.18.11 Configuring test history recording

Configure test history recording for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#nqa test-instance <i>admin-name operate-tag [type { icmp-echo udp-echo tcp dns http ftp snmp }]</i>	Enter any NQA test instance.
3	Raisecom(nqa-admin-test-icmp-echo)#history-record enable	Enable test history recording.
4	Raisecom(nqa-admin-test-icmp-echo)#history-record keep-time <i>time-minutes</i>	(Optional) configure the period for saving history records, in units of minute.

10.18.12 Configuring test statistics

Configure test statistics for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#nqa test-instance <i>admin-name</i> <i>operate-tag</i> [type { icmp-echo udp-echo tcp dns http ftp snmp }]	Enter any NQA test instance.
3	Raisecom(nqa-admin-test-icmp-echo)#statistics enable	Enable test statistics.
4	Raisecom(nqa-admin-test-icmp-echo)#statistics interval <i>interval-minutes</i>	(Optional) configure the statistic period.

10.18.13 Configuring test Trap

Configure test Trap for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#nqa test-instance <i>admin-name</i> <i>operate-tag</i> [type { icmp-echo udp-echo tcp dns http ftp snmp }]	Enter any NQA test instance.
3	SwitchA(nqa-admin-test-icmp-echo)#reaction trap probe-failure <i>fail-count</i>	Configure NQA to send a Trap when each probe encounters n consecutive failures.
4	SwitchA(nqa-admin-test-icmp-echo)#reaction trap test-failure <i>fail-count</i>	Configure NQA to send a Trap when each probe encounters n total failures.
5	SwitchA(nqa-admin-test-icmp-echo)#reaction trap test-complete	Configure NQA to send a Trap when each probe is complete.

10.18.14 Checking results

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show nqa config	Show NQA configurations.

10.18.15 Maintenance

Maintain the device as below.

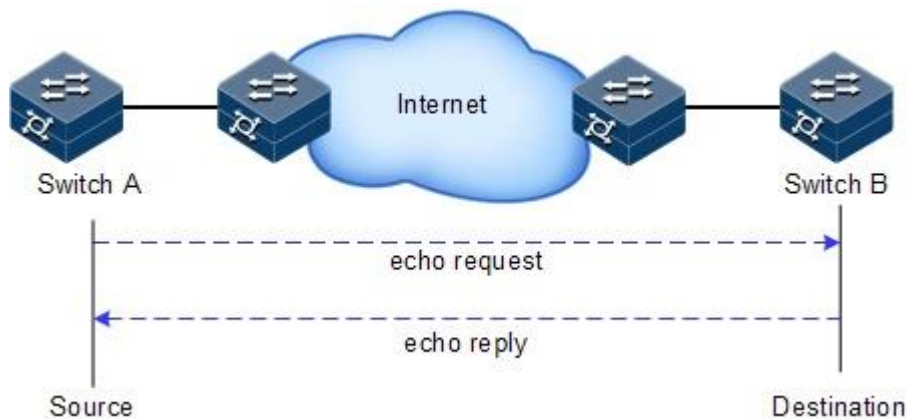
Command	Description
<code>Raisecom#show nqa agent</code>	Show information about NQA clients.
<code>Raisecom#show nqa server</code>	Show information about the NQA server.
<code>Raisecom#show nqa result <i>admin-name operate-tag</i></code>	Show the test result of NQA clients.
<code>Raisecom#show nqa history <i>admin-name operate-tag</i></code>	Show the history test result of NQA clients.
<code>Raisecom#show nqa statistics <i>admin-name operate-tag</i></code>	Show statistics on test results of NQA clients.

10.18.16 Example for configuring the ICMP-echo test

Networking requirements

As shown in Figure 10-21, enable the ICMP-echo test on switch A to detect the IP layer connectivity between switch A and switch B.

Figure 10-21 ICMP-echo test networking



Configuration steps

Step 1 Configure IP layer connectivity.

Configure Switch A.

```

Raisecom#hostname SwitchA
SwitchA#configure
SwitchA(config)#vlan 10
SwitchA(config-vlan-10)#quit
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port hybrid vlan 10 tagged
SwitchA(config-ge-1/0/1)#quit
SwitchA(config)#interface vlan 10
SwitchA(config-vlanif-10)#ip address 10.1.1.1/24

```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#configure
SwitchB(config)#vlan 10
SwitchB(config-vlan-10)#quit
SwitchB(config)#interface ge 1/0/1
SwitchB(config-ge-1/0/1)#port hybrid vlan 10 tagged
SwitchB(config-ge-1/0/1)#quit
SwitchB(config)#interface vlan 10
SwitchB(config-vlanif-10)#ip address 10.1.1.2/24
```

Step 2 Configure the icmp-echo probe instance of NQA.

Configure Switch A.

```
SwitchA(config)#nqa test-instance admin test type icmp-echo
SwitchA(nqa-admin-test-icmp-echo)#destination ip 10.1.1.2
SwitchA(nqa-admin-test-icmp-echo)#frequency 10000
SwitchA(nqa-admin-test-icmp-echo)#probe count 3
SwitchA(nqa-admin-test-icmp-echo)#history-record enable
SwitchA(nqa-admin-test-icmp-echo)#reaction trap probe-failure 3
SwitchA(config)#nqa schedule admin test start-time now life-time forever
```

Checking results

Use the **show nqa config** command to show local configurations.

```
SwitchA(config)#show nqa config
!
nqa test-instance admin test type icmp-echo
  frequency 10000
  history-record enable
  statistics enable
  reaction trap probe-failure 3
  probe count 3
  destination ip 10.1.1.2
nqa schedule admin test start-time now life-time forever
.....
```

Use the **show nqa history admin test** command to show history test results.

