www.raisecom.com

RAX721 (P200R003) Configuration Guide (Rel_01)

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

Website: http://www.raisecom.com

Tel: 8610-82883305

Fax: 8610-82883056

Email: export@raisecom.com

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

Postal code: 100094

Notice

Copyright © **2024**

Raisecom

All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in Writing from **Raisecom Technology Co., Ltd.**

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

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

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

Preface

Objectives

This document introduces features and related configurations supported by the RAX721, including basic principles and configuration procedures of IP routing, clock synchronization, MPLS, VPN, Ethernet, multicast, QoS, OAM, security, and system configurations. In addition, this document provides related configuration examples. The appendix provides terms, acronyms, and abbreviations involved in this guide.

This document helps you master principles and configurations of the RAX721 systematically, as well as networking with the RAX721.

Versions

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

Product name	Product version	Chassis version
RAX721-A	P200R003	B.00 or later
RAX721-A-XF	P200R003	B.00 or later
RAX721-B	P200R003	A.00 or later
RAX721-B-T	P200R003	A.01 or later
RAX721-C-2C24	P200R003	A.00 or later

Conventions

Symbol conventions

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

Symbol	Description
	Indicate a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.

Copyright © Raisecom Technology Co., Ltd.

Symbol	Description
	Indicate a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
	Provide additional information to emphasize or supplement important points of the main text.
	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	Names of files, directories, folders, and users are in **boldface**. For example, log in as user **root**.
Italic	Book titles are in *italics*.
`Lucida Console`	Terminal display is in `Lucida Console`.
Book Antiqua	Heading 1, Heading 2, Heading 3, and Block are in Book Antiqua.

Command conventions

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. Only 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.

Copyright © Raisecom Technology Co., Ltd.

Convention	Description
[x | y | ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. A minimum of none or a maximum of all can be selected.

Configuration mode prompt conventions

Convention	Description
/*	Indicate the interface ID/slot ID. For example, "Raisecom(config-eth/1)" indicates Ethernet interface 1 and "Raisecom(config-slot/4)" indicates slot 4.
/*/*	The first "/*" indicates the slot ID and the second "/*" indicates the interface ID. For example, "Raisecom(config-eth/1/1)" indicates Ethernet interface 1 of slot 1.

Interface type and value range conventions

Format	Description
interface-type	Interface type, with the following values: • vlan: VLAN interface • loopback: loopback interface • tunnel: tunnel interface • gigaethernet/tengigabitethernet: 1GE/10GE interface; layer 2 physical interface, layer 3 physical interface, and sub-interface • fastethernet: out-of-band network management interface • port-channel: LAG interface and its sub-interface
interface-number	Interface ID, with the values depending on device models and interface types: • vlan: 1–4094 • loopback: 1–1024 • tunnel: 1/1/1–1/1/20000 • hundredgige: 1/1/1–1/1/4 (application to the RAX721-C-2C24) • tengigabitethernet: 1/1/1–1/1/4 (application to the RAX721-A, RAX721-B, RAX721-A-XF, and RAX721-B-T) • tengigabitethernet: 1/2/1–1/2/24 (application to the RAX721-A-XF and RAX721-C-2C24) • gigaethernet: 1/2/1–1/2/24 (application to the RAX721-A) • gigaethernet: 1/2/1–1/2/48 (application to the RAX721-B and RAX721-B-T) • fastethernet: 1/0/1 • port-channel: 1–64

Copyright © Raisecom Technology Co., Ltd.

Interface configuration mode conventions

In screen outputs described in this document, we use `Raisecom(config-port)` to indicate that we have entered interface configuration mode.

However, based on the interface type, the actual screen outputs are in the form of `Raisecom(config-`*interface-type interface-number*`)`. The *interface-type* and *interface-number* parameters indicate the interface type and interface ID. For details about interface types and interface IDs, see interface type and value range conventions.

Actual screen outputs are shown as below.

Screen outputs in configuration modes of interfaces	Description
`Raisecom(config-fastethernet`*unit/slot/port*`)#`	Enter out-of-band interface configuration mode. The interface ID is in form of *unit/slot/port*, such as Raisecom(config-fastethernet1/2/1)#.
`Raisecom(config-gigaethernet`*unit/slot/port*`)#`	Enter Gigabit Ethernet interface configuration mode. The interface ID is in form of *unit/slot/port*, such as Raisecom(config-gigaethernet1/2/1)#.
`Raisecom(config-gigaethernet`*unit/slot/port.sub*`)#`	Enter Gigabit Ethernet sub-interface configuration mode. The interface ID is in form of *unit/slot/port.sub*, such as Raisecom(config-gigaethernet1/2/1.1)#.
`Raisecom(config-tengigabitethernet`*unit/slot/port*`)#`	Enter 10GE interface configuration mode. The interface ID is in form of *unit/slot/port*, such as Raisecom(config-gigaethernet1/1/1)#.
`Raisecom(config-tengigabitethernet`*unit/slot/port.sub*`)#`	Enter 10GE interface configuration mode. The interface ID is in form of *unit/slot/port.sub*, such as Raisecom(config-gigaethernet1/1/1.1)#.
`Raisecom(config-vlan`*port*`)#`	Enter VLAN interface configuration mode. The interface ID is an integer, such as Raisecom(config-vlan1)#.
`Raisecom(config-port-channel`*port*`)#`	Enter aggregation group interface configuration mode. The interface ID is an integer, such as Raisecom(config-port-channel1)#.
`Raisecom(config-port-channel`*port.sub*`)#`	Enter aggregation group sub-interface configuration mode. The interface ID is in form of *port.sub*, such as Raisecom(config-port-channel1.1)#.
`Raisecom(config-tunnel`*unit/slot/port*`)#`	Enter tunnel interface configuration mode. The interface ID is in form of *unit/slot/port*, such as Raisecom(config-tunnel1/1/1)#.

Copyright © Raisecom Technology Co., Ltd.

Screen outputs in configuration modes of interfaces	Description
`Raisecom(config-loopback`*port*`)#`	Enter loopback interface configuration mode. The interface ID is an integer, such as Raisecom(config-loopback1)#.

Change history

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

Issue 01 (2024-06-30)

Initial commercial release

Copyright © Raisecom Technology Co., Ltd.

Contents

1 Basic configurations 1
1.1 CLI 1
1.1.1 Overview 1
1.1.2 Levels 2
1.1.3 Modes 2
1.1.4 Shortcut keys 6
1.1.5 Acquiring help 7
1.2 Connecting device and login 9
1.2.1 Connecting device 9
1.2.2 Accessing device through Console interface 11
1.2.3 Accessing device through Telnet 12
1.2.4 Accessing device through SSHv2 14
1.3 Network management IP zero-configuration 16
1.3.1 Preparing for configurations 16
1.3.2 (Optional) configuring zero-configuration 16
1.3.3 (Optional) configuring zero-configuration polling 17
1.3.4 (Optional) configuring relay 17
1.3.5 Checking configurations 18
1.4 Backup and upgrade 18
1.4.1 Introduction 18
1.4.2 Backing up system 20
1.4.3 Copying files 20
1.4.4 Upgrading system 21
1.4.5 Checking configurations 21
1.5 Network management 21
1.5.1 Introduction 21
1.5.2 Preparing for configurations 23
1.5.3 Confiurating SNMP basic functions 23
1.5.4 Configuring Trap 24
1.5.5 Configuring KeepAlive Trap packets 25
1.5.6 Checking configurations 26
1.6 Configuring RMON 26

Copyright © Raisecom Technology Co., Ltd.

1.6.1 Introduction 26
1.6.2 Preparing for configurations 26
1.6.3 Configuring RMON alarm group 27
1.6.4 Configuring RMON event group 27
1.6.5 Configuring RMON statistics 27
1.6.6 Configuring RMON history statistics 27
1.6.7 Checking configurations 28
1.7 Configuration examples 28
1.7.1 Example for logging in to the device through Console interface 28
1.7.2 Example for logging in to device through Telnet 29
1.7.3 Example for logging in to device through SSHv2 30
1.7.4 Example for logging in to device through ACL 31
1.7.5 Example for upgrading system software (in privileged EXEC mode) 32
2 System management 35
2.1 User management 35
2.1.1 Configuring user management 36
2.1.2 Checking configurations 36
2.2 Device management 36
2.2.1 Fan management 36
2.2.2 Checking configurations 36
2.3 Saving configurations 36
2.4 Time management 37
2.4.1 Configuring time and time zone 37
2.4.2 Configuring DST 37
2.4.3 Configuring NTP/SNTP 38
2.4.4 Checking configurations 39
2.5 Log management 39
2.5.1 Basic configurations 39
2.5.2 Configuring log discriminator 40
2.5.3 Configuring log storage 40
2.5.4 Checking configurations 41
2.5.5 Maintenance 41
2.6 File management 41
2.6.1 Managing configuration files 41
2.7 Alarm management 41
2.7.1 Introduction 41
2.7.1 Configuring alarm inhibition 44
2.7.2 Configuring alarm delay 44
2.7.3 Configuring alarm storage modes 44
2.7.4 Clearing alarms 45
2.7.5 Configuring alarm reporting 45

Copyright © Raisecom Technology Co., Ltd.

2.7.6 Configuring alarm inverse 45
2.7.7 Configuring alarm monitoring 45
2.7.8 Configuring alarm output 46
2.7.9 Checking configurations 46
2.8 Key chain management 47
2.8.1 Introduction 47
2.8.2 Configuring key chain 47
2.8.3 Checking configurations 47
2.9 Performance statistics 48
2.9.1 Introduction 48
2.9.2 Preparing for configurations 48
2.9.3 Default configurations of performance statistics 48
2.9.4 Configuring performance statistics 49
2.9.5 Checking configurations 49
2.9.6 Maintenance 49
2.10 Remote device management 49
3 Interface management 51
3.1 Basic configurations of interface 51
3.1.1 Configuring basic information of interface 51
3.1.2 Configuring interface working mode 52
3.1.3 Configuring Ethernet interface mode 52
3.1.4 Configuring interface Jumboframe 52
3.1.5 Configuring MTU of interface 53
3.1.6 Configuring interface flapping suppression 53
3.1.7 Configuring MAC address of interface 54
3.2 Configuring Ethernet interface 54
3.3 Configuring Ethernet sub-interface 55
3.4 Configuring VLAN interface 55
3.5 Configuring optical module DDM 56
3.5.1 Preparing for configurations 56
3.5.2 Enabling optical module DDM 56
3.5.3 Checking configurations 56
3.6 Configuring loopback interface 57
3.7 Configuring out-of-band network management interface 57
3.7.1 Preparing for configurations 57
3.7.2 Configuring IP address of out-of-band network interface 57
3.8 Checking configurations 58
4 Ethernet 59
4.1 Configuring VLAN 59
4.1.1 Preparing for configurations 59
4.1.2 Configuring VLAN properties 60

Copyright © Raisecom Technology Co., Ltd.

4.1.3 Configuring VLANs based on Access interface 60
4.1.4 Configuring VLANs based on Trunk interface 61
4.1.5 Configuring VLAN based on MAC address 62
4.1.6 Configuring VLAN based on IP subnet 62
4.1.7 Configuring VLAN based on protocol 63
4.1.8 Checking configurations 63
4.2 Configuring PVLAN 63
4.2.1 Preparing for configurations 63
4.2.2 Configuring PVLAN type 64
4.2.3 Associating PVLAN 64
4.2.4 Checking configurations 64
4.3 Configuring MAC address table 65
4.3.1 Preparing for configurations 65
4.3.2 Configuring static MAC address table 65
4.3.3 Configuring dynamic MAC address table 65
4.3.4 Configuring blackhole MAC address 66
4.3.5 Configuring suppression of MAC address flapping 66
4.3.6 Checking configurations 66
4.4 Configuring QinQ 67
4.4.1 Preparing for configurations 67
4.4.2 Configuring basic QinQ 67
4.4.3 Configuring selective QinQ 68
4.4.4 Checking configurations 69
4.5 Configuring LLDP 69
4.5.1 Preparing for configurations 69
4.5.2 Enabling global LLDP 70
4.5.3 Enabling interface LLDP 70
4.5.4 Configuring LLDP basic functions 70
4.5.5 Configuring LLDP to send TLV packets 71
4.5.6 Configuring LLDP Trap 71
4.5.7 Checking configurations 72
4.6 Configuring loop detection 72
4.6.1 Preparing for configurations 72
4.6.2 Configuring loop detection 72
4.6.3 Checking configurations 73
4.6.4 Maintenance 73
4.7 Configuring L2CP 73
4.7.1 Preparing for configurations 73
4.7.2 Configuring L2CP to transparently transmit packets based on MAC address 74
4.7.3 Configuring L2CP profile 74
4.7.4 Applying L2CP profile to interface 74
4.7.5 Checking configurations 75

Copyright © Raisecom Technology Co., Ltd.

4.7.6 Maintenance 75
4.8 Configuring GARP/GVRP 75
4.8.1 Preparing for configurations 75
4.8.2 Default configurations 76
4.8.3 Configuring GARP basic functions 76
4.8.4 Configuring GVRP 76
4.8.5 Checking configurations 77
4.8.6 Maintenance 77
4.9 Configuring STP/RSTP 77
4.9.1 Preparing for configurations 77
4.9.2 Default configurations 78
4.9.3 Enabling STP 78
4.9.4 Configuring STP parameters 78
4.9.5 (Optional) configuring RSTP edge interface 79
4.9.6 (Optional) configuring RSTP link type 80
4.9.7 Checking configurations 80
4.9.8 Example for configuring STP 80
4.10 Configuring MSTP 83
4.10.1 Preparing for configurations 83
4.10.2 Default configurations 83
4.10.3 Enabling MSTP 84
4.10.4 Configuring MST region and its maximum number of hops 84
4.10.5 Configuring root/backup bridge 85
4.10.6 Configuring interface priority and system priority 86
4.10.7 Configuring network diameter for switch network 87
4.10.8 Configuring internal path cost of interface 87
4.10.9 Configuring external path cost of interface 88
4.10.10 Configuring maximum transmission rate on interface 88
4.10.11 Configuring MSTP timer 89
4.10.12 Configuring edge interface 90
4.10.13 Configuring BPDU filtering 90
4.10.14 Configuring BPDU Guard 91
4.10.15 Configuring STP/RSTP/MSTP/MRSTP mode switching 91
4.10.16 Configuring link type 92
4.10.17 Configuring root interface protection 92
4.10.18 Configuring interface loopguard 93
4.10.19 Configuring port TC packet suppression 93
4.10.20 Configuring TC protection 94
4.10.21 Checking configurations 94
4.10.22 Maintenance 95
4.11 Configuring interface protection 95
4.11.1 Preparing for configurations 95

Copyright © Raisecom Technology Co., Ltd.

4.11.2 Default configurations 95
4.11.3 Configuring interface protection 96
4.11.4 Checking configurations 96
4.12 Configuration examples 96
4.12.1 Example for configuring MAC table 96
4.12.2 Example for configuirng VLAN 98
4.12.3 Example for configuring basic QinQ 100
4.12.4 Example for configuring interface protection 102
5 Clock synchronization 105
5.1 Configuring SyncE-based clock synchronization 105
5.1.1 Preparing for configurations 105
5.1.2 Configure the clock source of SyncE 105
5.1.3 Manually selecting SyncE clock source 106
5.1.4 Checking configurations 106
6 IP services 107
6.1 Configuring IPv4 107
6.1.1 Preparing for configurations 107
6.1.2 Configuring IPv4 address on interface 107
6.1.3 Checking configurations 108
6.2 Configuring IPv6 108
6.2.1 Preparing for configurations 108
6.2.2 Configuring IPv6 basic functions 108
6.2.3 Checking configurations 109
6.3 Configuring basic properties of management packets 109
6.3.1 Preparing for configurations 109
6.3.2 Configuring management packets 109
6.4 Configuring ARP 110
6.4.1 Preparing for configurations 110
6.4.2 Configuring static ARP 110
6.4.3 Configuring dynamic ARP 110
6.4.4 Configuring proxy ARP 111
6.4.5 Clearing ARP entries 111
6.4.6 Checking configurations 112
6.5 Configuring NDP 112
6.5.1 Preparing for configurations 112
6.5.2 Configuring static NDP entries 112
6.5.3 Configuring dynamic NDP entries 112
6.5.4 Configuring proxy NDP 114
6.6 Configuring ND Snooping 115
6.6.1 Preparing for configurations 115
6.6.2 Default configurations 115

Copyright © Raisecom Technology Co., Ltd.

6.6.3 Configuring ND Snooping 115
6.6.4 Checking configurations 115
6.6.5 Maintenance 116
6.7 Configuring ICMP 116
6.7.1 Configuring IPv4 ICMP 116
6.7.2 Configuring IPv6 ICMP 117
6.7.3 Checking configurations 117
6.8 Configuring fault detection 118
6.8.1 PING 118
6.8.2 Traceroute 119
6.9 Configuring DNS 120
6.9.1 Configuring IPv4 DNS 120
6.9.2 Configuring IPv6 DNS 120
6.9.3 Checking configurations 120
6.9.4 Maintenance 120
6.10 Configuration examples 121
6.10.1 Example for configuring ARP 121
7 DHCP 123
7.1 Configuring DHCPv4 Server 123
7.1.1 Preparing for configurations 123
7.1.2 Creating and configuring IPv4 address pool 123
7.1.3 Configuring DHCP v4 Server on interface 124
7.1.4 Configuring trusted DHCP Relay server 124
7.1.5 Managing lease files 125
7.1.6 Checking configurations 125
7.2 Configuring DHCPv4 Client 125
7.2.6 Checking configurations 127
7.3 Configuring DHCPv4 Relay 127
7.3.1 Preparing for configurations 127
7.3.2 Configuring global DHCPv4 Relay 127
7.3.3 Configuring DHCPv4 relay on interface 128
7.3.4 Configuring DHCPv4 relay Option 82 128
7.3.5 Checking configurations 128
7.4 Configuring DHCPv4 Snooping 129
7.4.1 Preparing for configurations 129
7.4.2 Configuring DHCPv4 Snooping 129
7.4.3 Configuring DHCPv4 Snooping Option 82 130
7.4.4 Checking configurations 130
7.5 Configuring DHCPv4 Option 130
7.5.1 Preparing for configurations 130
7.5.2 Configuring IPv4 DHCP Option 82 131

Copyright © Raisecom Technology Co., Ltd.

7.5.3 Configuring IPv4 DHCP Option 61 131
7.5.4 Configuring IPv4 self-defined DHCP Option 131
7.5.5 Checking configurations 132
7.6 Configuring DHCPv6 Snooping 132
7.6.1 Preparing for configurations 132
7.6.2 Configuring DHCPv6 Snooping 132
7.6.3 Checking results 133
8 IP routing 134
8.1 Configuring routing management 134
8.1.1 Configuring routing management 134
8.1.2 Configuring flow table 134
8.1.3 Configuring IP FRR 135
8.1.4 Checking configurations 135
8.2 Configuring static route 136
8.2.1 Preparing for configurations 136
8.2.2 Configuring IPv4 static route 136
8.2.3 Configuring IPv6 static route 137
8.2.4 Configuring BFD for static routes 137
8.2.5 Checking configurations 138
8.3 Configuring routing policy 139
8.3.1 Configuring IPv4 routing policy 139
8.3.2 Configuring IPv6 routing policy 142
8.3.3 Checking configurations 143
8.4 Configuring OSPFv2 144
8.4.1 Configuring OSPF basic functions 144
8.4.2 Configuring OSPF route properties 145
8.4.3 Configuring OSPF network type 147
8.4.4 Configuring OSPF area 148
8.4.5 Configuring load balancing 149
8.4.6 Maximizing LSA metric 149
8.4.7 Optimizing OSPF network 150
8.4.8 Configuring OSPF authentication policy 154
8.4.9 Controlling OSPF redistributed routes 155
8.4.10 Configuring OSPF routing policy 156
8.4.11 Configuring BFD for OSPF 158
8.4.12 Configuring OSPF for MPLS-TE 159
8.4.13 Checking configurations 159
8.4.14 Maintenance 160
8.5 Configuring OSPFv3 160
8.5.1 Starting OSPFv3 process 160
8.5.2 Configuring OSPFv3 network type 161

Copyright © Raisecom Technology Co., Ltd.

8.5.3 Configuring OSPFv3 area 161
8.5.4 Configuring OSPFv3 interface 162
8.5.5 Controlling OSPFv3 redistributed routes 163
8.5.6 Configuring timer of OSPFv3 packets 164
8.5.7 Configuring OSPFv3 route management 165
8.5.8 Configuring OSPFv3 routing policy 169
8.5.9 Maximizing LSA metric 171
8.5.10 Configuring BFD for OSPFv3 171
8.5.11 Checking configurations 172
8.5.12 Maintenance 172
8.6 Configuring ISIS 173
8.6.1 Configuring ISIS basic functions 173
8.6.2 Configuring ISIS routing attributes 173
8.6.3 Configuring ISIS network 175
8.6.4 Optimizing ISIS network 176
8.6.5 Configure ISIS authentication 178
8.6.6 Controlling ISIS routing information 178
8.6.7 Configuring ISIS BFD 180
8.6.8 Configuring ISIS GR 181
8.6.9 Configuring ISIS TE 181
8.6.10 Checking configurations 181
8.6.11 Maintenance 182
8.7 Configuring ISISv6 182
8.7.1 Configuring ISISv6 basic functions 182
8.7.2 Configuring ISISv6 authentication 183
8.7.3 Configuring ISISv6 route selection parameters 184
8.7.4 Controlling ISISv6 routing information 185
8.7.5 Configuring ISISv6 load balancing 187
8.7.6 Configuring ISISv6 BFD 187
8.7.7 Checking configurations 187
8.7.8 Maintenance 188
8.8 Configuring BGP 188
8.8.1 Configuring BGP basic functions 188
8.8.2 Configuring BGP redistributed routes 192
8.8.3 Configuring BGP to redistribute routes 193
8.8.4 Configuring BGP routing attributes 195
8.8.5 Configuring BGP network 199
8.8.6 Configuring BGP GR 204
8.8.7 Configuring BGP FRR 205
8.8.8 Configuring BFD for BGP 205
8.8.9 Configuring BGP authentication 206
8.8.10 Checking configurations 207

Copyright © Raisecom Technology Co., Ltd.

8.8.11 Maintenance 207
8.9 Configuring BGP4+ 208
8.9.1 Configuring BGP4+ basic functions 208
8.9.2 Configuring BGP4+ advertised routes 210
8.9.3 Configuring BGP4+ redistributed routes 210
8.9.4 Configuring BGP4+ route attributes 211
8.9.5 Configuring BGP4+ network 212
8.9.6 Configuring BGP4+ authentication 214
8.9.7 Checking configurations 214
8.9.8 Maintenance 214
8.10 Configuring RIP 214
8.10.1 Configuring RIP basic functions 214
8.10.2 Configuring RIP version 215
8.10.3 Redistributing external routes 215
8.10.4 Configuring timer 216
8.10.5 Configuring loop suppression 216
8.10.6 Configuring RIP authentication 217
8.10.7 Configuring routing policy 217
8.10.8 Configuring route preference 218
8.10.9 Checking configurations 218
8.11 Configuring RIPng 218
8.11.1 Configuring RIPng basic functions 218
8.11.2 Controlling routing information 219
8.11.3 Configuring timer 220
8.11.4 Configuring loop suppression 220
8.11.5 Configuring RIPng authentication 221
8.11.6 Configuring routing policy 221
8.11.7 Configuring route preference 221
8.11.8 Configuring route summarization 222
8.11.9 Checking configurations 222

9 MPLS 223

9.1.1 Preparing for configurations 223
9.1.2 Configuring MPLS basic functions 223
9.1.3 Checking configurations 224
9.2 Configuring MPLS Tunnel 224
9.2.1 Configuring MPLS Tunnel basic functions 224
9.2.2 Configuring MPLS Tunnel policy 226
9.2.3 Configuring hot backup of the tunnel 226
9.2.4 Configuring tunnel label recording 227
9.2.5 Configuring tunnel re-optimization 227
9.2.6 Checking configurations 227

Copyright © Raisecom Technology Co., Ltd.

9.3.1 Preparing for configurations 228
9.3.2 Configuring static unidirectional LSP with IP capability 228
9.3.3 Configuring static unidirectional LSP without IP capability 228
9.3.4 Configuring static bidirectional LSP with IP capability 229
9.3.5 Configuring static bidirectional LSP without IP capability 230
9.3.6 Checking configurations 231
9.4.1 Preparing for configurations 232
9.4.2 Configuring global LDP 232
9.4.3 Configuring LDP on interface 232
9.4.4 Configuring LDP remote session 233
9.4.5 Configuring LDP MD5 233
9.4.6 Configuring LDP policy 234
9.4.7 Configuring BFD for TLDP 234
9.4.8 Configuring LDP FRR 234
9.4.9 Checking configurations 235
9.4.10 Maintenance 236
9.5.1 Preparing for configurations 236
9.5.2 Enabling RSVP-TE 236
9.5.3 Configuring RSVP-TE authentication 237
9.5.4 Configuring CSPF 237
9.5.5 Configuring explicit path and Tunnel 239
9.5.6 Configuring TE protection 239
9.5.7 Configuring BFD for RSVP-TE 241
9.5.8 Checking configurations 242
9.6.1 Preparing for configurations 242
9.6.2 Configuring MPLS Tunnel fault acknowledgment 243
9.6.3 Configuring MPLS Tunnel fault location 243
9.7 Configuration examples 243
9.7.1 Example for configuring static bidirectional LSP with IP capability 243
9.7.2 Example for configuring dynamic LSP based on LDP 249
9.7.3 Example for configuring dynamic LSP based on RSVP-TE 252

10 Segment Routing 256

10.1 Configuring ISIS to additionally support SR 256
10.2 Configuring OSPFv2 to additionally support SR 257
10.3 Configuring OSPFv3 to additionally support SR 258
10.4 Configuring SR-MPLS 259
10.4.1 Preparing for configurations 259
10.4.2 Configuring SR-MPLS BE 259
10.4.3 Configuring SR-MPLS TE 260
10.5 Configuring SRv6 263
10.5.1 Configuring SRv6 BE 263

Copyright © Raisecom Technology Co., Ltd.

10.5.2 Configuring SRv6 TE Policy 263
10.5.3 Configuring SRv6 compression 264
10.5.4 Checking results 265
10.6 Configuring SRv6 network slicing 266
10.6.1 Configuring basic information about network slicing 266
10.6.2 Configuring the network slicing instance 266
10.6.3 Configuring the prefix of network slicing 266
10.6.4 Configuring network slicing on the interface 267
10.6.5 Checking configurations 267
10.7 Configuration examples 267
10.7.1 Example for configuring EVPN VPWS for SRv6-TE Policy 267
11 VPN 275
11.1.1 Preparing for configurations 275
11.1.2 Configuring static L2VC 277
11.1.3 Configuring dynamic L2VC 279
11.1.4 Configuring MS-PW 281
11.1.5 (Optional) configuring BFD for PW 282
11.1.6 Checking configurations 283
11.2 Configuring CCC L2VPN 283
11.2.1 Preparing for configurations 283
11.2.2 Configuring CCC 285
11.2.3 Checking configurations 285
11.3.1 Preparing for configurations 286
11.3.2 Configuring VSI 286
11.3.3 Configuring VPLS traffic label 289
11.3.4 Checking configurations 290
11.4.1 Preparing for configurations 290
11.4.2 Configuring VRF basic attributes 291
11.4.3 Binding VRF with interfaces 291
11.4.4 Configuring public routes 291
11.4.5 Configuring public Tunnel 292
11.4.6 Configuring MP-IBGP peer 292
11.4.7 Configuring PE-CE route switching 293
11.4.8 Checking configurations 296
11.5 Configuring MPLS VPN fault detection 297
11.5.1 Preparing for configuration 297
11.5.2 Configuring MPLS VPN fault acknowledgement 297
11.5.3 Configuring MPLS VPN fault location 297
11.6 Configuring EVPN 298
11.6.1 Preparing for configurations 298
11.6.2 Configuring basic properties of EVPN 298

Copyright © Raisecom Technology Co., Ltd.

11.6.3 Configuring MP-BGP to advertise EVPN routes 298
11.6.4 Configuring EVPN VPWS 299
11.6.5 Configuring EVPN VPLS 301
11.6.6 Configuring EVPN L3VPN 301
11.7 Configuring the VPN tunnel policy 302
11.7.1 Preparing for configurations 302
11.7.2 Configuring VPN tunnel policy 302
11.8 Maintenance 303
11.9 Configuration examples 304
11.9.1 Example for configuring static Tunnel to carry static VPWS services 304
11.9.2 Example for configuring RSVP-TE-based static Tunnel to carry dynamic VPWS services 307
11.9.3 Example for configuring MPLS L2VPN typical networking 311
11.9.4 Examples for configuring MPLS L3VPN typical networking 322
11.9.5 Configuring EVPN VPWS for SR-MPLS BE 331

12 QoS 339

12.1 Configuring ACL 339
12.1.1 Preparing for configurations 339
12.1.2 Configuring ACL 339
12.1.3 Configuring filter 343
12.1.4 Checking configurations 343
12.2 Configuring priority trust and priority mapping 343
12.2.1 Preparing for configurations 343
12.2.2 Configuring priority trust 344
12.2.3 Configuring DSCP-to-local priority mapping 344
12.2.4 Configuring CoS-to-local priority mapping 345
12.2.5 Configuring the ToS-to-local priority mapping 345
12.2.6 Configuring Exp-to-local priority mapping 345
12.2.7 Configuring local-to-DSCP priority mapping 346
12.2.8 Configuring local-to-ToS priority mapping 346
12.2.9 Configuring CoS priority remarking 346
12.2.10 Configuring local-to-Exp priority mapping 347
12.2.11 Checking configurations 347
12.3 Configuring traffic classification and traffic policy 348
12.3.1 Preparing for configurations 348
12.3.2 Creating and configuring traffic classification 348
12.3.3 Creating and configuring traffic policing profile 349
12.3.4 Creating and configuring traffic policy 349
12.3.5 Checking configurations 350
12.4 Configuring congestion avoidance and queue shaping 351
12.4.1 Preparing for configurations 351
12.4.2 Configuring WRED profile 351

Copyright © Raisecom Technology Co., Ltd.

12.4.3 Configuring flow queue profile 352
12.4.4 Configuring queue shaping 352
12.4.5 Checking configurations 352
12.5 Configuring interface rate limiting 353
12.5.1 Preparing for configurations 353
12.5.2 Configuring interface-based rate limiting 353
12.5.3 Checking configurations 353
12.6 Configuring hierarchical bandwidth rate limiting 354
12.6.1 Preparing for configurations 354
12.6.2 Configuring bandwidth assurance 354
12.6.3 Configuring hierarchical bandwidth assurance 354
12.6.4 Checking configurations 355
12.7 Configuring MPLS QoS 356
12.7.1 Configuring Tunnel QoS 356
12.7.2 Configuring PW QoS 356
12.7.3 Configuring VPLS QoS 357
12.7.4 Checking configurations 357
12.8 Configuring L3VPN QoS 357
12.8.1 Preparing for configurations 357
12.8.2 Configuring VRF QoS 357
12.8.3 Checking configurations 358
12.9 Configuring HQoS 358
12.9.1 Configuring the HQoS profile 358
12.9.2 Configuring the HQoS user or user group profile 358
12.9.3 Configuring the HQoS queue profile 359
12.9.4 Applying the HQoS profile to the interface 359
12.9.5 Checking configurations 359
12.10 Maintenance 360
12.11 Configuration examples 360
12.11.1 Example for configuring rate limiting based on traffic policy 360
12.11.2 Example for configuring queue scheduling and congestion avoidance 364
12.11.3 Example for configuring interface-based rate limiting 368

13 Multicast 370

13.1 Configuring IGMP 370
13.1.1 Preparing for configurations 370
13.1.2 Configuring Layer 2 IGMP 371
13.1.3 Configuring Layer 3 IGMP 371
13.1.4 Configuirng IGMP proxy 372
13.1.5 Configuring static group members 372
13.1.6 Querying IGMP packets 372
13.1.7 Configuring robustness coefficient 373

Copyright © Raisecom Technology Co., Ltd.

13.1.8 Configure the time for querying the last member 373
13.1.9 Configuring the maximum query response time 373
13.1.10 Configuring immediate leave of multicast members 373
13.1.11 Configuring IGMP SSM Mapping 374
13.1.12 Configuring IGMP multicast VLAN copy 374
13.1.13 Configuring packet track 374
13.1.14 Checking configurations 375
13.1.15 Maintenance 375
13.2 Configuring IGMP MVR 375
13.2.1 Preparing for configurations 375
13.2.2 Default configurations of IGMP MVR 376
13.2.3 Configuring IGMP MVR 376
13.2.4 Checking configurations 377
13.3 Configuring IGMP filtering 378
13.3.1 Preparing for configurations 378
13.3.2 Default configurations of IGMP filtering 378
13.3.3 Enabling IGMP filtering globally 378
13.3.4 Configuring IGMP filtering template 379
13.3.5 Configuring maximum number of groups 379
13.3.6 Checking configurations 380
13.4 Configuring PIM 380
13.4.1 Preparing for configurations 380
13.4.2 Enabling PIM 380
13.4.3 Configuring PIM domain DR election 381
13.4.4 Configuring PIM domain RP election 381
13.4.5 Configuring PIM multicast source 382
13.4.6 Switching from RPT to SPT 383
13.4.7 Configuring PIM GR 384
13.4.8 Checking configurations 384
13.4.9 Maintenance 385
13.5 Configuring multicast VPN 385
13.5.1 Preparing for configurations 385
13.5.2 Configuring the mLDP P2MP tunnel 385
13.5.3 Configuring mLDP In-Band MVPN 386
13.6 Configuration examples 386
13.6.1 Example for applying IGMP filtering to interface 386
13.6.2 Example for configuring IGMP MVR 388
14 OAM 391
14.1 Configuring EFM 391
14.1.1 Preparing for configurations 391
14.1.2 Configuring EFM basic functions 392

Copyright © Raisecom Technology Co., Ltd.

14.1.3 Configuring EFM active functions 392
14.1.4 Configuring EFM passive functions 393
14.1.5 Configuring link monitoring and fault indication 394
14.1.6 Checking configurations 395
14.2 Configuring CFM 396
14.2.1 Preparing for configurations 396
14.2.2 Enabling CFM 396
14.2.3 Configuring CFM basic functions 397
14.2.4 Configuring fault detection 398
14.2.5 Configuring fault acknowledgement 398
14.2.6 Configuring fault location 399
14.2.7 Configuring Ethernet signal lock 400
14.2.8 Configuring AIS 400
14.2.9 Configuring CSF 401
14.2.10 Configuring LM statistics 402
14.2.11 Configuring performance monitoring 402
14.2.12 Checking configurations 402
14.3 Configuring BFD 403
14.3.1 Preparing for configurations 403
14.3.2 Configuring BFD for IPv4 403
14.3.3 Configuring BFD for PW 405
14.3.4 Configuring BFD for VRF 406
14.3.5 Configuring BFD for LAG member interfaces 406
14.3.6 Configuring BFD Trap 407
14.3.7 Configuring SBFD 407
14.3.8 Checking configurations 407
14.4 Configuring SLA 408
14.4.1 Preparing for configurations 408
14.4.2 Configuring Y.1731-based SLA 409
14.4.3 Configuring SLA operation scheduling 409
14.4.4 Configuring SLA archive 410
14.4.5 Configuring iOAM 410
14.4.6 Checking configurations 411
14.5 Configuring MPLS-TP OAM 411
14.5.1 Preparing for configurations 411
14.5.2 Enabling MPLS-TP CFM 412
14.5.3 Configuring MPLS-TP CFM 412
14.5.4 Configuring MPLS-TP fault detection 413
14.5.5 Configuring MPLS-TP fault acknowledgement 414
14.5.6 Configuring MPLS-TP fault location 414
14.5.7 Configuring MPLS-TP AIS 415
14.5.8 Configuring MPLS-TP CSF 415

Copyright © Raisecom Technology Co., Ltd.

14.5.9 Configuring MPLS-TP LCK 416
14.5.10 Configuring basic information about MPLS-TP SLA operations 416
14.5.11 Configuring SLA scheduling information and enabling operation scheduling 417
14.5.12 Configuring fault relay based on association of MPLS-TP OAM and BFD alarms 417
14.5.13 Checking configurations 418
14.6 Configuring RFC2544 418
14.6.1 Configuring type of test packets 418
14.6.2 Configuring RFC2544 delay test 419
14.6.3 Configuring RFC2544 packet loss test 419
14.6.4 Configuring RFC2544 throughput test 419
14.6.5 Configuring RFC2544 performance test 420
14.6.6 Configuring RFC2544 operation scheduling 420
14.6.7 Checking configurations 421
14.7 Configuring Y.1564 421
14.7.1 Configuring service throughput test operation 421
14.7.2 Configuring service performance test operation 424
14.7.3 Configuring Y.1564 operation recognition 426
14.7.4 Configuring Y.1564 operation scheduling 426
14.7.5 Checking configurations 427
14.8 Configuring SLA test alarm 427
14.9 Configuring interface loopback 428
14.9.1 Preparing for configurations 428
14.9.3 Configuring loopback duration 429
14.9.4 Checking configurations 429
14.10 Configuring smart probe 430
14.10.1 Preparing for configurations 430
14.10.2 Configuring smart probe TCP channel 430
14.10.3 Configuring the uploading of smart probe operation 430
14.10.4 Checking configurations 431
14.11 Configuring ULDP 431
14.11.1 Preparing for configurations 431
14.11.2 Default configurations of ULDP 431
14.11.3 Configuring ULDP 431
14.11.4 Checking configurations 432
14.12 Configuring Traceroute 432
14.12.1 Preparing for configurations 432
14.12.2 Configuring Traceroute 432
14.13 Configuring PING 433
14.13.1 Preparing for configurations 433
14.13.2 PING IPv4 network 433
14.13.3 PING IPv6 network 434
14.13.4 PING MPLS network 434

Copyright © Raisecom Technology Co., Ltd.

14.13.5 PING DHCP Server 434
14.13.6 PING the SR network 435
14.14 Maintenance 435
15 Security 436
15.1 Configuring AAA 436
15.1.1 Preparing for configurations 436
15.1.2 Default configurations 437
15.1.3 Configuring AAA 437
15.1.4 Configuring RADIUS 438
15.1.5 Configuring TACACS+ 439
15.1.6 Checking configurations 440
15.1.7 Maintenance 440
15.2 Configuring storm control 441
15.2.1 Preparing for configurations 441
15.2.2 Configuring storm control 441
15.2.3 Checking configurations 441
15.3 Configuring CPU protection 442
15.3.1 Preparing for configurations 442
15.3.2 Configuring global CPU CAR 442
15.3.3 Clearing statistics 442
15.3.4 Checking configurations 442
15.4 Configuring CPU monitoring 443
15.4.1 Preparing for configurations 443
15.4.2 Configuring CPU monitoring alarm 443
15.5 Configuring port mirroring 443
15.5.1 Preparing for configurations 443
15.5.2 Configuring port mirroring 444
15.5.3 Configuring RSPAN 444
15.5.4 Checking configurations 445
15.6 Configuring attack prevention 445
15.6.1 Preparing for configurations 445
15.6.2 Enabling attack prevention 445
15.6.3 Configuring prevention against traffic attacks 446
15.7 Configuring ARP attack prevention 447
15.7.1 Preparing for configurations 447
15.7.2 Default configurations 448
15.7.3 Configuring ARP attack prevention 448
15.7.4 Checking configurations 449
15.8 Configuring dynamic ARP inspection 449
15.8.1 Preparing for configurations 449
15.8.2 Configuring trusted interface of dynamic ARP inspection 449

Copyright © Raisecom Technology Co., Ltd.

15.8.3 Configuring static binding of dynamic ARP inspection 449
15.8.4 Configuring dynamic binding of dynamic ARP inspection 450
15.8.5 Configuring protection VLAN of dynamic ARP inspection 450
15.8.6 Checking configurations 451
15.9 Configuring URPF 451
15.9.1 Preparing for configurations 451
15.9.2 Configuring URPF 451
15.9.3 Checking configurations 451
15.10 Configuring 802.1x 452
15.10.1 Preparing for configurations 452
15.10.2 Default configurations 452
15.10.3 Configuring basic functions of 802.1x 453
15.10.4 Configuring 802.1x re-authentication 454
15.10.5 Configuring 802.1x timer 454
15.10.6 Checking configurations 454
15.10.7 Maintenance 455
15.11 Configuring password management 455
15.11.1 Preparing for configurations 455
15.11.2 Configuring MD5 encryption keys 455
15.11.3 Checking configurations 455
15.12 Configuration examples 456
15.12.1 Example for configuring port mirroring 456
15.12.2 Example for configuring RADIUS 457
15.12.3 Example for configuring 802.1x 459
16 Reliability 461
16.1 Configuring link aggregation 461
16.1.1 Preparing for configurations 461
16.1.2 Configuring manual link aggregation 462
16.1.3 Configuring static LACP link aggregation 462
16.1.4 Configuring manual backup link aggregation 464
16.1.5 Configuring static LACP active/standby link aggregation 465
16.1.6 Checking configurations 466
16.2 Configuring interface backup 466
16.2.1 Preparing for configurations 466
16.2.2 Configuring interface backup group 466
16.2.3 Checking configurations 467
16.3 Configuring PW redundancy 468
16.3.1 Preparing for configurations 468
16.3.2 Configuring PW redundancy 468
16.3.3 Configuring VPLS PW Redundancy 469
16.3.4 Checking configurations 469

Copyright © Raisecom Technology Co., Ltd.

16.4 Configuring VRRP 470
16.4.1 Preparing for configurations 470
16.4.2 Creating and enabling VRRP 470
16.4.3 Configuring VRRP backup group 470
16.4.4 Configuring VRRP Ping 471
16.4.5 Configuring VRRP Trap 471
16.4.6 Configuring VRRP monitoring interface 472
16.4.7 Configuring BFD for VRRP 472
16.4.8 Checking configurations 472
16.4.9 Maintenance 473
16.5 Configuring VRRPv3 473
16.5.1 Preparing for configurations 473
16.5.2 Default configurations 473
16.5.3 Creating and enabling VRRPv3 474
16.5.4 Configuring VRRPv3 backup group 474
16.5.5 Configuring VRRPv3 PING 475
16.5.6 Configuring VRRPv3 Trap 475
16.5.7 Configuring VRRPv3 monitoring interface 475
16.5.8 Configuring BFD for VRRPv3 476
16.5.9 Checking configurations 476
16.5.10 Maintenance 476
16.6 Configuring ERPS 477
16.6.1 Preparing for configurations 477
16.6.2 Creating ERPS protection ring 477
16.6.3 (Optional) creating ERPS protection tributary ring 479
16.6.4 Configuring ERPS fault detection modes 480
16.6.5 (Optional) configuring ERPS switching control 481
16.6.6 Checking configurations 481
16.6.7 Maintenance 482
16.7 Configuring MPLS linear protection 482
16.7.1 Preparing for configurations 482
16.7.2 Configuring MPLS linear protection switching 482
16.7.3 Checking configurations 483
16.8 Configuring HA hot backup 484
16.8.1 Preparing for configurations 484
16.8.2 Configuring HA switching 484
16.8.3 Checking configurations 484
16.9 Configuring EVPL dual-homing protection 484
16.9.1 Preparing for configurations 484
16.9.2 Configuring mLACP link aggregation 485
16.9.3 Configuring EVPL dual-homing 486
16.10 Maintenance 486

Copyright © Raisecom Technology Co., Ltd.

16.11 Configuration examples 486
16.11.1 Example for configuring VRRP single backup group 486
16.11.2 Example for configuring VRRP multiple backup groups 489
17 Appendix 493
17.1 Terms 493
17.2 Acronyms and abbreviations 495

Copyright © Raisecom Technology Co., Ltd.

Figures

Figure 1-1 Direct connection 10
Figure 1-2 USB connection 10
Figure 1-3 Out-of-band network management 10
Figure 1-4 Configuring parameters for Hyper Terminal 12
Figure 1-5 Working as the Telnet server 13
Figure 1-6 Working as the Telnet client 14
Figure 1-7 Logging in to the RAX721 through Console interface 28
Figure 1-8 Logging in to the RAX721 through Telnet 30
Figure 1-9 Managing device through SSHv2 31
Figure 1-10 Telneting to the RAX721 based on ACL 32
Figure 1-11 System software upgrade 33
Figure 4-1 STP networking 81
Figure 4-2 Networking for MAC application 97
Figure 4-3 Networking for VLAN application 98
Figure 4-4 Networking for basic QinQ 100
Figure 4-5 Interface protection networking 103
Figure 6-1 Proxy ARP application scenario 111
Figure 6-2 Configuring ARP 121
Figure 9-1 Networking for configuring bidirectional static LSP 244
Figure 9-2 Data preparation 244
Figure 9-3 Networking for configuring LDP LSP 249
Figure 9-4 Networking for configuring RSVP-TE LSP 252
Figure 10-1 Configuring EVPN VPWS for SRv6-TE 268
Figure 11-1 CCC local connection 283
Figure 11-3 Configuring static Tunnel to carry static VPWS services 304
Figure 11-4 Data preparation 304

Copyright © Raisecom Technology Co., Ltd.

Figure 11-5 Configuring RSVP-TE-based static Tunnel to carry dynamic VPWS services 308
Figure 11-6 Configuring MPLS L2VPN services 311
Figure 11-7 Configuring L3VPN networking 323
Figure 11-8 Configuring EVPN VPWS for SR-BE 332
Figure 12-1 Configuring rate limiting based on traffic policy 361
Figure 12-2 Configuring queue scheduling networking 364
Figure 12-3 Configuring interface-based rate limiting 369
Figure 13-1 IGMP MVR application 376
Figure 13-2 Applying IGMP filtering to the interface 387
Figure 13-3 IGMP MVR networking 389
Figure 15-1 Configuring port mirroring 456
Figure 15-2 RADIUS application 457
Figure 15-3 802.1x networking 459
Figure 16-1 VRRP single backup group networking 487
Figure 16-2 VRRP multiple backup groups networking 489

Copyright © Raisecom Technology Co., Ltd.

1 Basic configurations

This chapter describes basic information and configuration procedures of the RAX721, as well as related configuration examples, including following sections:

- CLI
- Connecting device and login
- Network management IP zero-configuration
- Backup and upgrade
- Network management
- Configuring RMON
- Configuration examples

1.1 CLI

1.1.1 Overview

The Command Line Interface (CLI) is a medium for you to communicate with the RAX721. You can configure, monitor, and manage the RAX721 through the CLI.

You can log in to the RAX721 through the terminal equipment or through a computer that runs the terminal emulation program. Enter commands at the system prompt.

The CLI supports the following features:

- Configure the RAX721 locally through the Console interface.
- Configure the RAX721 locally or remotely through Telnet/Secure Shell v2 (SSHv2).
- Commands are classified into different levels. You can execute the commands that correspond to your level only.
- The commands available to you depend on which mode you are currently in.
- Shortcut keys can be used to execute commands.
- Check or execute a historical command by checking command history. The last 20 historical commands can be saved on the RAX721.
- Enter a question mark (?) at the system prompt to obtain online help.
- The RAX721 supports multiple intelligent analysis methods, such as fuzzy match and context association.

Copyright © Raisecom Technology Co., Ltd.

1.1.2 Levels

The RAX721 classifies commands into 16 levels in a descending order:

- 0–4: checking level. You can execute basic commands, such as clear and history, for clearing system information and showing command history.
- 5–10: monitoring level. You can execute commands, such as show, for system maintenance.
- 11–14: configuration level. You can execute commands for configuring services, such as Virtual Local Area Network (VLAN) and Internet Protocol (IP) routing.
- 15: management level. You can execute commands for system running.

1.1.3 Modes

The command mode is an environment where a command is executed. A command can be executed in one or multiple certain modes. The commands available to you depend on which mode you are currently in.

After connecting the RAX721, if the RAX721 adopts default configurations, a Login prompt will be displayed. Enter the user name (raisecom) and password (raisecom) to enter the user EXEC mode, where the following command is displayed:

```
Raisecom>
```

Enter the **enable** command and press **Enter**. Then enter the correct password, and press **Enter** to enter privileged EXEC mode. The default password is **raisecom**.

```
Raisecom>enable
Password:
Raisecom#
```

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

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

- The CLI prompts Raisecom is a default host name. You can modify it by executing the hostname *string* command in privileged EXEC mode.
- Commands executed in global configuration mode can also be executed in other modes. The functions vary on command modes.
- You can enter the exit or quit command to return to the upper command mode. However, in privileged EXEC mode, you need to execute the disable command to return to user EXEC mode. In address family configuration mode, you need to execute the exit-address-family command to return to BGP configuration mode.

Copyright © Raisecom Technology Co., Ltd.

- You can enter the end command to return to privileged EXEC mode from any modes but user EXEC mode and privileged EXEC mode.

Command modes supported by the RAX721 are listed in the following table.

Mode	Entry	Prompt
User EXEC	Log in to the RAX721, and then enter the correct user name and password.	`Raisecom>`
Privileged EXEC	In user EXEC mode, use the **enable** command and correct password.	`Raisecom#`
Global configuration	In privileged EXEC mode, use the **config** command.	`Raisecom(config)#`
Interface configuration	In global configuration mode, use the **interface fastethernet 1/0/1** command.	`Raisecom(config-fastethernet1/0/1)#`
	In global configuration mode, use the **interface gigaethernet** *unit/slot/port* command.	`Raisecom(config-gigaethernetunit/slot/port)#`
	In global configuration mode, use the **interface tengigaethernet** *unit/slot/port* command.	`Raisecom(config-tengigaethernetunit/slot/port)#`
Sub-interface configuration	In global configuration mode, use the **interface gigaethernet** *unit/slot/port.sub-interface* command.	`Raisecom(config-gigaethernetunit/slot/port.subid)#`
VLAN interface configuration	In global configuration mode, use the **interface vlan** *vlan-id* command.	`Raisecom(config-vlanid)#`
Tunnel interface configuration	In global configuration mode, use the **interface tunnel** *tunnel-id* command.	`Raisecom(config-tunnelid)#`
Loopback interface configuration	In global configuration mode, use the **interface loopback** *interface-number* command.	`Raisecom(config-loopbackid)#`
VRF configuration	In global configuration mode, use the **ip vrf** *vrf-name* command.	`Raisecom(config-vrf)#`
Route mapping configuration	In global configuration mode, use the **route-map** *map-name* { **permit** | **deny** } *number* command.	`Raisecom(config-route-map)#`
OSPF configuration	In global configuration mode, use the **router ospf** *process-id* [**router-id** *router-id*] command.	`Raisecom(config-router-ospf)#`
OSPFv3 configuration	In global configuration mode, use the **ipv6 router ospf** *process-id* [**vrf** *vrf-name*] command.	`Raisecom(config-ospf6)#`
BGP configuration	In global configuration mode, use the **router bgp** [*as-id*] command.	`Raisecom(config-router)#`

Copyright © Raisecom Technology Co., Ltd.

Mode	Entry	Prompt
BGP VPNv4 address family configuration	In BGP configuration mode, use the **address-family vpnv4** [**unicast**] command.	`Raisecom(config-router-af)#`
BGP VPN instance IPv4 unicast address family configuration	In BGP configuration mode, use the **address-family ipv4 vrf** *vrf-name* command.	`Raisecom(config-router-af)#`
ILSP configuration	In global configuration mode, use the **mpls bidirectional static-lsp ingress** *lsp-name* **lsr-id** *egress-lsr-id* **tunnel-id** *tunnel-id* command.	`Raisecom(config-ingress-lsp)#`
ELSP configuration	In global configuration mode, use the **mpls bidirectional static-lsp egress** *lsp-name* **lsr-id** *ingress-lsr-id* **tunnel-id** *tunnel-id* command.	`Raisecom(config-egress-lsp)#`
TLSP configuration	In global configuration mode, use the **mpls bidirectional static-lsp transit** *lsp-name* **lsr-id** *ingress-lsr-id egress-lsr-id* **tunnel-id** *tunnel-id* [**standby**]] command.	`Raisecom(config-transit-lsp)#`
Explicit path configuration	In global configuration mode, use the **mpls explicit-path** *path-name* command.	`Raisecom(config-mpls-exp-path)#`
Tunnel policy configuration	In global configuration mode, use the **tunnel-policy** *policy-name* command.	`Raisecom(config-tunnelpolicy)#`
Remote peer configuration	In global configuration mode, use the **mpls ldp targeted neighbour** *ip-address* command.	`Raisecom(config-ldp-remote-peer)#`
VSI configuration	In global configuration mode, use the **mpls vsi** *vsi-name* **static** command.	`Raisecom(config-vsi)#`
VLAN configuration	In global configuration mode, use the **vlan** *vlan-id* command.	`Raisecom(config-vlan)#`
Basic IP ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. The *acl-number* parameter ranges from 1000 to 1999.	`Raisecom(config-acl-ipv4-basic)#`
Extended IP ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. The *acl-number* parameter ranges from 2000 to 2999.	`Raisecom(config-acl-ipv4-advanced)#`
MAC ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. The *acl-number* parameter ranges from 3000 to 3999.	`Raisecom(config-acl-mac)#`

Copyright © Raisecom Technology Co., Ltd.

Mode	Entry	Prompt
MPLS ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. The *acl-number* parameter ranges from 4000 to 4999.	`Raisecom(config-acl-mpls)#`
User ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. The *acl-number* parameter ranges from 5000 to 5999.	`Raisecom(config-acl-map)#`
cos-remark configuration	In global configuration mode, use the **mls qos mapping cos-remark** *profile-id* command.	`Raisecom(cos-remark)#`
cos-to-pri configuration	In global configuration mode, use the **mls qos mapping cos-to-local-priority** *profile-id* command.	`Raisecom(cos-to-pri)#`
dscp-mutation configuration	In global configuration mode, use the **mls qos mapping dscp-mutation** *profile-id* command.	`Raisecom(dscp-mutation)#`
dscp-to-pri configuration	In global configuration mode, use the **mls qos mapping dscp-to-local-priority** *profile-id* command.	`Raisecom(dscp-to-pri)#`
exp-to-pri configuration	In global configuration mode, use the **mls qos mapping exp-to-local-priority** *profile-id* command.	`Raisecom(exp-to-pri)#`
pri-to-exp configuration	In global configuration mode, use the **mls qos mapping local-priority-to-exp** *profile-id* command.	`Raisecom(pri-to-exp)#`
WRED profile configuration	In global configuration mode, use the **mls qos wred profile** *profile-id* command.	`Raisecom(wred)#`
Flow profile configuration	In global configuration mode, use the **mls qos flow-queue profile** command.	`Raisecom(flow-queue)#`
CMAP configuration	In global configuration mode, use the **class-map** *class-map-name* command.	`Raisecom(config-cmap)#`
Traffic monitoring profile configuration	In global configuration mode, use the **mls qos policer-profile** *policer-name* [**single**] command.	`Raisecom(traffic-policer)#`
PMAP configuration	In global configuration mode, use the **policy-map** *policy-map-name* command.	`Raisecom(config-pmap)#`
Traffic policy bound with traffic classification configuration	In PMAP configuration mode, use the **class-map** *class-map-name* command.	`Raisecom(config-pmap-c)#`

Copyright © Raisecom Technology Co., Ltd.

Mode	Entry	Prompt
Service instance configuration	In global configuration mode, use the **service** *instance-name* **level** *md-level* command.	`Raisecom(config-service)#`
BFD session configuration	In global configuration mode, use the **bfd** *session-id* command.	`Raisecom(config-bfd-session)#`
	In global configuration mode, use the **bfd** *session-id* **bind peer-ip** *ip-address* [**vrf-name** *vrf-name*] command.	
	In global configuration mode, use the **bfd** *session-id* **bind peer-ip** *ip-address* **interface gigaethernet** *interface-number* command.	

1.1.4 Shortcut keys

The RAX721 supports the following shortcut keys.

Shortcut key	Description
Press the up arrow (↑) key.	The previous command is displayed. If no previous command is available, no change is shown on the screen after you press the key.
Press the down arrow (↓) key.	The next command is displayed. If no previous command is available, no change is shown on the screen after you press the key.
Press the left arrow (←) key.	Move the cursor back one character. If the cursor is in front of the command, no change is shown on the screen after you press the key.
Press the right arrow (→) key.	Move the cursor forward one character. If the cursor is behind the command, no change is shown on the screen after you press the key.
Press the **Backspace** key.	Erase the character to the left of the cursor. If the cursor is in front of the command, no change is shown on the screen after you press the key.

Copyright © Raisecom Technology Co., Ltd.

Shortcut key	Description
Press the **Tab** key.	When you press it after entering an incomplete keyword, the system automatically executes some commands: • If the incomplete keyword matches a unique complete keyword, the unique complete keyword replaces the incomplete keyword, with the cursor forward a space from the unique complete keyword. • If the incomplete keyword matches more complete keywords, you can press the **Tab** key to alternate the matched complete keywords. • If the incomplete keyword matches no complete key word, you can press the **Tab** key to wrap, and then error information is displayed.
Press **Ctrl**+**A**.	Move the cursor to the beginning of the command line.
Press **Ctrl+D** or the **Delete** key.	Delete the character at the cursor.
Press **Ctrl**+**E**.	Move the cursor to the end of the command line.
Press **Ctrl**+**K**.	Delete all characters from the cursor to the end of the command line.
Press **Ctrl**+**X**.	Delete all characters from the cursor to the beginning of the command line.
Press **Ctrl**+**Z**.	Return to privileged EXEC mode from the current mode (excluding user EXEC mode).

1.1.5 Acquiring help

Complete help

You can acquire complete help under following three conditions:

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

```
Raisecom>?
```

The output is displayed as below:

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


Copyright © Raisecom Technology Co., Ltd.

```
  terminal  Configure terminal
```

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

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

The output is displayed as below:

```
access-list       Access list
acl              Access control list
alarm             Alarm
arp              ARP table information
banner            banner
bfd              Bidirectional Forwarding Detection
```

- After you enter a parameter, press the **Space bar** and enter a question mark (?), associated parameters and descriptions of these parameters are displayed if the question mark (?) matches a parameter.

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

The output is displayed as below:

```
<1-1024>  Tunnel interface number
```

Incomplete help

You can acquire incomplete help under following three conditions:

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

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

The output is displayed as below:

```
cfm         Connectivity fault management protocol
```


Copyright © Raisecom Technology Co., Ltd.

```
class-map   Set class map
clear       Clear screen
command-log  Log the command to the file
cpu         Configure cpu parameters
create      Create static VLAN
cspf        Cspf capability
```

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

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

The output is displayed as below:

```
license         license
link-aggregation  Link aggregation
```

- After you enter a partial command name and press the Tab, the full form of the keyword is displayed if there is a unique match command. Otherwise, after you press the Tab, different keywords will be displayed circularly and you can select one as required.

Error messages

The following table lists error messages that you may encounter while configure the RAX721 on the CLI.

Error message	Description
% Incomplete command.	The input command is incomplete.
Error input in the position market by '^'	The keyword marked with "^" is invalid or does not exist.

1.2 Connecting device and login

1.2.1 Connecting device

Users can log in to the device for configuration management through direct connection and network connection.

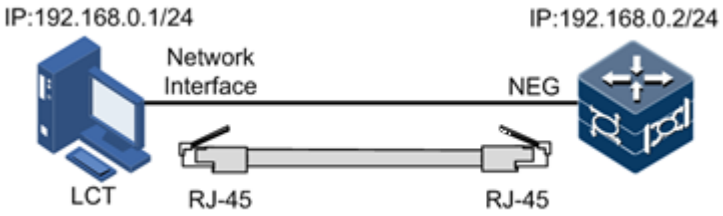
Direct connection

- Direction connection through a network cable

Copyright © Raisecom Technology Co., Ltd.

As shown in Figure 1-1, directly connect the NEG interface on the device to the network interface on the computer with a network cable, configure the device IP address and the computer IP address on the same network segment, and then start the terminal maintenance software on the computer to log in to the device for configuration management.

Figure 1-1 Direct connection



- Direct connection through a USB cable

As shown in Figure 1-2, use a USB cable to directly connect the Console interface on the device to the USB interface on the computer, start the terminal maintenance software on the computer, configure the serial port parameters, and log in to the device for configuration management. There is no need for configuring an IP address for this scenario.

Figure 1-2 USB connection

Network connection

The device supports out-of-band network management.

As shown in Figure 1-3, the device is connected to the DCN through the NEG interface, and the computer accesses the device management IP address through the DCN to configure and manage the device. Keep the route between the computer and the device available (the computer and device should be able to ping through each other) and then start the terminal maintenance software on the computer to log in to the device.

Figure 1-3 Out-of-band network management

Copyright © Raisecom Technology Co., Ltd.

1.2.2 Accessing device through Console interface

Note

- The Console interface of the RAX721 is a Universal Serial Bus (USB) A-shaped female interface, which is translated into a Universal Asynchronous Receiver/Transmitter (UART) in the device.
- Before logging in to the RAX721 through the USB interface, install the driver for converting the USB interface into the UART interface on the PC.
- Visit https://www.raisecom.com/sites/default/files/USBConsoleDriver.zip to download the driver.

The Console interface is an interface for directly configuring and managing the device, which is connected to the USB interface on the PC that runs the maintenance terminal software through a USB cable. You can configure and manage the RAX721 through this interface. This management method does not involve network communication.

You must log in to the RAX721 through the Console interface under the following 2 conditions:

- The RAX721 is powered on for the first time.
- You cannot log in to the RAX721 through Telnet.

To log in to the RAX721 through the Console interface, follow these steps:

Step 1 Use an USB configuration cable to connect the Console interface of the RAX721 with the USB interface of the PC.

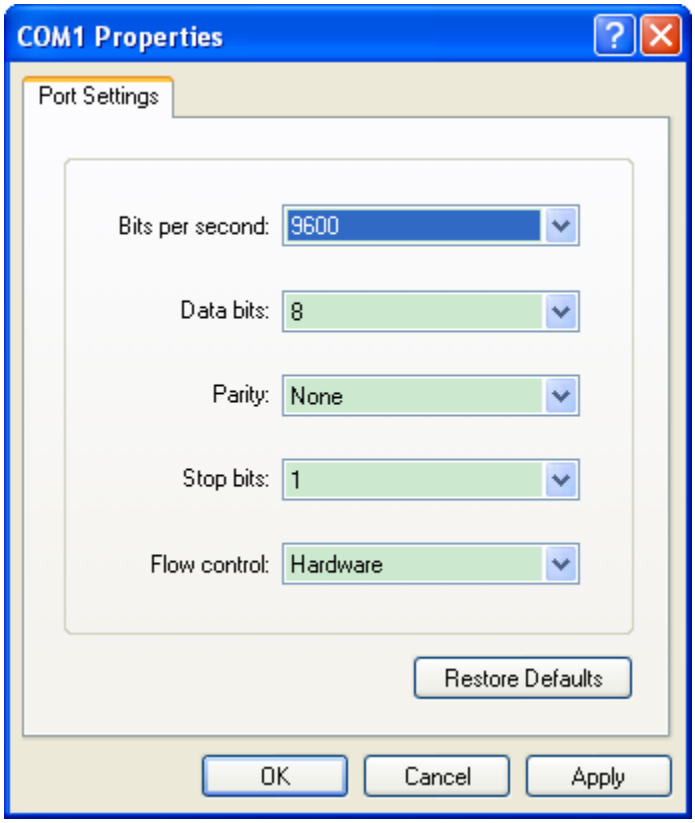
Step 2 Run the terminal maintenance program on the PC, such as Hyper Terminal on Microsoft Windows XP. Enter the connection name at the Connection Description dialog box and then click **OK**.

Step 3 Select COM N (N refers to the COM interface ID into which the USB interface is translated.) at the Connect To dialog box and then click **OK**.

Step 4 Configure parameters as shown in Figure 1-4 and then click **OK**

Copyright © Raisecom Technology Co., Ltd.

Figure 1-4 Configuring parameters for Hyper Terminal



Step 5 Enter the configuration interface and then enter the user name and password to log in to the RAX721. By default, both the user name and password are set to raisecom.

Note

Hyper Terminal is not available on Windows Vista or Windows 7 Operating System (OS). For these OSs, download Hyper Terminal package and install it.

1.2.3 Accessing device through Telnet

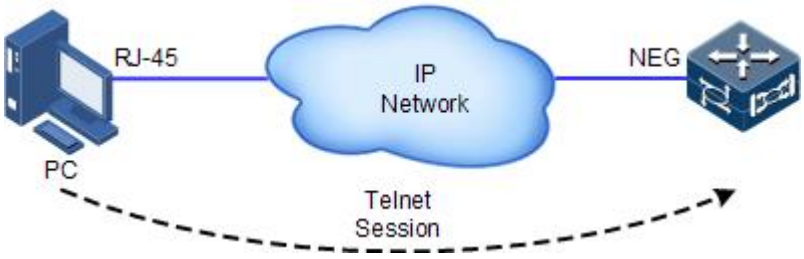
Through Telnet, you can remotely log in to the RAX721 through a PC. In this way, it is not necessary to prepare a PC for each RAX721.

The RAX721 provides the following Telnet services:

- Telnet Server: as shown in Figure 1-5, connect the PC and the RAX721 and ensure that the route between them is available. You can log in to and configure the RAX721 by running Telnet Client program on a PC.

Copyright © Raisecom Technology Co., Ltd.

Figure 1-5 Working as the Telnet server



Note

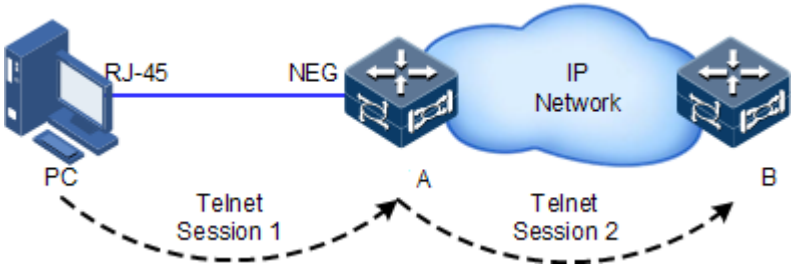
Before logging in to the RAX721 through Telnet, you must log in to the RAX721 through the Console interface and configure the IP address of the SNMP interface.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#telnet-server enable`	Start the Telnet server.
3	`Raisecom(config)#telnet-server port` *port-id* `[ confirm ]`	(Optional) configure the listen port ID of the Telnet server.
4	`Raisecom(config)#interface fastethernet 1/0/1`	Enter SNMP interface configuration mode.
5	`Raisecom(config-fastethernet1/0/1)#ip address` *ip-address* `[` *ip-mask* `]` `Raisecom(config-fastethernet1/0/1)#exit`	Configure the IP address of the SNMP interface and return to global configuration mode. By default, the IP address of the SNMP interface is 192.168.4.28.
6	`Raisecom(config)#telnet-server close terminal-telnet` *session-number*	(Optional) disconnect the specified Telnet connection.
7	`Raisecom(config)#telnet-server max-session` *session-number*	(Optional) configure the maximum number of Telnet connections supported by the device. By default, it is 10.
8	`Raisecom(config)#telnet-server access-list` *acl-number*	Configure ACL Telnet. **Note** You need to configure the ACL rules by using the **access-list** *acl-number* command and other related commands. For details, refer to section 12.1 Configuring ACL.
9	`Raisecom(config)#interface` *interface-type interface-number*	Enter physical interface configuration mode.
10	`Raisecom(config-port)#telnet-server accept`	Configure the interface to support Telnet.

- Telnet Client: after connecting the RAX721 through the terminal emulation program running on the PC, you can log in to another device by entering the telnet command and then configure and manage the device. As shown in Figure 1-6, device A works as both the Telnet Server and Telnet Client.

Copyright © Raisecom Technology Co., Ltd.

Figure 1-6 Working as the Telnet client



Step	Command	Description
1	`Raisecom#telnet` *ip-address* `[ port` port-id `]` `[ source-ip` *ip-address* `] [ vrf` *vrf-name* `]`	On the IPv4 network, log in to another device through Telnet.
2	`Raisecom#telnet` *ipv6-address* `[ port` port-id `]` `[ source-ip` *ipv6-address* `] [ vrf` *vrf-name* `]`	On the IPv6 network, log in to another device through Telnet.

Note

The RAX721 supports configuring the console terminal exit timeout in the privileged EXEC mode through the **terminal time-out** { **0** | *period* } command.
When you use the **terminal time-out** { **0** | *period* } command, the logged user's connection will not be terminated, so use this command with caution. This command may cause security problems (for example, when the maintenance personnel leave the server for a long time, other person may execute the operation incorrectly because the connection is not terminated due to timeout), cause the actual connections to reach the upper limit so that no new connection can be established.

1.2.4 Accessing device through SSHv2

Telnet is an authentication mode that is lack of security. In addition, it adopts Transmission Control Protocol (TCP) to transmit the password and data in clear text. It will cause malicious attack, such as Deny of Service (DoS), IP address spoofing, and route spoofing because only Telnet service is provided. With more attention is put on network security, the traditional modes (Telnet and FTP) for transmitting the password and data in clear text are not accepted gradually.

Secure Shell (SSH) is a protocol, which is used to provide secure remote login and other security network services in an insecure network. When you log in to a device in an insecure network environment, SSH will encrypt the data automatically when you transmit these data. When data is transmitted to the destination, the SSH will decrypt the data automatically. Therefore, SSH can provide secure information assurance. SSH can prevent devices from being attacked by clear text password intercepting and middleman, as well as prevent Domain Name Server (DNS) spoofing and IP spoofing. Because the transmitted data is compressed, the SSH can provide the greater transmission speed.

SSH adopts the client-server mode. The SSH server receives requests from SSH clients and then begin to authenticate them. After successful authentication, SSH connection is established. Therefore, you can log in to the SSH server through the SSH client. The authentication is a series of key processing actions performed between the server and client.

At present, SSH has a new version of SSHv2. The RAX721 supports SSHv2.

Copyright © Raisecom Technology Co., Ltd.

Before accessing the RAX721 through SSHv2, you must log in to the RAX721 through the Console interface and enable SSH service.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**generate ssh-key** *length*	Generate local SSHv2 key pair and designate its length.
3	Raisecom(config)#**ssh2 server**	Start the SSHv2 server.
4	Raisecom(config)#**ssh2 server authentication** { **dss** | **rsa** } *key-name* **public-key** [*public-key*]	(Optional) configure the public key of the SSHv2 client.
5	Raisecom(config)#**ssh2 server authentication** { **dss-key** | **password** | **rsa-key** }	(Optional) configure the SSHv2 authentication mode of the device.
6	Raisecom(config)#**ssh2 server authentication-timeout** *period*	(Optional) configure SSHv2 authentication timeout. The RAX721 refuses to authenticate and open the connection when client authentication time exceeds the upper threshold.
7	Raisecom(config)#**ssh2 server authentication-retries** *times*	(Optional) configure the allowable times for SSHv2 authentication failure. The RAX721 refuses to authenticate and open the connection when client authentication failure times exceed the upper threshold.
8	Raisecom(config)#**ssh2 server port** *port-id*	(Optional) configure the SSHv2 listening port ID. **Note** When configuring the SSHv2 listening port ID, the input parameter cannot take effect immediately without rebooting the SSHv2 service.
9	Raisecom(config)#**show ssh2** { **server** | **session** }	(Optional) show SSHv2 server or sessions.
10	Raisecom(config)#**show ssh2 public-key** [**authentication**]	(Optional) show the public key for SSHv2 on the device and client.

By using the RAX721 as an SSH client, log in to another device.

Step	Command	Description
1	Raisecom#**ssh** { *ip-address* / **dns** *dns-domain-name* } [**port** *port-id*] [**source-ip** *ip-address*] [**vrf** *vpn-instance-name*]	Log in to another device on the IPv4 network.
2	Raisecom#**ssh ipv6** { *ipv6-address* | **dns** *dns-domain-name* } [**port** *port-id*] [**source-ip** *ipv6-address*] [**vrf** *vpn-instance-name*]	Log in to another device on the IPv6 network.

Copyright © Raisecom Technology Co., Ltd.

1.3 Network management IP zero-configuration

1.3.1 Preparing for configurations

Scenario

A large number of remote devices are deployed and distributed widely at the end of the network and device provisioning is time-consuming and labor-intensive. The remote zero configuration function supports the automatic application of management IP address, management VLAN, default gateway and other network management parameters after the device is powered on, so that the device can be quickly managed by the NMS, improving the efficiency of device provisioning.

In general, if the central office equipment has been correctly configured with functions such as the DHCP server address pool, the remote equipment can be plugged and play without manual configuration.

When this device is used as a zero-configuration remote device and the network management parameters need to be modified, you can configure it according to the content of this section.

When implementing zero configuration based on DHCP, you can configure the automatically obtained IP address on the Loopback 1 interface of the remote device, and the remote device can borrow the interface IP address to be managed by the NMS.

Prerequisite

- The central office device has been configured with the DHCPv4 Server address pool function. For specific configuration, refer to section 7.1 Configuring DHCPv4 Server.
- All interfaces of the local device are not configured with management VLAN.
- The status of the uplink interface of the local device is UP.

1.3.2 (Optional) configuring zero-configuration

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip dhcp client mode { zeroconfig | normal }`	Configure the device as a zero-configuration remote device or an ordinary DHCP client. By default, the device is in zero configuration mode. **Caution** After the device obtains network management parameters in zero configuration mode and completes the service configuration, in principle, you cannot modify the mode to the normal DHCP client mode.
3	`Raisecom(config)#interface interface-type interface-number`	Enter Layer 3 physical interface configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-port)#**ip address dhcp** [**server-ip** *ip-address*]	Enable zero configuration on the device, and at the same time, you can specify the IP address of the central office DHCP server. If the user specifies the IP address of the DHCP server, only the IP address assigned by the specified server will be obtained.
5	Raisecom(config-port)#**ip dhcp client** { **class-id** *class-id* | **client-id** *client-id* | **hostname** *host-name* }	Configure the DHCP Client information of the device, including the host name, Class ID, and Client ID. The packets sent by the client will carry the information.

Note

- If the local device has obtained an IP address through DHCP, regardless of whether the default gateway is successfully configured, the local device is considered to have successfully obtained an IP address.
- The IP address automatically obtained through DHCP can be overwritten by the manually configured IP address under the same interface. The interface can be a Layer 3 physical interface, sub-interface or VLAN interface.
- You can manually configure the IP addresses based on Layer 3 physical interfaces, sub-interfaces, VLAN interfaces, or Layer 3 Trunk ports.

1.3.3 (Optional) configuring zero-configuration polling

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp client zeroconfig polling period** *min*	Configure the zero-configuration remote polling cycle, which is in units of minute. The polling cycle ranges from 0 to 1440. By default, the remote polling cycle of zero configuration is 120min.

1.3.4 (Optional) configuring relay

The local device can be connected to the secondary remote device. After the first-level remote device obtains the IP address through zero configuration, you can enable Relay on the downstream interface connected to the second-level remote device to realize the zero configuration of the second-level remote device.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp relay**	Enable global DHCP Relay.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode. **Note** • The interface is the downlink interface connected to the second-level remote device. • You need to configure an IP address for the interface.
4	Raisecom(config-port)#**ip dhcp relay**	Enable interface DHCP Relay.
5	Raisecom(config-port)#**ip dhcp relay target-ip** *ip-address*	(Optional) you can configure the destination IP address, which is the IP address of the DHCP Server.

1.3.5 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show ip dhcp client**	Show information about DHCP client and the automatically obtained information.

1.4 Backup and upgrade

1.4.1 Introduction

The RAX721 uses the file system to manage system files. The file system is used to create, delete, and modify files and directories.

System files refer to files required for operating the RAX721, including the BootROM file, License file, Paf file, log file, configuration file, and system software. Based on the download location, these files are saved to the memory of the NXU card or service card.

System file

System files refer to the software and files required for operating the RAX721, including the BootROM file, system configuration file, system startup file and FPGA file. These files are saved to the memory of the RAX721.

File management includes backup, update, load and deletion of files.

System Bootrom file

The system Bootrom file (BootROM software) is used to boot the device. After the device is powered on, the BootROM software is running to initialize the RAX721. You can upgrade the BootROM software if a new version is available.

Copyright © Raisecom Technology Co., Ltd.

System startup file

The system startup file is used to start and operate the RAX721, support normal operating, and implement functions.

You can upgrade the system startup file if a new version is available. In addition, to prevent a system fault, you can back up the system startup file.

The RAX721 supports 2 sets of system startup software simultaneously, providing primary and secondary switching between dual systems.

PAF file

PAF is used to control functions and specifications of the device. The PAF file defines all specification parameters supported by the device. It is able to confirm specifications supported by the device according to the parameter range.

After configuring parameters is complete, you could download parameters to the device through the **download** command and reboot the RAX721 through the **reboot** command. Then the RAX721 will take effect.

Other functions of the PAF file are as below:

- Support customizing the default IP address of the NMS interface.
- Support the naming convention of the product version, such as "product version.paf" for the PAF file.

System configuration file

The system configuration file (with the .conf as the suffix) is configuration items to be loaded when the device is booted at this time or next time.

After being powered on, the RAX721 reads the configuration file from the memory for initialization. If there is no configuration file in the memory, the RAX721 will use the default configuration file.

Configuration parameters in the configuration file are divided into the following 2 types:

- Configuration parameters used for initialization are startup configurations.
- Configuration parameters used when a device is running properly are running configurations.

You can modify running configurations through CLI. To make these modified running configurations as startup configurations when the RAX721 is powered on next time, you should save running configurations to the memory (by using the **write** command) as a configuration file.

Operations on the system configuration file include loading, upgrading, backing up, and deleting the system configuration file.

Backup

Backup means saving system files by copying them from the device memory and save them into the server memory to recover files if the RAX721 fails. By doing so, the RAX721 will run normally as before. The pervious system file should be restored under the following conditions:

Copyright © Raisecom Technology Co., Ltd.

- System files are lost or damaged due to the device fault.
- The device fails due to failure in system upgrade.

The RAX721 supports backing up system configuration files, system startup files, and system log files.

Upgrade

After features are added or known bugs are fixed, a new software version will be released. Then you can upgrade the software.

The RAX721 supports 2 upgrade modes:

- TFTP upgrade in BootROM mode
- SFTP/FTP/TFTP upgrade in system configuration mode

1.4.2 Backing up system

You need to establish a SFTP/FTP/TFTP environment before backing up system files. Generally, you can use a PC to serve as the FTP/TFTP server and the RAX721 as the client, with the basic requirements as below:

- Connect the RAX721 to the PC through the NEG interface.
- Configure the IP address of the PC to interconnect with the RAX721.

Step	Command	Description
1	Raisecom# upload { **accident-logfile** | **alarm-logfile** | **all-logfile** | **command-logfile** | **backup-config** | **dhcplease** | **dhcpsnooping-binding** | file | **paf** | **running-config** | **running-logfile** | **startup-config** } { **ftp** *ip-address username password* | **ftp-active** *ip-address username password* | **tftp** *ip-address file-name* | **sftp** *ip-address user-name password* } [**slot** *slot-id*] [**source** *source-address*] [**vrf** *vrf-name*] *file-name* [*directory*]	Upload the system configuration files, log files, and operation files to the backup server.

1.4.3 Copying files

Step	Command	Description
1	Raisecom#**copy backup-config startup-config**	Copy the backup configuration file to the primary configuration file.
2	Raisecom#**copy startup-config backup-config**	Copy the primary configuration file to the backup configuration file.

Copyright © Raisecom Technology Co., Ltd.

1.4.4 Upgrading system

Upgrading files in privileged EXEC mode

You need to establish a SFTP/FTP/TFTP environment before upgrading system files. Generally, you can use a PC to serve as the SFTP/FTP/TFTP server and the RAX721 to be the client, with the basic requirements as below:

- Connect the RAX721 to the PC through the NEG interface.
- Configure the IP address of the PC to interconnect with the RAX721.

Step	Command	Description
1	Raisecom# **download** { **system1** | **system2** | **bootstrap** | **cpld** | **dhcplease** | **dhcpsnooping-binding** | **startup-config** | **backup-config** | **paf** | **file** } { **ftp** *ip-address username password* | **ftp-active** *ip-address username password* | **tftp** *ip-address* | **sftp** *ip-address user-name password* } [**slot** *slot-id*] [**source** *source-address*] [**vrf** *vrf-name*] *filename* [*directory*]	Download system files to the device or service card.
2	Raisecom#**boot next-startup** { **system1** | **system2** }	Specify the next bootstrap file for the device. The device supports dual systems (active and standby) for backup.
3	Raisecom#**reboot** [**now** | **in** *delayed-time*]	Restart the device. The device will automatically load the downloaded system startup file.
4	Raisecom#**show version**	Show the device version.

1.4.5 Checking configurations

No.	Command	Description
1	Raisecom#**show version**	Show the version.
2	Raisecom#**show running-config**	Show system configurations.
3	Raisecom#**show startup-config**	Show initial configuration files.