```
SwitchA(config)#show nqa history admin test
```

Index	Response	Status	Time
9	11	succeeded	2023-11-10 17:05:26

8	7	successed	2023-11-10 17:05:26
7	10	successed	2023-11-10 17:05:26
6	12	successed	2023-11-10 17:05:16
5	7	successed	2023-11-10 17:05:16
4	9	successed	2023-11-10 17:05:16
3	11	successed	2023-11-10 17:05:05
2	8	successed	2023-11-10 17:05:05
1	9	successed	2023-11-10 17:05:05

10.19 POE

10.19.1 Introduction

Power over Ethernet (PoE) refers to the power supply through an Ethernet network, also known as a power supply system Power over LAN (PoL) or Active Ethernet.

10.19.2 Preparing for configurations

Scenario

With the increasing popularity of IP phones, network video monitoring, and wireless Ethernet applications on the network, the demand for power support through Ethernet is becoming increasingly urgent. In most cases, the Access Point (AP) device requires direct current power supply, and it is usually installed on the ceiling or outdoors. It is difficult to reach power sockets nearby. Even if there are sockets, the AC/DC converters required by the AP device are difficult to locate. In many large-scale LAN applications, the administrator need to manage multiple AP devices simultaneously, which require unified power supply and management and cause great inconvenience to power supply management. PoE precisely solves this problem.

PoE is a wired Ethernet powering technology and is currently the most widely used technology in LANs. PoE allows electrical power to be transmitted to terminal devices through data transmission lines or idle lines. When the terminal devices are powered by 10BASE-T, 100BASE-TX, and 1000BASE-T Ethernet networks, the reliable power supply distance can reach up to 100 m. Through this method, the centralized power supply of terminals can be available, such as IP phones, wireless APs, portable device chargers, card readers, cameras, and data collectors. For these terminals, there is no need to consider the issue of indoor power system wiring, and they can be powered on while being connected to the network.

Prerequisite

N/A

10.19.3 Default configurations of PoE

Default configurations of PoE are as below.

Function	Default value
PoE status	Enable
Working mode of the PoE interface	Auto

10.19.4 Enabling PoE

Enable PoE 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.  Note The physical interface to be used must support PoE.
3	Raisecom(config-ge-1/0/*)#poe { enable disable }	Enable or disable PoE.
4	Raisecom(config-ge-1/0/*)#poe power-management { auto manual default }	Configure the working mode of PoE.

10.19.5 Configuring the maximum output power of PoE

Configure the maximum output power of PoE for the device as below:

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#interfac e interface-type <i>interface-number</i>	Enter physical interface configuration mode. The physical interface to be used must support PoE.
3	Raisecom(config-ge- 1/0/*)#poe max-power <i>power-value</i>	Configure the maximum output power of PoE.

10.19.6 Configuring power-on and power-off of PoE

Configure power-on and power-off of PoE for the device as below:

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

Step	Command	Description
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical interface configuration mode. The physical interface to be used must support PoE.
3	<code>Raisecom(config-ge-1/0/*)#poe power-priority { critical high low default }</code>	Configure the power supply priority of the PoE interface.  Note Some devices do not support this function. See the descriptions.
4	<code>Raisecom(config-ge-1/0/*)#poe { power-on power-off }</code>	Configure manual power-on and power-off of the PoE interface.
5	<code>Raisecom(config-ge-1/0/*)#poe shutdown time-range <i>timer-range-list</i></code>	Configure the power-off period of the PoE interface.
6	<code>Raisecom(config-ge-1/0/1)#poe inrush { af at bt4 default }</code>	Configure the power standard of the PoE interface.
7	<code>Raisecom(config-ge-1/0/1)#poe high-inrush { enable disable }</code>	Configure the high inrush current of the PD upon power-on by the PoE interface

10.19.7 Configuring smart PoE

Configure smart PoE for the device as below.

Step	Command	Description
1	<code>Raisecom#configure</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical interface configuration mode. The physical interface to be used must support PoE.
3	<code>Raisecom(config-ge-1/0/1)#poe alive action { reboot alarm reboot-alarm none }</code>	Configure the action to be taken upon detection of an abnormal PD.
4	<code>Raisecom(config-ge-1/0/1)#poe reboot interval <i>reboot-interval</i></code>	Configure the interval for restarting the detected abnormal PD.
5	<code>Raisecom(config-ge-1/0/1)#poe track-naq <i>admin-name operate-tag</i></code>	Configure abnormal PD detection bound with the NAQ instance.

10.19.8 Configuring the PD description

Configure the PD description 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. The physical interface to be used must support PoE.
3	Raisecom(config-ge-1/0/*)#poe description <i>descr-str</i>	Configure the PD description.

10.19.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show poe config	Show PoE configurations.

10.19.10 Maintenance

Maintain the device as below.

Command	Description
Raisecom#show poe information	Show PoE information about the device.
Raisecom#show poe interface	Show the power supply status of the PoE interface.

10.19.11 Example for configuring PoE

Networking requirements

Configure PoE interfaces GE1/0/1, GE1/0.2, and GE1/0/3 to be connected to three PDs respectively.

Configuration steps

Step 1 Configure the working mode to auto.

```
Raisecom#configure
Raisecom(config)#interface ge 1/0/1
```



```
Raisecom(config-ge-1/0/1)#poe power-management auto
Raisecom(config-ge-1/0/1)#quit
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#poe power-management auto
Raisecom(config-ge-1/0/2)#quit
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#poe power-management auto
Raisecom(config-ge-1/0/3)#quit
```

Step 2 Configure the maximum output power of the PoE interfaces.

```
Raisecom#configure
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#poe max-power 1500
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#poe max-power 1500
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#poe max-power 1500
```

Step 3 Configure power supply priorities of the PoE interfaces.

```
Raisecom#configure
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#poe power-priority critical
Raisecom(config)#interface ge 1/0/2
Raisecom(config-ge-1/0/2)#poe power-priority high
Raisecom(config)#interface ge 1/0/3
Raisecom(config-ge-1/0/3)#poe power-priority high
```

Checking results

Use the **show poe config** command to show local PoE configurations.

```
Raisecom#show poe config
!
interface ge 1/0/1
  poe power-priority critical
  poe max-power 1500
!
interface ge 1/0/2
  poe power-priority high
  poe max-power 1500
!
interface ge 1/0/3
  poe power-priority high
  poe max-power 1500
.....
```

Use the **show poe interface** command to show history test results.

Raisecom#**show poe interface**

Interface	State	PowerMode	PowerPri	DetectStatus	PowerClass
CurrentPower(mW)	Descr				

ge-1/0/1	enable	auto	critical	deliveringPower	class4
24000	-				
ge-1/0/2	enable	auto	high	searching	-- 0
-					
ge-1/0/3	enable	auto	high	deliveringPower	class4
24000	-				
ge-1/0/4	enable	auto	low	searching	-- 0
-					
ge-1/0/5	enable	auto	low	searching	-- 0
-					
ge-1/0/6	enable	auto	low	searching	-- 0
-					
ge-1/0/7	enable	auto	low	searching	-- 0
-					
ge-1/0/8	enable	auto	low	searching	-- 0
-					

10.19.12 Example for configuring Smart PoE

Networking requirements

Configure the PoE interface GE 1/0/1 to be connected to a PD.

Configuration steps

Step 1 Configure the working mode to auto.

```
Raisecom#configure
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#poe power-management auto
Raisecom(config-ge-1/0/1)#quit
```

Step 2 Configure the connectivity upon detection of a PD by the NAQ instance.