1.5 Network management

1.5.1 Introduction

Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to solve problems in managing network devices connected to the Internet. Through SNMP, a the NMS can manage all network devices that support SNMP, including

Copyright © Raisecom Technology Co., Ltd.

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

Working mechanism

SNMP is divided into two parts: Agent and the NMS. The Agent is someone being managed in the SNMP network while the NMS is the manager for the SNMP network. The Agent and the NMS communicate with each other by sending SNMP packets through UDP.

The RAX721 communicates with Raisecom Network Management System (the NMS) through SNMP packets. Raisecom the NMS can provide friendly Human Machine Interface (HMI) to facilitate network management. The following functions can be implemented through it:

- Send request packets to the RAX721.
- Receive reply packets and Trap packets from the RAX721, and show result.

The Agent is a program installed in the RAX721, implementing the following functions:

- Receive/reply request packets from the NMS
- Read/write packets and generate response packets according to the packets type, then return the result to the NMS.

Define trigger condition according to protocol modules, enter/exit from system or reboot device when conditions are satisfied; the replying module sends Trap packets to the NMS through Agent to report current status of device.

Note

An Agent can be configured with several versions concurrently, and different versions communicate with different the NMSs. However, the SNMP version of the NMS must be consistent with that of the connected agent so that they can intercommunicate properly.

Protocol versions

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 password. The NMS can visit the agent only by specifying its community name correctly. If the community name carried in a SNMP packet is not authenticated by the RAX721, the packet will be dropped.
- 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) and View-based Access Control Model (VACM) security mechanism. You can configure whether USM authentication is enabled and whether encryption is enabled to provide higher security. USM authentication mechanism is used to authenticate the senders so that illegal users will not be able to access them. Encryption is to encrypt packets transmitted between the NMS and agents, thus preventing interception.

The RAX721 supports SNMPv1, SNMPv2c, and SNMPv3.

Copyright © Raisecom Technology Co., Ltd.

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 the NMS and Agent, through which the NMS can read/write every managed object in Agent to manage and monitor the RAX721.

MIB stores information in a tree structure, with unnamed root on the top. Nodes of the tree are the managed objects, which take a unique path starting from root (OID) for identification. SNMP protocol packets can access network devices by checking the nodes in MIB tree directory.

The RAX721 supports standard MIB and Raisecom-customized MIB.

1.5.2 Preparing for configurations

Scenario

To log in to the RAX721 through the NMS, you should first configure SNMP basic functions.

Prerequisite

- Configure the IP addresses on the SNMP interface.
- Configure static router to link RAX721 and the NMS through the router.

1.5.3 Confiurating SNMP basic functions

For SNMP v3, SNMP v1 or SNMP v2c, you should configure them respectively:

Configure SNMP v3 on the target device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server access** *group-name* [**read** *view-name*] [**write** *view-name*] [**notify** *view-name*][**context** *context-name* { **exact** | **prefix** }] **usm** { **noauthnopriv** | **authnopriv** | **authpriv** }	Create and configure the SNMP access groups.
3	Raisecom(config)#**snmp-server group** *name* **user** *user* **usm**	Configure the mapping between users and access groups.
4	Raisecom(config)#**snmp-server contact** *syscontact*	(Optional) configure the ID and contact of network administrators.
5	Raisecom(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version 3** { **noauthnopriv** | **authnopriv** | **authpriv** } *user-name* [**udpport** *udpport*]	Configure the IP address of the SNMP target host.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config)#**snmp-server location** *sysLocation*	(Optional) specify the location for placing the RAX721.
7	Raisecom(config)#**snmp-server user** *user-name* [**remote** *engine-id*] **authentication** { **md5** | **sha** } *authpassword* [**privacy** { **aes128** | **aes192** | **aes256** | **des** } *privword*]	Create a SNMP user, and configure its authentication algorithm, authentication password, encryption algorithm, and encryption password.
8	Raisecom(config)#**snmp-server user** *user-name* [**remote** *engine-id*] **authkey** { **md5** | **sha** } *keyword* [**privkey** { **aes128** | **aes192** | **aes256** | **des** } *privkey*]	Create a SNMP user, and configure its authentication algorithm, authentication key, encryption algorithm, and encryption key.
9	Raisecom(config)#**snmp-server view** *view-name oid-tree* [*mask*] { **included** | **excluded** }	Configure SNMP view.

Configure SNMP v1 or v2c on the target device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server community** *name* [**view** *view*] { **ro** | **rw** }	Create a community name and configure its corresponding view and access priority.
3	Raisecom(config)#**snmp-server contact** *contact*	(Optional) configure the ID and contact of network administrators.
4	Raisecom(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version** { 1 | 2c } *community-string* [**udpport** *port-id*]	Configure the IP address of the SNMP target host.
5	Raisecom(config)#**snmp-server location** *location*	(Optional) specify the location of the RAX721.

1.5.4 Configuring Trap

Note

Configuration steps in SNMP v1, v2c and v3 are the same except the configuration of the target host. Choose it as required.

A Trap is used by the RAX721 to send unrequested information to the NMS automatically, which is used to report some critical events.

Finish the following tasks before configuring Trap:

- Configure SNMP basic functions. SNMP v3 requires configuring the user name and SNMP view.
- Configure routing protocols, and ensure routing between the RAX721 and the NMS is available.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**ip address** *ip-address*	Configure the IP address of the RAX721.
	Raisecom(config-port)#**ipv6 address** *ipv6-address/prefix-length* [**eui-64**]	Configure the IPv6 address of the interface.
4	Raisecom(config-port)#**exit**	Exit Layer 3 physical interface configuration mode. Enter global configuration mode.
5	Raisecom(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version 3** { **noauthnopriv** | **authnopriv** | **authpriv** } *name* [**udpport** *udpport*]	(Optional) configure the SNMPv3 Trap target host.
6	Raisecom(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version** { **1** | **2c** } *name* [**udpport** *udpport*]	(Optional) configure the SNMP v1 and SNMP v2c Trap target host.

1.5.5 Configuring KeepAlive Trap packets

By sending KeepAlive Trap packets, the RAX721 makes the NMS discovery it in a short time to improve working efficiency of the NMS and reduce workloads of network administrators.

The prerequisite for configuring KeepAlive Trap packets is that the route between the RAX721 and the NMS is reachable.

Caution

To avoid multiple devices to concurrently send KeepAlive Trap in the same period and overburdened network management, configure the KeepAlive Trap packets to be sent within a random period of "sending period+5s".

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server keepalive-trap enable**	Enable sending KeepAlive Trap packets. By default, it is disable to send KeepAlive Trap packets.
3	Raisecom(config)#**snmp-server keepalive-trap interval** *period*	(Optional) configure the period for sending KeepAlive Trap packets. By default, the period for sending KeepAlive Trap packets is 300s.
4	Raisecom(config)#**snmp-server keepalive-trap pause**	(Optional) suspend the sending of KeepAlive Trap packets.

Copyright © Raisecom Technology Co., Ltd.

1.5.6 Checking configurations

No.	Command	Description
1	Raisecom#**show snmp access**	Show configurations of the SNMP access group.
2	Raisecom#**show snmp community**	Show configurations of the SNMP community.
3	Raisecom#**show snmp config**	Show SNMP basic configurations.
4	Raisecom#**show snmp group**	Show mapping between SNMP user and access group.
5	Raisecom#**show snmp host**	Show information about the SNMP target host.
6	Raisecom#**show snmp statistics**	Show SNMP statistics.
7	Raisecom#**show snmp user**	Show SNMP user information.
8	Raisecom#**show snmp view**	Show SNMP view information.
9	Raisecom#**show keepalive**	Show KeepAlive configurations.

1.6 Configuring RMON

1.6.1 Introduction

Remote Network Monitoring (RMON) is a standard stipulated by IETF (Internet Engineering Task Force) for network data monitoring through different network Agent and the NMS. RMON is derived from SNMP. Compared with SNMP, RMON can monitor remote devices more actively and more effectively, network administrators can track the network, network segment or device malfunction more quickly. This approach reduces the data flows between the NMS and Agent, makes it possible to manage large networks simply and powerfully, and makes up the limitations of SNMP in the ever-growing distributed Internet.

RMON implements 4 function groups: statistics group, history group, alarm group, and event group.

- Statistics group: gather statistics on each interface, including number of received packets and packet size distribution statistics.
- History group: similar with the statistics group, but it only collects statistics in an assigned detection period.
- Alarm group: monitor an assigned MIB object, configure the upper and lower thresholds in an assigned time interval, and trigger an event if the monitored object exceeds the threshold.
- Event group: cooperating with the alarm group, when alarm triggers an event, it records the event, such as sending Trap or writing it into the log, and so on.

1.6.2 Preparing for configurations

Scenario

RMON helps monitor and gather statistics about network traffics.

Copyright © Raisecom Technology Co., Ltd.

Compared with SNMP, RMON is a more high-efficient monitoring method. After you specify an alarm threshold, the RAX721 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 RAX721 and the NMS is reachable.

1.6.3 Configuring RMON alarm group

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rmon alarm** *alarm-id mibvar* [**interval** *second*] { **absolute** | **delta** } **rising-threshold** *rising-num* [*rising-event*] **falling-threshold** *falling-num* [*falling-event*] [**owner** *owner-name*]	Configure related parameters of the RMON alarm group.

1.6.4 Configuring RMON event group

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rmon event** *event-id* [**log**] [**trap**] [**description** *string*] [**owner** *owner-name*]	Configure related parameters of the RMON event group.

1.6.5 Configuring RMON statistics

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**rmon statistics** [**owner** *owner-name*]	Enable RMON statistics on an interface and configure related parameters. By default, RMON statistics on all interfaces is enabled.

1.6.6 Configuring RMON history statistics

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**rmon history** [**shortinterval** *period*] [**longinterval** *period*] [**buckets** *buckets-number*] [**owner** *string*]	Enable RMON history statistics on an interface and configure related parameters. By default, RMON history statistics on all interfaces is disabled.

1.6.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show rmon**	Show RMON configurations.
2	Raisecom#**show rmon alarms**	Show information about the RMON alarm group.
3	Raisecom#**show rmon events**	Show information about the RMON event group.
4	Raisecom#**show rmon statistics**	Show information about the RMON statistics group.
5	Raisecom#**show rmon history** *interface-type interface-number*	Show information about the RMON history group.

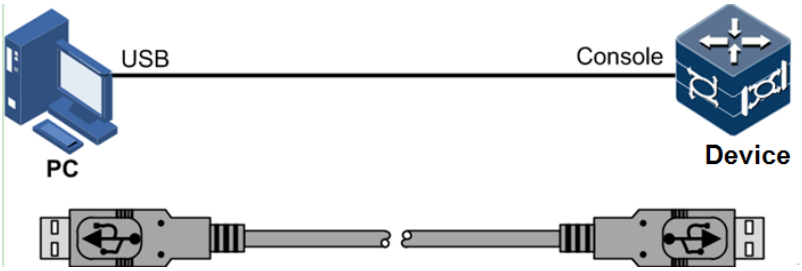
1.7 Configuration examples

1.7.1 Example for logging in to the device through Console interface

The maintenance personnel can log in to the device through the Console interface to configure the RAX721 for the first time. Connect the Console interface on the RAX721 to the USB interface of the computer through the USB cable delivered with the device, as shown in Figure 1-7.

As shown in Figure 1-7, use a USB cable to directly connect the Console interface on the RAX721 to the USB interface of the computer, and then start the terminal maintenance software on the computer, configure the serial port parameters, and log in to the RAX721 to perform configuration management.

Figure 1-7 Logging in to the RAX721 through Console interface



Copyright © Raisecom Technology Co., Ltd.

Step 1 Connect the Console interface on the RAX721 to the USB interface on the computer with a USB cable.

Step 2 Start the terminal maintenance program on the computer. The configuration protocol is "Serial". The port is the serial port number corresponding to the computer's USB port, such as "COM5", and the baud rate is "9600", which is used to establish a connection with the device.

Step 3 When the terminal maintenance program will prompt "Login:", enter raisecom for both the user name and the password to enter the common EXEC mode. The system will display:

```
Raisecom>
```

Step 4 Enter the enable command and the correct password to enter privileged EXEC mode. The default password is Raisecom.

```
Raisecom>enable
Password:
Raisecom#
```

Step 5 In privileged EXEC mode, enter the config command to enter global configuration mode.

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

Step 6 In global configuration mode, enter interface fastethernet 1/0/1 to enter the NEG interface configuration mode.

```
Raisecom(config)#interface fastethernet 1/0/1
Raisecom(config-fastethernet 1/0/1)#
```

Step 7 In NEG interface configuration mode, configure the network management IP address, such as 10.10.10.1.

```
Raisecom(config-fastethernet 1/0/1)#ip address 10.10.10.1 255.255.255.0
```

1.7.2 Example for logging in to device through Telnet

The RAX721 supports Telnet, through which you can remotely log into the RAX721, configure it through the terminal maintenance software, and implement remote control and management of the RAX721. The premise of Telnet login is that the NEG interface on the RAX721 device has been configured with an IP address (for the configuration method, see

Copyright © Raisecom Technology Co., Ltd.

section 1.7.1 Example for logging in to the device through Console interface), and the device IP address can be pinged on the computer. The networking diagram is shown in Figure 1-8.

Figure 1-8 Logging in to the RAX721 through Telnet

Step 1 The computer is installed with a terminal maintenance software which supports Telnet, such as the "Hyper Terminal" program that comes with Microsoft's Windows operating system.

Step 2 Connect the network interface on the computer to the network through a network cable. The RAX721 accesses the network through the NEG interface of the NXU network card. Check the network connectivity. You should be able to ping the RAX721 on the computer.

Step 3 Start the terminal maintenance software on the computer and configure the protocol type to Telnet, the host name to the device IP address, such as 10.10.10.1, to establish a connection with the RAX721.

Step 4 If the RAX721 uses the default configuration, the terminal maintenance software will prompt "Login". Enter Raisecom for both the user name and password to enter common EXEC mode. The system will display:

```
Raisecom>
```

Step 5 Enter the enable command and the correct password to enter privileged EXEC mode. The default password is Raisecom.

```
Raisecom>enable
Password:
Raisecom#
```

Step 6 In privileged EXEC mode, enter the config command to enter global configuration mode.

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

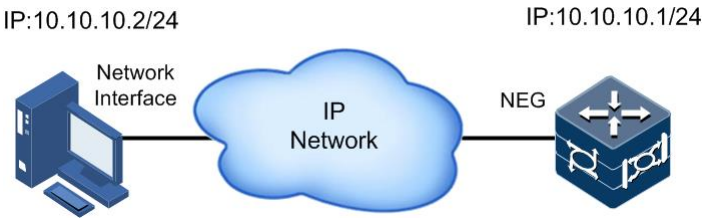
1.7.3 Example for logging in to device through SSHv2

The RAX721 can manage the remote device through SSHv2. Configure the RAX721 through the terminal maintenance software on the computer to realize the remote control and management of the equipment. The prerequisite for SSHv2 login is that the NEG interface of the RAX721 device has been configured with an IP address (for the configuration method, see

Copyright © Raisecom Technology Co., Ltd.

1.7.1 Example for logging in to the device through Console interface), and the device IP can be pinged on the computer. The networking diagram is shown in Figure 1-9.

Figure 1-9 Managing device through SSHv2



Step 1 Open the terminal maintenance software on the computer and perform the following configurations:

```
Login:raisecom
password:
Raisecom>enable
Password:
Raisecom#config
Raisecom(config)#
```

Step 2 In global configuration mode, use the generate ssh-key command to generate the product key.

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

Generate and save rsa key done!
```

Step 3 In global configuration mode, use the ssh2 server command to enable SSHv2 services.

```
Raisecom(config)#ssh2 server
Set successfully
```

Step 4 In the connection configuration interface of the terminal maintenance software, select the protocol type as "SSHv2" and the host name as the device IP address, click the connect button, and a dialog box for the new host key will pop up.

Step 5 Operate the SSHv2 key processing method according to the prompt of the host key dialog box, and enter the user name and password to log in to the device. The user name and password are still the default values, such as raisecom and raisecom.

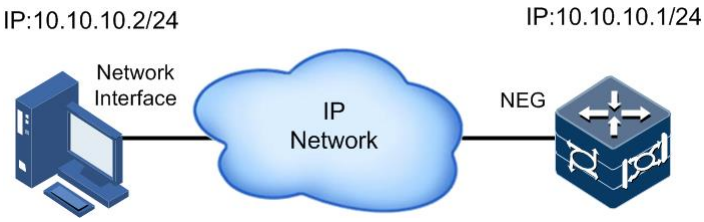
1.7.4 Example for logging in to device through ACL

When logging in to the RAX721 through Telnet, you can configure ACL to realize the access control management of the device. By configuring an IP-based access control list, you can allow or deny the specified IP address to log in to the management device through Telnet or

Copyright © Raisecom Technology Co., Ltd.

SSHv2. As shown in Figure 1-10, the configuration allows a computer with an IP address of 10.10.10.2 to connect to the RAX721 through Telnet.

Figure 1-10 Telneting to the RAX721 based on ACL



Step 1 Manage the RAX721 through Telnet or SSHv2. For detailed configurations, refer to section 1.7.2 Example for logging in to device through Telnet and section 1.7.3 Example for logging in to device through SSHv2.

Step 2 Use the access-list command to configure the IP ACL.

```
Raisecom#config
Raisecom(config)#access-list 1000
Raisecom(config-acl-ip-std)#
```

Step 3 Use the rule command to configure ACLs.

```
Raisecom(config-acl-ip-std)#rule 1 permit 10.10.10.2 255.255.255.0
Raisecom(config-acl-ip-std)#rule 2 deny any
Raisecom(config-acl-ip-std)#exit
```

Step 4 Use the telnet-server access-list command to configure ACL-based Telnet services.

```
Raisecom(config)#telnet-server access-list 1000
```

Step 5 Exit the terminal maintenance software.

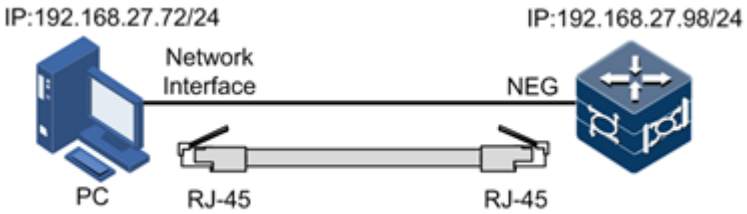
Step 6 Reconnect the RAX721 through the terminal maintenance software. In this case, only the computer with the IP address of 10.10.10.2 can Telnet to the RAX721.

1.7.5 Example for upgrading system software (in privileged EXEC mode)

The network connection during system software upgrade is shown in Figure 1-11. Use a network cable to connect the network management interface (in-band network management interface or out-of-band network management interface) of the RAX721 to the computer's network interface directly, so that the device IP address can ping the computer IP address. Then save the system software file package to the path specified by the FTP software, start the FTP tool software on the computer, and log in to the command line configuration interface of the RAX721 through the terminal maintenance software on the computer.

Copyright © Raisecom Technology Co., Ltd.

Figure 1-11 System software upgrade



Step 1 Run the FTP Server software installed on the PC and configure the FTP user name, password, and file path. In this section, the user name is configured to 111111 and the password is configured to 111111.

Step 2 Configure the IP address of the network management interface and ensure that the device IP address can ping the computer IP address. In this section, the IP address of the network management interface is configured to 192.168.27.98 and the IP address of the PC is configured to 192.168.27.72.

```
Raisecom#config
Raisecom(config)#interface fastethernet 1/0/1
Raisecom(config-fastethernet1/0/1)#ip address 192.168.27.98 255.255.255.0
```

Step 3 Download the system software.

```
Raisecom(config)#exit
Raisecom#download system1 ftp 192.168.27.72 111111 111111 system.z
```

Step 4 Wait for downloading the file. The file is downloaded successfully when the prompt "Set successfully" is displayed.

```
Waiting...Start
OK
OK
Downloading 12204Kb
Set successfully
```

Step 5 Configure the file to the system file used for rebooting the device at the next time.

```
Raisecom#boot next-startup system1
Slot 1 upgrade success.
```

Step 6 Reboot the device and enter **yes**.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom#reboot
Please input 'yes' to confirm:yes
```


Copyright © Raisecom Technology Co., Ltd.

2 System management

This chapter describes principles and configuration procedures of system management, including following sections:

- User management
- Device management
- Saving configurations
- Time management
- Log management
- File management
- Alarm management
- Key chain management
- Performance statistics
- Remote device management

2.1 User management

When you start the RAX721 for the first time, connect the PC through Console interface to the device, input the initial user name and password in Hyper Terminal to log in to and configure the RAX721.

Note

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

If there is not any privilege restriction, any remote can log in to the RAX721 through Telnet, when the Simple Network Management Protocol (SNMP) interface or other service interfaces of device are configured with IP addresses. This is unsafe to the RAX721 and network. Creating user and setting password and privilege help to manage the login users and ensure network and device security.

Copyright © Raisecom Technology Co., Ltd.

2.1.1 Configuring user management

Step	Command	Description
1	Raisecom#**user name** *user-name* **password** *password*	Create or modify the user name and password.
2	Raisecom#**user name** *user-name* **privilege** *privilege-level*	Configure the level and privilege of the user.

2.1.2 Checking configurations

No.	Command	Description
1	Raisecom#**show user** { **active** [**onlineid** *online-id*] | **table** [**detail** | *username*]	Show user information.

2.2 Device management

2.2.1 Fan management

When the device is placed in a relatively hot environment, the excessively high temperature will affect the heat dissipation performance of the device. At this time, you can configure fan monitoring so that the fan automatically adjusts to the ambient temperature to maintain the normal operation of the device.

Step	Command	Description
1	Raisecom#**show fan**	Show the running status of the fan, such as the speed.

2.2.2 Checking configurations

No.	Command	Description
1	Raisecom#**show manufacture info**	Show factory information.
2	Raisecom(config)#**show power**	Show power information.

2.3 Saving configurations

Step 1 and step 2 can be in any sequence.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**write** { **all** | **backup-config** }	Save current configurations.
2	Raisecom#**auto-write** { **enable** | **disable** }	(Optional) enable automatic saving of configurations.
	Raisecom#**auto-write interval** *minutes*	

2.4 Time management

2.4.1 Configuring time and time zone

To ensure that the RAX721 can cooperate with other devices, you need to configure system time and time zone precisely for the RAX721.

Step	Command	Description
1	Raisecom#**clock display** { **default** | **utc** }	Configure the system time display mode. By default, it is **default**.
2	Raisecom#**clock set** *hour minute second year month day*	Configure the system time. By default, the system time is 8:00:00, Jan 1, 1970.
3	Raisecom#**clock timezone** { **+** | **-** } *hour minute*	Configure the timezone of the system. By default, it is UTC/GMT+08:00.

2.4.2 Configuring DST

Daylight Saving Time (DST) is set locally to save energy. About 110 countries around the world apply DST in summer, but vary in details. Thus, you need to consider detailed DST rules locally before configuration.

Step	Command	Description
1	Raisecom#**clock summer-time enable**	Enable DST on the RAX721. By default, DST is disabled.
2	Raisecom#**clock summer-time recurring** { *start-week* | **last** } { **sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat** } *start-month start-hour start-minute* { *end-week* | **last** } { **sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat** } *end-month end-hour end-minute offset-mm*	Configure the begin time, end time, and offset of DST.

- For example, if DST starts from 02:00 a.m. second Monday of April to 02:00 a.m. second Monday of September, the clock is moved ahead 60 minutes. Thus, the

Copyright © Raisecom Technology Co., Ltd.

period between 02:00 and 03:00 second Monday of April does not exist. Configuring time during this period will fail.

- DST in the Southern Hemisphere is opposite to that in the Northern Hemisphere. It is from September this year to April next year. If the starting month is later than the ending month, the system judges that it is located in the Southern Hemisphere.

2.4.3 Configuring NTP/SNTP

Configuring NTP/SNTP basic functions

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ntp enable**	Enable global NTP.
3	Raisecom(config)#**ntp server** { *ip-address* | *ipv6-address* } [**vrf** *vrf-name*] [**version** *version-number*] [**keyid** *key-id*]	(Optional) configure the NTP server address for the client device that works in the server/client mode.
4	Raisecom(config)#**ntp peer** { *ip-address* | *ipv6-address* } [**vrf** *vrf-name*] [**version** *version-number*] [**keyid** *key-id*]	(Optional) configure the NTP peer address for the device that works in peer mode.
5	Raisecom(config)#**sntp server** { *ip-address* | *ipv6-address* } **version** { **v1** | **v2** | **v3** | **v4** }	Configure the IP address of the SNTP server that works in SNTP client mode.
6	Raisecom(config)#**ntp refclock-master** *ip-address* [*stratum*]	Configure the device as the NTP master clock, namely, the reference clock source. By default the local device is not the reference clock source.

Configuring NTP identity authentication

In a network with high security requirements, identity authentication is required when using NTP. The NTP client only synchronizes with the authenticated server after enabling the authentication function, which ensures the security of the network. The NTP client authenticates the server only when the authentication function is enabled. If the authentication function is not enabled, even if the server carries the key information, the client will not authenticate the server but directly synchronizes time with the server.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ntp authenticate enable**	Enable NTP server/client identity authentication.
3	Raisecom(config)#**ntp authentication-keyid** *key-id* **md5** *password*	Configure the key ID and key value for NTP server/client identity authentication.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config)#**ntp trusted-keyid** *key-id*	Configure the identity authentication key ID of the NEP client/server as a trusted ID. **Note** The NTP client will verify the server only when the authentication function is enabled, and the client will only synchronize with the server that provides the trusted key.

Note

- If the device is configured as an NTP reference clock source, the configuration of the NTP server or NTP peer fails and the device cannot be synchronized by other devices; vice versa, if the NTP server or peer is configured, the device cannot be configured as the NTP reference clock source.
- SNTP and NTP conflict with each other. If the SNTP server address is configured on the device, NTP cannot be configured for the device, and vice versa.

2.4.4 Checking configurations

No.	Command	Description
1	Raisecom#**show clock** [**summer-time recurring**]	Show whether configurations of the system time, timezone, and DST are correct.
2	Raisecom#**show sntp**	Show the time obtained by SNTP and whether configurations are correct.
3	Raisecom#**show ntp status**	Show whether NTP configurations are correct.
4	Raisecom#**show ntp associations** [**detail**]	Show whether NTP connections are correct.
5	Raisecom#**show ntp authentication**	Show NTP authentication.

2.5 Log management

2.5.1 Basic configurations

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**logging on**	Enable global system log. By default, global system log is enabled.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**logging rate-limit** *number*	Configure the rate limiting value of logs. By default, it is 0. It means that no rate is configured on logs.
4	Raisecom(config)#**logging sequence-number**	Configure the log to display the sequence number. By default, the sequence number is not displayed.
5	Raisecom(config)#**logging buginf** [**high** | **low** | **none** | **normal**]	Configure the level of the Debug information. By default, it is **none**.

2.5.2 Configuring log discriminator

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**logging discriminator** *number* { **facility** | **mnemonics** | **msg-body** } { **none** | { **drops** | **includes** } *string* }	Configure the log discriminator.
3	Raisecom(config)#**logging** { **buffered** | **console** | **file** | **trap** } **discriminator** *number*	Associate the log buffer, Console log, log file, and Trap with the log discriminator.

2.5.3 Configuring log storage

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**logging buffered size** *size*	Configure the size of the log buffer. By default, it is 4 Kbytes.
3	Raisecom(config)#**logging file**	Save logs to the log file.
4	Raisecom(config)#**logging facility** { **alert** | **audit** | **auth** | **clock** | **cron** | **daemon** | **ftp** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **ntp** | **security** | **syslog** | **user** | **uucp** }	Configure the facility type of logs in the log host. By default, it is local7.
5	Raisecom(config)#**logging history**	Save logs to the historical log table.
6	Raisecom(config)#**logging history size** *size*	Configure the size of the historical log table. By default, it is 1.

Copyright © Raisecom Technology Co., Ltd.

2.5.4 Checking configurations

No.	Command	Description
1	Raisecom#**show logging**	Show system log configurations.
2	Raisecom#**show logging buffer**	Show buffer parameters of the system log.
3	Raisecom#**show logging discriminator**	Show configurations of log discriminator.
4	Raisecom#**show logging file**	Show log files.
5	Raisecom#**show logging history**	Show information about the historical log table.

2.5.5 Maintenance

No.	Command	Description
1	Raisecom(config)#**clear logging buffer**	Clear contents from the log buffer.
2	Raisecom(config)#**clear logging statistics**	Clear log statistics in the buffer.

2.6 File management

2.6.1 Managing configuration files

Step	Command	Description
1	Raisecom#**erase** [*file-name* | **backup-config** | **all**]	Delete the file in the storage. **Caution** Use this command with caution.
2	Raisecom#**dir**	Show system files.
3	Raisecom#**show startup**	Show system startup files.

2.7 Alarm management

2.7.1 Introduction

An alarm refers to information generated by the system based on module failures when a fault is generated on the RAX721 or some working condition changes.

Copyright © Raisecom Technology Co., Ltd.

The alarm is used to report some urgent and important events and notify them to the network administrator promptly, which provides strong support for monitoring device operation and diagnosing faults.

The alarm is stored in the alarm buffer. If the NMS is configured, the alarm will be sent to it through SNMP. The information sent to the NMS is called Trap.

Alarm classification

There are 3 kinds of alarms according to properties of an alarm:

- Fault alarm: alarms generated because of hardware failure or anomaly of important functions, such as port Down alarm
- Recovery alarm: alarms generated when device failure or abnormal function returns to normal, such as port Up alarm;
- Event alarm: prompted alarms or alarms that are generated because the fault alarm and recovery alarm cannot be related, such as alarms generated because of failing to Ping.

Alarms are divided into 4 types according to functions:

- Service quality alarm: alarms caused by service quality degradation, including congestion, performance decline, high resource utilization rate, and the bandwidth reducing
- Processing error alarm: alarms caused by software or processing errors, including software errors, memory overflow, version mismatching, and abnormal program aborts
- Environmental alarm: alarms caused by equipment location-related problems, including the temperature, humidity, ventilation. and other abnormal working conditions
- Device alarm: alarms caused by failure of physical resources, including the power supply, fan, processor, clock, input/output interface, and other hardware.

Alarm output

There are 2 alarm output modes:

- Alarm buffer: alarms are recorded in tabular form, including the current alarm table and history alarm table.
  - Current alarm table: records alarms which are not cleared or restored.
  - History alarm table: consists of restored alarms and records the cleared and auto-restored alarms.
- Trap: alarms sent to the NMS when the NMS is configured

Alarms will be broadcasted according to various terminals configured on the RAX721, including CLI terminal and the NMS.

Related concepts

Related concepts about alarm management are displayed as below:

- Alarm auto-report

Auto-report refers that an alarm will be reported to the NMS automatically with its generation and the NMS does not need to query or synchronize alarms actively.

You can set auto-report to some alarm, some alarm source, or the specified alarm from specified alarm source.

Copyright © Raisecom Technology Co., Ltd.

The alarm source refers to an entity that generates related alarms, such as interfaces, devices, or cards.

- Alarm monitoring

Alarm monitoring is used to process alarms generated by modules:

  - When alarm monitoring is enabled, the alarm module will receive alarms generated by modules, and process them according to configurations of the alarm module, such as recording alarm in the alarm buffer, etc.
  - When alarm monitoring is disabled, the alarm module will discard alarms generated by modules without follow-up treatment. In addition, alarms will not be recorded on the RAX721.

You can perform alarm monitoring on some alarm, alarm source, or specified alarm from specified alarm source.

- Alarm inverse

Alarm inverse (taking alarms of the interface for examples) refers that the reported alarm status of the interface is opposite to the actual alarm status. The interface will not report an alarm if it is unused but it will report alarms if it is used. If the interface returns to the unused status, the reported alarm will be cleared. There are 3 alarm inverse modes available:

  - Non- inverse mode: alarms are reported normally
  - Manual inverse mode: in this mode, whatever the current alarm status of the interface is, the reported alarm status of the interface is changed to the one opposite to the actual alarm status. It means that the interface reports the related recovery alarm if there is an alarm and reports an alarm if there is no alarm.
  - Auto inverse mode: in this mode, if there is no alarm to be inversed, operations are configured successfully but not take effect. If there is an alarm to be inversed, operations are configured successfully. The related recovery alarm is reported and the interface will enter the inverse mode, which means status of all reported alarms is opposite to the real one. After the alarm is completed, the interface enters the non-inverse mode automatically and reports alarms properly.

- Alarm delay

Alarm delay refers that the device will record alarms and report them to the NMS after a delay but not immediately when alarms generate. Delay for recording and reporting alarms are identical.

- Alarm storage mode

Alarm storage mode refers to how to record new generated alarms when the alarm buffer is full. There are two ways:

  - stop：stop mode, when the alarm buffer is full, new generated alarms will be discarded without recording.
  - loop: loop mode, when the alarm buffer is full, the new generated alarms will replace old alarm information and take rolling records.

For the RAX721, the current alarm table can record up to 1000 alarms and the historical alarm table can record up to 500 alarms. Use the configured alarm storage mode to deal with newly-generated alarms when the alarm table is full.

- Alarm clearance

Copyright © Raisecom Technology Co., Ltd.

Clear the current alarm, which means deleting current alarms from the current alarm table. The cleared alarms will be saved to the historical alarm table.

- Viewing alarms

The administrator can view alarms and monitor alarms directly on the RAX721. If the RAX721 is configured with the NMS, the administrator can monitor alarms on the NMS.

2.7.1 Configuring alarm inhibition

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm inhibit enable**	Enable alarm inhibition. By default, it is enabled.

2.7.2 Configuring alarm delay

The alarm delay can be divided into alarm generation delay and alarm clearance delay.

- Alarm generation delay refers to the delay after an alarm is generated.
- Alarm clearance delay refers to the delay after an alarm is finished.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm active delay** *second*	Configure the alarm generation delay. By default, it is 0s.
3	Raisecom(config)#**alarm clear delay** *second*	Configure the alarm clearance delay. By default, it is 0s.

2.7.3 Configuring alarm storage modes

Alarm storage modes are modes for Network Elements (NEs) storing alarms, which can be divided into loop and stop modes.

- In stop alarm storage mode, if there is no more capacity for alarms stored by NEs, newly-reported alarms will be discarded.
- In loop alarm storage mode, if there is no more capacity for alarms stored by NEs, newly-reported alarms will overwrite the old ones and will be stored at the initial position of the memory.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm active storage-mode** { **loop** | **stop** }	Configure the alarm storage mode. By default, it is stop.

Copyright © Raisecom Technology Co., Ltd.

2.7.4 Clearing alarms

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm clear type** *module_name*	Clear alarms of a specified function module.

2.7.5 Configuring alarm reporting

Auto-report refers that the device will automatically report an alarm to the NMS when the alarm is generated, without querying or synchronizing the alarm. Trap is the information sent by the device to the NMS. Trap is used to report some emergent and critical events (for example, the managed device is restarted).

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm auto-report** *interface-type interface-number* **enable**	Enable alarm auto-report based on different types of interfaces, including Ethernet interfaces, sub-interfaces, loopback interfaces, VLAN interfaces, and link aggregation interfaces. By default, it is enabled.
3	Raisecom(config)#**alarm auto-report type** *module-name* **enable**	Enable alarm auto-report for a function module. By default, it is enabled.
4	Raisecom(config)#**alarm auto-report all enable**	Enable alarm auto-report for all alarm. By default, it is enabled.

2.7.6 Configuring alarm inverse

Alarm reverse refers to shielding the actual alarm when the interface is not enabled or there is no service. That is, the interface does not report an alarm when there is an actual alarm, and reports an alarm when there is no actual alarm.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm inverse** *interface-type interface-number* { **auto** | **manual** | **none** }	Configure the alarm inverse mode.

2.7.7 Configuring alarm monitoring

Alarm monitoring is used to process alarms generated by interfaces or various modules.

- After alarm monitoring is enabled, the alarm module will receive alarms generated by all modules and process them based on configurations of the alarm module, such as, saving alarms to the alarm buffer.

Copyright © Raisecom Technology Co., Ltd.

- After alarm monitoring is disabled, the alarm module will discard alarms generated by all modules without processing them. These alarms will not be record to the device.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm monitor** *interface-type interface-number* **enable**	Enable alarm monitoring based on various types of interfaces, including Ethernet interface, sub-interface, loopback interface, VLAN interface and link aggregation interface. By default, alarm monitoring is enabled.
3	Raisecom(config)#**alarm monitor type** *module_name* [*group-name*] [*interface-type interface-number*] **enable**	Enable alarm monitoring based on function module. By default, it is enabled.
4	Raisecom(config)#**alarm monitor all enable**	Enable alarm monitoring for all alarms. By default, it is enabled.

2.7.8 Configuring alarm output

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm syslog enable**	Enable alarm syslog. By default, it is enabled.

2.7.9 Checking configurations

No.	Command	Description
1	Raisecom#**show alarm active** [*module_name* | **severity** *severity*]	Show currently active alarms.
2	Raisecom#**show alarm cleared** [*module_name* | **severity** *severity*]	Show historical alarms.
3	Raisecom#**show alarm management** [*module_name*]	Show alarm management configurations.
4	Raisecom#**show alarm management statistics**	Show alarm statistics.
5	Raisecom#**show alarm log**	Show alarm logs.

Copyright © Raisecom Technology Co., Ltd.

2.8 Key chain management

2.8.1 Introduction

For security, you need to constantly modify the authentication information of the application layer on the network. The authentication algorithm and the shared security key jointly determine whether the information has been tampered with when it is transmitted on an insecure network. When you authenticate data using this method, you have to ensure that the security key and authentication algorithm are shared between the data sender and the receiver. And the key cannot be transmitted on the network.

If each application layer protocol maintains a set of authentication rules (including authentication algorithms and keys), there will be a large number of applications using the same authentication method. This will cause the authentication information to be copied and changed. Similarly, if each application uses a fixed authentication key, each change needs to be manually modified by the network administrator. Manually changing the key or authentication algorithm will be very complicated and cumbersome. It will be very difficult to change the passwords of all routers without losing packets.

Therefore, the system needs to be able to centrally manage all authentication processes and change authentication algorithms and keys without excessive manual intervention. However, key-chain realizes this function.

Key-chain provides authentication for all application layer protocols, and Key-chain can dynamically change the password chain without packet loss.

2.8.2 Configuring key chain

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**key-chain** *key-chain-name*	Create a key chain and enter Keychain configuration mode.
3	Raisecom(config-keychain)#**accept-tolerance** { *time-value* | **infinite** }	Configure the Rx tolerance time.
4	Raisecom(config-keychain)#**key** *key-id* **key-string** [**0** | **7**] *keystring*	Configure the key and password.
5	Raisecom(config-keychain)#**key** *key-id* **send-lifetime** *start-time* { **duration** *duration-time* | *end-time* | **infinite** }	Configure the key sending time.
6	Raisecom(config-keychain)#**key** *key-id* **accept-lifetime** *start-time* { **duration** *duration-time* | *end-time* | **infinite** }	Configure the key receiving time.

2.8.3 Checking configurations

No.	Command	Description
1	Raisecom#**show key-chain**	Show key configurations and statistics.
2	Raisecom#**show key-chain** *key-chain-name* **key** *key-id*	Show key configurations and statistics of the specified key.

Copyright © Raisecom Technology Co., Ltd.

2.9 Performance statistics

2.9.1 Introduction

Performance statistics are used to monitor device interfaces and gather statistics about messages to enable users to understand network performance. Performance statistics gathers short-period or long-period statistics based on interface or service flow measurement points. The short statistical period is 15 minutes, and the long statistical period is 24 hours. The statistical data in a statistical period is stored in the Flash memory in the form of data blocks in accordance with the write period, which is convenient for users to view.

Performance statistics based on interfaces:

- Short/long-period performance statistics of interfaces: including short/long-period performance statistics of service ports and management ports.
- Storage of short/long-period performance statistics data of the interface: including short/long period performance statistics data of the service port and management port, which are stored in the Flash according to the configured write period.

Performance statistics based on service flow:

- Short/long-period performance statistics of service flow: short/long-period performance statistics including service VLAN or priority.
- Storage of short/long-period performance statistics of service flows: short/long-period performance statistics including service VLAN or priority are stored in Flash according to the configured write period.

2.9.2 Preparing for configurations

Scenario

When you need to understand the performance of the device, enable performance statistics to gather packet statistics about interfaces or service flows, and show you the historical and current statistics on packets.

Prerequisite

N/A

2.9.3 Default configurations of performance statistics

Function	Default value
Performance statistics	Disabled
Number of stored data blocks	16

Copyright © Raisecom Technology Co., Ltd.

2.9.4 Configuring performance statistics

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**performance statistics interval buckets** *buckets-number*	Configure the number of data blocks storage in the statistics flash file.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.
4	Raisecom(config-port)#**performance statistics** [**vlan** *vlan-id* [**cos** *statistics-cos*]] { **enable** | **disable** }	Enable performance statistics in interface configuration mode. Use the **disable** form of this command to disable this function.

Note

The time for gathering performance statistics has nothing to do with the time configured by the command, but is related to the system time. Performance statistics takes 15 minutes as a period to complete a statistics. For example, when performing statistics for the first time, if performance statistics is enabled at the 5th minute, the statistics will start in 15 minutes and the statistics will be completed in 30 minutes.

2.9.5 Checking configurations

Step	Command	Description
1	Raisecom#**show performance statistics interval buckets** Raisecom#**show performance statistics interface** *interface-type interface-number* { **current** | **history** } Raisecom#**show interface** *interface-type interface-number* **vlan** *vlan-id* [**cos** *cos-value*] { **current** | **history** }	Show performance statistics.

2.9.6 Maintenance

Command	Description
Raisecom(config)#**clear performance statistics**	Clear performance statistics.

2.10 Remote device management

The RAX721 interface which is connected to the remote device can be configured to remote device configuration mode. Therefore, you can configure the remote device without going to the site, reducing operation and maintenance costs.

Copyright © Raisecom Technology Co., Ltd.

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter physical interface configuration mode.
3	`Raisecom(config-port)#remote-device` `Raisecom(config-remote)#`	Enter remote device management mode.

Copyright © Raisecom Technology Co., Ltd.

3 Interface management

This chapter describes principles and configuration procedures of interface management, including following sections:

- Basic configurations of interface
- Configuring Ethernet interface
- Configuring Ethernet sub-interface
- Configuring VLAN interface
- Configuring optical module DDM
- Configuring loopback interface
- Configuring out-of-band network management interface
- Checking configurations

3.1 Basic configurations of interface

3.1.1 Configuring basic information of interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**no portswitch**	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**ip address** *ip-address* [*ip-mask*] [**sub**]	Configure the primary and secondary IP addresses, as well as subnet mask of the Layer 3 physical interface.
4	Raisecom(config-port)#**description** *string*	Configure descriptions of the interface.
5	Raisecom(config-port)#**als enable**	Enable ALS. By default, it is disabled.
6	Raisecom(config-port)#**mdi** { **auto** | **normal** | **xover** }	Configure MDI wiring on the interface. By default, it is forced straight-through.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
7	Raisecom(config-port)#**shutdown**	(Optional) shut down the interface.

3.1.2 Configuring interface working mode

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**mode** { **l2** | **l3** }	Configure Layer 3 physical interface working mode. • L2: access L2VPN. • L3: access L3 routes.

3.1.3 Configuring Ethernet interface mode

Note

- After the working mode is switched, all commands under the Ethernet interface will be restored to the default conditions in the new mode except for the shutdown command.
- The Ethernet interface of the device works in Layer 3 routing mode (route) by default. Unless otherwise specified, the Ethernet interfaces involved in other functional modules are all in Layer 3 routing mode.

By default, the Ethernet interfaces of the device work in Layer 3 routing mode (route).

- If the working mode is set to Layer 2 switching mode L2 (bridge), it will be used as a Layer 2 Ethernet interface.
- If the working mode is set to Layer 3 routing mode L3 (route), it will be used as a Layer 3 Ethernet interface.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type unit-id/slot-id/port*	Enter Layer 3 Ethernet interface configuration mode.
3	Raisecom(config-port)#**portswitch**	(Optional) change the interface mode to switching mode from routing mode. You can use the **no portswitch command** to restore to the routing mode.

3.1.4 Configuring interface Jumboframe

When exchanging high-throughput data, such as transmitting files, the Ethernet interface may receive the Jumbo frame, whose size is greater than the standard Ethernet frame size. The

Copyright © Raisecom Technology Co., Ltd.

system will directly discard Jumbo frames. If you configure to allow Jumbo frames to pass, the system will continue to process them, when the size of these Jumbo frames is greater than the standard size but in specified value range.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**jumboframe** *frame-size*	Configure the interface to allow Jumbo frames to pass. By default, it is 9600 bytes.

3.1.5 Configuring MTU of interface

The Maximum Transmission Unit (MTU) is the largest bytes of packets that can be transmitted in a physical network. After you configure the RAX721 to allow Jumbo frames to pass, the IP layer will compare the MTU with the size of the packet to be sent. If the size of the packet is greater than the MTU, the IP layer will fragment the packet. The fragmented packet can be smaller than or equal to the MTU. When MTUs of two connected devices are configured inconsistently, these 2 devices fail to communicate with each other. In this case, you should adjust MTU configurations.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**mtu** *size*	Configure the MTU of the interface. By default, it is 1500 bytes.

3.1.6 Configuring interface flapping suppression

When working on the network, the interface of the device may alternately appear up and down status due to various reasons, such as, physical signal interference, configuration error in link layer. Frequency alternation leads routing protocol repetitive flapping and has bad effects on the device and the network, what's worse, the network and some devices may be disabled.

You should configure the flapping suppression period so as to reduce the switching frequency between up and down status.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-port)#**vibration-suppress period** *second*	Configure the flapping suppression period of the interface. By default, the suppression period is 0s.

3.1.7 Configuring MAC address of interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**mac** *mac-address*	Configure the MAC address of the interface. **Caution** If different interfaces are configured with the same MAC address, conflicts will occur. When configuring the MAC address, make a plan in advance.
4	Raisecom(config-port)#**shutdown** Raisecom(config-port)#**no shutdown**	Restart the interface to make the MAC address take effect.

3.2 Configuring Ethernet interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode. By default, the interface is in Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**speed** { **auto** | **10** | **100** | **1000** | **10000** }	Configure the interface rate. **Caution** When you use this command to configure the rate of one uplink interface, the other three interfaces will be adjusted to the same rate.
4	Raisecom(config-port)#**duplex** { **auto** | **full** | **half** }	Configure interface duplex mode.
5	Raisecom(config-port)#**flowcontrol** { **receive** | **send** } { **on** | **off** }	Configure interface flow control. By default, bidirectional flow control is disabled on the interface.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config-port)#**snmp trap link-fault** { **enable** | **disable** }	Enable link fault Traps sending on an interface.
7	Raisecom(config-port)#**snmp trap link-status enable**	Disable link fault Traps sending on an interface.

3.3 Configuring Ethernet sub-interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config-port)#**interface** *interface-type unit/slot/port.sub-interface*	Enter Ethernet sub-interface configuration mode in Layer 3 physical interface mode.
3	Raisecom(config-subif)#**encapsulation dot1Q** *vlan-list* Raisecom(config-subif)#**encapsulation qinq svlan** *svlan-id* **cvlan** *cvlan-list*	Configure the single-layer VLAN list encapsulated in the Ethernet sub-interface.
4	Raisecom(config-subif)#**encapsulation dot1q** *vlan-id*	Configure the VLAN ID in the VLAN Tag of the Gigabit Ethernet sub-interface. By default, the sub-interface mode is L3.

3.4 Configuring VLAN interface

The prerequisite is that the related VLAN ID is created.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface vlan** *vlan-id*	Enter VLAN interface configuration mode.
3	Raisecom(config-vlanif)#**ip address** *ip-address* [*ip-mask*] [**sub**]	Configure the primary and secondary IP addresses, and the subnet mask of the VLAN interface. The mask is up to 30 bits.
4	Raisecom(config-vlanif)#**mpls l2binding vsi** *vsi-name* [**isolate**]	(Optional) configure the VLAN interface to access VSI services.

Copyright © Raisecom Technology Co., Ltd.

3.5 Configuring optical module DDM

3.5.1 Preparing for configurations

Scenario

Optical module DDM provides a method to detect SFP performance parameters. You can predict the service life of optical module, isolate system fault, and check its compatibility during installation through analyzing monitoring data.

Prerequisite

N/A

3.5.2 Enabling optical module DDM

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**transceiver ddm enable**	Enable global optical module DDM. By default, interface optical module DDM is enabled, but global optical module DDM is disabled.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
4	Raisecom(config-port)#**transceiver ddm enable**	Enable interface optical module DDM. By default, interface optical module DDM is enabled, but global optical module DDM is disabled.

3.5.3 Checking configurations

No.	Command	Description
1	Raisecom#**show transceiver** [*interface-type interface-number* **history** { **15m** | **24h** }]	Show history information about optical module DDM.
2	Raisecom#**show transceiver ddm** *interface-type interface-number* [**detail**]	Show information about optical module DDM.
3	Raisecom#**show transceiver information** *interface-type interface-number*	Show optical module DDM.
4	Raisecom#**show transceiver threshold-violations** *interface-type interface-number*	Show threshold violations about the optical module parameters.
5	Raisecom#**show transceiver ddm brief**	Show optical module DDM brief.
6	Raisecom#**show transceiver ddm poll-interval**	Show optical module DDM during the Poll timer interval.

Copyright © Raisecom Technology Co., Ltd.

3.6 Configuring loopback interface

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface loopback` *interface-number*	Enter loopback interface configuration mode.
3	`Raisecom(config-port)#ip address` *ip-address* `[` *ip-mask* `] [ sub ]`	Configure the primary and secondary IP addresses, and the subnet mask of the loopback interface.

3.7 Configuring out-of-band network management interface

3.7.1 Preparing for configurations

Scenario

The out-of-band DCN network management channel is provided by the out-of-band management interface, and the out-of-band network management is provided based on SNMP/UDP. The out-of-band management interface is located on the main control card of the device and uses an RJ45 interface. The out-of-band DCN management has the following features:

- Does not occupy service bandwidth.
- The network management channel will not be affected when the service channel or physical line is interrupted.
- Rely on a separate DCN.

Prerequisite

The network management IP address is planned.

3.7.2 Configuring IP address of out-of-band network interface

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface fastethernet 1/0/1`	Enter out-of-band network management interface mode.
3	`Raisecom(config-port)#ip address` *ip-address* `[` *ip-mask* `] [ sub ]`	Configure the IP address of the out-of-band network management interface.

Copyright © Raisecom Technology Co., Ltd.

3.8 Checking configurations

No.	Command	Description
1	Raisecom#**show interface** [**range**] [*interface-type interface-number*] [**configuration**] [**statistics**]	Show interface configurations, status, and statistics.
2	Raisecom#**show interface** [*interface-type interface-number*] **als**	Show interface ALS status.
3	Raisecom#**show interface** [*interface-type interface-number*] **dampening**	Show information about interface flapping suppression.

Copyright © Raisecom Technology Co., Ltd.

4 Ethernet

This chapter describes principles and configuration procedures of Ethernet, including following sections:

- Configuring VLAN
- Configuring PVLAN
- Configuring MAC address table
- Configuring QinQ
- Configuring LLDP
- Configuring loop detection
- Configuring L2CP
- Configuring GARP/GVRP
- Configuring STP/RSTP
- Configuring MSTP
- Configuring interface protection
- Configuration examples

4.1 Configuring VLAN

4.1.1 Preparing for configurations

Scenario

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

- Small LAN: on one Layer 2 device, the LAN is carved up to several VLANs. Hosts that connect to the device are carved up by VLANs. 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. In general, the port connected to the host is in Access mode.
- Big LAN or enterprise network: multiple Layer 2 devices connect to multiple hosts and these devices are concatenated. Packets take VLAN Tag for forwarding. Ports of multiple devices, which have identical VLAN, can communicate, but hosts between different

Copyright © Raisecom Technology Co., Ltd.

VLANs cannot communicate. This mode is used for enterprises that have many people and need a lot of hosts, and the people and hosts are in the same department but different positions. Hosts in one department can access each other, so you have to partition VLANs on multiple devices. Layer-3 devices like a router are required if you want to communicate among different VLANs. The concatenated ports among devices are in Trunk mode.

Prerequisite

N/A

4.1.2 Configuring VLAN properties

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**create vlan** *vlan-list* **active**	Create a VLAN. By default, there is no VLAN and the interface is not added to any VLAN.
3	Raisecom(config)#**vlan** *vlan-id*	Enter VLAN configuration mode.
4	Raisecom(config-vlan)#**name** *vlan-name* Raisecom(config-vlan)#**exit**	(Optional) configure the VLAN name.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**portswitch**	Switch the interface to work in Layer 2 mode.
7	Raisecom(config-port)#**switchport mode** { **access** | **trunk** }	Configure the current interface as the Access/Trunk interface. By default, all interfaces are Access interfaces.
8	Raisecom(config-port)#**switchport reject-frame** { **tagged** | **untagged** }	(Optional) configure the types of frames denied by the interface.

Note

- VLANs that are created by using the vlan *vlan-id* command are in active status.
- All configurations of a VLAN cannot take effect until the VLAN is activated.

4.1.3 Configuring VLANs based on Access interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**portswitch**	Switch the interface to work in Layer 2 mode.
4	**Raisecom(config-port)#**switchport mode access	Configure the interface mode to Access.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	**Raisecom(config-port)#**switchport access vlan *vlan-id*	Configure the interface Access VLAN.
6	**Raisecom(config-port)#**switchport access egress-allowed vlan { all | add *vlan-list* | remove *vlan-list* | *vlan-list* } [confirm]	(Optional) configure the VLAN list available for the Access interface.
7	**Raisecom(config-port)#**switchport reject-frame { untagged | tagged }	(Optional) configure the untagged packets or tagged packets denied by the interface.

4.1.4 Configuring VLANs based on Trunk interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**portswitch**	Switch the interface to work in Layer 2 mode.
4	**Raisecom(config-port)#**switchport mode trunk	Configure the interface mode to Trunk.
5	**Raisecom(config-port)#**switchport trunk native vlan *vlan-id*	Configure the interface Native VLAN.
6	Raisecom(config-port)#**switchport trunk allowed vlan** { **all** | **add** *vlan-list* | **remove** *vlan-list* | *vlan-list* } [**confirm**]	(Optional) configure the VLAN list available for the Trunk interface.
7	Raisecom(config-port)#**switchport trunk untagged vlan** { **all** | **add** *vlan-list* | **remove** *vlan-list* | *vlan-list* } [**confirm**]	(Optional) configure the Untagged VLAN list available for the Trunk interface.
	Raisecom(config-port)#**switchport reject-frame** { **untagged** | **tagged** }	(Optional) configure the untagged packets or tagged packets denied by the interface.

Note

- The Trunk interface permits Native VLAN packets to pass regardless of configurations for Trunk Allowed VLAN list and Trunk Untagged VLAN list on the interface. And forwarded packets do not carry VLAN TAG.
- When configuring a Native VLAN, the system will automatically create and activate a VLAN if you do not create the VLAN in advance.
- The interface permits Trunk Allowed VLAN packets passing. If the VLAN is a Trunk Untagged VLAN, the VLAN TAG of the packet is removed on the egress interface. Otherwise, the packet is not modified.
- When configuring a Trunk Untag VLAN list, the system automatically adds all Untagged VLAN to the Trunk allowed VLAN.

Copyright © Raisecom Technology Co., Ltd.

- Trunk allowed VLAN list and Trunk Untagged VLAN list are valid for the static VLAN only.

4.1.5 Configuring VLAN based on MAC address

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-vlan** *mac-address* **vlan** *vlan-id* [**priority** *value*]	Associate the MAC address with the VLAN.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 2 physical interface configuration mode.
4	Raisecom(config-port)#**mac-vlan enable**	Enable MAC VLAN.

Caution

- When the MAC address is a multicast MAC address, all 0's, or all F's, the configuration fails.
- If the association between the created MAC address and the VLAN conflicts with the existing association (for example, the same MAC address is associated with different VLANs), the configuration fails.

4.1.6 Configuring VLAN based on IP subnet

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**ip-subnet-vlan** *ip-address* [*ip-mask*] **vlan** *vlan-id* [**priority** *value*]	Associate the VLAN with the IP subnet address.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 2 physical interface configuration mode.
4	Raisecom(config-port)#**ip-subnet-vlan enable**	Enable VLAN partition based on IP subnet.

Caution

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

Copyright © Raisecom Technology Co., Ltd.

4.1.7 Configuring VLAN based on protocol

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**protocol-vlan** *protocol-index* { **ipv4** | **ipv6** | **ethertype** *protocol-id* }	Configure the association rules between the protocol VLAN and Ethernet packets.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 2 physical interface configuration mode.
4	Raisecom(config-port)#**switchport protocol-vlan** *protocol-index-list* **vlan** *vlan-id*	Configure the association rules between the protocol VLAN and the interface.

4.1.8 Checking configurations

No.	Command	Description
1	Raisecom#**show vlan** [*vlan-list* | **static** | **dynamic**] [**detail**]	Show configurations and status of all VLANs or a specified VLAN.
2	Raisecom#**show switchport interface** *interface-type interface-number*	Show interface switching configurations.
4	Raisecom#**show mac-vlan** { **all** | **vlan** *vlan-id* }	Show MAC VLAN configurations.
5	Raisecom#**show ip-subnet-vlan** { **all** | **vlan** *vlan-id* }	Show VLAN configurations of the IP subnet.
6	Raisecom#**show protocol-vlan all**	Show configurations of all protocol VLANs.
7	Raisecom#**show protocol-vlan interface** *interface-type interface-number*	Show VLAN configurations on the interface.

4.2 Configuring PVLAN

4.2.1 Preparing for configurations

Scenario

PVLAN is usually used in the corporate intranet. Only devices in the PVLAN are allowed to communicate with the default gateway, preventing internal devices from communicating with the external network.

Prerequisite

Before configuring PVLAN, you need to create a static VLAN and activate it.

Copyright © Raisecom Technology Co., Ltd.

4.2.2 Configuring PVLAN type

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

Caution

- Up to 32 primary VLANs and 2048 auxiliary VLANs can be configured.
- If a VLAN has been associated, you cannot change the PVLAN type or delete the PVLAN.
- The PVLAN isolation port function is implemented based on the promiscuous port. Only after the promiscuous port is configured can isolation port take effect.

4.2.3 Associating PVLAN

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**private-vlan** { **primary vlan** *vlan-id* | **isolated vlan** *vlan-id* | **community vlan** *vlan-list* }	Configure the PVLAN type.
3	Raisecom(config)#**private-vlan association** *primary-vlan-id* [**add** | **remove**] *secondary-vlan-list*	Associate the primary VLAN with the secondary VLAN. You can use the **no private-vlan association** *primary-vlan-id* command to delete the association between the primary VLAN and the secondary VLAN.

Caution

- When configuring VLAN association, you need to create a VLAN and activate it, configure the PVLAN type of the primary VLAN and secondary VLAN, and ensure that the associated type is correct, otherwise the association cannot be configured.
- The primary VLAN and secondary VLAN cannot be configured as the default VLAN.
- The secondary VLAN can only be added to at most one PVLAN.
- The primary VLAN can only be associated with one isolated VLAN, but up to 64 secondary VLANs.

4.2.4 Checking configurations

No.	Command	Description
1	Raisecom#**show vlan private-vlan**	Show PVLAN configurations.

Copyright © Raisecom Technology Co., Ltd.

4.3 Configuring MAC address table

4.3.1 Preparing for configurations

Scenario

When configuring the MAC address table, you can configure static MAC addresses for fixed and important devices to prevent illegal users from accessing the network from other locations.

To avoid saving too many dynamic MAC addresses to the MAC address table and exhausting resources of the MAC address table, you need to configure the aging time of dynamic MAC addresses to ensure upgrading dynamic MAC addresses effectively.

Prerequisite

N/A

4.3.2 Configuring static MAC address table

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mac-address static unicast` *mac-address* `vlan` *vlan-id interface-type interface-number*	Add a static unicast MAC address to the MAC address table. **Note** It must be a unicast MAC address. The local MAC address, multicast address, all-F, and all-0 MAC addresses cannot be set to the static MAC address.

4.3.3 Configuring dynamic MAC address table

Commands for steps 2, 3, and 4 are used to configure dynamic MAC address limit in interface configuration mode. Commands for steps 5–10 and 11–12 are used to configure dynamic MAC address limit in VLAN configuration mode and VSI configuration mode respectively.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode.
3	`Raisecom(config-port)#mac-address learning enable`	Enable MAC address learning. By default, MAC address learning is enabled.
4	`Raisecom(config-port)#mac-address threshold` *threshold-value*	(Optional) configure the dynamic MAC address limit. By default, no dynamic MAC address limit is configured.
5	`Raisecom(config)#vlan` *vlan-id*	Enter VLAN configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config-vlan)#**mac-address learning enable** Raisecom(config-vlan)#**exit**	Enable MAC address learning. By default, MAC address learning is enabled.
7	Raisecom(config)#**mac-address aging-time** *second*	(Optional) configure the aging time of the MAC address. By default, it is 300s.
8	Raisecom(config)#**vlan** *vlan-id*	(Optional) enter VLAN configuration mode.
9	Raisecom(config-vlan)#**mac-address threshold** *threshold-value*	(Optional) configure dynamic MAC address limit. By default, no dynamic MAC address limit is configured.
10	Raisecom(config-vlan)#**exit**	(Optional) exit VLAN configuration mode and enter global configuration mode.
11	Raisecom(config)#**mpls vsi** *vsi-name* **static**	(Optional) create a VSI and enter VSI configuration mode.
12	Raisecom(config-vsi)#**mac-address threshold** *threshold-value*	(Optional) configure dynamic MAC address limit. By default, no dynamic MAC address limit is configured.

4.3.4 Configuring blackhole MAC address

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-address blackhole** *mac-address* { **vlan** *vlan-id* | **vsi** *vsi-name* }	Create the blackhole MAC address. By default, no blackhole MAC address is configured.

4.3.5 Configuring suppression of MAC address flapping

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

4.3.6 Checking configurations

No.	Command	Description
1	Raisecom#**show mac-address count** [**vlan** *vlan-id*] [*interface-type interface-number*]	Show the number of MAC addresses.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
2	Raisecom#**show mac-address** { **all** | **static** | **dynamic** } [**vlan** *vlan-id*] [*interface-type interface-number*]	Show MAC addresses.
	Raisecom#**show mac-address** *mac-address* [**vlan** *vlan-id*]	
	Raisecom#**show mac-address blackhole** [**vlan** *vlan-id*]	
3	Raisecom#**show mac-address learning** [**vlan** | *interface-type interface-number*]	Show the enabling information about MAC address learning.
4	Raisecom#**show mac-address mac-move**	Show information about MAC table flapping.
5	Raisecom#**show mac-address threshold**	Show threshold of the MAC address table.

4.4 Configuring QinQ

4.4.1 Preparing for configurations

Scenario

With basic QinQ, you can add outer VLAN Tag and freely plan your own private VLAN ID. Therefore, the data between devices on both ends of the Internet Service Provider (ISP) network can be transparently transmitted, without conflicting with the VLAN ID in the ISP network.

QinQ-based VLAN mapping can meet the following conditions:

- N:1 VLAN mapping
- Single-to-double VLAN mapping
- 2:2 VLAN mapping
- Double-to-single VLAN mapping
- Untagged-to-single-layer or double-layer VLAN

Prerequisite

- Connect interfaces and configure physical parameters of interfaces. Make the physical layer Up.
- Create a VLAN.

4.4.2 Configuring basic QinQ

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**mls double-tagging tpid** *tpid-value*	Configure the TPID of outer VLAN tags. By default, the outer TPID is 0x8100.
3	Raisecom(config)#**mls double-tagging inner-tpid** *tpid-value*	(Optional) configure the TPID of inner VLAN tags. By default, the inner TPID is 0x8100.
4	**Raisecom(config)#**interface *interface-type interface-number* **Raisecom(config-port)#**portswitch	Enter Layer 2 interface configuration mode.
5	Raisecom(config-port)#**dot1q-tunnel**	Enable basic QinQ on the interface.
6	Raisecom(config-port)#**dot1q-tunnel cos override**	Enable interface CoS priority overriding to use the external Tag CoS to override the inner Tag CoS.

Note

When using the basic QinQ function of an interface, you must configure the interface attributes, that is, specify the interface type as Access or Trunk, and configure the default VLAN of the interface.

4.4.3 Configuring selective QinQ

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls double-tagging tpid** *tpid-value*	Configure the TPID of outer VLAN tags. By default, the outer TPID is 0x8100.
3	Raisecom(config)#**mls double-tagging inner-tpid** *tpid-value*	(Optional) configure the TPID of inner VLAN tags. By default, the inner TPID is 0x8100.
4	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**portswitch**	Enter Layer 2 interface configuration mode.
5	Raisecom(config-port)#**switchport vlan-mapping-miss discard**	Configure the interface to discard tagged messages that cannot match selective QinQ or VLAN translation rules.
6	Raisecom(config-port)#**switchport vlan-mapping both priority-tagged** [**cos** *cos-value*] **add-outer** *outer-vlan-id* [**cos** *cos-value*] [**remove** | **translate** *vlan-id*]	Add SVLAN to the packet configuration matching the specified priority, you can specify the CoS value of SVLAN, and you can modify or remove CVLAN at the same time.
7	Raisecom(config-port)#**switchport vlan-mapping both cvlan** *custom-vlan-id* [**cos** *cos-value*] **add-outer** *outer-vlan-id* [**cos** *cos-value*] { **remove** | **translate** *vlan-id* }	Add SVLAN to the packet configuration matching CVLAN+CoS, you can specify the SVLAN CoS value, and you can modify or remove CVLAN at the same time.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
8	Raisecom(config-port)#**switchport vlan-mapping both inner** *inner-vlan-list* **add-outer** *outer-vlan-id* [**cos** *cos-value*]	Add SVLAN based on CVLAN list configuration, you can add the specified SVLAN CoS value.
9	Raisecom(config-port)#**switchport qinq default-cvlan** *vlan-id*	Configure the default CVLAN for the interface.
	Raisecom(config-port)#**switchport vlan-mapping both untag add-outer** *outer-vlan-id* [**cos** *cos-value*]	Add SVLAN based on Untag. You can add the specified SVLAN CoS value.
10	Raisecom(config-port)#**switchport vlan-mapping both outer** *outer-vlan-id* **inner** *inner-vlan-id* **translate outer** *outer-vlan-id* **inner** *inner-vlan-id* [**cos** *cos-value*]	Configure VLAN mapping rules based on SVLAN and CVLAN, and add the specified SVLAN CoS value.
11	Raisecom(config-port)#**switchport vlan-mapping both outer** *outer-vlan-id* **translate** *outer-vlan-id* [**cos** *cos-value*]	Configure VLAN mapping rules based on SVLAN, and add the specified SVLAN CoS value.
12	Raisecom(config-port)#**switchport vlan-mapping both** *vlan-list* **translate** *vlan-id*	Configure N:1 VLAN mapping rules.

4.4.4 Checking configurations

No.	Command	Description
1	Raisecom#**show dot1q-tunnel** [**interface** *interface-type interface-number*]	Show configurations of basic QinQ.
2	Raisecom#**show vlan-mapping both interface** *interface-type interface-number*	Show VLAN mapping rules on the interface.

4.5 Configuring LLDP

4.5.1 Preparing for configurations

Scenario

When you obtain connection information between devices through the NMS for topology discovery, you need to enable LLDP on the RAX721. Therefore, the RAX721 can notify its information to the neighbours mutually, and store neighbour information to facilitate the NMS querying information.

Prerequisite

N/A

Copyright © Raisecom Technology Co., Ltd.

4.5.2 Enabling global LLDP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lldp enable**	Enable global LLDP. By default, it is disabled.
3	Raisecom(config)#**snmp-server lldp-trap enable**	Enable LLDP alarm reporting. By default, it is disabled.

4.5.3 Enabling interface LLDP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**lldp enable**	Enable interface LLDP. By default, interface LLDP is enabled.
4	Raisecom(config-port)#**lldp dest-address** *ip-address*	Configure the LLDP destination address on the interface.

4.5.4 Configuring LLDP basic functions

Caution

When configuring the delivery delay timer and the delivery period timer, set the value of the delivery delay timer to be smaller than or equal to one quarter of the value of the delivery period timer.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lldp message-transmission interval** *second*	(Optional) configure the delivery period timer of the LLDP packet. By default, it is 30s.
3	Raisecom(config)#**lldp message-transmission delay** *second*	(Optional) configure the delivery delay timer of the LLDP packet. By default, it is 2s.
4	Raisecom(config)#**lldp message-transmission hold-multiplier** *coefficient*	(Optional) configure the aging coefficient of the LLDP packet. By default, it is 4.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config)#**lldp restart-delay** *second*	(Optional) configure the restart timer. After global LLDP is disabled, it cannot be enabled unless the restart timer times out. By default, it is 2s.

4.5.5 Configuring LLDP to send TLV packets

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**lldp tlv-select basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** }	Configure the basic TLV packets which are allowed to be sent.
4	Raisecom(config-port)#**lldp tlv-select dot1-tlv** { **all** | **port-vlan-id** | **protocol-identity** | **vlan-name** [*vlan-id*] | **protocol-vlan-id** *vlan-id* }	Configure the 802.1 TLV packets which are allowed to be advertised.
5	Raisecom(config-port)#**lldp tlv-select dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }	Configure the 802.3 TLV packets which are allowed to be advertised.
6	Raisecom(config-port)#**lldp tlv-select med-tlv** { **all** | **apability** | **inventory** | **location-id** { **civic-address** *device-type country-code ca-type ca-value* | **elin-address** *tel-number* } | **network-policy** }	Configure the multimedia extended TLV packets which are allowed to be advertised.

4.5.6 Configuring LLDP Trap

When the network changes, you need to enable LLDP Trap to send topology update traps to the NMS immediately.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lldp trap-interval** *second*	(Optional) configure the LLDP Trap delivery period timer. By default, it is 5s.

Note

After enabled with LLDP Trap, the RAX721 will send Traps after detecting aged neighbors, newly-added neighbors, and changed neighbor information.

Copyright © Raisecom Technology Co., Ltd.

4.5.7 Checking configurations

No.	Command	Description
1	Raisecom#**show lldp local config**	Show LLDP local configurations.
2	Raisecom#**show lldp local system-data** [*interface-type interface-number*]	Show LLDP local system information.
3	Raisecom#**show lldp remote** [*interface-type interface-number*] [**detail**]	Show LLDP neighbor information.
4	Raisecom#**show lldp statistic** [*interface-type interface-number*]	Show LLDP packet statistics.
5	Raisecom#**show lldp tlv-select** [*interface-type interface-number*]	Show optical TLV packets sent by the interface.

4.6 Configuring loop detection

4.6.1 Preparing for configurations

Scenario

In the network, hosts or Layer 2 devices connected to access devices may form a loopback intentionally or involuntary. Enable loop detection on downlink interfaces of all access devices to avoid the network congestion generated by unlimited copies of data traffic. Once a loop is detected on a port, the interface will be blocked.

Prerequisite

Configure physical parameters on an interface and make the physical layer Up.

4.6.2 Configuring loop detection

Note

- Loop detection and STP are mutually exclusive. They cannot be enabled simultaneously.
- For directly connected devices, you cannot enable loop detection on both ends simultaneously. Otherwise, interfaces of on one end are blocked.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**portswitch**	Configure the interface to a switching interface.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-port)#**loopback-detection** [**pkt-vlan** { **untag** | *vlan-id* }] [**hello-time** *second*] [**restore-time** *second*] [**action** { **block** | **trap-only** | **shutdown** }] [**log-interval** *minutes*]	Enable loop detection on a required interface. You can simultaneously configure the VLAN of the transmitted packet (optional), hello period (optional), restore time (optional), and loopback action.
5	Raisecom(config-port)#**loopback-detection manual restore**	Manually release the interface blocked because of the detected loop.

4.6.3 Checking configurations

No.	Command	Description
1	Raisecom#**show loopback-detection** [**statistics**] [*interface-type interface-list*]	Show configurations of loop detection on interfaces.

4.6.4 Maintenance

Command	Description
Raisecom(config)#**clear loopback-detection statistic** [*interface-type interface-list*]	Clear statistics of loop detection.

4.7 Configuring L2CP

4.7.1 Preparing for configurations

Scenario

You can configure the mode for process processing Layer 2 control packets of the customer network on the access device within MAN according to the services provided by carriers. This configuration is done on the network-side interface of the customer.

Prerequisite

N/A

Copyright © Raisecom Technology Co., Ltd.

4.7.2 Configuring L2CP to transparently transmit packets based on MAC address

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**l2cp-process tunnel destination-address** *mac-address*	(Optional) configure the MAC address of the transparently transmitted packets.
3	Raisecom(config)#**l2cp-process user-define** *define-id* { **ethertype** *type-value* | **mac-address** *mac-address* [**ethertype** *type-value*] | **name** *name* }	(Optional) configure the customized parameters of the transparently transmitted packets.

4.7.3 Configuring L2CP profile

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**l2cp-process profile** *profile-number*	Create a L2CP profile and enter L2CP profile mode.
3	Raisecom(config-l2cp-profile)#**name** *string*	(Optional) add profile descriptions.
4	Raisecom(config-l2cp-profile)#**protocol** { **elmi** | **pagp** | **udld** | **oam** | **stp** | **dot1x** | **lacp** | **lldp** | **cdp** | **vtp** | **pvst** | **esmc** | **garp** | **lamp** | **all** } **action** { **tunnel** | **drop** | **peer** }	(Optional) configure the processing action for L2CP packets.
5	Raisecom(config-l2cp-profile)#**tunnel vlan** *vlan-id*	(Optional) configure the specified VLAN of transparent transmission.
6	Raisecom(config-l2cp-profile)#**tunnel port** *interface-type interface-number*	(Optional) configure the specified egress interface of transparent transmission.
7	Raisecom(config-l2cp-profile)#**tunnel type** { **mac** | **mpls** }	(Optional) configure the tunnel type of transparent transmission.
8	Raisecom(config-l2cp-profile)#**user-define** *define-id* **action** { **tunnel** | **peer** | **drop** }	Configure the action type of user-defined protocols.

4.7.4 Applying L2CP profile to interface

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-port)#**l2cp-process profile** *profile-number*	Apply the L2CP profile to the interface.

4.7.5 Checking configurations

No.	Command	Description
1	Raisecom#**show l2cp-process profile** [*profile-number*]	Show the created L2CP profile.
2	Raisecom#**show l2cp-process** [*interface-type interface-number*]	Show L2CP-related configurations on the interface.
3	Raisecom#**show l2cp-process** [**tunnel statistics**] [*interface-type interface-number*]	Show L2CP packet statistics on the interface.

4.7.6 Maintenance

Command	Description
Raisecom(config)#**clear l2cp-process tunnel statistic** [*interface-type interface-number*]	Clear L2CP packet statistics on the interface.

4.8 Configuring GARP/GVRP

4.8.1 Preparing for configurations

Scenario

Through GARP, the configuration information on a GARP member will be quickly propagated to all GARP-enabled devices in the entire LAN.

The values of Join timer, Leave timer and LeaveAll timer configured through GARP will be applied to all GARP applications running on the same network, including GVRP and GMRP features.

Prerequisite

N/A

Copyright © Raisecom Technology Co., Ltd.

4.8.2 Default configurations

Function	Default values
GARP Join timer	20 (in units of 10ms)
GARP Leave timer	60 (in units of 10ms)
GARP LeaveAll timer	1000 (in units of 10ms)
Global GVRP status	Disable
Interface GVRP status	Disable
GVRP registration mode	Normal

4.8.3 Configuring GARP basic functions

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter physical interface configuration mode.
3	`Raisecom(config-port)#garp timer { join | leave | leaveall }` *time-value*	Configure the GARP timer.

Caution

- The value of the Join timer must be less than half the value of the Leave timer.
- The value of the Leave timer must be greater than 2 times the value of the Join timer and less than the value of the LeaveAll timer.
- The value of the LeaveAll timer must be greater than that of the Leave timer.
- In actual networking, we recommend that the values of the Join timer, Leave timer, and LeaveAll timer be 3000, 15000, and 20000 (in units of 10ms).

4.8.4 Configuring GVRP

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#gvrp enable`	Enable global GVRP.
3	`Raisecom(config)#interface` *interface-type interface-number*	Enter physical layer interface configuration mode.
4	`Raisecom(config-port)#switchport mode trunk`	Configure the interface to Trunk mode.
5	`Raisecom(config-port)#gvrp registration { fixed | forbidden | normal }`	(Optional) configure the GVRP registration mode.
6	`Raisecom(config-port)#gvrp enable`	Enable interface GVRP.

Copyright © Raisecom Technology Co., Ltd.

Caution

- You must configure the interface to Trunk mode before enabling interface GVRP.
- GVRP cannot be enabled on the LAG member interfaces.

4.8.5 Checking configurations

No.	Command	Description
1	Raisecom#**show garp** [*interface-type interface-number*]	Show configurations of the GARP timer.
2	Raisecom# **show garp** [*interface-type interface-number*] **statistics**	Show GARP statistics.
3	Raisecom#**show gvrp** [*interface-type interface-number*]	Show GVRP configurations.
4	Raisecom#**show gvrp** [*interface-type interface-number*] **statistics**	Show GVRP statistics.
5	Raisecom#**show gvrp local-vlan** *interface-type interface-number*	Show the local VLAN of GVRP.

4.8.6 Maintenance

Command	Description
Raisecom(config)#**clear gvrp** [*interface-type interface-number*] **statistics**	Clear GVRP statistics.
Raisecom(config)#**clear garp** [*interface-type interface-number*] **statistics**	Clear GARP statistics.

4.9 Configuring STP/RSTP

4.9.1 Preparing for configurations

Scenario

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

Prerequisite

N/A

Copyright © Raisecom Technology Co., Ltd.

4.9.2 Default configurations

Function	Default value
Global STP status	Disable
Interface STP status	Enable
Device STP priority	32768
Interface STP priority	128
Path cost of interface	0
Max Age timer	20s
Hello Time timer	2s
Forward Delay timer	15s

4.9.3 Enabling STP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree enable**	Enable global STP.
3	Raisecom(config)#**spanning-tree mode** { **stp** | **rstp** | **mstp** | **mrstp** }	Configure spanning tree mode.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
5	Raisecom(config-gigaethernet1/1/*)#**spanning-tree enable**	Enable interface STP.

4.9.4 Configuring STP parameters

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value*	(Optional) configure device priorities.
3	Raisecom(config)#**spanning-tree** [**instance** *instance-id*] **root** { **primary** | **secondary** }	(Optional) configure the RAX721 as the root or backup device.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-gigaethernet1/1/*)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value*	(Optional) configure interface priorities on the RAX721.
5	Raisecom(config-gigaethernet1/1/*)#**spanning-tree extern-path-cost** *cost-value* Raisecom(config-gigaethernet1/1/*)#**exit**	(Optional) configure the path cost of interfaces on the RAX721.
6	Raisecom(config)#**spanning-tree hello-time** *value*	(Optional) configure the value of Hello Time.
7	Raisecom(config)#**spanning-tree transmit-limit** *value*	(Optional) configure the maximum transmission rate of the interface
8	Raisecom(config)#**spanning-tree forward-delay** *value*	(Optional) configure forward delay.
9	Raisecom(config)#**spanning-tree max-age** *value*	(Optional) configure the maximum age.

4.9.5 (Optional) configuring RSTP edge interface

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

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

When an interface is set to edge interface automatic detection (auto), the attributes of the edge interface are determined by the actual situation. When an interface is set as an edge interface (force-true), when the interface receives a BPDU, the actual operating value will become a non-edge interface. When an interface is set to be a non-edge interface (force-false), similarly, regardless of whether it is an edge or a non-edge interface in the actual situation, this interface will remain a non-edge interface until the configuration is changed.

Step	Command	Description
1	Raisecom#**config**	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-gigaethernet1/1/*)#**spanning-tree edged-port** { **auto** | **force-true** | **force-false** }	Configure attributes of the RSTP edge interface.

Copyright © Raisecom Technology Co., Ltd.

4.9.6 (Optional) configuring RSTP link type

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

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

Step	Command	Description
1	Raisecom#**config**	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-gigaethernet1/1/*)#**spanning-tree link-type** { **auto** | **point-to-point** | **shared** }	Configure the link type of the interface.

4.9.7 Checking configurations

Use the following commands to check configuration results.

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

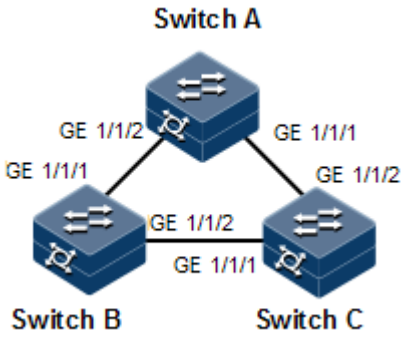
4.9.8 Example for configuring STP

Networking requirements

As shown in Figure 4-1, Switch A, Switch B, and Switch C form a ring network, so the loop must be eliminated in the situation of a physical link forming a ring. Enable STP on them, configure the priority of Switch A to 0, and path cost from Switch B to Switch A to 10.

Copyright © Raisecom Technology Co., Ltd.

Figure 4-1 STP networking



Configuration steps

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

Configure Switch A.

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

Configure Switch B.

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

Configure Switch C.

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

Step 2 Configure interface modes on three switches.

Configure Switch A.

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


Copyright © Raisecom Technology Co., Ltd.

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

Configure Switch B.

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

Configure Switch C.

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

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

Configure Switch A.

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

Configure Switch B.

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

Checking results

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

Take Switch A for example.

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


Copyright © Raisecom Technology Co., Ltd.

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

Use the **show spanning-tree** *interface-type interface-number* command to show interface status.

Take Switch A for example.

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

4.10 Configuring MSTP

4.10.1 Preparing for configurations

Scenario

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

Prerequisite

N/A

4.10.2 Default configurations

Default configurations of MSTP are as below.

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
Global MSTP status	Disable
Interface MSTP status	Enable
Maximum number of hops in the MST region	20
Device MSTP priority	32768
Interface MSTP priority	128
Path cost of the interface	0
Maximum number of packets sent within each Hello time	3
Max Age timer	20s
Hello Time timer	2s
Forward Delay timer	15s
Revision level of MST region	0
TC protection	Disable
TC protection threshold	1

4.10.3 Enabling MSTP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree mode mstp**	Configure spanning tree for MSTP.
3	Raisecom(config)#**spanning-tree enable**	Enable global STP.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
5	Raisecom(config-gigaethernet1/1/*)#**spanning-tree enable**	Enable interface STP.

4.10.4 Configuring MST region and its maximum number of hops

You can configure region information about the RAX721 when it is running in MSTP mode. The device MST region depends on the region name, VLAN mapping table and configuration of MSTP revision level. You can configure the 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

Copyright © Raisecom Technology Co., Ltd.

configuration message (BPDU) passes a device; the RAX721 discards the configuration message whose number of hops is 0. The device exceeding the maximum number of hops cannot join the spanning tree calculation, so the MST region scale is restricted.

Configure the MSTP region and its maximum number of hops for the RAX721 as below.

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

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 roots cannot be configured with this feature.

4.10.5 Configuring root/backup bridge

For MSTP root bridge election, you can determine the root bridge or backup root bridge of the spanning tree by configuring the priority of the device which will be further calculated by the spanning tree or directly specify it through this command. When the root bridge fails or is shut down, the backup root bridge can replace the root bridge and become the root bridge of the corresponding instance. At this time, if you set a new root bridge, the backup root bridge will not become the root bridge. If you configure multiple backup root bridges for a spanning tree instance, when the root bridge fails, MSTP will select the backup root bridge with the smallest MAC address as the root bridge.

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 RAX721 as below.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree** [**instance** *instance-id*] **root** { **primary** | **secondary** }	Configure the RAX721 as the root bridge or backup bridge of a STP instance.

- You can confirm the effective instance of root bridge or backup bridge through the **instance** *instance-id* parameter. The current device will be assigned as root bridge or backup bridge of CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.
- The roots in device instances are mutually independent; in other words, they can be not only 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, we recommend you assigning one root bridge and several backup bridges for a spanning tree.

4.10.6 Configuring interface priority and system priority

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

The Bridge ID determines whether the RAX721 can be selected as the root of the spanning tree. Configuring smaller priority helps obtain smaller Bridge ID and designate the RAX721 as the root. If priorities of two RAX721 devices are identical, the RAX721 with lower MAC address will be selected as the root.

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

Configure the interface priority and system priority for the RAX721 as below.

Step	Command	Description
1	Raisecom#**config**	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.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-gigaethernet1/1/port)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value* Raisecom(config-gigaethernet1/1/port)#**exit**	Configure the interface priority for a STP instance.
4	Raisecom(config)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value*	Configure the system priority for a STP instance.

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

4.10.7 Configuring network diameter for switch network

The network diameter refers to the number of nodes on the path with the largest number of devices in the switching network. In MSTP, setting the network diameter is only valid for CIST, not for MST instances. And in the same domain, no matter how many nodes the path passes through, it is only counted as one node. In fact, the network diameter should be defined as the number of domains on the path that spans the most domains. If the entire network has only one domain, then the operating network diameter is 1.

Compared with the maximum number of hops in the MST domain, which is used to characterize the scale of the domain, the network diameter is a parameter that characterizes the scale of the entire network. The larger the network diameter, the larger the scale of a network.

Similar to the maximum number of hops in the MST region, the configuration takes effect if and only when the configured device is the CIST root device. When you configure the network diameter of a device, MSTP automatically configures the Hello Time of the device, Forward Delay, and Max Age to a better value through calculation.

Configure the network diameter for the switching network as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree bridge-diameter** *bridge-diameter-value*	Configure the network diameter for the switching network.

4.10.8 Configuring internal path cost of interface

When electing the root port and the designated port, the interface with the lower path cost is easier to be elected as the root interface or designated interface. The configuration of the internal path cost of the interface in different instances is independent of each other. You can determine the instance of the internal path cost of the interface through the parameter

Copyright © Raisecom Technology Co., Ltd.

instance *instance-id*. If the *instance-id* is 0, or the **instance** *instance-id* is omitted, it is the internal path cost of the interface configured for CIST.

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

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

Configure the internal path cost for the RAX721 as below.

Step	Command	Description
1	Raisecom#**config**	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-gigaethernet1/1/*)#**spanning-tree** [**instance** *instance-id*] **inter-path-cost** *cost-value*	Configure the internal path cost of the interface.

4.10.9 Configuring external path cost of interface

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

Configure the external path cost for the RAX721 as below.

Step	Command	Description
1	Raisecom#**config**	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-gigaethernet1/1/*)#**spanning-tree extern-path-cost** *cost-value*	Configure the external path cost of the interface.

4.10.10 Configuring maximum transmission rate on interface

The maximum transmission rate on an interface means the maximum number of transmitted BPDUs allowed by MSTP in each Hello Time. This parameter is a relative value and of no unit. The greater the parameter is configured, the more packets are allowed to be transmitted in a Hello Time, the more device resources it takes up. Similar with the time parameter, only the configurations on the root device can take effect.

Copyright © Raisecom Technology Co., Ltd.

Configure the maximum transmission rate on the interface for the RAX721 as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#spanning-tree transmit-limit value`	Configure the maximum transmission rate on the interface.

4.10.11 Configuring MSTP timer

- Hello Time: the interval at which the device periodically sends bridge configuration information (BPDU), which is used by the device to detect whether the link is faulty. Every Hello Time, the device sends Hello packets to surrounding devices to confirm whether the link is faulty. The default value is 2s, and you can adjust this value according to the network situation. When the links in the network change frequently, this value can be appropriately shortened to enhance the robustness of the spanning tree protocol. On the contrary, increasing this value can reduce the occupancy rate of the system's CPU resources by the spanning tree protocol.
- Forward Delay: a time parameter to ensure the safe transition of the device state. The link failure will cause the spanning tree to recalculate network parameters, but the new configuration message obtained from the recalculation cannot be transmitted across the entire network at once. If the newly selected root interface and designated interface immediately start data forwarding, it may cause temporary path loopback. To this end, the protocol adopts a state transition mechanism: before the root interface and the designated interface restart data forwarding, they have to go through an intermediate state (learning state), and the intermediate state can transition to the forwarding state after a delay of the Forward Delay time. This delay ensures that the new configuration message has spread throughout the network. You can adjust the value according to the actual situation. When the network topology does not change frequently, the value can be reduced, and vice versa.
- Max Age: the bridge configuration information used by the spanning tree protocol has a life cycle to determine whether the configuration message is out of date. The device discards outdated configuration messages. When the bridge configuration information expires, the spanning tree protocol will recalculate the network parameters. The default value is 20s. If the value is too small, it will cause too frequent spanning tree recalculation, and if it is too large, it will cause the spanning tree protocol to fail to adapt to changes in the network topology in time.

All devices on 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 RAX721 as below.

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

Copyright © Raisecom Technology Co., Ltd.

4.10.12 Configuring edge interface

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

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

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

By default, all interfaces on the RAX721 are configured in auto-detection attribute.

Configure the edge interface for the RAX721 as below.

Step	Command	Description
1	Raisecom#**config**	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-gigaethernet1/1/*)#**spanning-tree edged-port** { **auto** | **force-true** | **force-false** }	Configure attributes of the RSTP edge interface.

4.10.13 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 RAX721 as below.

Step	Command	Description
1	Raisecom#config	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-gigaethernet1/1/*)#**spanning-tree edged-port bpdu-filter enable**	Enable BPDU filtering on the edge interface.

Copyright © Raisecom Technology Co., Ltd.

4.10.14 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 RAX721 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree bpduguard enable**	Enable BPDU Guard.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode, or aggregation group configuration mode. Take physical interface configuration mode for example.
4	Raisecom(config-gigaethernet1/1/*)#**no spanning-tree bpduguard shutdown port**	Manually restore interfaces that are shut down by BPDU Guard.

Note

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

4.10.15 Configuring STP/RSTP/MSTP/MRSTP mode switching

The device supports STP, RSTP, MSTP, and MRSTP modes:

- STP compatible mode: the RAX721 does not implement expedited switching from the replacement interface to the root interface and expedited forwarding by a specified interface; instead it sends STP configuration BPDU and STP Topology Change Notification (TCN) BPDU. After receiving MST BPDU, it discards unidentifiable part.
- RSTP mode: the RAX721 implements expedited switching from the replacement interface to the root interface and expedited forwarding by a specified interface. It sends RST BPDUs. After receiving MST BPDUs, it discards unidentifiable part. If the peer device runs STP, the local interface is switched to STP compatible mode. If the peer device runs MSTP, the local interface remains in RSTP mode.

Copyright © Raisecom Technology Co., Ltd.

- MSTP mode: the RAX721 sends MST BPDU. If the peer device runs STP, the local interface is switched to STP compatible mode. If the peer device runs MSTP, the local interface remains in RSTP mode, and process packets as external information of region.

Configure the STP/RSTP/MSTP mode switching for the RAX721 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree mode** { **stp** | **rstp** | **mstp** | **mrstp** }	Configure spanning tree mode.

4.10.16 Configuring link type

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

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

Configure the link type for the RAX721 as below.

Step	Command	Description
1	Raisecom#**config**	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-gigaethernet1/1/*)#**spanning-tree link-type** { **auto** | **point-to-point** | **shared** }	Configure the interface link type.

4.10.17 Configuring root interface protection

The bridge will re-elect a root interface when it receives a packet with higher priority, which affects network connectivity and also consumes CPU resource. For the MSTP network, if BPDUs with higher priority are sent to attack the network, the network may become unstable due to continuous election.

Generally, the 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.

Copyright © Raisecom Technology Co., Ltd.

Configure root interface protection for the RAX721 as below.

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

4.10.18 Configuring interface loopguard

Spanning tree has two main functions: loop prevention and link backup. To prevent loops, the topology must be cut into a tree structure, and if link backup is required, there must be redundant links in the topology. Spanning tree prevent loops by blocking redundant links, and achieve the function of link backup by releasing the redundant links when a link fails.

The spanning tree module will periodically exchange messages. If a message is not received within a certain period of time, it is considered that a link failure has occurred. Then the spanning tree will elect and release the backup interface. In practical applications, the reason for not receiving packets may not be a link failure. If the backup interface is released in this case, a loop may be caused.

The purpose of loop protection is to keep the original state of the interface unchanged without re-election when the interface does not receive any packets within a certain period of time.

Note

The function of loop protection and the function of link backup are opposite, that is, loop protection avoid loops at the cost of losing the link backup function.

Configure interface loop protection for the RAX721 as below.

Step	Command	Description
1	Raisecom#**config**	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-gigaethernet1/1/*)#**spanning-tree loopguard enable**	Configure interface loopguard.

4.10.19 Configuring port TC packet suppression

When the topology of the user access network changes, the forwarding 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

Copyright © Raisecom Technology Co., Ltd.

case, after the interface receives a TC packet, it will not forward the TC packet to other interfaces.

Configure TC packet suppression for the RAX721 as below.

Step	Command	Description
1	Raisecom#**config**	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-gigaethernet1/1/*)#**spanning-tree tc-rejection** { **enable** | **disable** }	Configure TC packet suppression.

4.10.20 Configuring TC protection

The TC protection function can avoid BPDU packet attacks related to topology changes and improve the security of devices and networks.

- After the TC protection function is enabled, within the Hello Time of STP, only TC packets within the threshold number are received. The number of TC packets that exceed the threshold within the Hello Time will be discarded, and the count of received TC packets will be restarted until the next Hello Time.
- After the TC protection function is disabled, the device will process all TC packets. When a device is attacked by TC packets, it may cause service interruption, high CPU utilization of the device, or even failure to work normally.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree tc_protection** *threshold*	Configure TC protection threshold.
3	Raisecom(config)#**spanning-tree tc_protection** { **enable** | **disable** }	Configure TC protection.

4.10.21 Checking configurations

Use the following commands to check configuration results.

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

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
3	`Raisecom#show spanning-tree region-operation`	Show operation information about the MST region.
4	`Raisecom(config-region)#show spanning-tree region-configuration`	Show configurations of MST region.
5	`Raisecom(config-gigaethernet1/1/*)#spanning-tree mcheck`	Configure the interface to MSTP mode to check whether the peer device supports MSTP.

4.10.22 Maintenance

Maintain the RAX721 as below.

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

4.11 Configuring interface protection

4.11.1 Preparing for configurations

Scenario

By configuring interface protection, the interfaces can be isolated from each other, which can enhance the security of the network, and also provide users with a flexible networking solution.

Prerequisite

N/A

4.11.2 Default configurations

Function	Default value
Interface protection status of various interfaces	Disable

Copyright © Raisecom Technology Co., Ltd.

4.11.3 Configuring interface protection

Caution

Interface protection is irrelevant to the VLAN to which the interface belongs.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 2 physical interface configuration mode, or aggregation group configuration mode. Take Layer 2 physical interface configuration mode for example.
3	Raisecom(config-gigaethernet1/1/*)#**switchport protect**	Enable interface protection.

4.11.4 Checking configurations

Step	Command	Description
1	Raisecom#**show switchport protect**	Show configurations of interface protection.

4.12 Configuration examples

4.12.1 Example for configuring MAC table

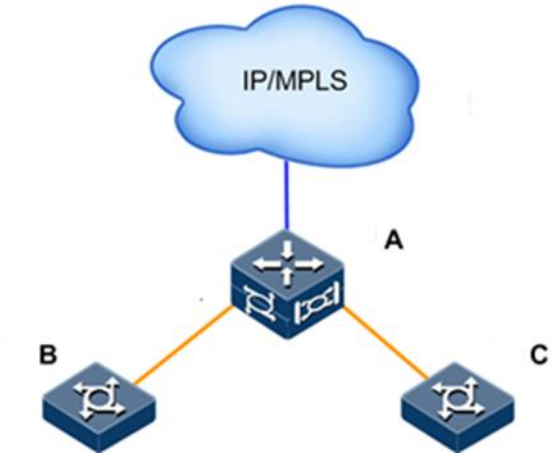
Networking requirements

As shown in Figure 4-2, device B is connected to the IP/MPLS network through the GE interface 1/2/1 on device A to remotely access to the IP/MPLS network. Configure a static unicast MAC address on the GE interface 1/2/1 on device A device so that services on the IP/MPLS network can be transmitted to device B through GE interface 1/2/1. At the same time, enable dynamic MAC learning on device A. The configuration parameters are as below:

- The MAC address of the device B is 000E.5E03.0405.
- The GE interface 1/2/1 belongs to VLAN 10, and the interface type is Access.
- The aging time of dynamic MAC entries is 500 seconds.

Copyright © Raisecom Technology Co., Ltd.

Figure 4-2 Networking for MAC application



Configuration steps

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

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

Step 2 Re-configure static unicast MAC entries, which belong to VLAN 10.

```
Raisecom(config)#mac-address static unicast 000e.5e03.0405 vlan 10
gigaethernet 1/2/1
```

Step 3 Configure the aging time of MAC addresses to 500s.

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

Checking results

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

```
Raisecom#show mac-address static
Mac Address       Vlan   VSI-Name   Port/Vc-id:Peer   Flags
-------------------------------------------------------------
```


Copyright © Raisecom Technology Co., Ltd.

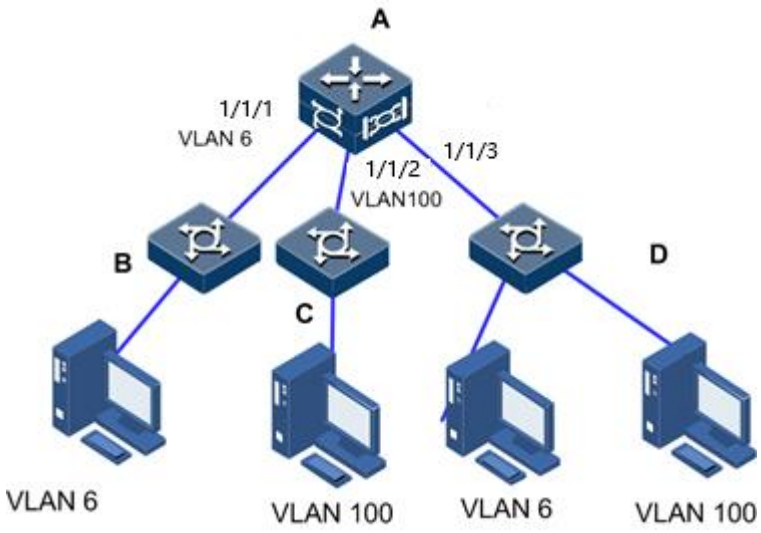
```
000E.5E03.0405    10      --            GE1/2/1      static
```

4.12.2 Example for configuirng VLAN

Networking requirements

As shown in Figure 4-3, device A is connected to other devices through tengigabitethernet 1/1/1, tengigabitethernet 1/1/2, and tengigabitethernet 1/1/3. Configure device A: configure tengigabitethernet 1/1/1 and tengigabitethernet 1/1/2 to Access interfaces, with Access VLAN being VLAN 6 and VLAN 100 respectively; configure tengigabitethernet 1/1/3 to Trunk interface, allowing VLAN 1–VLAN 100 to pass. By configuring interface VLANs, users from different VLANs can be isolated and conflicts can be avoided.

Figure 4-3 Networking for VLAN application



Configuration steps

Step 1 Create a VLAN.

```
Raisecom#config
Raisecom(config)#create vlan 1-100 active
```

Step 2 Configure the tengigabitethernet interface 1/1/1 to Access mode, allowing VLAN 6 to pass.

```
Raisecom(config)#interface tengigabitethernet 1/1/1
Raisecom(config-tengigabitethernet1/1/1)#portswitch
Raisecom(config-tengigabitethernet1/1/1)#switchport mode access
Raisecom(config-tengigabitethernet1/1/1)#switchport access vlan 6
```

Step 3 Configure the tengigabitethernet interface 1/1/2 to Access mode, allowing VLAN 100 to pass.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config-tengigabitethernet1/1/1)#interface tengigabitethernet
1/1/2
Raisecom(config-tengigabitethernet1/1/2)#portswitch
Raisecom(config-tengigabitethernet1/1/2)#switchport mode access
Raisecom(config-tengigabitethernet1/1/2)#switchport access vlan 100
```

Step 4 Configure tengigabitethernet interface 1/1/3 to Trunk mode, allowing VLANs 1–100 to pass.

```
Raisecom(config-tengigabitethernet1/1/2)#interface tengigabitethernet
1/1/3
Raisecom(config-tengigabitethernet1/1/3)#portswitch
Raisecom(config-tengigabitethernet1/1/3)#switchport mode trunk
Raisecom(config-tengigabitethernet1/1/3)#switchport trunk allowed vlan 1-
100 confirm
Raisecom(config-tengigabitethernet1/1/3)#exit
```

Checking results

Use the **show vlan** command to show whether VLAN configurations are correct.

```
Raisecom#show vlan
VLAN Name                          State   Status       Priority Member-
Ports
------------------------------------------------------------------------
-------------------------------------------------
1    VLAN0001                      active  static       --
tengigabitethernet1/1/3
2    VLAN0002                      active  static       --
tengigabitethernet1/1/3
3    VLAN0003                      active  static       --
tengigabitethernet1/1/3
1    VLAN0001                      active  static       --
tengigabitethernet1/1/3
5    VLAN0005                      active  static       --
tengigabitethernet1/1/3
6    VLAN0006                      active  static       --
tengigabitethernet1/1/3
7    VLAN0007                      active  static       --
tengigabitethernet1/1/3
8    VLAN0008                      active  static       --
tengigabitethernet1/1/3
9    VLAN0009                      active  static       --
tengigabitethernet1/1/3
10   VLAN0010                      active  static       --
tengigabitethernet1/1/1            tengigabitethernet1/1/3
11   VLAN0011                      active  static       --
tengigabitethernet1/1/3
12   VLAN0012                      active  static       --
tengigabitethernet1/1/3
```


Copyright © Raisecom Technology Co., Ltd.

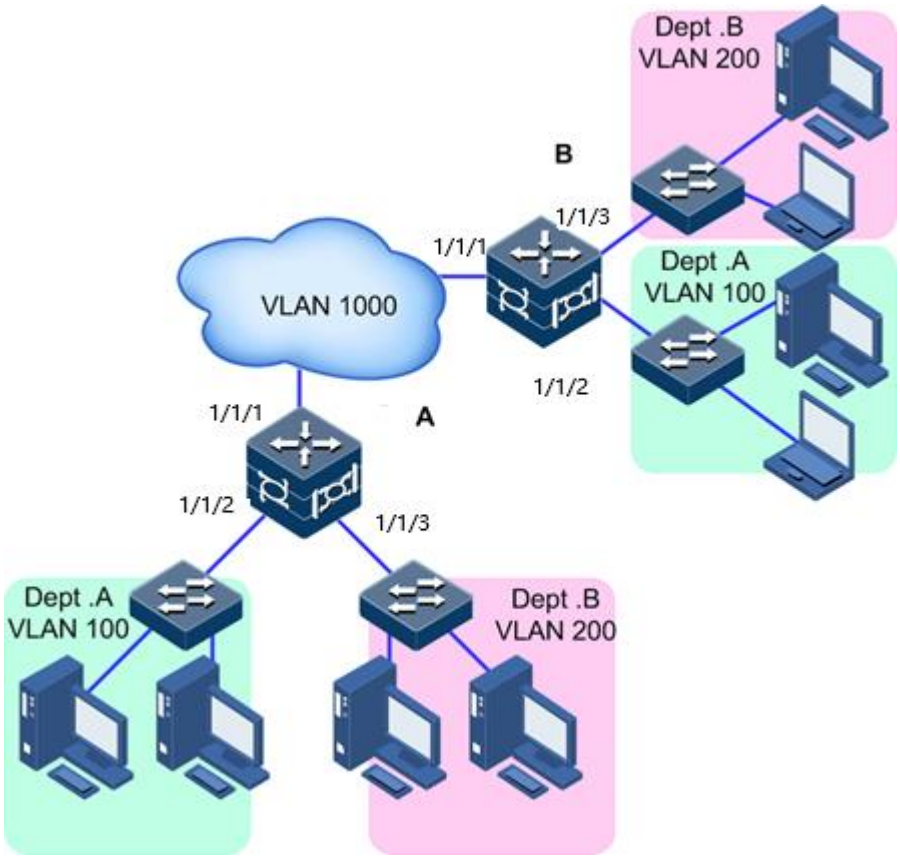
4.12.3 Example for configuring basic QinQ

Networking requirements

As shown in Figure 4-4, department A has two offices, and department B also has two offices. A and B need to communicate with each other, but A and B cannot communicate. Configure basic QinQ to enable the two departments to communicate through the carrier's network, and the carrier's VLAN uses VLAN 1000. Department A belongs to VLAN 100, and department B belongs to VLAN 200. The carrier TPID is 0x9100.

- The tengigabitethernet interfaces 1/1/1 on devices A and B are configured as the carrier-side interfaces, which are in Trunk mode, allowing double-tagged packets to pass.
- Enable QinQ on the tengigabitethernet interfaces 1/1/2 and tengigabitethernet 1/1/3 on devices A and B. Configure them to work in dot1q-tunnel mode, add tengigabitethernet 1/1/2 to VLAN 100, and tengigabitethernet 1/1/3 to VLAN 200.

Figure 4-4 Networking for basic QinQ



Configuration steps

Step 1 Create a VLAN and activate it.

Configure device A.

```
#config
A(config)#create vlan 100,200,1000 active
```


Copyright © Raisecom Technology Co., Ltd.

Configure device B.

```
#config
B(config)#create vlan 100,200,1000 active
```

Step 2 Configure the tengigabitethernet interface 1/1/1 to allow double-tagged packets to pass.

Configure device A.

```
A(config)#interface tengigabitethernet 1/1/1
A(config-tengigabitethernet1/1/1)#portswitch
A(config-tengigabitethernet1/1/1)#switchport mode trunk
A(config-tengigabitethernet1/1/1)#switchport trunk allowed vlan 1000
confirm
A(config-tengigabitethernet1/1/1)#exit
```

Configure device B.

```
B(config)#interface tengigabitethernet 1/1/1
B(config-tengigabitethernet1/1/1)#portswitch
B(config-tengigabitethernet1/1/1)#switchport mode trunk
B(config-tengigabitethernet1/1/1)#switchport trunk allowed vlan 1000
confirm
B(config-tengigabitethernet1/1/1)#exit
```

Step 3 Configure the tengigabitethernet interface 1/1/2 and tengigabitethernet interface 1/1/3 to dot1q mode and configure the outer TPID to 9100.

Configure device A.

```
A(config)#mls double-tagging tpid 9100
A(config)#interface tengigabitethernet 1/1/2
A(config-tengigabitethernet1/1/2)#portswitch

A(config-tengigabitethernet1/1/2)#switchport mode access
A(config-tengigabitethernet1/1/2)#switchport access vlan 1000
A(config-tengigabitethernet1/1/2)#dot1q-tunnel
A(config-tengigabitethernet1/1/2)#interface tengigabitethernet 1/1/3
A(config-tengigabitethernet1/1/3)#portswitch

A(config-tengigabitethernet1/1/3)#switchport mode trunk
A(config-tengigabitethernet1/1/3)#switchport trunk native vlan 1000
A(config-tengigabitethernet1/1/3)#dot1q-tunnel
A(config-tengigabitethernet1/1/3)#exit
```


Copyright © Raisecom Technology Co., Ltd.

Configure device B.

```
B(config)#mls double-tagging tpid 9100
B(config)#interface tengigabitethernet 1/1/2
B(config-tengigabitethernet1/1/2)#portswitch

B(config-tengigabitethernet1/1/2)#switchport mode access
B(config-tengigabitethernet1/1/2)#switchport access vlan 1000
B(config-tengigabitethernet1/1/2)#dot1q-tunnel
B(config-tengigabitethernet1/1/2)#interface tengigabitethernet 1/1/3
B(config-tengigabitethernet1/1/3)#portswitch
B(config-tengigabitethernet1/1/3)#switchport mode trunk
B(config-tengigabitethernet1/1/3)#switchport trunk native vlan 1000
B(config-tengigabitethernet1/1/3)#dot1q-tunnel
B(config-tengigabitethernet1/1/3)#exit
```

Checking results

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

Take device A as an example.

```
iTNA(config-port)#show dot1q-tunnel
Outer TPID: 0x9100
Inner TPID: 0x8100
Interface     QinQStatus   OuterTPID  CosOverride  MapMissDrop
-------------------------------------------------------------------
1/1/1       --          0x8100    disable     disable
1/1/2       Dot1q-tunnel  0x9100    disable     disable
1/1/3       Dot1q-tunnel  0x9100    disable     disable
```

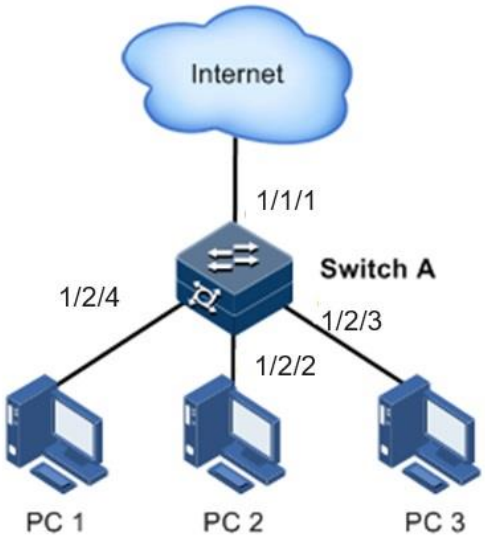
4.12.4 Example for configuring interface protection

Networking requirements

To make PC 1 and PC 2 unable to communicate with each other, but PC 1 and PC 2 can communicate with PC 3 respectively, you can enable interface protection on GE 1/2/4 and GE 1/2/2 on Switch A.

Copyright © Raisecom Technology Co., Ltd.

Figure 4-5 Interface protection networking



Configuration steps

Step 1 Enable interface protection on GE 1/2/4.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/2/4
Raisecom(config-gigaethernet1/2/4)#switchport protect
Raisecom(config-gigaethernet1/2/4)#exit
```

Step 2 Enable interface protection on GE 1/2/2.

```
Raisecom(config)#interface gigaethernet 1/2/2
Raisecom(config-gigaethernet1/2/2)#switchport protect
```

Checking results

Use the **show switchport protect** command to check whether configurations of interface protection are correct.

```
Raisecom#show switchport protect
Port             Protected State
-------------------------
gigaethernet1/2/1   disable
gigaethernet1/2/2   enable
gigaethernet1/2/3   disable
gigaethernet1/2/4   enable
……
```


Copyright © Raisecom Technology Co., Ltd.

Check PC 1 can ping PC 3 successfully and whether PC 2 can ping PC 3 successfully.

- PC 1 ping PC 3 successfully.
- PC 2 ping PC 3 successfully.

Check whether interface protection takes effect by testing whether PC 1 can ping PC 2 successfully.

If PC 1 cannot ping PC 2 successfully, it indicates that interface protection takes effect.

Copyright © Raisecom Technology Co., Ltd.

5 Clock synchronization

This chapter describes principles and configuration procedures of clock synchronization, as well as related configuration examples, including the following sections:

- Configuring SyncE-based clock synchronization

5.1 Configuring SyncE-based clock synchronization

5.1.1 Preparing for configurations

Scenario

In the packet transmission network, it is necessary to ensure that the sending end places the pulse in a specific time slot when sending a digital pulse signal, and the receiving end must be able to extract the pulse in a specific time slot to ensure normal communication between the sending end and the receiving end. Therefore, the first problem to be solved is clock synchronization.

SyncE can perform clock synchronization in packet transmission networks. The device supports automatic selection of the optimal clock source. You only need to configure the clock source of SyncE on the device. In addition, you can also manually select a specific clock source for the device.

Prerequisite

N/A

5.1.2 Configure the clock source of SyncE

No.	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#synce enable`	Enable SyncE. By default, it is not enabled.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
3	Raisecom(config)#**synce operation-type** { **auto-select** | **forced-freerun** | **forced-holdover** }	Configure the working status of SyncE. By default, forced-freerun is adopted.
4	Raisecom(config)#**synce source** { **internal** | **ptp** | **interface** *interface-type interface-number* } **priority** *priority-value* [**src-id** *src-id*] [**quality-level** *quality-level*] [**lockout**]	Configure the SSM quality level of the SyncE clock source.
5	Raisecom(config)#**synce ssm** { **standard** | **extend** | **disable** } [**transmit-threshold** *threshold*]	Enable SyncE SSM quality level to participate in source selection and configure the sending threshold.
6	Raisecom(config)#**synce switch-mode** { **revertive** [**wtr-time** *time*] | **non-revertive** }	(Optional) enable automatic recovery of SyncE clock source and configure the WTR time. By default, the device is enabled with clock source automatic recovery.
7	Raisecom(config)#**synce hold-off-time** *time*	Configure the hold-off time of the clock source.

5.1.3 Manually selecting SyncE clock source

No.	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**synce manual-source** { **internal** | **interface** *interface-type interface-type interface-number*}	Manually switch the SyncE clock source.
3	Raisecom(config)#**synce forced-source** { **internal** | **interface** *interface-type interface-number* }	Forcedly switch the SyncE clock source.

5.1.4 Checking configurations

No.	Command	Description
1	Raisecom#**show synce**	Show global configurations of SyncE.
2	Raisecom#**show synce source** [**id**]	Show clock source configurations of SyncE.
3	Raisecom#**show synce ssm**	Show SSM configurations of SyncE.

Copyright © Raisecom Technology Co., Ltd.

6 IP services

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

- Configuring IPv4
- Configuring IPv6
- Configuring basic properties of management packets
- Configuring ARP
- Configuring NDP
- Configuring ND Snooping
- Configuring ICMP
- Configuring fault detection
- Configuring DNS
- Configuration examples

6.1 Configuring IPv4

6.1.1 Preparing for configurations

Scenario

Before configuring the IPv4 services, you need to configure the IPv4 address and the MTU on the interface.

Prerequisite

N/A

6.1.2 Configuring IPv4 address on interface

No.	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip address** *ip-address* [*ip-mask*] [**sub**]	Configure the IPv4 address of the interface. The interface type includes the Ethernet physical interface, Loopback interface, and VLAN interface.
4	Raisecom(config-port)#**ip address unnumbered** *interface-type interface-number*	(Optional) configure the interface to borrow the IPv4 address of the loopback interface. The prerequisite is that the loopback interface has been configured with an IP address.

6.1.3 Checking configurations

No.	Command	Description
1	Raisecom#**show ip interface brief**	Show IPv4 address configurations of the L3 interface.

6.2 Configuring IPv6

6.2.1 Preparing for configurations

Scenario

With the rapid development of the network, IPv4 shows deficiencies gradually, and IPv6 has more advantages than IPv4. For example, IPv6 has a huge amount of address space, highly flexible message format, efficient routing and forwarding efficiency and so on. IPv6 can not only solve the problem of network address resource limitation, but also solve the problem of limited access to the Internet by various access devices.

Prerequisite

N/A

6.2.2 Configuring IPv6 basic functions

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **vlan** *vlan-id* | **loopback** *loopback-number* | **gigaethernet** *unit-id/slot-id/port-id* | **tunnel** *1/1/tunnel-id* }	Enter VLAN interface configuration mode/LoopBack interface configuration mode/Layer 3 Ethernet interface configuration mode/Tunnel interface configuration mode. The following takes the VLAN interface configuration mode for example for description.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-vlan*)#**ipv6 address** *ipv6-address/prefix-length* [**eui-64**]	Configure the IPv6 address of the interface.
4	Raisecom(config-vlan*)#**ipv6 address** *ipv6-address* **link-local**	Configure the IPv6 local link address of the interface.
5	Raisecom(config-vlan*)#**ipv6 address** *ipv6-address/prefix-length* **anycast**	Configure the IPv6 anycast address of the interface.
6	Raisecom(config-vlan*)#**ipv6 address auto**	Enable automatic configuration of IPv6 stateless address on the interface. The VxLAN interface, Tunnel interface, and loopback interface does not support this configuration.

6.2.3 Checking configurations

No.	Command	Description
1	Raisecom#**show ipv6 interface brief** [*interface-type interface-number*]	Show IPv6 address configurations of the L3 interface.
2	Raisecom#**show ipv6 address auto**	Show IPv6 address prefix.

6.3 Configuring basic properties of management packets

6.3.1 Preparing for configurations

Scenario

The IP interface is a VLAN-based virtual interface, which is used to manage the device or route multiple devices.

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

Prerequisites

N/A

6.3.2 Configuring management packets

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**interface vlan** *vlan-id* **Example:** Raisecom(config)#interface vlan 1	Enter VLAN interface configuration mode. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094
3	Raisecom(config-vlan*)#**ip management-traffic cos** *cos-value* **Example:** Raisecom(config-vlan1)#ip management-traffic cos 2	Configure the CoS of the management VLAN. By default, it is 6. • Cos-value: outer CoS, an integer, ranging from 0 to 7
4	Raisecom(config-vlan*)#**ip management-traffic mode double-tagging** [**inner-vlan** *vlan-id*] [**inner-cos** *cos-id*] **Example:** Raisecom(config-vlan1)#ip management-traffic mode double-tagging	Configure the double-tagged mode of management packets. • vlan-id: VLAN ID, an integer, ranging from 1 to 4094 • Cos-value: outer CoS, an integer, ranging from 0 to 7

6.4 Configuring ARP

6.4.1 Preparing for configurations

Scenario

ARP is a protocol for resolving the IPv4 address into Ethernet MAC address (or physical address).

Prerequisite

Configure the interface IPv4 address.

6.4.2 Configuring static ARP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**arp** *ip-address mac-address* [**vrf** *vrf-name*]	Configure static ARP.

6.4.3 Configuring dynamic ARP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**arp mode** { **learn-all** | **learn-reply-only** }	Configure the ARP mode. By default, it learns the MAC address of all hosts.

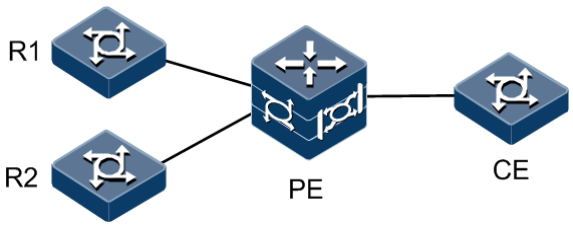
Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**arp aging-time** *time*	(Optional) configure the aging time of dynamic ARP. By default, the aging time is 1200 seconds.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
5	Raisecom(config-port)#**arp learning** [**strict**] **enable**	Enable dynamic ARP learning on the interface. By default, dynamic ARP learning on the interface is enabled.
6	Raisecom(config-port)#**arp max-learning-num** *number*	Configure the maximum number of dynamically learnt ARP entries on the interface. By default, it is 16384.
7	Raisecom(config-port)#**gratuitous-arp-learning** {**enable** | **disable** }	Configure gratuitous ARP learning on the interface. By default, it is enabled.

6.4.4 Configuring proxy ARP

As shown in Figure 6-1, the PE device is configured with interface isolation, and R1 and R2 cannot communicate directly. After proxy ARP is enabled on the PE, when R1 sends an ARP request to R2, the PE will, on behalf of R2, send an ARP reply message carrying its own MAC address and R2 IP address to R1.

Figure 6-1 Proxy ARP application scenario



Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**arp proxy enable**	Enable proxy ARP on the interface. By default, it is disabled.

6.4.5 Clearing ARP entries

Step	Command	Description
1	Raisecom(config)#**clear arp** [**vrf** *vrf-name*] [*ip-address* | **interface** *interface-type interface-number*] [**static**]	Clear ARP entries.

Copyright © Raisecom Technology Co., Ltd.

6.4.6 Checking configurations

No.	Command	Description
1	Raisecom#**show arp** [**vrf** *vrf-name*] [*ip-address* | **interface** *interface-type interface-number* | **static**]	Show ARP information.

6.5 Configuring NDP

6.5.1 Preparing for configurations

Scenario

IPv6 implements address resolution and obtains the device MAC address through Neighbor Discovery Protocol (NDP), and generates related routing information.

There are two ways for the NDP to resolve neighbor node IPv6 addresses into link layer addresses.

- By manually configuring static neighbor entries
- Through the Neighbor Solicitation (NS) message and Neighbor Announcement (NA) message

Prerequisite

Configure the interface IPv6 address.

6.5.2 Configuring static NDP entries

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 neighbor** *ipv6-address mac-address* [**vrf** *vrf-name*]	Configure static neighbor entries.

6.5.3 Configuring dynamic NDP entries

Configuring times of sending NS messages for detecting duplicated addresses

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 nd dad attempts** *value*	Configure times of sending NS messages for detecting duplicated addresses.

Copyright © Raisecom Technology Co., Ltd.

When the RAX721 obtains an IPv6 address, it uses the duplicated address detection function to determine whether the IPv6 address is already used by another device. After sending NS messages for certain specified times and receiving no response, it determines that the IPv6 address is not duplicated and thus can be used.

Configuring maximum number of NDPs allowed to be learnt

Configure the maximum number of NDPs allowed to be learnt on the Layer 3 interface for the RAX721 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 neighbor max-learning-num** *number*	Configure the maximum number of NDPs allowed to be learnt.

Configuring aging time of dynamic NDP entries

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 neighbor aging-time** *aging-time*	Configure the aging time of dynamic NDP.

Configuring NDP bandwidth rate limiting on interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.
3	Raisecom(config-port)#**ndp rate-limit** *rate-value*	Configure NDP bandwidth rate limiting.

Configuring RA message

Router Advertisement (RA) messages are NDP messages that are periodically sent by the device or for responding to the Router Solicitation (RS) messages in real time.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-port)#**ipv6 nd ra repression**	Enable RA repression. By default, RA suppression is enabled.
4	Raisecom(config-port)#**ipv6 nd ra interval** *interval*	Configure the interval for advertising RA messages.
5	Raisecom(config-port)#**ipv6 nd ra advlinkmtu** *mtu-value*	Configure the MTU information carried in the RA message.
6	Raisecom(config-port)#**ipv6 nd ra prefix** *ipv6-prefix-address/prefix-length valid-lifetime preferred-lifetime* [**no-autoconfig**] [**off-link**]	Configure the prefix information carried in the RA message.
7	Raisecom(config-port)#**ipv6 nd ra router-lifetime** { *time* | **0** }	Configure the lifetime of the router in the RA message.
8	Raisecom(config-port)#**ipv6 nd ra hop-limit** *hopsvalue*	Configure the hop limits in the RA message.
9	Raisecom(config-port)#**ipv6 nd ra reachable-time** *time*	Configure the peer reachable time in the RA message.
10	Raisecom(config-port)#**ipv6 nd ra retrans-timer** *value*	Configure the retransmission timer in the RA message.
11	Raisecom(config-port)#**ipv6 nd ra managed-config-flag**	Configure the management address configuration flag in the RA message.
12	Raisecom(config-port)#**ipv6 nd ra other-config-flag** Raisecom(config-port)#**exit**	Configure other configuration flags in the RA message.

6.5.4 Configuring proxy NDP

When a host on a network sends an NS request to another host on the same network segment but not on the same network, the other party will not receive the NS request message. In this case, a device with proxy enabled needs to respond to the request, namely, responding to the NA message. This process is called ND Proxy.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**ipv6 nd proxy** { **enable** | **disable** }	Enable or disable ordinary ND Proxy. By default, it is disabled.

Copyright © Raisecom Technology Co., Ltd.

6.6 Configuring ND Snooping

6.6.1 Preparing for configurations

Scenario

ND Snooping is used to prevent common ND spoofing attacks in the network, and isolate ND packets from insecure sources. You can configure the interface trust status to trust ND message or not, and the binding table to filter whether the messages meet the requirements.

Prerequisite

N/A

6.6.2 Default configurations

Function	Default value
ND Snooping status	Disable
RA Snooping status	Disable

6.6.3 Configuring ND Snooping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 nd snooping**	Enable global ND Snooping
3	Raisecom(config)#**interface gigaethernet** *unit-id/slot-id/port-id*	Enter Ethernet interface configuration mode.
4	Raisecom(config-gigaethernet*/*/*)#**portswitch**	Change the interface to Layer 2 switching mode from Layer 3 mode.
5	Raisecom(config-gigaethernet*/*/*)#**ipv6 nd snooping**	Enable ND Snooping on the interface.
6	Raisecom(config-gigaethernet*/*/*)#**ipv6 nd snooping trust**	Configure the interface as a trusted interface.

6.6.4 Checking configurations

Step	Command	Description
1	Raisecom#**show ipv6 nd snooping** [**interface gigaethernet** *unit-id/slot-id/port-id* | **port-channel** *channel-number*]	Show ND Snooping configurations.
2	Raisecom#**show ipv6 nd snooping binding** [**interface gigaethernet** *unit-id/slot-id/port-id* | **port-channel** *channel-number*]	Show the binding relationship on all or a specified interface.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom#**show ipv6 nd snooping statistics** [**interface gigaethernet** *unit-id/slot-id/port-id* | **port-channel** *channel-number*]	Show statistics on ND Snooping user packets.

6.6.5 Maintenance

Step	Command	Description
1	Raisecom(config)#**clear ipv6 nd snooping statistics** [**interface gigaethernet** *unit-id/slot-id/port-id* | **port-channel** *channel-number*]	Clear statistics on the ND Snooping user packets received by the device.
2	Raisecom(config)#**clear ipv6 nd snooping ip-address** *ipv6-address* **vlan** *vlan-id*	Clear ND Snooping dynamic learning entries in a specified VLAN.

6.7 Configuring ICMP

6.7.1 Configuring IPv4 ICMP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv4 icmp** { **type** *type-value* **code** *code-value* | **name** *icmp-name* | **all** } **send**	Enable ICMP packet sending.
3	Raisecom(config)#**ipv4 icmp** { **type** *type-value* **code** *code-value* | **name** *icmp-name* | **all** } **receive**	Enable ICMP packet receiving.
4	Raisecom(config)#**ipv4 icmp send-rate bucket** *bucket-size* **ratelimit** *interval*	Limit the rate for sending ICMPv4 packets.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**ipv4 icmp address-unreachable send**	Enable the function of sending ICMP packets when the IPv4 address is unreachable.
7	Raisecom(config-port)#**ipv4 icmp port-unreachable send**	Enable the function of sending ICMP packets when the interface is unreachable.
8	Raisecom(config-port)#**ipv4 icmp ttl-timeout send**	Enable the function of sending ICMP packets when the TTL exceeds the threshold.

Copyright © Raisecom Technology Co., Ltd.

6.7.2 Configuring IPv6 ICMP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 icmp** { **type** *type-value* **code** *icmpv6-code* | **name** *icmpv6-name* | **all** } **send**	Configure ICMPv6 packets.
3	Raisecom(config)#**ipv6 icmp** { **type** *type-value* **code** *icmpv6-code* | **name** *icmpv6-name* | **all** } **receive**	Enable the function of receiving ICMPv6 packets.
4	Raisecom(config)#**ipv6 icmp send-rate bucket** *bucket-size* **ratelimit** *interval*	Limit the rate for sending ICMPv6 packets.
5	Raisecom(config)#**ipv6 icmp redirect send**	Enable redirection sending of ICMPv6 packets.
6	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
7	Raisecom(config-port)#**ipv6 icmp address-unreachable send**	Enable the function of sending ICMPv6 packets when the IPv6 address is unreachable.
8	Raisecom(config-port)#**ipv6 icmp port-unreachable send**	Enable the function of sending ICMPv6 packets when the interface is unreachable.
9	Raisecom(config-port)#**ipv6 icmp hop-limit-exceeded send**	Enable the function of sending ICMPv6 packets when the number of hops exceeds the threshold.

6.7.3 Checking configurations

No.	Command	Description
1	Raisecom#**show ipv4 icmp status** { **receive** | **send** [**interface** *interface-type interface-number*] }	Check the status of the received or sent ICMPv4 packets.
2	Raisecom#**show ipv6 icmp status** { **receive** | **send** [**interface** *interface-type interface-number*] }	Check the status of the received or sent ICMPv6 packets.

Copyright © Raisecom Technology Co., Ltd.

6.8 Configuring fault detection

6.8.1 PING

PING IPv4 network

Step	Command	Description
1	Raisecom#**ping** [**vrf** *vpn-instance-name*] { *ip-address* | **dns** *dns-domain-name* } [**count** *count*] [**interface** *interface-type interface-number*] [**interval** *time*] [**size** *size*] [**waittime** *period*] [**source** *ip-address*] [**df-bit**]	Use the **ping** command to test the connectivity of the IPv4 network.

The RAX721 cannot perform other operations in the process of Ping. It can perform other operations only when Ping is finished or Ping is interrupted by pressing **Ctrl**+**C**.

PING IPv6 network

Step	Command	Description
1	Raisecom#**ping** [**vrf** *vpn-instance-name*] **ipv6** { *ipv6-address* | **dns** *dns-domain-name* } [**count** *count*] [**interface** *interface-type interface-number*] [**interval** *time*] [**size** *size*] [**waittime** *period*] [**source** *ipv6-address*]	Use the **ping** command to test the connectivity of the IPv6 network.

PING MPLS network

Step	Command	Description
1	Raisecom#**ping mpls ipv4** *ip-address/m* [**nexthop** *ip-address*] [**count** *count*] [**size** *size*] [**waittime** *period*] [**source** *ipv-address*] [**ttl**] [**tc**]	Use the **ping** command to test the MPLS network connectivity of a specified IPv4 address.
2	Raisecom#**ping mpls vc-id** *vc-id* **destination** *ip-address* [**count** *count*] [**size** *size*] [**waittime** *period*] [**source** *ipv-address*] [**ttl**] [**tc**]	Use the **ping** command to test the MPLS network connectivity of a specified VC-ID.

Ping DHCP Server

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp server ping** { **packet** *packet-num* | **timeout** *time* }	Configure the connectivity with the DHCPv4 server.

Copyright © Raisecom Technology Co., Ltd.

6.8.2 Traceroute

Traceroute IPv4 network

The interface is configured with an IPv4 address.

Step	Command	Description
1	Raisecom#**traceroute** [**vrf** *vpn-instance-name*] { *ip-address* | **dns** *dns-domain-name* } [**firstttl** *fitst-ttl*] [**maxttl** *max-ttl*] [**port** *port-number*] [**waittime** *period*] [**count** *times*] [**size** *size*] [**source** *ip-address*]	Use the **traceroute** command to test the IPv4 network connectivity and view nodes passed by the packet. By default, the initial TTL is configured to 1; the maximum TTL is configured to 30; the interface ID is configured to 33433; the timeout is configured to 3s; the number of detection packets is configured to 3.

Traceroute IPv6 network

Step	Command	Description
1	Raisecom#**traceroute** [**vrf** *vpn-instance-name*] **ipv6** { *ipv6-address* | **dns** *dns-domain-name* } [**firstttl** *fitst-ttl*] [**maxttl** *max-ttl*] [**port** *port-number*] [**waittime** *period*] [**count** *times*] [**size** *size*]	Use the **traceroute** command to test the IPv6 network connectivity and view nodes passed by the packet. By default, the initial TTL is configured to 1; the maximum TTL is configured to 30; the interface ID is configured to 33433; the timeout is configured to 3s; the number of detection packets is configured to 3.

Traceroute MPLS network

Step	Command	Description
1	Raisecom#**traceroute mpls ipv4** *ip-address/m* [**generic**] [**nexthop** *ip-address*] [**waittime** *seconds*] [**maxttl** *max-ttl*] [**reply dscp** *dscp-value*] [**reply mode udp** | **reply mode udp-alert**] [**source** *ip-addresss*] [**tc** *tc-value*] [**flags fec**]	Use the **traceroute** command to test the connectivity of the MPLS network with the specified IPv4 address and view the network nodes through which the packet passes.
2	Raisecom#**traceroute mpls vc-id** *vc-id* **destination** *ip-address* [**waittime** *seconds*] [**maxttl** *max-ttl*] [**reply dscp** *dscp-value*] [**reply mode udp** | **reply mode udp-alert** | **reply mode control-channel**] [**reply pad-tlv**] [**source** *ip-address*] [**tc** *tc-value*] [**flags fec**]	Use the **traceroute** command to test the connectivity of the MPLS network with the specified VC-ID and view the network nodes the packet passes through.

Copyright © Raisecom Technology Co., Ltd.

6.9 Configuring DNS

6.9.1 Configuring IPv4 DNS

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dns server** *ip-address*	Configure the IP address of the IPv4 DNS server.
3	Raisecom(config)#**ip dns resolve** { **enable** | **disable** }	Enable the resolving function of the IPv4 DNS client.

6.9.2 Configuring IPv6 DNS

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 dns server** *ipv6-address*	Configure the IP address of the IPv6 DNS server.
3	Raisecom(config)#**ipv6 dns resolve** { **enable** | **disable** }	Enable the resolving function of the IPv6 DNS client.

6.9.3 Checking configurations

No.	Command	Description
1	Raisecom#**show dns cache all**	Show all current DNS cache data.
2	Raisecom#**show dns config**	Show configurations of the current DNS.

6.9.4 Maintenance

No.	Command	Description
1	Raisecom# **dns cache clear all**	Clear all current DNS cache data. After this, you need to re-query DNS to use all DNSs next time. Use this command with caution.

Copyright © Raisecom Technology Co., Ltd.

6.10 Configuration examples

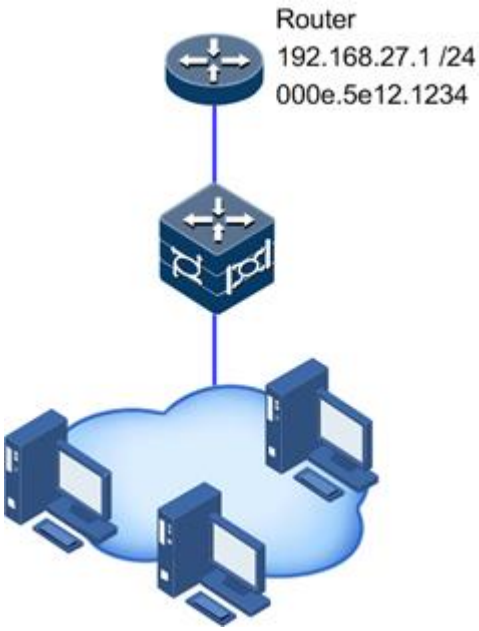
6.10.1 Example for configuring ARP

Networking requirements

As shown in Figure 6-2, the RAX721 connects to the host and connects to the upstream router through the interface. The IPv4 address of the router is 192.168.27.1/24, and the MAC address is 000e.5e12.1234.

Configure the aging time of dynamic ARP entries to 600s. At the same time, to increase the security of the communication between the RAX721 and the router, corresponding static ARP entries are configured on the RAX721.

Figure 6-2 Configuring ARP



Configuration steps

Step 1 Add one ARP static entry.

```
Raisecom(config)#arp 192.168.27.1 000e.5e12.1234
```

Step 2 Configure the aging time of dynamic ARP entries to 600s.

```
Raisecom(config)#arp aging-time 600
```


Copyright © Raisecom Technology Co., Ltd.

Checking results

Use the **show arp** command to show whether entries in the ARP mapping table are correct.

```
Raisecom#show arp
ARP aging-time: 600 seconds(default: 1200s)
ARP dynamic max: 16384
ARP mode: Learn all
ARP table:
Total: 7    Static: 1    Dynamic: 6

IP Address     Mac Address    Interface                    Vlan  Type
Age(s)   status      VRF
-------------------------------------------------------------------------
----------------------------------------
172.16.67.1    000C.2945.C51E  fastethernet1/0/1             --   dynamic
12       REACHABLE
172.16.67.10   0000.0000.0000  fastethernet1/0/1             --   dynamic
21       PROBE
172.16.67.81   14FE.B5E5.8291  fastethernet1/0/1             --   dynamic
29       REACHABLE
172.16.67.107  0000.0102.031E  fastethernet1/0/1             --   dynamic
19       REACHABLE
172.16.67.109  0000.5E00.2368  fastethernet1/0/1             --   dynamic
487      REACHABLE
172.16.67.202  782B.CB58.3C3D  fastethernet1/0/1             --   dynamic
1074     REACHABLE
192.168.27.1 000e.5e12.1234  fastethernet1/0/1            --   static
--       PERMANENT
```


Copyright © Raisecom Technology Co., Ltd.

7 DHCP

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

- Configuring DHCPv4 Server
- Configuring DHCPv4 Client
- Configuring DHCPv4 Relay
- Configuring DHCPv4 Snooping
- Configuring DHCPv4 Option
- Configuring DHCPv6 Snooping

7.1 Configuring DHCPv4 Server

7.1.1 Preparing for configurations

Scenario

When the RAX721 works as the DHCPv4 server, the DHCP v4 client can obtain the IP address from the server.

Prerequisite

The RAX721 is not enabled with DHCP v4 Client. In addition, DHCP Relay and DHCP Client can be concurrently enabled, and we do not recommend concurrently enabling other DHCP modules.

7.1.2 Creating and configuring IPv4 address pool

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip dhcp server pool` *`pool-name`*	Create the IPv4 address pool and enter address pool configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-pool)#**address** *start-ip-address end-ip-address* **mask** { *mask* | *mask-length* }	Configure the range of the IPv4 address pool.
4	Raisecom(config-pool)#**lease expired** { *minute* | **infinite** }	Configure the lease of the IPv4 address pool.
5	Raisecom(config-pool)#**dns-server** *ip-address* [**secondary**]	Configure the DNS of the IPv4 address pool.
6	Raisecom(config-pool)#**gateway** *ip-address*	Configure the default gateway of the IPv4 address pool.
7	Raisecom(config-pool)#**option 60** *vendor-string*	Configure the information carried by Option 60.
8	Raisecom(config-pool)#**option 43** [**sub-option** *option-id*] { **hex** | **ascii** } *string*	Configure the information carried by Option43.
9	Raisecom(config-pool)#**tftp-server** *ip-address*	Configure the TFTP server of the IPv4 address pool.
10	Raisecom(config-pool)#**trap server-ip** *ip-address* Raisecom(config-pool)#**exit**	Configure the Trap server of the IPv4 address pool.
11	Raisecom(config)#**ip dhcp static-bind** *ip-address mac-address pool-name*	(Optional) configure the DHCPv4 static lease.

7.1.3 Configuring DHCP v4 Server on interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**no portswitch**	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**ip dhcp server**	Enable DHCP v4 Server.

7.1.4 Configuring trusted DHCP Relay server

If the DHCP Server and the DHCP Client are not on the same network segment and you need to use the DHCP Relay to relay DHCP messages, you can use this command to configure the DHCP server to trust the DHCP Relay. The DHCP server will discard the messages received from the untrusted DHCP Relay.

To receive and process DHCP messages from a certain DHCP Relay, you must configure the DHCP Relay as the trusted DHCP Relay of the DHCP server.

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**ip dhcp server relay-ip** *ip-address* { *ip-mask* | *mask-length* }	Configure the IP address of the DHCP Relay trusted by the DHCP server.

7.1.5 Managing lease files

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp lease save**	Save the lease files on the DHCP server.
3	Raisecom(config)#**ip dhcp lease erase**	(Optional) delete the lease files on the DHCP server.

7.1.6 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show ip dhcp server**	Show DHCP server configurations.
2	Raisecom(config)#**show ip dhcp server lease**	Show assigned IPv4 addresses and client information.
3	Raisecom(config)#**show ip dhcp server statistics**	Show packet statistics of the DHCP v4 server.
4	Raisecom(config)#**show ip dhcp static-bind**	Show DHCP v4 static lease information.
5	Raisecom(config)#**show ip server pool** [*pool-name*]	Show configurations of the DHCPv4 address pool.
6	Raisecom(config)#**show ip server pool statistics** [*pool-name*]	Show statistics of the DHCPv4 address pool.

7.2 Configuring DHCPv4 Client

7.2.1 Preparing for configurations

Scenario

When working as the DHCPv4 client, the RAX721 can obtain an IP address from the DHCPv4 server. You can use the IP address to manage the RAX721.

When IP addresses are assigned in a dynamic mode, the IP address assigned to the DHCPv4 client has a lease period. When the lease period expires, the DHCPv4 server will withdraw the IP address. If the DHCPv4 client wishes to continue to use the IP address, it needs to renew the IP address. If the lease period does not expire and the DHCPv4 client does not need to use the IP address, it can release the IP address.

Copyright © Raisecom Technology Co., Ltd.

Prerequisite

The RAX721 is not enabled with DHCPv4 Server and works in common DHCP Client mode.

7.2.2 Configuring DHCPv4 client information

Before enabling the DHCPv4 client on the Layer 3 interface to apply for the IP address, configure DHCPv4 client information.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip dhcp client mode { normal | zeroconfig }`	Configure the DHCPv4 client to normal mode. By default, it is in remote zero-configuration mode.
3	`Raisecom(config)#interface interface-type interface-number`	Enter Layer 3 interface configuration mode.
4	`Raisecom(config-port)#ip dhcp client { class-id class-id | client-id client-id | hostname hostname }`	Configure DHCPv4 Option 60 client, including the type identifier, client identifier, and host name. This command only takes effect on the Layer 3 interface.

7.2.3 Configuring DHCPv4 Client on Layer 3 interface

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface interface-type interface-number`	Enter Layer 3 interface configuration mode.
3	`Raisecom(config-port)#ip address dhcp [ server-ip ip-address ]`	Configure DHCPv4 Client and specify the IP address of the DHCPv4 server. It means enabling the DHCPv4 client to apply for the IP address. The command is valid on the Layer 3 interface only.

7.2.4 Renewing or releasing IPv4 address

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface interface-type interface-number`	Enter Layer 3 physical interface configuration mode.
3	`Raisecom(config-port)#ip dhcp client renew`	Renew the IPv4 address. This command takes effect only on Layer 3 interface.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-port)#**no ip address dhcp**	Release the IPv4 address. This command takes effect on Layer 3 interfaces only.

7.2.5 Configuring link aggregation fault detection

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface vlan** *interface-number*	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-vlan*)#**ip dhcp client fault-detect port-channel** *channel-num*	Configure link aggregation fault detection. When the master/slave mode of link aggregation switches, DHCP sends the Release packet to release the IP address, and start the application for the new IP address.

7.2.6 Checking configurations

No.	Command	Description
1	Raisecom#**show ip dhcp client**	Show configurations of the DHCPv4 client.

7.3 Configuring DHCPv4 Relay

7.3.1 Preparing for configurations

Scenario

When the RAX721 works as the DHCPv4 relay, the DHCPv4 clients can communicate with DHCPv4 servers in other network segments through the DHCPv4 relay to obtain IP addresses. Therefore, DHCPv4 clients in different network segments can apply for IP addresses from the same DHCPv4 server. This facilitates saving costs and managing all devices together.

Prerequisite

The RAX721 is not enabled with DHCPv4 Client or DHCPv4 Server.

7.3.2 Configuring global DHCPv4 Relay

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**ip dhcp relay**	Enable global DHCPv4 relay.

7.3.3 Configuring DHCPv4 relay on interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip dhcp relay**	Enable DHCPv4 Relay on the interface.
4	Raisecom(config-port)#**ip dhcp relay target-ip** *ip-address*	Configure the destination IP address for forwarding the packets.
5	Raisecom(config-port)#**ip dhcp relay relay-ip** *ip-address*	Configure the relay IP address and interface relay.

7.3.4 Configuring DHCPv4 relay Option 82

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp relay information option**	Configure DHCPv4 relay Option 82.
3	Raisecom(config)#**ip dhcp relay information policy** { **drop** | **keep** | **replace** }	Configure the processing policy for the DHCPv4 relay to process DHCP packet containing Option 82.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
5	Raisecom(config-port)#**ip dhcp relay information trusted**	Configure DHCPv4 relay trusted interface.

7.3.5 Checking configurations

No.	Command	Description
1	Raisecom#**show ip dhcp relay**	Show configurations of DHCPv4 relay.
2	Raisecom#**show ip dhcp relay information**	Show DHCPv4 relay Option 82.
3	Raisecom#**show ip dhcp relay binding**	Show binding information about DHCPv4 relay.
4	Raisecom#**show ip dhcp relay statistics**	Show statistics about DHCPv4 relay.

Copyright © Raisecom Technology Co., Ltd.

7.4 Configuring DHCPv4 Snooping

7.4.1 Preparing for configurations

Scenario

As a security feature of DHCP, DHCP Snooping is used to ensure that the DHCP client obtains an IP address from a legitimate DHCP server and records the correspondence between the DHCP client IP address and MAC address.

The Option field in the DHCP packet records the location of the DHCP client. Administrators can use this option to locate the DHCP client to control the client's security and billing. A device configured with DHCP Snooping Option can process the packets according to whether the packet contains the Option field.

Prerequisite

N/A

7.4.2 Configuring DHCPv4 Snooping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp snooping**	Enable global DHCPv4 Snooping.
3	Raisecom(config)#**ip dhcp snooping binding max-learning-num** *number*	Configure the maximum number of DHCPv4 Snooping binding entries.
4	Raisecom(config)#**ip dhcp snooping option client-id**	(Optional) configure DHCPv4 Snooping Option61.
5	Raisecom(config)#**ip dhcp snooping option** *optiong-code*	Configure DHCPv4 Snooping Option.
6	Raisecom(config)#**ip dhcp snooping autosave enable**	(Optional) enable automatic saving of the DHCPv4 Snooping binding table.
7	Raisecom(config)#**ip dhcp snooping autosave write-interval** *time*	(Optional) configure the interval for automatically saving the DHCPv4 Snooping binding table.
8	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**portswitch**	Enter interface configuration mode. Configure the interface mode to switch.
9	Raisecom(config-port)#**ip dhcp snooping trust**	Configure the interface to a DHCP Snooping trusted interface.
10	Raisecom(config-port)#**ip dhcp snooping trust vlan** *vlan-list*	Configure the trusted VLAN list of the DHCP Snooping interface. When the interface processes the Offer or Ack packet, of which the op is 2, it discards the packet if the VLAN is in the untrusted VLAN list.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
11	Raisecom(config-port)#**ip dhcp snooping vlan** *vlan-id*	Enable DHCP Snooping on a specified interface and a specified VLAN.
12	Raisecom(config-port)#**portswitch** Raisecom(config-port)#**ip dhcp snooping check dhcp-chaddr**	Enable the Layer 2 interface to check the client hardware address.
13	Raisecom(config-port)#**ip dhcp snooping outer** *vlan-id* **inner** *vlan-list*	Enable DHCP Snooping based on interface and double-layer VLAN.

7.4.3 Configuring DHCPv4 Snooping Option 82

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp snooping information option**	Enable global DHCP Snooping Option 82.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
4	Raisecom(config-port)#**ip dhcp snooping information option vlan-list** *vlan-list*	Configure the VLAN list of interface DHCP Snooping Option 82.

7.4.4 Checking configurations

No.	Command	Description
1	Raisecom#**show ip dhcp snooping**	Show configurations of DHCPv4 Snooping.
2	Raisecom#**show ip dhcp snooping autosave**	Show the automatic saving status of the DHCPv4 Snooping binding table.
3	Raisecom#**show ip dhcp snooping binding** [**max-learning-num**]	Show the DHCPv4 Snooping binding table.

7.5 Configuring DHCPv4 Option

7.5.1 Preparing for configurations

Scenario

The 61 and 82 fields in the DHCP Option are options for the relay agent information in the DHCP message. When the DHCP client sends a request message to the DHCP server, if the request packet needs to go through DHCP Snooping or DHCP relay, the DHCP Snooping or DHCP relay adds the Option field to the request message.

Copyright © Raisecom Technology Co., Ltd.

The DHCP Option 61 and 82 fields are used to record DHCP client information based on IPv4. Based on this type of information, the DHCP server can be used in conjunction with other software to implement functions such as IP address allocation restrictions and accounting.

Prerequisite

DHCP Option needs to be used on the DHCP Snooping device. To validate DHCP Option, you need to enable DHCP Snooping on the device.

7.5.2 Configuring IPv4 DHCP Option 82

Option 82 should be used on the device with DHCP Relay enabled.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp information option attach-string** *attach-string*	Configure additional information for the Option 82 field.
3	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**ip dhcp information option circuit-id** *circuit-id*	Configure the circuit ID sub-option of the Option 82 field under the interface.
4	Raisecom(config-port)#**exit** Raisecom(config)#**ip dhcp information option remote-id** { **client-mac** | **client-mac-string** | **hostname** | **switch-mac** | **switch-mac-string** | **string** *string* }	Configure the remote ID sub-option in the Option 82 field.

7.5.3 Configuring IPv4 DHCP Option 61

Option 61 should be used on the device with DHCP Snooping enabled.

The follow steps can be in any sequence.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv4 dhcp option client-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	Configure Option 61.
3	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**ipv4 dhcp option client-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	Configure Option 61 on the interface.

7.5.4 Configuring IPv4 self-defined DHCP Option

Self-defined Option should be used on the device with DHCP Snooping enabled.

The follow steps can be in any sequence.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv4 dhcp option** *option-id* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	(Optional) create a self-defined Option field based on IPv4.
3	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**ipv4 dhcp option** *option-id* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	(Optional) create a self-defined Option field based on IPv4 on the interface.

7.5.5 Checking configurations

No.	Command	Description
1	Raisecom#**show ip dhcp information option**	Show DHCP Option configurations.

7.6 Configuring DHCPv6 Snooping

7.6.1 Preparing for configurations

Scenario

DHCP Snooping, as a security feature of DHCP, is used to ensure that DHCP clients obtain IP addresses from legitimate DHCP servers and record the mapping between IP addresses and MAC addresses of DHCP clients.

Prerequisites

N/A

7.6.2 Configuring DHCPv6 Snooping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 dhcp snooping**	Enable global DHCPv6 Snooping.
3	Raisecom(config)#**ipv6 dhcp snooping binding max-learning-num** *number*	Configure the maximum number of entries in the DHCPv6 Snooping binding table.
4	Raisecom(config)#**ipv6 dhcp snooping option** *optiong-code*	Configure DHCPv6 Snooping to support the Option function.
5	Raisecom(config)#**ipv6 dhcp snooping autosave enable**	(Optional) enable auto-saving of the DHCPv6 Snooping binding table.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config)#**ipv6 dhcp snooping autosave write-interval** *time*	(Optional) configure the interval for saving the DHCPv6 Snooping binding table.
7	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
8	Raisecom(config-port)#**portswitch**	Configure the interface mode to switch.
9	Raisecom(config-port)#**ipv6 dhcp snooping trust**	Configure the interface as the trusted interface of DHCPv6 Snooping.
10	Raisecom(config-port)#**ipv6 dhcp snooping vlan** *vlan-id*	Enable DHCP Snooping on the specified interface and VLAN.

7.6.3 Checking results

No.	Command	Description
1	Raisecom#**show ipv6 dhcp snooping**	Show configurations of DHCPv6 Snooping.
2	Raisecom#**show ipv6 dhcp snooping autosave**	Show the status of auto-saving of the DHCPv6 Snooping binding table.
3	Raisecom#**show ipv6 dhcp snooping binding** [**max-learning-num**]	Show information about the DHCPv6 Snooping binding table.

Copyright © Raisecom Technology Co., Ltd.

8 IP routing

This chapter describes principles and configuration procedures of IP routing, including following sections:

- Configuring routing management
- Configuring static route
- Configuring routing policy
- Configuring OSPFv2
- Configuring OSPFv3
- Configuring ISIS
- Configuring ISISv6
- Configuring BGP
- Configuring BGP4+
- Configuring RIP
- Configuring RIPng

8.1 Configuring routing management

8.1.1 Configuring routing management

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router id** *router-id*	Configure the Router ID. By default, the Router ID is 192.168.1.1.

8.1.2 Configuring flow table

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**flow route** *flow-route-name*	Configure the flow table name and enter flow table configuration mode.
3	Raisecom(flow-route)# **match** { **dest-ip** { *dest-ip-address dest-ip-mask* | **any** } | **dest-port** *dest-port* | **dscp** *dscp-value* | **fragment** | **icmp-type** *icmp-type-id* | **port** *port-id* | **protocol** *protocol-id* | **source-ip** { *source-ip-address source-ip-mask* | **any** }| **source-port** *source-port* | **tcpflag** *tcp-flag* }	Configure the flow table matching rule.

8.1.3 Configuring IP FRR

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip frr route-map** *map-name* [**wtr-timer** *timer*]	Configure IP FRR.
3	Raisecom(config)#**frr auto-create-bfd**	Configure automatic creation of BFD session detection by IP FRR.
4	Raisecom(config)#**frr trigger ipv4 bfd** [**vrf** *vrfname*] **peer-ip** *ipv4-address* **interface** *interface-type interface-num*	Configure IP FRR to trigger bidirectional forwarding detection.
	Raisecom(config)#**frr trigger ipv6 bfd** [**vrf** *vrfname*] **peer-ip** *ipv6-address* **interface** *interface-type interface-num*	
	Raisecom(config)#**frr trigger ldp-lsp bfd peer-ip** *ipv4-address*	

8.1.4 Checking configurations

No.	Command	Description
1	Raisecom#**show router id**	Show the router ID.
2	Raisecom#**show fib** [**vrf** *vrf-name*] [*ip-address* | *ipv6-address/m*]	Show the routing table.
3	Raisecom#**show fib** [**vrf** *vrf-name*] [**domain** { **ipv4** | **ipv6** }]	Show the primary domain of the routing table.
4	Raisecom#**show fib summary** [**all** | **vrf vrf-name**]	Show statistics on the routing table.
5	Raisecom#**show flow-route** [*flow-route-name*]	Show information about the flow table.
6	Raisecom#**show lfib** [**ac** | **frr** | **ilm** | **nhlfe** | **pw** | **summary** | **vpn** *vpn-id*]	Show information about the label forwarding table.

Copyright © Raisecom Technology Co., Ltd.

8.2 Configuring static route

8.2.1 Preparing for configurations

Scenario

The static route has the following advantages:

- Consume less time for the CPU to process them.
- Facilitate the administrator to learn the route.
- Be configured easily.

However, when configuring the static route, you need to consider the whole network. If the network structure is changed, you need to modify the routing table manually. Once the network scale is enlarged, it will consume lots of time to configure and maintain the network. In addition, it may cause more errors.

The default route is a specific static route. It will be used when no matched route is found in the routing table.

Prerequisite

N/A

8.2.2 Configuring IPv4 static route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip route** [**vrf** *vrf-name*] *ip-address mask-address* { *next-hop* [*interface-type interface-num*] | **NULL 0** } [**distance** *distance-value*] [**description** *text*] [**tag** *tag-value*]	Configure IPv4 static route.
	Raisecom(config)#**ip route** [**vrf** *vrf-name*] *ip-address mask-address* **vrf** *vrf-name* { *next-hop* [*interface-type interface-num*] | **NULL 0** } [**distance** *distance-value*] [**description** *text*] [**tag** *tag-value*]	
	Raisecom(config)#**ip route** [**vrf** *vrf-name*] *ip-address/m* { *next-hop* [*interface-type interface-num*] | **NULL 0** } [**distance** *distance-value*] [**description** *text*] [**tag** *tag-value*]	
	Raisecom(config)#**ip route** [**vrf** *vrf-name*] *ip-address/m* **vrf** *vrf-name* { *next-hop* [*interface-type interface-num*] | **NULL 0** } [**distance** *distance-value*] [**description** *text*] [**tag** *tag-value*]	
3	Raisecom(config)#**ip route** [**vrf** *vrf-name*] *ip-address mask-address* **NULL 0** [**distance** *distance-value*] [**description** *words*] [**tag** *tag-value*]	(Optional) configure the IPv4 static route of the Null interface.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config)#**ip route static distance** *distance*	(Optional) configure the default administrative distance of IPv4 static route. By default, it is 1.

8.2.3 Configuring IPv6 static route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 route** [**vrf** *vrf-name*] { *ipv6-address/0* | *ipv6-address/m* } [**vrf** *vrf-name*] *ipv6-next-hop* [*interface-type interface-number*] [**distance** *distance-value*] [**description** *words*] [**tag** *tag-value*]	Configure the IPv6 static route.
3	Raisecom(config)#**ipv6 route** [**vrf** *vrf-name*] { *ipv6-address/0* | *ipv6-address/m* } **NULL 0** [**distance** *distance-value*] [**description** *words*] [**tag** *tag-value*]	(Optional) configure the IPv6 static route of the NULL interface.
4	Raisecom(config)#**ipv6 route static distance** *distance*	(Optional) configure the default administrative distance of the IPv6 static route. By default, the administrative distance is 1.

8.2.4 Configuring BFD for static routes

BFD for IPv4 static routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip route** [**vrf** *vrf-name*] { *ip-address mask-address* | *ip-address/m* } [**vrf** *vrf-name*] *next-hop* [*interface-type interface-number* | **vlan** *vlan-id*] **track** [**bfd-session** *bfd-session-id*] [**track ping-session** *session-id*] [**trap** { **enable** | **disable** }]	Bind static routes with sessions and implement fast response to faults and route switching by BFD.
	Raisecom(config)#**ip route** [**vrf** *vrf-name*] *ip-address mask-address* **NULL 0 track** [**bfd-session** *bfd-session-id*] [**track ping-session** *session-id*] [**trap** { **enable** | **disable** }]	

Copyright © Raisecom Technology Co., Ltd.

BFD for IPv6 static routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 route** [**vrf** *vrf-name*] { *ipv6-address/0* | *ipv6-address/m* } [**vrf** *vrf-name*] *ipv6-next-hop* [*interface-type interface-number*] [**track bfd-session** *bfd-session-id*] [**track ping-session** *session-id*] [**trap** { **enable** | **disable** }]	Bind static routes with sessions and implement fast response to faults and route switching by BFD.
	Raisecom(config)#**ipv6 route** [**vrf** *vrf-name*] { *ipv6-address/0* | *ipv6-address/m* } **NULL 0** [**track bfd-session** *bfd-session-id*] [**track ping-session** *session-id*] [**trap** { **enable** | **disable** }]	

8.2.5 Checking configurations

Step	Command	Description
1	Raisecom#**show ip route** [**all** | **vrf** *vrf-name*] [**protocol** { **static** | **connected** | **bgp** | **ospf** | **isis** | **rip** }] [**detail**]	Show information about the IPv4 routing table.
2	Raisecom#**show ip route** [**vrf** *vrf-name*] *ip-address* [*mask-address*] [**longer-prefixes**] [**detail**]	Show routing information about the IPv4 address destined to a certain destination.
3	Raisecom#**show ip route** [**vrf** *vrf-name*] *ip-address1* [*mask-address1*] *ip-address2* [*mask-address2*] [**detail**]	Show routes between two IPv4 address ranges.
4	Raisecom#**show ipv6 route** [**all** | **vrf** *vrf-name*] [**protocol** { **static** | **connected** | **bgp** | **ospf** | **isis** | **rip** }] [**detail**]	Show IPv6 routing table.
5	Raisecom#**show ip route** [**vrf** *vrf-name*] **summary**	Show IPv4 routing summary.
6	Raisecom#**show ipv6 route** [**vrf** *vrf-name*] **summary**	Show IPv6 routing summary.
7	Raisecom#**show ipv6 route** [**vrf** *vrf-name*] { *start-ipv6-address/***0** | *start-ipv6-address/m* } { *end-ipv6-address/***0** | *end-ipv6-address/m* } [**detail**]	Show routes between two IPv6 address ranges.
8	Raisecom#**show ipv6 route** [**vrf** *vrf-name*] *ipv6-address* [*prefix-length*] [**longer-prefixes**] [**detail**]	Show routing information about the IPv6 address destined to a certain destination.

Copyright © Raisecom Technology Co., Ltd.

8.3 Configuring routing policy

8.3.1 Configuring IPv4 routing policy

IPv4 prefix list

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip prefix-list** *prefix-name* [**seq** *seq-number*] { **deny** | **permit** } { *ip-address/mask* | **any** | **default** }	Create an IPv4 prefix-list or add a node to the IP prefix-list. If no prefix-list ID (*seq-number*) is configured, the system will generate a prefix-list ID automatically. The generated pre-fix list ID has 5 digits.
	Raisecom(config)#**ip prefix-list** *prefix-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-address/mask* { **ge** *min-length* | **ge** *min-length* **le** *max-length* }	
	Raisecom(config)#**ip prefix-list** *prefix-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-address/mask*{ **ge** *min-length* **le** *max-length* | **le** *max-length* }	
3	Raisecom(config)#**ip prefix-list** *prefix-name* **description** *string*	Configure descriptions of the IPv4 prefix-list. If the length of descriptions exceeds 80 characters, the first 80 characters are available.

Note

- If one record is in permit type, all mismatched routes are in deny type by default. Only matched routes can pass filtering of the IP prefix-list.
- If one record is in deny type, all mismatched routes are in deny type by default. Even matched routes cannot pass filtering of the IP prefix-list. Therefore, you need to add a permit record after multiple deny records to allow other routes to pass.
- If there are multiple records in the IP prefix-list, there must be a record in permit type.

Configuring BGP filtering table

The BGP routing policy filters include: AS path filters, community attribute filters, extended community attribute filters, and RD filters.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip as-path access-list** *access-list-number* { **permit** | **deny** } *regexp*	(Optional) configure the filter that is based on AS path of the BGP route.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**ip community-list** { *standard-list-number* | **standard** *standard-list-name* }{ **permit** | **deny** } *community-number* [**internet**] [**local-as**] [**no-advertise**] [**no-export**]	(Optional) configure the filter that is based on standard or advanced community properties of the BGP route.
	Raisecom(config)#**ip community-list** { *expanded-list-number* | **expanded** *expanded-list-name* } { **permit** | **deny** } *regexp*	
4	Raisecom(config)#**ip extcommunity-list** { *standard-list-number* | **standard** *standard-list-name* }{ **permit** | **deny** } **rt** *rout-target-number*	(Optional) configure the filter that is based on standard community properties of the BGP route.
5	Raisecom(config)#**ip rd-filter** *rd-filter-number* { **permit** | **deny** } **rd** *rd -number*	(Optional) configure the filter that is based on RD property of the BGP route.