```
Raisecom#configure
Raisecom(config)#naq test-instance admin test1 type icmp-echo
Raisecom(naq-admin-test1-icmp-echo)#destination ip 10.1.1.1
Raisecom(naq-admin-test1-icmp-echo)#frequency 10000
```

```
Raisecom(nqa-admin-test1-icmp-echo)#quit
Raisecom(config)#nqa schedule admin test1 start-time now life-time
forever
```

- Step 3 Configure the NQA instance bound with PoE. When an abnormal PD is detected, it is restarted and sends an alarm.

```
Raisecom#configure
Raisecom(config)#interface ge 1/0/1
Raisecom(config-ge-1/0/1)#poe alive action reboot-alarm
Raisecom(config-ge-1/0/1)#poe track-nqa admin test1
```

Checking results

Use the **show poe config** command to show local PoE configurations.

```
Raisecom#show poe config
!
interface ge 1/0/1
poe alive action reboot-alar
poe track-nqa admin test1
```

10.20 Patching

10.20.1 Introduction

The patching function can fix system loopholes online with a patch without updating the system software and fix software defects. The system supports up to 32 patches.

10.20.2 Preparing for configurations

Scenario

The problem found in the system can be solved by patching, needless of device restart.

Prerequisite

Prepare the patch file.

10.20.3 Loading the patch file

Load the patch file for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#patch 1 load filename	Load the patch file.

10.20.4 Activating the patch file

Activate the patch file for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#patch 1 active	Activate the patch file.

10.20.5 Deactivating the patch file

Deactivate the patch file for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#patch 1 deactivate	Deactivate the patch file.

10.20.6 Deleting the patch file

Delete the patch file for the device as below.

Step	Command	Description
1	Raisecom#configure	Enter global configuration mode.
2	Raisecom(config)#patch 1 delete	Delete the patch file to make it invalid.

10.20.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show patch information	Show the patch of the device.

10.20.8 Example for configuring patching

Networking requirements

The problem found in the system can be solved by patching.

The SNMP interface on the device is connected to the PC, which is installed with the TFTP software. The device downloads the patch file from the PC.

Configuration steps

Step 1 Download the patch file from the PC to the device through TFTP.

```
Raisecom(config)#tftp get 22.1.1.1 libmspaaa_patch.pat localfile  
libmspaaa_patch.pat
```

Step 2 Load the patch file.

```
Raisecom(config)#patch 1 load libmspaaa_patch.pat
```

Step 3 Activate the patch file.

```
Raisecom(config)#patch 1 active
```

Checking results

Use the **show patch information** command to show the patch status.

```
Raisecom(config)#show patch information  
Patch max number      : 32  
Patch current number  : 1  
Seq ProcName  State  Type  Valid  EffetiveTime      PatchName  
-----  
1   mspaaa    ACTIVE REP   YES   2024-03-20 17:08:52 libmspaaa_patch.pat
```

10.21 Periodically backing up configurations

10.21.1 Introduction

This function is implemented by the combination of automatic configuration uploading and time range.

10.21.2 Preparing for configurations

Scenario

Periodically back up configurations to the specified server.

Prerequisite

The device and PC can ping each other. Enable the TFTP or FTP server on the PC.

10.21.3 Configuring time range

Configure a time range list for the device as below.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# time-range list id	Create a time range list.
3	Raisecom(config-timerange-*)# time-range timerange-id absolute from <i>hour:minute:second</i> <i>year/month/monthday to</i> <i>hour:minute:second</i> <i>year/month/monthday</i> Raisecom(config-timerange-*)# time-range timerange-id everyhour <i>minute:second to minute:second</i> Raisecom(config-timerange-*)# time-range timerange-id everyday <i>hour:minute:second to</i> <i>hour:minute:second</i> Raisecom(config-timerange-*)# time-range timerange-id everyweek <i>hour:minute:second { mon tue wed</i> <i> thu fri sat sun } to { mon </i> <i>tue wed thu fri sat sun }</i> Raisecom(config-timerange-*)# time-range timerange-id everymonth <i>hour:minute:second monthday to</i> <i>hour:minute:second monthday</i> Raisecom(config-timerange-*)# time-range timerange-id everyweekend <i>hour:minute:second to</i> <i>hour:minute:second</i> Raisecom(config-timerange-*)# time-range timerange-id everyyear <i>hour:minute:second month/monthday</i> <i>to hour:minute:second month/monthday</i>	Create a time range for automatic uploading. - Relative time range (periodic time range): periodic time range of one week described by the everyxxx parameter. It can be indicated by an absolute time range to indicate the effective date of the time range. - Absolute time range: a specific time range specified by the absolute parameter. You can limit the relative time range (periodic time range) to take effect within a specific time range specified by the absolute time range. If multiple effective times are configured for this time range, the effective principle is to perform OR between periodic time ranges, and to perform AND between the periodic time range and absolute time range.

10.21.4 Configuring automatic uploading

Configure automatic uploading for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#auto-upload start	Enable automatic uploading.
3	Raisecom(config)#auto-upload tftp server { <i>ipv4-address</i> <i>ipv6-address</i> } <i>remotefile</i> { config running-config log } [interval <i>interval-value</i> port <i>port-number</i> time-range <i>list-number</i>]*	Configure the attributes of the TFTP server for automatic uploading, and specify the file to be uploaded and the bound time range list.
4	Raisecom(config)#auto-upload ftp server { <i>ipv4-address</i> <i>ipv6-address</i> } <i>username password</i> <i>remotefile</i> { config running-config log } [interval <i>interval-value</i> port <i>port-number</i> time-range <i>list-number</i>]*	Configure the attributes of the FTP server for automatic uploading, and specify the file to be uploaded and the bound time range list.

10.21.5 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom#show auto-upload server	Show configured automatic uploading entries.
2	Raisecom#show auto-upload config	Show configurations of automatic uploading.

10.21.6 Example for configuring periodic backup

Networking requirements

Configure the device to automatically back up current configurations through TFTP to the PC.

The device and PC are connected by the SNMP interface. Enable the TFTP server on the PC.

Configuration steps

Step 1 Configure time range list 1, and configure rule 1 (take the 1h periodic backup for example).

```
Raisecom(config)#time-range list 1
Raisecom(config-timerange-1)#time-range 1 everyhour 3:10 to 13:10
```

- Step 2 Configure properties of automatic uploading. Enable automatic uploading. Create an entry (the IP address of the TFTP server is 192.168.62.1, the local file is the running configuration file, and the file to be uploaded to the TFTP server is config.txt), and bound time range list 1.