IPv4 mapping table

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**route-map** *map-name* { **permit** | **deny** } *number*	Create the route mapping table and enter route mapping configuration mode.
3	Raisecom(config-route-map)#**description** *string*	Configure descriptions of the route mapping table. If there is any space in descriptions, descriptions should be within quotes.
4	Raisecom(config-route-map)#**on-match next**	Configure the on-match sub-clause to continuing to match at the next node. By default, the process is finished after matching.
5	Raisecom(config-route-map)#**on-match goto** *number*	Configure the on-match sub-clause to continuing to match at some node. By default, the process is finished after matching.
6	Raisecom(config-route-map)#**call** *map-name*	Continue to match routes by scheduling other routing table after matching the route. By default, the process is finished after matching.
7	Raisecom(config-route-map)#**match ip next-hop** *acl-number*	Configure the match sub-clause which is to match the next hop based on extended IP ACL.
8	Raisecom(config-route-map)#**match ip next-hop prefix-list** *prefix-name*	Configure the match sub-clause which is to match the next hop based on IP prefix-list.
9	Raisecom(config-route-map)#**match ip address** *acl-number*	Configure the match sub-clause which is to match the IP address based on extended IP ACL.
10	Raisecom(config-route-map)#**match ip address prefix-list** *prefix-name*	Configure the match sub-clause which is to match the IP address based on IP prefix-list.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
11	Raisecom(config-route-map)#**match interface** *name*	Configure the match sub-clause which is to match the interface name.
12	Raisecom(config-route-map)#**match metric** *metric*	Configure the match sub-clause which is to match the rule based on route metric value.
13	Raisecom(config-route-map)#**match tag** *tag*	Configure the match sub-clause which is to match the rule based on Tag field of the route tagging.
14	Raisecom(config-route-map)#**match as-path** *path-list-number*	Configure the match sub-clause to the BGP routing information matching rule that is based on AS-Path filter.
15	Raisecom(config-route-map)#**match community** { *community-list-number* | *community-list-name* } [**exact-match**]	Configure the match sub-clause to the BGP routing information matching rule that is based on community filter.
16	Raisecom(config-route-map)# #**match extcommunity** { *extcommunity-list-number* | *extcommunity-list-name* }	Configure the match sub-clause to the BGP routing information matching rule that is based on extcommunity filter.
17	Raisecom(config-route-map)#**match ip route-source prefix-list** *prefix-name*	Configure the match sub-clause to the BGP routing information matching rule that is based on prefix-list matching with source address of the route.
18	Raisecom(config-route-map)# **match rd-filter** *rd-filter-number*	Configure the match sub-clause to the BGP routing information matching rule that is based on RD property filter.
19	Raisecom(config-route-map)#**set metric** [**+** | **-**] *metric*	Configure the set sub-clause which is to modify the route metric value after matching.
20	Raisecom(config-route-map)#**set metric-type** { **internal** | **external** | **type-1** | **type-2** | **internal-inc-ibgp** }	Configure the set sub-clause which is to modify the route metric type after matching.
21	Raisecom(config-route-map)#**set src** *ip-address*	Configure the set sub-clause which is to modify the source IP address after matching.
22	Raisecom(config-route-map)#**set ip next-hop** *ip-address*	Configure the set sub-clause which is to modify the next-hop IP address of the route after matching.
23	Raisecom(config-route-map)#**set tag** *tag*	Configure the set sub-clause which is to modify the routing information tag after matching.
24	Raisecom(config-route-map)#**set origin** { **egp** *as-number* | **igp** | **incomplete** }	Configure the set sub-clause which is to modify the route source of the BGP routing information that matches with the routing policy.
25	Raisecom(config-route-map)#**set as-path prepend** *as-number*	Configure the set sub-clause which is to modify the as-path property of the BGP routing information that matches with the routing policy.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
36	Raisecom(config-route-map)#**set local-preference** *preference*	Configure the set sub-clause which is to modify the local priority of the BGP routing information that matches with the routing policy.
27	Raisecom(config-route-map)#**set community** { *community-number* | **internet** | **local-as** | **no-advertise** | **no-export** } * [**additive**] Raisecom(config-route-map)# **set community none**	Configure the set sub-clause which is to set or delete the community property of the BGP routing information that matches with the routing policy.
28	Raisecom(config-route-map)#**set comm-list** { *community-list-number* | *community-list-name* }**delete**	Configure the set sub-clause which is to delete the community property of the BGP routing information that matches with the routing policy.
29	Raisecom(config-route-map)# **set extcommunity** { **rt** *route-target-number* **additive** | **color** *color-value* [**additive**] | **soo** *soo-value* [**additive**] }	Configure the set sub-clause which is to add or modify the community property of the BGP routing information that matches with the routing policy.
30	Raisecom(config-route-map)#**set ip backup-interface** *interface-type interface-number*	Configure the set sub-clause which is to modify the egress interface after meeting the matching rule.
31	Raisecom(config-route-map)#**set ip backup-nexthop** *nexthop-address*	Configure the set sub-clause which is to modify the backup next-hop address after meeting the matching rule.
32	Raisecom(config-route-map)#**set label** *label-id*	Configure the set sub-clause which is to modify the routing label.

8.3.2 Configuring IPv6 routing policy

IPv6 prefix list

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 prefix-list** *prefix-name* [**seq** *seq-number*] { **deny** | **permit** } { *ipv6-address/mask* | **any** | **default** } Raisecom(config)#**ipv6 prefix-list** *prefix-name* **seq** *seq-number* { **deny** | **permit** } *ipv6-address/mask* [**ge** *min-length*] [**le** *max-length*]	Create an IPv6 prefix list, or add a node to it. If you do not configure the prefix list *seq-number*, the sequence number be automatically generated by the system with a step of 5.
3	Raisecom(config)#**ipv6 prefix-list** *prefix-name* **description** *string*	Configure description of the IPv6 prefix list. If the input description exceeds 80 characters, the first 80 characters will be applied.

Copyright © Raisecom Technology Co., Ltd.

IPv6 routing table

Step	Command	Description
1	Raisecom(config)#**route-map** *map-name* { **permit** | **deny** } *number*	Create a routing table and enter routing table configuration mode.
2	Raisecom(config-route-map)#**match ipv6 address** *acl-number*	Configure a match clause which is to match the IP address based on extended IP ACL. The corresponding ACL list ranges from 7000 to 7999.
3	Raisecom(config-route-map)#**match ipv6 address prefix-list** *prefix-name*	Configure a match clause which is to match the IP address based on IP prefix list.
4	Raisecom(config-route-map)#**match ipv6 next-hop** *acl-number*	Configure a match clause which is to match the next hop based on extended IP ACL. The corresponding ACL list ranges from 7000 to 7999.
5	Raisecom(config-route-map)#**match ipv6 next-hop prefix-list** *prefix-name*	Configure a match clause which is to match the next hop based on IP prefix list.
6	Raisecom(config-route-map)#**match ipv6 route-source prefix-list** *prefix-name*	Configure a match clause which is to match the routing source address based on prefix list for the BGP routing matching rules.
7	Raisecom(config-route-map)#**set ipv6 next-hop** { *ipv6-address* | peer-address }	Configure the set clause which is to modify the next-hop IP address after meeting the matching requirements.
8	Raisecom(config-route-map)#**set ipv6 backup-interface** *interface-type interface-number*	Configure the set clause which is to modify the egress interface after meeting the matching requirements.
9	Raisecom(config-route-map)#**set ipv6 backup-nexthop** *ipv6-address*	Configure the set clause which is to modify the next-hop address after meeting the matching requirements.

8.3.3 Checking configurations

No.	Command	Description
1	Raisecom#**show ip as-path access-list** *access-list-number*	Show filtering information about the AS-path list.
2	Raisecom#**show ip prefix-list** [*prefix-name*] [**seq** *seq-number*]	Show information about the IP prefix list.
3	Raisecom#**show ip prefix-list** *prefix-name ip-address/m* { **longer** | **first-match** }	
4	Raisecom#**show ip prefix-list summary** [*prefix-name*]	Show summary of the IP prefix list.
5	Raisecom#**show ip prefix-list detail** [*prefix-name*]	Show statistics on the IP prefix list.
6	Raisecom#**show ipv6 prefix-list** [*prefix-name*] [**seq** *seq-number*]	Show information about the IPv6 prefix list.
7	Raisecom#**show ipv6 prefix-list** *prefix-name ipv6-address/m* { **longer** | **first-match** }	

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
8	Raisecom#**show ipv6 prefix-list summary** [*prefix-name*]	Show summary of the IPv6 prefix list.
9	Raisecom#**show ipv6 prefix-list detail** [*prefix-name*]	Show statistics on the IPv6 prefix list.
10	Raisecom#**show route-map** *map-name*	Show information about the routing table.
11	Raisecom#**show ip rd-filter**	Show detailed configurations of the RD attribute filter.
12	Raisecom#**show ip community-list** [*community-list-number*] [*community-list-name*]	Show information about the group attribute list.
13	Raisecom#**show ip extcommunity-list** [community-list-number] [community-list-name]	Show information about the extended group attribute list.

8.4 Configuring OSPFv2

The device supports OSPFv2 and OSPFv3.

- In terms of working mechanism, OSPFv2 is basically the same as OSPFv3.
- In terms of network suitability,
  - OSPFv2 is mainly applicable to IPv4 networks.
  - OSPFv3 is mainly applicable to IPv6 networks.

Note

OSPF runs on L3 interfaces. By default, the interface is in routed mode. If the current interface is configured to the switch mode, you have to use the **no portswitch** command to return the interface to the routed mode.

8.4.1 Configuring OSPF basic functions

Starting OSPF network process

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**vrf** *vrf-name*] [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**network** *ip-address wild-card-mask* **area** *area-id*	Configure network segments included in the OSPF area.

Copyright © Raisecom Technology Co., Ltd.

- If you manually configure the *router-id* parameter through the optional parameters in the **router ospf** *process-id* [**router-id** *router-id*] command, the OSPF process will select the *router-id* parameter first. Otherwise, the parameter is selected automatically.
- If the OSPF process is configured or selects the *router-id* parameter, after being modified, the *router-id* parameter takes effect after the OSPF process is rebooted.

(Optional) configuring OSPF DCN process

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**capability opaque**	Enable OSPF opaque LSA. By default, opaque LSA is disabled.
4	Raisecom(config-router-ospf)#**capability dcn**	Enable OSPF network management self-connection. By default, OSPF network management self-connection is enabled.

(Optional) configuring no aging of OSPF neighbors

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**capability inactivity timer**	Enable no aging of OSPF neighbors By default, it is disabled.

8.4.2 Configuring OSPF route properties

Configuring OSPF cost value of interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip ospf cost** *cost*	Configure the OSPF cost of the IP interface. By default, the interface routing cost is not configured.

Copyright © Raisecom Technology Co., Ltd.

Configuring bandwidth reference value

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**reference-bandwidth** *bandwidth*	Configure the bandwidth reference value of the link. By default, the bandwidth reference value is 100 Mbit/s.

Note

- After the routing cost is manually configured through the ip ospf cost command, the manually-configured routing cost takes effect.
- If the routing cost is not configured manually but the link bandwidth reference value is configured, the routing cost is automatically configured based on link bandwidth reference value. The formula is: cost = link bandwidth reference value (bit/s) / link bandwidth. If the cost value is greater than 65535, it is configured to 65535. If no link bandwidth reference value is configured, it is configured to 100 Mbit/s by default.

Configuring OSPF administrative distance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**distance** *administrative-distance*	Configure the OSPF administrative distance. By default, it is 110.
4	Raisecom(config-router-ospf)#**distance ospf** { **intra-area** | **inter-area** | **external** } *distance*	Configure the administrative distance of OSPF specified route. By default, it is 0. However, it takes 110 as the standard.

Configuring device to be compatible with RFC1583

The purpose of configuring compatible RFC1583 is to determine the method of external route calculation.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-router-ospf)#**compatible rfc1583**	Configure the OSPF to be compatible with RFC1583. By default, the OSPF is compatible with RFC1583.

8.4.3 Configuring OSPF network type

Configuring OSPF network

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip ospf network** { **broadcast** | **non-broadcast** | **ptmp** | **ptp** }	Configuring the network type of the interface. By default, it is the broadcast network.

Configuring DR election priority

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip ospf priority** *priority*	Configure the DR election priority on the IP interface. By default, it is 1.

Configuring OSPF NBMA network neighbor

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip ospf network non-broadcast** Raisecom(config-port)#**exit**	Configure the interface network mode to NBMA and exit interface configuration mode.
4	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
5	Raisecom(config-router-ospf)#**neighbor** *ip-address* [**priority** *priority*]	Configure the NBMA neighbor and its priority. By default, no NBMA neighbor is configured and the priority is 0 when you configure the NBMA neighbor.

Copyright © Raisecom Technology Co., Ltd.

Caution

Priorities configured by the **neighbour** and **ip ospf priority** *priority* commands are different:

- The priority configured by the neighbor command indicates that whether the neighbor has the right to vote. If you set the priority to 0 when configuring the neighbor, the local router believes that the neighbor has no right to vote and will not sent Hello packets to the neighbor. This method helps reduce the number of Hello packets transmitted through the network during DR and BDR election processes. However, if the local router is a DR or BDR, it will send the Hello packet to the neighbor, whose priority is configured to 0, to establish the neighboring relationship.
- The priority configured by the **ip ospf priority** *priority* command is used for actual DR election.

8.4.4 Configuring OSPF area

Configuring OSPF NSSA area

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter the OSPF configuration mode.
3	Raisecom(config-router-ospf)#**area** *area-id* **nssa** [**no-summary**]	Configure the area to be NSSA area. Only non-backbone area can be NSSA area. By default, the non-backbone areas are all common areas.

Configuring Stub area

For the non-backbone area at the edge of Autonomous System (AS), you can configure the **stub** command on all routers in the area to configure the area to a Stub area. In this case, Type5 LSA, which is used to describe external routes of the AS, cannot be flooded in the Stub area. This facilitates reducing the routing table size.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**area** *area-id* **stub** [**no-summary**]	Configure the area to a Stub area. The **no-summary** parameter is used to disable the ABR to send Summary LSA to the Stub area. It means that it is a Totally Stub area and the ABR is available for the Stub only. By default, no area is the Stub area.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-router-ospf)#**area** *area-id* **default-cost** *cost*	Configure the default route cost of the Stub area. This command is available for the ABR in the Stub area only. By default, it is 1.

Caution

- All routers in the Stub area must be configured with the Stub property through the **area** *area-id* **stub** command.
- To set an area to a Totally Stub area, all routers in the area must be configured by the **area** *area-id* **stub** command. In addition, all ABRs in the area must be configured by the **area** *area-id* **stub** no-summary command.
- The backbone area cannot be set to the Stub area.
- ASBR should not be in the Stub area. It means that routers beyond the AS cannot be transmitted in the Stub area.

8.4.5 Configuring load balancing

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**maximum load-balancing** *number*	Configure the maximum number of IP equal-cost multi-path load balancing.

8.4.6 Maximizing LSA metric

Increase the metric value (65535) of the link in the LSA generated by the device to inform other OSPF devices of not using this Stub device to forward data.

- After enabling the maximum metric value function of OSPF LSA packets by using the **max-metric router-lsa** command, the metric values of all non-Stub area adjacency relationships will be configured to 0xFFFF (0xFFFF is still available, and 0xFFFFFF is unavailable). The adjacency measurement value of the Stub region is not affected, and the cost of the interface is filled in according to its normal value.
- After enabling the maximum metric function of OSPF LSA packets by using the **max-metric router-lsa include-stub** command, the metric values of all adjacency relationships (including stub area adjacency relationships) are configured to 0xFFFF by the device.
- You can use the **on-startup** *time* parameter to configure the timer that lasts for the maximum value after restart. After the timer expires, the metric value will return to its original value.
- When optional parameters **summary lsa** and **external lsa** are configured, the corresponding area LSA will be refreshed according to the configured metric values.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**max-metric router-lsa** [**include-stub**] [**on-startup** *time*] [**summary-lsa** *summary-metric*] [**external-lsa** *external-metric*]	Enable maximum metric of OSPF LSA packets. The metric of LSA packet in the corresponding area will be automatically configured to 0xFFFF. By default, it is disabled.

8.4.7 Optimizing OSPF network

Configuring OSPF packet timer

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip ospf dead-interval** *seconds*	Configure the OSPF neighbor dead interval. By default, it is 4 times of Hello packet delivery interval. If no Hello packet delivery interval is configured, it is 40s for P2P and Broadcast interfaces and 120s for P2MP and NBMA interfaces by default.
4	Raisecom(config-port)#**ip ospf hello-interval** *seconds*	Configure the ODPF Hello packet delivery interval. By default, it is 10s for P2P and Broadcast interfaces and 30s for P2MP and NBMA interfaces
5	Raisecom(config-port)#**ip ospf poll-interval** *seconds*	Configure the OSPF Poll timer interval. By default, it is 120s.
6	Raisecom(config-port)#**ip ospf retransmit-interval** *seconds*	Configure the LAS retransmission interval on the IP interface. By default, it is 5s.
7	Raisecom(config-port)#**ip ospf transmit-delay** *seconds*	Configure the LSA retransmission delay on the IP interface. By default, it is 1s.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
8	Raisecom(config-port)#**ip ospf neighbor hold-max-cost timer** *mill-seconds*	Configure the maximum time for holding the cost in the router-lsa of the local device by OSPF after the neighbor status become full to delay the switching of routes. When the OSPF interface changes from Down to Up, OSPF neighbor relation will be re-established. After IGP routes converge, traffic will be switched back. Due to the fast convergence speed of IGP routes, multiple services that rely on IGP routes may need the delay switching of IGP route. By configuring the **ip ospf neighbor hold-max-cost** command, after the OSPF neighbor status is full, OSPF will maintain the maximum cost advertised in the LSA of the local device for the configured time. In this way, traffic continues to be forwarded on the original path. When the maximum cost timer expires, the cost returns to normal and traffic will switch back normally. By default, the maximum time for holding the cost is not configured after neighbor establishment.

Caution

- When the dead-interval is not manually configured, after hello-interval is configured, dead-interval and poll-interval is changed to 4 times of hello-interval.
- When the dead-interval is manually configured, after hello-interval is configured, no effect is brought to the dead-interval and poll-interval. No matter whether you configure the poll interval or not, the poll-interval changes with the dead-interval.
- Therefore, we recommend configuring these 3 values in the following order: hello-interval, dead-interval, and poll-interval.

Configuring SPF calculation interval

When the OSPF Link State Database (LSDB) changes, it needs to re-calculate the shortest path. If the network changes frequently and it needs to calculate the shortest path immediately, it will occupy a great amount of system resources and affect efficiency of the router. By adjusting the SPF calculation interval, you can prevent some effects brought by frequent network changes.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**timers spf** { *delay-time hold-time* | **millisecond** *delay-milliseconds hold-milliseconds* }	Configure the calculation delay and interval of the OSPF route. By default, the calculation delay is 2s and the calculation interval is 3s.
4	Raisecom(config-router-ospf)#**timers spf-intelligent-timer** *max-interval start-interval hold-interval*	Configure the intelligent timer for calculating OSPF routes.

Copyright © Raisecom Technology Co., Ltd.

Configuring partial route calculation

When there are a large number of devices on the network, and the cause to route change is route change (such as adding a network segment) instead of adding devices, enable partial route calculation to speed up OSPF convergence. This is applicable when the topology is not changed.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router ospf` *process-id* `[ router-id` *router-id* `]`	Start an OSPF process and enter OSPF configuration mode.
3	`Raisecom(config-router-ospf)#spf prc { enable | disable }`	Configure partial route calculation. By default, it is disabled.

Configuring OSPF passive interface

To make some OSPF routing information not obtained by some router on the network, you can set the interface to an OSPF passive interface to disable the interface to send OSPF packets.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode.
3	`Raisecom(config-port)#ip ospf passive-interface enable`	Enable passive interface on the OSPF interface. By default, it is disabled.

Configuring MTU ignorance

By default, the value of MTU domain in the DD packet is the MTU value of the interface, which sends the packet. Default MTU values may vary on devices. In addition, if the MTU value of the DD packet is greater than the one of the interface, the packet will be discarded. To ensure receiving the packet properly, enable MTU ignorance to set the MTU value to 0. Therefore, all devices can receive the packet.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode.
3	`Raisecom(config-port)#ip ospf mtu-ignore enable`	Enable MTU ignorance on the IP interface. By default, MTU ignorance is disabled on the IP interface to check MTU of the OSPF DD packet.

Copyright © Raisecom Technology Co., Ltd.

Preventing Hello reverse packet attacks

To prevent Hello reverse packet attacks, configure the interval for sending Hello packets, that is, the interval at which the router periodically sends Hello packets to neighbor routers.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**hello-reverse-attack suppression** *interval*	Configure the sending interval of Hello packets. By default, the sending interval of Hello packets is 10s.

Configuring LDP synchronization on interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip ospf ldp-sync**	Enable LDP-OSPF synchronization on the interface. LDP-OSPF synchronization is used to solve the problem that the LSP traffic is lost on the network with master and standby links of LSP. The specific scenario is as below: When the active link is normal, but the LDP local session or LDP adjacency between active link nodes fails, the LSP traffic switches from the active link to the standby link, while IGP continues to use the active link, resulting in LSP traffic loss. After LDP-OSPF synchronization is configured, when the LDP local session or LDP adjacency between the active link nodes fails, IGP will advertise the maximum cost value on that link, switching the route to the standby link, and LSP will also switch to the standby link. When the active link fault is cleared, due to the faster convergence speed of IGP than LDP, IGP will switch back to the active link before LDP, resulting in LSP traffic loss. After LDP-OSPF synchronization is configured, when the active link fault is cleared, IGP releases the maximum cost value on the active link, delaying the switch back of the IGP route until the LSP of the active link is successfully established before switching back. By default, it is disabled.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-port)#**ip ospf timer ldp-sync** { **hold-down** *hold-down-seconds* | **hold-max-cost** { *hold-max-cost-seconds* | **infinite** } }	Configure the OSPF LDP synchronization timer. • Hold-down timer: hold-down interval for waiting for establishing the LDP and LSP adjacency without establishing OSPF neighbor relationship • Hold-max-cost: hold time for advertising the maximum cost value by OSPF on the local device By default, the hold-down timer is 10s, and the hold-max-cost timer is 90s.

8.4.8 Configuring OSPF authentication policy

Configuring OSPF area authentication policy

All routers in an area need to be configured with the identical area authentication policy (non-authentication, simple authentication, or MD5 authentication). The OSPF area has no authentication password but adopts the interface authentication password. If no interface authentication password is configured, the empty password will be used for authentication.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**area** *area-id* **authentication** { **md5** | **simple** }	Configure the area authentication mode. By default, it is non-authentication.

Configuring OSPF interface authentication policy

Packet authentication prioritizes selecting the interface authentication mode. If the interface authentication mode is configured to non-authentication mode, the area authentication mode will be selected. OSPF interfaces cannot establish the neighbor relationship unless the authentication mode and authentication password are identical.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip ospf authentication** { **md5** | **simple** }	Configure the authentication mode of the IP interface. By default, it is non-authentication. It means adopting the area authentication mode.
4	Raisecom(config-port)#**ip ospf authentication-key** { **simple** [**0** | **7**] *password* | **md5** { [*key-id* [**0** | **7**] *password*] | **keychain** *keychain-name* } }	Configure the authentication password of the IP interface.

Copyright © Raisecom Technology Co., Ltd.

8.4.9 Controlling OSPF redistributed routes

Configuring OSPF redistributed routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**redistribute** { **static** | **connected** | **bgp** } [**metric** *metric*] [**metric-type** { **1** | **2** }] [**tag** *tag-value*] [**route-map** *map-name*] Raisecom(config-router-ospf)#**redistribute** { **ospf** | **isis** } *process-id* [**metric** *metric*] [**metric-type** { **1** | **2** }] [**tag** *tag-value*] [**route-map** *map-name*]	Configure OSPF route redistribution polity. By default, no external route is redistributed. When an external route is redistributed: • When the directly-connected and static route is redistributed, the metric is 1 by default. When other routes are redistributed, take the original metric of the external route as the metric of the LSA. • If no Metric-type is specified, the Metric-type is Type2 by default. • If no Tag is specified, take the original Tag of the external route as the Tag of the LSA.
4	Raisecom(config-router-ospf)#**redistribute limit** *limit-number*	Configure the threshold of redistributed OSPF external routes. By default, no threshold is configured.

Configuring inter-area route summarization

If there are sequent network segments in the area, you can configure route summarization on the ABR to aggregate these network segments to a network segment. When sending routing information, the ABR generates Type3 LSA by taking the network segment as the unit.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**area** *area-id* **range** *ip-address ip-mask* [**not-advertise**]	Configure the inter-area route summarization. By default, no inter-area route summarization is configured. When you configure the summary route, the cost is the maximum Metric of the LSA by default. In addition, the summary route is redistributed.

Copyright © Raisecom Technology Co., Ltd.

Aggregating redistributed external routes

After the external route is redistributed, configure route summarization on the ASBR. The RAX721 just puts the summary route on the ASE LSA. This helps reduces the number of LSAs in the LSDB.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router ospf process-id [ router-id router-id ]`	Start an OSPF process and enter OSPF configuration mode.
3	`Raisecom(config-router-ospf)#summary-address ip-address ip-mask [ not-advertise ] [ metric metric ]`	Aggregate external routes. By default, external routes are not aggregated. When external aggregates are aggregated, the Metric is the maximum Metric of the LSA by default.

Advertising default route

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router ospf process-id [ router-id router-id ]`	Start an OSPF process and enter OSPF configuration mode.
3	`Raisecom(config-router-ospf)#default-information originate [ always ] [ metric metric ] [ type { 1 | 2 } ]`	Advertise the default route. By default, no default route is generated. When the default LSA is generated, if the **always** key word is specified, the default Metric is 1. If the **always** key word is not specified, the Metric is 10.

8.4.10 Configuring OSPF routing policy

Configuring OSPF receiving policy

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip prefix-list list-name { permit | deny } ip-address mask-length [ ge ge-length ] [ le le-length ]`	Configure the IP prefix-list.
3	`Raisecom(config)#access-list acl-number`	Create an ACL and enter ACL configuration mode. When the *acl-number* ranges from 2000 to 2999, the device enters the extended IP ACL configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config-acl-ip-ext)# **rule** [*rule-id*] { **deny** | **permit** } **ip** { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** }	Configure the extended IP ACL rules.
4	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
5	Raisecom(config-router-ospf)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* } **in**	Configure the OSPF filtering policy for receiving the OSPF inter-area routes, intra-area routes, and AS external routes.

Note

- Before configuring OSPF receiving policy, ensure that the IP ACL used by the OSPF receiving policy has been created.
- When the RAX721 performs filtering based on IP ACL, if the ACL mode is configured to permit, all routes, which match with the ACL, can pass. Others are filtered.
- You cannot modify the IP ACL unless it is not used by any routing policy.
- Different from IP ACL, the IP prefix-list can be modified even it is being used.
- If the configured IP prefix-list does not exist, do not filter received routes.

Configuring OSPF releasing policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip prefix-list** *list-name* { **permit** | **deny** } *ip-address mask-length* [**ge** *ge-length*] [**le** *le-length*]	Configure the IP prefix-list. You can use the **no ip prefix-list** *list-name* command to delete the configuration.
3	Raisecom(config)#**access-list** *acl-number*	When the *acl-number* ranges from 2000 to 2999, the device enters the extended IP ACL configuration mode.
	Raisecom(config-acl-ip-ext)# **rule** [*rule-id*] { **deny** | **permit** } **ip** { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** }	Configure the extended IP ACL rule.
4	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
5	Raisecom(config-router-ospf)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* } **out**	Configure the filtering policy that the OSPF releases 5 types of LSAs to the AS.
6	Raisecom(config-router-ospf)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* } **out** [**static** | **connected** | **bgp** | **rip**]	Configure the OSPF releasing policy.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config-router-ospf)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* } **out** { **ospf** | **isis**} *process-id*	

Note

- Before configuring OSPF global releasing policy, ensure that the IP ACL used by the OSPF global releasing policy has been created.
- You cannot modify the IP ACL unless it is not used by any routing policy.
- Different from IP ACL, the IP prefix-list can be modified even it is being used.
- After global releasing policy is configured, routes cannot be redistributed to the local LSDB unless it passes the global releasing policy. After protocol releasing policy is configured, the route can be redistributed through the protocol releasing policy.
- After protocol releasing policy is configured, the redistributed protocol route can be redistributed to the local LSDB through the protocol releasing policy. If global releasing policy is also configured, the route must be redistributed through the global releasing policy.

Configuring inter-area route filtering policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip prefix-list** *list-name* { **permit** | **deny** } *ip-address mask-length* [**ge** *ge-length*] [**le** *le-length*]	Configure the IP prefix-list. You can use the **no ip prefix-list** *list-name* command to delete the configuration.
3	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
4	Raisecom(config-router-ospf)#**area** *area-id* **filter prefix-list** *list-name* { **in** | **out** }	Configure Type3 LSA filtering policy in the area.

Note

If the configured filtering policy does not exist, it believes that the command fails to configure the filtering policy and no filtering operation is performed on received routes.

8.4.11 Configuring BFD for OSPF

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enter OSPF configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-router-ospf)#**bfd all-interfaces**	Enable global BFD. By default, it is disabled.
4	Raisecom(config-router-ospf)#**exit**	Enter global configuration mode.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**ip ospf bfd**	Enable BFD on the interface. By default, it is disabled.

Note

- If global BFD is enabled through the bfd all-interfaces command, no matter what BFD configurations are set on the interface, BFD is enabled.
- If global BFD is disabled, BFD configurations on the interface take effect.

8.4.12 Configuring OSPF for MPLS-TE

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**capability opaque**	Enable OSPF opaque LSA. By default, it is disabled.
4	Raisecom(config-router-ospf)#**mpls traffic-eng area** *area-id*	Enable TE in the OSPF area. By default, it is disabled.
5	Raisecom(config-router-ospf)#**mpls traffic-eng router-id** *router-id*	Configure the Router ID of the MPLS-TE router.

8.4.13 Checking configurations

No.	Command	Description
1	Raisecom#**show ip ospf** [*process-id*]	Show OSPF basic information.
2	Raisecom#**show ip ospf** [*process-id*] **route**	Show OSPF routing information.
3	Raisecom#**show ip ospf** [*process-id*] **interface** [*interface-type interface-number*]	Show OSPF interface information.
4	Raisecom#**show ip ospf** [*process-id*] **neighbor** [*interface-type interface-number*] [*ip-address*]	Show OSPF neighbor information.
5	Raisecom#**show ip ospf** [*process-id*] **neighbor statistics**	Show OSPF neighbor statistics.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
6	Raisecom#**show ip ospf** [*process-id*] **database** [**max-age** | **self-originate**]	Show information about OSPF link status database.
7	Raisecom#**show ip ospf** [*process-id*] **database** { **asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as** } [*ip-address*] [**adv-router** *ip-address* | **self-originate**]	Show details about the OSPF link status database.
8	Raisecom#**show ip ospf** [*process-id*] **database statistics**	Show database statistics on the OSPF link status.
9	Raisecom#**show ip ospf** [*process-id*] **border-routers**	Show information about area border router and ASBR.
10	Raisecom#**show ip ospf** [*process-id*] **summay-address**	Show summary about the OSPF ASBR external route.

8.4.14 Maintenance

Command	Description
Raisecom#**clear ip ospf** [*process-id*] **process** [**graceful**]	Restart the OSPF process.
Raisecom(config-router-ospf)#**capability restart** { **graceful** | **signaling** }	Configure OSPF GR which can ensure that routers running OSPF forward services normally when the active/standby switchover starts or OSPF restarts.

8.5 Configuring OSPFv3

8.5.1 Starting OSPFv3 process

Starting OSPFv3 process

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**router-id** *router-id*	Configure the Router-ID of the OSPF process.

Copyright © Raisecom Technology Co., Ltd.

8.5.2 Configuring OSPFv3 network type

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 ospf network** { **broadcast** | **nbma** | **ptmp** | **ptp** } [**instance-id** *instance-id*]	Configure the network type of the OSPFv3 area interface. By default, the network type of the OSPFv3 area is broadcast.

8.5.3 Configuring OSPFv3 area

Configuring Stub area

For non-backbone areas at the edge of the AS, you can configure the stub command on all routing devices in the area to configure the area as a stub area. In this way, Type5 LSAs describing external routes of the autonomous system will not flood in the stub area, reducing the size of the routing table.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	Start an OSPFv3 process and enter OSPFv3 configuration mode. **Note** The device supports at most one OSPFv3 process, and one process can contain multiple OSPFv3 instances.
3	Raisecom(config-ospf6)#**area** { *area-id* | *ip-format-area-id* } **stub** [**no-summary**]	Configure the area to a Stub area. The no-summary parameter is used to prevent the ABR from sending a Summary LSA to the Stub area, that is, the Totally Stub area, which is only used for the ABR of the Stub area.

Caution

- All routing devices in the stub area must be configured with the stub attribute using the **area** *area-id* **stub** command.
- If you want to configure an area as a totally stub area, all routers in the area must be configured with the **area** *area-id* **stub** command, and the ABR routing device in the area must be configured with the **area** *area-id* **stub no-summary** command.
- Only non-backbone areas can be configured as stub areas.
- ASBR cannot exist in the stub area, that is, routes outside the autonomous system cannot be propagated in the area.

Copyright © Raisecom Technology Co., Ltd.

Configuring area virtual link

OSPF uses a regional design, and conventional areas can only exchange LSAs with backbone areas. However, in actual networking, some conventional areas cannot be directly connected to the backbone area but can only be directly connected to other conventional areas. In this scenario, OSPF virtual links are used to virtualize the adjacent conventional areas as the backbone area, so that those conventional areas that cannot be directly connected to the backbone area can also obtain routes from other OSPF areas.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**area** *area-id* **virtual-link** *router-id* [**dead-interval** *dead-interval* | **hello-interval** *hello-interval*] [**retransmit-interval** *retransmit-interval*] [**transmit-delay** *transmit-delay*] [**instance-id** *instance-id*]	Configure the virtual link.

8.5.4 Configuring OSPFv3 interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 ospf** *process-id* **area** *area-id* [**instance-id** *instance-id*]	Configure the local area of the interface.
4	Raisecom(config-port)#**ipv6 ospf mtu-ignore** [**instance-id** *instance-id*]	Configure the OSPFv3 area interface to ignore MTU check when checking packets. By default, the OSPFv3 area interface checks the MTU.
5	Raisecom(config-port)#**ipv6 ospf passive-interface** [**instance-id** *instance-id*]	(Optional) configure the interface to a passive interface. By default, the interface is a passive interface.
6	Raisecom(config-port)#**ipv6 ospf neighbor router-id** *router-id ipv6-address* [**priority** *priority*] [**poll-interval** *poll-interval*] [**instance-id** *instance-id*]Raisecom(config-ospf6)#**exit**	Configure the NBMA neighbor, its priority, and sending interval.
7	Raisecom(config-port)#**ipv6 ospf poll-interval** *interval* [**instance-id** *instance-id*]	Configure the Poll-Interval timer in the NBMA network. By default, the Poll-Interval timer is 60s.

Copyright © Raisecom Technology Co., Ltd.

8.5.5 Controlling OSPFv3 redistributed routes

Configuring OSPFv3 redistributed routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**redistribute** { **static** | **connected** | **isisv6** *process-id* | **bgp4+** | **ripng** | **ospfv3** *process-id* } [**metric** *metric*] [**metric-type** { **1** | **2** }] [**tag** *tag-value*] [**route-map** *map-name*]	Configure OSPFv3 route redistributing policies. By default, no external route is redistributed. When redistributing the external routes: • When direct routes and static routes are imported, the metric is 1 by default. When other types of routes are imported, the original metric of the external route is used as the LSA metric. • If Metric-type is not specified, the default Metric-type is Type2. • If no tag is specified, the original tag of the external route is used as the LSA tag.

Configuring inter-domain route summarization

If there are some continuous network segments in an area, you can configure route summarization on the ABR to aggregate these continuous network segments into one network segment. When ABR sends routing information to other areas, it generates Type3 LSAs in units of network segments.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode. **Note** The device supports up to one OSPFv3 process, and one process can contain multiple OSPFv3 instances.
3	Raisecom(config-ospf6)#**area** *area-id* **range** *ipv6-address/mask* [**not-advertise**]	Configure inter-domain route summarization.

Aggregating redistributed external routes

After ASBR imports external routes, if you configure route summarization, the device only puts the summary routes in ASE LSA for announcement, reducing the number of LSAs in LSDB.

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**summary-address** *ipv6-address/mask* [**not-advertise**]	Configure external route summarization. By default, external routes are not aggregated.

Advertising default routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**default-information originate** [**always**] [**metric** *metric*] [**metric-type** { **1** | **2** }]	Advertise the default route. By default, no default route is generated. When the system generates the default LSA, if the **always** keyword is specified, the default metric is 1, otherwise the metric is 10.

8.5.6 Configuring timer of OSPFv3 packets

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 ospf hello-interval** *seconds* [**instance-id** *instance-id*]	Configure the interval for sending Hello packets on the OSPFv3 area interface. By default, the interval is 10s.
4	Raisecom(config-port)#**ipv6 ospf dead-interval** *seconds* [**instance-id** *instance-id*]	Configure the neighbor dead time on the OSPFv3 area interface. By default, the neighbor dead time is 4 times the interval for sending Hello packets; if the interval for sending Hello packets is not configured, then it is 40s by default.
5	Raisecom(config-port)#**ipv6 ospf transmit-delay** *seconds* [**instance-id** *instance-id*]	Configure the transmission delay time of LSA on the OSPFv3 area interface. By default, it is 1s.
6	Raisecom(config-port)#**ipv6 ospf retransmit-interval** *seconds* [**instance-id** *instance-id*]	Configure the interval for retransmitting the lost LSA packets on the OSPFv3 area interface. By default, it is 5s.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
7	Raisecom(config-port)#**ipv6 ospf neighbor hold-max-cost timer** *mill-seconds*	Configure the maximum time for holding the cost in the router-lsa of the local device by OSPF after the neighbor status become full to delay the switching of routes. When the OSPF interface changes from Down to Up, OSPF neighbor relation will be re-established. After IGP routes converge, traffic will be switched back. Due to the fast convergence speed of IGP routes, multiple services that rely on IGP routes may need the delay switching of IGP route. By configuring the **ip ospf neighbor hold-max-cost** command, after the OSPF neighbor status is full, OSPF will maintain the maximum cost advertised in the LSA of the local device for the configured time. In this way, traffic continues to be forwarded on the original path. When the maximum cost timer expires, the cost returns to normal and traffic will switch back normally. By default, the maximum time for holding the cost is not configured after neighbor establishment.

8.5.7 Configuring OSPFv3 route management

Configuring route attributes on OSPFv3 interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 ospf cost** *value* [**instance-id** *instance-id*]	Configure the routing cost on the OSPFv3 area interface. By default, the routing cost of an OSPFv3 interface = 10^8 (bit/s)/interface bandwidth (bit/s). If the calculated cost is greater than 65535, the maximum value is 65535.
4	Raisecom(config-port)#**ipv6 ospf priority** *value* [**instance-id** *instance-id*]	Configure the routing priority on the OSPFv3 area interface. By default, the routing priority on the OSPFv3 area interface is 1.

Configuring OSPFv3 administrative distance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-ospf6)#**distance** *administrative-distance*	Configure OSPFv3 administrative distance. By default, it is 110.

Configuring bandwidth reference value

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**reference-bandwidth** *bandwidth*	Configure the bandwidth reference value of the link. By default, the bandwidth reference value is 100 Mbit/s.

Configuring SPF calculation interval

When the OSPF Link State Database (LSDB) changes, the shortest path needs to be recalculated. If the network changes frequently, and the shortest path is calculated immediately for each change, it will occupy a lot of system resources and affect the efficiency of the routing device. By adjusting the SPF calculation interval, you can suppress the impact of frequent network changes.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**timers spf** *delay-time hold-time*	Configure the delay time and interval of OSPFv3 route calculation. By default, the delay is 2s and the interval is 3s.
4	Raisecom(config-ospf6)#**timers spf-intelligent-timer** *max-interval start-interval hold-interval*	Configure the intelligent timer for calculating OSPFv3 routes.

Configuring load balancing

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-ospf6)#**maximum load-balancing** *number*	Configure the maximum number of IP ECMP paths supported by OSPFv3.

Configuring DN bit interference

When the DN bit is set, it indicates that the route is an redistributed route. When the device receives a DN bit set LSA, it will not perform routing calculations to prevent loop formation.

When VPNv4 route is redistributed into OSPF scenarios, the formed Class 3, Class 5, and Class 7 LSAs will have DN bits set to 1. When the PE receives LSA with DN bit set to 1 in VPN instance, it does not perform routing calculation. To address this issue,

- Use the dn **bit set disable** command to disable DN bit set, so that LSAs with DN bits set can still participate in routing calculations and calculate routes normally.
- Use the **dn bit check disable** command to disable DN bit check and directly calculate the route normally, so that LSAs with DN bit set can participate in route calculation normally.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**dn-bit-set disable**	Disable DN bit set. By default, the DN bit in the LSA can be configured.
4	Raisecom(config-ospf6)#**dn-bit-check disable** { **summary** | **ase** }	Disable the check of the DN bit in the LSA. By default, the check of the DN bit in the LSA is enabled.

Configuring the Route-Tag of VPN routes

The route tag Route-Tag serves as an anti-ring function, and the system supports configuring the Route-Tag.

By default, the first two bytes of the Tag are fixed at 0xD000, and the last two bytes are the AS ID of the local BGP. For example, if the AS ID of the local BGP is 100, the default decimal value of the Tag is 3489661028; If the BGP AS ID is greater than 65535, the Tag value is 0 and manual configuration of the Tag value is required. If BGP is not configured, the default value is 0.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-ospf6)#**route-tag** { **enable** | **disable** }	After the **route tag disable** command is configured, the OSPFv3 process of the private network ignores the check of tag value when performing route calculation. If the DN bit check passes, the OSPFv3 process can perform route calculation on the LSA and possibly calculate the route. By default, VPN route tag loop detection is enabled.
4	Raisecom(config-ospf6)#**route-tag** *tag-value*	After this command is configured, the OSPFv3 process of the private network configures the tag value of the generated Type-5 LSA according to the configured value when the BGP route is redistributed.

Configuring no aging of OSPFv3 neighbors

After no aging of OSPFv3 neighbors is enabled, OSPFv3 refreshes the neighbor keepalive time when receiving non-hello packets. This function solves the problem of neighbor involuntary interruption upon massive update packets.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**capability inactivity timer**	Enable no aging of OSPFv3 neighbors. By default, it is disabled.

Configuring partial route calculation

When there are a large number of devices on the network, and the cause to route change is route change (such as adding a network segment) instead of adding devices, enable partial route calculation to speed up OSPFv3 convergence. This is applicable when the topology is not changed.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**spf prc** { **enable** | **disable** }	Configure OSPFv3 partial route calculation. By default, it is disabled.

Copyright © Raisecom Technology Co., Ltd.

8.5.8 Configuring OSPFv3 routing policy

Configuring OSPFv3 receiving policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 prefix-list** *prefix-name* **seq** *seq-number* { **deny** | **permit** } *ip-address/mask* [**ge** *min-length*] [**le** *max-length*]	(Optional) configure the address prefix list.
3	Raisecom(config)#**access-list** *acl-number*	(Optional) create an ACL and enter ACL configuration mode. When the *acl-number* ranges from 7000 to 7999, the system will enter extended IPv6 ACL configuration mode.
	Raisecom(config-acl-ipv6-advanced)#**rule** [*rule-id*] { **deny** | **permit** } { *protocol-id* | **ipv6** } { *source-ip-address/prefix-length* | **any** } { *destination-ip-address/prefix-length* | **any** } [**dscp** *dscp-value*]	(Optional) configure extended IPv6 ACL rules.
4	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
5	Raisecom(config-ospf6)#**distribute-list** { **ipv6-access-list** *acl-number* | **ipv6-prefix-list** *list-name* } **in**	Configure the filtering policy for OSPFv3 to receive OSPF intra-area, inter-area, and AS external routes.

Note

- Before configuring the OSPFv3 acceptance filtering policy, you need to ensure that the IPv6 ACL referenced by the policy has been created.
- When filtering is based on IPv6 ACL, if the ACL mode is permit, the route matching the ACL will pass, otherwise the routes will be denied.
- The IPv6 ACL can only be modified if and only if it is not referenced by any routing policy.
- Unlike IPv6 ACL, the address prefix list can be modified when it is referenced.
- If the configured prefix list does not exist, the received routes are not filtered.

Configuring OSPFv3 advertisement policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 prefix-list** *prefix-name* **seq** *seq-number* { **deny** | **permit** } *ip-address/mask* [**ge** *min-length*] [**le** *max-length*]	(Optional) configure the address prefix list.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**access-list** *acl-number*	(Optional) create an ACL and enter ACL configuration mode. When the *acl-number* ranges from 7000 to 7999, the system will enter extended IPv6 ACL configuration mode.
	Raisecom(config-acl-ipv6-advanced)#**rule** [*rule-id*] { **deny** | **permit** } { *protocol-id* | **ipv6** } { *source-ip-address/prefix-length* | **any** } { *destination-ip-address/prefix-length* | **any** } [**dscp** *dscp-value*]	(Optional) configure extended IPv6 ACL rules.
4	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
5	Raisecom(config-ospf6)#**distribute-list** { **ipv6-access-list** *acl-number* | **ipv6-prefix-list** *list-name* } **out** [**static** | **connected** | **bgp4+** | **ripng** | **ospfv3** *process-id* | **isisv6** *process-id*]	Configure a filtering policy that OSPFv3 advertises the imported routing information to the autonomous system in form of Type 5 LSA.

Note

- Before configuring the OSPF global advertisement policy, you need to ensure that the IP ACL referenced by the policy has been created.
- The IP ACL can only be modified if and only if it is not referenced by any routing policy.
- Unlike IP ACL, the address prefix list can be modified when it is referenced.
- After the global advertisement policy is configured, only imported routes can be imported into the local LSDB after matching the global advertisement policy. After the protocol advertisement policy is configured, the routes need to match the protocol advertising policy to be imported.
- After the protocol advertisement policy is configured, the imported protocol routes can be imported into the local LSDB only when they match the protocol advertisement policy. If the global advertisement policy is configured at the same time, the routes need to match the global advertisement policy to be imported.

Configuring inter-area route filtering policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 prefix-list** *prefix-name* **seq** *seq-number* { **deny** | **permit** } *ip-address/mask* [**ge** *min-length*] [**le** *max-length*]	(Optional) configure the address prefix list.
3	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-ospf6)#**area** { *area-id* | *ip-format-area-id* } **filter ipv6-prefix-list** *list-name* { **in** | **out** }	Configure the filtering rule in the egress/ingress direction of the area. Configure the rules for filtering the Summary-LSA in the ingress or egress directions of the area on the ABR.

8.5.9 Maximizing LSA metric

Increase the metric value (65535) of the link in the LSA generated by the device to inform other OSPF devices of not using this Stub device to forward data.

- After enabling the maximum metric value function of OSPF LSA packets by using the **max-metric router-lsa** command, the metric values of all non-Stub area adjacency relationships will be configured to 0xFFFF (0xFFFF is still available, and 0xFFFFFF is unavailable). The adjacency measurement value of the Stub region is not affected, and the cost of the interface is filled in according to its normal value.
- After enabling the maximum metric function of OSPF LSA packets by using the **max-metric router-lsa include-stub** command, the metric values of all adjacency relationships (including stub area adjacency relationships) are configured to 0xFFFF by the device.
- You can use the **on-startup** *time* parameter to configure the timer that lasts for the maximum value after restart. After the timer expires, the metric value will return to its original value.
- When optional parameters **summary lsa** and **external lsa** are configured, the corresponding area LSA will be refreshed according to the configured metric values.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**max-metric router-lsa** [**include-stub**] [**on-startup** *time*] [**summary-lsa** *summary-metric*] [**external-lsa** *external-metric*]	Enable maximum metric of OSPFv3 LSA packets. The metric of LSA packet in the corresponding area will be automatically configured to 0xFFFF. By default, it is disabled.

8.5.10 Configuring BFD for OSPFv3

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id* [**router-id** *router-id*]	Enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**bfd all-interfaces**	Enable global BFD. By default, global BFD is not enabled.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-router-ospf)#**exit**	Enter global configuration mode.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**ipv6 ospf bfd** [**instance-id** *instance-id*]	Enable interface BFD. By default, interface BFD is not enabled.

8.5.11 Checking configurations

Step	Command	Description
1	Raisecom#**show ipv6 ospf** [*process-id*]	Show basic information about OSPFv3.
2	Raisecom#**show ipv6 ospf** [*process-id*] **interface** [*interface-type interface-number*]	Show information about the OSPFv3 interface.
3	Raisecom#**show ipv6 ospf** [*process-id*] **neighbor** [*neighbor-id*]	Show information about OSPFv3 neighbors.
4	Raisecom#**show ipv6 ospf** [*process-id*] **route**	Show OSPFv3 routes.
5	Raisecom#**show ipv6 ospf database** { **router** | **network** | **inter-area-prefix** | **inter-area-router** | **external** | **nssa-external** | **link** | **intra-area-prefix** }	Show information about OSPFv3 link status database.
6	Raisecom#**show ipv6 ospf** [*process-id*] **asbr**	Show basic information about ASBR.
7	Raisecom#**show ipv6 ospf** [*process-id*] **topology**	Show information about the OSPFv3 topology.
8	Raisecom#**show ipv6 ospf** [*process-id*] **vlink**	Show information about OSPFv3 virtual links.

8.5.12 Maintenance

Command	Description
Raisecom#**clear ipv6 ospf** [*process-id*] **process** [**graceful**]	Restart the OSPFv3 process.
Raisecom(config-ospf6)#**ospf restart grace-period** *seconds*	Configure the graceful restart period of OSPFv3.
Raisecom(config-ospf6)#**capability restart graceful**	Configure OSPFv3 GR. OSPFv3 GR can ensure that routers running OSPFv3 forward the service normally when the master/slave switchover starts or OSPFv3 restarts.
Raisecom(config-ospf6)#**ospf restart helper** { **never** | **planned-only** }	Configure rules to enter help mode in OSPFv3 restart mode.

Copyright © Raisecom Technology Co., Ltd.

Command	Description
Raisecom(config-ospf6)#**ospf restart helper** [**planned-only**] **max-grace-period** *seconds*	Configure the maximum restart period in OSPFv3 restart help mode.

8.6 Configuring ISIS

8.6.1 Configuring ISIS basic functions

To run ISIS normally, two steps need to be done: start ISIS process and configure the name of network entity.

- Use the **router isis** command to start ISIS process.
- Use the **ip router isis** command to start ISIS process on the interface.

step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*] [**vrf** *vrf-name*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config)#**interface** *interface-type interface-number*	(Optional) enter interface configuration mode.
4	Raisecom(config-port)#**ip router isis** [*area tag*] Raisecom(config-port)#**exit**	(Optional) start an ISIS process on the interface.
5	Raisecom(config)#**router isis** [*area-tag*]	Enter ISIS configuration mode.
6	Raisecom(config-router-isis)#**net** *network-entity*	Configure the network identifier entity of ISIS routing process.

8.6.2 Configuring ISIS routing attributes

Configuring router type

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**is-type** { **level-1** | **level-1-2** | **level-2-only** }	Configure the router type. By default, it is level-1-2.
4	Raisecom(config-router-isis)#**hostname dynamic**	(Optional) enable the switching mechanism of dynamic hostname. By default, it is disabled.

Copyright © Raisecom Technology Co., Ltd.

Configuring overhead

The ISIS overhead can be configured automatically or manually. After the automatic calculation of the overhead on the interface is enabled, the ISIS will automatically calculate the overhead on the interface according to the following rules:

- When the type of overhead is configured to wide, ISIS will automatically calculate the value according to the interface rate, the formula is: overhead on the interface = reference rate/interface rate ×10, and the max value obtained is 16777214.
- When the type of overhead is configured to narrow, the interface overhead is:
  - 60 for interface rate between 1 and 10 Mbit/s
  - 50 for interface rate between 1 and 100 Mbit/s
  - 40 for interface rate between 101 and 155 Mbit/s
  - 30 for interface rate between 156 and 622 Mbit/s
  - 20 for interface rate between 623 and 2500 Mbit/s
  - 10 for other conditions

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**metric-style** { **narrow** | **transition** | **wide** } Raisecom(config-router-isis)#**exit**	Configure the type of ISIS overhead. By default, it is narrow.
4	Raisecom(config-router-isis)#**auto-metric** { **enable** | **disable** }	Enable automatic calculation of overhead on the interface. By default, it is disabled.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**isis metric** *metric* [**level-1** | **level-2**]	Configure the overload value on the interface. By default, it is 10.

Configuring reference bandwidth

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**reference-bandwidth** *bandwidth*	Configure reference rate referred to while calculating technical link overhead. By default, it is 100 Mbit/s.

Copyright © Raisecom Technology Co., Ltd.

Configuring ISIS administrative distance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**distance** *distance* [*ip-address mask-address*]	Configure the management distance of ISIS routing. By default, it is 115.

8.6.3 Configuring ISIS network

Configuring type of ISIS network

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis network point-to-point**	Configure the type of interface network to P2P. By default, it is broadcast.

Adjacencies

This configuration is only applied to Level-1-2 routers.

- If the host is Level-1-2 router, it needs to establish association with peer router in certain area (Level-1 or Level-2). Configuring an area for establishing adjacency can restrain the interface from receiving and sending the Hello packet only from that certain area.
- In the point-to-point link, the interface can only receive and send one type of Hello packet. Configuring an area for establishing adjacency can reduce the processing time between routers and save bandwidth.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis circuit-type** { **level-1** | **level-1-2** | **level-2-only** }	Configure an area for establishing interface adjacency. By default, it is Level-1-2.

Configuring DIS priority

The Designated Intermedia System (DIS) election of the ISIS is preemptive and predictable. There is not backup DIS in the ISIS. Therefore, when one DIS does not work, another DIS will be elected. The rules for electing the DIS are as below:

Copyright © Raisecom Technology Co., Ltd.

- The router with highest DIS election priority will be elected. If all routers have the same priority, the router with biggest MAC address will be elected.
- The DIS in Level-1 and Level-2 are elected respectively but the result may be not the same IS.
- The interval between sending Hello packet by DIS is 1/3 times of that by common routers, which can ensure that the invalid DIS be detected in no time.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis priority** *priority* [**level-1** | **level-2**]	Configure the DIS priority on the interface in different areas. By default, it is 64.

8.6.4 Optimizing ISIS network

Configuring ISIS packet timer

The invalid number of Hello packet is decided by the Hold-down time. If the router cannot receive Hello packet sent by the peer router within the Hold-down time, the peer router can be considered invalid. The Hold-down time is configured based on interface and different router in the same area can set different the Hold-down time.

By changing the interval for sending Hello packets of ISIS or the invalid number of Hello packet, you can adjust the Hold-down time.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis hello-interval** *seconds* [**level-1** | **level-2**]	Configure the interval between sending Hello packets on the interface of different areas. By default, it is 10s.
4	Raisecom(config-port)#**isis hello-multiplier** *number* [**level-1** | **level-2**]	Configure the number of invalid ISIS neighbor Hello packets on the interface of different areas.
5	Raisecom(config-port)#**isis csnp-interval** *seconds* [**level-1** | **level-2**]	Configure the interval between sending CSNP packets on the interface of different areas in the broadcast network. By default, it is 10s.

Copyright © Raisecom Technology Co., Ltd.

Configuring LSP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis lsp-interval** *milliseconds*	Configure the interval between sending LSP packets. By default, it is 33ms.
4	Raisecom(config-port)#**isis retransmit-interval** *seconds* Raisecom(config-port)#**exit**	Configure retransmission interval between sending LSP packets on the point-to-point link. By default, it is 5s.
5	Raisecom(config)#**router isis** [*area-tag*] Raisecom(config-router-isis)#**lsp-gen-interval** *seconds* [**level-1** | **level-2**]	Configure the interval between generating LSP. By default, it is 5s.
6	Raisecom(config-router-isis)#**max-lsp-lifetime** *seconds* [**level-1** | **level-2**]	Configure the longest TTL of the LSP generated. By default, it is 1200s.
7	Raisecom(config-router-isis)#**lsp-refresh-interval** *seconds* [**level-1** | **level-2**]	Configure the refresh time of LSP. By default, it is 900s.
8	Raisecom(config-router-isis)#**ignore-lsp-errors**	Enable the function of ignoring the checkout for LSP. By default, it is disabled.

Configure ISIS passive interface

If you do not wish the ISIS routing information to be obtained by the router in a network, you can configure the interface to ISIS passive interface to prevent it from sending ISIS packets.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis passive**	Enable the passive function on ISIS interface. By default, it is disabled.

Configure Hello packet padding

Hello packet padding refers to padding Hello packet with MTU field, thus notifying peer and local interface of the MTU.

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**hello padding**	Enable Hello Packet padding. By default, all types of interface are padded with standard Hello packets.

8.6.5 Configure ISIS authentication

Configuring ISIS interface authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis password** { **clear** *password* | **md5** *password* } [**level-1** | **level-2**]	Configure the ISIS authentication mode and password of the interface.

Configuring ISIS area authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**area-password** { **clear** *password* | **md5** *password* } [**authenticate snp** { **send-only** | **validate** }]	Configure Level-1 area authentication.
4	Raisecom(config-router-isis)#**domain-password** { **clear** *password* | **md5** *password* } [**authenticate snp** { **send-only** | **validate** }]	Configure Level-2 area authentication.

8.6.6 Controlling ISIS routing information

Configuring ISIS redistributed routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-router-isis)#**redistribute** { **connected** | **static** | **rip** | **ospf** *process-id* | **isis** *area-tag* | **bgp** } [**level-1** | **level-2** | **level-1-2**] [**metric** *metric*] [**metric-type** { **external** | **internal** }]	Configure protocol route redistributed policy. By default, ISIS does not redistribute other protocol routes. If you do not specify the area when it redistributes routes, it will redistribute routes to Level-2 by default.
4	Raisecom(config-router-isis)#**redistribute isis ip level-2 into level-1**	Configure ISIS route redistributed policy among areas. By default, the routing information in level-2 will not be distributed to Level-1.

Advertising default route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**default-information originate**	Advertise Level-2 default routes.

Configuring ISIS route summarization

Route aggregation can not only reduce the scale of routing table but also shrink the size of LSP packet generated by the local router and reduce the scale of LSDB.

- The summary route can be the route found by the ISIS and the route redistributed externally.
- The overload of summary route takes the minimum overload among all the routes aggregated.
- The router only aggregates the route generated in the local LSP.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**summary-address** *ip-address mask-address* [**level-1** | **level-2** | **level-2-only**]	Configure route summarization among areas. By default, there is no route summarization. The overload while configuring route summarization is the maximum Metric in the LSA. And the route summarization will be advertised.

Copyright © Raisecom Technology Co., Ltd.

Configuring ISIS equal-cost multi-path load balancing

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**maximum load-balancing** *number*	Configure the maximum number of ISIS equal-cost multi-path load balancing paths.

Configuring ISIS route filtering

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*] [**vrf** *vrf-name*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *map-name* } **out** [**connected** | **static** | **rip** | **ospf** *process-id* | **isis** *area-tag* | **bgp**]	Configure route filtering rules and filter the routes which are to be advertised. By default, route filtering is disabled.
4	Raisecom(config-router-isis)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *map-name* } **in**	Configure the route filtering rules to filter the receiving rules. By default, route filtering is disabled.

8.6.7 Configuring ISIS BFD

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis bfd enable**	Enable interface ISIS BFD. By default, it is disabled.
4	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
5	Raisecom(config-router-isis)#**bfd all-interfaces**	Enable ISIS BFD on all interfaces. By default, it is disabled.

Copyright © Raisecom Technology Co., Ltd.

8.6.8 Configuring ISIS GR

Configure ISIS graceful restart, that is, the switchover ensures no service interruption while the RAX721 is rebooted.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**graceful-restart**	Enable ISIS graceful restart. By default, it is disabled.
4	Raisecom(config-router-isis)#**graceful-restart interval** *seconds*	Enable the interval of ISIS graceful restart. By default, it is 300s.
5	Raisecom(config-router-isis)#**graceful-restart sa enable**	Enable ISIS GR to restrain the neighbor device from advertising routes. By default, it is enabled.

8.6.9 Configuring ISIS TE

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**mpls traffic-eng** { **level-1** | **level-2** }	Enable MPLS-TE and configure the MPLS-TE level. By default, it is disabled.
4	Raisecom(config-router-isis)#**mpls traffic-eng router-id** *router-id*	Configure the Router ID of the MPLS-TE router. By default, the ISIS Router ID is used.

8.6.10 Checking configurations

Step	Command	Description
1	Raisecom#**show isis interface** [**detail**]	Show ISIS interface.
2	Raisecom#**show isis neighbor** [*system-id* | **detail**]	Show ISIS neighbors.
3	Raisecom#**show isis hostname**	Show the mapping between host name and system ID.
4	Raisecom#**show isis route**	Show ISIS IPv4 route.
5	Raisecom#**show isis topology** [**level-1** | **level-2**]	Show ISIS topology.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom#**show isis database** [*lsp-id* | **detail**]	Show database about ISIS link status.
7	Raisecom#**show isis summary**	Show basic configurations about ISIS.
8	Raisecom#**show isis mpls traffic-eng advertisements**	Show interface advertised by the router.

8.6.11 Maintenance

Command	Description
Raisecom#**clear isis process** *process-id* [**graceful-restart**]	Clear ISIS.
Raisecom#**clear isis neighbor** [*system-id*]	Clear ISIS neighbors.

8.7 Configuring ISISv6

8.7.1 Configuring ISISv6 basic functions

The normal operation of ISIS requires two steps: starting the ISIS process and configuring the network entity name.

- Use the **router isis** command to start the ISIS process.
- Use the **ipv6 router isis** command to start the ISIS process on the interface.

Starting ISIS process

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*] [**vrf** *vrf-name*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
4	Raisecom(config-port)#**ipv6 router isis** [*area tag*] Raisecom(config-port)#**exit**	Enable ISISv6 capabilities on the interface. Establish ISIS neighbor relationship through the interface.
5	Raisecom(config)#**router isis** [*area-tag*]	Enter ISIS configuration mode.
6	Raisecom(config-router-isis)#**net** *network-entity*	Configure the network ID entity of the ISIS routing process.

Copyright © Raisecom Technology Co., Ltd.

Configuring the level

The device establishes neighbor relationship according to the level and maintains the link status database.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*] [**vrf** *vrf-name*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**is-type** { **level-1** | **level-1-2** | **level-2-only** }	Configure the type of the ISIS router. By default, the type of the ISIS router is level-1-2**.**

Enabling IPv6 multi-topology

- If IPv6 multi-topology is enabled, the system will maintain two independent routing tables, namely IPv4 routing table and IPv6 routing table. If the network is a mixed topology of IPv4 and IPv6, two topology trees of IPv4 and IPv6 will be generated and the IPv4 and IPv6 routes will be calculated respectively.
- If IPv6 multi-topology is disabled, the system will recalculate the topology tree and routes. You can view the topology information through the **show isis topology** command and you can view the calculated routing information through the **show isis route** command.

Please perform the following configuration on the device.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*] [**vrf** *vrf-name*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**ipv6 multi-topology**	Enable IPv6 route multi-topology. By default, it is disabled.

8.7.2 Configuring ISISv6 authentication

Configuring interface authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis password** { **clear** *password* | **md5** *password* } [**level-1** | **level-2**]	Configure the ISIS authentication mode and password of the interface.

Copyright © Raisecom Technology Co., Ltd.

Configuring area authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**area-password** { **clear** *password* | **md5** *password* } [**authenticate snp** { **send-only** | **validate** }]	Configure Level-1 area authentication.
4	Raisecom(config-router-isis)#**domain-password** { **clear** *password* | **md5** *password* } [**authenticate snp** { **send-only** | **validate** }]	Configure Level-2 area authentication.

8.7.3 Configuring ISISv6 route selection parameters

Configuring cost value

The ISIS cost can be calculated automatically or manually configured. After automatic cost calculation is enabled on the interface, the interface cost is calculated automatically according to the following rules:

When the cost type is wide, ISIS will automatically calculate the cost based on the bandwidth of the interface. The formula: interface cost = bandwidth reference value/interface bandwidth *10, the maximum value of the calculated cost is 16777214.

When the cost value type is narrow,

- if the interface bandwidth is 1–10 Mbit/s, the interface cost is 60.
- if the interface bandwidth is 11–100 Mbit/s, the interface cost is 50.
- if the interface bandwidth is 101–155 Mbit/s, the interface cost is 40.
- if the interface bandwidth is 156–622 Mbit/s, the interface cost is 30.
- if the interface bandwidth is 623–2500 Mbit/s, the interface cost is 20.
- In other cases, the interface cost is 10.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**metric-style** { **narrow** | **transition** | **wide** } Raisecom(config-router-isis)#**exit**	Configure the type of ISIS cost. By default, the cost type is narrow.
4	Raisecom(config-router-isis)#**auto-metric** { **enable** | **disable** }	Enable automatic calculation of interface cost. By default, it is not enabled.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**ipv6 isis metric** *metric-value* [**level-1** | **level-2**]	Configure the link cost of the ISISv6 interface. By default, the cost of the ISIS interface is 10.

Copyright © Raisecom Technology Co., Ltd.

Configuring administrative distance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**ipv6 distance** *distance* [*ip-address mask-address*]	Configure the administrative distance of ISIS routes. By default, the administrative distance of ISIS routes is 115.

8.7.4 Controlling ISISv6 routing information

Advertising default routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**ipv6 default-information originate**	Advertise Level-2 default routes.

Redistributing routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**ipv6 redistribute** { **connected** | **static** | **ripng** | **ospfv3** *process-id* | **isisv6** *area-tag* | **bgp4+** } [**level-1** | **level-2** | **level-1-2**] [**metric** *metric-value*] [**metric-type** { **external** | **internal** }] [**route-map** *map-name*]	Redistribute the routing information about other IPv6 routing protocols and notify related areas. By default, ISIS does not redistribute other protocol routes. If no area is specified during redistribution, the routes will be redistributed to Level-2 by default. Metric-type is internal by default. If no metric is specified when redistributing a route, the metric value of the original route will be inherited.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-router-isis)#**ipv6 redistribute limit** *max-number* [**level-1** | **level-1-2** | **level-2**]	Configure the limit on the number of IPv6 routes redistributed from other routing protocols. By default, the number of external routes is not limited. When this number limit is configured, the default value of Level is level-2. **Note** If level-1 is configured first, and then the same number of level-2 is configured, the **show running-config** command displays level-1-2.
5	Raisecom(config-router-isis)#**redistribute isis ipv6 level-2 into level-1**	Redistribute routes in Level-2 area to Level-1 area. By default, the routing information in Level-2 area is not advertised to the Level-1 area.

Configuring ISISv6 route summarization

Route aggregation can not only reduce the size of routing tables, but also reduce the size of LSP packets and the size of LSDB generated by this router.

- The route being aggregated may be a route discovered by ISIS or a redistributed external route.
- The cost of the summary route takes the minimum value of the cost of all summary routes.
- The router only aggregates the routes in the locally generated LSP.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**ipv6 summary-prefix** *ipv6-address/m* [**level-1** | **level-2** | **level-2-only**]	Configure IPv6 route summarization. By default, there is no summary route. If you configure an aggregate route without specifying a domain, only Level-2 routes are aggregated.

Configuring ISISv6 route filtering

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*] [**vrf** *vrf-name*]	Start an ISIS process and enter ISIS configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-router-isis)#**ipv6 distribute-list** { **ipv6-access-list** *acl-number* | **ipv6-prefix-list** *list-name* | **route-map** *map-name* } **out** [**connected** | **static** | **ripng** | **ospfv3** *process-id* | **isisv6** *area-tag* | **bgp4+**]	Configure IPv6 route filtering rules to filter the IPv6 routes to be advertised. By default, it is not filtered.
4	Raisecom(config-router-isis)#**ipv6 distribute-list** { **ipv6-access-list** *acl-number* | **ipv6-prefix-list** *list-name* | **route-map** *map-name* } **in**	Configure IPv6 route filtering rules to filter the received IPv6 routes. By default, it is not filtered.

8.7.5 Configuring ISISv6 load balancing

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**ipv6 maximum load-balancing** *number*	Configure the maximum number of ISIS ECMPs.

8.7.6 Configuring ISISv6 BFD

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis ipv6 bfd enable** Raisecom(config-port)#**exit**	Enable global ISISv6 BFD. By default, it is disabled.
4	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
5	Raisecom(config-router-isis)#**ipv6 bfd all-interfaces**	Enable ISIS BFD on all interfaces. By default, it is disabled.

8.7.7 Checking configurations

Step	Command	Description
1	Raisecom#**show isis interface** [**detail**] [*interface-number*]	Show information about the ISIS interface.
2	Raisecom#**show isis neighbor** [*system-id* | **detail**]	Show ISIS neighbor information.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom#**show isis hostname**	Show the mapping table between the host name and the system ID.
4	Raisecom#**show isis topology** [**level-1** | **level-2**]	Show information about the ISIS topology.
5	Raisecom#**show isis database** [**local**] [**level-1** | **level-2**] [*lsp-id*] [**detail**]	Show the ISIS link status database.
6	Raisecom#**show isis summary**	Show ISIS basic configurations.

8.7.8 Maintenance

Command	Description
Raisecom#**clear isis process** *process-id* [**graceful-restart**]	Clear ISISv6 information.
Raisecom#**clear isis neighbor** [*system-id*]	Clear ISISv6 neighbor information.

8.8 Configuring BGP

8.8.1 Configuring BGP basic functions

Enabling BGP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enable BGP and create a BGP instance. Enter BGP configuration mode.
3	Raisecom(config-router)#**bgp router-id** *router-id*	(Optional) configure the BGP Router ID. By default, the BGP router ID should be the same as the global router ID.

Configuring BGP peer

BGP uses the TCP connection. Therefore, when configuring BGP, you need to configure the IP address of the BGP neighbor. The BGP neighbor can be non-adjacent routers. You can establish a BGP neighborship. To enhance stability of the BGP connection, we recommend using the loopback interface address to establish the connection.

Specified IP addresses of BGP neighbors are divided into 2 types:

- Interface IP address of the directly-connected BGP neighbor

Copyright © Raisecom Technology Co., Ltd.

- Loopback interface address of the BGP neighbor, where the route is available. In this mode, you need to configure the route update source to ensure that the BGP neighbor is established properly.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**neighbor** *ip-address* **remote-as** *as-id*	Create a BGP neighbor and specify the AS ID of the BGP neighbor. • IBGP peer: configure the peer AS ID to be the same as the local AS ID. • EBGP peer: configure the peer AS ID to be different from the local AS ID. By default, there is no BGP neighbor.
4	Raisecom(config-router)#**neighbor** *ip-address* **activate**	Enable the BGP neighbor to exchange the specified address family route. By default, enable the BGP neighbor to exchange the IPv4 unicast address family route only.
5	Raisecom(config-router)#**neighbor** *ip-address1* **update-source** *ip-address2* Raisecom(config-router)#**neighbor** *ip-address* **update-source** *interface-type interface-number*	Configure using the specified source IP address or local source interface when establishing a BGP connection. Local source interfaces include physical layer interfaces, VLAN interfaces, loopback interfaces, and sub-interfaces. If one of the two ends of the connection is configured with the correct update source, the BGP connection can be successfully established, but there may be a problem that the connection establishment time is too long. To ensure the stability of the connection establishment at both ends, it is recommended that both ends of the peer be configured to update the source address at the same time.
6	Raisecom(config-router)#**neighbor** *ip-address* **weight** *weight*	(Optional) configure the weight of the routes learned from the BGP peer. By default, it is 0.
7	Raisecom(config-router)#**neighbor** *ip-address* **default-originate** [**route-map** *route-map-name*]	(Optional) enable the feature of sending the default route to the BGP neighbor. By default, do not send the default route to the BGP neighbor.
8	Raisecom(config-router)#**neighbor** *ip-address* **description** *string*	(Optional) configure descriptions of the BGP neighbor. By default, there is no description of the BGP neighbor.
9	Raisecom(config-router)#**neighbor** *ip-address* **next-hop-self**	(Optional) configure the router to modify the next-hop address of the route to the IP address of the Tx end, when the router releases the route to the BGP neighbor. By default, when the router releases the route to the BGP neighbor, the next-hop address of the route is identical to the next-hop IP address of the route in the local BGP routing table.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
10	Raisecom(config-router)#**bgp log-neighbor-changes**	(Optional) enable the log which is used to inform the BGP neighbor of state change. By default, it is enabled.
11	Raisecom(config-router)#**neighbor** *ip-address* **shutdown**	(Optional) disallow the RAX721 to establish the BGP connection with the specified BGP neighbor. By default, establishing the BGP connection with the BGP neighbor is allowed.
12	Raisecom(config-router)#**neighbor** *ip-address* **ebgp-multihop** [*ttl*]	(Optional) allow the RAX721 to establish the EBGP connection with BGP neighbors in the indirectly-connected network. In addition, specify the maximum hops allowable for the specified EBGP connection. By default, only physically directly-connected BGP neighbors can establish the EBGP connection.
13	Raisecom(config-router)#**bgp redistribute-internal**	(Optional) allow the device to redistribute the routing information, learned from the IBGP neighbor, to the IGP. By default, redistributing the IBGP route to the IGP is disabled.
14	Raisecom(config-router)#**bgp enforce-first-as**	For the route received from the EBGP peer, the first AS number in the as-patch must be the same as the AS where the EBGP peer is located.

Configuring BGP peer (IPv4 address family based on VPN instance)

This configuration applies to the MPLS L3VPN.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enable BGP, create a BGP instance, and enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**neighbor** *ip-address* **remote-as** *as-id*	Create the MP-BGP peer and specify the peer AS ID.
5	Raisecom(config-router-af)#**neighbor** *ip-address* **activate**	Enable the exchange of routing information of the specified IP address family between BGP peers.
6	Raisecom(config-router-af)#**neighbor** *ip-address1* **update-source** *ipv6-address2*	Use the specified source IP address or local source interface when establishing a BGP connection. Local source interfaces include physical layer interfaces, VLAN

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config-router-af)#**neighbor** *ip-address* **update-source** *interface-type interface-number*	interfaces, loopback interfaces, and sub-interfaces. If one of the two ends of the connection is configured with the correct update source, the BGP connection can be successfully established, but there may be a problem that the connection establishment takes too long. To ensure the stability of the connection establishment at both ends, we recommend configuring both ends of the peer with the update source address.
7	Raisecom(config-router-af)#**neighbor** *ip-address* **weight** *weight*	(Optional) configure the weight of routes learned from BGP peers. By default, the weight of routes learned from BGP peers is 0.
8	Raisecom(config-router-af)#**neighbor** *ip-address* **default-originate** [**route-map** *route-map-name*]	(Optional) enable the function of sending the default route to the peer. By default, no default route is sent to the peer.
9	Raisecom(config-router-af)#**neighbor** *ip-address* **next-hop-self**	(Optional) configure the router to modify the next hop address of the route to its own IP address when advertising the route to the peer. By default, when the router advertises routes to IBGP peers, the next-hop IP address of the route is the same as the next-hop IP address of the route in the local BGP routing table.
10	Raisecom(config-router-af)#**neighbor** *ip-address* **ebgp-multihop** [*ttl*]	(Optional) configure the peers on the non-directly connected network to establish EBGP connections, and specify the maximum number of hops allowed for EBGP connections. By default, only physically directly-connected peers are allowed to establish EBGP connections.
11	Raisecom(config-router-af)#**bgp log-neighbor-changes**	(Optional) enable logging for prompting the status change of BGP peers. By default, it is enabled.
12	Raisecom(config-router-af)#**bgp redistribute-internal**	(Optional) re-advertise the routing information learned from IBGP peers to the IGP. By default, it is prohibited to redistribute IBGP routes to IGP.
13	Raisecom(config-router-af)#**neighbor** *ip-address* **shutdown**	(Optional) prohibit the establishment of BGP connection with the specified peer. By default, BGP connections with BGP peers are allowed.
14	Raisecom(config-router-af)#**neighbor** *ip-address* **description** *string*	(Optional) configure description of the BGP peer. By default, there is no description for the BGP peer.

Configuring BGP peer (VPNv4)

The configuration is applicable to the MPLS L3VPN.

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**router bgp** *as-id*	Enable BGP, create a BGP instance, and enter BGP configuration mode.
3	Raisecom(config-router)#**neighbor** *ip-address* **remote-as** *as-id*	Create an MP-BGP peer and specify the AS ID of the peer.
4	Raisecom(config-router)#**address-family vpnv4**	Enter BGP VPNv4 address family configuration mode.
5	Raisecom(config-router-af)#**neighbor** *ip-address* **activate**	Enable the function of exchanging routing information of the specified VPNv4 address family between BGP peers.

Configuring BGP peer (IPv4 unicast label address family)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enable BGP, create a BGP instance, and enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the IPv4 unicast address family configuration mode.
5	Raisecom(config-router-af)#**neighbor** *ip-address* **activate**	Enable the exchange of routing information of the specified IP address family between BGP peers.
6	Raisecom(config-router-af)#**neighbor** *ip-address1* **update-source** *ipv6-address2* Raisecom(config-router-af)#**neighbor** *ip-address* **update-source** *interface-type interface-number*	(Optional) configure the router to modify the next hop address of the route to the sender's own IP address when it advertises routes to peers. By default, when the router advertises routes to IBGP peers, the next hop IP address of the route is the same as the next hop IP address of the route in the local BGP routing table.
7	Raisecom(config-router-af)#**neighbor** *ip-address* **weight** *weight*	(Optional) configure the device not to change the next hop when advertising routes to IBGP peers.

8.8.2 Configuring BGP redistributed routes

BGP redistributed routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**network** *ip-address* [*mask-address*] [**route-map** *route-map-name*]	Inject static routes into the BGP routing table and advertise them to other ASs or local AS peers.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-router)#**redistribute-rib labeled-unicast** [**route-map** *route-map-name*]	Redistribute the active label route in the address family of the public network label to the unicast routing table of the public network.

BGP redistributed routes (VPN-based IPv4)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**network** *ip-address* [*mask-address*] [**route-map** *route-map-name*]	Inject static routes into the BGP routing table and advertise them to other ASs or local AS peers.

BGP redistributed routes (IPv4 unicast label address family)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router-af)#**address-family ipv4 labeled-unicast**	Enter the IPv4 unicast label address family configuration mode.
4	Raisecom(config-router-af)#**network** *ip-address* [*mask-address*] [**route-map** *route-map-name*]	Configure the local network route advertised by BGP.

8.8.3 Configuring BGP to redistribute routes

Redistributing default route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**default-information originate**	Configure the BGP to redistribute the default route.

Copyright © Raisecom Technology Co., Ltd.

Redistributing default route (IPv4 based on VPN instance)

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router bgp as-id`	Enter BGP configuration mode.
3	`Raisecom(config-router)#address-family ipv4 vrf vrf-name`	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	`Raisecom(config-router-af)#default-information originate`	Configure the BGP to redistribute the default route.

Configuring BGP to redistribute IGP routes

BGP cannot discover routes by itself, so it is necessary to redistribute routes of other protocols (such as IGP or static routes) into the BGP routing table and advertise these routes to other ASs or local AS peers.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router bgp as-id`	Enter BGP configuration mode.
3	`Raisecom(config-router)#redistribute { connected | static | rip | ospf process-id | isis process-id } [ metric metric ] [ route-map map ]`	Configure BGP to redistribute routes of other protocols into the BGP routing table through re-advertising.

Configuring BGP to redistribute IGP routes (IPv4 based on VPN instance)

BGP cannot discover routes by itself, so it is necessary to redistribute routes of other protocols (such as IGP or static routes) into the BGP routing table and advertise these routes to other ASs or local AS peers.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router bgp as-id`	Enter BGP configuration mode.
3	`Raisecom(config-router)#address-family ipv4 vrf vrf-name`	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	`Raisecom(config-router)#redistribute { connected | static | rip | ospf process-id | isis process-id } [ metric metric ] [ route-map map ]`	Configure BGP to redistribute routes of other protocols through re-advertising.

Copyright © Raisecom Technology Co., Ltd.

Configuring BGP to redistribute IGP routes (IPv4 unicast label address family)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 labeled-unicast**	Enter the IPv4 unicast label address family configuration mode.
4	Raisecom(config-router-af)#**redistribute** { **connected** | **static** | **rip** | **ospf** *process-id* | **isis** *process-id* } [**metric** *metric*] [**route-map** *map*]	Configure BGP to redistribute routes of other protocols.

8.8.4 Configuring BGP routing attributes

BGP routing attributes are a set of parameters advertised together with routing information. The route attribute is information that further describes a specific route, so that the route receiver can filter and select the route based on the route attribute value.

Configuring BGP administrative distance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**distance bgp ebgp** *distance1* **ibgp** *distance2* **local** *distance3*	Configure the administrative distance of the BGP route. • The administrative distance of external routes (routes learned through the EBGP) is 20 by default. • The administrative distance of internal routes (routes learned through the IBGP) is 200 by default. • The administrative distance of local routes (BGP routes redistributed through the aggregation command) is 200 by default.

Configuring BGP administrative distance (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the IPv4 address family configuration mode of the BGP VPN instance.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-router-af)#**distance bgp ebgp** *distance1* **ibgp** *distance2* **local** *distance3*	Configure the administrative distance of BGP routes. By default: • The administrative distance of external routes (routes learned through EBGP) is 20. • The administrative distance of internal routes (routes learned through IBGP) is 200. • The administrative distance of local routes (routes redistributed into BGP through aggregation commands) is 200.

Configuring BGP path selection policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**bgp deterministic-med**	(Optional) configure the BGP not to consider the receiving sequence when selecting the route. By default, the BGP considers the receiving sequence when selecting the route.
4	Raisecom(config-router)#**bgp always-compare-med**	Configure the BGP to compare the MED for all paths.
5	Raisecom(config-router)#**bgp bestpath compare-routerid**	Configure BGP to compare the EBGP Router-ID for selecting the best path. By default, BGP prefers the earliest received EBGP route, without comparing the EBGP Router-ID.
6	Raisecom(config-router)#**bgp bestpath as-path ignore**	Configure the BGP to ignore the AS-PATH property when selecting the optimum path.

Configuring BGP path selection policy (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the IPv4 address family configuration mode of the BGP VPN instance.
3	Raisecom(config-router-af)#**bgp deterministic-med**	(Optional) configure BGP route preference without considering the route receiving order. By default, BGP route preference considers the route receiving order.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-router-af)#**bgp always-compare-med**	Configure BGP to compare MED for all paths.
5	Raisecom(config-router-af)#**bgp bestpath compare-routerid**	Configure BGP to compare the EBGP Router-ID for selecting the best path. By default, BGP prefers the earliest received EBGP route, without comparing the EBGP Router-ID.
6	Raisecom(config-router-af)#**bgp bestpath as-path ignore**	Configure the BGP to ignore the AS-PATH attribute when selecting the optimal path.

Configuring default MED of BGP default route

The Multi Exit Discriminator (MED) attribute is equivalent to the metric used by IGP. It is used to determine the best route for traffic to enter the AS. When a BGP router obtains multiple routes through different EBGP peers, the destination addresses of these routes are the same, but the next-hop addresses are different. Under the same conditions, the router will choose the route with the smaller MED as the best route.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**default-metric** *metric-value*	Configure the default MED of the local BGP router. This configuration only takes effect on redistributed routes and summary routes.

Configuring BGP and IGP route synchronization

After BGP synchronization is enabled,

- The BGP route can participate into selection if it meets the following requirements. Then, if it is selected, the RM is applied to the routing table.
  - In the RM, the BGP route learned through IBGP can exactly match the route learned through IGP.
  - The administrative distance of the IGP route is shorter than the administrative distance of the BGP route.
- The BGP route status will flap and it may participate into selection or not, if it meets the following requirements:
  - The BGP route learned through IBGP can exactly match the route learned through IGP.
  - The administrative distance of the IGP route is greater than the administrative distance of the BGP route.

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**synchronization**	Enable BGP and IGP route synchronization. By default, it is disabled.

Configuring route dampening

Route flapping is one route instability form. Route flapping refers that a route appears and then disappears alternatively. Route dampening can be used to overcome route flapping.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**bgp dampening** *half-life reuse suppress max-suppress-time*	Enable BGP route dampening or modify the BGP route dampening parameter. By default, BGP route dampening is disabled. After BGP dampening is enabled, the default values of all parameters are shown as below. • Half-life: 15min • Reuse value: 750 • Dampening threshold: 2000 • Maximum suppress time: 60min

Configuring BGP community attribute

The community attribute is an optional delivery attribute of BGP routes and can be added to the prefix of each route. If a route contains a community attribute, it indicates that the route is a member of a routing community with routes of one or more the same characteristics. According to these features, the configuration of the routing policy can be greatly simplified, and the capability of the routing policy is also enhanced.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
3	Raisecom(config-router)#**neighbor** *ip-address* **send-community** [**standard** | **extended**]	Enable the BGP-enabled device to send standard community attribute to the peer.

Copyright © Raisecom Technology Co., Ltd.

Configuring BGP community attribute (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**neighbor** *ip-address* **send-community standard**	Enable BGP to send standard group attributes to the peer.

8.8.5 Configuring BGP network

Configuring RR

Prefix notification rules of the Router Reflector (RR) are shown as below:

- Rule 1: the RR just notifies or reflects the optimum path to which it returns.
- Rule 2: the RR always notifies the prefix to the BGP neighbor.
- Rule 3: when notifying the prefix, the RR client follows the common IBGP loopback prevention rule.
- Rule 4: to notify the IBGP neighbor, client, or non-client of the prefix, follow rules 5, 6, and 7.
- Rule 5: the RR will notify all its clients and non-clients of the prefix, which is learned from the external BGP neighbor.
- Rule 6: the RR will notify all its clients of the prefix, which reaches the RR through a non-client IBGP neighbor.
- Rule 7: the RR will notify other clients and non-clients of the route, if the prefix reaches the RR through a client.

In some networks, clients of the RR have established a full-connection. They can exchange routing information directly without using route reflection. In this case, you can use the **no bgp client-to-client reflection** command to disable route reflection among clients of the RR.
To enhance network reliability and prevent faults from occurring at a node, you need to configure one or more RR in a cluster. You can configure the identical cluster ID for all RRs in the cluster to identify the cluster. This helps avoid the loopback.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**neighbor** *ip-address* **route-reflector-client**	Configure the device to the RR and set the specified neighbor as the client of the RR. By default, route reflection is disabled.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-router)#**bgp client-to-client reflection**	Enable route reflection among clients of the RR. By default, route reflection among clients of the RR is enabled.
5	Raisecom(config-router)#**bgp cluster-id** *cluster-id*	Configure the cluster ID of the RR. By default, it is the Router ID.
6	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter IPv4 address family configuration mode of the BGP VPN instance.
	Raisecom(config-router)#**address-family vpnv4**	Enter BGP VPNv4 address family configuration mode.
	Raisecom(config-router)#**address-family ipv4 labeled-unicast**	Enter IPv4 unicast label address family configuration mode.
7	Raisecom(config-router-af)#**neighbor** *ip-address* **route-reflector-client**	Configure the local device as the reflector, and configure the specified peer as the client of the route reflector. By default, the route reflector is disabled.

Configuring route reflector (VPNv4)

Step	Command	Description
1	Raisecom#**config**	Enter IPv4 address family configuration mode of the BGP VPN instance.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP VPNv4 address family configuration mode.
3	Raisecom(config-router)#**address-family vpnv4**	Enter IPv4 unicast label address family configuration mode.
4	Raisecom(config-router-af)#**neighbor** *ip-address* **route-reflector-client**	Configure the local device as the route reflector, and specify the peer as the client of the route reflector. By default, route reflector is disabled.

Configuring BGP default local priority

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**bgp default local-preference** *priority*	Configure BGP default local priority. By default, it is 100.

Copyright © Raisecom Technology Co., Ltd.

Configuring BGP timer

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**bgp scan-time** *time*	Configure the interval for scanning the BGP routing table. By default, it is 60s.
4	Raisecom(config-router)#**timers bgp** *keep-alive-time hold-time*	Configure the KeepAlive and hold time of the global BGP connection. By default, the KeepAlive and hold time of the global BGP connection are configured to 60s and 180s respectively.
5	Raisecom(config-router)#**neighbor** *ip-address* **timers** *keep-alive-time hold-time*	Configure the KeepAlive and hold time of the neighbor. By default, the KeepAlive and hold time of the neighbor are identical to the ones of the global BGP connection.

Configuring route selection delay

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**route-select delay** *time*	Enable route selection delay. By default, it is disabled.
4	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Configure the KeepAlive and hold time of the global BGP connection. By default, the KeepAlive and hold time of the global BGP connection are configured to 60s and 180s respectively.
5	Raisecom(config-router)#**address-family vpnv4**	Configure the KeepAlive and hold time of the neighbor. By default, the KeepAlive and hold time of the neighbor are identical to the ones of the global BGP connection.

Configuring BGP route summarization

At present, the RAX721 supports BGP manual aggregation. Manual aggregation is only valid for existing routes in the BGP local routing table. If there is no route, whose mask size is greater than 16 bytes, in the BGP routing table, the BGP will not release the summary route even you use the aggregate 10.1.1.1 255.255.0.0 command to aggregate the route.

The summary route cannot be set to the default route (0.0.0.0/0).

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**aggregate-address** *ip-address mask-address*	Configure BGP route summarization and release the summary route and detail route.
4	Raisecom(config-router)#**aggregate-address** *ip-address mask-address* **summary-only**	Configure BGP route summarization, release the summary route only and dampens the detail route.
5	Raisecom(config-router)#**aggregate-address** *ip-address mask-address* **as-set**	Configure BGP route summarization and set the AS_SET option. The generated summary route includes all AS IDs in the AS_PATH and takes them as an AS_SET to prevent the route loop.

Configuring BGP route summarization (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**aggregate-address** *ip-address mask-address*	Configure BGP route summarization and advertise summary routes and detailed routes.
5	Raisecom(config-router-af)#**aggregate-address** *ip-address mask-address* **summary-only**	Configure BGP route summarization. Advertise summary routes but suppress detailed routes.
6	Raisecom(config-router-af)#**aggregate-address** *ip-address mask-address* **as-set**	Configure BGP route summarization and configure the AS_SET option. The generated summary route includes all AS IDs in the AS_PATH and will be considered as an AS_SET to prevent loops.

Configuring BGP route filtering

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip as-path access-list** *access-list-number* { **permit** | **deny** } *regexp*	Configure the filter of the AS_PATH list.
3	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-router)#**neighbor** *ip-address* **filter-list** *access-list-number* { **in** | **out** }	Configure the BGP route filtering policy based on AS_PATH list. By default, it is disabled. It receives all route updates from the peer.
5	Raisecom(config-router)#**neighbor** *ip-address* **route-map** *map-name* { **in** | **out** }	Apply the routing policy to the specified neighbor to filter or release the route.
6	Raisecom(config-router)#**neighbor** *ip-address* **prefix-list** *prefix-list-name* { **in** | **out** }	Configure the specified neighbor to filter received or advertised routes based on IP prefix-list.

Configuring BGP route filtering (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip as-path access-list** *access-list-number* { **permit** | **deny** } *regexp*	Configure the filter of AS path list.
3	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
4	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter IPv4 address family configuration mode of the BGP VPN instance.
5	Raisecom(config-router-af)#**neighbor** *ip-address* **filter-list** *access-list-number* { **in** | **out** }	Configure the BGP route filtering policy based on AS path list.
6	Raisecom(config-router-af)#**neighbor** *ip-address* **route-map** *map-name* { **in** | **out** }	Apply the routing policy to a specified peer to filter the received or advertised routes.
7	Raisecom(config-router-af)#**neighbor** *ip-address* **prefix-list** *prefix-list-name* { **in** | **out** }	Configure a specified peer to filter the received or advertised routes based on IP prefix list.

Configuring BGP route filtering (VPNv4)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip as-path access-list** *access-list-number* { **permit** | **deny** } *regexp*	Configure the filter of AS path list.
3	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
4	Raisecom(config-router)#**address-family vpnv4**	Enter BGP VPNv4 address family configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config-router-af)#**neighbor** *ip-address* **filter-list** *access-list-number* { **in** | **out** }	Configure the BGP route filtering policy based on AS path list.
6	Raisecom(config-router-af)#**neighbor** *ip-address* **route-map** *map-name* { **in** | **out** }	Apply the routing policy to a specified peer to filter the received or advertised routes.
7	Raisecom(config-router-af)#**neighbor** *ip-address* **prefix-list** *prefix-list-name* { **in** | **out** }	Configure a specified peer to filter the received or advertised routes based on IP prefix list.

Configuring BGP route filtering (IPv4 unicast label address family)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 labeled-unicast**	Enter IPv4 unicast label address family configuration mode.
4	Raisecom(config-router-af)#**neighbor** *ip-address* **route-map** *map-name* { **in** | **out** }	Apply the routing policy to a specified peer to filter the received or advertised routes.
5	Raisecom(config-router-af)#**neighbor** *ip-address* **prefix-list** *prefix-list-name* { **in** | **out** }	Configure a specified peer to filter the received or advertised routes based on IP prefix list.

Configuring the tunnel policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 labeled-unicast**	Enter IPv4 unicast label address family configuration mode.
4	Raisecom(config-router-af)#**tunnel-policy** *policy-name*	Configure the tunnel policy to be used.

8.8.6 Configuring BGP GR

You can configure Graceful Restart (GR) to avoid interruption caused by device restart.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**bgp graceful-restart all**	Enable BGP GR.
4	Raisecom(config-router)#**bgp graceful-restart restart-time** *seconds*	Configure the time upper threshold for e-establishing neighbor relationship during GR. By default, it is 120s.
5	Raisecom(config-router)#**bgp graceful-restart stalepath-time** *seconds*	Configure the time upper threshold for the Helper to keep Stale routes during GR. By default, it is 360s.

8.8.7 Configuring BGP FRR

Fast Re-Route (FRR) is usually used with BFD to rapidly detect link faults and to switch services to the backup path upon a fault.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**auto-frr**	Enable BGP FRR. By default, it is disabled.
4	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter IPv4 address family configuration mode of the BGP VPN instance.
	Raisecom(config-router)#**address-family vpnv4**	Enter BGP VPNv4 address family configuration mode.
	Raisecom(config-router)#**address-family ipv4 labeled-unicast**	Enter IPv4 unicast label address family configuration mode.
5	Raisecom(config-router-af)#**auto-frr**	Enable BGP FRR. By default, it is disabled.

8.8.8 Configuring BFD for BGP

BGP routing mode

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-router)#**neighbor** *ip-address* **fall-over bfd**	Enable BFD for BGP. By default, it is disabled.

IPv4 mode based on VPN instance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**neighbor** *ip-address* **fall-over bfd**	Enable BFD for peer BGP connections. By default, it is disabled.

8.8.9 Configuring BGP authentication

Configuring BGP authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**neighbor** *ip-address* **password** *password*	Enable to perform MD5 authentication on the BGP message when the BGP neighbor establishes the TCP connection. By default, it is disabled.

Configuring BGP authentication (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**neighbor** *ip-address* **password** *password*	Enable MD5 authentication on BGP messages when the BGP peer establishes TCP connections. By default, it is disabled.

Copyright © Raisecom Technology Co., Ltd.

8.8.10 Checking configurations

No.	Command	Description
1	Raisecom#**show ip bgp**	Show contents of the local BGP routing table.
2	Raisecom#**show ip bgp** *ip-address* [*ip-mask*]	Show information about the specified network in the local BGP routing table.
3	Raisecom#**show ip bgp dampening dampened-paths**	Show information about the dampened routes.
4	Raisecom#**show ip bgp dampening parameters**	Show route dampening parameters.
5	Raisecom#**show ip bgp dampening flap-statistics**	Show route flapping statistics.
6	Raisecom#**show ip bgp summary**	Show summary of the BGP peer.
7	Raisecom#**show ip bgp neighbors** [*ip-address*]	Show detailed status of the BGP peer.
8	Raisecom#**show ip bgp vpnv4** { **all** | **rd** *rd* | **vrf** *vrf-name* }	Show routing information about all or the specified BGP VPNv4.
9	Raisecom#**show ip bgp vpnv4** { **all** | **vrf** *vrf-name* } *ip-address* [*mask-address*]	Show routing information in the specified network segment of the BGP VPNv4 address family.
10	Raisecom#**show ip bgp vpnv4** { **all** | **vrf** *vrf-name* } **summary**	Show summary routing information about the BGP VPNv4 address family.
11	Raisecom#**show ip bgp vpnv4** { **all** | **vrf** *vrf-name* } **neighbors** *router-id* [**routes**]	Show routing information about the specified BGP VPNv4 peer.
12	Raisecom#**show ip bgp vpnv4 all labels**	Show label information about the BGP VPNv4 route prefix.

8.8.11 Maintenance

Command	Description
Raisecom#**clear ip bgp dampening** [*network-address* [*network-mask*]]	Clear information about routing attenuation.
Raisecom#**clear ip bgp external** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*]	Hard reset all or specified EBGP connections and the connection is interrupted.
Raisecom#**clear ip bgp external** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*] { **in** | **out** | **soft** }	Soft reset all or specified EBGP connections. The connection is not interrupted and only the route is refreshed.
Raisecom#**clear ip bgp internal** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast**]	Hard reset all or specified IBGP connections, and the connection is interrupted.
Raisecom#**clear ip bgp internal** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast**] { **in** | **out** | **soft** }	Soft reset all or specified IBGP connections. The connection is not interrupted and only the route is refreshed.

Copyright © Raisecom Technology Co., Ltd.

Command	Description
Raisecom#**clear ip bgp** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*] *as-id*	Hard reset the BGP connection of the specified AS, or hard reset the BGP connection of the specified address family under the specified AS, and the connection is interrupted.
Raisecom#**clear ip bgp** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*] *as-id* { **in** | **out** | **soft** }	Soft reset the BGP connection of the specified AS, or soft reset the BGP connection of the specified address family under the specified AS. The connection is not interrupted and only the route is refreshed.
Raisecom#**clear ip bgp all** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*]	Hard reset all BGP connections, or reset all BGP connections of the specified address family, and the connection is interrupted.
Raisecom#**clear ip bgp all** [**ipv4 unicast** | **ipv6 unicast** | **pnv4 unicast** | **vrf** *vrf-name*] { **in** | **out** | **soft** }	Soft reset all BGP connections, or reset all BGP connections of the specified address family. The connection is not interrupted and only the route is refreshed.
Raisecom#**clear ip bgp** *ip-address* [**ipv4 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*]	Hard reset the BGP connection with the specified IP address, and the connection is interrupted.
Raisecom#**clear ip bgp** *ip-address* [**ipv4 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*] { **in** | **out** | **soft** }	Soft reset the BGP connection of the specified IP address. The connection is not interrupted and only the route is refreshed.

8.9 Configuring BGP4+

8.9.1 Configuring BGP4+ basic functions

Enabling BGP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enable BGP and create a BGP instance. Enter BGP configuration mode.
3	Raisecom(config-router)#**bgp router-id** *router-id*	(Optional) configure BGP Router ID. By default, the BGP Router ID is the same as the global Router ID of the router.

Copyright © Raisecom Technology Co., Ltd.

Configuring BGP4+ peer

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enable BGP and create a BGP instance. Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**neighbor** *ipv6-address* **remote-as** *as-id*	Create a BGP peer and specify the AS ID of the peer.
5	Raisecom(config-router-af)#**neighbor** *ipv6-address1* **update-source** *ipv6-address2* Raisecom(config-router-af)#**neighbor** *ipv6-address* **update-source** *interface-type interface-number*	Use the specified source IPv6 address or local source interface when establishing a BGP connection. Local source interfaces include physical layer interfaces, VLAN interfaces, loopback interfaces, and sub-interfaces. If one of the two ends of the connection is configured with the correct update source, the BGP connection can be successfully established, but there may be a problem that the connection establishment takes too long. To ensure the stability of the connection establishment at both ends, we recommend configuring both ends of the peer with the update source address.
6	Raisecom(config-router-af)#**neighbor** *ipv6-address* **weight** *weight*	(Optional) configure the weight of routes learned from BGP peers. By default, the weight of routes learned from BGP peers is 0.
7	Raisecom(config-router-af)#**neighbor** *ipv6-address* **default-originate** [**route-map** *route-map-name*]	(Optional) enable the function of sending the default route to the peer. By default, no default route is sent to the peer.
8	Raisecom(config-router-af)#**neighbor** *ipv6-address* **next-hop-self**	(Optional) configure the router to modify the next hop address of the route to its own IP address when advertising the route to the peer. By default, when the router advertises routes to IBGP peers, the next-hop IP address of the route is the same as the next-hop IP address of the route in the local BGP routing table.
9	Raisecom(config-router-af)#**neighbor** *ipv6-address* **ebgp-multihop** [*ttl*]	(Optional) configure the peers on the non-directly connected network to establish EBGP connections, and specify the maximum number of hops allowed for EBGP connections. By default, only physically directly-connected peers are allowed to establish EBGP connections.
10	Raisecom(config-router-af)#**neighbor** *ipv6-address* **route-update-interval** *second*	(Optional) configure the interval for sending packets with the same route prefix to the peer.

Copyright © Raisecom Technology Co., Ltd.

8.9.2 Configuring BGP4+ advertised routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**network** *ipv6-address* [**route-map** *route-map-name*]	Inject static routes into the BGP routing table and advertise them to other ASs or local AS peers.

8.9.3 Configuring BGP4+ redistributed routes

Redistributing default route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**default-information originate**	Configure the BGP to redistribute the default route.

Redistributing IGP routes

BGP cannot discover routes by itself, so it is necessary to redistribute routes of other protocols (such as IGP or static routes) into the BGP routing table and advertise these routes to other ASs or local AS peers.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**redistribute** { **connected** | **static** | **ripng** | **ospfv3** *process-id* | **isisv6** *process-id* } [**metric** *metric*] [**route-map** *map*]	Configure BGP to redistribute routes of other protocols into the BGP routing table through re-advertising.

Copyright © Raisecom Technology Co., Ltd.

8.9.4 Configuring BGP4+ route attributes

Configuring BGP4+ administrative distance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**distance bgp ebgp** *distance1* **ibgp** *distance2* **local** *distance3*	Configure the administrative distance of the BGP route. • The administrative distance of external routes (routes learned through the EBGP) is 20 by default. • The administrative distance of internal routes (routes learned through the IBGP) is 200 by default. • The administrative distance of local routes (BGP routes redistributed through the aggregation command) is 200 by default.

Configuring default MED of BGP4+ route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**default-metric** *metric-value*	Configure the default MED of the local BGP router. This configuration only takes effect on imported routes and summary routes.

Synchronizing BGP4+ with IGP route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**synchronization**	Enable BGP and IGP route synchronization. By default, the synchronization between BGP and IGP routes is disabled.

Copyright © Raisecom Technology Co., Ltd.

Configuring BGP4+ group attribute

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**neighbor** *ipv6-address* **send-community standard**	Enable BGP to send standard community attributes to peers. By default, this feature is disabled.
5	Raisecom(config-router-af)#**neighbor** *ipv6-address* **send-community extended**	Enable BGP to send extended community attributes to peers. By default, this feature is disabled.

8.9.5 Configuring BGP4+ network

Configuring BGP4+ route summarization

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**aggregate-address** *ipv6-address/prefix-length*	Configure BGP route summarization, and advertise summary routes and detailed routes.
5	Raisecom(config-router-af)#**aggregate-address** *ipv6-address/prefix-length* **summary-only**	Configure BGP route summarization and only advertise summary routes to suppress detailed routes.
6	Raisecom(config-router-af)#**aggregate-address** *ipv6-address/prefix-length* **as-set**	Configure BGP route summarization and set the AS_SET option so that the summary route includes AS path information of its detailed routes, effectively preventing routing loops.

Configuring BGP4+ route reflector

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-router-af)#**neighbor** *ipv6-address* **route-reflector-client**	Configure the host as a route reflector and use the specified peer as a client of the route reflector. By default, the route reflector is disabled.
5	Raisecom(config-router-af)#**bgp client-to-client reflection**	Enable route reflection between route reflector clients. By default, route reflection between route reflector clients is enabled.

Configuring BGP4+ default local priority

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**bgp default local-preference** *priority*	Configure the default local priority of BGP. By default, the default local priority of BGP is 100.

Configuring BGP4+ route filtering

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip as-path access-list** *access-list-number* { **permit** | **deny** } *regexp*	Configure the filter of the AS path list.
3	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
4	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
5	Raisecom(config-router-af)#**neighbor** *ipv6-address* **filter-list** *access-list-number* { **in** | **out** }	Configure the BGP route filtering policy based on the AS path list. By default, it is not based on AS path filtering and receives all routing updates from this peer.
6	Raisecom(config-router-af)#**neighbor** *ipv6-address* **route-map** *map-name* { **in** | **out** }	Apply routing policies to the specified peers to filter received or advertised routes.
7	Raisecom(config-router-af)#**neighbor** *ipv6-address* **prefix-list** *prefix-list-name* { **in** | **out** }	Configure the specified peer to filter the received or advertised routes based on IP prefix list.

Copyright © Raisecom Technology Co., Ltd.

8.9.6 Configuring BGP4+ authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**neighbor** *ipv6-address* **password** *password*	Enable BGP peers to establish MD connections and perform MD5 authentication on BGP packets. By default, this feature is disabled.

8.9.7 Checking configurations

Step	Command	Description
1	Raisecom#**show ip bgp ipv6 unicast summary**	Show summary information about IPv6 BGP peers.
23	Raisecom#**show ip bgp ipv6 unicast neighbors** [*ipv6-address*]	Show the status information about IPv6 BGP peers.
3	Raisecom#**show ip bgp ipv6 unicast dampening dampened-paths**	Show suppressed routing information in the IPv6 unicast routing table.
4	Raisecom#**show ip bgp ipv6 unicast dampening flap-statistics**	Show the statistics of route flapping in the IPv6 unicast routing table.
5	Raisecom#**show ip bgp ipv6 unicast** [*ipv6-address* | *ipv6-address/prefix-length*]	Show information about the specified network in the BGP routing table.

8.9.8 Maintenance

For BGP4+ maintenance commands, refer to section 8.8.11 Maintenance.

8.10 Configuring RIP

8.10.1 Configuring RIP basic functions

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)#**network** *ip-address*	Configure a directly-connected and effective network based on RIP.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-rip)#**offset-list** access-list-name { **in** | **out** } offset-value [*interface-type interface-number*]	Configure the additional metrics when the interface receives or sends RIP routes. By default, it is 0.
5	Raisecom(config-rip)#**passive-interface** { *interface-type interface-number* | **default** }	(Optional) configure the interface to be a passive interface. By default, it is a non-passive interface.

8.10.2 Configuring RIP version

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)#**version** *version-id* Raisecom(config-rip)#**exit**	Configure global RIP version ID. By default, global RIP version is not configured. In this case, interfaces which are configured with RIP but not configured with the RIP version in the Tx direction will send V1 packets. Interfaces which are enabled with RIP but not configured with the RIP version in the Rx direction will receive packets of any version.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
5	Raisecom(config-port)#**ip rip receive version** { **1** | **2** }*	Configure the receiving RIP version. By default, the receiving RIP version is subjected to the global RIP version.
6	Raisecom(config-port)#**ip rip send version** { **1** | **2** } *	Configure the sending RIP version. By default, the sending RIP version is subjected to the global RIP version.
7	Raisecom(config-port)#**ip rip v2-broadcast**	Configure the interface which runs RIPv2 to send broadcast updates. By default, it sends multicast updates.

Note

You can configure RIP version globally and on the interface of the RAX721. If the interface is configured with RIP version, then this RIP version prevails.

8.10.3 Redistributing external routes

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)#**host-route**	Enable the function of receiving host routes. By default, it is enabled.
4	Raisecom(config-rip)#**default-information originate**	Enable broadcasting the default route. By default, it is disabled.
5	Raisecom(config-rip)#**redistribute** { **static** | **connected** | **isis** *process-id* | **bgp** | **ospf** *process-id* } [**metric** *metric*] [**route-map** *map-name*] [**tag** *tag-value*]	Configure the policy for redistributing RIP routes.
6	Raisecom(config-rip)#**default-metric** *metric*	Configure the default metrics of redistributing external routes. By default, it is 1.
7	Raisecom(config-rip)#**auto-summary**	Enable automatic aggregation (support RIPv2 only). By default, it is enabled.
8	Raisecom(config-rip)#**validate-update-source**	Enabled the function of checking the source IP address of the received RIP packets. By default, it is enabled.

8.10.4 Configuring timer

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)#**timers basic** *update-time aged-time holddown-time garbage-collection-time*	Configure the RIP timer. By default, the update interval is 30s; the aging interval is 180s; the suppression interval is 120s; and the garbage collection interval is 120s.

8.10.5 Configuring loop suppression

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-port)#**ip rip split-horizon**	Enable split horizon on the interface, that is, the route learned from one interface will not be broadcasted back to the interface again. Be default, it is enabled.
4	Raisecom(config-port)#**ip rip poisoned-reverse**	Enable poison reverse on the interface, that is, the route learned from one interface can be advertised to other interfaces through this interface. However, the metrics of those routes is configured to 16, namely, unreachable. By default, it is disabled.

If poison reverse and split horizon are enabled together, split horizon will be invalid.

8.10.6 Configuring RIP authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip rip authentication mode** { **text** | **md5** }	Configure the packet authentication mode on the interface. By default, the authentication mode of RIPv2 packets on the interface is no authentication.
4	Raisecom(config-port)#**ip rip authentication string** *password-string*	Configure the interface-associated password.
5	Raisecom(config-port)#**ip rip authentication key-chain** *key-chain-name*	Configure the interface-associated authentication secret string.

8.10.7 Configuring routing policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *rmap-name* } **in** [*interface-type interface-number*]	Configure the RIP ingress routing policy.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-rip)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *rmap-name* } **out** [*interface-type interface-number*]	Configure RIP egress routing policy.
5	Raisecom(config-rip)#**distribute-list gateway** *list-name* **in** [*interface-type interface-number*]	Execute routing policies on the source address of the received packets through RIP.

8.10.8 Configuring route preference

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)#**distance** *distance-value* [*ip-address wild-card-mask*]	Configure the administrative distance of RIP, namely, the protocol priority. The shorter the administrative distance is, the higher the priority will be. By default, the administrative distance is 120.
4	Raisecom(config-rip)#**maximum load-balancing** *number*	Configure the maximum number of IP equal-cost multi-path load balancing paths.

8.10.9 Checking configurations

No.	Command	Description
1	Raisecom#**show ip rip**	Show basic information about RIP.
2	Raisecom#**show ip rip database**	Show information about RIP routing database.
3	Raisecom#**show ip rip interface** [*interface-type interface-number*]	Show configurations and status of the interface which runs RIP.

8.11 Configuring RIPng

8.11.1 Configuring RIPng basic functions

Starting RIPng process

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**router ripng**	Start the RIPng process and enter RIPng configuration mode.
3	Raisecom(config-ripng)#**ipv6 ripng offset-list** *ipv6-access-list-name* { **in** | **out** } *offset-value* Raisecom(config-ripng)#**exit**	Configure additional metrics when the interface receives or sends RIPng routes. By default, the additional metric value when an interface receives or sends a RIPng route is 0.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
5	Raisecom(config-port)#**ipv6 ripng enable**	Enable RIPng capacity on the interface.

Configuring RIPng passive interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 ripng passive-interface enable**	Configure the interface as a RIPng passive interface. By default, no interface is a passive interface.

8.11.2 Controlling routing information

Redistributing routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ripng**	Start the RIPng process and enter RIPng configuration mode.
3	Raisecom(config-ripng)#**redistribute** { **static** | **connected** | **isisv6** *process-id* | **bgp4+** | **ospfv3** *process-id* } [**metric** *metric*] [**route-map** *map-name*] [**tag** *tag-value*]	Configure the RIPng route redistributing policy.

Configuring broadcast default route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ripng**	Start the RIPng process and enter RIPng configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-ripng)#**default-information originate** Raisecom(config-ripng)#**exit**	Enable the function of broadcasting the default route. By default, it is disabled.

Advertising summary routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
5	Raisecom(config-port)#**ipv6 ripng summary-address** *ipv6-address/m*	Advertise the aggregated IPv6 prefix information on the interface.

8.11.3 Configuring timer

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ripng**	Start the RIPng process and enter RIPng configuration mode.
3	Raisecom(config-ripng)#**timers basic** *update-time aged-time holddown-time garbage-collection-time*	Configure the RIPng timer. By default, the update interval is 30s, the aging interval is 180s, the suppression interval is 120s, and the garbage collection interval is 120s.

8.11.4 Configuring loop suppression

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 ripng split-horizon**	Enable split horizon, that is, the routes learned from an interface will not be broadcast back to the interface. By default, split horizon is enabled.
4	Raisecom(config-port)#**ipv6 ripng poisoned-reverse**	Enable poison reverse, that is, the routes learned from an interface can also be advertised out from this interface, but the metric of these routes has been configured to 16, which is unreachable. By default, poison reverse is disabled.

Copyright © Raisecom Technology Co., Ltd.

If poison reverse and split horizon are enabled at the same time, split horizon will be invalid.

8.11.5 Configuring RIPng authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 ripng ipsec policy** *policy-name* Raisecom(config-port)#**exit**	Configuring IPsec authentication on the interface.
4	Raisecom(config)#**router ripng**	Start the RIPng process and enter RIPng configuration mode.
5	Raisecom(config-ripng)#**ipsec policy** *policy-name*	Configure process IPsec authentication.

8.11.6 Configuring routing policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ripng**	Start an RIPng process and enter RIP configuration mode.
3	Raisecom(config-ripng)#**distribute-list** { **ipv6-access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *rmap-name* } **in** [*interface-type interface-number*]	Configure the routing policy of RIPng in the ingress direction.
4	Raisecom(config-ripng)#**distribute-list** { **ipv6-access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *rmap-name* } **out** [*interface-type interface-number*]	Configure the routing policy of RIPng in the egress direction.

8.11.7 Configuring route preference

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ripng**	Start an RIPng process and enter RIP configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-ripng)#**distance** *distance-value*	Configure the RIPng administrative distance, namely, the routing priority. The smaller the administrative distance is, the higher the priority will be. By default, the RIPng administrative distance is 120.

8.11.8 Configuring route summarization

Route aggregation can not only reduce the size of the routing table, but also reduce the routing protocol packets exchanged between routers.

- The device advertises summary routes that match the IPv6 prefix, and multiple original routes can be replaced by one route.
- The summary route can be the route discovered by RIPng or the imported external route.
- The cost value of the summary route is the smallest one of all the summary routes.

The RIPng route summarization supports the configuration of Layer 3 Ethernet interfaces, sub-interfaces, and VLAN interfaces. This chapter only uses Layer 3 Ethernet interfaces as an example to describe the configuration steps.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *unit-id/slot-id/port-id*	Enter Layer 3 Ethernet interface configuration mode.
3	Raisecom(config-gigaethernet*/*/*)#**ipv6 ripng summary-address** *ipv6-address/address-length*	Configure IPv6 RIPng route summarization.

8.11.9 Checking configurations

No.	Command	Description
1	Raisecom#**show ipv6 ripng protocol**	Show RIPng basic information.
2	Raisecom#**show ipv6 ripng database** [**statistics**]	Show information about the RIPng routing database.
3	Raisecom#**show ipv6 ripng interface** [*interface-type interface-number*]	Show configurations and status of the interface running RIPng.

Copyright © Raisecom Technology Co., Ltd.

9 MPLS

This chapter describes principles and configuration procedures of MPLS-TP, including following sections:

- Configuring MPLS basic functions
- Configuring MPLS Tunnel
- Configuring static LSP
- Configuring LDP LSP
- Configuring MPLS TE
- Configuring MPLS Tunnel fault detection
- Configuration examples

9.1 Configuring MPLS basic functions

9.1.1 Preparing for configurations

Scenario

Configuring MPLS basic functions are prerequisites for making other MPLS functions effective. The Label Switching Router (LSR) is the network device, which can exchange and forward the MPLS label. The LSR is also called the MPLS node. The LSR is the basic element in the MPLS network. All LSRs support MPLS. To enable global MPLS, you must enable the LSR ID.

Prerequisite

N/A

9.1.2 Configuring MPLS basic functions

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mpls lsr-id` *`lsr-id`*	Configure the LSR ID of the device.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**mpls enable**	Enable global MPLS. By default, it is disabled.
4	Raisecom(config)#**mpls label-advertise** { **implicit-null** | **non-null** | **explicit-null** }	(Optional) configure the label distribution mode for the last but one hop.

9.1.3 Checking configurations

Step	Command	Description
1	Raisecom#**show mpls**	Show global MPLS configurations.

9.2 Configuring MPLS Tunnel

9.2.1 Configuring MPLS Tunnel basic functions

Configuring Tunnel working mode

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter Tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#**tunnel mode** { **mpls** | **ipsec** { **ipv4** | **ipv6** } | **ipv4-ipv6** [**ds-lite**] | **ipv6-ipv4** [**6rd** | **6to4**] }	Configure the Tunnel mode.
4	Raisecom(config-tunnelif)#**description** *description*	(Optional) configure descriptions of the Tunnel interface.
5	Raisecom(config-tunnelif)#**mtu** *mtu-value*	Configure the Tunnel MTU.

Configuring Tunnel IPv4 address

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter Tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#**tunnel mode mpls**	Configure the Tunnel mode to MPLS.
4	Raisecom(config-tunnelif)#**destination** *ip-address*	Configure the destination IPv4 address of the Tunnel interface.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config-tunnelif)#**ip address** *ip-address* [**sub**]	Configure the IPv4 address of the Tunnel interface.
6	Raisecom(config-tunnelif)#**ip address unnumbered loopback** *interface-number*	Configure the Tunnel interface to borrow the IP address of the loopback interface. The prerequisite is that the loopback interface has been configured with an IP address.

Configuring Tunnel IPv6 address

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter Tunnel interface configuration mode.
3	Raisecom(config)#**tunnel mode mpls**	Configure the Tunnel mode to MPLS.
4	Raisecom(config-tunnelif)#**ipv6 address** *ipv6-address/m* [**eui-64**]	Configure the IPv6 address of the Tunnel interface.
	Raisecom(config-tunnelif)#**ipv6 address** *ipv6-address/m* **anycast**	

Configuring Tunnel type

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter Tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#**tunnel mode mpls**	Configure the Tunnel interface mode to MPLS.
4	Raisecom(config-tunnelif)#**mpls signal-protocol** { **rsvp-te** | **static** |**segment-routing** }	Configure the protocol type of the Tunnel interface. By default, it is static.
5	Raisecom(config-tunnelif)#**mpls tunnel-id** *tunnel-id*	Configure the Tunnel ID of the Tunnel interface.
6	Raisecom(config-tunnelif)#**mpls te bypass-tunnel**	(Optional) configure the current Tunnel as a bypass Tunnel.
7	Raisecom(config-tunnelif)#**destination** *ip-address*	Configure the destination IP address of the Tunnel interface. The prerequisite is that the Tunnel interface has been configured to MPLS mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
8	Raisecom(config-tunnelif)#**mpls te commit**	Submit the above configurations.

Committing tunnel configuration parameters

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter Tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#**tunnel mode mpls**	Configure the Tunnel interface mode to MPLS.
4	Raisecom(config-tunnelif)#**mpls tunnel-id** tunnel-id	Configure the Tunnel ID of the Tunnel interface.
5	Raisecom(config-tunnelif)#**mpls te commit**	Commit the Tunnel interface attributes.

9.2.2 Configuring MPLS Tunnel policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**tunnel-policy** *policy-name*	Enter Tunnel policy configuration mode.
3	Raisecom(config-tunnelpolicy)#**tunnel select-seq cr-lsp** [**lsp**] Raisecom(config-tunnelpolicy)#**tunnel select-seq lsp** [**cr-lsp**]	Configure Tunnel selection policy. By default, the Tunnel optimization policy parameter is cr-lsp lsp, which means that the CR-LSP tunnel will be selected first, followed by LSP Tunnel. The GRE Tunnel will not be selected.
4	Raisecom(config-tunnelpolicy)#**tunnel binding destination** *peer-ip* **tunnel** *interface-number*	Bind the tunnel with the destination IP address so that the tunnel can carry the specified VPN services only.

9.2.3 Configuring hot backup of the tunnel

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter Tunnel interface configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-tunnelif)#**mpls te hot-standby** [**overlap** | **wtr** *second*]	Configure hot backup of the tunnel. You can also enable the overlapping function of the hot backup path and primary CR-LSP path if needed. You can configure the hot backup switching time.

9.2.4 Configuring tunnel label recording

The device supports recording routes of the tunnel. You can choose to enable this function. Route recording and label recording are used to record the various nodes that MPLS TE tunnels pass through and the label values assigned to each node, so that users can understand the path and label allocation of MPLS TE tunnels based on the recorded information. When a fault occurs in the MPLS TE tunnel, users can also locate the fault based on the recorded information.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter Tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#**mpls te record-route** [**label**]	Enable route recording of the tunnel. You can choose to enable this function.

9.2.5 Configuring tunnel re-optimization

Tunnel re-optimization refers to the periodic or manual execution of the **mpls te reoptimization** command to trigger the Ingress node of the tunnel to re-select the path, to switch the MPLS TE tunnel to the current optimal path.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter Tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#**mpls te reoptimization** [**frequency** *seconds*]	Enable tunnel re-optimization.

9.2.6 Checking configurations

No.	Command	Description
1	Raisecom#**show interface tunnel**	Show information about the Tunnel interface.
2	Raisecom#**show mpls te tunnel**	Show configurations of the Tunnel interface.

Copyright © Raisecom Technology Co., Ltd.

9.3 Configuring static LSP

9.3.1 Preparing for configurations

Scenario

The static LSP is established by the administrator by manually assigning labels for all FECs. It is suitable for simple and stable small-size network. To manually assign labels, the outgoing label value of the last node is the incoming label value of the next mode.

The static LSP does not use the label distribution protocol and does not exchange the control packet. Therefore, it consumes fewer resources. However, the LSP, established by statically assigning labels, cannot be dynamically adjusted according to the network topology changes. The administrator needs to manually adjust the static LSP.

Prerequisite

Configure MPLS basic functions.

9.3.2 Configuring static unidirectional LSP with IP capability

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls static-lsp ingress** *lsp-name dest-network mask* **nexthop** *ip-address* **out-label** *out-label* **lsr-id** *egress-lsr-id* **tunnel-id** *tunnel-id*	Configure the static unidirectional LSP Ingress node.
3	Raisecom(config)#**mpls static-lsp transit** *lsp-name* **in-label** *in-label* **nexthop** *ip-address* **out-label** *out-label* **lsr-id** *ingress-lsr-id egress-lsr-id* **tunnel-id** *tunnel-id*	Configure the static unidirectional LSP Transit node.
4	Raisecom(config)#**mpls static-lsp egress** *lsp-name* **in-label** *in-label* **lsr-id** *ingress-lsr-id* **tunnel-id** *tunnel-id*	Configure the static unidirectional LSP Egress node.
5	Raisecom(config)#**mpls static-lsp egress** *lsp-name* **diffserv-mode** { **pipe** | **uniform** [**exp-to-local-priority** *profile-number*] }	(Optional) configure the differential service mode of the static unidirectional LSP Egress node.

9.3.3 Configuring static unidirectional LSP without IP capability

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls static-lsp ingress** *lsp-name dest-network* [*mask*] **nexthop-mac** *mac-address interface-type interface-number* **out-label** *out-label* **lsr-id** *egress-lsr-id* **tunnel-id** *tunnel-id*	Configure the static unidirectional LSP Ingress node.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**mpls static-lsp transit** *lsp-name* **in-label** *in-label* **nexthop-mac** *mac-address interface-type interface-number* **out-label** *out-label* **lsr-id** *ingress-lsr-id egress-lsr-id* **tunnel-id** *tunnel-id*	Configure the static unidirectional LSP Transit node.
4	Raisecom(config)#**mpls static-lsp egress** *lsp-name* **in-label** *in-label* **lsr-id** *ingress-lsr-id* **tunnel-id** *tunnel-id*	Configure the static unidirectional LSP Egress node.
5	Raisecom(config)#**mpls static-lsp egress** *lsp-name* **diffserv-mode** { **pipe** | **uniform** [**exp-to-local-priority** *profile-number*] }	(Optional) configure the differential service mode of the static unidirectional LSP Egress node.

9.3.4 Configuring static bidirectional LSP with IP capability

Configuring static bidirectional LSP Ingress node

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls bidirectional static-lsp ingress** *lsp-name* **lsr-id** *egress-lsr-id* **tunnel-id** *tunnel-id*	Create the static bidirectional corouted LSP and enter Ingress LSP (ILSP) configuration mode.
3	Raisecom(config-ingress-lsp)#**forward** *dest-network mask* **nexthop** *ip-address* **out-label** *out-label*	Configure the next hop of the ingress node (with IP capability) forward LSP.
4	Raisecom(config-ingress-lsp)#**backward in-label** *in-label*	Configure the incoming label of the ingress node backward LSP.

Configuring static bidirectional LSP Transit node

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls bidirectional static-lsp transit** *lsp-name* **lsr-id** *ingress-lsr-id egress-lsr-id* **tunnel-id** *tunnel-id*	Create the static bidirectional corouted LSP and enter TLSP configuration mode.
3	Raisecom(config-transit-lsp)#**forward in-label** *in-label* **nexthop** *ip-address* **out-label** *out-label*	Configure the next hop of the Transit node forward LSP.
4	Raisecom(config-transit-lsp)#**backward in-label** *in-label* **nexthop** *ip-address* **out-label** *out-label*	Configure the incoming label of the Transit node backward LSP.

Copyright © Raisecom Technology Co., Ltd.

Configuring static bidirectional LSP Egress node

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls bidirectional static-lsp egress** *lsp-name* **lsr-id** *ingress-lsr-id* **tunnel-id** *tunnel-id*	Create the static bidirectional corouted LSP and enter ELSP (ELSP) configuration mode.
3	Raisecom(config-egress-lsp)#**forward in-label** *in-label*	Configure the incoming label of the Egress node forward LSP.
4	Raisecom(config-ingress-lsp)#**backward** *dest-network mask* **nexthop** *ip-address* **out-label** *out-label*	Configure the outgoing label of the Egress node backward LSP.

9.3.5 Configuring static bidirectional LSP without IP capability

Note

To configure static bidirectional LSP without IP capability, you must configure the physical interface to Layer 3 physical interface mode; otherwise, the configuration will fail.

Configuring static bidirectional LSP Ingress node

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls bidirectional static-lsp ingress** *lsp-name* **lsr-id** *egress-lsr-id* **tunnel-id** *tunnel-id*	Create the static bidirectional corouted LSP and enter ILSP configuration mode.
3	Raisecom(config-ingress-lsp)#**forward** *dest-network* [*mask*] **nexthop-mac** *mac-address interface-type interface-number* **out-label** *out-label*	Configure the next hop of the Ingress node forward LSP.
4	Raisecom(config-ingress-lsp)#**backward in-label** *in-label*	Configure the incoming label of the Ingress node backward LSP.

Configuring static bidirectional LSP Transit node

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls bidirectional static-lsp transit** *lsp-name* **lsr-id** *ingress-lsr-id egress-lsr-id* **tunnel-id** *tunnel-id*	Create the static bidirectional corouted LSP and enter Transit LSP (TLSP) configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-transit-lsp)#**forward in-label** *in-label* **nexthop-mac** *mac-address interface-type interface-number* **out-label** *out-label*	Configure the next hop of the Transit node forward LSP.
4	Raisecom(config-transit-lsp)#**backward in-label** *in-label* **nexthop-mac** *mac-address interface-type interface-number* **out-label** *out-label*	Configure the next hop of the Transit node backward LSP.

Configuring static bidirectional LSP Egress node

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls bidirectional static-lsp egress** *lsp-name* **lsr-id** *ingress-lsr-id* **tunnel-id** *tunnel-id*	Create the static bidirectional corouted LSP and enter Egress LSP configuration mode.
3	Raisecom(config-egress-lsp)#**forward in-label** *in-label*	Configure the incoming label of the Egress node forward LSP.
4	Raisecom(config-egress-lsp)#**backward** *dest-network* [*mask*] **nexthop-mac** *mac-address interface-type interface-number* **out-label** *out-label*	Configure the next hop of the Egress node backward LSP.

9.3.6 Checking configurations

No.	Command	Description
1	Raisecom#**show mpls lsp statistics**	Show all LSP configurations
2	Raisecom#**show mpls bidirectional static-lsp** [*lsp-name*]	Show static bidirectional LSP configurations.
3	Raisecom#**show mpls static-lsp** [*lsp-name*] Raisecom#**show mpls static-lsp** [**egress** | **ingress** | **transit**]	Show static unidirectional LSP configurations.
4	Raisecom#**show mpls lsp static** [**ingress** | **transit** | **egress**]	Show status of static LSP.

Copyright © Raisecom Technology Co., Ltd.

9.4 Configuring LDP LSP

9.4.1 Preparing for configurations

Scenario

The LDP is used to dynamically assign labels for LSRs to establish the LSP dynamically. The LDP is used to exchange label information among LSRs. Therefore, when forwarding the packet, the LSR can add related Tag to the packet based on label requirement of the next-hop LSP. Then, the packet can be processed properly at the next-hop LSR.

Prerequisite

Enable MPLS.

9.4.2 Configuring global LDP

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mpls ldp`	Enable global LDP.
3	`Raisecom(config)#lsp-trigger { all | host | none }`	Configure the LDP to dynamically establish the LSP trigger policy. By default, the triggering policy for the LDP to dynamically establish the LSP is Host.
4	`Raisecom(config)#mpls label-advertise { implicit-null | non-null | explicit-null }`	(Optional) configure the label distribution mode popped out in the last but one hop.

9.4.3 Configuring LDP on interface

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`*	Enter interface configuration mode.
3	`Raisecom(config-port)#mpls ldp`	Enable LDP on the interface.
4	`Raisecom(config-port)#mpls ldp transport-address interface`	(Optional) set the transport address of the LDP local session to the IP address of the current interface. By default, the transport address of the local session is LSR ID.
5	`Raisecom(config-port)#mpls ldp timer hello-hold` *`hello-time`*	(Optional) configure the Hello-hold timer of the LDP local session. By default, the Hello-hold timer of the LDP local session is 15s.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config-port)#**mpls ldp timer keepalive-hold** *keepalive-time*	(Optional) configure the Keepalive-hold timer of the LDP local session. By default, the Keepalive-hold timer of the LDP local session is 45s.
7	Raisecom(config-port)#**mpls ldp local-lsr-id loopback** *loopback-num*	(Optional) specify the IP address of the loopback interface as the LSR ID of the local LDP session.

9.4.4 Configuring LDP remote session

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls ldp targeted neighbour** *ip-address*	Enable LDP remote discovery and enter remote neighbor configuration mode.
3	Raisecom(config-ldp-remote-peer)#**mpls ldp timer hello-hold** *hello-time*	Configure the Hello-hold timer of the LDP remote session. By default, the Hello-hold timer of the LDP remote session is 45s.
4	Raisecom(config-ldp-remote-peer)#**mpls ldp timer keepalive-hold** *keepalive-time*	Configure the Keepalive-hold timer of the LDP remote session. By default, the Hello-hold timer of the LDP remote session is 45s.
5	Raisecom(config-ldp-remote-peer)#**mpls ldp local-lsr-id loopback** *loopback-num*	(Optional) specify the IP address of the loopback interface as the LSR ID of the remote LDP session.

9.4.5 Configuring LDP MD5

LDP Message Digest Algorithm 5 (MD5) encryption can generate the unique digest information for the same information segment. LDP MD5 can implement LDP packet anti-tampering check to improve information security. This encryption method is stricter than the TCP in the general sense.

Configure the RAX721 as below. Step 2 and step 3 can implement different encryption functions respectively. Choose one as required.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls ldp md5-password plain** *peer-ip-address password*	Configure LDP MD5 cleartext password. Use the **show running-config** command to show the cleartext password.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**mpls ldp md5-password cipher** *peer-ip-address* [**encrpty**] *password*	Configure LDP MD5 ciphertext password. Support cleartext and ciphertext inputs. • For cleartext input, enter letters, numbers, and characters. Use the **show running-config** command to show the cleartext password which is displayed in cleartext. • For ciphertext password, enter the MD5 special ciphertext password. Use the **show running-config** command to show the password which is displayed in ciphertext.

9.4.6 Configuring LDP policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls ldp** { **inbound** | **outbound** } **peer** { *ip-address* | **all** | **peer-group** *peer-group-name* } **fec** { **none** | **host** | **ip-prefix** *prefix-name*)	Configure the MPLS LDP policy.

9.4.7 Configuring BFD for TLDP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls ldp targeted neighbour** *ip-address*	Enable LDP remote discovery and enter remote symmetric configuration mode.
3	Raisecom(config-ldp-remote-peer)#**mpls ldp bfd enable**	Enable BFD for TLDP.

9.4.8 Configuring LDP FRR

Automatic LDP FRR

The formation of dynamic LDP FRR depends on the FRR formed by routes. Here takes OSPF FRR for example.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-router-ospf)#**loop-free-alternate** Raisecom(config-router-ospf)#**exit**	Enable OSPF LFA.
4	Raisecom(config)#**mpls ldp auto-frr lsp-trigger** { **all** | **host** | **none** }	Configure a policy that the backup route triggers the LDP to create a backup LSP. By default, the policy to create a backup LSP is triggered based on host routes.

Static LDP FRR

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**mpls ldp frr nexthop** *nexthop-address*	Enable LDP FRR and specify the IP address of the next hop. By default, LDP FRR is disabled.

9.4.9 Checking configurations

No.	Command	Description
1	Raisecom#**show mpls ldp**	Show LDP global information.
2	Raisecom#**show mpls ldp history** [*ip-address*]	Show LDP history information.
3	Raisecom#**show mpls ldp interface** [*interface-type interface-number*] [**detail**]	Show LDP interface information.
4	Raisecom#**show mpls ldp targeted neighbour** *ip-address*	Show remote neighbor information.
5	Raisecom#**show mpls ldp session** [**detail**] [**peer** *peer-address*]	Show LDP session information.
6	Raisecom#**show mpls ldp peer**	Show LDP neighbor information.
7	Raisecom#**show mpls ldp lsp**	Show LDP LSP information.
8	Raisecom#**show mpls ldp adjacency** [**peer** *peer-address*]	Show LDP adjacency information.
9	Raisecom#**show mpls ldp lsp record** [*ip-address*] [**detail**] [{ **libral** | **lsp** }]	Show details about LDP LSP.
10	Raisecom#**show mpls ldp lsp record last** *number* [**detail**]	Show LDP LSP records.
11	Raisecom#**show mpls ldp policy** [{ **inbound** | **outbound** }] [{ **peer-id** *ip-address* | **peer-group** *group-name* }]	Show LDP strategies.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
12	Raisecom#**show mpls lsp** [**ldp**] [**ingress** | **transit** | **egress**]	Show LDP LSP configurations.
13	Raisecom#**show mpls ldp lsp record** [*ip-address*] [**detail**] [{ **libral** | **lsp** }]	Show LDP LSP of all types.

9.4.10 Maintenance

Command	Description
Raisecom#**clear mpls ldp lsp record**	Clear LDP LSP records.
Raisecom#**clear mpls ldp peer** { **all** | *peer-ip* }	Clear LDP sessions.
Raisecom(config)#**mpls ldp graceful-restart**	Configure LDP LSP graceful restart.
Raisecom(config)#**mpls ldp refresh fec** *addr*	Configure LDP refreshing, which can trigger mapping and issue entries.

9.5 Configuring MPLS TE

9.5.1 Preparing for configurations

Scenario

MPLS TE is for solving the traffic congestion on the link caused by unbalanced load which cannot be resolved by traditional routing. It can accurately control traffic paths to avoid congestion nodes, thus solving the problem of some paths being overloaded but some paths being unoccupied.

RSVP is used for dynamically creating public network LSP tunnel in the MPLS TE. It can create, maintain, and remove MPLS TE LSP and provide false alarm.

The device supports choosing the shortest path through Constraint-based Shortest Path First (CSPE) and supports 32 neighbors at most.

Prerequisite

The MPLS is enabled.

9.5.2 Enabling RSVP-TE

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**mpls rsvp-te**	Enable global RSVP-TE. By default, it is disabled.
3	Raisecom(config)#**mpls rsvp-te hello**	Configure RSVP-TE Hello.
4	Raisecom(config)#**mpls rsvp-te hello** { **interval** *seconds* | **lost** *lost-times* }	Configure the sending interval of Hello packets or lost times.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.
6	Raisecom(config-port)#**mpls rsvp-te**	Enable RSVP-TE on the Layer 3 physical interface. By default, it is disabled.

9.5.3 Configuring RSVP-TE authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**mpls rsvp-te authentication** { **cipher** | **plain** } *password*	Configure the RSVP-TE authentication password.
4	Raisecom(config-port)#**mpls rsvp-te authentication lifetime** *seconds*	Configure the lifetime of RSVP-TE authentication. By default, it is 1800s.
5	Raisecom(config-port)#**mpls rsvp-te authentication window-size** *size-value*	Configure the RSVP-TE authentication window.
6	Raisecom(config-port)#**mpls rsvp-te authentication handshake**	Configure RSVP-TE handshaking authentication.

9.5.4 Configuring CSPF

CSPF is the core of MPLS TE for choosing path and is mainly for calculating and establishing path. MPLS-TE calculates the shortest path to various nodes on the network through CSPF algorithm. The CSPF algorithm supports OSPF and ISIS and the multi-process of these two protocols.

Enabling CSPF

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**cspf enable** [**isis-preferred** | **ospf-preferred**]	Enable CSPE. • If you use the **isis-preferred** command, calculation will be done based on ISIS. • If you use the **ospf-preferred** command, calculation will be done based on OSPF. By default, it is disabled.

Configuring OSPF TE

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**vrf** *vrf-name*] [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**capability opaque**	Enable OSPF opaque LSA. By default, it is not enabled.
4	Raisecom(config-router-ospf)#**mpls traffic-eng area** *area-id*	Enable TE for the OSPF area. By default, it is not enabled.
5	Raisecom(config-router-ospf)#**mpls traffic-eng router-id** *router-id*	Configure the Router ID of the MPLS-TE router.

Configuring ISIS TE

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** *area-tag* [**vrf** *vrf-name*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**metric-style wide**	Configure the cost type and use the wide TLV.
4	Raisecom(config-router-isis)#**mpls traffic-eng** { **level-1** | **level-2** }	Enable TE for the ISIS area.
5	Raisecom(config-router-isis)#**mpls traffic-eng router-id** *router-id*	Configure the Router ID of the MPLS-TE router.

Copyright © Raisecom Technology Co., Ltd.

9.5.5 Configuring explicit path and Tunnel

step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls explicit-path** *path-name*	Create MPLS-TE explicit path and enter explicit path configuration mode.
3	Raisecom(config-mpls-exp-path)#**next-hop** *ip-address* { **exclude** | **loose** | **strict** }	Specify the next node of the explicit path.
	Raisecom(config-mpls-exp-path)#**exit**	Exit explicit path configuration mode.
4	Raisecom(config)#**interface tunnel** *interface-number*	Enter tunnel interface configuration mode.
5	Raisecom(config-tunnel)#**description** *description*	(Optional) configure the description information about Tunnel interface.
6	Raisecom(config-tunnel)#**mpls signal-protocol** { **rsvp-te** | **static** | **segment-routing** }	Configure the protocol type of the Tunnel interface. Select RSVP-TE. By default, it is static.
7	Raisecom(config-tunnel)#**mpls tunnel-id** *tunnel-id*	Configure the Tunnel ID of the Tunnel interface.
8	Raisecom(config-tunnelif)#**destination** *ip-address*	Configure Tunnel ID on the Tunnel interface.
9	Raisecom(config-tunnelif)#**mpls explicit-path** *path-name* [**secondary**]	Configure the destination IP address of the Tunnel interface. The prerequisite is that the interface has been configured to MPLS mode.
10	Raisecom(config-tunnelif)#**mpls te commit**	Hand configuration information about MPLS Tunnel interface, including Tunnel ID and destination IP address.
11	Raisecom(config-tunnelif)#**mpls te bypass-tunnel**	(Optional) configure the current Tunnel as a bypass tunnel.
12	Raisecom(config)#**mpls label-advertise** { **explicit-null** | **implicit-null** | **non-null** }	(Optional) configure the label allocation mode popped up in the last but one hop.

9.5.6 Configuring TE protection

Configuring FRR protection

To improve the reliability of the tunnel, deploy TE FRR. TE FRR provides local protection for specified nodes or links through bypass tunnel.

According to different protocols, FRR can be divided into two types: static RSVP FRR and dynamic RSVP FRR.

Copyright © Raisecom Technology Co., Ltd.

step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter Tunnel interface configuration mode.
3	Raisecom(config-tunnel)#**tunnel mode mpls**	Configure the Tunnel mode to MPLS.
4	Raisecom(config-tunnelif)#**mpls signal-protocol** { **rsvp-te** | **static** | **segment-routing** }	Configure the protocol type of the Tunnel interface to RSVP-TE. By default, it is static.
5	Raisecom(config-tunnelif)#**mpls te fast-reroute**	Enable FRR on the Tunnel interface. By default, it is disabled.
6	Raisecom(config-tunnelif)#**mpls te bypass-tunnel**	Configure the current tunnel as the bypass tunnel.
7	Raisecom(config-tunnelif)#**mpls te protected-interface** *interface-type interface-number*	Configure the interface to be protected by the bypass tunnel.
8	Raisecom(config-tunnelif)#**mpls te bypass-attributes affinity property** *properties* **mask** *mask-value*	(Optical) configure the affinity properties of the bypass tunnel. In the scenario of deploying MPLS TE Auto FRR, if you want to control the path selection of Auto bypass tunnel, you can configure the affinity properties of the bypass tunnel. The affinity attribute is a 32-bit vector that identifies the preference of the tunnel for the links that it passes. After this command is configured, when the Auto bypass tunnel is established, the main tunnel will compare the affinity attributes with the management group attributes of the link to determine whether to choose or avoid certain attribute links.
9	Raisecom(config-tunnelif)#**mpls te commit** Raisecom(config-tunnelif)#**exit**	Commit the properties of the Tunnel interface. Exit Tunnel interface configuration mode.
10	Raisecom(config)#**mpls te auto-frr reoptimization** [**frequency** *interval*]	Configure re-optimization of MPLS TE auto bypass-Tunnel.
11	Raisecom(config)#**mpls te auto-frr**	(Optional) enable global Auto FRR. After this command is configured, all MPLS TE interfaces are automatically enabled with Auto FRR.
12	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
13	Raisecom(config-port)#**mpls te auto-frr**	Enable the MPLS TE automatic re-optimization of the egress interface. When the interface works as the egress interface of the master tunnel, it automatically generates a bypass-tunnel for the master tunnel to form FRR protection.

Copyright © Raisecom Technology Co., Ltd.

step	Command	Description
14	Raisecom(config-port)#**mpls te auto-frr block**	(Optional) after global auto FRR is configured, use this command to disable auto FRR on the specified interface. When global auto FRR is not configured, this command does not take effect.

Configuring LSP hot backup

The RSVP-TE is enabled and the explicit path and related function of Tunnel is configured.

step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#**tunnel mode mpls**	Configure the Tunnel interface mode to MPLS.
4	Raisecom(config-tunnelif)#**mpls signal-protocol** { **rsvp-te** | **static** | **segment-routing** }	Configure the protocol type of the Tunnel interface. Select RSVP-TE. By default, the protocol type of the Tunnel interface is static.
5	Raisecom(config-tunnelif)#**destination** *ip-address*	Configure the destination IP address of the Tunnel interface. The prerequisite is that the Tunnel interface has been configured to MPLS mode.
6	Raisecom(config-tunnelif)#**mpls explicit-path** *path-name*	Configure the primary LSP as the specified explicit path.
7	Raisecom(config-tunnelif)#**mpls explicit-path** *path-name* **secondary**	Specify the explicit path as the hot backup LSP and enable hot backup protection.
8	Raisecom(config-tunnelif)#**mpls te commit**	Submit related configurations of the MPLS Tunnel interface, including the Tunnel ID and the destination IP address.
9	Raisecom(config-tunnelif)#**mpls te hot-standby** [**overlap** | **wtr** *second*]	(Optional) enable hot backup of the tunnel. Configure this command to establish both the master LSP and slave LSP.

9.5.7 Configuring BFD for RSVP-TE

step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls rsvp-te bfd all-interface**	Enable BFD based on RSVP-TE globally.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.

Copyright © Raisecom Technology Co., Ltd.

step	Command	Description
4	Raisecom(config-port)#**mpls rsvp-te bfd**	Enable BFD based on RSVP-TE on the interface.

9.5.8 Checking configurations

Step	Command	Description
1	Raisecom#**show mpls rsvp-te**	Show status of RSVP-TE globally.
2	Raisecom#**show mpls rsvp-te interface** [*interface-type interface-number*]	Show status of RSVP-TE on the interface.
3	Raisecom#**show mpls rsvp-te session** [**destination** *ip-address* **tunnel-id** *tunnel-id*]	Show RSVP-TE session.
4	Raisecom#**show interface tunnel**	Show Tunnel interface.
5	Raisecom#**show mpls te tunnel**	Show Tunnel.
6	Raisecom#**show mpls te bypass-tunnel** [*interface-number*]	Show the bypass Tunnel.
7	Raisecom#**show mpls explicit-path** [*path-name*]	Show explicit path.
8	Raisecom#**show mpls te frr protecting** [**bypass-tunnel tunnel** *interface-number*]	Show FRR protection.
9	Raisecom#**show cspf tedb** [**detail** | *ip-address*]	Show TEDB database.
10	Raisecom#**show mpls lsp rsvp-te** [**ingress** | **transit** | **egress**]	Show MPLS-TE LSP configurations.

9.6 Configuring MPLS Tunnel fault detection

9.6.1 Preparing for configurations

Scenario

At the MPLS control plane, you cannot detect the fault when the traffic is forwarded along the LSP. However, you can acknowledge and locate the fault through Ping and Traceroute operations.

Prerequisite

- Establish the path before the Ping test is performed.
- Establish the path before the Traceroute test is performed.

Copyright © Raisecom Technology Co., Ltd.

9.6.2 Configuring MPLS Tunnel fault acknowledgment

Step	Command	Description
1	Raisecom#**ping mpls ipv4** *ip-address/mask* [**generic**] [**nexthop** *ip-address*] [**interval** *interval*] [**count** *count*] [**waittime** *seconds*] [**ttl** *ttl*] [**reply dscp** *dscp-value*] [**reply mode udp** | **reply mode udp-alert**] [**reply pad-tlv**] [**size** *size*] [**source** *ip-address*] [**tc** *tc-value*]	Configure the MPLS LSP Ping test.
2	Raisecom#**ping mpls te tunnel** *tunnel-interface* [**interval** *interval*] [**count** *count*] [**waittime** *seconds*] [**ttl** *ttl*] [**reply dscp** *dscp-value*] [**reply mode udp** | **reply mode udp-alert**] [**reply pad-tlv**] [**size** *size*] [**source** *ip-address*] [**tc** *tc-value*]	Configure the MPLS Tunnel Ping test.

9.6.3 Configuring MPLS Tunnel fault location

Step	Command	Description
1	Raisecom#**traceroute mpls ipv4** *ip-address/mask* [**generic**] [**nexthop** *ip-address*] [**waittime** *seconds*] [**maxttl** *ttl*] [**reply dscp** *dscp-value*] [**reply mode udp** | **reply mode udp-alert**] [**reply pad-tlv**] [**source** *ip-address*] [**tc** *tc-value*] [**flags fec**]	Configure the MPLS LSP Traceroute test.
2	Raisecom#**traceroute mpls te tunnel** *tunnel-interface* [**waittime** *seconds*] [**maxttl** *ttl*] [**reply dscp** *dscp-value*] [**reply mode udp** | **reply mode udp-alert**] [**reply pad-tlv**] [**source** *ip-address*] [**tc** *tc-value*] [**flags fec**]	Configure the MPLS Tunnel Traceroute test.

9.7 Configuration examples

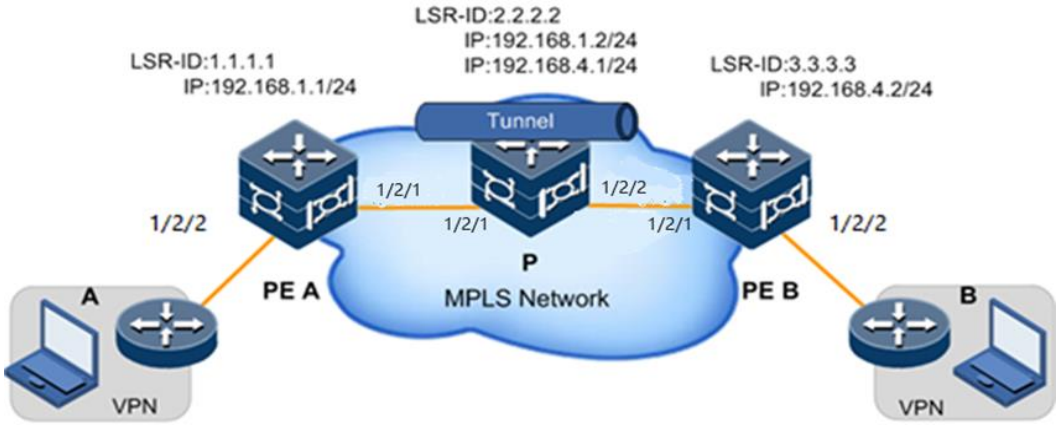
9.7.1 Example for configuring static bidirectional LSP with IP capability

Networking requirements

As shown in Figure 9-1, the user has branches in A and B, which need to communicate through a point-to-point VPN dedicated line. Because the network is small in scale and the topology is stable, a two-way static LSP can be configured between PE A and PE B as the public network tunnel of L2VPN. The default device has been configured with an IP address.

Copyright © Raisecom Technology Co., Ltd.

Figure 9-1 Networking for configuring bidirectional static LSP



Data preparation

Figure 9-2 lists the data to be prepared.

Figure 9-2 Data preparation

Device	LSR-ID	Interface	IP address
PE A	1.1.1.1	gigaethernet 1/2/1	192.168.1.1/24
		loopback 2	1.1.1.1/32
P	2.2.2.2	gigaethernet 1/2/1	192.168.1.2/24
		gigaethernet 1/2/2	192.168.4.1/24
		loopback 2	2.2.2.2/32
PE B	3.3.3.3	gigaethernet 1/2/1	192.168.4.2/24
		loopback 2	3.3.3.3/32

Configuration steps

Step 1 Configure the IP address of the loopback interface and network-side interface.

Configure PE A. The method for configuring PE A, PE B, and P devices are the same as PE A.

```
PEA#config
PEA(config)#interface loopback 2
PEA(config-loopback2)#ip address 1.1.1.1 255.255.255.255
PEA(config-loopback2)#interface gigaethernet 1/2/1
PEA(config-gigaethernet1/2/1)#ip address 192.168.1.1 255.255.255.0
PEA(config-gigaethernet1/2/1)#exit
```


Copyright © Raisecom Technology Co., Ltd.

Step 2 Enable MPLS.

Configure PE A.

```
PEA(config)#mpls lsr-id 1.1.1.1
PEA(config)#mpls enable
```

Configure the P device.

```
P(config)#mpls lsr-id 2.2.2.2
P(config)#mpls enable
```

Configure PE B.

```
PEB(config)#mpls lsr-id 3.3.3.3
PEB(config)#mpls enable
```

Step 3 Configure basic functions of the Tunnel.

Configure PE A.

```
PEA(config-tunnel1/1/1)#tunnel mode mpls
PEA(config-tunnel1/1/1)#destination 3.3.3.3
PEA(config-tunnel1/1/1)#mpls tunnel-id 1
PEA(config-tunnel1/1/1)#mpls te commit
PEA(config-tunnel1/1/1)#exit
```

Configure PE B.

```
PEB(config)#interface tunnel 1/1/1
PEA(config-tunnel1/1/1)#tunnel mode mpls
PEB(config-tunnel1/1/1)#destination 1.1.1.1
PEB(config-tunnel1/1/1)#mpls tunnel-id 1
PEB(config-tunnel1/1/1)#mpls te commit
PEB(config-tunnel1/1/1)#exit
```

Step 4 Configure static bidirectional LSP.

Configure the ingress node PE A.

```
PEA(config)#mpls bidirectional static-lsp ingress lspAB lsr-id 3.3.3.3
tunnel-id 1
```


Copyright © Raisecom Technology Co., Ltd.

```
PEA(config-ingress-lsp)#forward 3.3.3.3 255.255.255.255 nexthop
192.168.1.2 out-label 1001
PEA(config-ingress-lsp)#backward in-label 2001
```

Configure the intermediary node P.

```
P(config)#mpls bidirectional static-lsp transit lspAB lsr-id 1.1.1.1
3.3.3.3 tunnel-id 1
P(config-transit-lsp)#forward in-label 1001 nexthop 192.168.4.2 out-label
1002
P(config-transit-lsp)#backward in-label 2002 nexthop 192.168.1.1 out-
label 2001
```

Configure the egress node PE B.

```
PEB(config)#mpls bidirectional static-lsp egress lspAB lsr-id 1.1.1.1
tunnel-id 1
PEB(config-egress-lsp)#forward in-label 1002
PEB(config-egress-lsp)#backward 1.1.1.1 255.255.255.255 nexthop
192.168.4.1 out-label 2002
```

Checking results

Use the **show mpls bidirectional static-lsp** command to show whether bidirectional static LSP configurations on PE A, P, and PE B are correct.

- Configure the ingress node PE A.

```
PEA(config)#show mpls bidirectional static-lsp lspAB
LSP-Index:             1
LSP-Name:              lspAB
LSR-Role:              Ingress
LSP-Flag:              Working
Ingress-Lsr-Id:         1.1.1.1
Egress-Lsr-Id:          3.3.3.3
Tunnel-Id:             1
LSP Status:            Down
Forward Destination:    3.3.3.3
Forward In-Label:       --
Forward Out-Label:      1001
Forward In-Interface:    --
Forward Out-Interface:   --
Forward Next-Hop:       192.168.1.2
Forward Next-Mac:       --
Forward Vlan-Id:        --
Forward Svlan-Id:       --
Forward XcIndex:        2
```


Copyright © Raisecom Technology Co., Ltd.

```
Forward Ds mode:        --
Forward PipeServClass:   --
Forward Exp2LocalPriMap:  --
Forward LocalPri2ExpMap:  --
Backward Destination:    --
Backward In-Label:      2001
Backward Out-Label:     --
Backward In-Interface:   all interfaces
Backward Out-Interface:  --
Backward Next-Hop:      --
Backward Next-Mac:      --
Backward Vlan-Id:       --
Backward SVlan-Id:      --
Backward XcIndex:       3
Backward Ds mode:       uniform
Backward PipeServClass:  --
Backward Exp2LocalPriMap: Default
Backward LocalPri2ExpMap: Default
```

- Configure the intermediary node P.

```
P(config)#show mpls bidirectional static-lsp lspAB
LSP-Index:             4
LSP-Name:              lspAB
LSR-Role:              Transit
LSP-Flag:              Working
Ingress-Lsr-Id:         1.1.1.1
Egress-Lsr-Id:          3.3.3.3
Tunnel-Id:             1
LSP Status:            Down
Forward Destination:     --
Forward In-Label:       1001
Forward Out-Label:      1002
Forward In-Interface:    all interfaces
Forward Out-Interface:   --
Forward Next-Hop:       192.168.4.2
Forward Next-Mac:       --
Forward Vlan-Id:        --
Forward Svlan-Id:       --
Forward XcIndex:        2
Forward Ds mode:        --
Forward PipeServClass:   --
Forward Exp2LocalPriMap:  --
Forward LocalPri2ExpMap:  --
Backward Destination:    --
Backward In-Label:      2002
Backward Out-Label:     2001
Backward In-Interface:   all interfaces
Backward Out-Interface:  --
Backward Next-Hop:      192.168.1.1
Backward Next-Mac:      --
Backward Vlan-Id:       --
Backward SVlan-Id:      --
```


Copyright © Raisecom Technology Co., Ltd.

```
Backward XcIndex:       3
Backward Ds mode:       --
Backward PipeServClass:  --
Backward Exp2LocalPriMap: --
Backward LocalPri2ExpMap: --
```

- Configure the egress node PE B.

```
PEB(config)#show mpls bidirectional static-lsp lspAB
LSP-Index:             6
LSP-Name:              lspac
LSR-Role:              Egress
LSP-Flag:              Working
Ingress-Lsr-Id:         1.1.1.1
Egress-Lsr-Id:          3.3.3.3
Tunnel-Id:             1
LSP Status:            Down
Forward Destination:    --
Forward In-Label:       1002
Forward Out-Label:      --
Forward In-Interface:    all interfaces
Forward Out-Interface:   --
Forward Next-Hop:       --
Forward Next-Mac:       --
Forward Vlan-Id:        --
Forward Svlan-Id:       --
Forward XcIndex:        4
Forward Ds mode:        Uniform
Forward PipeServClass:   --
Forward Exp2LocalPriMap:  Default
Forward LocalPri2ExpMap:  Default
Backward Destination:    192.168.1.0
Backward In-Label:      --
Backward Out-Label:     2002
Backward In-Interface:   --
Backward Out-Interface:  --
Backward Next-Hop:      1.1.1.1
Backward Next-Mac:      --
Backward Vlan-Id:       --
Backward SVlan-Id:      --
Backward XcIndex:       5
Backward Ds mode:       --
Backward PipeServClass:  --
Backward Exp2LocalPriMap: --
Backward LocalPri2ExpMap: --
```

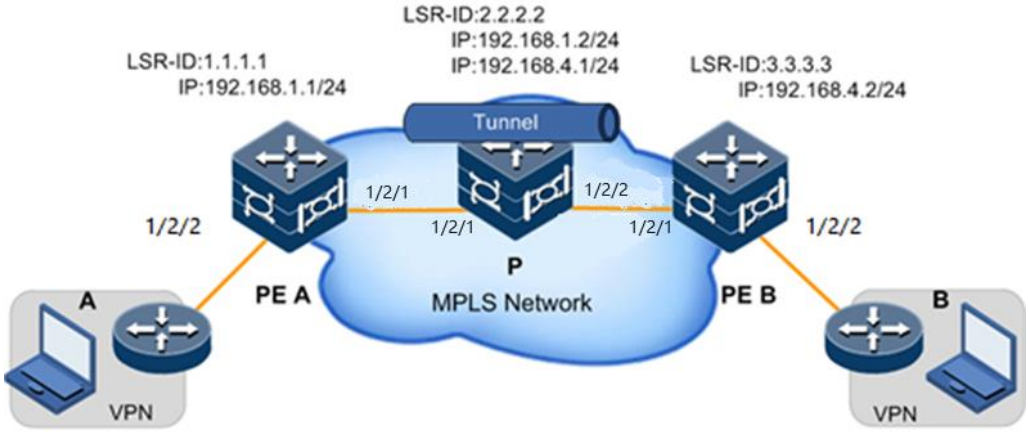

Copyright © Raisecom Technology Co., Ltd.

9.7.2 Example for configuring dynamic LSP based on LDP

Networking requirements

As shown in Figure 9-3, the user has branches in A and B, which need to communicate through a point-to-point VPN dedicated line. To facilitate network maintenance and reduce manual intervention, you need to configure a dynamic LSP between PE A and PE B as the public network tunnel of L2VPN. The default device has been configured with an IP address.

Figure 9-3 Networking for configuring LDP LSP



Data preparation

Table 9-1 lists the data to be prepared.

Table 9-1 Data preparation

Device	LSR-ID	Interface	IP address
PE A	1.1.1.1	gigaethernet 1/2/1	192.168.1.1/24
		loopback 2	1.1.1.1/32
P	2.2.2.2	gigaethernet 1/2/1	192.168.1.2/24
		gigaethernet 1/2/2	192.168.4.1/24
		loopback 2	2.2.2.2/32
PE B	3.3.3.3	gigaethernet 1/2/1	192.168.4.2/24
		loopback 2	3.3.3.3/32

Configuration steps

Step 1 Enable MPLS and LDP globally.

Copyright © Raisecom Technology Co., Ltd.

Configure PE A.

```
PEA(config)#mpls lsr-id 1.1.1.1
PEA(config)#mpls enable
PEA(config)#mpls ldp
```

Configure the P device.

```
P(config)#mpls lsr-id 2.2.2.2
P(config)#mpls enable
P(config)#mpls ldp
```

Configure PE B.

```
PEB(config)#mpls lsr-id 3.3.3.3
PEB(config)#mpls enable
PEB(config)#mpls ldp
```

Step 2 Enable LDP on the interface and configure LDP basic properties.