```
Raisecom(config)#auto-upload start
Raisecom(config)#auto-upload tftp server 192.168.62.1 config.txt running-
config time-range 1
```

- Step 3 After configurations are complete, the device automatically uploads the configuration file to the TFTP server on the PC every 1h3min10s.

Checking results

Use the **show auto-upload server** command to show configurations of automatic uploading.

```
Raisecom(config)#show auto-upload server
Type Server          Port  Interval(min) Localfile      vpn
TimerangeId
-----
tftp 192.168.62.1    69    10          running-config  n/a
1
-----
Raisecom(config)#
```


11 L3VPN services

This chapter describes basic principles and configuration procedures for L3VPN services, including the following sections:

- Basic configurations of L3VPN

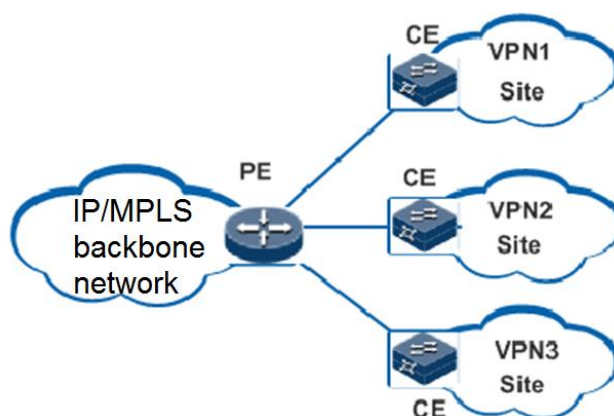
11.1 Basic configurations of L3VPN

11.1.1 Introduction

The L3VPN function mentioned in this chapter implements the Multi-VPN-Instance CE (MCE) function. Devices with MCE can undertake the CE function of multiple VPN instances in VPN networking applications, reducing user network equipment investment.

VPN solves the problem of transmitting private network data on the public network through tunneling, but the traditional VPN architecture requires each VPN instance to be connected to PE by using a separate CE, as shown in Figure 11-1.

Figure 11-1 Networking before deploying MCE

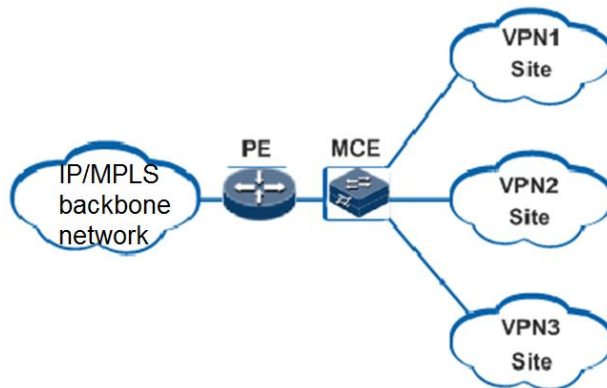


With the continuous refinement of user services and the improvement of security requirements, in many cases, users within a private network need to be divided into multiple VPNs, and services of different VPN users need to be completely isolated. At this point, configuring a separate CE for each VPN increases the user's device expenses and maintenance

costs; moreover, multiple VPNs sharing the same CE and using the same routing table cannot guarantee data security.

MCE can effectively solve the contradiction between data security and network costs brought about by multiple VPNs, as shown in Figure 11-2.

Figure 11-2 Networking after deploying MCE



MCE extends some functions of the PE to CE devices by binding different interfaces to VPNs and creating and maintaining independent routing and forwarding tables (Multi VRF) for each VPN. This not only isolates the packet forwarding paths of different VPNs within the private network, but also, through cooperation with the PE, correctly advertises routes of each VPN to the peer PE, ensuring the transmission of VPN packets within the public network.

11.1.2 Preparing for configurations

Scenario

Configure the VPN instance on the MCE (configure one VPN instance for each service).

Prerequisites

Configure the VPN instance name and VLAN interface.

11.1.3 Creating a VPN instance

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip vpn-instance <i>name</i>	Create a VPN instance.
3	Raisecom(config-vpn-instance-*)#ipv4-family	Enable the IPv4 address family of the VPN instance.
4	Raisecom(config-vpn-instance-*af-ipv4)#route-distinguisher <i>9:9</i>	Configure the RD.
5	Raisecom(config-vpn-instance-*af-ipv4)#vpn-target <i>9:9 both</i>	Associate the current VPN instance with the VPN target.

11.1.4 Binding the VLAN interface with the VPN instance

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlanif-*)#ip vpn-instance <i>name</i>	Bind the VLAN interface with the VPN instance.

11.1.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show ip vpn- instance	Show information about all VPN instances.

11.1.6 Example for binding the VLAN interface with the VPN instance

Networking requirements.

Bind the VLAN interface on the switch with the VPN instance

Configuration steps

Step 1 Create a VLAN. 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 on the switch.

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

Step 3 Create a VPN instance.

```
Raisecom(config)#ip vpn-instance 123
Raisecom(config-vpn-instance-123)#ipv4-family
Raisecom(config-vpn-instance-123-af-ipv4)#route-distinguisher 9:9
Raisecom(config-vpn-instance-123-af-ipv4)#vpn-target 9:9 both
Raisecom(config-vpn-instance-123-af-ipv4)#quit
Raisecom(config-vpn-instance-123)#quit
```

Step 4 Bind the VLAN with the VPN instance.

```
Raisecom(config-vlanif-10)#ip vpn-instance 123
```

Checking result

Use the **show ip vpn-instance verbose** command to show VPN configurations.

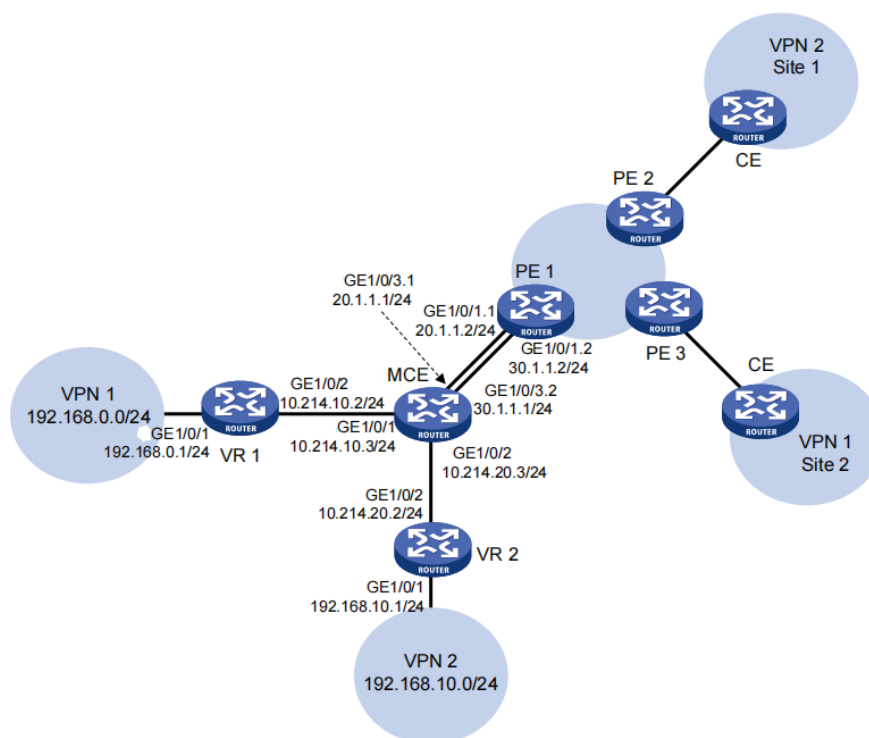
```
Raisecom(config)#show ip vpn-instance verbose
```