Configure PE A.

```
PEA(config)#interface gigaethernet 1/2/1
PEA(config-port)#ip address 192.168.1.1 255.255.255.0
PEA(config-port)#mpls ldp
PEA(config-port)#exit
```

Configure the P device.

```
P(config)#interface gigaethernet 1/2/1
P(config-port)#ip address 192.168.1.2 255.255.255.0
P(config-port)#mpls ldp
P(config-port)#interface gigaethernet 1/2/2
P(config-port)#ip address 192.168.4.1 255.255.255.0
P(config-port)#mpls enable
P(config-port)#mpls ldp
P(config-port)#exit
```

Configure PE B.

Copyright © Raisecom Technology Co., Ltd.

```
PEB(config)#interface gigaethernet 1/2/1
PEB(config-port)#ip address 192.168.4.2 255.255.255.0
PEB(config-port)#mpls ldp
PEB(config-port)#exit
```

Step 3 Configure the IP address and OSPF routes of the loopback interface.

Configure PE A.

```
PEA(config)#interface loopback 2
PEA(config-loopbackif)#ip address 1.1.1.1 255.255.255.0
PEA(config-loopbackif)#exit
PEA(config)#router ospf 1
PEA(config-router-ospf)#network 1.1.1.1 255.255.255.255 area 0.0.0.0
PEA(config-router-ospf)#network 192.168.1.1 255.255.255.255 area 0.0.0.0
PEA(config-router-ospf)#exit
```

Configure the P device.

```
P(config)#interface loopback 2
P(config-loopbackif)#ip address 2.2.2.2
P(config)#router ospf 1
P(config-router-ospf)#network 2.2.2.2 255.255.255.255 area 0.0.0.0
P(config-router-ospf)#network 192.168.1.2 255.255.255.255 area 0.0.0.0
P(config-router-ospf)#network 192.168.4.1 255.255.255.255 area 0.0.0.0
P(config-router-ospf)#exit
```

Configure PE B.

```
PEB(config)#interface loopback 2
PEB(config-loopbackif)#ip address 3.3.3.3 255.255.255.0
PEB(config)#router ospf 1
PEB(config-router-ospf)#network 3.3.3.3 255.255.255.255 area 0.0.0.0
PEB(config-router-ospf)#network 192.168.4.2 255.255.255.255 area 0.0.0.0
PEB(config-router-ospf)#exit
```

Step 4 Triger the device to assign LSP labels for all IP prefixes.

Configure PE A.

```
PEA(config)# mpls ldp lsp-trigger all
```

Configure the P device.

Copyright © Raisecom Technology Co., Ltd.

```
P(config)# mpls ldp lsp-trigger all
```

Configure PE B.

```
PEB(config)# mpls ldp lsp-trigger all
```

Checking results

Use the **show mpls lsp** command to show whether configurations are correct.

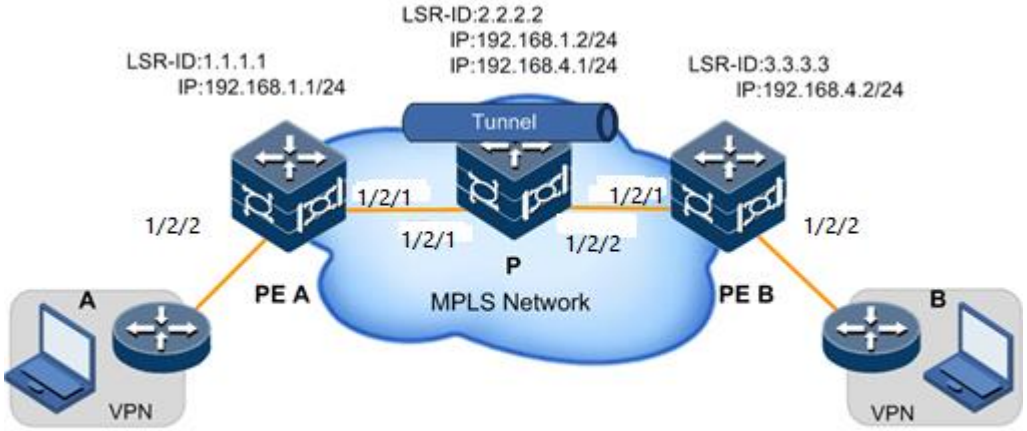
```
PEA(config)#show mpls lsp
LSR-Type    FEC                In/Out-Label         In/Out-IF      Next-Hop
LSP-Status LSP-Type  LSP-Flag XCIndex
--------------------------------------------------------------------------
Ingress     3.3.3.3             --/10246            --/GE1/2/1
192.168.1.2      Up        Ldp      Working  11
Ingress     192.168.4.2          --/10248            --/GE1/2/1
192.168.1.2      Up        Ldp      Working  13
```

9.7.3 Example for configuring dynamic LSP based on RSVP-TE

Networking requirements

As shown in Figure 9-4, the user has branches in A and B, which need to communicate through a point-to-point VPN dedicated line. To provide accurate bandwidth assurance, you can configure RSVP-TE LSP between PE A and PE B as the public network tunnel of L2VPN. The default device has been configured with an IP address.

Figure 9-4 Networking for configuring RSVP-TE LSP



Copyright © Raisecom Technology Co., Ltd.

Data preparation

Table 9-2 lists data to be configured.

Table 9-2 Data preparation

Device	LSR-ID	Interface	IP address
PE A	1.1.1.1	gigaethernet 1/2/1	192.168.1.1/24
		loopback 2	1.1.1.1/32
P	2.2.2.2	gigaethernet 1/2/1	192.168.1.2/24
		gigaethernet 1/2/2	192.168.4.1/24
		loopback 2	2.2.2.2/32
PE B	3.3.3.3	gigaethernet 1/2/1	192.168.4.2/24
		loopback 2	3.3.3.3/32

Configuration steps

Step 1 Configure RSVP-TE basic functions

Configure PE A.

```
PEA#config
PEA(config)#interface loopback 2
PEA(config-loopback2)#ip address 1.1.1.1 255.255.255.255
PEA(config-loopback2)#interface gigaethernet 1/2/1
PEA(config-gigaethernet1/2/1)#ip address 192.168.1.1 255.255.255.0
PEA(config-gigaethernet1/2/1)#exit
PEA(config)#mpls lsr-id 1.1.1.1
PEA(config)#mpls enable
PEA(config)#mpls rsvp-te
PEA(config)#interface gigaethernet 1/2/1
PEA(config-gigaethernet1/2/1)#mpls rsvp-te
PEA(config-gigaethernet1/2/1)#exit
```

Configure the P device.

```
P#config
P(config)#interface loopback 2
P(config-loopback2)#ip address 2.2.2.2 255.255.255.255
P(config-loopback2)#interface gigaethernet 1/2/1
P(config-gigaethernet1/2/1)#ip address 192.168.1.2 255.255.255.0
P(config-gigaethernet1/2/1)#interface gigaethernet 1/2/2
P(config-gigaethernet1/2/2)#ip address 192.168.4.1 255.255.255.0
P(config-gigaethernet1/2/2)#exit
```


Copyright © Raisecom Technology Co., Ltd.

```
P(config)#mpls lsr-id 2.2.2.2
P(config)#mpls enable
P(config)#mpls rsvp-te
P(config)#interface gigaethernet 1/2/1
P(config-gigaethernet1/2/1)#mpls rsvp-te
P(config-gigaethernet1/2/1)#interface gigaethernet 1/2/2
P(config-gigaethernet1/2/2)#mpls rsvp-te
P(config-gigaethernet1/2/2)#exit
```

Configure PE B.

```
PEB#config
PEB(config)#interface loopback 2
PEB(config-loopback2)#ip address 3.3.3.3 255.255.255.255
PEB(config-loopback2)#interface gigaethernet 1/2/1
PEB(config-gigaethernet1/2/1)#ip address 192.168.1.1 255.255.255.0
PEB(config-gigaethernet1/2/1)#exit
PEB(config)#mpls lsr-id 3.3.3.3
PEB(config)#mpls enable
PEB(config)#mpls rsvp-te
PEB(config)#interface gigaethernet 1/2/1
PEB(config-gigaethernet1/2/1)#ip address 192.168.4.2 255.255.255.0
PEB(config-gigaethernet1/2/1)#mpls rsvp-te
PEB(config-gigaethernet1/2/1)#exit
```

Step 2 Configure the explicit path.

Configure PE A.

```
PEA(config)#mpls explicit-path PathAB
PEA(config-mpls-exp-path)#next-hop 192.168.1.2 strict
PEA(config-mpls-exp-path)#next-hop 192.168.4.2 strict
```

Configure PE B.

```
PEB(config)#mpls explicit-path PathBA
PEB(config-mpls-exp-path)#next-hop 192.168.4.1 strict
PEB(config-mpls-exp-path)#next-hop 192.168.1.1 strict
```

Step 3 Configure the RSVP-TE tunnel.

Configure PE A.

```
PEA(config)#interface tunnel 1/1/1
```


Copyright © Raisecom Technology Co., Ltd.

```
PEA(config-tunnel1/1/1)#tunnel mode mpls
PEA(config-tunnel1/1/1)#destination 3.3.3.3
PEA(config-tunnel1/1/1)#mpls signal-protocol rsvp-te
PEA(config-tunnel1/1/1)#mpls tunnel-id 101
PEA(config-tunnel1/1/1)#mpls explicit-path PathAB
PEA(config-tunnel1/1/1)#mpls te commit
```

Configure PE B.

```
PEB(config)#interface tunnel 1/1/1
PEB(config-tunnel1/1/1)#tunnel mode mpls
PEB(config-tunnel1/1/1)#destination 1.1.1.1
PEB(config-tunnel1/1/1)#mpls signal-protocol rsvp-te
PEB(config-tunnel1/1/1)#mpls tunnel-id 101
PEB(config-tunnel1/1/1)#mpls explicit-path PathAB
PEB(config-tunnel1/1/1)#mpls te commit
```

Checking results

Use the **show mpls rsvp-te lsp** command to check LSP configurations on the PE A, PE B, and P devices.

- Configure the ingress node PE A.

```
PEA(config)#show mpls rsvp-te lsp
```

- Configure the intermediary node P.

```
P(config)#show mpls rsvp-te lsp
```

- Configure the ingress node PE B.

```
PEB(config)#show mpls rsvp-te lsp
```


Copyright © Raisecom Technology Co., Ltd.

10 Segment Routing

This chapter describes principles and configuration procedures of segment routing, including following sections:

- Configuring ISIS to additionally support SR
- Configuring OSPFv2 to additionally support SR
- Configuring OSPFv3 to additionally support SR
- Configuring SR-MPLS
- Configuring SRv6
- Configuring SRv6 network slicing
- Configuration examples

10.1 Configuring ISIS to additionally support SR

Before configuring SR based on ISIS, use the **metric-style wide** command to configure the overhead type of ISIS to wide.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router isis [ area-tag ]`	Start an ISIS process. Enter ISIS configuration mode.
3	`Raisecom(config-router-isis)#segment-routing mpls`	Enable Segment Routing (SR) in the ISIS process. The forwarding plane is MPLS.
	`Raisecom(config-router-isis)#segment-routing ipv6 locator locname [ auto-sid-disable ]`	Enable SRv6 in the ISIS process.
4	`Raisecom(config-router-isis)#segment-routing global-block begin_label_value-end_label_value`	Configure the label segment range of the global label block of the SR in the ISIS process.
5	`Raisecom(config-router-isis)#loop-free-alternate [ level-1 | level-1-2 | level-2 ]`	Enable IS-IS Auto FRR, which calculates loop-free alternate route through LFA.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config-router-isis)#**ipv6 loop-free-alternate** [**level-1** | **level-1-2** | **level-2**]	
6	Raisecom(config-router-isis)#**ti-lfa** { **level-1** | **level-1-2** | **level-2** }	Enable FRR based on TILFA.
	Raisecom(config-router-isis)#**ipv6 ti-lfa** { **level-1** | **level-1-2** | **level-2** }	
7	Raisecom(config-router-isis)#**exit** Raisecom(config)#**interface loopback** *loopback-num*	Enter loopback interface configuration mode.
8	Raisecom(config-loopback)#**isis prefix-sid** { **absolute** *sid_value* | **index** *index_value* } [**node-disable**] [**php-off** | **explicit-null**]	Configure the SID of the loopback interface. Then, the LSP of ISIS carriers the SID index of the prefix.

10.2 Configuring OSPFv2 to additionally support SR

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**vrf** *vrf-name*] [**router-id** *router-id*]	Start an ISIS process. Enter ISIS configuration mode.
3	Raisecom(config-router-ospf)#**bgp-ls enable**	Enable topology reporting in the OSPF process. After BGP-LS is configured, OSPF reports topology information to BGP.
4	Raisecom(config-router-ospf)#**bgp-ls identifier** *value*	Configure the BGP link status ID, which identify the BGP-LS.
5	Raisecom(config-router-ospf)#**segment-routing mpls**	Enable SR in the OSPF process. The forwarding plane is MPLS.
6	Raisecom(config-router-ospf)#**segment-routing global-block** *begin_label_value-end_label_value*	Configure the label segment range of the global label block of the SR in the OSPF process.
7	Raisecom(config-router-ospf)#**loop-free-alternate**	Enable OSPF Auto FRR, which calculates loop-free alternate route through LFA.
8	Raisecom(config-router-ospf)#**ti-lfa enable**	Enable FRR based on TILFA.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
9	Raisecom(config-router-ospf)#**segment-routing avoid-microloop** [**rip-update-delay** *timer*]	Enable SR anti-micro-loop, and configure the delay time for SR anti-micro-loop. After anti-micro-loop is enabled, OSPF calculates the anti-micro-loop table when the routes change, and issues the calculated anti-micro-loop table to the RM. By default, anti-micro-loop is disabled. After anti-micro-loop is enabled, the default delay time for anti-micro-loop is 5000ms.
10	Raisecom(config-router-ospf)#**exit** Raisecom(config)#**interface loopback** *loopback-num*	Enter loopback interface configuration mode.
11	Raisecom(config-loopback)#**ip ospf prefix-sid** { **absolute** *sid_value* | **index** *index_value* } [**node-disable**] [**php-off** | **explicit-null**]	Configure the SID of the loopback interface. Then, the LSP of OSPF carriers the SID index of the prefix.

10.3 Configuring OSPFv3 to additionally support SR

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	Start an OSPFv3 process. Enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**segment-routing ipv6 locator** *locname* [**auto-sid-disable**]	Enable SRv6 in the OSPFv3 process.
4	Raisecom(config-ospf6)#**loop-free-alternate**	Enable OSPFv3 Auto FRR, which calculates loop-free alternate route through LFA.
5	Raisecom(config-ospf6)#**ti-lfa enable**	Enable FRR based on TILFA.
6	Raisecom(config-ospf6)#**segment-routing avoid-microloop** [**rip-update-delay** *timer*]	Enable SRv6 anti-micro-loop, and configure the delay time for SRv6 anti-micro-loop. After anti-micro-loop is enabled, OSPF calculates the anti-micro-loop table when the routes change, and issues the calculated anti-micro-loop table to the RM. By default, anti-micro-loop is disabled. After anti-micro-loop is enabled, the default delay time for anti-micro-loop is 5000ms.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
7	Raisecom(config-ospf6)#**segment-routing ipv6 sid-sub-tlv-type** { **end-x** | **lan-end-x** } *sub-tlv-type*	After SRv6 is enabled, OSPFv3 will advertise related information about the end.x sid and lan-end-x sid in its generated ext-router-lsa. When the corresponding sub-tlv type values configured for different devices are inconsistent, they cannot be parsed properly. Configure this command to make the corresponding sub-tlv types consistent across different devices. By default, the end-x type is 31, and the lan-end-x is type is 32.

10.4 Configuring SR-MPLS

10.4.1 Preparing for configurations

Scenario

To import SR into the existing MPLS frame and expand and optimize the existing IGP and BGP, configure the SR-MPLS tunnel so as to transmit EVPN services and other services.

Prerequisites

- Configure basic functions of MPLS.
- Configuring basic functions of routing.

10.4.2 Configuring SR-MPLS BE

Configuring the prefix SR

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**segment-routing**	Enable global SR, and enter SR configuration mode.
3	Raisecom(segment-routing)#**global-block** *begin_label_value-end_label_value*	Configure the label segment range of the global label block of SR.
4	Raisecom(segment-routing)#**tunnel-prefer segment-routing**	Configure the tunnel to preferentially select the path based on SR.

Copyright © Raisecom Technology Co., Ltd.

Configuring the adjacent SR

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**segment-routing**	Enable global SR, and enter SR configuration mode.
3	Raisecom(segment-routing)#**local-block** *begin_label_value-end_label_value*	Configure the label segment range of the global label block of SR.
4	Raisecom(segment-routing)#**ipv4 adjacency local-ip-addr** *ip-address* **remote-ip-addr** *ip-address* **sid** { *min_index_value-max_index_value* }	Configure the SID range of the adjacent link of the SR node.
5	Raisecom(segment-routing)#**tunnel-prefer segment-routing**	Configure the tunnel to preferentially select the path based on SR.

Configuring the mapping of SR and LDP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**segment-routing**	Enable global SR, and enter SR configuration mode.
3	Raisecom(segment-routing)#**mapping-server prefix-sid-mapping** *ip-address mask-length index-segment* [**range** *range-value*]	Configure the mapping between the prefix address and SID.

10.4.3 Configuring SR-MPLS TE

Configuring SR-MPLS TE label stack

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls explicit-path** *path-name*	Create an MPLS-TE explicit path, and enter explicit path configuration mode.
3	Raisecom(config-mpls-exp-path)#**next-sid** [**index** *index-number*] **label** *label-value* **type** { **adjacency** | **binding-sid** | **prefix** }	Configure the next node of the explicit path.

Copyright © Raisecom Technology Co., Ltd.

Configuring SR-MPLS TE static tunnel

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#**destination** *ip-address*	Configure the destination IP address of the tunnel interface.
4	Raisecom(config-tunnelif)#**mpls signal-protocol** { **rsvp-te** | **static** | **segment-routing** }	Configure the protocol type of the tunnel interface to segment-routing. By default, it is static.
5	Raisecom(config-tunnelif)#**mpls tunnel-id** *tunnel-id*	Configure the tunnel ID of the tunnel interface.
6	Raisecom(config-tunnelif)#**mpls explicit-path** *path-name* [**secondary**]	Configure the explicit path associated with the tunnel interface.
7	Raisecom(config-tunnelif)#**mpls te commit**	Commit properties of the tunnel interface.

Configuring hot backup of the SR-MPLS TE static channel

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#**destination** *ip-address*	Configure the destination IP address of the tunnel interface.
4	Raisecom(config-tunnelif)#**mpls signal-protocol** { **rsvp-te** | **static** | **segment-routing** }	Configure the protocol type of the tunnel interface to segment-routing. By default, it is static.
5	Raisecom(config-tunnelif)#**mpls tunnel-id** *tunnel-id*	Configure the tunnel ID of the tunnel interface.
6	Raisecom(config-tunnelif)#**mpls te hot-standby** [**overlap** | **wtr** *second*]	Enable hot backup of the tunnel.
7	Raisecom(config-tunnelif)#**mpls explicit-path** *path-name*	Configure the explicit path associated with the tunnel interface.
8	Raisecom(config-tunnelif)#**mpls explicit-path** *path-name* **secondary**	Configure the backup explicit path associated with the tunnel interface.
9	Raisecom(config-tunnelif)#**mpls te sbfd**	Enable LSP SBFD session of the tunnel.
10	Raisecom(config-tunnelif)#**mpls te sbfd secondary**	Enable backup LSP SBFD session of the tunnel.
11	Raisecom(config-tunnelif)#**mpls te commit**	Commit properties of the tunnel interface.

Copyright © Raisecom Technology Co., Ltd.

Configure the SBFD session of the SR-MPLS TE tunnel LSP

The static SR-TE cannot sense the fault of the LSP path, so SBFD must be configured as a detection method accordingly.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#**destination** *ip-address*	Configure the destination IP address of the tunnel interface.
4	Raisecom(config-tunnelif)#**mpls signal-protocol** { **rsvp-te** | **static** | **segment-routing** }	Configure the protocol type of the tunnel interface to segment-routing. By default, it is static.
5	Raisecom(config-tunnelif)#**mpls tunnel-id** *tunnel-id*	Configure the tunnel ID of the tunnel interface.
6	Raisecom(config-tunnelif)#**mpls te sbfd** [**min-tx-interval** *interval-value*] [**detect-multiplier** *multiplier-value*]	Configure the internal for sending SBFD sessions and detection multiples.
7	Raisecom(config-tunnelif)#**mpls te commit**	Commit properties of the tunnel interface.

Configuring the binding label of the SR-MPLS TE tunnel.

When the static SR-TE tunnel is bound with the binding-sid label, it can be used in the label stack of the MPLS explicit path and can be used to implement tunnel binding. This is used in the cross-domain SR-MPLS TE scenario.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#**destination** *ip-address*	Configure the destination IP address of the tunnel interface.
4	Raisecom(config-tunnelif)#**mpls signal-protocol** { **rsvp-te** | **static** | **segment-routing** }	Configure the protocol type of the tunnel interface to segment-routing. By default, it is static.
5	Raisecom(config-tunnelif)#**mpls tunnel-id** *tunnel-id*	Configure the tunnel ID of the tunnel interface.
6	Raisecom(config-tunnelif)#**mpls te binding-sid label** *label-value*	Configure the binding label of the SR-MPLS TE tunnel.

Copyright © Raisecom Technology Co., Ltd.

10.5 Configuring SRv6

10.5.1 Configuring SRv6 BE

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**segment-routing ipv6**	Enable global SRv6, and enter SRv6 configuration mode.
3	Raisecom(segment-routing-ipv6)#**encapsulation source-address** *ipv6-address* [**ip-ttl** *ttl_value*]	Configure the source address of the IPv6 packet header to be encapsulated for transmitting data in the IPv6 over SRv6 networking environment.
4	Raisecom(segment-routing-ipv6)#**locator** *locname* **ipv6-prefix** *ipv6-addr/mask-length* [**static** *length*] [**args** *length*]	Configure the locator segment, and enter SRv6 Locator configuration mode.
5	Raisecom(segment-routing-locator)#**opcode** *opcode-id* **end**	Configure the SRv6 SID with functions of the End type, used to identify the address prefix of a destination address on the network.
	Raisecom(segment-routing-locator)#**opcode** *opcode-id* **end-otp**	Configure the SRv6 SID with functions of the End-OTP type.
	Raisecom(segment-routing-locator)#**opcode** *opcode-id* **end-x** *interface-type interface-num* **nexthop** *ipv6-addr*	Configure the SID with functions of the End.X SID type, used to identify a link on the network.
	Raisecom(segment-routing-locator)#**opcode** *opcode-id* { **end-dt4** | **end-dt6** } [**vrf** *vrfname* [**evpn** | **evpn-l3vpn**]]	Configure the SID with functions of the End.DT type, used to identify an IP VPN on the network. The forwarding action corresponding to the End.DT SID is to de-encapsulate packets and to query the IP VPN instance routing table for forwarding. The End.DT SID is used in the IP L3VPN and IP EVPN L3VPN scenarios.
	Raisecom(segment-routing-locator)#**opcode** *opcode-id* { **end-dt2m** | **end-dt2u** } **evpn-vpls** *evpn-vpls-instance-id*	Configure the SID type to End. DT2, used in the EVPN VPLS scenario.
	Raisecom(segment-routing-locator)# **opcode** *opcode-id* { **end-dx2** | **end-dx2l** } **evpl-instance** *instance-id*	Configure the SID with functions of the End.DX2 type, used in the EVPL scenario.

10.5.2 Configuring SRv6 TE Policy

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**segment-routing ipv6**	Enable global SRv6, and enter SRv6 configuration mode.
3	Raisecom(segment-routing-ipv6)#**srv6 segment-list** *listname*	Create an SRv6 segment list, and enter SRv6 segment list configuration mode.

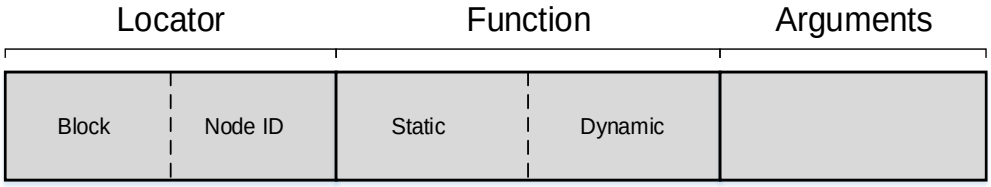
Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(segment-routing-ipv6-list)# **index** *index-value* **sid ipv6** *srv6-sid* [**compress block** *block-length*]	Configure the SRv6 SID corresponding with the index in the SRv6 segment list. Support the SRv6 TE policy compression.
5	Raisecom(segment-routing-ipv6-list)#**exit** Raisecom(segment-routing-ipv6)#**srv6 policy color** *color-value* **endpoint** *ipv6-addr*	Create a static SRv6 policy, and enter SRv6 policy configuration mode.
6	Raisecom(config-sr-policy)#**backup hot-standby** { **enable** | **disable** }	Enable SRv6 hot backup. By default, it is disabled.
7	Raisecom(config-sr-policy)#**srv6 candidate-path preference** *preference-value* **explicit segment-list** *listname*	Configure the priority of the SRv6 candidate path and the associated segment list.
8	Raisecom(config-sr-policy)#**exit** Raisecom(segment-routing-ipv6)#**srv6 policy commit**	Commit the modification of the SRv6 policy.

10.5.3 Configuring SRv6 compression

Locator compression

The SRv6 SID uses the IPv6 address format, but does not correspond to any interface address on any device. It consists of three parts: Locator (which can be further divided into the Block and Node ID), Function (which can be further divided into the static segment and dynamic segment), and Arguments (namely, parameter segment).



The Locator identifies the network segment to which the SID belongs. In fact, the Block is the same in the same scenario, so the only variable parts are the Node ID and Function. By configuring SID compression, packet overhead can be reduced and bearer efficiency can be improved.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**segment-routing ipv6**	Enable global SRv6, and enter SRv6 configuration mode.
3	Raisecom(segment-routing-ipv6)#**locator** *locname* **ipv6-prefix** *ipv6-addr/mask-length* **compress block** *length* **compress-static** *length* [**static** *length*] [**args** *length*]	Configure the length of SID compression.

Copyright © Raisecom Technology Co., Ltd.

Opcode compression

The Opcode segment (namely, the Function segment) identifies the network functions of the device, such as forwarding packets and executing specific services. After receiving the service packets, the device node in the SR domain performs relevant operations based on the Opcode segment of the SRv6 SID. The device supports the following compression behaviors:

- Penultimate Segment POP of the SRH (PSP): to reduce the burden on the tail node of the SRv6 network and improve forwarding efficiency, remove the SRH from the penultimate SRv6 node. The tail node does not need to view the SRH information, but only needs to search the Local SID table based on the destination IPv6 address for processing.
- Ultimate Segment POP of the SRH (USP): on the SRv6 VPN network, after the PE node finds the corresponding forwarding action based on the SID, it performs the SRH removal operation and forwards the packet to the CE.
- Ultimate Segment Decomposition (USD): in the TI-LFA scenario, the last endpoint node of the Repair List needs to remove the outer IPv6 header and forward the inner packet to the destination node.
- Continue of Compression (COC): used in SID compression scenarios to reduce SRH size

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**segment-routing ipv6**	Enable global SRv6, and enter SRv6 configuration mode.
3	Raisecom(segment-routing-ipv6)#**locator** *locname* **ipv6-prefix** *ipv6-addr/mask-length* [**static** *length*] [**args** *length*]	Configure the locator segment, and enter SRv6 locator configuration mode.
4	Raisecom(segment-routing-locator)#**opcode compress** *opcode-id* **end** [**coc** | **psp** | **psp-coc** | **psp-usp-usd** | **psp-usp-usd-coc**]	Configure the compression behavior of the opcode segment of the End type.
5	Raisecom(segment-routing-locator)#**opcode compress** *opcode-id* **end-x** *interface-type interface-num* **nexthop** *ipv6-addr* [**coc** | **psp** | **psp-coc** | **psp-usp-usd** | **psp-usp-usd-coc**]	Configure the compression behavior of the opcode segment of the End.X type.

10.5.4 Checking results

No.	Command	Description
1	Raisecom(config)#**show srv6 segment-list** [**detail**]	Show information about the SRv6 segment list.
2	Raisecom(config)#**show srv6 policy** [**color** *color-value* **endpoint** *ipv6-addr*] [**detail**]	Show information about the SRv6 Policy.

Copyright © Raisecom Technology Co., Ltd.

10.6 Configuring SRv6 network slicing

SRv6 network slicing can slice an SRv6 network into multiple virtual networks, which are independent from each other. You can deploy different policies on different virtual networks according to service characteristics of tenants to meet their requirements.

10.6.1 Configuring basic information about network slicing

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**network-slice encapsulation ipv6-source**	Configure the encapsulation type of network slicing.
3	Raisecom(config)#**network-slice statistics** { **enable** | **disable** }	Enable network slicing statistics.
4	Raisecom(config)#**clear network-slice statistics** [**slice-id** *slice-instance-id*] [**interface** *interface-type interface-number*]	(Optional) clear network slicing statistics.

10.6.2 Configuring the network slicing instance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**network-slice instance** *instance-id*	Create a network slicing instance, and enter network slicing instance configuration mode.
3	Raisecom(config-slice)#**description** *string*	Configure the description of the network slicing instance.

10.6.3 Configuring the prefix of network slicing

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**network-slice prefix** *prefix-name*	Create a network slicing instance, and enter network slicing instance configuration mode.
3	Raisecom(config-prefix)#**ipv6-prefix** *ipv6-addr/mask-length* **slice-prefix-len** *slice-lenth*	Configure the slicing prefix of the network slicing instance.

Copyright © Raisecom Technology Co., Ltd.

10.6.4 Configuring network slicing on the interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode or slicing network virtual Ethernet interface configuration mode.
3	Raisecom(config-port)#**network-slice** { **enable** | **disable** }	Enable network slicing on the interface.
4	Raisecom(config-port)#**slice-id** *slice-instance-id* **flex-channel** *bandwidth*	Configure the network slicing ID associated with the interface and its bandwidth.

10.6.5 Checking configurations

No.	Command	Description
1	Raisecom#**show network-slice configuration**	Show basic configurations of network slicing.
2	Raisecom#**show network-slice prefix** [*prefix-name*]	Show prefix configurations of network slicing.
3	Raisecom#**show network-slice slice-id** [*slice-instance-id*]	Show instance configurations of network slicing.
4	Raisecom#**show network-slice binding-list** [**slice-id** *slice-instance-id*] [**interface** *interface-type interface-number*]	Show the binding relation of the network slicing instance and interface.
5	Raisecom#**show network-slice statistics** [**slice-id** *slice-instance-id*] [**interface** *interface-type interface-number*]	Show network slicing statistics.

10.7 Configuration examples

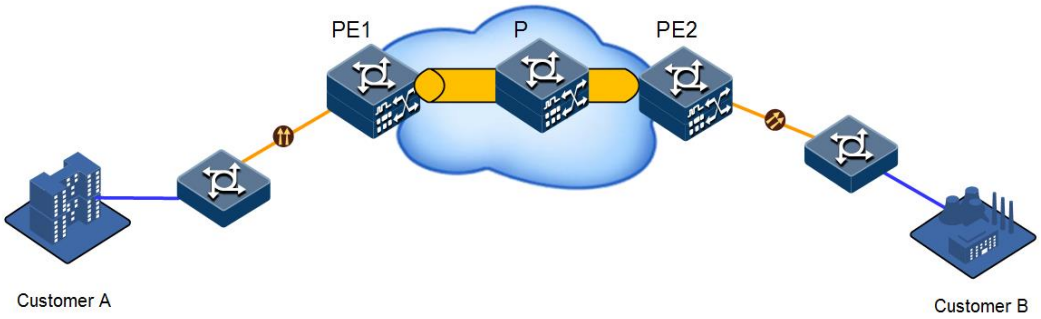
10.7.1 Example for configuring EVPN VPWS for SRv6-TE Policy

Networking requirements

As shown in Figure 10-1, PE 1 and PE 2 are located in two places, and they require leased lines for communication in point-to-point mode. Create an EVPN-VPWS instance, provide a P2P L2VPN service scheme, and use the SR-TE tunnelling technology to traverse the backbone network, and provide the method for forwarding Layer 2 packets without querying the MAC address table for the connection between client A and client B.

Copyright © Raisecom Technology Co., Ltd.

Figure 10-1 Configuring EVPN VPWS for SRv6-TE



Preparing data

Prepare data as listed in Table 10-1.

Table 10-1 Preparing data

Device	Client-side interface	Network-side interface	LSR ID
PE 1	1/1/4	1/1/3	1.1.1.1
P	1/1/1 (PE1 side)	1/2/24 (PE2 side)	3.3.3.3
PE 2	1/1/15	1/2/22	2.2.2.2

Configuration thoughts

- Establish an SRv6-TE tunnel based on ISIS or OSPF. Assign SID label addresses of the SRv6-TE tunnel.
- Configure EVPN VPWS.

Configuring routing

- Configure PE 1.

```
PE1(config)#interface loopback 2
PE1(config-loopback)#ip address 1.1.1.1 255.255.255.255
PE1(config-loopback)# ipv6 address 1::1/128
PE1(config-loopback)#ip router isis 10
PE1(config-loopback)#ipv6 ospf 1000 area 0.0.0.0

PE1(config)#interface tengigabitethernet 1/1/3.100
PE1(config-tengigabitethernet 1/1/3.100)#encapsulation dot1Q 100
PE1(config-tengigabitethernet 1/1/3.100)#ipv6 address 2010::1/64
PE1(config-tengigabitethernet 1/1/3.100)#ipv6 ospf 1000 area 0.0.0.0
PE1(config-tengigabitethernet 1/1/3.100)#ipv6 router isis 10

PE1(config)#router isis 10
PE1(config-router-isis)#net 10.0000.0000.0001.00
PE1(config-router-isis)#metric-style wide
```


Copyright © Raisecom Technology Co., Ltd.

```
PE1(config-router-isis)#segment-routing ipv6 locator 88-E-18 /*bind the
locator based on SRv6 */

PE1(config)#ipv6 router ospf 1000
PE1(config-router-ospf)#router-id 1.1.1.1
PE1(config-router-ospf)#segment-routing ipv6 locator 88-E-18 /* bind the
locator based on SRv6 */
```

- Configure the P.

```
P(config)#interface loopback 2
P(config-loopback)#ip address 3.3.3.3 255.255.255.255
P(config-loopback)# ipv6 address 3::3/128
P(config-loopback)#ip router isis 10
P(config-loopback)#ipv6 ospf 1000 area 0.0.0.0

P(config)#interface tengigabitethernet 1/1/3.100
P(config-tengigabitethernet 1/1/3.100)#encapsulation dot1Q 100
P(config-tengigabitethernet 1/1/3.100)#ipv6 address 2010::2/64
P(config-tengigabitethernet 1/1/3.100)#ipv6 ospf 1000 area 0.0.0.0
P(config-tengigabitethernet 1/1/3.100)#ipv6 router isis 10

P(config)#interface tengigabitethernet 1/2/24.100
P(config-tengigabitethernet 1/2/24.100)#encapsulation dot1Q 100
P(config-tengigabitethernet 1/2/24.100)#ipv6 address 2110::2/64
P(config-tengigabitethernet 1/2/24.100)#ipv6 ospf 1000 area 0.0.0.0
P(config-tengigabitethernet 1/2/24.100)#ipv6 router isis 10

P(config)#router isis 10
P(config-router-isis)#net 10.0000.0000.0003.00
P(config-router-isis)#metric-style wide
P(config-router-isis)#segment-routing ipv6 locator 721-B-15 /* bind the
locator based on SRv6 */

P(config)#ipv6 router ospf 1000
P(config-router-ospf)#router-id 3.3.3.3
P(config-router-ospf)#segment-routing ipv6 locator 721-B-15 /* bind the
locator based on SRv6 */
```

- Configure PE 2.

```
PE2(config)#interface loopback 2
PE2(config-loopback)#ip address 2.2.2.2 255.255.255.255
PE2(config-loopback)# ipv6 address 2::2/128
PE2(config-loopback)#ip router isis 10
PE2(config-loopback)#ipv6 ospf 1000 area 0.0.0.0

PE2(config)#interface tengigabitethernet 1/2/24.100
PE2(config-tengigabitethernet 1/2/24.100)#encapsulation dot1Q 100
PE2(config-tengigabitethernet 1/2/24.100)#ipv6 address 2110::1/64
```


Copyright © Raisecom Technology Co., Ltd.

```
PE2(config-tengigabitethernet 1/2/24.100)#ipv6 ospf 1000 area 0.0.0.0
PE2(config-tengigabitethernet 1/2/24.100)#ipv6 router isis 10

PE2(config)#router isis 10
PE2(config-router-isis)#net 10.0000.0000.0002.00
PE2(config-router-isis)#metric-style wide
PE2(config-router-isis)#segment-routing ipv6 locator 721-B-31 /* bind the
locator based on SRv6 */

PE2(config)#ipv6 router ospf 1000
PE2(config-router-ospf)#router-id 2.2.2.2
PE2(config-router-ospf)#segment-routing ipv6 locator 721-B-31 /* bind the
locator based on SRv6 */
```

Configuring the SRv6-TE Policy

- Configure PE 1.

```
PE1(config)#segment-routing ipv6
PE1(segment-routing-ipv6)#encapsulation source-address 1::1
PE1(segment-routing-ipv6)#locator 88-E-18 ipv6-prefix 2023::/64 static
8/*statically configure end-x sid address */
PE1(segment-routing-ipv6-locator-88-E-18)#opcode ::3 end-x
tengigabitethernet 1/2/3.100 nexthop fe80::20e:5eff:fe39:5406
PE1(segment-routing-ipv6-locator-88-E-18)#opcode ::ab end
PE1(segment-routing-ipv6-locator-88-E-18)#exit
PE1(segment-routing-ipv6)#srv6 segment-list sp/* show the path list,
composed of the end SID, end-x SID, or both */
PE1(segment-routing-ipv6-list)#index 1 sid ipv6 2023::3/* if the end-x
SID is used, the fist hop must be the egress interface of the local
device */
PE1(segment-routing-ipv6-list)#index 2 sid ipv6 1401:721::30
PE1(segment-routing-ipv6-list)#exit
```

- Configure the P.

```
P(config)#segment-routing ipv6
P(segment-routing-ipv6)#encapsulation source-address 3::3
P(segment-routing-ipv6)#locator 721-B-15 ipv6-prefix 1401:721::/64 static
16
P(segment-routing-ipv6-locator-721-B-15)#opcode ::10 end
P(segment-routing-ipv6-locator-721-B-15)#opcode ::20 end-x
tengigabitethernet 1/1/3.100 nexthop fe80::20e:5eff:feaa:1139
P(segment-routing-ipv6-locator-721-B-15)#opcode ::30 end-x
tengigabitethernet 1/2/24.100 nexthop fe80::20e:91ff:fe58:152c
P(segment-routing-ipv6-locator-721-B-15)#exit
```

- Configure PE 2.

Copyright © Raisecom Technology Co., Ltd.

```
PE2(config)#segment-routing ipv6
PE2(segment-routing-ipv6)#encapsulation source-address 2::2
PE2(segment-routing-ipv6)#locator 721-B-31 ipv6-prefix 2902:721::/64
static 32
PE2(segment-routing-ipv6-locator-721-B-31)#opcode ::1 end
PE2(segment-routing-ipv6-locator-721-B-31)#opcode ::3 end-x
tengigabitethernet 1/2/22.100 nexthop fe80::20e:5eff:fe39:542f
PE2(segment-routing-ipv6-locator-721-B-31)#exit
PE2(segment-routing-ipv6)#srv6 segment-list sp
PE2(segment-routing-ipv6-list)#index 1 sid ipv6 2902:721::3
PE2(segment-routing-ipv6-list)#index 2 sid ipv6 1401:721::20
PE2(segment-routing-ipv6-list)#exit
```

Configuring EVPN VPWS services

- Configure PE 1.

Step 1 Configure EVPN VPWS instance 100.

```
PE1(config)#evpn vpws 100
PE1(config-evpn-vpws)#rd 100:1
PE1(config-evpn-vpws)#route-target import 1000:1000
PE1(config-evpn-vpws)#route-target export 1000:1000
PE1(config-evpn-vpws)#segment-routing ipv6 traffic-engineer best-effort
/*select SRv6 TE or BE as the transport tunnel */
```

Step 2 Configure EVPN EVPL instance 101.

```
PE1(config)#evpn evpl 101 srv6-mode
PE1(config-evpn-evpl)#evpn vpws 100 /* configure EVPN EVPL instance to be
associated with the EVPN VPWS instance */
PE1(config-evpn-evpl)#local-service-id 101 remote-service-id 102
PE1(config-evpn-evpl)#segment-routing ipv6 locator 88-E-18
```

Step 3 Configure the AC interface that accesses VLAN 100 services.

```
PE1(config)#interface tengigabitethernet 1/1/4.100
PE1(config-tengigabitethernet1/1/4.100)#encapsulation dot1Q 100
PE1(config-tengigabitethernet1/1/4.100)#mode l2
PE1(config-tengigabitethernet1/1/4.100)#evpn evpl 101 /* configure the AC
interface to be associated with the EVPN EVPL instance */
```

- Configure PE 2.

Step 4 Configure EVPN VPWS instance 200.

Copyright © Raisecom Technology Co., Ltd.

```
PE2(config)#evpn vpws 200
PE2(config-evpn-vpws)#rd 200:1
PE2(config-evpn-vpws)#route-target import 1000:1000
PE2(config-evpn-vpws)#route-target export 1000:1000
PE2(config-evpn-vpws)#segment-routing ipv6 traffic-engineer best-effort
/* select the SRv6 TE or BE as the transport tunnel */
```

Step 5 Configure EVPN EVPL instance 201.

```
PE2(config)#evpn evpl 201 srv6-mode
PE2(config-evpn-evpl)#evpn vpws200 /* configure EVPN EVPL instance to be
associated with the EVPN VPWS instance */
PE2(config-evpn-evpl)#local-service-id 102 remote-service-id 101
PE2(config-evpn-evpl)#segment-routing ipv6 locator 721-B-31
```

Step 6 Configure the AC interface that accesses VLAN 100 services.

```
PE2(config)#interface tengigabitethernet 1/2/15.100
PE2(config-tengigabitethernet1/2/15.100)#encapsulation dot1Q 100
PE2(config-tengigabitethernet1/2/15.100)#mode l2
PE2(config-tengigabitethernet1/2/15.100)#evpn evpl 201 /* configure the
AC interface to be associated with the EVPN EVPL instance */
```

Configuring BGP

- Configuring PE 1

```
PE1(config)#router bgp 100
PE1(config-router-bgp)#address-family ipv6
PE1(config-router-af)#neighbor 2::2 remote-as 100
PE1(config-router-af)#neighbor 2::2 update-source 1::1
PE1(config-router-af)#exit
PE1(config-router-bgp)#address-family l2vpn evpn
PE1(config-router-af)#neighbor  2::2 activate /* configure the remote EVPN
neighbor */
PE1(config-router-af)#neighbor  2::2 advertise encap-type srv6 /*
configure EVPN services to be encapsulated by the SRv6 tunnel */
PE1(config-router-af)#neighbor  2::2 send-community extended /* enable BGP
to send extended community perperties (route target) to the peer */
PE1(config-router-af)#exit-address-family
```

- Configure PE 2.

```
PE2(config)#router bgp 100
```


Copyright © Raisecom Technology Co., Ltd.

```
PE2(config-router-bgp)#address-family ipv6
PE2(config-router-af)#neighbor 1::1 remote-as 100
PE2(config-router-af)#neighbor 1::1 update-source 2::2
PE2(config-router-af)#exit
PE2(config-router-bgp)#address-family l2vpn evpn
PE2(config-router-af)#neighbor 1::1 activate /* configure the remote EVPN
neighbor */
PE2(config-router-af)#neighbor 1::1 advertise encap-type srv6 /*
configure EVPN services to be encapsulated by the SRv6 tunnel */
PE2(config-router-af)#neighbor 1::1 send-community extended /* enable BGP
to send extended community properties (route target) to the peer */
PE2(config-router-af)#exit-address-family
```

Checking results

- Show configurations of the tunnel.

```
PE1(config)#show fib
Destination/Mask    Gateway   Flags   Use   Interface    Metric    Age
inHw
------------------------------------------------------------------------
-------------------------------------------------
1401:721::/64  fe80::20e:5eff:fe39:5406 Ip#34 0
tengigabitethernet1/1/3.100  0  20:24:36  TRUE
2023::/64          :: If#11    UGSBRM    0        NULL0     0  20:24:45
TRUE
2023::3/128     Srv6-local#35   UHSRM     0          *      0   20:24:36
TRUE
2023::AB/128     Srv6-local#12   UHSRM    0          *     0   20:24:45   TRUE
2023::100/128    Srv6-local#4    UHSRM    0        *    0   20:39:36   TRUE
2023::101/128   Srv6-local#5    UHSRM     72025      *    0   1d00h05m   TRUE
2023::102/128  Srv6-local#6    UHSRM      0     *      0   1d00h05m   TRUE
```

In the previous FIB entries:

- 2023::3/128 is the route of the IPv6 address generated by the static end-x configured for the local device locator. Note that the location for issuing the FIB is Srv6-local#xx.
- 2023::AB/128 is the route of the IPv6 address generated by the static end configured for the local device locator. Note that the location for issuing the FIB is Srv6-local#xx.
- 2023::100-102/128 is the IP address dynamically applied for by services under BGP of the local device. Note that the location for issuing the FIB is Srv6-local#xx.
- 1401:721::/64 is the route of the IPv6 address generated by the peer device locator.

```
PE1(config)#show ipv6 route
P&s Destination/Mask    Dis/Metric   NextHop        Age       Interface
I>* 2023::/64         115/0         ::          1d00h10m      NULL0
I>* 2023::3/128   115/0   fe80::20e:5eff:fe39:5406  03:28:06
tengigabitethernet1/1/3.100
I>* 2023::ab/128    115/0         ::1        1d00h10m    loopback0
```


Copyright © Raisecom Technology Co., Ltd.

```
B>* 2023::100/128    200/0    2023::100      1d00h10m    loopback0
B>* 2023::101/128    200/0      2023::101     1d00h10m    loopback0
B>* 2023::102/128    200/0      2023::102          1d00h10m    loopback0
```

The previous entries and FIB are in corresponding relation, and its assigning routing protocol can be shown.

- Show configurations of EVPN services.

```
PE1(config)#show evpn evpl
Total Evpl: 7
------------------------------------------------------------------------
-----
Evpl ID: 101
Evpl Mode: dynamic srv6-mode
Evpn Vpws ID: 20000099
Interface: GE1/1/4.100 (up)
Local Redundancy Mode: all-active
Local DF State: Primary
Local MTU : 1500
Local Control Word : false
Local Service ID : 101
Remote Service ID: 102
LOCAL SID : 2023::100
SID TYPE  : Dynamic
NHP Count : 1
NHP Type  : Srv6 TE
NHP Index : 2
BFD CFG Enable      : False
BFD CFG Tx Interval  : 0
BFD CFG Rx Interval  : 0
BFD CFG Detect Multi : 0
------------------------------------------------------------------------
-----
  VPN SID      : 2902:721::1:0:0
  NHP Index    : 1000007
  FWD Index    : 0
  Tunnel Type   : Srv6 TE
  EndPoint     : 2::2
  Color        : 100
  Rmt MTU      : 1500
  Rmt CW       : 0
------------------------------------------------------------------------
```


Copyright © Raisecom Technology Co., Ltd.

11 VPN

This chapter describes principles and configuration procedures of MPLS VPN, as well as related configuration examples, including following sections:

- Configuring VPWS
- Configuring CCC L2VPN
- Configuring VPLS
- Configuring MPLS L3VPN
- Configuring MPLS VPN fault detection
- Configuring EVPN
- Configuring the VPN tunnel policy
- Maintenance
- Configuration examples

11.1 Configuring VPWS

11.1.1 Preparing for configurations

Scenario

VPWS is a point-to-point L2VPN technology. It forms a service mode that multiple services can be provided in a network. Therefore, the carrier can provide Layer 2 services and Layer 3 services in a MPLS network.

The access modes for the L2VPN to extract sub-interface services are different. Therefore, the modes adopted by the system to process the Tags of Ethernet packets are also differently, which are divided into symmetric mode and asymmetric mode as shown in Table 11-1 and Table 11-2.

Copyright © Raisecom Technology Co., Ltd.

Table 11-1 Extracting sub-interface services in symmetric mode

Type of sub-interface	Function	VPWS/VSI	
		Raw encapsulation	Tagged encapsulation
Dot1q sub-interface	Ingress interface	No action	Add the outer Tag to the packet. The TPID and VLAN Tag are configurable. By default, the TPID is 0x8100 and the VLAN Tag is 0.
	Egress interface	No action	Remove the outer Tag of the packet.
QinQ sub-interface	Ingress interface	No action	Add the outer Tag to the packet. The TPID and VLAN Tag are configurable. By default, the TPID is 0x8100 and the VLAN Tag is 0.
	Egress interface	No action	Remove the outer Tag of the packet.
Ethernet interface	Ingress interface	No action	Add the outer Tag of the packet. The TPID and VLAN Tag are configurable. By default, the TPID is 0x8100 and the VLAN Tag is 0.
	Egress interface	No action	Remove the outer Tag of the packet.

Table 11-2 Extracting sub-interface services in asymmetric mode

Type of sub-interface	Function	VPWS/VSI	
		Raw encapsulation	Tagged encapsulation
Dot1q sub-interface	Ingress interface	Remove the outer Tag of the packet.	Remove the outer Tag of the packet first and then add outer Tag according to the interface configurations. By default, the TPID and the VLAN Tag of the added outer Tag are 0x8100 and 0 respectively.
	Egress interface	Add the outer Tag to the packet. The added Tag is the SVLAN encapsulated by the sub-interface.	Replace the outer Tag of the packet. The added Tag is the SVLAN encapsulated by the sub-interface.

Copyright © Raisecom Technology Co., Ltd.

Type of sub-interface	Function	VPWS/VSI	
		Raw encapsulation	Tagged encapsulation
QinQ sub-interface	Ingress interface	Remove the outer Tag of the packet. Use the **vlan translation svlan untag cvlan untag** command to enable the interface to remove the outer double Tag. Otherwise, the Tag cannot be removed.	Remove the outer double Tag of the packet first and then add outer Tag according to the interface configurations. Use the **vlan translation svlan untag cvlan untag** command to enable the interface to remove the outer double Tag. Otherwise, the Tag cannot be removed. By default, the TPID and the VLAN Tag of the added outer Tag are 0x8100 and 0 respectively.
	Egress interface	Remove the outer double Tag of the packet. Use the **vlan translation svlan untag cvlan untag** command to enable the interface to add the outer double Tag. Otherwise, the Tag cannot be removed. The added Tag is the SVLAN and CVLAN encapsulated by the interface.	Remove the outer Tag of the packet first and then add outer double Tag according to the interface configurations. Use the **vlan translation svlan untag cvlan untag** command to enable the interface to remove the outer Tag and then add outer double Tag. Otherwise, the Tag cannot be added.

Prerequisite

- Configure the basic attributes of Layer 3 physical interface, sub-interface, and LAG interface.
- Configure MPLS basic functions.
- Configure Tunnel-related functions.

11.1.2 Configuring static L2VC

Configuring service extraction interface

The device supports extracting L2VPN services on the Layer 3 physical interface.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`*	Enter physical layer interface configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config-port)#**no portswitch**	(Optional) switch the interface to Layer 3 router mode. By default, the interface is in Layer 3 router mode.
	Raisecom(config-port)#**mode l2**	Configure the VPN mode of the Layer 3 physical interface to L2VPN. By default, the VPN mode of the Layer 3 physical interface is L3VPN.
3	Raisecom(config)#**interface** *interface-type interface-number*.subif	Enter sub-interface configuration mode.
	Raisecom(config-*subif*)#**encapsulation** { **dot1Q** | **qinq** }	Configure the sub-interface encapsulation mode.
	Raisecom(config-*subif*)#**mode l2**	Configure the sub-interface to L2VPN mode.
	Raisecom(config-subif)#**l2vpn access-mode asymmetry**	(Optional) configure the access mode of the L2VPN service extraction interface to asymmetric. By default, it is asymmetric.

Configuring static L2VC

Configure static L2VC in the corresponding service extraction interface configuration mode.

Step	Command	Description
1	Raisecom(config-port)#**mpls static-l2vc destination** *ip-address* **raw vc-id** *vc-id* **in-label** *in-label* **out-label** *out-label* [**tunnel-policy** *policy-name* | **tunnel** *tunnel-number*] [**no-control-word**] [**mtu** *mtu*] [**backup**]	Configure static L2VC by specifying the input label and the output label. The encapsulation mode of PW packets is Raw. That is, there is no VLAN tag.
2	Raisecom(config-port)#**mpls static-l2vc destination** *ip-address* [**tagged**] **vc-id** *vc-id* **in-label** *in-label* **out-label** *out-label* [**tunnel-policy** *policy-name* | **tunnel** *interface-number*] [**no-control-word**] [**mtu** *mtu*] [**tpid** *tpid*] [**svlan** *vlan-id*] [**backup**]	Configure static L2VC by specifying the input label and the output label. The encapsulation mode of PW packets is Tagged. You can choose to configure the client VLAN ID.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	`Raisecom(config-port)#l2vpn { raw-mode | tag-mode } standard`	(Optional) configure the label encapsulation type of L2VPN services, and encapsulate them in the standard mode. The device supports two encapsulation modes, standard encapsulation and non-standard encapsulation. You can use this command to configure the device to use standard encapsulation. If this command is not configured, the device uses the non-standard encapsulation mode by default. In non-standard encapsulation mode, if the tags of the sub-interfaces on both ends of a PW are different, the **l2vpn access-mode asymmetry** command must be used to configure the tag mode to asymmetric; otherwise, the service will be blocked. In standard encapsulation mode, there is no need to configure the **l2vpn access-mode asymmetry** command. If the device to be used is not targeted at being compatible with the Raisecom device with the earlier version, we recommend using the standard encapsulation mode (the encapsulation type of services in interface configuration mode is raw encapsulation; the encapsulation type of services in sub-interface configuration mode is tag encapsulation) to increase the convenience of interoperability with third-party devices.

11.1.3 Configuring dynamic L2VC

Enabling Martini

VPWS has multiple implementation modes, and Martini is LDP-based dynamic implementation mode among them. Use the following command to enable Martini to dynamically establish L2VPN.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mpls l2vpn default martini`	Enable global Martini.

Copyright © Raisecom Technology Co., Ltd.

Configuring service extraction interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
	Raisecom(config-port)#**no portswitch**	(Optional) switch the interface to Layer 3 router mode. By default, the interface is in Layer 3 router mode.
	Raisecom(config-port)#**mode l2**	Configure the VPN mode of the Layer 3 physical interface to L2VPN. By default, the VPN mode of the Layer 3 physical interface is L3VPN.
3	Raisecom(config)#**interface** *interface-type interface-number.subif*	Enter sub-interface configuration mode.
	Raisecom(config-*subif*)#**encapsulation** { **dot1Q** | **qinq** }	Configure the sub-interface encapsulation mode.
	Raisecom(config-*subif*)#**mode l2**	Configure the sub-interface to L2VPN mode.
	Raisecom(config-subif)#**l2vpn access-mode asymmetry**	(Optional) configure the access mode of the L2VPN service extraction interface to asymmetric. By default, it is asymmetric.

Configuring dynamic L2VC

Step	Command	Description
1	Raisecom(config-port)#**mpls l2vc destination** *ip-address* **raw vc-id** *vc-id* [**tunnel-policy** *policy-name* | **tunnel** *tunnel-number*] [**no-control-word**] [**mtu** *mtu*] [[**backup**]	Configure dynamic L2VC. The encapsulation mode of PW packets is Raw. That is, there is no VLAN tag.
2	Raisecom(config-port)#**mpls l2vc destination** *ip-address* [**tagged**] **vc-id** *vc-id* [**tunnel-policy** *policy-name* | **tunnel** *tunnel-number*] [**no-control-word**] [**mtu** *mtu*] [**backup**]	Configure dynamic L2VC. The encapsulation mode of PW packets is Tagged. You can choose to configure the client VLAN ID.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-port)#**l2vpn { raw-mode | tag-mode } standard**	(Optional) configure the label encapsulation type of L2VPN services, and encapsulate them in the standard mode. The device supports two encapsulation modes, standard encapsulation and non-standard encapsulation. You can use this command to configure the device to use standard encapsulation. If this command is not configured, the device uses the non-standard encapsulation mode by default. In non-standard encapsulation mode, if the tags of the sub-interfaces on both ends of a PW are different, the **l2vpn access-mode asymmetry** command must be used to configure the tag mode to asymmetric; otherwise, the service will be blocked. In standard encapsulation mode, there is no need to configure the **l2vpn access-mode asymmetry** command. If the device to be used is not targeted at being compatible with the Raisecom device with the earlier version, we recommend using the standard encapsulation mode (the encapsulation type of services in interface configuration mode is raw encapsulation; the encapsulation type of services in sub-interface configuration mode is tag encapsulation) to increase the convenience of interoperability with third-party devices.

Configuring L2VPN flow label

Configure L2VPN flow label to load-balance traffic through the hash algorithm and to improve forwarding efficiency.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls l2vpn flow-label hash-fields { l2 | l3 | l4 }**	Configure the L2VPN flow label to load-balance traffic through the hash algorithm and to improve forwarding efficiency.

11.1.4 Configuring MS-PW

Configuring static-to-static PW switching

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**mpls switch-l2vc** *ip-address vc-id* **in-label** *in-label* **out-label** *out-label* [**tunnel-policy** *policy-name* | **tunnel** *tunnel-number*] **between** *ip-address vc-id* [**in-label** *in-label* **out-label** *out-label*] [**tunnel-policy** *policy-name* | **tunnel** *tunnel-number*] { **raw** | **tagged** } [**no-control-word**] [**mtu** *mtu*]	Configure the static-to-static MS-PW.

Configuring dynamic-to-static PW switching

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls switch-l2vc** *ip-address vc-id* [**tunnel-policy** *policy-name* | **tunnel** *tunnel-number*] **between** *ip-address vc-id* [**in-label** *in-label* **out-label** *out-label*] [**tunnel-policy** *policy-name* | **tunnel** *tunnel-number*] { **raw** | **tagged** } [**no-control-word**] [**mtu** *mtu*]	Configure dynamic-to-static MS-PW.

Configuring dynamic-to-dynamic PW switching

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls switch-l2vc** *ip-address vc-id* [**tunnel-policy** *policy-name* | **tunnel** *tunnel-number*] **between** *ip-address vc-id* [**tunnel-policy** *policy-name* | **tunnel** *tunnel-number*] { **raw** | **tagged** }	Configure dynamic-to-dynamic MS-PW, which is encapsulated based on Ethernet.

Note

In the command lines of the above configuration steps, different parameters are configured to distinguish the static PW from the dynamic PW.

- To configure a static PW, you need to specify the **in-label** *in-label* and **out-label** *out-label.*
- To configure a dynamic PW, you do not need to specify the **in-label** *in-label* and **out-label** *out-label,* control word, and MTU.

11.1.5 (Optional) configuring BFD for PW

After configuring PW, you can configure PW-based BFD.

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**mpls l2vpn pw bfd** [**min-tx-interval** *tx-interval*] [**min-rx-interval** *rx-interval*] [**detect-multiplier** *multiplier*] [**backup**]	Configure PW-based BFD.

11.1.6 Checking configurations

No.	Command	Description
1	Raisecom#**show mpls l2vc** [**static**] [*interface-type interface-number*]	Show status of the static PW or dynamic PW.
2	Raisecom#**show mpls switch-l2vc** [*ip-address vc-id*]	Show the MS-PW status.

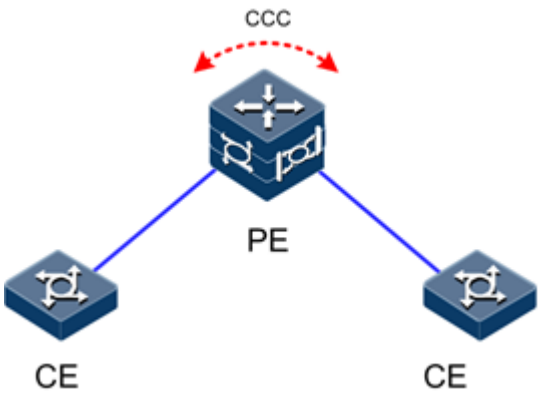
11.2 Configuring CCC L2VPN

11.2.1 Preparing for configurations

Scenario

Circuit Cross Connect (CCC) is a method to implement MPLS L2VPN through static LSP. As shown in Figure 11-1, CCC is applied to the local connection scenario. CE 1 and CE 2 are connected to the same PE. The PE acts as a Layer 2 device. Data exchange is implemented by configuring the interface type and encapsulation mode.

Figure 11-1 CCC local connection



The corresponding packet processing methods vary with the encapsulation mode configured for the PE interface.

- The ingress packets on the interface are untagged packets.

Copyright © Raisecom Technology Co., Ltd.

Ingress/Egress interface	Raw+Raw mode	Tagged+Tagged mode	Raw+Tagged mode
Physical interface + physical interface	Transparently transmitted packets	Transparently transmitted packets	Transparently transmitted packets
Sub-interface + sub-interface	The ingress interface drops the packets.	The ingress interface drops the packets.	The ingress interface drops the packets.
Physical interface + sub-interface	Add a VLAN ID to the packet when it leaves the sub-interface. The physical interface transparently transmit it.	Add a VLAN ID to the packet when it leaves the sub-interface. The physical interface transparently transmit it.	Add a VLAN ID to the packet when it leaves the sub-interface. The physical interface transparently transmit it.

- The ingress packets on the interface are tagged packets.

Ingress/Egress interface	Raw+Raw mode	Tagged+Tagged mode	Raw+Tagged mode
Physical interface + physical interface	Transparently transmitted packets	Transparently transmitted packets	Transparently transmitted packets
Sub-interface + sub-interface	The packet with a VLAN ID meeting the rule will pass when it enters the sub-interface. When the packet leaves the sub-interface, its VLAN ID will be modified to the corresponding one.	The packet with a VLAN ID meeting the rule will pass when it enters the sub-interface. When the packet leaves the sub-interface, its VLAN ID will be modified to the corresponding one.	The packet with a VLAN ID meeting the rule will pass when it enters the sub-interface. When the packet leaves the sub-interface, its VLAN ID will be modified to the corresponding one.

Copyright © Raisecom Technology Co., Ltd.

Ingress/Egress interface	Raw+Raw mode	Tagged+Tagged mode	Raw+Tagged mode
Physical interface + sub-interface	When the packet leaves the sub-interface, its VLAN ID will be modified into the one of the sub-interface. When the packet leaves the physical interface, the Tag will be removed.	When the packet leaves the sub-interface, its VLAN ID will be modified into the one of the sub-interface. When the packet leaves the physical interface, the VLAN ID keeps the same.	When the packet leaves the sub-interface, its VLAN ID will be modified into the one of the sub-interface. When the sub-interface is Raw, the tag will be removed when the packet leaves the physical interface. When the sub-interface is tagged, the tag of the packet will not be removed when it leaves the physical interface.

Prerequisite

- Prepare the interface plan of the PE and select the interface type and interface ID.
- Determine whether the packet VLAN be converted, and select the corresponding encapsulation mode.

11.2.2 Configuring CCC

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ccc` *ccc-name* `interface` *interface-type interface-number* `[ access-port ] [ raw | tagged | double-tagged ] out-interface` *interface-type interface-number* `[ access-port ] [ raw | tagged | double-tagged ]`	Configure CCC.

11.2.3 Checking configurations

No.	Command	Description
1	`Raisecom#show l2vpn ccc` *ccc-name*	Show CCC configurations.

Copyright © Raisecom Technology Co., Ltd.

11.3 Configuring VPLS

11.3.1 Preparing for configurations

Scenario

VPLS is a L2VPN technology which is based on MPLS and Ethernet technology. VPLS can provide point-to-multipoint VPN networking topology. VPLS provides a more perfect solution for carriers, who use point-to-point L2VPN services. In addition, it does not need to manage internal routing information of users, which is required in L3VPN.

Prerequisite

- Configure basic attributes, such as Layer 3 physical interfaces, sub-interfaces, and link aggregation group interfaces.
- Configure MPLS basic functions.
- Configure Tunnel functions.

11.3.2 Configuring VSI

The tunnel label and PW label of the same device belong to the same label domain, that is, the two cannot overlap.

Configuring VSI basic functions

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mpls vsi` *vsi-name* `static`	Create a VSI and enter VSI configuration mode.
3	`Raisecom(config-vsi)#vsi-id` *id*	Configure the VSI ID.
4	`Raisecom(config-vsi)#vsi-mtu` *mtu*	Configure the VSI MTU.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config-vsi)#**encapsulation** { **raw** | **tagged** } [**standard**]	Configure the encapsulation type and encapsulation mode of VSI services. The device supports two encapsulation modes, standard encapsulation and non-standard encapsulation. You can use this command to configure the device to use standard encapsulation. If this command is not configured, the device uses the non-standard encapsulation mode by default. In non-standard encapsulation mode, if the tags of the sub-interfaces on both ends of a PW are different, the **l2vpn access-mode asymmetry** command must be used to configure the tag mode to asymmetric; otherwise, the service will be blocked. In standard encapsulation mode, there is no need to configure the **l2vpn access-mode asymmetry** command. If the device to be used is not targeted at being compatible with the Raisecom device with the earlier version, we recommend using the standard encapsulation mode to increase the convenience of interoperability with third-party devices.
6	Raisecom(config-vsi)#**l2vpn access-mode asymmetry**	(Optional) configure the VSI service access mode to asymmetric. By default, it is symmetric.
7	Raisecom(config-vsi)#**mpls static-peer** *ip-address* [**vc-id** *vc-id*] **in-label** *in-label* **out-label** *out-label* [**tunnel-policy** *policy-name* | **tunnel** *tunnel-number*] [**no-control-word**] [**upe** | **upe-isolate**]	Configure the VSI static peer. Create a PW and specify the Tunnel for the PW to isolate PWs.
8	Raisecom(config-vsi)#**mpls peer** *ip-address* [**vc-id** *vc-id*] [**tunnel-policy** *policy-name* | **tunnel** *tunnel-number*] [**no-control-word**] [**upe** | **upe-isolate**]	Configure the MPLS dynamic peer. Create a PW and specify a Tunnel for the PW to implement PW isolation.
9	Raisecom(config-vsi)#**ratelimit** { **broadcast** | **unknown-multicast** | **dlf** } **cir** *cir-value* [**cbs** *cbs-value*]	Configure rate limiting. Currently, broadcast rate limiting is not supported.
10	Raisecom(config-vsi)#**storm-filter** { **broadcast** | **multicast** | **dlf** | **all** } **enable** Raisecom(config-vsi)#**exit**	Enable VSI storm control.
11	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config)#**mode l2**	Enter Layer 3 interface configuration mode and switch it to L2VPN mode.
12	Raisecom(config-port)#**mpls l2binding vsi** *vsi-name* [**isolate**]	Bind VPLS services to implement AC isolation.

Copyright © Raisecom Technology Co., Ltd.

Configuring the QinQ sub-interface to access VSI

The device supports creating QinQ sub-interfaces on the Layer 2 physical interface and accessing VSI, meeting requirements for the STP dual-homed access scenario.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config-port)#**interface** *interface-type unit/slot/port.sub-interface*	Enter Ethernet sub-interface configuration mode.
3	Raisecom(config-subif)#**encapsulation dot1Q** vlan-list	Configure the single-tagged VLAN list for Ethernet sub-interface encapsulation.
4	Raisecom(config-subif)#**mode l2**	Configure the sub-interface mode for accessing L2VPN. By default, it is L3.
5	Raisecom(config-subif)#**vlan translate svlan** *svlan-id* **cvlan** { *cvlan-id* | **unchanged** }	Configure VLAN mapping for sub-interface encapsulation.
6	Raisecom(config-subif)#**mpls l2binding vsi** *vsi-name* [**isolate**]	Bind VPLS services.

Configuring VSI MAC address rules

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls vsi** *vsi-name* **static**	Create a VSI and enter VSI configuration mode.
3	Raisecom(config-vsi)#**mac-address learning** { **enable** | **disable** }	Enable VSI MAC address learning.
4	Raisecom(config-vsi)#**mac-address threshold** *threshold-value*	Configure MAC address limits of the VSI.
5	Raisecom(config-vsi)#**mac-policy** { **blacklist** | **whitelist** } Raisecom(config-vsi)#**exit**	Configure the MAC address policy of the VSI.
6	Raisecom(config)#**mac-address static unicast** *mac-address* **vsi** *vsi-name interface-type interface-number*	Configure the VSI unicast MAC address to bind the AC-side MAC address.
7	Raisecom(config)#**mac-address static unicast** *mac-address* **vsi** *vsi-name* **vc-id** *vc-id* **peer** *ip-address*	Configure the unicast MAC address of the VSI to bind the PW-side MAC address.
8	Raisecom(config)#**mac-address blackhole** *mac-address* **vsi** *vsi-name*	Configure the blackhole MAC address of the VSI.

Copyright © Raisecom Technology Co., Ltd.

Configuring VSI storm control

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls vsi** *vsi-name* **static**	Create a VSI and enter VSI configuration mode.
3	Raisecom(config-vsi)#**storm-control** { **broadcast** | **unknown-multicast** | **dlf** | **all** } **enable**	Enable storm control.

Configuring VSI traffic statistics

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls vsi** *vsi-name* **static**	Create a VSI and enter VSI configuration mode.
3	Raisecom(config-vsi)#**traffic-statistics** [**peer** *ip-address* **vc-id** *vc-id*] **enable**	Enable VSI traffic statistics.

11.3.3 Configuring VPLS traffic label

Configuring traffic label in VSI mode

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls vsi** *vsi-name* **static**	Create a VSI and enter VSI configuration mode.
3	Raisecom(config-vsi)#**flow-label** { **both** | **send** | **receive** } [**static**]	Configure the VPLS traffic label.

Configuring traffic label for a specified PW

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls vsi** *vsi-name* **static**	Create a VSI and enter VSI configuration mode.
3	Raisecom(config-vsi)#**mpls peer** *ip-address* **vc-id** *vc-id* **flow-label** { **both** | **send** | **receive** } [**static**]	Enable traffic label for a specified PW.

Copyright © Raisecom Technology Co., Ltd.

11.3.4 Checking configurations

No.	Command	Description
1	`Raisecom#show mpls vsi detail [ vsi-name ]`	Show VSI detailed information.
2	`Raisecom#show mpls vsi pw [ vsi-name ]`	Show VSI PW configurations.
3	`Raisecom#show mpls vsi services [ vsi-name ]`	Show VSI service information.
4	`Raisecom#show mpls vsi statistics`	Show VSI statistics.
5	`Raisecom#show mpls vsi traffic-statistics vsi-name [ peer ip-address vc-id vc-id ]`	Show VSI traffic statistics.

11.4 Configuring MPLS L3VPN

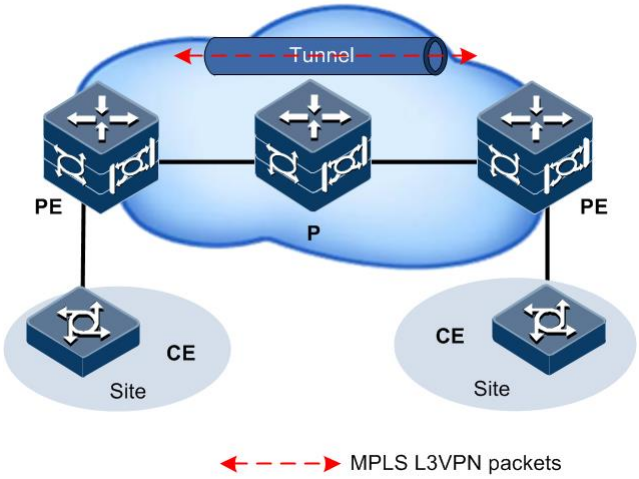
11.4.1 Preparing for configurations

Scenario

MPLS L3VPN is a PE-based L3VPN technology for ISP's solutions. It uses the BGP to release the VPN route and uses MPLS to forward VPN packets in the ISP network.

As shown in Figure 11-2, in MPLS L3 VPN topology, the PE device and CE device exchange routes through EBGP. Static routes, ISIS routes, and OSPF routes are also supported.

Figure 11-2 MPLS L3VPN network topology



MPLS L3VPN provides a flexible networking mode and is of good expansibility. In addition, it supports MPLS QoS and MPLS TE well. Therefore, it is applied to increasing larger scales.

Prerequisite

- Configure basic attributes, such as Layer 3 physical interface, sub-interface, and link aggregation interface.

Copyright © Raisecom Technology Co., Ltd.

- Configure MPLS basic functions.
- Configure Tunnel related functions.

11.4.2 Configuring VRF basic attributes

Configure VRF on the PE device in the backbone network and connect the CE to the PE.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip vrf** *vrf-name*	Create a VRF and enter VRF configuration mode.
3	Raisecom(config-vrf)#**rd** *rd*	Configure the VRF RD.
4	Raisecom(config-vrf)#**route-target** [**export** | **import** | **both**] *rt*	Configure the VRF RT.

11.4.3 Binding VRF with interfaces

This configuration is for binding the PE UNI in the backbone network with VRF. After configurations are complete, PE devices can ping through their respectively connected CE devices. The configuration prerequisite is that the UNIs of PE devices and the interfaces of CE devices are all configured with IP addresses.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface, VLAN sub-interface, and sub-interface configuration modes.
3	Raisecom(config-port)#**ip vrf forwarding** *vrf-name*	Apply VRF to UNIs, such as the Layer 3 physical interface, VLAN sub-interface, sub-interface, Port+VLAN interface, and QinQ sub-interface. **Note** When applying VRF to the Layer 3 sub-interface, you should configure the encapsulation VLAN of the sub-interface to Dot1.Q or QinQ.

11.4.4 Configuring public routes

Configure IGP routes on the PE and P devices in the backbone network. After configurations are complete, PE device and P device can establish IGP neighbor relationship, then they can ping through each other.

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**network** *ip-address wild-card-mask* **area** *area-id*	Advertise the network, that is, define the IP address of the interface or the network which participates in the OSPF process and specify the area to which the interface or network belongs.

11.4.5 Configuring public Tunnel

Configuring public Tunnel

Public network tunnels can be static LSP tunnels or dynamic LDP tunnels. Establish MPLS tunnels by configuring MPLS basic functions, static LSPs, or MPLS LDP functions on the PE and P devices in the backbone network. After the configuration is complete, public network tunnels are established between the PE devices at both ends.

For the configuration of the public network tunnel, see chapter 9 MPLS.

Configuring public Tunnel policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**tunnel-policy** *policy-name*	Configure a Tunnel policy and enter Tunnel policy configuration mode.
3	Raisecom(config-tunnelpolicy)#**tunnel select-seq** { **lsp** | **cr-lsp** } * Raisecom(config-tunnelpolicy)#**exit**	Configure the Tunnel selection sequence.
4	Raisecom(config)#**ip vrf** *vrf-name*	Enter VRF configuration mode.
5	Raisecom(config-vrf)#**tunnel-policy** *policy-name*	Apply the Tunnel policy to the current VRF.

11.4.6 Configuring MP-IBGP peer

Configure MP-IBGP VPNv4 neighbor relations on the PE devices at both ends in the backbone network, transferring VPNv4 routes.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enable BGP and create a BGP instance and enter BGP configuration mode.
3	Raisecom(config-router)#**bgp router-id** *router-id*	Configure BGP router ID.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-router)#**neighbor** *ip-address* **remote-as** *as-id*	Create a MP-IBGP peer and specify the peer AS ID. The peer AS ID should be the same with the local AS ID.
5	Raisecom(config-router)#**neighbor** *ip-address1* **update-source** *ip-address2*	Configure the device to use the specified route to update the source interface while establishing BGP connections.
6	Raisecom(config-router)#**address-family vpnv4**	Enter BGP VPNv4 address family configuration mode.
7	Raisecom(config-router-af)#**neighbor** *ip-address* **activate**	Enable the function of exchanging information about the specified VPNv4 address family among BGP neighbors.
8	Raisecom(config-router-af)#**neighbor** *ip-address* **send-community extended**	Enable BGP to send extended community attributes to the peer.
9	Raisecom(config-router-af)#**exit-address-family**	Exit BGP VPNv4 address family configuration mode.
10	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter IPv4 address family configuration mode of the BGP VPN instance.
11	Raisecom(config-router-af)#**redistribute connected**	Configure the BGP to import direct routes through redistribution.
12	Raisecom(config-router-af)#**redistribute static**	Configure the BGP to import static routes through redistribution.
13	Raisecom(config-router-af)#**redistribute ospf** *process-id* [**metric** *metric*] [**route-map** *map-name*]	Configure the BGP to redistribute OSPF routes through redirection.
14	Raisecom(config-router-af)#**neighbor** *ipv6-address* **prefix-sid**	Enable the IPv6 neighbor to carry the prefix SID on the Ipv6 peer in the L3VPN over SRv6-be scenario.
15	Raisecom(config-router-af)#**exit-address-family**	Exit IPv4 address family configuration mode based on BGP VPN instance.

11.4.7 Configuring PE-CE route switching

Static routes, EBGP routes, ISIS routes, and OSPF routes can be used for PE-CE route switching. Select one mode according to the actual network requirement.

Configuring PE-CE static routes.

Configure the PE device as below.

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**ip route vrf** vrf-name destination-address mask-address { next-hop | **NULL 0** } *interface-type interface-number* [**distance** distance] [**description** text] [**tag** tag]	Configure static routes in the specified VRF.
3	Raisecom(config)#**router bgp** *as-id*	Enable BGP. Create a BGP instance and enter BGP configuration mode.
4	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Specify the IPv4 unicast address family routing table of the specified VPN instance and enter VPN instance IPv4 unicast address family configuration mode.
5	Raisecom(config-router-af)#**redistribute static**	Redistribute routes to the IPv4 unicast address family routing table of the VPN instance.

Configure the CE device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip route** *destination-address* { *mask-address* | *mask-length* } { *next-hop* | **NULL 0** } *interface-type interface-number* [**distance** *distance*] [**description** *text*] [**tag** *tag*]	Configure static routes from CE to PE.

Configure PE-CE EBGP routes

Configure the PE device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Create BGP VRF and enter IPv4 unicast address family configuration mode.
4	Raisecom(config-router-af)#**neighbor** *ip-address* **remote-as** *as-id*	Configure the CE to the VPN EBGP peer and specify the peer AS ID. The peer AS ID is different from the local AS ID. By default, there is no BGP peer.
5	Raisecom(config-router-af)#**neighbor** *ip-address* **activate**	Enable the feature of switching IPv4 unicast address family routes with the EBGP peer. By default, switching IPv4 unicast address family routes with the EBGP peer is enabled. Switching route information about other address families is prohibited.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config-router-af)#**redistribute** { **connected** | **static** | **ospf** } [**metric** *metric*] [**route-map** *map*]	Redistribute OSPF routes with the CE. Redistribute the CE routes to the VPN routing table to advertise them to the peer PE on the network.
	Raisecom(config-router-af)#**network** *ip-address* [*mask-address*] [**route-map** *route-map-name*]	Advertise local routes. Advertise local routes of the CE in the specified network segments to the VPN routing table.

Configure the CE device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**neighbor** *ip-address* **remote-as** *as-id*	Configure the PE as the EBGP peer and specify the peer AS ID. By default, there is no BGP peer.
4	Raisecom(config-router)#**redistribute** { **connected** | **static** | **ospf** } [**metric** *metric*] [**route-map** *map*]	Redistribute VPN routes. CE advertises the address of the VPN network segment that it can arrive to the accessed PE and then PE will send the information to the peer CE.
	Raisecom(config-router)#**network** *ip-address* [*mask-address*] [**route-map** *route-map-name*]	Advertise local routes. Advertise the routes of the specified network segment to the EBGP peer, namely, the accessed PE.

Configuring PE-CE OSPF routes

Configure the PE device as below:

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* **vrf** *vrf-name* [**router-id** *router-id*]	Start an OSPF process, bind it with the already-known VPN instance, and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**network** *ip-address wild-card-mask* **area** *area-id*	Advertise routes, that is, define the interface or network which participates in the OSPF process and specify the area to which the interface or network belongs.
4	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
5	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Create a BGP VRF and enter its IPv4 unicast address family configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config-router-af)#**redistribute ospf** [**metric** *metric*] [**route-map** *map*]	Redistribute CE routes. Redistribute the CE routes to the VPN routing table so that they can be advertised to the peer PE.

Configure the CE device as below:

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**network** *ip-address wild-card-mask* **area** *area-id*	Advertise private network routes to the OSPF process.

11.4.8 Checking configurations

No.	Command	Description
1	Raisecom#show ip vrf [**vrf-name** *vrf-name*]	Show VRF information.
2	Raisecom#**show tunnel-policy** [*policy-name*]	Show Tunnel policy information.
3	Raisecom#show ip bgp vpnv4 vrf *vrf-name* summary	Show summary about the VRF-based BGP peer.
4	Raisecom#**show ip bgp vpnv4 vrf** *vrf-name* **neighbour** [*ip-address*]	Show details about the VRF-based BGP peer.
5	Raisecom#**show ip bgp vpnv4 vrf** *vrf-name* **network-address** [mask-address]	Show information about VRF-based BGP routes.
6	Raisecom#**show ip ospf** [*process-id*] **route**	Show information about OSPF routes.
7	Raisecom#**show ip bgp** [*ip-address* [*ip-mask*]]	Show information about BGP routes.
8	Raisecom#**show ip route vrf** *vrf-name dest-ip-address mask-address end-dest-ip-address mask-address* [**detail**]	Show information about VRF routing.
	Raisecom#**show ip route vrf** *vrf-name dest-ip-address* [*mask-address*] [**longer-prefixes**] [**detail**]	
	Raisecom#**show ip route vrf** *vrf-name* [**protocol** { **static** | **connected** | **bgp** | **ospf** | **isis** | **rip** }] [**detail**]	

Copyright © Raisecom Technology Co., Ltd.

11.5 Configuring MPLS VPN fault detection

11.5.1 Preparing for configuration

Scenario

Because the MPLS control plane cannot detect the failure of traffic forwarding on the LSP. You can confirm and locate the faults through Ping and Traceroute.

Prerequisite

- Create a corresponding channel before starting the Ping test.
- Create a corresponding channel before starting the Traceroute test.

11.5.2 Configuring MPLS VPN fault acknowledgement

Step	Command	Description
1	Raisecom#**ping mpls vc-id** *vc-id* **destination** *ip-address* [**interval** *interval*] [**count** *count*] [**waittime** *seconds*] [**ttl** *ttl*] [**reply dscp** *dscp-value*] [**reply mode udp** | **reply mode udp-alert** | **reply mode control-channel**] [**reply pad-tlv**] [**size** *size*] [**source** *ip-address*] [**tc** *tc-value*]	Configure the MPLS PW Ping test.
2	Raisecom#**ping vrf** *vpn-name ip-address* [**count** *count*] [**df-bit**] [**size** *size*] [**source** *ip-address*] [**waittime** *seconds*]	Configure the MPLS VRF PING detection.

11.5.3 Configuring MPLS VPN fault location

Step	Command	Description
1	Raisecom#**traceroute mpls vc-id** *vc-id* **destination** *ip-address* [**waittime** *seconds*] [**maxttl** *ttl*] [**reply dscp** *dscp-value*] [**reply mode udp** | **reply mode udp-alert**] [**reply pad-tlv**] [**source** *ip-address*] [**tc** *tc-value*] [**flags fec**]	Configure the MPLS PW Traceroute test.
2	Raisecom#**traceroute** [**vrf** *instance-name*] *ip-address* [**firstttl** *first-ttl*] [**maxttl** *max-ttl*] [**port** *port-number*] [**waittime** *second*] [**count** *times*] [**size** *size*]	Configure the MPLS L3VPN Traceroute test.
3	Raisecom#**traceroute mpls ipv4** *ip-address/m* [**generic**] [**next-hop** *ip-address*] [**waittime** *seconds*] [**maxttl** *max-ttl*] [**reply dscp** *dscp-value*] [**reply pad-tlv**] [**source** *ip-addresss*] [**tc** *tc-value*] [**flags fec**]	Use the **Traceroute** command to test the connectivity of the MPLS network of the specified IPv4 address and check the network nodes through which packets have passed.

Copyright © Raisecom Technology Co., Ltd.

11.6 Configuring EVPN

11.6.1 Preparing for configurations

Scenario

EVPN is a VPN technology, which learns the MAC address and IP address on the control plane, guides data forwarding, and separates forwarding and controlling. It supports the following scenarios:

- EVPN VPWS
- EVPN VPLS
- EVPN L3VPN

Prerequisites

Configure the AC interface, service bearing tunnel, and other basic functions.

11.6.2 Configuring basic properties of EVPN

Configure the PE as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#evpn source-address` *ipv4-address*	Configure the EVPN source address, used to identify the PE in the EVPN networking.

11.6.3 Configuring MP-BGP to advertise EVPN routes

Enabling MP-BGP to advertise EVPN routes

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)# router bgp` *as-id*	Enable BGP, create a BGP instance, and enter BGP configuration mode.
3	`Raisecom(config-router)# neighbor` *ip-address* `remote-as` *as-id*	Configure the remote PE as the MP-BGP peer, and specify the AS ID of the peer.
4	`Raisecom(config-router)#address-family l2vpn evpn`	Enable EVPN address family route switching between the device and peer, and enter BGP EVPN address family mode.
5	`Raisecom(config-router-af)#neighbor` *ipv4-address* `advertise arp`	Enable BGP EVPN neighbors to advertise ARP routes among them.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config-router-af)#**neighbor** *ipv4-address* **advertise encap-type mpls**	Enable BGP EVPN neighbors to advertise EVPN routes encapsulated by MPLS among them.
7	Raisecom(config-router-af)#**neighbor** *ipv6-address* **advertise encap-type srv6**	Enable BGP EVPN neighbors to advertise EVPN routes encapsulated by SRv6 among them.

Controlling the advertisement of BGP EVPN routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enable BGP, create a BGP instance, and enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**advertise l2vpn evpn**	Configure the advertisement of routes of the IP prefix type.
5	Raisecom(config-router-af)#**auto-frr**	Enable auto-FRR.
6	Raisecom(config-router-af)#**maximum load-balancing** [**ebgp** | **ibgp**] *number*	Configure the maximum number of paths for IP equivalent multi-path load balancing.
7	Raisecom(config-router-af)#**neighbor** *ip-address* **split-horizon**	Enable horizontal split from BGP to the peer. After this function is enabled, the route received from an IBGP neighbor is not advertised to other IBGP neighbors. By default, this function is enabled.
8	Raisecom(config-router-af)#**route-select delay** *time*	Enable BGP route selection delay.

11.6.4 Configuring EVPN VPWS

Configuring EVPN VPWS instance

Configure the PE as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**evpn vpws** *evpn-vpws-instance-id*	Create an EVPN VPWS instance, and enter EVPN VPWS configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-evpn-vpws)#**rd** { *ip-address* : *number1* | *as-id* : *number2* }	Configure the Route Discriminator (RD) of the EVPN VPWS instance. **Note** It does not support 0:0.
4	Raisecom(config-evpn-vpws)#**route-target** [**export** | **import** | **both**] { *ip-address* : *number1* | *as-id* : *number2* }	Configure the RT in the ingress and egress directions of the EVPN VPWS instance. **Note** It does not support 0:0.
5	Raisecom(config-evpn-vpws)#**tunnel-policy** *policy-name*	Configure the tunnel that carries the EVPN VPWS instance.
6	Raisecom(config-evpn-vpws)#**default-color** *default-color-value*	Configure the EVPN VPWS instance to iterate the default color of the SRv6 TE tunnel.
7	Raisecom(config-evpn-vpws)#**segment-routing ipv6** { **best-effort** | **traffic-engineer** [**best-effort**] }	Configure the EVPN VPWS instance to iterate the default color of the SRv6 tunnel.

Configuring the EVPN EVPL instance

Configure the PE as below:

- Configure the EVPL instance to be associated with the EVPN VPWS instance to establish the mapping relation between the EVPL instance and EVPN VPWS instance.
- The EVPL instance is identified by the service ID. Configure the service IDs of both the local PE and peer PE. Establish the one-to-one mapping relation between the EVPL instance of the local PE and the EVPL instance of the remote PE.
- Configure the interface to be associated with the EVPL instance, and establish the mapping relation between the AC interface and EVPL instance.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**evpn evpl** *evpn-evpl-instance-id* { **srv6-mode** [**static**] | **mpls-mode** }	Create an EVPN EVPL instance, and enter EVPN EVPL configuration mode.
3	Raisecom(config-evpn-evpl)#**evpn vpws** *evpn-vpws-instance-id*	Create an EVPN EVPL instance, and associate it with an EVPN VPWS instance.
4	Raisecom(config-evpn-evpl)#**evpn local-frr**	(Optional) configure EVPN instance FRR.
5	Raisecom(config-evpn-evpl)#**segment-routing ipv6 locator** *locator-name*	Configure the locator quoted by the EVPL instance.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config-evpn-evpl)#**segment-routing ipv6 remote vpn-sid** *vpn-sid-value* **endpoint** *endpoint-addr* [**secondary** | **bypass**]	Configure the remote end of the EVPL stance.
7	Raisecom(config-evpn-evpl)#**local-service-id** *local-service-id* **remote-service-id** *remote-service-id* Raisecom(config-evpn-evpl)#**exit**	Configure the service IDs of both the local PE and peer PE.
8	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
9	Raisecom(config-port)#**evpn evpl** *evpn-evpl-instance-id*	Configure the interface to be associated with an EVPL instance.

11.6.5 Configuring EVPN VPLS

Configure the EVPN VPLS instance on the PE as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**evpn vpls** *evpn-vpls-instance-id*	Create a EVPN VPLS instance, and enter EVPN VPLS configuration mode.
3	Raisecom(config-evpn-vpls)#**rd** { *ip-address* : *number1* | *as-id* : *number2* }	Configure the RD of the EVPN VPLS instance. **Note** It does not support 0:0.
4	Raisecom(config-evpn-vpls)#**route-target** [**export** | **import** | **both**] { *ip-address* : *number1* | *as-id* : *number2* }	Configure the RT in the ingress and egress directions of the EVPN VPLS instance. **Note** It does not support 0:0.
5	Raisecom(config-evpn-vpls)#**tunnel-policy** *policy-name* Raisecom(config-evpn-vpls)#**exit**	Configure the tunnel that carries the EVPN VPLS instance.
6	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
7	Raisecom(config-port)#**evpn vpls** *evpn-vpls-instance-id*	Configure the EVPN VPLS instance associated with the interface.

11.6.6 Configuring EVPN L3VPN

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**ip vrf** *vrf-name*	Create a VPN route forwarding instance, and enter VPF mode.
3	Raisecom(config-vrf)#**address-family ipv6**	(Optional) enter VRF IPv6 address family configuration mode. Steps 4–6 can be configured in VRF configuration mode or VRF IPv6 address family configuration mode. You can configure step 3 as needed.
4	Raisecom(config-*)#**route-target** [**export** | **import** | **both**] *rt* **evpn**	Configure attributes of the VPN-target extended community for exchanging routes with the EVPN instance for the VRF instance.
5	Raisecom(config-*)#**rd** rd	Configure the RD of the VRF.
6	Raisecom(config-*)#**tunnel binding destination** *ip-address* **tunnel** *tunnel-number*	Configure L3VPN services to be bound with the Tunnel interface.
7	Raisecom(config-*)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
8	Raisecom(config-port)#**ip vrf forwarding** *vrf-name*	Bind the Layer 3 interface to the specified VRF.

11.7 Configuring the VPN tunnel policy

11.7.1 Preparing for configurations

Scenario

After the VPN tunnel policy is configured, it can be quoted to configure the VPN instance.

Prerequisites

N/A

11.7.2 Configuring VPN tunnel policy

Configure the PE as below. Step 3 and step 4 are mutually exclusive, so choose one of them. Before the device supports binding, the system assigns the policy a default tunnel select behavior, namely, cr-lsp > lsp.

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**tunnel-policy** *policy-name*	Create a tunnel policy, and enter tunnel policy configuration mode.
3	Raisecom(config-tunnelpolicy)#**tunnel select-seq** { **cr-lsp** [**lsp**] | **lsp** [**cr-lsp**] | **sr-be-lsp** [**sr-te-tunnel**] | **sr-te-tunnel** [**sr-be-lsp**] }[**load-balance-number** *number*] Raisecom(config-tunnelpolicy)#**exit**	(Optional) configure the VPN tunnel selection policy. • The type and priority order of LSP include LDP LSP -> SR-MPLS-BE -> BGP-LSP. • The types and priority order of cr lsp include MPLS-TE -> SR-TE. When no tunnel policy is configured for services, the system built-in default policy is used, namely, tunnel select cr lsp lsp load balance 1; first iterate RSVP. If it does not exist, iterate SR-TE. If it does not exist, iterate LDP LSP, and then SR-MPLS-BE ->BGP-LSP in sequence. This function is mainly used to solve the inter-IGP-domain scenario where the iteration policy cannot be satisfied when a VPN exists both within and between domains: for VIP services, the VPN should iterate TE; for common services, iterate SR-BE within the domain, and use BGP-LSP between domains.
4	Raisecom(config-tunnelpolicy)#**tunnel binding destination** *peer-ip* **tunnel** *interface-number*	(Optional) bind the tunnel with the destination IP address to restrict the tunnel to carry specified VPN services. The tunnel supports RSVP/SR-TE.

Note

- The device supports the default tunnel policy. By default, the parameter of the tunnel selection policy is cr lsp lsp, which prioritizes the CR-LSP tunnel over the LSP tunnel. When L2VPN/3VPN services are configured, the tunnel policy can be left unspecified, and the default tunnel policy can be used.
- When configuring services, using the **tunnel-policy** *policy-name* command keyword can quote a non-existent tunnel policy, but no tunnel can be iterated at this time.
- A tunnel policy can be bound with up to 32 tunnels and does not support load balancing; in other words, only one record with the same destination can be configured.
- When tunnel binding is configured, the consistency between the destination in the record and the tunnel destination is not verified, and during iteration, only the destination in the binding record is matched.

11.8 Maintenance

Command	Description
Raisecom#**clear ip bgp** [**all** | *ip-address* | **external**] **vrf** *vrf-name* [*as-id*]	Reset all BGP connections or a specified BGP connection in the VRF.

Copyright © Raisecom Technology Co., Ltd.

Command	Description
Raisecom#**clear ip bgp** [**all** | *ip-address* | **external**] **vrf** *vrf-name* [*as-id*] { **in** | **out** | **soft** }	Upgrade all BGP routes or a specified BGP route in the VRF instead of disconnecting BGP connections, namely, soft reset.
Raisecom(config-vrf)#**clear traffic-statistics vrf** *vrf-name*	Clear VRF traffic statistics.

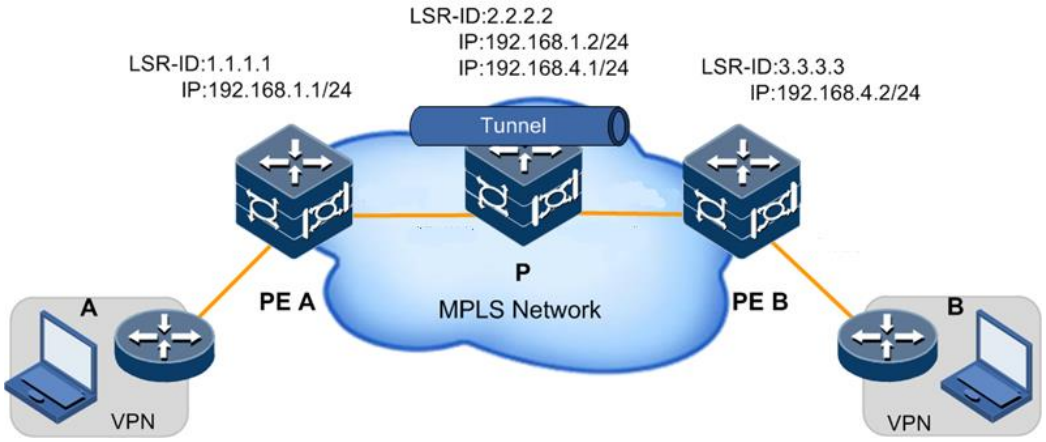
11.9 Configuration examples

11.9.1 Example for configuring static Tunnel to carry static VPWS services

Networking requirements

As shown in Figure 11-3, the user has branches in areas A and B. Branches need to communicate with each other through a point-to-point VPN leased-line. Because the network scale is small and the topology is stable, you can configure bidirectional static LSP between PE A and PE B to work as the public Tunnel of the L2VPN. By default, devices are configured with IP addresses.

Figure 11-3 Configuring static Tunnel to carry static VPWS services



Data preparation

Figure 11-4 lists the data to be configured.

Figure 11-4 Data preparation

Device	LSR-ID	Interface	IP address
PE A	1.1.1.1	gigaethernet 1/2/1	192.168.1.1/24
		loopback 2	1.1.1.1/32

Copyright © Raisecom Technology Co., Ltd.

Device	LSR-ID	Interface	IP address
P	2.2.2.2	gigaethernet 1/2/1	192.168.1.2/24
		gigaethernet 1/2/2	192.168.4.1/24
		loopback 2	2.2.2.2/32
PE B	3.3.3.3	gigaethernet 1/2/1	192.168.4.2/24
		loopback 2	3.3.3.3/32

Configuration steps

Step 1 For how to configure static Tunnels, refer to 9.7.1 Example for configuring static bidirectional LSP with IP capability.

Step 2 Configure the static L2VC.

Configure PE A.

```
PEA(config)#interface gigaethernet 1/2/2
PEA(config-gigaethernet1/2/2)#mode l2
PEA(config-gigaethernet1/2/2)#mpls static-l2vc destination 3.3.3.3 raw
vc-id 1 in-label 101 out-label 101 tunnel 1/1/1
PEA(config-gigaethernet1/2/2)#exit
```

Configure PE B.

```
PEB(config)#interface gigaethernet 1/2/2
PEB(config-gigaethernet1/2/2)#mode l2
PEB(config-gigaethernet1/2/2)#mpls static-l2vc destination 1.1.1.1 raw
vc-id 1 in-label 101 out-label 101 tunnel 1/1/1
PEB(config-gigaethernet1/2/2)#exit
```

Checking results

Use the **show mpls l2vc static** command to check whether static VPWS configurations of PE A and PE B are correct.

- Show static VPWS configuration of PE A.

```
PEA(config)#show mpls l2vc static
Client interface         : gigaethernet1/2/2
  Pw index               : 1
  Vc id                  : 1
  Encapsulation type       : raw
  Ac fault relay action    : relay
```


Copyright © Raisecom Technology Co., Ltd.

```
  Destination             : 3.3.3.3
  Tunnel policy           : --
  Tunnel type             : mplsTe
  Tunnel number           : 1/1/1
  Local vc label          : 101
  Remote vc label         : 101
  Ac status               : down(*bfd:<L:up,R:up>, *cc:<L:up,R:up>)
  Pw state                : down(*bfd:<L:up,R:up>, *cc:<L:up,R:up>, sd:up,
cd:up)
  Vc state                : down
  Vc signal               : manual
  Local cw                : enable
  Operational cw          : enable
  Local vc mtu            : 9600
  Remote vc mtu           : --
  Tpid                    : 0x8100
  Svlan                   : --
  Pw role                 : PrimaryPw
  Pw work status          : Working
  Pw access mode          : mesh
  Pw QosMode              : --
  Pw Bandwidth Cir        : --
  Pw Bandwidth Pir        : --
  Pw Bandwidth Valid      : InValid
  Pw Weight               : --
  Pw Flow Queue           : --
  Pw DsMode               : Uniform
  Pw PipeServClass        : --
  Pw Exp2LocalPriMap      : Default
  Pw LocalPri2ExpMap      : Default
  Pw ShortPipeTrust       : --
  Pw Cos2LocalPriMap      : Default
  Pw Dscp2LocalPriMap     : Default
  Create time             : 1980-01-05,07:14:40
  Up time                 : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time        : 1980-01-05,07:14:40
------------------------------------------
```

- Show static VPWS configurations of PE B.

```
PEB(config)#show mpls l2vc static

  Client interface    : gigaethernet1/2/2
  Pw index          : 4
  Vc id             : 1
  Encapsulation type  : raw
  Ac fault relay action     : relay
  Destination             : 1.1.1.1
  Tunnel policy           : --
  Tunnel type             : mplsTe
  Tunnel number      : 1
  Local vc label     : 102
  Remote vc label    : 102
```


Copyright © Raisecom Technology Co., Ltd.

```
Ac status         : down
Pw state          : down
Vc state          : down
Vc signal         : manual
Local cw          : enable
Operational cw     : enable
Local vc mtu       : 9600
Remote vc mtu      : --
Tpid              : 0x8100
Svlan             : --
Pw role           : PrimaryPw
Pw work status     : Working
Pw access mode     : mesh
Pw QosMode        : --
Pw Bandwidth Cir   : --
Pw Bandwidth Pir   : --
Pw Bandwidth Valid  : InValid
Pw Weight         : --
Pw Flow Queue      : --
Pw DsMode         : Uniform
Pw PipeServClass   : --
Pw Exp2LocalPriMap  : 0
Pw LocalPri2ExpMap  : 0
Pw ShortPipeTrust        : --
Pw Cos2LocalPriMap       : Default
Pw Dscp2LocalPriMap      : Default
Create time       : 2000-11-11,16:18:27
Up time           : 0 days, 0 hours, 0 minutes, 0 seconds
Last change time   : 2000-11-11,16:18:27
```

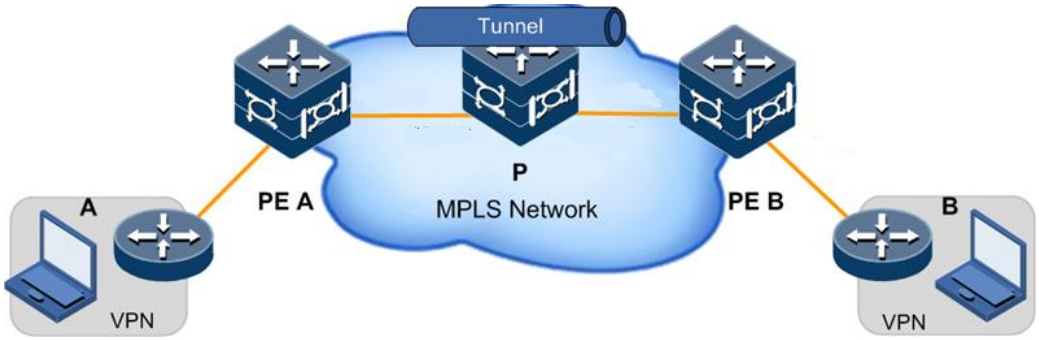
11.9.2 Example for configuring RSVP-TE-based static Tunnel to carry dynamic VPWS services

Networking requirements

As shown in Figure 11-5, the user has branches in areas A and B. Branches need to communicate with each other through a point-to-point VPN leased-line. To facilitate network maintenance and reduce manual intervention, you can configure the RSVP-TE-based static Tunnel to carry dynamic VPWS services to meet user's leased-line telecommunication requirements. By default, devices are configured with IP addresses.

Copyright © Raisecom Technology Co., Ltd.

Figure 11-5 Configuring RSVP-TE-based static Tunnel to carry dynamic VPWS services



Data preparation

Table 11-3 lists the data to be configured.

Table 11-3 Data preparation

Device	LSR-ID	Interface	IP address
PE A	1.1.1.1	gigaethernet 1/2/1	192.168.1.1/24
		loopback 2	1.1.1.1/32
P	2.2.2.2	gigaethernet 1/2/1	192.168.1.2/24
		gigaethernet 1/3/2	192.168.4.1/24
		loopback 2	2.2.2.2/32
PE B	3.3.3.3	gigaethernet 1/2/1	192.168.4.2/24
		loopback 2	3.3.3.3/32

Configuration steps

Step 1 For how to configure dynamic Tunnels based on RSVP-TE, refer to 9.7.3 Example for configuring dynamic LSP based on RSVP-TE.

Step 2 Configure static L2VC.

Configure PE A.

```
PEA(config)#interface gigaethernet 1/2/2
PEA(config-gigaethernet1/2/2)#mode l2
PEA(config-gigaethernet1/2/2)#mpls static-l2vc destination 3.3.3.3 raw
vc-id 1 in-label 101 out-label 101 tunnel 1/1/1
PEA(config-gigaethernet1/2/2)#exit
```

Configure PE B.

Copyright © Raisecom Technology Co., Ltd.

```
PEB(config)#interface gigaethernet 1/2/2
PEB(config-gigaethernet1/2/2)#mode l2
PEB(config-gigaethernet1/2/2)#mpls static-l2vc destination 1.1.1.1 raw
vc-id 1 in-label 101 out-label 101 tunnel 1/1/1
PEB(config-gigaethernet1/2/2)#exit
```

Checking results

Use the **show mpls l2vc** command to show whether static VPWS configurations of PE A and PE B are correct.

- Show static VPWS configurations of PE A.

```
PEA(config)#show mpls l2vc gigaethernet 1/2/2
Client interface         : gigaethernet1/2/2
  Pw index               : 2
  Session State           : up
  Vc id                  : 1
  Encapsulation type      : raw
  Ac fault relay action    : relay
  Destination            : 3.3.3.3
  Tunnel policy           : --
  Tunnel type            : mplsTe
  Tunnel number           : 1/1/1
  Local vc label          : 10241
  Remote vc label         : --
  Ac status              : down(*bfd:<L:up,R:up>, *cc:<L:up,R:up>)
  Pw state               : down(*bfd:<L:up,R:up>, *cc:<L:up,R:up>, sd:up,
cd:up)
  Vc state               : down
  Local statuscode        : 0xb
  Remote statuscode       : 0x1
  Vc signal              : pwIdFecSignaling
  Local cw               : enable
  Operational cw          : enable
  Local vc mtu           : 9600
  Remote vc mtu           : --
  Tpid                   : 0x8100
  Svlan                  : --
  Pw role                : PrimaryPw
  Pw work status          : Working
  Pw access mode          : mesh
  Pw QosMode             : --
  Pw Bandwidth Cir        : --
  Pw Bandwidth Pir        : --
  Pw Bandwidth Valid       : InValid
  Pw Weight              : --
  Pw Flow Queue           : --
  Pw DsMode              : Uniform
  Pw PipeServClass        : --
  Pw Exp2LocalPriMap      : Default
  Pw LocalPri2ExpMap      : Default
  Pw ShortPipeTrust       : --
```


Copyright © Raisecom Technology Co., Ltd.

```
  Pw Cos2LocalPriMap       : Default
  Pw Dscp2LocalPriMap      : Default
  Create time             : 1980-01-05,23:58:00
  Up time                : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time         : 1980-01-05,23:58:00
--------------------------------------
```

- Show static VPWS configurations of PE B.

```
PEB(config)#show mpls l2vc gigaethernet 1/2/2
  Client interface   : gigaethernet 1/2/2
  Pw index          : 4
  Session State      : down
  Vc id             : 1
  Encapsulation type  : raw
  Ac fault relay action     : relay
  Destination             :1.1.1.1
  Tunnel policy           : --
  Tunnel type             : mplsTe
  Tunnel number           : 1/1/1
  Local vc label     : 10243
  Remote vc label    : --
  Ac status         : down
  Pw state          : down
  Vc state          : down
  Local statuscode   : 0xa
  Remote statuscode  : 0x0
  Vc signal         : pwIdFecSignaling
  Local cw          : enable
  Operational cw     : enable
  Local vc mtu       : 9600
  Remote vc mtu      : --
  Tpid              : 0x8100
  Svlan             : --
  Pw role           : PrimaryPw
  Pw work status     : Working
  Pw access mode     : mesh
  Pw QosMode        : --
  Pw Bandwidth Cir   : --
  Pw Bandwidth Pir   : --
  Pw Bandwidth Valid  : InValid
  Pw Weight         : --
  Pw Flow Queue      : --
  Pw DsMode         : Uniform
  Pw PipeServClass   : --
  Pw Exp2LocalPriMap  : 0
  Pw LocalPri2ExpMap  : 0
  Pw ShortPipeTrust        : --
  Pw Cos2LocalPriMap       : Default
  Pw Dscp2LocalPriMap      : Default
  Create time       : 2014-07-25,10:13:17
  Up time           : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time   : 2014-07-25,10:13:17
```


Copyright © Raisecom Technology Co., Ltd.

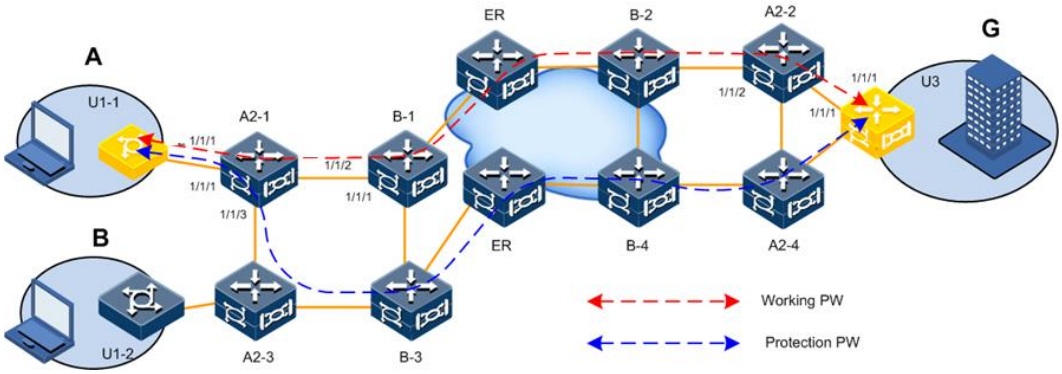
11.9.3 Example for configuring MPLS L2VPN typical networking

Networking requirements

As shown in Figure 11-6, the headquarter G exchanges leased-line services with branch A over the IP RAN where end-to-end communication is implemented through multi-section PW and protection implemented by deploying active/standby Tunnel and active/standby PW. In this networking topology, the IP RAN device is named based on the network where it resides, which should be the same with the carrier network name. For example, U1 is the client-side IPRAN access device. A2 is the network-side access device. And B is the aggregation core layer device.

- Deploy active/standby static PWs between U1-1 and A2-1, and U3 and A2-1.
- Deploy active/standby dynamic PWs between A2-1 and B-1, and A2-2 and B-2.
- Deploy dynamic PWs between B-1 and B-2, and B-3 and B-4.
- Configure static-to-dynamic PW on A2-1 and A2-2 respectively.
- Configure dynamic-to-dynamic PW on B-1, B-2, B-3, and B-4.
- The configuration process is similar, so this section only takes the configurations of B-1/B-3 device from the branch side to the core network for example. Configurations for the headquarter-side devices will not be detailed.

Figure 11-6 Configuring MPLS L2VPN services



Configuration principle

- Configure LSR-ID on U1, A2, and B. Enable MPLS globally. Enable LDP on A2 and B globally.
- Configure the IP address of the service interface and loopback interface planned by U1, A2, and B.
- Configure the active/standby static Tunnel between U1-1 and A2-1 and configure the active/standby static PW.
- Enable OSPF on A2-1, B-1, and B-3. Advertise and learn routes over the entire network.
- Enable LDP sessions on A2-1, B-1, and B-3 and establish LDP remote sessions respectively, preparing for the assignment of PW labels.
- Configure active/standby PWs on A2-1, B-1, and B-3 respectively. The labels are automatically distributed according to LDP.
- Configure the static-to-dynamic PW on A2.
- Enable BFD and establish PW redundancy protection.

Copyright © Raisecom Technology Co., Ltd.

- (Optional) configure QoS rate limiting for the PW.

Data preparation

Table 11-4 lists the data to be configured.

Table 11-4 Data preparation

Device	LSR-ID	Interface	IP address
U1-1	1.1.1.1	gigaethernet 1/1/1	10.10.1.1/24
		hundredgige 1/2/1.100	10.10.10.2/24
		loopback 2	1.1.1.1/32
A2-1	2.2.2.2	gigaethernet 1/1/1	10.10.1.2/24
		gigaethernet 1/1/2	10.10.2.1/24
		gigaethernet 1/1/3	100.10.1.1/24
		loopback 2	2.2.2.2/32
B-1	3.3.3.3	gigaethernet 1/1/1	10.10.2.2/24
		loopback 2	3.3.3.3/32
B-3	5.5.5.5	gigaethernet 1/1/1	10.10.5.1/24
		loopback 2	5.5.5.5/32

Note

Loopback 1 is a dedicated interface for the DCN network management. To prevent conflicts, loopback 1 interface is prohibited. You can enable another loopback interface of which the IP address can be used as the IP address of the LSR-ID. Loopback 2 is used in this example.

Configuration steps

Step 1 Configure MPLS globally.

U1-1

```
U1-1(config)#mpls lsr-id 1.1.1.1
U1-1(config)#mpls enable
```

A2-1

```
A2-1(config)#mpls lsr-id 2.2.2.2
A2-1(config)#mpls enable
```


Copyright © Raisecom Technology Co., Ltd.

```
A2-1(config)#mpls ldp
```

B-1

```
B-1(config)#mpls lsr-id 3.3.3.3
B-1(config)#mpls enable
B-1(config)#mpls ldp
```

B-3

```
B-3(config)#mpls lsr-id 5.5.5.5
B-3(config)#mpls enable
B-3(config)#mpls ldp
```

Step 2 Configure the IP address of the planning interface and enable LDP session.

U1-1

```
U1-1(config)#interface loopback 2
U1-1(config-loopback2)#ip address 1.1.1.1 255.255.255.255
U1-1(config-loopback2)#interface gigaethernet 1/1/1
U1-1(config-gigaethernet1/1/1)#ip address 10.10.1.1 255.255.255.0
U1-1(config-gigaethernet1/1/1)#exit
```

A2-1

```
A2-1(config)#interface loopback 2
A2-1(config-loopback2)#ip address 2.2.2.2 255.255.255.255
A2-1(config-loopback2)#interface gigaethernet 1/1/1
A2-1(config-gigaethernet1/1/1)#ip address 10.10.1.2 255.255.255.0
A2-1(config-gigaethernet1/1/1)#interface gigaethernet 1/1/2
A2-1(config-gigaethernet1/1/2)#ip address 10.10.2.1 255.255.255.0
A2-1(config-gigaethernet1/1/2)#mpls ldp
A2-1(config-gigaethernet1/1/2)#interface gigaethernet 1/1/3
A2-1(config-gigaethernet1/1/3)#ip address 100.10.1.1 255.255.255.0
A2-1(config-gigaethernet1/1/3)#mpls ldp
/*configure the IP address of the interface on the ring and enable LDP.
```

B-1

```
B-1(config)#interface loopback 2
B-1(config-loopback2)#ip address 3.3.3.3 255.255.255.255
```


Copyright © Raisecom Technology Co., Ltd.

```
B-1(config-loopback2)#interface gigaethernet 1/1/1
B-1(config-gigaethernet1/1/1)#ip address 10.10.2.2 255.255.255.0
B-1(config-gigaethernet1/1/1)#mpls ldp
```

B-3

```
B-3(config)#interface loopback 2
B-3(config-loopback2)#ip address 5.5.5.5 255.255.255.255
B-3(config-loopback2)#interface gigaethernet 1/1/1
B-3(config-gigaethernet1/1/1)#ip address 10.10.5.1 255.255.255.0
B-3(config-gigaethernet1/1/1)#mpls ldp
```

Step 3 Configure static active/standby Tunnel between U1-1 and A2-1.

- Configure active Tunnel on U1-1.

```
U1-1(config)#interface tunnel 1/1/1
U1-1(config-tunnel1/1/1)#tunnel mode mpls
U1-1(config-tunnel1/1/1)#mpls tunnel-id 1
U1-1(config-tunnel1/1/1)#destination 2.2.2.2
U1-1(config-tunnel1/1/1)#mpls te commit
U1-1(config-tunnel1/1/1)#exit
U1-1(config)#mpls bidirectional static-lsp ingress lsp1-1 lsr-id 2.2.2.2
tunnel-id 1
U1-1(config-ingress-lsp)#forward 2.2.2.2 255.255.255.255 nexthop
10.10.1.2 out-label 101
U1-1(config-ingress-lsp)#backward in-label 102
U1-1(config-ingress-lsp)#exit
```

- Configure a standby Tunnel on U1-1.

```
U1-1(config)#interface tunnel 1/1/2
U1-1(config-tunnel1/1/1)#tunnel mode mpls
U1-1(config-tunnel1/1/2)#mpls tunnel-id 2
U1-1(config-tunnel1/1/2)#destination 2.2.2.2
U1-1(config-tunnel1/1/2)#mpls te commit
U1-1(config-tunnel1/1/2)#exit
U1-1(config)#mpls bidirectional static-lsp ingress lsp1-2 lsr-id 2.2.2.2
tunnel-id 2
U1-1(config-ingress-lsp)#forward 2.2.2.2 255.255.255.255 nexthop
10.10.1.2 out-label 103
U1-1(config-ingress-lsp)#backward in-label 104
```

- Configure active Tunnel on A2-1.

Copyright © Raisecom Technology Co., Ltd.

```
A2-1(config)#interface tunnel 1/1/1
A2-1(config-tunnel1/1/1)#tunnel mode mpls
A2-1(config-tunnel1/1/1)#mpls tunnel-id 1
A2-1(config-tunnel1/1/1)#destination 1.1.1.1
A2-1(config-tunnel1/1/1)#mpls te commit
A2-1(config-tunnel1/1/1)#exit
A2-1(config)#mpls bidirectional static-lsp egress lsp1-1 lsr-id 1.1.1.1
tunnel-id 1
A2-1(config-ingress-lsp)#forward in-label 101
A2-1(config-ingress-lsp)#backward 1.1.1.1 255.255.255.255 nexthop
10.10.1.1 out-label 102
```

- Configure standby Tunnel on A2-1.

```
A2-1(config)#interface tunnel 1/1/1
A2-1(config-tunnel1/1/1)#tunnel mode mpls
A2-1(config-tunnel1/1/1)#mpls tunnel-id 2
A2-1(config-tunnel1/1/2)#destination 1.1.1.1
A2-1(config-tunnel1/1/2)#mpls te commit
A2-1(config-tunnel1/1/2)#exit
A2-1(config)#mpls bidirectional static-lsp egress lsp1-1 lsr-id 1.1.1.1
tunnel-id 2
A2-1(config-ingress-lsp)#forward in-label 103
A2-1(config-ingress-lsp)#backward 1.1.1.1 255.255.255.255 nexthop
10.10.1.1 out-label 104
```

Step 4 Configure a static PW between U1-1 and A2-1.

U1-1

```
U1-1(config)#interface hundredgige 1/2/1.1
U1-1(config-gigaethernet1/2/1.1)#encapsulation dot1Q 1
U1-1(config-gigaethernet1/2/1.1)#mode l2
U1-1(config-gigaethernet1/2/1.1)#mpls static-l2vc destination 2.2.2.2 raw
vc-id 1 in-label 201 out-label 201 tunnel 1/1/1
U1-1(config-gigaethernet1/2/1.1)#mpls static-l2vc destination 2.2.2.2 raw
vc-id 2 in-label 202 out-label 202 tunnel 1/2/1 backup
```

Step 5 Enable OSPF on U1, A2, and B and advertise routes.

U1-1

```
U1-1(config)#router ospf 1
U1-1(config-router-ospf)#network 1.1.1.1 255.255.255.255 area 0
U1-1(config-router-ospf)#network 10.10.1.1 255.255.255.0 area 0
U1-1(config-router-ospf)#exit
```


Copyright © Raisecom Technology Co., Ltd.

A2-1

```
A2-1(config)#router ospf 1
A2-1(config-router-ospf)#network 2.2.2.2 255.255.255.255 area 0
A2-1(config-router-ospf)#network 10.10.1.2 255.255.255.0 area 0
A2-1(config-router-ospf)#network 10.10.2.1 255.255.255.0 area 0
A2-1(config-router-ospf)#network 100.10.1.1 255.255.255.0 area 0
A2-1(config-router-ospf)#exit
```

B-1

```
B-1(config)#router ospf 1
B-1(config-router-ospf)#network 3.3.3.3 255.255.255.255 area 0
B-1(config-router-ospf)#network 10.10.2.2 255.255.255.0 area 0
B-1(config-router-ospf)#exit
```

B-3

```
B-3(config)#router ospf 1
B-3(config-router-ospf)#network 5.5.5.5 255.255.255.255 area 0
B-3(config-router-ospf)#network 10.10.5.1 255.255.255.0 area 0
B-3(config-router-ospf)#exit
```

Step 6 Establish LDP sessions between A2-1, B-1, and B-3.

A2-1

```
A2-1(config)#mpls ldp targeted neighbour 3.3.3.3
/*Configure an active LDP pointing to B-1.*/
A2-1(config)#mpls ldp targeted neighbour 5.5.5.5
/*Configure a standby LDP pointing to B-3.*/
```

B-1

```
B-1(config)#mpls ldp targeted neighbour 2.2.2.2
/*Configure a standby LDP pointing to A2-1.*/
```

B-3

```
B-3(config)#mpls ldp targeted neighbour 2.2.2.2
/*Configure a standby LDP pointing to A2-1.*/
```


Copyright © Raisecom Technology Co., Ltd.

Step 7 Configure a static-to-dynamic PW on A2-1.

```
A2-1(config)#mpls switch-l2vc 1.1.1.1 1 in-label 201 out-label 201 tunnel
1/1/1 between 3.3.3.3 14 raw
/*static-to-dynamic active PW*/
A2-1(config)#mpls switch-l2vc 1.1.1.1 2 in-label 202 out-label 202 tunnel
1/2/2 between 5.5.5.5 15 raw
/* static-to-dynamic standby PW*/
```

Step 8 Enable BFD on U1-1 and establish PW FRR redundancy protection.

```
U1-1(config)#interface gigaethernet 1/2/1.1
U1-1(config-gigaethernet1/2/1.1)#mpls l2vpn pw bfd
U1-1(config-gigaethernet1/2/1.1)#mpls l2vpn pw bfd backup
U1-1(config-gigaethernet1/2/1.1)#mpls l2vpn redundancy master switch-mode
revertive wtr-time 120
```

Checking results

- Use the **show mpls l2vc** command to show PW working status.

```
U1-1#show mpls l2vc
Client interface         : tengigabitethernet1/2/1.1
  Pw index               : 1
  Vc id                  : 1
  Encapsulation type       : raw
  Ac fault relay action    : relay
  Destination            : 2.2.2.2
  Tunnel policy          : --
  Tunnel type            : mplsTe
  Tunnel number          : 1/1/1
  Local vc label         : 201
  Remote vc label        : 201
  Ac status              : up(bfd:up, cc:up)
  Pw state               : up(bfd:up, cc:up)
  Vc state               : up
/*If the above three items are all Up, the PW is configured successfully
and devices can communicate with each other. If AC is Down, it indicates
that the UNI is not Up. If PW is Down, it indicates that the NNI is not
Up, the PW parameters are inconsistent, or the network-side routes are
non-reachable.*/
  Vc signal              : manual
  Local cw               : enable
  Operational cw         : enable
  Local vc mtu           : 9600
  Remote vc mtu          : --
  Tpid                   : 0x8100
  Svlan                  : --
```


Copyright © Raisecom Technology Co., Ltd.

```
  Pw role                : PrimaryPw
  Pw work status          : Working
  Pw access mode          : mesh
  Pw QosMode             : --
  Pw Bandwidth Cir        : --
  Pw Bandwidth Pir        : --
  Pw Bandwidth Valid      : InValid
  Pw Weight              : --
  Pw Flow Queue           : --
  Pw DsMode              : Uniform
  Pw PipeServClass        : --
  Pw Exp2LocalPriMap      : Default
  Pw LocalPri2ExpMap      : Default
  Pw ShortPipeTrust       : --
  Pw Cos2LocalPriMap      : Default
  Pw Dscp2LocalPriMap     : Default
  Create time            : 1970-03-21,12:36:32
  Up time                : 0 days, 0 hours, 1 minutes, 20 seconds
  Last change time        : 1970-03-21,12:36:32
----------------------------------------
  Client interface        : tengigabitethernet1/2/1.1
  Pw index               : 3
  Vc id                  : 2
  Encapsulation type      : raw
  Ac fault relay action    : relay
  Destination            : 2.2.2.2
  Tunnel policy           : --
  Tunnel type            : mplsTe
  Tunnel number           : 1/1/1
  Local vc label          : 202
  Remote vc label         : 202
  Ac status              : up(bfd:up, cc:up)
  Pw state               : up(bfd:up, cc:up)
  Vc state               : up
  Vc signal              : manual
  Local cw               : enable
  Operational cw          : enable
  Local vc mtu           : 9600
  Remote vc mtu          : --
  Tpid                   : 0x8100
  Svlan                  : --
  Pw role                : SecondaryPw
  Pw work status          : NoWorking
  Pw access mode          : mesh
  Pw QosMode             : --
  Pw Bandwidth Cir        : --
  Pw Bandwidth Pir        : --
  Pw Bandwidth Valid      : InValid
  Pw Weight              : --
  Pw Flow Queue           : --
  Pw DsMode              : Uniform
  Pw PipeServClass        : --
  Pw Exp2LocalPriMap      : Default
  Pw LocalPri2ExpMap      : Default
  Pw ShortPipeTrust       : --
```


Copyright © Raisecom Technology Co., Ltd.

```
  Pw Cos2LocalPriMap       : Default
  Pw Dscp2LocalPriMap      : Default
  Create time             : 1970-03-21,12:37:36
  Up time                 : 0 days, 0 hours, 0 minutes, 16 seconds
  Last change time         : 1970-03-21,12:37:36
---------------------------------------
Total l2vc : 2   2 up   0 down
```

- Use the **show mpls ldp targeted neighbour** command to check the status of LDP neighbor sessions.

```
A2-1#show mpls ldp targeted neighbor
LDP Remote Entity Information
------------------------------------------------------------------------
Remote Peer IP           : 3.3.3.3        LDP ID               : 2.2.2.2:0
Transport Address        : 2.2.2.2        LDP AdminStatus          : Up
LDP OperStatus           : Up           Configured Keepalive Timer : 45Sec
Configured Hello Timer    : 45 Sec       Negotiated Hello Timer    : 45Sec
BFD configuration        : Disable        Bfd Session ID           : 0
Hello Packet sent/received : 40698/44929
------------------------------------------------------------------------
Remote Peer IP           : 5.5.5.5        LDP ID               : 2.2.2.2:0
Transport Address        : 2.2.2.2        LDP AdminStatus          : Up
LDP OperStatus           : Up           Configured Keepalive Timer : 45Sec
Configured Hello Timer    : 45 Sec       Negotiated Hello Timer    : 45Sec
BFD configuration        : Disable        Bfd Session ID           : 0
Hello Packet sent/received : 40698/44929
------------------------------------------------------------------------
TOTAL : 2 Remote-Peer(s) Found.
/*the remote LDP session exists and it is Up, which indicates that it is
normal.*/
```

- Use the **show mpls ldp interface** command to show whether physical layer interface is enabled with LDP.

```
A2-1#show mpls ldp interface

LDP Interface Information
------------------------------------------------------------------------
If-Name   LDP STATUS  LAM  TransportAddress HelloSent/Rcv  LDP OperStatus
------------------------------------------------------------------------
GE1/1/1      Disable    DU      --              0/0
GE1/1/2      Enable     DU      2.2.2.2         99809/12682       Up
GE1/1/3      Enable     DU      2.2.2.2         122206/122129     Up
GE1/1/4      Disable    DU      --             0/0          --
GE1/2/1      Disable    DU      --             0/0          --
……
------------------------------------------------------------------------
LAM: Label Advertisement Mode       IF-Name: Interface name
```


Copyright © Raisecom Technology Co., Ltd.

- Use the **show mpls ldp session** command to show LDP sessions and the running status.

```
A2-1#show mpls ldp session

LDP Session Information
LDP Session Count : 2
------------------------------------------------------------------------------
Peer-ID           Status        LAM     SsnRole   SsnAge     KA-Sent/Rcv
------------------------------------------------------------------------------
3.3.3.3:0         Operational    DU      Passive   0000:06:37  1587/1587
5.5.5.5:0         Operational    DU      Passive   0000:06:37  1587/1587
------------------------------------------------------------------------------
TOTAL: 2 Session(s) Found.
LAM : Label Advertisement Mode     SsnAge Unit : DDDD:HH:MM
```

- After step 7, you can use the **show mpls switch-l2vc** command to show configurations of PW switching.

```
A2-1#show mpls switch-l2vc
Switch-l2vc type   :            SVC <---> LDP            (BACKUP)
  Peer ip address    :        1.1.1.1 <---> 3.3.3.3        --
  Encapsulation type  :           raw <---> raw           --
/*The RAW/TAG mode of the two PW segments must be the same. */
  Vc id            :             1 <---> 14            --
  Fault relay       :           off
  Vc state          :            up <---> up           --
  Local statuscode   :           0x0 <---> 0x0           --
  Remote statuscode  :           0x0 <---> 0x0           --
  Pw state          :            up <---> up           --
  Bfd state         :            up <---> up           --
  Cc state          :            up <---> up           --
  Sd state          :            up <---> up           --
  In label          :           201 <---> 10247         --
  Out label         :           201 <---> 10241         --
/*The VC-Label of the dynamic PW is automatically assigned. It must have
a value.*/
  Local cw          :         enable <---> enable         --
  Operational cw     :         enable <---> enable         --
  Local vc mtu      :          9600 <---> 9600          --
  Remote vc mtu     :          9600 <---> 9600          --
/*The MTUs of the two PW segments must be the same.*/
  Tunnel policy     :            -- <---> --            --
  Tunnel number     :         1/3/1 <---> --            --
  Out xc index      :            -- <---> 1522          --
/*LSP interface index, for dynamic PW, this item must have a value.*/
  Out ecmp index     :            -- <---> --            --
  Pw QosMode        :           -- <---> --           --
  Pw Bandwidth Cir   :            -- <---> --            --
  Pw Bandwidth Pir   :            -- <---> --            --
  Pw Bandwidth Valid  :        InValid <---> InValid        --
  Pw Weight         :           -- <---> --           --
  Pw Flow Queue      :            -- <---> --            --
```


Copyright © Raisecom Technology Co., Ltd.

```
  Work satus         :        working <---> working        --
-------------------------------------------------------------------------
Switch-l2vc type    :           SVC <---> LDP           (BACKUP)
  Peer ip address     :        1.1.1.1 <---> 3.3.3.3        --
  Encapsulation type  :            raw <---> raw            --
  Vc id             :            2 <---> 15            --
  Fault relay        :           off
  Vc state          :            up <---> up            --
  Local statuscode    :           0x0 <---> 0x0           --
  Remote statuscode   :           0x0 <---> 0x0           --
  Pw state          :            up <---> up            --
  Bfd state         :            up <---> up            --
  Cc state          :            up <---> up            --
  Sd state          :            up <---> up            --
  In label          :           202 <---> 10248          --
  Out label         :           202 <---> 10242          --
  Local cw          :         enable <---> enable         --
  Operational cw     :         enable <---> enable         --
  Local vc mtu       :          9600 <---> 9600           --
  Remote vc mtu      :          9600 <---> 9600           --
  Tunnel policy      :            -- <---> --            --
  Tunnel number      :          1/3/2 <---> --            --
  Out xc index       :            -- <---> 1523          --
  Out ecmp index     :            -- <---> --            --
  Pw QosMode        :            -- <---> --            --
  Pw Bandwidth Cir    :            -- <---> --            --
  Pw Bandwidth Pir    :            -- <---> --            --
  Pw Bandwidth Valid  :        InValid <---> InValid        --
  Pw Weight         :            -- <---> --            --
  Pw Flow Queue      :            -- <---> --            --
  Work satus         :        working <---> working        --
```

- After all configurations are complete, you can execute the Ping operation based on MPLS VC to check the connectivity of the L2VPN.

```
U1-1#ping mpls vc-id 1 destination 2.2.2.2
Sending 5, 200-byte MPLS Echoes to 2.2.2.2,VC ID is 1, timeout is 3
seconds,send interval is 1 seconds,
Press CTRL + C to abort:
Reply from 3.3.3.3: bytes=84, Sequence=1, time<1ms.
Reply from 3.3.3.3: bytes=84, Sequence=2, time<1ms.
Reply from 3.3.3.3: bytes=84, Sequence=3, time<1ms.
Reply from 3.3.3.3: bytes=84, Sequence=4, time<1ms.
Reply from 3.3.3.3: bytes=84, Sequence=5, time<1ms.
---- PING Statistics----
5 packets transmitted,5 packets received,
Success rate is 100 percent(5/5),
round-trip (ms)  min/avg/max = 0/0/0
```

- Use the **show bfd state** command to show BFD status.

Copyright © Raisecom Technology Co., Ltd.

```
U1-1#show bfd state
SessionId State co-Tx-Interval(ms) co-Rx-Interval(ms) co-Detect-
Interval(ms)
------------------------------------------------------------------
129      Up       10              10              30
130      Up       10              10              30
```

Common questions

After a LDP session is configured, it is not Up.

- Check whether the network-side interface IP address is correctly configured.
- Check whether the OSPF route is enabled and whether routes of the entire network have been advertised and learned.
- Check whether the NNI is enabled with LDP.
- Check whether the NNI is up.

After static-to-dynamic PW switching is configured, the PW is not Up.

- Check whether the UNI of PE3 is configured with a dynamic PW.
- Check whether the UNI of PE3 is Up.
- Check whether the binding between the static tunnel and the PW is correct in the PW switching configuration. That is, the tunnel should be bound to the static PW at the local end.
- Check whether the MTU, Raw/Tag, MTU, TPID, and control word of the two PWs are the same.

The end-to-end PW cannot be pinged through.

- Check whether the configuration of the tunnel parameters is correct and whether the status is Up.
- Check whether LDP is Up.
- Check whether the static PW and dynamic PW are up.
- Check whether the interface planning is consistent with the network topology.
- Check whether the configuration process is correct.

11.9.4 Examples for configuring MPLS L3VPN typical networking

Networking requirements

Figure 11-7 shows a mobile backhaul CE+L3VPN network solution. The base station is connected to device A which functions as the CE on the service network. CE 1 and CE 2 belong to VPN1, which are accessed to the MPLS L3VPN network through PE 1 and PE 2. The RT of VPN 1 is 1:100. Different VPN users cannot access each other. Run OSPF between PE 1 and PE 2 and configure interconnection of public network routes. Configure MP-BGP between PE 1 and PE 2 for advertising L3VPN private network routes. Configure static routes between PEs and CEs. This completes the deployment of the mobile backhaul network.

Copyright © Raisecom Technology Co., Ltd.

Figure 11-7 Configuring L3VPN networking

Configuration principle

- Configure basic MPLS functions on PE devices and configure VRF.
- Configure the IP addresses of the interfaces on PE and CE devices.
- After configuring the IP address of the PE client-side interface, bind the VRF to the client-side interface.
- Enable OSPF public network routes between PE 1 and PE 2.
- Configure a MPLS static public network tunnel between PE 1 and PE 2.
- Enable MP-IBGP routes between PE 1 and PE 2, and enable VPNv4.
- Configure a static route between the PE and the CE. Configure the static VRF-based private network route to the CE on the PE and configure the gateway from the CE to the PE.

Data preparation

Table 11-5 lists the data to be configured.

Table 11-5 Data configuration

Device	LSR-ID	Interface	IP address
CE 1	–	gigaethernet 1/2/1	10.10.10.1/24
		Loopback 2	5.5.5.5/32
PE 1	1.1.1.1	gigaethernet 1/2/1	10.10.10.2/24
		gigaethernet 1/2/2	10.10.1.1/24
		Loopback 2	1.1.1.1/32
P	2.2.2.2	gigaethernet 1/2/1	10.10.1.2/24
		gigaethernet 1/2/2	10.10.3.1/24
		Loopback 2	2.2.2.2/32
PE 2	4.4.4.4	gigaethernet 1/2/1	10.10.4.1/24

Copyright © Raisecom Technology Co., Ltd.

Device	LSR-ID	Interface	IP address
		gigaethernet 1/2/2	10.10.3.2/24
		Loopback 2	4.4.4.4/32
CE 2	–	gigaethernet 1/2/1	10.10.4.2/24
		Loopback 2	6.6.6.6/32

Configuration steps

Step 1 Configure VRF on PE 1 and PE 2.

PE 1

```
PE1#config
PE1(config)#ip vrf VPN1
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target import 100:1
PE1(config-vrf)#route-target export 100:1
PE1(config-vrf)#exit
```

PE 2

```
PE2#config
PE2(config)#ip vrf VPN1
PE2(config-vrf)#rd 100:1
PE2(config-vrf)#route-target import 100:1
PE1(config-vrf)#route-target export 100:1
PE2(config-vrf)#exit
```

Step 2 Configure the IP address of related interfaces of CE 1, CE 2, PE 1, PE 2, and P. Configurations are similar, take PE 1 for example.

PE 1

```
PE1(config)#interface gigaethernet 1/2/2
PE1(config-gigaethernet1/2/2)#ip address 10.10.1.1 255.255.255.0
PE1(config-gigaethernet1/2/2)#interface Loopback 2
PE1(config-Loopback2)#ip address 1.1.1.1 255.255.255.255
PE1(config-Loopback2)#exit
```

Step 3 Configure the IP address of the customer-side interfaces on the PE 1 and PE 2.

PE 1

Copyright © Raisecom Technology Co., Ltd.

```
PE1(config)#interface gigaethernet 1/2/1
PE1(config-gigaethernet1/2/1)#ip address 10.10.10.2 255.255.255.0
```

PE 2

```
PE2(config)#interface gigaethernet 1/2/1
PE2(config-gigaethernet1/2/1)#ip address 10.10.4.1 255.255.255.0
```

Step 4 Bind the customer-side interfaces on PE 1 and PE 2 with VRF.

PE 1

```
PE1(config)#interface gigaethernet 1/2/1
PE1(config-gigaethernet1/2/1)#ip vrf forwarding vpn1
PE1(config-gigaethernet1/2/1)#exit
```

PE 2

```
PE2(config)#interface gigaethernet 1/2/1
PE2(config-gigaethernet1/2/1)#ip vrf forwarding vpn1
PE2(config-gigaethernet1/2/1)#exit
```

Step 5 Configure the route of public network between PE 1 and PE 2.

PE 1

```
PE1(config)#router ospf 1
PE1(config-router-ospf)#network 10.10.1.0 0.0.0.255 area 0
PE1(config-router-ospf)#network 1.1.1.1 0.0.0.0 area 0
PE1(config-router-ospf)#exit
```

P

```
P1(config)#router ospf 1
P1(config-router-ospf)#network 10.10.1.0 0.0.0.255 area 0
P1(config-router-ospf)#network 10.10.3.0 0.0.0.255 area 0
P1(config-router-ospf)#network 2.2.2.2 0.0.0.0 area 0
P1(config-router-ospf)#exit
```

PE 2

Copyright © Raisecom Technology Co., Ltd.

```
PE2(config)#router ospf 1
PE2(config-router-ospf)#network 10.10.3.0 0 0 0.0.0.255 area 0
PE2(config-router-ospf)#network 4.4.4.4 0.0.0.0 area 0
PE2(config-router-ospf)#exit
```

Step 6 is for configuring the static public network tunnels. Step 7 is for configuring dynamic public network tunnels. You can choose one as required.

Step 6 (Optional) configure a static public network tunnel between PE 1 and PE 2.

PE 1

```
PE1(config)#mpls lsr-id 1.1.1.1
PE1(config)#mpls enable
PE1(config)#interface tunnel 1/1/1
PE1(config-tunnel1/1/1)#tunnel mode mpls
PE1(config-tunnel1/1/1)#destination 4.4.4.4
PE1(config-tunnel1/1/1)#mpls tunnel-id 200
PE1(config-tunnel1/1/1)#mpls te commit
PE1(config-tunnel1/1/1)#exit
PE1(config)#mpls static-lsp ingress lsp12 4.4.4.4
255.255.255.255 nexthop 10.10.1.2 out-label 1001 lsr-id 4.4.4.4 tunnel-id
200
PE1(config)#mpls static-lsp egress lsp21 in-label 2003 lsr-id 4.4.4.4
tunnel-id 200
```

P

```
P1(config)#mpls lsr-id 2.2.2.2
P1(config)#mpls enable
P1(config)#mpls static-lsp transit lsp12 in-label 1001 nexthop 10.10.3.2
out-label 1003 lsr-id 1.1.1.1 4.4.4.4 tunnel-id 200
P1(config)#mpls static-lsp transit lsp21 in-label 2001 nexthop 10.10.1.1
out-label 2003 lsr-id 4.4.4.4 1.1.1.1 tunnel-id 200
```

PE 2

```
PE2(config)#mpls lsr-id 4.4.4.4
PE2(config)#mpls enable
PE2(config)#interface tunnel 1/1/1
PE2(config-tunnel1/1/1)#tunnel mode mpls
PE2(config-tunnel1/1/1)#destination 1.1.1.1
PE2(config-tunnel1/1/1)#mpls tunnel-id 200
PE2(config-tunnel1/1/1)#mpls te commit
PE2(config-tunnel1/1/1)#exit
```


Copyright © Raisecom Technology Co., Ltd.

```
PE2(config)#mpls static-lsp egress lsp12 in-label 1003 lsr-id 1.1.1.1
tunnel-id 200
PE2(config)#mpls static-lsp ingress lsp21 1.1.1.1 255.255.255.255 nexthop
10.10.2.2 out-label 2001 lsr-id 1.1.1.1 tunnel-id 200
```

Step 7 (Optional) configure a dynamic public network tunnel between PE 1 and PE 2.

PE 1

```
PE1(config)#mpls lsr-id 1.1.1.1
PE1(config)#mpls enable
PE1(config)#interface gigaethernet 1/2/2
PE1(config-gigaethernet1/2/2)#mpls ldp
```

P

```
P(config)#mpls lsr-id 2.2.2.2
P(config)#mpls enable
P(config)#interface gigaethernet 1/2/1
P(config-gigaethernet1/2/1)#mpls ldp
P(config-gigaethernet1/2/1)#interface gigaethernet 1/3/2
P(config-gigaethernet1/2/2)# mpls ldp
```

PE 2

```
PE2(config)#mpls lsr-id 4.4.4.4
PE2(config)#mpls enable
PE2(config)#interface gigaethernet1/2/2
PE2(config-gigaethernet1/2/2)#mpls ldp
```

Step 8 Establish a MP-IBGP peer between PE 1 and PE 2

PE 1

```
PE1(config)#router bgp 1
PE1(config-router)#bgp router-id 1.1.1.1
PE1(config-router)#neighbor 4.4.4.4 remote-as 1
/*The ASs at both ends must be the same. If they are the same, the device
is in IBGP routing mode. Otherwise the device is in EBGP mode.*/
PE1(config-router)#neighbor 4.4.4.4 update-source 1.1.1.1
PE1(config-router)#address-family vpnv4
/*Configure a public network neighbor and ensure that the public network
routes are available, that is, the LSR-ID of the peer is reachable. If
there are multiple PE devices, you need to configure multiple public
```


Copyright © Raisecom Technology Co., Ltd.

```
network neighbors which are irrelevant with IPv4 private network
neighbors.*/
PE1(config-router-af)#neighbor 4.4.4.4 activate
PE1(config-router-af)#neighbor 4.4.4.4 send-community extended
/*You must adopt the extended mode. L3VPN is implemented based on
extended BGP.*/
PE1(config-router-af)#exit-address-family
PE1(config-router)#address-family ipv4 vrf vpn1
/*Configure IPv4 private network neighbors to match VRFs. If there are
multiple VRFs, configure multiple IPv4 neighbors and configure multiple
IPv4 private network neighbors on the peer end. This does not affect
VPNv4 public network neighbors.*/
PE1(config-router-af)#redistribute static
PE1(config-router-af)#redistribute connected
PE1(config-router-af)#exit-address-family
PE1(config-router)#exit
```

PE 2

```
PE2(config)#router bgp 1
PE2(config-router)#bgp router-id 4.4.4.4
PE2(config-router)#neighbor 1.1.1.1 remote-as 1
PE2(config-router)#neighbor 1.1.1.1 update-source 4.4.4.4
PE2(config-router)#address-family vpnv4
PE2(config-router-af)#neighbor 1.1.1.1 activate
PE2(config-router-af)#neighbor 1.1.1.1 send-community extended
PE2(config-router-af)#exit-address-family
PE2(config-router)#address-family ipv4 vrf vpn1
PE2(config-router-af)#redistribute static
PE2(config-router-af)#redistribute connected
PE2(config-router-af)#exit-address-family
PE2(config-router)#exit
```

Step 9 Configure a static route pointing to CE 1 on PE 1 and configure a static route pointing to CE 2 on PE 2.

PE 1

```
PE1(config)#ip route vrf vpn1 5.5.5.5 255.255.255.255 10.10.10.1
```

PE 2

```
PE2(config)#ip route vrf vpn1 6.6.6.6 255.255.255.255 10.10.1.2
```

Step 10 Configure the gateway IP address on CE 1 and CE 2 respectively.

CE 1

Copyright © Raisecom Technology Co., Ltd.

```
CE1(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

CE 2

```
CE2(config)#ip route 0.0.0.0 0.0.0.0 10.10.4.1
```

Checking configurations

- Use the **show ip vrf detail** command to show VRF configurations on PE 1 and PE 2.

PE 1

```
PE1(config)#show ip vrf detail
Total VRF configured : 1

VRF: vpn1                       ID: 1
Creation time: 2016/02/14 03:22:40
Up time: 1d18h04m
Route Distinguisher: 100:1
Import RT: 100:1
Export RT: 100:1
Label policy: label per vrf       Label: 10241
```

PE 2

```
PE2(config)#show ip vrf detail
Total VRF configured : 1

VRF: vpn1                       ID: 1
Creation time: 2016/02/14 03:22:40
Up time: 1d18h04m
Route Distinguisher: 100:1
Import RT: 100:1
Export RT: 100:1
Label policy: label per vrf       Label: 10241
```

- Use the **show ip route** command to show whether the routes of public network learned by various PE devices and P devices are correct. Take PE 1 for example.

PE 1

```
PE1(config)#show ip route
Routing Tables: Default-IP-Routing-Table
------------------------------------------------------------------------
--
```


Copyright © Raisecom Technology Co., Ltd.

```
Flag:  C - connected, S - static, R - RIP, B - BGP, O - OSPF, I - IS-IS
      P - Protocol, s - States, > - selected , * - active, Dis - Distance

P&s Destination/Mask   Dis/Metric    NextHop        Age       Interface


C>* 1.0.0.0/8          0/0         1.1.1.2        1d20h13m   GE1/2/1
C>* 1.1.1.2/32         0/0         127.0.0.1       1d20h13m   lo0
O>* 132.1.84.18/32    110/2         132.1.84.18     00:12:42   GE1/2/1.4094
C>* 10.10.1.0/24       0/0         10.10.1.2     04w4d21h   GE1/2/2
C>* 172.16.70.82/32     0/0         127.0.0.1       04w4d21h   lo0
```

- Use the **show interface tunnel** command to show whether Tunnel configurations on PE 1 and PE 2 are correct. Take PE 1 for example.

PE 1

```
PE1(config)#show interface tunnel
tunnel1/1/1 is DOWN, Admin status is UP
   Hardware is NULL, MAC is 0000.0000.0000
   Peer Address is 0.0.0.0
   MTU 1500 bytes
   Last  300 seconds period input rate 0 bytes/sec,  0 packets/sec
   Last  300 seconds period output rate 0 bytes/sec,  0 packets/sec
   Input Statistics:
     0 ifInPkts,
     0 ifInbytes,
     0 ifInDropPkts,
     0 ifInDropbytes,
   Output Statistics:
     0 ifOutPkts,
     0 ifOutbytes,
     0 ifOutDropPkts,
     0 ifOutDropbytes,
```

- Use the **show ip bgp neighbor** command to show whether PE 1 and PE 2 have established BGP neighbors.

```
PE1(config)#show ip bgp neighbor
BGP neighbor is 4.4.4.4, remote AS 1, local AS 1, internal link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:10:57, hold time is 180, keepalive interval is 60 seconds
  Message statistics:
    Inq depth is 0
    Outq depth is 0
                      Sent       Rcvd
    Opens:               0          0
    Notifications:         0          0
    Updates:             0          0
    Keepalives:           0          0
```


Copyright © Raisecom Technology Co., Ltd.

```
    Route Refresh:        0        0
    Total:               0        0
  Minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  0 accepted prefixes

 For address family: VPNv4 Unicast
  Community attribute sent to this neighbor(extended)
  0 accepted prefixes

  Connections established 0; dropped 0
  Last reset never
Next connect timer due in 73 seconds
Read thread: off  Write thread: off
BFD session ID:0
```

- Use the **show ip bgp vpnv4 all** command to check whether PE devices have learned vpnv4 neighbor.

```
PE1(config)#show ip bgp vpnv4 all
Local router ID is 1.1.1.1
Status codes: s - suppressed, d - damped, h - history, * - valid, > -
best, i - internal, S - Stale, R - Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric    LocPrf Weight Path
Route Distinguisher: 1:1
*> 30.0.0.0         100.0.0.10             0           32768 ?
Routes of vpn-instance: 1
*> 30.0.0.0         100.0.0.10             0           32768 ?
---------------------------------------
```

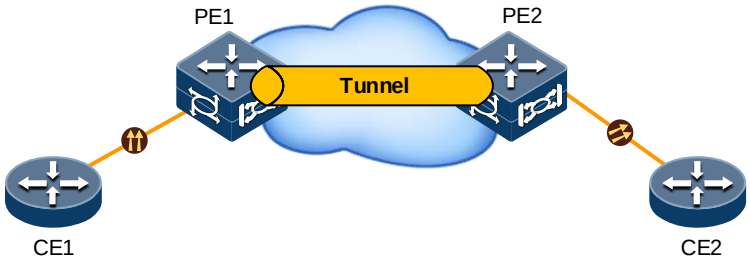
11.9.5 Configuring EVPN VPWS for SR-MPLS BE

Networking requirements

As shown in Figure 11-8, PE 1 and PE 2 are located in two places, and they require leased lines for communication in point-to-point mode. Create an EVPN-VPWS instance, provide a P2P L2VPN service scheme, and use the MPLS tunnelling technology to traverse the backbone network, and provide the method for forwarding Layer 2 packets without querying the MAC address table for the connection between Access Circuits (ACs).

Copyright © Raisecom Technology Co., Ltd.

Figure 11-8 Configuring EVPN VPWS for SR-BE



Preparing data

Prepare data as listed in Table 10-1.

Table 11-6 Preparing data

Device	Client-side interface	Network-side interface	LSR ID
PE 1	1/2/4	1/1/1	1.1.1.1
PE 2	1/2/16	1/1/2	2.2.2.2

Configuration steps

- Configure the SR-MPLS-ISIS tunnel.

Configure PE 1 as below.

Step 1 Configure basic parameters of MPLS.

```
PE1(config)#mpls lsr-id 1.1.1.1
PE1(config)#mpls enable
```

Step 2 Configure basic parameters of SR.

```
PE1(config)#segment-routing
```

Step 3 Configure the prefix type SR.

```
PE1(config)#interface loopback 2
PE1(config-loopback)#ip address 1.1.1.1 255.255.255.255
PE1(config-loopback)#ip router isis 10
PE1(config-loopback)#isis prefix-sid index 10
```


Copyright © Raisecom Technology Co., Ltd.

Step 4 Configure the network-side interface.

```
PE1(config)#interface tengigabitethernet 1/1/1.100
PE1(config-tengigabitethernet1/1/1.100)#encapsulation dot1Q 100
PE1(config-tengigabitethernet1/1/1.100)#ip address 13.0.0.1 255.0.0.0
PE1(config-tengigabitethernet1/1/1.100)#ip router isis 10
```

Step 5 Configure the ISIS process.

```
PE1(config)#router isis 10
PE1(config-router-isis)#net 10.0000.0000.0001.00
PE1(config-router-isis)#metric-style wide
PE1(config-router-isis)#segment-routing mpls
PE1(config-router-isis)#segment-routing global-block 20000 21000
```

Step 6 Configure the BGP process.

```
PE1(config)#router bgp 100
PE1(config-router-bgp)#neighbor 2.2.2.2 remote-as 100
PE1(config-router-bgp)#neighbor 2.2.2.2 update-source 1.1.1.1
PE1(config-router-bgp)#address-family l2vpn evpn
PE1(config-router-af)#neighbor 2.2.2.2 activate /* enable the BGP peer to
switch the specified address family route */
PE1(config-router-af)#neighbor 2.2.2.2 send-community extended /* enable
BGP to send the community properties (Route Target) to the peer */
PE1(config-router-af)#neighbor 2.2.2.2 advertise encap-type mpls /*
enable BGP EVPN to advertise EVPN routes in MPLS encapsulation between
them */
PE1(config-router-af)#exit-address-family
```

Configure PE 2.

Step 7 Configure basic parameters of MPLS.

```
PE2(config)#mpls lsr-id 2.2.2.2
PE2(config)#mpls enable
```

Step 8 Configure basic parameters of SR.

```
PE2(config)#segment-routing
```

Step 9 Configure the prefix type SR.

Copyright © Raisecom Technology Co., Ltd.

```
PE2(config)#interface loopback 2
PE2(config-loopback)#ip address 2.2.2.2 255.255.255.255
PE2(config-loopback)#ip router isis 10
PE2(config-loopback)#isis prefix-sid index 30
```

Step 10 Configure the network-side interface.

```
PE2(config)#interface twenty-fivegige 1/2/16.100
PE2(config-twenty-fivegige1/2/16.100)#encapsulation dot1Q 100
PE2(config-twenty-fivegige1/2/16.100)#ip address 13.0.0.2 255.0.0.0
PE2(config-twenty-fivegige1/2/16.100)#ip router isis 10
```

Step 11 Configure the ISIS process.

```
PE2(config)#router isis 10
PE2(config-router-isis)#net 10.0000.0000.0002.00
PE2(config-router-isis)#metric-style wide
PE2(config-router-isis)#segment-routing mpls
PE2(config-router-isis)#segment-routing global-block 20000 21000/* we
recommend configuring the same global label block for PE 1 and PE 2.*/
```

Step 12 Configure the BGP process.

```
PE2(config)#router bgp 100
PE2(config-router-bgp)#neighbor 1.1.1.1 remote-as 100
PE2(config-router-bgp)#neighbor 1.1.1.1 update-source 2.2.2.2
PE2(config-router-bgp)#address-family l2vpn evpn
PE2(config-router-af)#neighbor 1.1.1.1 activate /* enable the BGP peer to
switch the specified address family route */
PE2(config-router-af)#neighbor 1.1.1.1 send-community extended /* enable
BGP to send the community properties (Route Target) to the peer */
PE2(config-router-af)#neighbor 1.1.1.1 advertise encap-type mpls /*
enable BGP EVPN to advertise EVPN routes in MPLS encapsulation between
them */
PE2(config-router-af)#exit-address-family
```

- Configure EVPN VPWS services.

Configure PE 1 as below.

Step 13 Configure the EVPN source address to identify the device on the EVPN.

```
PE1(config)#evpn source-address 1.1.1.1
```


Copyright © Raisecom Technology Co., Ltd.

Step 14 Configure the policy for selecting the tunnel.

```
PE1(config)#tunnel-policy sr /*create a tunnel policy sr*/
PE1(config-tunnelpolicy)#tunnel select-seq sr-be-lsp /* select the SR-BE
tunnel as the tunnel policy */
```

Step 15 Configure EVPN VPWS instance 100 (corresponding with user service VLAN 100).

```
PE1(config)#evpn vpws 100
PE1(config-evpn-vpws)#rd 100:1
PE1(config-evpn-vpws)#route-target import 1000:1000
PE1(config-evpn-vpws)#route-target export 1000:1000
PE1(config-evpn-vpws)#tunnel-policy sr
```

Step 16 Configure EVPN VPWS instance 200(corresponding with user service VLAN 200).

```
PE1(config)#evpn vpws 200
PE1(config-evpn-vpws)#rd 200:1
PE1(config-evpn-vpws)#route-target import 2000:2000
PE1(config-evpn-vpws)#route-target export 2000:2000
PE1(config-evpn-vpws)#tunnel-policy sr
```

Step 17 Configure EVPN EVPL instance 100 (corresponding with user service VLAN 100).

```
PE1(config)#evpn evpl 1000 mpls-mode
PE1(config-evpn-evpl)#evpn vpws 100 /* configure the EVPN EVPL instance
to be associated with the EVPN VPWS instance */
PE1(config-evpn-evpl)#local-service-id 10 remote-service-id 20
```

Step 18 Configure EVPN EVPL instance 2000 (corresponding with user service VLAN 200).

```
PE1(config)#evpn evpl 2000 mpls-mode
PE1(config-evpn-evpl)#evpn vpws 200 /* configure the EVPN EVPL instance
to be associated with the EVPN VPWS instance */
PE1(config-evpn-evpl)#local-service-id 30 remote-service-id 40
```

Step 19 Configure the AC interface that accessing VLAN 100 services.

```
PE1(config)#interface twenty-fivegige 1/2/4.100
PE1(config-twenty-fivegige1/2/4.100)#encapsulation dot1Q 100
PE1(config-twenty-fivegige1/2/4.100)#mode l2
```


Copyright © Raisecom Technology Co., Ltd.

```
PE1(config-twenty-fivegige1/2/4.100)#evpn evpl 1000 /* configure the AC
interface to be associated with the EVPN EVPL instance */
```

Step 20 Configure the AC interface that accessing VLAN 200 services.

```
PE1(config)#interface twenty-fivegige 1/2/4.200
PE1(config-twenty-fivegige1/2/4.200)#encapsulation dot1Q 200
PE1(config-twenty-fivegige1/2/4.200)#mode l2
PE1(config-twenty-fivegige1/2/4.200)#evpn evpl 2000 /* configure the AC
interface to be associated with the EVPN EVPL instance */
```

Configure PE 2.

Step 21 Configure the EVPN source address to identify the device on the EVPN.

```
PE2(config)#evpn source-address 2.2.2.2
```

Step 22 Configure the policy for selecting the tunnel.

```
PE2(config)#tunnel-policy sr /* create a tunnel policy sr*/
PE2(config-tunnelpolicy)#tunnel select-seq sr-be-lsp /* select the SR-BE
tunnel as the tunnel policy */
```

Step 23 Configure EVPN VPWS instance 100 (corresponding with user service VLAN 100).

```
PE2(config)#evpn vpws 100
PE2(config-evpn-vpws)#rd 1000:1
PE2(config-evpn-vpws)#route-target import 1000:1000
PE2(config-evpn-vpws)#route-target export 1000:1000
PE2(config-evpn-vpws)#tunnel-policy sr
```

Step 24 Configure EVPN VPWS instance 200(corresponding with user service VLAN 200).

```
PE2(config)#evpn vpws 200
PE2(config-evpn-vpws)#rd 2000:1
PE2(config-evpn-vpws)#route-target import 2000:2000
PE2(config-evpn-vpws)#route-target export 2000:2000
PE2(config-evpn-vpws)#tunnel-policy sr
```

Step 25 Configure EVPN EVPL instance 100 (corresponding with user service VLAN 100).

Copyright © Raisecom Technology Co., Ltd.

```
PE2(config)#evpn evpl 1000 mpls-mode
PE2(config-evpn-evpl)#evpn vpws 100 /* configure the EVPN EVPL instance
to be associated with the EVPN VPWS instance */
PE2(config-evpn-evpl)#local-service-id 20 remote-service-id 10
```

Step 26 Configure EVPN EVPL instance 2000 (corresponding with user service VLAN 200).

```
PE2(config)#evpn evpl 2000 mpls-mode
PE2(config-evpn-evpl)#evpn vpws 200 /* configure the EVPN EVPL instance
to be associated with the EVPN VPWS instance */
PE2(config-evpn-evpl)#local-service-id 40 remote-service-id 30
```

Step 27 Configure the AC interface that accessing VLAN 100 services.

```
PE2(config)#interface twenty-fivegige 1/2/16.100
PE2(config-twenty-fivegige1/2/16.100)#encapsulation dot1Q 100
PE2(config-twenty-fivegige1/2/16.100)#mode l2
PE2(config-twenty-fivegige1/2/16.100)#evpn evpl 1000 /* configure the AC
interface to be associated with the EVPN EVPL instance */
```

Step 28 Configure the AC interface that accessing VLAN 200 services.

```
PE2(config)#interface twenty-fivegige 1/2/16.200
PE2(config-twenty-fivegige1/2/16.200)#encapsulation dot1Q 200
PE2(config-twenty-fivegige1/2/16.200)#mode l2
PE2(config-twenty-fivegige1/2/16.200)#evpn evpl 2000 /* configure the AC
interface to be associated with the EVPN EVPL instance */
```

Checking results

Show information about the EVPN VPWS instance. Take EVPN VPWS instance 100 of PE 1 for example.

```
PE1#show evpn vpws 100
------------------------------------------------------------------------
Evpn instance ID:100
Evpn tunnel policy : sr
Route Distinguisher:  100:1
Evpn RT import num :  1
       Import RT :  1000:1000

Evpn RT export num :  1
       Export RT :  1000:1000
```


Copyright © Raisecom Technology Co., Ltd.

Show information about the EVPN EVPL instance. Take EVPN EVPL instance 1000 of PE 1 for example.