```
-----
VPN-Instance Name      : 123
VPN-Instance ID       : 2
Creation Time          : 1970-01-01 08:00:02
Description            : --
Ipv4 Family
Route Distinguisher   : 9:9
Multicast              : disable
Apply Mode             : Route
Shared Group          : --
Source Interface       : --
Binding               : --
Vpn Target Import     : 9:9
Vpn Target Export     : 9:9
```

11.1.7 Example for configuring MCE

Networking requirements

The MCE is connected to two VPNs: VPN 1 and VPN 2. Their edge devices are VR 1 and VR 2 respectively. Wherein, VPN 2 runs RIP. The MCE isolates routes between two VPNs, and advertises routes of each VPN to PE 1 through OSPF.



```
MCE(config-ge-1/0/1)#port hybrid vlan 12 untagged
MCE(config-ge-1/0/1)#port hybrid pvid 12
MCE(config-ge-1/0/1)#interface vlan 12
MCE(config-vlanif-12)#ip bind vpn-instance vpn1
    %All IP related configurations on this interface are removed!
MCE(config-vlanif-12)#ip address 10.214.10.3/24
```

Bind interface GE 1/0/2 with VPN instance vpn2. Configure the IP address of the interface.

```
MCE(config)#interface ge 1/0/2
MCE(config-ge-1/0/2)#port hybrid vlan 13 untagged
MCE(config-ge-1/0/2)#port hybrid pvid 13
MCE(config-ge-1/0/2)#interface vlan 13
MCE(config-vlanif-13)#ip bind vpn-instance vpn2
    %All IP related configurations on this interface are removed!
MCE(config-vlanif-13)#ip address 10.214.20.3/24
```

Configure two VPN instances on PE 1, name them vpn1 and vpn2, configure their RDs to 10:1 and 20:1 respectively, configure their VPN Target values to be same with RDs, and configure Export and Import target values to be the same.

```
PE1#config
PE1(config)#ip vpn-instance vpn1
PE1(config-vpn-instance-vpn1)#ipv4-family
PE1(config-vpn-instance-vpn1-af-ipv4)#route-distinguisher 10:1
PE1(config-vpn-instance-vpn1-af-ipv4)#vpn-target 10:1 import-extcommunity
PE1(config-vpn-instance-vpn1-af-ipv4)#vpn-target 10:1 export-extcommunity
PE1(config-vpn-instance-vpn1-af-ipv4)#ip vpn-instance vpn2
PE1(config-vpn-instance-vpn2)# ipv4-family
PE1(config-vpn-instance-vpn2-af-ipv4)#route-distinguisher 20:1
PE1(config-vpn-instance-vpn2-af-ipv4)#vpn-target 20:1 import-extcommunity
PE1(config-vpn-instance-vpn2-af-ipv4)#vpn-target 20:1 export-extcommunity
```

Step 2 Configure the route between the MCE and site.

The MCE and VPN 1 are directly connected. No routing protocol is used in VPN 1, so the static route can be configured.

For VR 1, configure the IP address of the interface, connected to the MCE, to 10.214.10.2/24; connect the IP address of the interface, connected to VPN 1, to 192.168.0.1/24 (configuration steps are omitted).

Configure the default route on VR 1. Specify the next hop IP address of packets in the egress direction to 10.214.10.3.

```
VR1(config)#ip route-static 0.0.0.0 0.0.0.0 10.214.10.3
```

Specify the static route on the MCE. Configure the next hop IP address of the packets, sent to 192.168.0.0/24, to 10.214.10.2. Bind the route with VPN instance vpn1.

```
MCE(config)#ip route-static 192.168.0.0 255.255.255.0 10.214.10.2
destination-vpn-instance vpn1 nexthop-vpn-instance vpn1
```

Run RIP in VPN 2. Configure the RIP process 20 on the MCE, and bind it with VPN instance vpn2 so that routes in VPN 2 are learnt by the routing table of VPN instance vpn2.

```
MCE(config)#rip 20 vpn-instance vpn2
```

Advertise routes of network segment 10.0.0.0.

```
MCE(config-rip-20)#network 10.0.0.0
```

For VR 2, configure the IP address of the interface, connected to the MCE, to 10.214.20.2/24; connect the IP address of the interface, connected to VPN 2, to 192.168.10.1/24 (configuration steps are omitted).

Configure RIP, and advertise routes of network segments 192.168.10.0 and 10.0.0.0.

```
VR2(config)#rip 20
VR2(config-rip-20)#network 192.168.10.0
VR2(config-rip-20)#network 10.0.0.0
```

On the MCE, show routing information about VPN instances vpn1 and vpn2.

```
MCE(config)#show ip route vpn-instance vpn1
```

Routing Tables: Vpn					
Destination	Gateway	Pre/Cost	Proto	Interface	
Mpls	Status	Vpn-Instance			

10.214.10.0/24	10.214.10.3	0/0	local	vlan-12	
no	Up	vpn1			
10.214.10.3/32	10.214.10.3	0/0	local	vlan-12	
no	Up	vpn1			
20.1.1.0/24	20.1.1.1	0/0	local	vlan-20	
no	Up	vpn1			
20.1.1.1/32	20.1.1.1	0/0	local	vlan-20	
no	Up	vpn1			
192.168.0.0/24	10.214.10.2	60/60	static	vlan-12	
no	Up	vpn1			

```

-----
Total: 5          Static: 1          Down: 0          Destination: 5
MCE(config)#show ip route vpn-instance vpn2
Routing Tables: vpn
Destination      Gateway          Pre/Cost         Proto Interface
Mpls      Status  Vpn-Instance
-----
10.214.20.0/24    10.214.20.3      0/0             local  vlan-13
no            Up      vpn2
10.214.20.3/32    10.214.20.3      0/0             local  vlan-13
no            Up      vpn2
30.1.1.0/24       30.1.1.1         0/0             local  vlan-30
no            Up      vpn2
30.1.1.1/32       30.1.1.1         0/0             local  vlan-30
no            Up      vpn2
192.168.10.0/24   10.214.20.2      100/1           rip    vlan-13
no            Up      vpn2
-----
Total: 5          Static: 0          Down: 0          Destination: 5

```

As you can see, the MCE has learnt private routes in VPN 2 through RIP, and maintains them and routing information in VPN 1 in two routing tables respectively and effectively isolates them.

Step 3 Configure the route between MCE and PE.

The MCE is connected to PE 1 through the sub-interface or VLAN. Add interface GE 1/0/3 on the MCE to VLAN 20, bind it with VPN instance vpn1, and configure its IP address.

```

MCE(config)#interface ge 1/0/3
MCE(config-ge-1/0/3)#port hybrid vlan 20 untagged
MCE(config-ge-1/0/3)#port hybrid pvid 20
MCE(config-ge-1/0/3)#interface vlan 20
MCE(config-vlanif-20)#ip bind vpn-instance vpn1
%All IP related configurations on this interface are removed!
MCE(config-vlanif-20)#ip address 20.1.1.1/24

```

Add interface GE 1/0/4 on the MCE to VLAN 30, bind it with VPN instance vpn2, and configure its IP address.

```

MCE(config)#interface ge 1/0/4
MCE(config-ge-1/0/4)#port hybrid vlan 30 untagged
MCE(config-ge-1/0/4)#port hybrid pvid 30
MCE(config-ge-1/0/4)#interface vlan 30
MCE(config-vlanif-30)#ip bind vpn-instance vpn2
%All IP related configurations on this interface are removed!

```



```
MCE(config-vlanif-30)#ip address 30.1.1.1/24
```

Add interface GE 1/0/3 on PE 1 to VLAN 20, bind it with VPN instance vpn1, and configure its IP address.

```
PE1(config)#interface ge 1/0/3  
PE1(config-ge-1/0/3)#port hybrid vlan 20 untagged  
PE1(config-ge-1/0/3)#port hybrid pvid 20  
PE1(config-ge-1/0/3)#interface vlan 20  
PE1(config-vlanif-20)#ip bind vpn-instance vpn1  
%All IP related configurations on this interface are removed!  
PE1(config-vlanif-20)#ip address 20.1.1.2/24
```

Add interface GE 1/0/4 on PE 1 to VLAN 30, bind it with VPN instance vpn2, and configure its IP address.

```
PE1(config)#interface ge 1/0/4  
PE1(config-ge-1/0/4)#port hybrid vlan 30 untagged  
PE1(config-ge-1/0/4)#port hybrid pvid 30  
PE1(config-ge-1/0/4)#interface vlan 30  
PE1(config-vlanif-30)#ip bind vpn-instance vpn2  
%All IP related configurations on this interface are removed!  
PE1(config-vlanif-30)#ip address 30.1.1.2/24
```

Start OSPF process 10 on the MCE. Bind it to VPN instance vpn1.

```
MCE(config)#ospf 10 vpn-instance vpn1
```

Advertise routes in network segment 20.1.1.0/24 in area 0, and redistribute static routes of VPN 1.

```
MCE(config-ospf-10)#network 20.1.1.0 255.255.255.0 area 0  
MCE(config-ospf-10)#import-route static
```

Start OSPF process 10 on PE 1. Bind it to VPN instance vpn1. Advertise routes in network segment 20.1.1.0/24 in area 0.

```
PE1(config)#ospf 10 vpn-instance vpn1  
PE1(config-ospf-10)#network 20.1.1.0 255.255.255.0 area 0
```

Configure OSPF process 20 between the MCE and PE 1. The steps for redistributing routes of VPN instance vpn2 are similar with previous configurations, but the difference is that the route redistributed in the MCE through OSPF is the route of RIP process 20. These are omitted here.

Checking results

Show information about routes in VPN 1 on PE 1. As you can see, the static routes in VPN 1 are redistributed into the OSPF routing table between the MCE and PE 1.

```
PE1(config)#show ip route vpn-instance vpn1
```

Routing Tables: Vpn					
Destination		Gateway	Pre/Cost	Proto	Interface
Mpls	Status	Vpn-Instance			

20.1.1.0/24		20.1.1.2	0/0	local	vlan-20
no	Up	vpn1			
20.1.1.2/32		20.1.1.2	0/0	local	vlan-20
no	Up	vpn1			
192.168.0.0/24		20.1.1.1	150/1	ospf	vlan-20
no	Up	vpn1			

Total: 3		Static: 0	Down: 0		Destination: 3

Show information about routes in VPN 2 on PE 1. As you can see, the RIP routes in VPN 2 are redistributed into the OSPF routing table between the MCE and PE 1.

```
PE1(config)#show ip route vpn-instance vpn2
```

Routing Tables: Vpn					
Destination		Gateway	Pre/Cost	Proto	Interface
Mpls	Status	Vpn-Instance			

10.214.20.0/24		30.1.1.1	150/1	ospf	vlan-30
no	Up	vpn2			
30.1.1.0/24		30.1.1.2	0/0	local	vlan-30
no	Up	vpn2			
30.1.1.2/32		30.1.1.2	0/0	local	vlan-30
no	Up	vpn2			
192.168.10.0/24		30.1.1.1	150/1	ospf	vlan-30
no	Up	vpn2			

Total: 4		Static: 0	Down: 0		Destination: 4

Till now, routes in two VPN instances are completely advertised to PE 1. The configurations are complete.

12 GRE

This chapter describes basic principles and configuration procedures for GRE services, including the following sections:

- Configuring GRE

12.1 Configuring GRE

12.1.1 Introduction

Generic Routing Encapsulation (GRE) can encapsulate data packets of some network layer protocols, such as IPX, IPv6 and AppleTalk so that encapsulated packets can be transmitted by another network layer protocol, such as IPv4.

GRE provide a mechanism for encapsulating packets of one protocol in packets of another protocol. As a Layer 3 tunnelling encapsulation technology, GRE enables packets to be transparently transmitted in the GRE tunnel, so it can solve the problem of transmitting packets on the heterogeneous network.

12.1.2 Preparing for configurations

Scenario

After the basic commands are configured, packets can be transparently transmitted in the GRE tunnel.

Prerequisites

The route between the source interface and destination interface is reachable.

12.1.3 Default configurations of GRE

Default configurations of GRE are as be below.

Function	Default value
GRE	The default value of the tunnelling protocol is none.

Function	Default value
GRE Keepalive detection	Disable

12.1.4 Configuring the GRE tunnel



Caution

- To configure the GRE IPv4 tunnel, configure the IPv6 address of the Tunnel interface in advance.
- To configure the GRE IPv6 tunnel, configure the IPv4 address of the Tunnel interface in advance.

Configure the GRE tunnel for the device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface tunnel <i>tunnel-id</i>	Enter the Tunnel interface view.
3	Raisecom(config-tunnel-<i>tunnel-id</i>)#tunnel-protocol gre [ipv4 ipv6]	Configure the tunnel protocol to GRE.
4	Raisecom(config-tunnel-<i>tunnel-id</i>)#source interface vlan <i>vlan-id</i>	Configure the type and ID of the GRE tunnel source interface.
5	Raisecom(config-tunnel-<i>tunnel-id</i>)#destination { ip <i>ip-address</i> ipv6 <i>ipv6-address</i> } [vpn-instance <i>name</i>]	Configure the destination IP address of the tunnel.
6	Raisecom(config-tunnel-<i>tunnel-id</i>)# { ip address <i>ip-address mask</i> ipv6 address <i>ipv6-address prefix-len</i> }	Configure the IP address of the tunnel.
7	Raisecom(config){ ip route-static <i>ip-address ipv6-address</i> ipv6 route-static <i>ipv6-address ipv6-prefixlen</i> } interface <i>tunnel-id</i>	Configure the static route.

12.1.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show interface tunnel config	Show configurations of the tunnel.

12.1.6 Maintenance

In daily maintenance work, you can choose to execute the following commands in any view to understand the operation of the GRE protocol. You can check whether the GRE tunnel interface is up, whether there are error packets, and whether the routing information to the destination address is forwarded normally through the Tunnel interface.

Command	Description
<code>Raisecom(config)#show interface tunnel 1</code>	Show the status and statistics of the Tunnel interface.

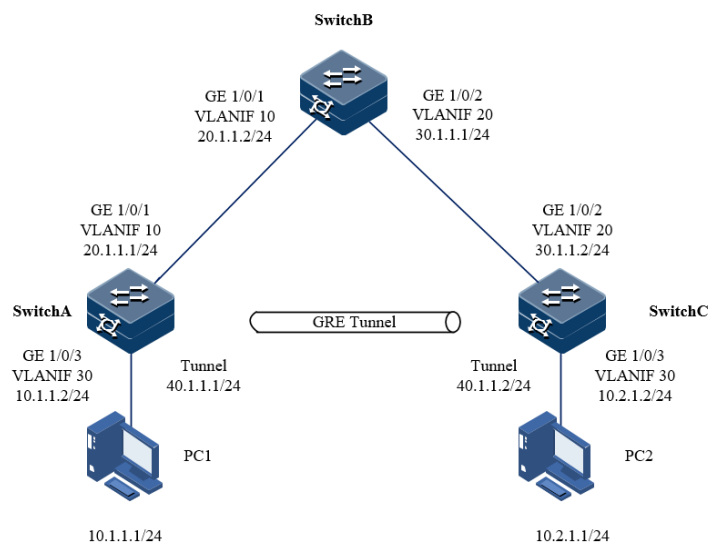
12.1.7 Example for configuring GRE

Networking requirements

As shown in Figure 12-1:

- Switch A, Switch B, and Switch C are interconnected on the public network (using the OSPF protocol in this example).
- Run the IPv4 private network protocol on PC 1 and PC 2. Make them interconnected in terms of IPv4 private network through the public network.
- Specify Switch A as the default gateway for PC 1. Specify Switch C as the default gateway for PC 2.

Figure 12-1 GRE networking



Configuration steps

Step 1 Configure IP addresses of physical interfaces.

Configure Switch A.

```
Raisecom#configure
Raisecom(config)#vlan 10,30
Raisecom(config)# interface ge 1/0/1
Raisecom (config-ge-1/0/1)# port hybrid vlan 10 untagged
Raisecom (config-ge-1/0/1)# port hybrid pvid 10
Raisecom(config)# interface ge 1/0/3
Raisecom (config-ge-1/0/3)# port hybrid vlan 30 untagged
Raisecom (config-ge-1/0/3)# port hybrid pvid 30
Raisecom (config)#int vlan 10
Raisecom (config-vlanif-10)#ip address 20.1.1.1/24
Raisecom (config)#int vlan 30
Raisecom (config-vlanif-30)#ip address 10.1.1.2/24
```

Configure Switch B.

```
Raisecom#configure
Raisecom(config)#vlan 10,20
Raisecom(config)# interface ge 1/0/1
Raisecom (config-ge-1/0/1)# port hybrid vlan 10 untagged
Raisecom (config-ge-1/0/1)# port hybrid pvid 10
Raisecom(config)# interface ge 1/0/2
Raisecom (config-ge-1/0/2)# port hybrid vlan 20 untagged
Raisecom (config-ge-1/0/2)# port hybrid pvid 20
Raisecom (config)#int vlan 10
Raisecom (config-vlanif-10)#ip address 20.1.1.2/24
Raisecom (config)#int vlan 20
Raisecom (config-vlanif-30)#ip address 30.1.1.2/24
```

Configure Switch C.

```
Raisecom#configure
Raisecom(config)#vlan 20,30
Raisecom(config)# interface ge 1/0/2
Raisecom (config-ge-1/0/2)# port hybrid vlan 20 untagged
Raisecom (config-ge-1/0/2)# port hybrid pvid 20
Raisecom(config)# interface ge 1/0/3
Raisecom (config-ge-1/0/3)# port hybrid vlan 30 untagged
Raisecom (config-ge-1/0/3)# port hybrid pvid 30
Raisecom (config)#int vlan 20
Raisecom (config-vlanif-20)#ip address 30.1.1.2/24
Raisecom (config)#int vlan 30
Raisecom (config-vlanif-30)#ip address 10.2.1.2/24
```

Step 2 Configure OSPF among these devices.

Configure Switch A.

```
Raisecom#configure
```

```
Raisecom(config)#ospf 1
Raisecom(config-ospf-1)#network 20.1.1.0 255.255.255.0 area 0
```

Configure Switch B.

```
Raisecom#configure
Raisecom(config)#ospf 1
Raisecom(config-ospf-1)#network 20.1.1.0 255.255.255.0 area 0
Raisecom(config-ospf-1)#network 30.1.1.0 255.255.255.0 area 0
```

Configure Switch C.

```
Raisecom#configure
Raisecom(config)#ospf 1
Raisecom(config-ospf-1)#network 30.1.1.0 255.255.255.0 area 0
```

Step 3 Configure the Tunnel interface.

Configure Switch A.

```
Raisecom#configure
Raisecom(config)#interface tunnel 1
Raisecom(config-tunnel-1)#tunnel-protocol gre
Raisecom(config-tunnel-1)#ip address 40.1.1.1/24
Raisecom(config-tunnel-1)#source 20.1.1.1
Raisecom(config-tunnel-1)#destination 30.1.1.2
```

Configure Switch B.

```
Raisecom#configure
Raisecom(config)#interface tunnel 1
Raisecom(config-tunnel-1)#tunnel-protocol gre
Raisecom(config-tunnel-1)#ip address 40.1.1.2/24
Raisecom(config-tunnel-1)#source 30.1.1.2
Raisecom(config-tunnel-1)#destination 20.1.1.1
```

Step 4 After configurations are complete, the status of the Tunnel interface becomes Up. This indicates that the Tunnel is established.

Step 5 Configure the static route.

Configure Switch A.

```
Raisecom#configure
Raisecom(config)#ip route-static 10.2.1.0 255.255.255.0 interface tunnel
1
```

Step 6 After configurations are complete, PC 1 can ping through PC 2.

Checking results

Use the show interface tunnel 1 command to show the status and statistics of the Tunnel interface.

```
Raisecom#configure
Raisecom(config)#show interface tunnel 1
Interface tunnel 1 information :
-----
Description:
Admin state: up, Operation state: up, MTU: 9216, Pmtu: n/a
Tunnel source is 20.1.1.1,destination is 30.1.1.2
Vpn name is public
Tunnel protocol/transport GRE/IPV4,key disable
keepalive disable
Checksumming of packets disable
Tunnel tos not set
Tunnel ttl not set
Last 300 seconds input rate: 0 bytes/sec, 0 packets/sec, 0 bits/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec, 0 bits/sec
Input peak rate: 0 bytes/sec, 0 packets/sec, Record time: ----
Output peak rate: 0 bytes/sec, 0 packets/sec, Record time: ----

Input: 0 bytes, 0 packets
  Unicast      : 0          , Multicast      : 0
  Broadcast    : 0          , Jumbo          : 0
  CRC          : 0          , Giants         : 0
  Jabbers      : 0          , Fragments      : 0
  Runt         : 0          , DropEvents     : 0
  Alignments   : 0          , Symbols        : 0
  Ignoreds     : 0          , Frames         : 0
  Discard      : 0          , Error          : 0
  Pause        : 0
  64 octets    : 0          , 65-127 octets  : 0
  128-255 octets : 0        , 256-511 octets : 0
  512-1023 octets : 0        , 1024-1518 octets : 0

Output: 0 bytes, 0 packets
  Unicast      : 0          , Multicast      : 0
  Broadcast    : 0          , Jumbo          : 0
  Collisions    : 0          , Deferreds      : 0
  Late Collisions : 0        , Excess Collisions : 0
  Buffers Purged : 0          , Discard        : 0
  Error         : 0          , Pause          : 0
  65-127 octets : 0          , 64 octets      : 0
  256-511 octets : 0          , 128-255 octets : 0
```


512-1023 octets : 0 , 1024-1518 octets : 0

13 Appendix

This chapter lists terms, acronyms, and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

13.1 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 on the network. With DAI, the administrator can intercept, record, and discard ARP packets with invalid MAC address/IP address to prevent common ARP attacks.
Dynamic Host Configuration Protocol (DHCP)	A technology used for assigning IP address dynamically. It can automatically assign IP addresses for all clients on the network to reduce workload of the administrator. In addition, it can implement centralized management of IP addresses.

E

Ethernet in the First Mile (EFM)	Complying with IEEE 802.3ah protocol, EFM is a link-level Ethernet OAM technology. It provides the link connectivity detection, link fault monitoring, and remote fault notification for a link between two directly-connected devices. EFM is mainly used for the Ethernet link on edges of the network accessed by users.
Ethernet Ring Protection Switching (ERPS)	It is an APS protocol based on ITU-T G.8032 standard, which is a link-layer protocol specially used for the Ethernet ring. In normal conditions, it can avoid broadcast storm caused by the data loop on the Ethernet ring. When the link or device on the Ethernet ring fails, services can be quickly switched to the backup line to enable services to be recovered in time.

F

Full duplex	In a communication link, both parties can receive and send data concurrently.

G

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 on the network. Therefore, the devices can provide different applications based on a unified time. In addition, NTP can ensure a very high accuracy with an error of 10ms or so.

O

Open Shortest Path First (OSPF)	An internal gateway dynamic routing protocol, which is used to determine the route in an Autonomous System (AS)

Optical Distribution Frame (ODF)	A distribution connection device between the fiber and a communication device. It is an important part of the optical transmission system. It is mainly used for fiber splicing, optical connector installation, fiber adjustment, additional pigtail storage, and fiber protection.

P

Password Authentication Protocol (PAP)	PAP is an authentication protocol that uses a password in Point-to-Point Protocol (PPP). It is a twice handshake protocol and transmits unencrypted user names and passwords over the network. Therefore, it is considered 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 on the network. RADIUS works in client/server mode. The RADIUS server is responsible for receiving users' connection requests, authenticating users, and replying configurations required by all clients to provide services for users.

S

Simple Network Management Protocol (SNMP) A network management protocol defined by Internet Engineering Task Force (IETF) used to manage devices in the Internet. SNMP can make the network management system to remotely manage all network devices that support SNMP, including monitoring network status, modifying network device configurations, and receiving network event alarms. At present, SNMP is the most widely-used network management protocol in the TCP/IP network.

Simple Network Time Protocol (SNTP) SNTP is mainly used for synchronizing time of devices on the network.

Single-Mode Fiber (SMF) In this fiber, single-mode optical signals are transmitted.

Spanning Tree Protocol (STP) STP can be used to eliminate network loops and back up link data. It blocks loops in logic to prevent broadcast storms. When the unblocked link fails, the blocked link is re-activated to act as the backup link.

V

Virtual Local Area Network (VLAN)	VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segments logically rather than physically, thus implementing multiple virtual work groups which are based on Layer 2 isolation and do not affect each other.
VLAN mapping	VLAN mapping is mainly used to replace the private VLAN Tag of the Ethernet service packet with the ISP's VLAN Tag, making the packet transmitted according to ISP's VLAN forwarding rules. When the packet is sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Thus, the packet is sent to the destination correctly.

13.2 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