```
PE1#show evpn evpl instance-id 1000
Evpl ID: 1000
Evpl Mode: mpls-mode
Evpn Vpws ID: 100
Interface: 1/2/4.100 (up)
Local Redundancy Mode: all-active
Local DF State: Primary
Local MTU : 1500
Local Control Word : False
Local Service ID : 10
Remote Service ID: 20
```


Copyright © Raisecom Technology Co., Ltd.

12 QoS

This chapter describes principles and configuration procedures of QoS, as well as related configuration examples, including following sections:

- Configuring ACL
- Configuring priority trust and priority mapping
- Configuring traffic classification and traffic policy
- Configuring congestion avoidance and queue shaping
- Configuring interface rate limiting
- Configuring hierarchical bandwidth rate limiting
- Configuring MPLS QoS
- Configuring L3VPN QoS
- Configuring HQoS
- Maintenance
- Configuration examples

12.1 Configuring ACL

12.1.1 Preparing for configurations

Scenario

To filter data packets, the device needs to be configured with ACL to identify data packets to be filtered. Devices allow/disallow related data packets to pass based on pre-configured policies unless they identify specified data packets.

Prerequisite

N/A

12.1.2 Configuring ACL

Select steps 3–7 as required.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**access-list** *acl-number*	Create an ACL, select an ACL value, and enter the corresponding ACL configuration mode. The value of *acl-number* parameter defines the type of ACL configuration mode. • Values 1000–0999: basic IP ACL • Values 2000–2999: extended IP ACL • Values 3000–3999: MAC ACL • Values 4000–4999: MPLS ACL • Values 5000–5999: user-defined ACL • Values 6000–6999: basic IPv6 ACL • Values 7000–7999: extended IPv6 ACL • Values 8000–8999: advanced ACL • Values 9000–9999: advanced IPv6 ACL
3	Raisecom(config-acl-ip-std)#**rule** [*rule-id*] { **deny** | **permit** } { *source-ip-address source-ip-mask* | **any** } [**vrf** *vrf-name*] [**time-range** *time-range-name*]	Configure the basic IP ACL rule in basic IP ACL configuration mode.
4	Raisecom(config-acl-ip-ext)#**rule** [*rule-id*] { **deny** | **permit** } { *protocol-id* | **ip** } { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** } [**dscp** *dscp-value* | **precedence** *precedence-value* | **tos** *tos-value*] [**ttl** *ttl-value*] [**vrf** *vrf-name*] [**fragment**] [**time-range** *time-range-name*]	(Optional) configure the extended IP ACL rule in IP ACL configuration mode.
	Raisecom(config-acl-ip-ext)#**rule** [*rule-id*] { **deny** | **permit** } **udp** { *source-ip-address source-ip-mask* | **any** } [*source-port*]{ *destination-ip-address destination-ip-mask* | **any** } [*destination-port*] [**dscp** *dscp-value* | **precedence** *precedence-value* | **tos** *tos-value*] [**ttl** *ttl-value*] [**vrf** *vrf-name*] [**fragment**] [**time-range** *time-range-name*]	
	Raisecom(config-acl-ip-ext)#**rule** [*rule-id*] { **deny** | **permit** } **tcp** { *source-ip-address source-ip-mask* | **any** } [*source-port*]{ *destination-ip-address destination-ip-mask* | **any** } [*destination-port*] [**tcpflag** *flag-value* **tcpflagmask** *mask-value*] [**dscp** *dscp-value* | **precedence** *precedence-value* | **tos** *tos-value*] [**ttl** *ttl-value*] [**vrf** *vrf-name*] [**fragment**] [**time-range** *time-range-name*]	

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config-acl-ip-ext)# **rule** [*rule-id*] { **deny** | **permit** } **igmp** { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** } [**dscp** *dscp-value* | **precedence** *precedence-value* | **tos** *tos-value*] [**ttl** *ttl-value*] [**fragment**] [**time-range** *time-name*]	
	Raisecom(config-acl-ip-ext)#**rule** [*rule-id*] { **deny** | **permit** } **icmp** { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** } [[**icmp-type** *icmp-type-value*] *icmp-code*] [**dscp** *dscp-value* | **precedence** *precedence-value* | **tos** *tos-value*] [**ttl** *ttl-value*] [**vrf** *vrf-name*] [**fragment**] [**time-range** *time-range-name*]	
5	Raisecom(config-acl-mac)#**rule** [*rule-id*] { **deny** | **permit** } { *source-mac-address source-mac-mask* | **any** } { *destination-mac-address destination-mac-mask* | **any** } [**ethertype** { *ethertype* [*ethertype-mask*] | **ip** | **arp** }] [**svlan** *svlanid*] [**cvlan** *cvlanid*] [**svlan-cos** *svlan-cos*] [**cvlan-cos** *cvlan-cos*] [**time-range** *time-range-name*]	(Optional) configure the MAC ACL rules in MAC ACL configuration mode.
6	Raisecom(config-acl-mpls)#**rule** [*rule-id*] { **deny** | **permit** } **label** { *label-value* | **any** } [**exp** *exp-value*] [**ttl** *ttl-value*] [**second-label** { *label-value* | **any** } [**second-exp** *exp-value*] [**second-ttl** *ttl-value*]] [**third-label** { *label-value* | **any** } [**third -exp** *exp-value*] [**third -ttl** *ttl-value*]] [**time-range** *time-range-name*]	Configure the MPLS ACL rules in MPLS ACL configuration mode.
7	Raisecom(config-acl-udf)#**rule** [*rule-id*] { **deny** | **permit** } { **layer2** | **ipv4** } *rule-string rule-mask offset* [**time-range** *time-range-name*]	Configure user-defined ACL rules in user-defined ACL configuration mode.
8	Raisecom(config-acl-ipv6-std)#**rule** [*rule-id*] { **deny** | **permit** } { *source-ip-address/prefix-length* | **any** } [**vrf** *vrf-name*] [**time-range** *time-range-name*]	Configure IPv6 ACL rules in IPv6 ACL configuration mode.
9	Raisecom(config-acl-ipv6-ext)#**rule** [*rule-id*] { **deny** | **permit** } **tcp** { *source-ip-address/prefix-length* | **any** } [*source-port*] { *destination-ip-address/prefix-length* | **any** } [*destination-port*] [**tcpflag** *flag-value* **tcpflagmask** *mask-value*] [**dscp** *dscp-value*] [**ttl** *ttl-value*] [**flow-label** *label-value*] [**vrf** *vrf-name*] [**fragment**] [**time-range** *time-range-name*]	(Optional) configure the extended IPv6 ACL rules in extended IPv6 ACL configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config-acl-ipv6-ext)#**rule** [*rule-id*] { **deny** | **permit** } **udp** { *source-ip-address/prefix-length* | **any** } [*source-port*] { *destination-ip-address destination-ip-mask* | **any** } [*destination-port*] [**dscp** *dscp-value*] [**ttl** *ttl-value*] [**flow-label** *label-value*] [**vrf** *vrf-name*] [**fragment**] [**time-range** *time-range-name*]	
	Raisecom(config-acl-ipv6-ext)#**rule** [*rule-id*] { **deny** | **permit** } { *protocol-id* | **ipv6** } { *source-ipv6-address/prefix* | **any** } { *destination-ipv6-address/prefix* | **any** } [**dscp** *dscp*] [**ttl** *ttl-value*] [**flow-label** *flow label-value*] [**vrf** *vrf-name*] [**fragment**] [**time-range** *time-name*]	
	Raisecom(config-acl-ipv6-ext)#**rule** [*rule-id*] { **deny** | **permit** } **icmpv6** { *source-ip-address/prefix-length* | **any** } { *destination-ip-address destination-ip-mask* | **any** } [**icmpv6-type** *icmpv6-value* [*icmpv6-code*]] [**dscp** *dscp-value*] [**ttl** *ttl-value*] [**flow-label** *label-value*] [**fragment**] [**time-range** *time-range-name*]	
10	Raisecom(config-acl-advanced)#**rule** [*rule-id*] { **deny** | **permit** } { *source-mac-address source-mac-mask* | **any** } { *destination-mac-address destination-mac-mask* | **any** } [**svlan** *svlanid*] [**cvlan** *cvlanid*] [**cos** *cos-value*] [**inner-cos** *inner-cos-value*] { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** } [**dscp** *dscp-value* | **precedence** *precedence-value* | **tos** *tos-value*] [**ttl** *ttl-value*] [**fragment**] [**time-range** *time-range-name*]	In advanced IP ACL mode, configure advanced IP ACL rules.
11	Raisecom(config-acl-ipv6-advanced)# **rule** [*rule-id*] { **deny** | **permit** } { *source-mac-address source-mac-mask* | **any** } { *destination-mac-address destination-mac-mask* | **any** } [**svlan** *svlanid*] [**cvlan** *cvlanid*] [**cos** *cos-value*] [**inner-cos** *inner-cos*] { *source-ipv6-address/prefix-length* | **any** } { *destination-ipv6-address/prefix-length* | **any** } [**dscp** *dscp-value*] [**flow-label** *flow-label-value*] [**fragment**] [**time-range** *time-name*]	In advanced IPv6 ACL mode, configure advanced IPv6 ACL rules.
12	Raisecom(config)#**access-list copy** *dest-acl-number source-acl-number*	Copy to generate the same ACL rule.

Copyright © Raisecom Technology Co., Ltd.

12.1.3 Configuring filter

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**filter** { **ingress** | **egress** } **access-list** { *acl-number* | **name** *acl-name* } [**statistics**] Raisecom(config-port)#**exit**	Apply the ACL rule to the ingress and egress interfaces. The ACL rule cannot be modified once it is applied to the interface and the number of ACL rules must be greater than 0.
4	Raisecom(config)#**clear filter statistics interface** *interface-type interface-number* { **ingress** | **egress** } [**access-list** { *acl-number* | **name** *acl-name* }]	(Optional) clear filter statistics.

12.1.4 Checking configurations

No.	Command	Description
1	Raisecom#**show access-list** [*acl-number* | **name** *acl-name*]	Show ACL information.
2	Raisecom#**show filter interface**	Show filter information.
	Raisecom#**show filter interface** *interface-type interface-number* [**ingress** | **egress**]	
	Raisecom#**show filter statistics interface** *interface-type interface-number* { **ingress** | **egress** } **access-list** *acl-number* { *acl-number* | **name** *acl-name* }	
3	Raisecom#**show time-range** [*time-range-name*]	Show configurations of the time period.
4	Raisecom#**show local-access access-list**	Show information about local ACL.

12.2 Configuring priority trust and priority mapping

12.2.1 Preparing for configurations

Scenario

For packets from upstream devices, you can select to trust the priorities taken by these packets. For packets whose priorities are not trusted, you can process them with traffic classification and traffic policy. In addition, you can modify DSCP priorities by configure interface-based DSCP priority remarking. After configuring priority trust, the RAX721 can perform different operations on packets with different priorities, providing related services.

Copyright © Raisecom Technology Co., Ltd.

Before performing queue scheduling, you need to assign a local priority for a packet. For packets from the upstream device, you can map the outer priorities of these packets to various local priorities. In addition, you can directly configure local priorities for these packets based on interfaces. And then device will perform queue scheduling on these packets basing on local priorities.

In general, for IP packets, you need to configure the mapping between DHCP priority and local priority, and mapping between IP Precedence (IPP) and local priority. For VLAN packets, you need to configure the mapping between CoS priority and local priority. For MPLS packets, you need to configure the mapping between the Exp field and the local priority.

Prerequisite

N/A

12.2.2 Configuring priority trust

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode.
3	`Raisecom(config-port)#mls qos trust { cos | dscp }`	Configure the priority trusted by an interface. By default, the Layer 2 interface trusts the CoS priority and the Layer 3 interface trusts the DHCP priority.
4	`Raisecom(config-port)#mls qos trust tos`	Configure the interface to trust ToS priority.
5	`Raisecom(config-port)#mls qos trust port-priority`	Configure the interface to trust interface priority.
6	`Raisecom(config-port)#mls qos priority` *priority*	Configure the interface priority. By default, it is 5.

12.2.3 Configuring DSCP-to-local priority mapping

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mls qos mapping dscp-to-local-priority` *profile-id*	Create the DSCP-to-local priority (color) mapping profile and enter dscp-to-pri configuration mode.
3	`Raisecom(dscp-to-pri)#dscp` *dscp-value* `to local-priority` *localpri-value* `[ color { green | red | yellow } ]`	Configure the DSCP-to-local priority (color) mapping.
4	`Raisecom(dscp-to-pri)#exit` `Raisecom(config)#interface` *interface-type interface-number*	Exit dscp-to-pri configuration mode. Enter interface configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config-port)#**mls qos dscp-to-local-priority** *profile-id*	Apply the DSCP-to-local priority (color) mapping profile to an interface.

12.2.4 Configuring CoS-to-local priority mapping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping cos-to-local-priority** *profile-id*	Create the CoS-to-local priority (color) mapping profile and enter cos-to-pri configuration mode.
3	Raisecom(dscp-to-pri)#**cos** *cos-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }]	Configure the CoS-to-local priority (color) mapping.
4	Raisecom(dscp-to-pri)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Exit cos-to-pri configuration mode. Enter interface configuration mode.
5	Raisecom(config-port)#**mls qos cos-to-local-priority** *profile-id* [**dei enable**]	Apply the CoS-to-local priority (color) mapping profile to an interface or enable color marking for outgoing packets on the interface.

12.2.5 Configuring the ToS-to-local priority mapping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping tos-to-local-priority** *profile-id*	Create the CoS-to-local priority (color) mapping profile and enter tos-to-pri configuration mode.
3	Raisecom(tos-to-pri)#**tos** *tos-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }]	Configure the ToS-to-local priority (color) mapping.
4	Raisecom(tos-to-pri)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Exit tos-to-pri configuration mode. Enter interface configuration mode.
5	Raisecom(config-port)#**mls qos tos-to-local-priority** *profile-id*	Apply the ToS-to-local priority (color) mapping profile to an interface

12.2.6 Configuring Exp-to-local priority mapping

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**mls qos mapping exp-to-local-priority** *profile-id*	Create an Exp-to-local priority (color) mapping profile and enter exp-to-pri configuration mode.
3	Raisecom(exp-to-pri)#**exp** *exp-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }]	Configure the Exp-to-local priority (color) mapping.

12.2.7 Configuring local-to-DSCP priority mapping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping local-priority-to-dscp** *profile-id*	Create the local-to-DSCP priority mapping profile and enter pri-to-dscp configuration mode.
3	Raisecom(pri-to-dscp)#**local-priority** *localpri-value* **to dscp** *dscp-value*	Configure the local-to-DSCP priority mapping.
4	Raisecom(pri-to-dscp)#**exit** Raisecom(config)#**interface gigaethernet** *unit-id/slot-id/port-id*	Exit pri-to-dscp configuration mode. Enter interface configuration mode.
5	Raisecom(config-port)#**mls qos local-priority-to-dscp** *profile-id*	Apply the local-to-DSCP priority mapping profile to an interface.

12.2.8 Configuring local-to-ToS priority mapping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping local-priority-to-tos** *profile-id*	Create the local-to-ToS priority mapping profile and enter pri-to-tos configuration mode.
3	Raisecom(pri-to-tos)#**local-priority** *localpri-value* **to tos** *tos-value*	Configure the local-to-ToS mapping.
4	Raisecom(pri-to-tos)#**exit** Raisecom(config)#**interface gigaethernet** *unit-id/slot-id/port-id*	Exit pri-to-tos configuration mode. Enter interface configuration mode
5	Raisecom(config-port)#**mls qos local-priority-to-tos** *profile-id*	Apply the local-to-ToS priority mapping profile to an interface.

12.2.9 Configuring CoS priority remarking

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**mls qos mapping cos-remark** *profile-id*	Create the CoS remarking profile and enter dscp-remark configuration mode.
3	Raisecom(cos-remark)#**local-priority** *localpri-value* **to cos** *cos-value*	Configure the mapping between the local priority and CoS priority.
4	Raisecom(cos-remark)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Exit cos-remark configuration mode. Enter interface configuration mode.
5	Raisecom(config-port)# **mls qos cos-remark-mapping enable** [**dei enable**]	Enable local priority-to-CoS mapping or enable color marking for outgoing packets on the interface.
6	Raisecom(config-port)#**mls qos cos-remark** *profile-id*	Apply the CoS remarking profile to an interface.

12.2.10 Configuring local-to-Exp priority mapping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping local-priority-to-exp** *profile-id*	Create a local-to-Exp priority mapping profile and enter pri-to-exp configuration mode.
3	Raisecom(pri-to-exp)#**local-priority** *localpri-value* **to exp** *exp-value*	Configure local-to-Exp priority mapping.

12.2.11 Checking configurations

No.	Command	Description
1	Raisecom#**show mls qos mapping dscp-to-local-priority** [**default** | *profile-id*]	Show information about the DSCP-to-local priority (color) mapping profile.
2	Raisecom#**show mls qos mapping cos-to-local-priority** [**default** | *profile-id*]	Show information about the CoS-to-local priority (color) mapping profile.
3	Raisecom#**show mls qos mapping exp-to-local-priority** [**default** | *profile-id*]	Show information about Exp-to-local priority (color) mapping.
4	Raisecom#**show mls qos mapping tos-to-local-priority** [**default** | *profile-id*]	Show ToS-to-local priority (color) mapping profile.
5	Raisecom#**show mls qos mapping cos-remark** [**default** | *profile-id*]	Show information about the CoS remarking profile.
6	Raisecom#**show mls qos mapping local-priority-to-exp** [**default** | *profile-id*]	Show information about the local priority-to-Exp mapping profile.
7	Raisecom#**show mls qos mapping local-priority-to-dscp** [**default** | *profile-id*]	Show local-to-DSCP mapping profile.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
8	Raisecom#**show mls qos mapping local-priority-to-tos** [**default** | *profile-id*]	Show local-to-ToS mapping profile.
9	Raisecom#**show mls qos interface** [*interface-type interface-number*]	Show QoS information on the interface.

12.3 Configuring traffic classification and traffic policy

12.3.1 Preparing for configurations

Scenario

Traffic classification is the basis of QoS. For packets from upstream devices, you can classify them according to ACL rules. After traffic classification, the device can provide related operations for different packets, providing differentiated services.

After configurations, the traffic classification cannot take effect until being bound to traffic policy. The selection of traffic policy depends on the packet status and current network load status. In general, when a packet is sent to the network, you need to limit the speed according to Committed Information Rate (CIR) and remark the packet according to the service feature.

Prerequisite

N/A

12.3.2 Creating and configuring traffic classification

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**class-map** *class-map-name* [**match all** | **match any**]	Create traffic classification and enter CMAP configuration mode.
3	Raisecom(config-cmap)#**match access-list** { *acl-number* | **name** *acl-name* }	Define the ACL matched with the traffic classification. ACL rules cannot be modified once they are applied to the interface. The number of ACL rules must be greater than 0.
4	Raisecom(config-cmap)#**match dscp** *dscp-value*	Configure the traffic classification which matches DSCP.
5	Raisecom(config-cmap)#**match cos** *cos-value*	Configure the traffic classification which matches CoS.
6	Raisecom(config-cmap)#**match exp** *exp-value*	Configure the traffic classification which matches EXP.
7	Raisecom(config-cmap)#**match inner-cos** *cos-value*	Configure the traffic classification which matches the inner CoS.
8	Raisecom(config-cmap)#**match inner-vlan** *vlan-id*	Configure the traffic classification which matches the inner VLAN.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
9	Raisecom(config-cmap)#**match ip precedence** *ipp-value*	Configure the traffic classification which matches the IP priority.
10	Raisecom(config-cmap)#**match ip tos** *tos-value*	Configure the traffic classification which matches the IP ToS.
11	Raisecom(config-cmap)#**match ipv6 dscp** *dscp-value*	Configure the traffic classification which matches the IPv6 DSCP.
12	Raisecom(config-cmap)#**match label** *label-value*	Configure the traffic classification which matches the traffic label.
13	Raisecom(config-cmap)#**match second-label** *label-value*	Configure the traffic classification which matches the second-layer label.
14	Raisecom(config-cmap)#**match vlan** *vlan-id*	Configure the traffic classification which matches the VLAN ID.

12.3.3 Creating and configuring traffic policing profile

To perform traffic policing on packets, you need to configure traffic policing profile and then quote this profile under the traffic classification, which is bound to traffic policy.

On the traffic policing profile, you can configure traffic policing rules or perform relate operations on specified packets based on color.

The single bucket does not support the color-sensitive mode or commands with the yellow key word.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos policer-profile** *policer-name* [**single**]	Create the traffic policing profile and enter traffic policing profile configuration mode.
3	Raisecom(traffic-policer)#**cir** *cir* **cbs** *cbs* [**ebs** *ebs*]	(Optional) configure rate limiting parameters.
	Raisecom(traffic-policer)#**cir** *cir* **cbs** *cbs* **eir** *eir* **ebs** *ebs* [**coupling**]	

12.3.4 Creating and configuring traffic policy

Steps 5–10 are coordinate. You can select one as required.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**policy-map** *policy-map-name*	Create a traffic policy and enter PMAP configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-pmap)#**class-map** *class-map-name*	Add the traffic classification to the traffic policy and enter CMAP configuration mode. **Note** The traffic classification, bound with the traffic policy, must be based on at least one rule. Otherwise, the binding operation fails. When the traffic policy is applied to an interface, you cannot delete the bound traffic classification or modify its configuration. One traffic classification can be applied to multiple traffic policies.
4	Raisecom(config-pmap-c)#**policer** *policer-name*	Import a traffic policing profile (policer) into the traffic policy.
5	Raisecom(config-pmap-c)#**set** { **cos** *cos-value* | **local-priority** *value* } Raisecom(config-pmap-c)#**set** { **inner-vlan** *inner-vlan-id* | **vlan** *vlan-id* }	(Optional) configure packet remarking.
6	Raisecom(config-pmap-c)#**add outer-vlan** *vlan-id*	(Optional) configure the VLAN ID of the added outer VLAN Tag.
7	Raisecom(config-pmap-c)#**redirect-to** *interface-type interface-number*	(Optional) configure the redirection rule to forward matched packets through the specified interface.
8	Raisecom(config-pmap-c)#**copy-to-mirror mirror-group** *group-id*	(Optional) copy the traffic to the mirroring monitoring interface.
9	Raisecom(config-pmap-c)#**forward-to-cpu**	(Optional) forward traffic to the CPU.
10	Raisecom(config-pmap-c)#**statistics enable**	(Optional) enable traffic statistics.
11	Raisecom(config-pmap-c)#**exit** Raisecom(config-pmap)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Exit CMAP configuration mode. Exit PMAP configuration mode. Enter interface configuration mode.
12	Raisecom(config-port)#**service-policy** { **ingress** | **egress** } *policy-map-name*	Apply the traffic policy to an interface.

12.3.5 Checking configurations

No.	Command	Description
1	Raisecom#**show class-map** [*class-map-name*]	Show traffic classification information.
2	Raisecom#**show mls qos policer** [*policer-name*]	Show traffic policing rules.
3	Raisecom#**show policy-map** [*policy-map-name*] [**class-map** *class-map-name*]	Show traffic policy information.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
4	Raisecom#**show service-policy interface**	Show information about applied policies.
	Raisecom#**show service-policy interface** *interface-type interface-number* [**egress** | **ingress**]	
5	Raisecom#**show service-policy statistics interface** *interface-type interface-number* { **egress** | **ingress** } **policy-map** *policy-map-name* [**class-map** *class-map-name*]	Show statistics about applied traffic policies.

12.4 Configuring congestion avoidance and queue shaping

12.4.1 Preparing for configurations

Scenario

To prevent network congestion from occurring and to resolve TCP global synchronization, you can configure congestion avoidance to adjust the network traffic and resolve network overload. The RAX721 supports WRED-based congestion avoidance.

When the interface speed of downstream devices is smaller than the one of upstream devices, congestion avoidance may occur on interfaces of downstream devices. At this time, you can configure queue and traffic shaping on the egress interface of upstream devices to shape upstream traffic.

Prerequisite

N/A

12.4.2 Configuring WRED profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos wred profile** *profile-id*	Create the WRED profile and enter WRED profile configuration mode.
3	Raisecom(wred)#**wred** [**color** { **green** | **red** | **yellow** }] **start-drop-threshold** *start-drop* **end-drop-threshold** *end-drop* **max-drop-probability** *max-drop*	Configure WRED profile information. For non-TCP packets, it does not distinguish the color. You need to configure the **wred start-drop-threshold**/**wred color green** parameter.
4	Raisecom(wred)#**wred start-drop-threshold** *start-value* **end-drop-threshold** *end-value* **max-drop-probability** *max-value*	Configure the drop threshold of the WRED profile.

Copyright © Raisecom Technology Co., Ltd.

12.4.3 Configuring flow queue profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos flow-queue profile** *flow-profile-id*	Create a flow profile and enter flow profile configuration mode.
3	Raisecom(flow-queue)#**scheduler wrr**	Configure the queue scheduling mode. By default, it is SP.
4	Raisecom(flow-queue)#**queue** *queue-id* [**weight** *weight-value*] [**shaping cir** *cir-value* [**cbs** *cbs-value*] **pir** *pir-value* [**pbs** *pbs-value*]] [**wred profile** *profile-id*]	Configure the queue, weight, shaping, and WRED information of the flow profile. If no weight is configured, SP scheduling mode is adopted.
5	Raisecom(flow-queue)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Exit flow profile configuration mode. Enter interface configuration mode.
6	Raisecom(config-port)# **mls qos flow-queue** *profile-id*	Apply the flow profile to an interface.

12.4.4 Configuring queue shaping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**mls qos shaping egress pir** *pir-value* [**pbs** *pbs-value*]	Configure queue shaping for queues of the interface.

12.4.5 Checking configurations

No.	Command	Description
1	Raisecom#**show mls qos wred profile** [*profile-list*]	Show WRED profile configurations.
2	Raisecom#**show mls qos flow-queue profile** *flow-profile-list*	Show flow profile configurations.
3	Raisecom#**show mls qos queue max-buffer** *interface-type interface-number*	Show the maximum buffer of the queue.
4	Raisecom#**show mls qos shaping interface** [*interface-type interface-number* [**ingress** | **egress**]]	Show queue shaping information.
5	Raisecom#**show mls qos queue statistics interface** *interface-type interface-number*	Show queue statistics of the interface.

Copyright © Raisecom Technology Co., Ltd.

12.5 Configuring interface rate limiting

12.5.1 Preparing for configurations

Scenario

To avoid/remit network congestion, you can configure interface-based rate limiting. Rate limiting is used to make packets transmitted at a relative average speed by controlling the burst traffic on an interface.

Prerequisite

N/A

12.5.2 Configuring interface-based rate limiting

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**rate-limit** { **egress** | **ingress** } **cir** *cir-value* **cbs** *cbs-value* [**pir** *pir-value* **pbs** *pbs-value*] Raisecom(config-port)#**exit**	Configure rate limiting based on the interface. Rate limiting can be based on the following interfaces: • Layer 3 physical interface • Layer 2 physical interface • Sub-interface • Link aggregation interface
4	Raisecom(config)#**rate-limit mode** { **l1** | **l2** }	(Optional) configure the rate limiting mode. • l1: physical layer mode • l2: data link layer mode

12.5.3 Checking configurations

No.	Command	Description
1	Raisecom#**show rate-limit interface**	Show interface-based rate limiting.
	Raisecom#**show rate-limit interface** *interface-type interface-number* **ingress**	
2	Raisecom#**show rate-limit mode**	Show interface bandwidth rate limiting mode.

Copyright © Raisecom Technology Co., Ltd.

12.6 Configuring hierarchical bandwidth rate limiting

12.6.1 Preparing for configurations

Scenario

In order to ensure that special services can still be transmitted as required when the network is congested, you can configure hierarchical bandwidth rate limiting. Configure a bandwidth assurance profile and a hierarchical bandwidth assurance profile to match the packets received on the interface with the profile to ensure the normal transmission of special services.

Prerequisite

N/A

12.6.2 Configuring bandwidth assurance

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#bandwidth-profile bwp-profile-id cir cir cbs cbs [ pir pir-value pbs pbs-value ] [ color-aware ]`	Create a bandwidth assurance template.
	`Raisecom(config)#bandwidth-profile bwp-profile-id cir cir cbs cbs eir eir ebs ebs [ color-aware [ coupling ] ]`	
3	`Raisecom(config)#bandwidth-profile bwp-profile-id description word`	Configure the description of the bandwidth assurance template.

Note

If the bandwidth assurance template is quoted by other hierarchical templates or is applied, you will fail to delete it.

12.6.3 Configuring hierarchical bandwidth assurance

Configuring hierarchical VLAN bandwidth assurance

No.	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#bandwidth-profile profile-id cir cir cbs cbs [ eir eir ebs ebs ] [ color-aware ]`	Create a bandwidth assurance template.
3	`Raisecom(config)#hierarchy-vlan bandwidth-profile hvlan-profile-id`	Create a hierarchical VLAN template and enter hierarchical VLAN configuration mode.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
4	Raisecom(config-hvlan)#**bandwidth vlanlist** *vlan-list bwp-profile-id* Raisecom(config-hcos)#**exit**	Configure a hierarchical VLAN template.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**bandwidth ingress vlan** *vlan-id bwp-profile-id*	Apply the VLAN bandwidth rate limiting template to the interface.
7	Raisecom(config-port)#**bandwidth ingress** *bwp-profile-id* [**hierarchy-vlan** *hvlan-profile-id*]	Apply the hierarchical VLAN profile to the interface.

Configuring hierarchical CoS bandwidth assurance

No.	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**bandwidth-profile** *profile-id* **cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**color-aware**]	Create a bandwidth assurance template.
3	Raisecom(config)#**hierarchy-cos bandwidth-profile** *hc-profile-id*	Create a hierarchical CoS template and enter HCoS configuration mode.
4	Raisecom(config-hcos)#**bandwidth coslist** *cos-list bwp-profile-id* Raisecom(config-hcos)#**exit**	Configure a hierarchical CoS template.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**bandwidth ingress vlan** *vlan-id* **coslist cos-value** *bwp-profile-id*	Apply the VLAN+CoS bandwidth rate limiting template to the interface.
7	Raisecom(config-port)#**bandwidth ingress vlan** *vlan-id bwp-profile-id* [**hierarchy-cos** *hcos-profile-id*]	Apply the VLAN+CoS hierarchical bandwidth rate limiting template to the interface.

12.6.4 Checking configurations

No.	Command	Description
1	Raisecom#**show bandwidth-profile** [*bwp-profile-id*]	Show information about the bandwidth assurance template.
2	Raisecom#**show bandwidth interface** *interface-type interface-number*	Show bandwidth assurance configurations on the interface.
3	Raisecom#**show hierarchy-cos-bandwidth profile** [*hc-profile-id*]	Show information about the hierarchical CoS bandwidth assurance template.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
4	Raisecom#**show hierarchy-vlan-bandwidth profile** [*hd-profile-id*]	Show information about hierarchical VLAN bandwidth assurance template.

12.7 Configuring MPLS QoS

12.7.1 Configuring Tunnel QoS

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *interface-number*	Enter Tunnel interface configuration mode.
4	Raisecom(config-tunnel)#**traffic-statistics enable**	Enable traffic statistics. By default, it is disabled.
5	Raisecom(config-tunnel)#**diffserv-mode** { **pipe** *exp-value* | **uniform** [**local-priority-to-exp** *profile-id*] }	Configure the Tunnel differential service mode.
6	Raisecom(config-tunnel)#**exit** Raisecom(config)#**mpls static-lsp egress** *lsp-name* **diffserv-mode** { **pipe** | **uniform** [**exp-to-local-priority** *profile-id*] }	Exit Tunnel interface configuration mode. Configure the Egress differential service mode.

12.7.2 Configuring PW QoS

Use the following commands to configure the device. Before configuring the device, ensure that the corresponding interface has been configured with the following functions.

- The interface should work in routing mode. By default, the interface is in routing mode. If the interface is currently configured to switch mode, you need to use the **no portswitch** command to configure the interface mode to routing mode.
- Use the **mode l2** command to enter L2VPN mode and access L2VPN services.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**mode l2**	Enter interface configuration mode.
3	Raisecom(config-port)#**mpls l2vpn pw diffserv-mode** { **pipe** *exp-value* [**exp-to-local-priority** *profile-id*] | **uniform** [**exp-to-local-priority** *profile-id*] [**local-priority-to-exp** *profile-id*] } [**backup**]	Configure the PW differential service mode.
4	Raisecom(config-port)#**mpls l2vpn pw traffic-statistics enable** [**backup**]	Enable PW traffic statistics. By default, it is disabled.

Copyright © Raisecom Technology Co., Ltd.

12.7.3 Configuring VPLS QoS

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls vsi** *vsi-name* **static**	Create a VSI and enter VSI configuration mode.
3	Raisecom(config-port)#**diffserv-mode** { **pipe** *exp-value* [**exp-to-local-priority** *profile-id*] | **uniform** [**exp-to-local-priority** *profile-id*] [**local-priority-to-exp** *profile-id*] }	Configure VPLS differential service mode.
4	Raisecom(config-vsi)#**traffic-statistics** [**peer** *peer-ip-address* [**vc-id** *vc-id*]] **enable**	Enable VPLS traffic statistics. By default, it is disabled.

12.7.4 Checking configurations

No.	Command	Description
1	Raisecom# **show mpls te traffic-statistics tunnel** *unit/slot/port*	Show LSP traffic statistics.
2	Raisecom#**show mpls l2vpn pw traffic-statistics** *interface-type interface-number*[**backup**]	Show PW traffic statistics.
3	Raisecom#**show mpls vsi traffic-statistics** *vsi-name* **peer** *peer-ip-address* **vc-id** *vc-id*	Show VPLS traffic statistics.

12.8 Configuring L3VPN QoS

12.8.1 Preparing for configurations

Scenario

To avoid network congestion or alleviate network congestion, you can configure L3VPN QoS.

Prerequisite

N/A

12.8.2 Configuring VRF QoS

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip vrf** *vrf-name*	Create a VRF and enter VRF configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-vrf)#**bandwidth car** [**cir** *cir-value* **pir** *pir-value*] **peer** *ip-address*	Configure peer-based bandwidth rate limiting in CAR mode.
4	Raisecom(config-vrf)#**traffic-statistics enable**	Enable L3VPN VRF statistics. By default, it is disabled.
5	Raisecom(config-vrf)#**diffserv-mode** { **pipe** *exp-value* [**exp-to-local-priority** *profile-id*] | **uniform** [**exp-to-local-priority** *profile-id*] [**local-priority-to-exp** *profile-id*] }	Configure the L3VPN differential service mode.
6	Raisecom(config-vrf)#**ttl** { **pipe** | **uniform** }	Configure the TTL mode. By default, the TTL mode is Pipe.

12.8.3 Checking configurations

No.	Command	Description
1	Raisecom#**show traffic-statistics vrf** *vrf-name*	Show VRF traffic statistics.

12.9 Configuring HQoS

12.9.1 Configuring the HQoS profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls hqos profile** *profile-number*	Create a HQoS profile.
3	Raisecom(hqos)#**mls hqos user-group profile** *profile-number*	Apply the queue user group profile to the HQoS profile.

12.9.2 Configuring the HQoS user or user group profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls hqos user profile** *profile-number*	Create a HQoS user profile.
3	Raisecom(config)#**mls hqos user-group profile** *profile-number*	Create a HQoS user group profile.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(hqos-user)#**match type inner-vlan** *vlan-id* Raisecom(hqos-user-group)#**match type vlan** *vlan-id*	Configure the HQoS user or user group to match VLAN parameters.
5	Raisecom(hqos-user)#**car cir** *cir-value* **cbs** *cbs-value* [**pir** *pir-value* **pbs** *pbs-value*] Raisecom(hqos-user-group)#**car cir** *cir-value* **cbs** *cbs-value* [**pir** *pir-value* **pbs** *pbs-value*]	Configure queue rate limiting parameters of the HQoS user or user group.

12.9.3 Configuring the HQoS queue profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls hqos queue profile** *profile number*	Create a HQoS queue profile.
3	Raisecom(hqos-queue)#**scheduler** { **sp** | **wrr** }	Configure the mode for scheduling the user group.
4	Raisecom(hqos-queue)#**queue** *queue-id* [**weight** *weight-value*] [**car cir** *cir-value* **cbs** *cbs-value* [**pir** *pir-value* **pbs** *pbs-value*]] Raisecom(hqos-queue)#**exit**	Configure the weight and rate limiting parameters of the queue.

12.9.4 Applying the HQoS profile to the interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**mls hqos profile** *profile-number* [**outbound**]	Apply the HQoS profile to the interface.

12.9.5 Checking configurations

No.	Command	Description
1	Raisecom#**show mls hqos profile** [*profile-number*]	Show configurations of the HQoS profile.
2	Raisecom#**show mls hqos queue profile** [*profile-number*]	Show configurations of the HQoS queue profile.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
3	Raisecom#**show mls hqos user profile** [*profile-number*]	Show configurations of the HQoS user profile.
4	Raisecom#**show mls hqos user-group profile** [*profile-number*]	Show configurations of the HQoS user group profile.

12.10 Maintenance

Command	Description
Raisecom(config)#**clear service-policy statistics interface** *interface-type interface-number* { **egress** | **ingress** }	Clearing traffic policy statistics.
Raisecom(config)#**clear service-policy statistics interface** *interface-type interface-number* { **egress** | **ingress** } **policy-map** *policy-map-name* [**class-map** *class-map-name*]	
Raisecom(config)#**clear mls qos queue statistics interface** *interface-type interface-number* [**queueid** *queue-id*]	Clear queue statistics of interfaces.
Raisecom(config)#**clear filter statistics interface** *interface-type interface-number* { **ingress** | **egress** } [**access-list** *acl-number*]	Clear ACL statistics.
Raisecom(config)#**clear performance statistics history**	Clear performance statistics of all history groups.
Raisecom(config)# **clear mpls te traffic-statistics tunnel** *tunnel-if-num*	Clear LSP statistics.
Raisecom(config)#**clear mpls l2vpn pw traffic-statistics** *interface-type interface-number* [**backup**]	Clear PW statistics.
Raisecom(config)#**clear mpls vsi traffic-statistics** *vsi-name* [**peer** *peer-ip-address* **vc-id** *vc-id*]	Clear VPLS statistics.

12.11 Configuration examples

12.11.1 Example for configuring rate limiting based on traffic policy

Networking requirements

As shown in Figure 12-1, User A, User B, and User C are respectively connected to device A through device 1, device 2, and device 3.

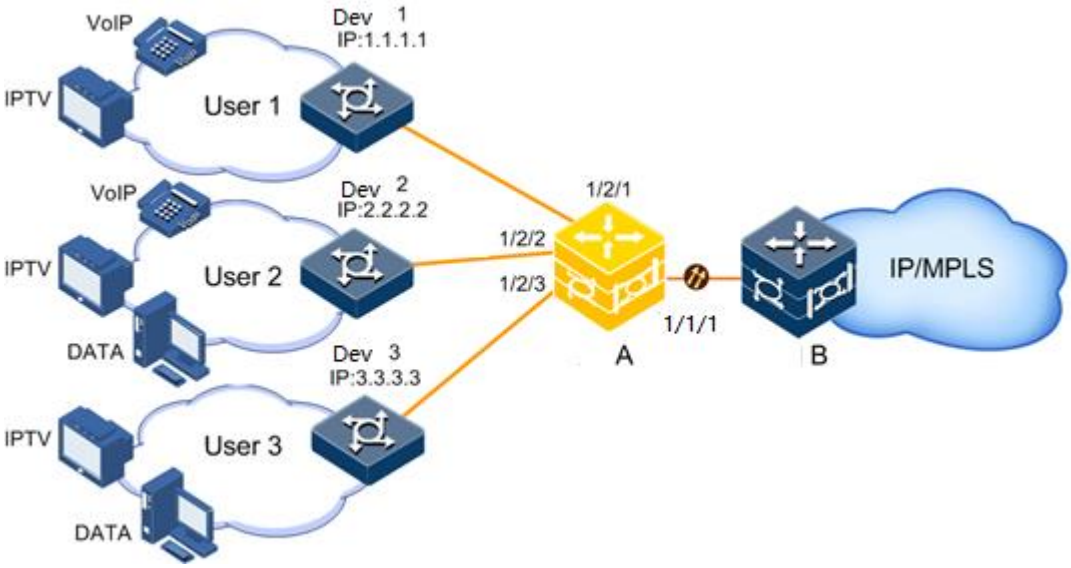
User 1 uses voice and video services; User 2 uses voice, video, and data services; User 3 uses video and data services.

According to users' requirements, make the following rules:

Copyright © Raisecom Technology Co., Ltd.

- For User 1, provide 100 Mbit/s assured bandwidth; configure the burst traffic to 200 Kbytes, and discard the redundant traffic.
- For User 2, provide 150 Mbit/s assured bandwidth; configure the burst traffic to 250 Kbytes, and discard the redundant traffic.
- For User 3, provide 130 Mbit/s assured bandwidth; configure the burst traffic to 230 Kbytes, and discard the redundant traffic.

Figure 12-1 Configuring rate limiting based on traffic policy



Configuration steps

Step 1 Create and configure traffic classification on device A.

```
Raisecom#config
Raisecom(config)#access-list 1001
Raisecom(config-acl-ip-std)#rule 1 permit 1.1.1.1 255.255.255.255
Raisecom(config-acl-ip-std)#exit
Raisecom(config)#class-map usera match-all
Raisecom(config-cmap)#match acl 1001
Raisecom(config-cmap)#exit
Raisecom(config)#access-list 1002
Raisecom(config-acl-ip-std)#rule 2 permit 2.2.2.2 255.255.255.255
Raisecom(config-acl-ip-std)#exit
Raisecom(config)#class-map userb
Raisecom(config-cmap)#match acl 1002
Raisecom(config-cmap)#exit
Raisecom(config)#access-list 1003
Raisecom(config-acl-ip-std)#rule 3 permit 3.3.3.3 255.255.255.255
Raisecom(config-acl-ip-std)#exit
Raisecom(config)#class-map userc
Raisecom(config-cmap)#match acl 1003
Raisecom(config-cmap)#exit
```


Copyright © Raisecom Technology Co., Ltd.

Step 2 Create traffic policing profiles and configure rate limiting rules.

```
Raisecom(config)#mls qos policer-profile usera single
Raisecom(traffic-policer)#cir 100000 cbs 200
Raisecom(traffic-policer)#drop-color red
Raisecom(traffic-policer)#exit
Raisecom(config)#mls qos policer-profile userb single
Raisecom(traffic-policer)#cir 150000 cbs 250
Raisecom(traffic-policer)#drop-color red
Raisecom(traffic-policer)#exit
Raisecom(config)#mls qos policer-profile userc single
Raisecom(traffic-policer)#cir 150000 cbs 250
Raisecom(traffic-policer)#drop-color red
Raisecom(traffic-policer)#exit
```

Step 3 Create and configure traffic policies.

```
Raisecom(config)#policy-map usera
Raisecom(config-pmap)#class-map usera
Raisecom(config-pmap-c)#policer usera
Raisecom(config-pmap-c)#exit
Raisecom(config-pmap)#exit
Raisecom(config)#interface gigaethernet 1/2/1
Raisecom(config-gigaethernet1/2/1)#service-policy ingress usera
Raisecom(config-gigaethernet1/2/1)#exit
Raisecom(config)#policy-map userb
Raisecom(config-pmap)#class-map userb
Raisecom(config-pmap-c)#policer userb
Raisecom(config-pmap-c)#exit
Raisecom(config-pmap)#exit
Raisecom(config)#interface  gigaethernet 1/2/2
Raisecom(config-port)#service-policy ingress userb
Raisecom(config)#policy-map userc
Raisecom(config-pmap)#class-map userc
Raisecom(config-pmap-c)#policer userc
Raisecom(config-pmap-c)#exit
Raisecom(config-pmap)#exit
Raisecom(config)#interface gigaethernet 1/2/3
Raisecom(config-port)#service-policy ingress userc
```

Checking results

Use the **show class-map** command to show configurations of traffic classification.

```
Raisecom#show class-map usera
Class Map usera (id 0) (ref 1)
    Match acl 1001
Raisecom#show class-map userb
```


Copyright © Raisecom Technology Co., Ltd.

```
Class Map userb (id 1) (ref 1)
    Match acl 1002
Raisecom#show class-map userc
Class Map userb (id 2) (ref 0)
    Match acl 1003
```

Use the **show mls qos policer-profile** command to show configurations of rate limiting rules.

```
Raisecom#show mls qos policer-profile
single-policer: usera        mode:flow   color-mode:blind
cir: 100000 kbps  cbs: 200 kB
red  drop
single-policer: userb        mode:flow   color-mode:blind
cir: 150000 kbps  cbs: 250 kB
red  drop
single-policer: userc        mode:flow   color-mode:blind
cir: 150000 kbps  cbs: 250 kB
red  drop
```

Use the **show policy-map** command to show configurations of the traffic policy.

```
Raisecom#show policy-map usera
  Policy Map usera
    Class-map usera
        police usera
Raisecom#show policy-map userb
  Policy Map userb
    Class-map userb
        police userb
Raisecom#show policy-map userc
  Policy Map userc
    Class-map userc
        police userc
```

Use the **show service-policy interface** command to show the application status of the traffic policy on the interface.

```
Raisecom#show service-policy interface
Interface                   Direction PolicyMap
------------------------------------------------------------

gigaethernet1/2/1             ingress   usera
gigaethernet1/2/2             ingress   userb
gigaethernet1/2/3             ingress   userc
```


Copyright © Raisecom Technology Co., Ltd.

12.11.2 Example for configuring queue scheduling and congestion avoidance

Networking requirements

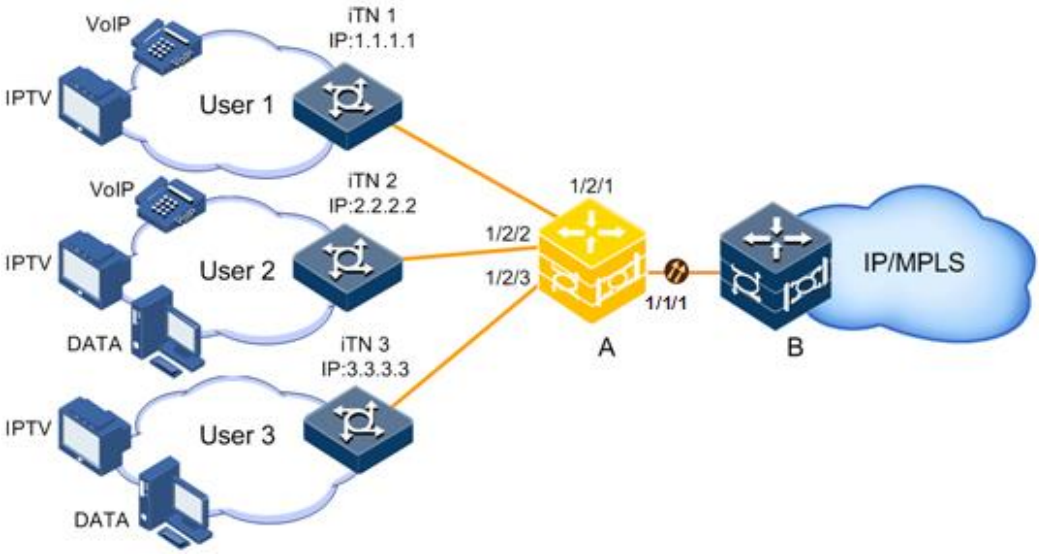
As shown in Figure 12-2, User 1 uses voice and video services; User 2 uses voice, video, and data services; User 3 uses video and data services.

CoS priorities for voice, video and, data services are configured to 5, 4, and 2 respectively. CoS priorities are mapped to local priorities 6, 5, and 2 respectively.

Make the following rules based on service types.

- Perform SP scheduling on the voice service to ensure that the traffic is preferentially transmitted. By default, the device adopts the SP scheduling.
- Perform WRR scheduling on the video service and configure the weight to 50.
- Perform WRR scheduling on the data service and configure the weight to 20. In addition, you need to configure the discarding threshold to 50, to avoid network congestion caused by too large instantaneous traffic.

Figure 12-2 Configuring queue scheduling networking



Configuration steps

Step 1 Create a WRED profile.

```
Raisecom#config
Raisecom(config)#mls qos wred profile 1
Raisecom(wred)#wred start-drop-threshold 50 end-drop-threshold 90 max-drop-probability 60
Raisecom(wred)#exit
```


Copyright © Raisecom Technology Co., Ltd.

Step 2 Configure the priority trust and congestion avoidance on interfaces and apply the traffic queue to egress interface tengigabitethernet 1/1/1.

```
Raisecom(config)#mls qos flow-queue profile 6
Raisecom(flow-queue)#scheduler wrr
Raisecom(flow-queue)#queue 6 weight 50
Raisecom(flow-queue)#queue 3 weight 20 wred profile 1
Raisecom(flow-queue)#exit
Raisecom(config)#interface tengigabitethernet 1/1/1
Raisecom(config-tengigabitethernet1/1/1)#mls qos flow-queue 6
Raisecom(config-tengigabitethernet)#interface tengigabitethernet 1/2/1
Raisecom(config-tengigabitethernet1/2/1)#mls qos trust cos
Raisecom(config-tengigabitethernet1/2/1)#exit
Raisecom(config)#interface tengigabitethernet 1/2/2
Raisecom(config-tengigabitethernet1/2/2)#mls qos trust cos
Raisecom(config-tengigabitethernet1/2/2)#exit
Raisecom(config)#interface tengigabitethernet 1/2/3
Raisecom(config-tengigabitethernet1/2/3)#mls qos trust cos
Raisecom(config-tengigabitethernet1/2/3)#exit
```

Before configuration, ensure that each interface is in switch mode.

Step 3 Configure the mapping between the CoS priority and local priority.

```
Raisecom(config)#mls qos mapping cos-to-local-priority 1
Raisecom(cos-to-pri)#cos 5 to local-priority 6
Raisecom(cos-to-pri)#cos 4 to local-priority 5
Raisecom(cos-to-pri)#cos 2 to local-priority 2
Raisecom(cos-to-pri)#exit
Raisecom(config)#interface tengigabitethernet 1/2/1
Raisecom(config-tengigabitethernet1/2/1)#mls qos cos-to-local-priority 1
Raisecom(config-tengigabitethernet1/2/1)#interface tengigabitethernet
1/2/2
Raisecom(config-tengigabitethernet1/2/2)#mls qos cos-to-local-priority 1
Raisecom(config-tengigabitethernet1/2/2)#interface tengigabitethernet
1/2/3
Raisecom(config-tengigabitethernet1/2/3)#mls qos cos-to-local-priority 1
Raisecom(config-tengigabitethernet1/2/3)#exit
```

Checking results

Use the **show mls qos mapping cos-to-local-priority** command to show mapping configurations on specified priorities.

```
Raisecom#show mls qos mapping cos-to-local-priority
G:GREEN
```


Copyright © Raisecom Technology Co., Ltd.

```
Y:YELLOW
R:RED
cos-to-localpriority(color)
Index Description     Ref   CoS:          0      1      2      3      4
5      6      7
--------------------------------------------------------------------------
--------------------------------
1     --              3     localpri(color) :0(G)    1(G)    2(G)    3(G)    5(G)
6(G)    6(G)    7(G)
```

Use the **show mls os** command to show configurations of priority trust and queue scheduling mode on specified interfaces.

```
Raisecom(config)#show mls qos interface tengigabitethernet 1/2/1
Current interface name: tengigabitethernet1/2/1
Current interface QoS configuration information:
--------------------------------------------------------------------------
----------------------
 Trust mode                 : Cos          |  Priority                   :
untagged 0
 Pri-Set/Override based on SMAC : --           |  Priority Override
State       : Disable
 Pri-Set/Override based on DMAC : --           |  Pri-Set/Override based
on VLAN : --
 Default DSCP               : --           |  Dei State                  :
Disable
 Cos-remark-profile          : 0            |  Color Aware
state            : Disable
 Cos-local-priority-profile    : 1            |  Cos-remark-
mapping           : Disable
 Dscp-local-priority-profile   : 0            |  Ipp-local-priority-
profile    : --
 Tos-local-priority-profile    : 0            |  Dscp-mutation-profile

Raisecom(config)#show mls qos interface tengigabitethernet 1/2/2
Current interface QoS configuration information:
--------------------------------------------------------------------------
----------------------
 Trust mode                 : Cos          |  Priority                   :
untagged 0
 Pri-Set/Override based on SMAC : --           |  Priority Override
State       : Disable
 Pri-Set/Override based on DMAC : --           |  Pri-Set/Override based
on VLAN : --
 Default DSCP               : --           |  Dei State                  :
Disable
 Cos-remark-profile          : 0            |  Color Aware
state            : Disable
 Cos-local-priority-profile    : 1            |  Cos-remark-
mapping           : Disable
 Dscp-local-priority-profile   : 0            |  Ipp-local-priority-
profile    : --
```


Copyright © Raisecom Technology Co., Ltd.

```
 Tos-local-priority-profile    : 0           |  Dscp-mutation-
profile        : --

Raisecom(config)#show mls qos interface tengigabitethernet 1/2/3
Current interface QoS configuration information:
------------------------------------------------------------------------
----------------------
 Trust mode                 : Cos          |  Priority                   :
untagged 0
 Pri-Set/Override based on SMAC : --           |  Priority Override
State       : Disable
 Pri-Set/Override based on DMAC : --           |  Pri-Set/Override based
on VLAN : --
 Default DSCP               : --           |  Dei State                  :
Disable
 Cos-remark-profile          : 0            |  Color Aware
state            : Disable
 Cos-local-priority-profile    : 1           |  Cos-remark-
mapping           : Disable
 Dscp-local-priority-profile   : 0           |  Ipp-local-priority-
profile    : --
 Tos-local-priority-profile    : 0           |  Dscp-mutation-
profile        : --
```

Use the **show mls qos flow-queue** command to show configurations of queue scheduling.

```
Raisecom#show mls qos flow-queue profile 6
CIR: Committed information rate,unit:Kbps
CBS: Committed burst size,unit:KB
PIR: Peak information rate,unit:Kbps
PBS: Peak burst size,unit:KB
ProfileIndex :6
Flow-Queue-Description :--
Flow-Queue-Reference :1
Flow-Queue-Scheduler :wrr
QueueId   Weight   Wred  CIR(Kbps)  CBS(KB)  PIR(Kbps)  PBS(KB)
-----------------------------------------------------------------

0       0       0     --        --       --        --
1       0       0     --        --       --        --
2       0       0     --        --       --        --
3       20      1     --        --       --        --
4       0       0     --        --       --        --
5       0       0     --        --       --        --
6       50      0     --        --       --        --
7       0       0     --        --       --        --
```

Use the **show mls qos wred profile** command to show configurations of the WRED profile.

```
Raisecom#show mls qos wred profile
```


Copyright © Raisecom Technology Co., Ltd.

```
GSDT:Green Start Drop Threshold
GEDT:Green End Drop Threshold
GDP :Green Drop Probability
YSDT:Yellow Start Drop Threshold
YEDT:Yellow End Drop Threshold
YDP :Yellow Drop Probability
RSDT:Red Start Drop Threshold
REDT:Red End Drop Threshold
RDP :Red Drop Probability

Index Description     Ref   GSDT     GEDT     GDP      YSDT     YEDT
YDP      RSDT     REDT     RDP
------------------------------------------------------------------------
-----------------------------------------------
1                     1     50       90       60       50       90       60
50       90       60
```

12.11.3 Example for configuring interface-based rate limiting

Networking requirements

As shown in Figure 12-3, User 1, User 2, and User 3 are connected to the aggregation device Device A through device 1, device 2, and device 3, and the backbone network through device B.

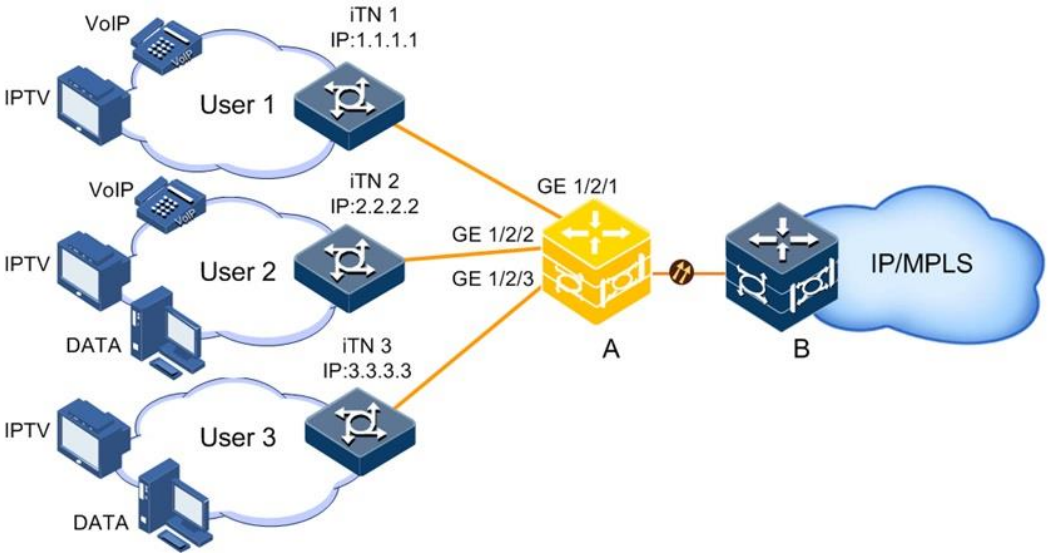
User 1 uses voice and video services; User 2 uses voice, video, and data services; User 3 uses video and data services.

According to users' requirements, make the following rules:

- For User 1, provide 100 Mbit/s assured bandwidth; configure the burst traffic to 200 Kbytes; set the PIR to 500 Mbit/s, and configure the PBS to 300 Kbytes.
- For User 2, provide 200 Mbit/s assured bandwidth; configure the burst traffic to 300 Kbytes; set the PIR to 700 Mbit/s, and configure the PBS to 400 Kbytes.
- For User 3, provide 300 Mbit/s assured bandwidth; configure the burst traffic to 500 Kbytes; set the PIR to 700 Mbit/s, and configure the PBS to 400 Kbytes.

Copyright © Raisecom Technology Co., Ltd.

Figure 12-3 Configuring interface-based rate limiting



Configuration steps

Configure interface-based rate limiting.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/2/1
Raisecom(config-gigaethernet1/2/1)#rate-limit ingress cir 100000 cbs 200
pir 500000 pbs 300
Raisecom(config)#interface gigaethernet 1/2/2
Raisecom(config-gigaethernet1/2/1)#rate-limit ingress cir 200000 cbs 300
pir 700000 pbs 400
Raisecom(config)#interface  gigaethernet 1/2/3
Raisecom(config-gigaethernet1/2/1)#rate-limit ingress cir 300000 cbs 500
pir 700000 pbs 400
```

Checking results

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

```
Raisecom#show rate-limit interface
Interface                 Direction Cir(kbps)  Cbs(kB)  Pir(kbps)  Pbs(kB)
CirOper(kbps)  CbsOper(kB)  PirOper(kbps)  PbsOper(kB)
------------------------------------------------------------------------
------------------------------------------------------------
gigaethernet1/2/1           ingress   100000     200      500000     500
100000        200         200000        300
gigaethernet1/2/2           ingress   200000     300      700000     500
200000        300         700000        400
gigaethernet1/2/3           ingress   300000     500      500000     700
300000        400         500000        400
```


Copyright © Raisecom Technology Co., Ltd.

13 Multicast

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

- Configuring IGMP
- Configuring IGMP MVR
- Configuring IGMP filtering
- Configuring PIM
- Configuring multicast VPN
- Configuration examples

13.1 Configuring IGMP

13.1.1 Preparing for configurations

Scenario

IGMP is applied to the network segment where the routing device is connected to the user host. You can configure IGMP on the interface of the multicast device connected to the user network segment, to enable the user host to access the multicast network so that multicast packets can reach the receiver.

The host informs the local routing device through IGMP that it wants to join and receive the information of a specific multicast group. At the same time, the routing device periodically queries whether the members of a known group in the network are active through IGMP, collecting and maintaining information about all connected group members.

Prerequisite

Before configuring IGMP:

- Configure the network-layer properties of the interface to ensure the network connectivity.
- Enable multicast routing.

Copyright © Raisecom Technology Co., Ltd.

13.1.2 Configuring Layer 2 IGMP

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**igmp member-timeout** { *seconds* | **infinite** }	Configure the aging time of IGMP members.
3	Raisecom(config)#**igmp report-suppression**	Enable Report suppression. Packet suppression and Proxy conflict with each other.
4	Raisecom(config)#**igmp last-member-query-count** *count*	Configure the times for querying IGMP last member.
5	Raisecom(config)#**igmp last-member-query-interval** *interval*	Configure the last member query interval, that is, the interval between query messages for a specific group. This value can be used to adjust the "leave delay" of the network.
6	Raisecom(config)#**igmp mrouter** { **mcast-vlan** *vlan-list* **priority** *priority-number* | **vlan** *vlan-id interface-type interface-number* }	Configure the multicast routing port.
7	Raisecom(config)#**igmp multicast-tag** { **translate** | **transparent** }	Configure the multicast VLAN tag mode.
8	Raisecom(config)#**igmp robust-count** *value*	Configure the robustness coefficient, that is, the number of packet retransmissions caused by network packet loss.
9	Raisecom(config)#**igmp proxy**	Enable IGMP proxy.
10	Raisecom(config)#**igmp last-member-query-interval** *interval*	Configure the query interval of the last member, namely, the interval between query messages of the specified group. This value can be used to adjust the leave-delay.
11	Raisecom(config)#**igmp query-max-response-time** *period*	Configure the maximum query response time, which is shorter than the IGMP message query interval.
12	Raisecom(config)#**igmp version** { **2** | **3** }	Configure the supported IGMP version.

13.1.3 Configuring Layer 3 IGMP

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip igmp send-router-alert enable**	Enable IGMP to send router alarms.
3	Raisecom(config)#**ip igmp vlan-flooding enable**	Enable IGMP VLAN flooding.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Configuration	Description
5	Raisecom(config-port)#**ip igmp version** { **1** | **2** | **3** }	Configure the version of IGMP supported.
6	Raisecom(config-port)#**ip igmp enable**	Enable IGMP on the VLAN interface.

13.1.4 Configuirng IGMP proxy

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip igmp proxy enable**	Enable IGMP proxy.

13.1.5 Configuring static group members

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip igmp static group** *group-address*	Configure static group members on the interface.
4	Raisecom(config-gigaethernet*/*/*)#**ip igmp bind backup-id** *number*	(Optional) bind the IGMP with the backup ID.
5	Raisecom(config-gigaethernet*/*/*)#**exit**	Return to global configuration mode.
6	Raisecom(config)#**ip igmp bind iccp-channel** *channel-id*	(Optional) bind the IGMP with the ICCP channel.

13.1.6 Querying IGMP packets

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip igmp querier-election enable**	Configure IGMP querier selection.
4	Raisecom(config-port)#**ip igmp query-interval** *period*	Configure the interval for querying IGMP packets.

Copyright © Raisecom Technology Co., Ltd.

13.1.7 Configuring robustness coefficient

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip igmp robustness-variable** *value*	Configure the robustness coefficient, that is, the number of packet retransmissions caused by network packet loss.

13.1.8 Configure the time for querying the last member

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip igmp last-member-query-interval** *interval*	Configure the last member query interval, that is, the time interval between query messages for a specific group. This value can be used to adjust the "leave delay" of the network.

13.1.9 Configuring the maximum query response time

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip igmp query-max-response-time** *period*	Configure the maximum query response time, which should be smaller than the IGMP packet query interval.

13.1.10 Configuring immediate leave of multicast members

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip igmp immediate-leave** [**vlan** *vlan-list*]	Configure immediate leave of multicast members.

Copyright © Raisecom Technology Co., Ltd.

13.1.11 Configuring IGMP SSM Mapping

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)# **ip igmp ssm-mapping** { *group-ip-address group-ip-mask* | *group-ip-addresss/mask* } *source-ip-address*	(Optional) configure the mapping rules for the specified multicast group and multicast source.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
4	Raisecom(config-port)#**ip igmp ssm-mapping** { **enable** | **disable** }	(Optional) enable mapping of the specified multicast group and multicast source.

13.1.12 Configuring IGMP multicast VLAN copy

Before configuring IGMP multicast VLAN copy, you need to disable IGMP Snooping and IGMP MVR on the device.

Default configurations of multicast VLAN copy

Function	Default value
Global multicast VLAN copy	Disable
Interface multicast VLAN copy	Disable
Static forwarding table of the multicast VLAN	N/A
Binding relationship between the multicast VLAN and the multicast group	N/A

Configuring multicast VLAN copy

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**igmp vlan-copy**	Enable global multicast VLAN copy.
3	Raisecom(config)#**igmp vlan-copy mcast-vlan** *vlan-id* **group** { *start-ip-address* [*end-ip-address*] | **any** }	Configure the binding relationship between the multicast VLAN and the multicast group.

13.1.13 Configuring packet track

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

Copyright © Raisecom Technology Co., Ltd.

Step	Configuration	Description
2	Raisecom(config)#**interface vlan** *interface-number*	Enter interface configuration mode.
3	Raisecom(config-vlanport)#**ip igmp track vrrp virtual-ip** *ip-address*	Configure the virtual IP address for the IGMP packets to trace VRRP packets.

13.1.14 Checking configurations

No.	Configuration	Description
1	Raisecom#**show ip igmp group** [*group-address* | *interface-type interface-number* | **vlan** *vlan-id*]	Show the multicast group member relationship.
2	Raisecom#**show ip igmp interface** [*interface-type interface-number* | **vlan** *vlan-id*]	Show IGMP configurations of the Layer 3 interface.
3	Raisecom#**show ip igmp statistics** [*interface-type interface-number* | **vlan** *vlan-id*]	Show IGMP packet statistics.
4	Raisecom#**show ip igmp ssm-mapping group**	Show the mapping relationship between the multicast group and multicast source.

13.1.15 Maintenance

You can maintain IGMP features through the following commands.

Command	Description
Raisecom(config)#**clear ip igmp statistics** [*interface-type interface-number*]	Clear IGMP packet statistics.
Raisecom(config)#**clear ip igmp group** [*group-address* | *interface-type interface-number*]	Clear the multicast forwarding table.

13.2 Configuring IGMP MVR

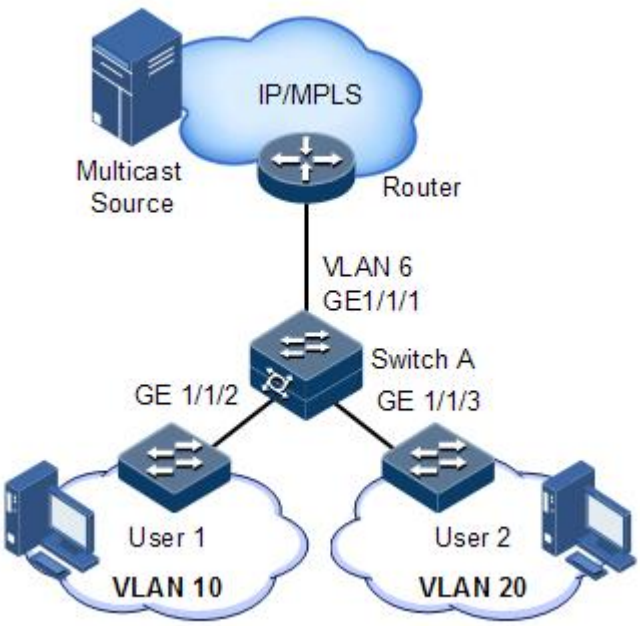
13.2.1 Preparing for configurations

Scenario

As shown in Figure 13-1, multiple users receive data from the multicast source, and multiple users and multicast routers belong to different VLANs. You can run IGMP MVR on Switch A and configure multicast VLANs to enable users in different VLANs to share the same multicast VLAN to receive the same multicast data, while also reducing bandwidth waste.

Copyright © Raisecom Technology Co., Ltd.

Figure 13-1 IGMP MVR application



Prerequisite

Before configuring IGMP MVR, complete the following tasks:

- Disable multicast VLAN copy on the device.
- Create a VLAN and add the corresponding interface to the VLAN.

13.2.2 Default configurations of IGMP MVR

Function	Default value
Global IGMP MVR status	Disable
Interface IGMP MVR status	Disable
Multicast VLAN and group address set	N/A

13.2.3 Configuring IGMP MVR

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp mvr`	Enable IGMP MVR.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**igmp mvr mcast-vlan** *vlan-id* **group** { *start-ip-address* [*end-ip-address*] | **any** }	Configure the group address set of multicast VLAN. **Note** After IGMP MVR is enabled on the device, you need to configure the multicast VLAN and the bound group address set. If the received IGMP Report packet does not belong to any VLAN group address set, the report packet is not processed and the user cannot subscribe to multicast flow.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter L2 physical interface configuration mode.
5	Raisecom(config-port)#**igmp mvr**	Enable interface IGMP MVR.
6	Raisecom(config-port)#**igmp mvr user-vlan** *vlan-list*	(Optional) configure the effective range of multicast cross-VLAN copy.

Note

- IGMP MVR and IGMP snooping cannot be enabled at the same time in the same multicast VLAN, otherwise the configuration fails.
- IGMP MVR and multicast VLAN copy cannot be enabled simultaneously in the same multicast VLAN and multicast group, otherwise the configuration fails.

13.2.4 Checking configurations

Step	Command	Description
1	Raisecom#**show igmp mvr** [**interface** | *interface-type interface-number*]	Show configurations of the IGMP MVR of the specified interface.
2	Raisecom#**show igmp mvr member** [*interface-type interface-number* | **user-vlan** *vlan-id*]	Show information about IGMP MVR multicast group members.
3	Raisecom#**show igmp mvr member count** [*interface-type interface-number* | **user-vlan** *vlan-id*]	Show the number of members in the IGMP MVR multicast group.
4	Raisecom#**show igmp mvr vlan-group** [**mcast-vlan** *vlan-id*]	Show the multicast VLAN and its group address set.

Copyright © Raisecom Technology Co., Ltd.

13.3 Configuring IGMP filtering

13.3.1 Preparing for configurations

Scenario

Different users in the same multicast have different requirements or permissions to receive multicast packets. It is allowed to configure the filtering rules on the device connected to the multicast router and the host to restrict the multicast users.

You can also configure the maximum number of multicast groups that users are allowed to join.

IGMP filtering is generally used in conjunction with IGMP Snooping or IGMP MVR.

Prerequisite

Before configuring IGMP, complete the following tasks:

- Create a VLAN.
- Add the corresponding interface to the VLAN.

13.3.2 Default configurations of IGMP filtering

Function	Default value
Global IGMP filtering	Disable
IGMP filtering profile	N/A
Action of IGMP filtering profile	Deny
Interface IGMP filtering	• No limits for the maximum groups • Action of the maximum group: drop • No filtering profile applied
"Interface + VLAN" IGMP filtering	• No limits for the maximum groups • Action of the maximum group: drop • No filtering profile applied

13.3.3 Enabling IGMP filtering globally

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp filter`	Enable IGMP filtering globally.

Copyright © Raisecom Technology Co., Ltd.

When configuring the IGMP filtering templates or the maximum number of groups, you need to execute the **igmp filter** command to enable IGMP filtering globally.

13.3.4 Configuring IGMP filtering template

The IGMP filtering template can be used under the interface, and can also be applied on "interface + VLAN".

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**igmp filter profile** *profile-number*	Create an IGMP profile and enter profile configuration mode.
3	Raisecom(config-igmp-profile)#{ **permit** | **deny** }	Configure IGMP profile actions.
4	Raisecom(config-igmp-profile)#**range** *range-id start-ip-address* [*end-ip-address*]	Configure the IP multicast address or range of control access.
5	Raisecom(config-igmp-profile)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 2 physical interface configuration mode or aggregation group configuration mode. The following takes Layer 2 physical interface configuration mode for example.
6	Raisecom(config-port)#**igmp filter profile** *profile-number* [**vlan** *vlan-list*]	Apply the IGMP profile filtering template to the physical interface or "interface+VLAN".

By executing the **igmp filter profile** *profile-number* command in interface configuration mode, you can apply the created IGMP profile to the specified interface. An IGMP profile can be applied to multiple interfaces, but each interface can only have one IGMP profile.

13.3.5 Configuring maximum number of groups

The maximum number of groups that a user can join can be applied to the interface or "interface + VLAN".

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 2 physical interface configuration mode or aggregation group configuration mode. The following takes physical interface configuration mode for example.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-gigaethernet1/1/*)#**igmp filter max-groups** *group-number* [**vlan** *vlan-list*]	(Optional) configure the maximum number of groups allowed on the interface or "interface + VLAN".
4	Raisecom(config-gigaethernet1/1/*)#**igmp filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	(Optional) configure actions to be taken when the number of interfaces or "interface + VLAN" groups exceeds the maximum number of groups.

13.3.6 Checking configurations

No.	Command	Description
1	Raisecom#**show igmp filter** [{ **interface** | *interface-type interface-number* } [**vlan** [*vlan-id*]]]	Show configurations of IGMP filtering.
2	Raisecom#**show igmp filter profile** [*profile-number*]	Show information about the IGMP Profile.

13.4 Configuring PIM

13.4.1 Preparing for configurations

Scenario

Compared with unicast and broadcast, the biggest advantage of multicast is that it implements single-point transmission and multipoint reception with minimal network overhead. Configure the PIM to build a multicast distribution tree, so that the multicast source only needs to send a piece of information, and the transmitted information is copied and distributed only at the network node (RP) as far as possible from the multicast source.

Prerequisite

N/A

13.4.2 Enabling PIM

Enabling IPv4 PIM

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-port)#**ip pim sparse-mode**	Enable IPv4 PIM-SM on the interface. By default, PIM-SM is disabled on the interface.
4	Raisecom(config-port)#**ip pim bsr-boundary**	Configure the interface Bootstrap routing border.
5	Raisecom(config-port)#**ip pim bfd** { **enable** | **disable** }	Configure interface PIM bidirectional forwarding detection.
6	Raisecom(config-port)#**ip pim dense-mode**	Enable IPv4 PIM-DM on the interface. By default, PIM-DM is disabled.

Enabling IPv4 PIM GR

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router pim**	Enter IPv4 PIM configuration mode.
3	Raisecom(config-router-pim)#**graceful-restart**	Enable IPv4 PIM GR, which ensures no service interruption during master/slave switching.

13.4.3 Configuring PIM domain DR election

Configuring IPv4 PIM domain DR

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip pim dr-priority** *priority-value*	In the IPv4-based PIM domain, configure the priority of interfaces participating in DR elections. By default, the DR priority on the interface is 1.

13.4.4 Configuring PIM domain RP election

Configuring IPv4-based PIM domain RP election

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router pim**	Enter IPv4 PIM configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-router-pim)#**bsr-candidate** *interface-type interface-number* [**hash-mask-length** *hash-mask-length* [**priority** *priority*]]	Configure the candidate election router of the PIM domain.
4	Raisecom(config-router-pim)#**rp-candidate** *interface-type interface-number* [**group** *ip-address/m*]	Configure the candidate RP parameter of the PIM domain.

Configuring IPv6-based PIM domain RP election

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ipv6 pim**	Enter IPv6-based PIM configuration mode.
3	Raisecom(config-router-pim6)#**bsr-candidate** *ipv6-address* [**hash-mask-length** *hash-mask-length* [**priority** *priority*]]	Configure the candidate election router of the PIM domain.
4	Raisecom(config-router-pim6)#**rp-candidate** *ipv6-address* [**group** *ipv6-address/m*]	Configure the candidate RP parameter of the PIM domain.

13.4.5 Configuring PIM multicast source

Configuring IPv4 multicast source

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router pim**	Enter IPv4 PIM configuration mode.
3	Raisecom(config-router-pim)#**source-lifetime** *interval*	Configure the aging time of the multicast source. By default, the aging time of the multicast source is 210s.
4	Raisecom(config-router-pim)#**dr-ignore**	Configure the ignore DR function. After ignoring the DR function, the device ignores the DR information in the Hello packet of the PIM neighbor and always considers itself to be the DR.
5	Raisecom(config-router-pim)#**group-backup**	Configure to enable the multicast group backup function. The information of the active multicast group is transmitted to the standby multicast group through PIM, and the standby multicast group sends IGMP to join the multicast route for layer 2 diversion.

Copyright © Raisecom Technology Co., Ltd.

13.4.6 Switching from RPT to SPT

The PIM-SM multicast router initially forwards multicast data via RPT, but if the rate at which multicast data passes exceeds a certain threshold, the receiver-side DR will initiate the RPT-to-SPT switch.

IPv4-based switching

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router pim`	Enter IPv4 PIM configuration mode.
3	`Raisecom(config-router-pim)#spt-threshold { traffic-rate | infinity } [ group-policy acl-number ]`	Configure the control parameters for multicast members to switch from RPT to SPT. By default, SPT is switched immediately after receiving the first multicast data packet from RPT.
4	`Raisecom(config-router-pim)#timer spt-switch interval`	Configure the interval to check whether the multicast data rate reaches the threshold before switching from RPT to SPT. By default, the interval to check whether the multicast data rate reaches the threshold before RPT-to-SPT switching is 15s.

Note

IPv6 multicast is not supported at present.

Configuring IPv6-based switching

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router ipv6 pim`	Enter IPv6 PIM configuration mode.
3	`Raisecom(config-router-pim6)#spt-threshold { traffic-rate | infinity } [ group-policy acl-number ]`	Configure the control parameters for multicast members to switch from RPT to SPT. By default, SPT switching is performed immediately after the first multicast data packet is received from RPT.
4	`Raisecom(config-router-pim6)#timer spt-switch interval`	Configure the interval to check whether the multicast data rate reaches the threshold before RPT-to-SPT switching is performed. By default, the interval to check whether the multicast data rate reaches the threshold before RPT-to-SPT switching is 15s.

Copyright © Raisecom Technology Co., Ltd.

13.4.7 Configuring PIM GR

Configuring PIM restart based on IPv4

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router pim**	Enter IPv4 PIM configuration mode.
3	Raisecom(config-router-pim)#**graceful-restart**	Configure IPv4-based PIM graceful restart. By default, it is disabled.

Note

IPv6 multicast is not supported at present.

Configuring IPv6-based PIM restart

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ipv6 pim**	Enter IPv6 PIM configuration mode.
3	Raisecom(config-router-pim6)#**graceful-restart**	Configure IPv6-based PIM graceful restart. By default, it is disabled.

13.4.8 Checking configurations

No.	Command	Description
1	Raisecom#**show** { **ip** | **ipv6** } **pim bsr-router**	Show election router of the PIM domain.
2	Raisecom#**show** { **ip** | **ipv6** } **pim interface**	Show information about the PIM interface.
3	Raisecom#**show** { **ip** | **ipv6** } **pim routing-table**	Show information about the PIM routing table.
4	Raisecom#**show** { **ip** | **ipv6** } **pim rp**	Show RP information about the PIM.
5	Raisecom#**show** { **ip** | **ipv6** } **pim rp-candidate**	Show candidate RP information about the PIM.
6	Raisecom#**show** { **ip** | **ipv6** } **pim neighbor**	Show PIM neighbor information.
7	Raisecom#**show** { **ip** | **ipv6** } **pim route** [**group** *ip-address* [**source** *ip-address*]]	Show PIM routing information.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
8	Raisecom#**show { ip | ipv6 } pim vmroute**	Show PIM virtual routes.

13.4.9 Maintenance

Command	Description
Raisecom#**clear ip pim process**	Reconfigure IPv4/IPv6 PIM multicast and clear PIM configurations on the current device.

13.5 Configuring multicast VPN

13.5.1 Preparing for configurations

Scenario

With the widespread application of VPN technologies, users' demand for running multicast services on VPN networks is becoming increasingly urgent. Multicast VPN is mainly based on BGP/MPLS VPN networks to implement multicast data transmission.

Prerequisites

N/A

13.5.2 Configuring the mLDP P2MP tunnel

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls lsr-id** *lsr-id*	Configure the LSR ID of the device.
3	Raisecom(config)#**mpls enable**	Enable global MPLS. By default, it is disabled.
4	Raisecom(config)#**mpls ldp**	Enable global LDP.
5	Raisecom(config)#**mpls mldp p2mp**	Enable global LDP P2MP.
6	Raisecom(config)#**multicast mvpn** *mvpn_id*	Configure the multicast MVPN ID, which is usually the IP address of the start PE of the MVPN. The main function of the MVPN ID is to import the value of the Administrator field for VRF Route Import Extended Community as a private network route.

Copyright © Raisecom Technology Co., Ltd.

13.5.3 Configuring mLDP In-Band MVPN

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip vrf** *vrf-name*	Create a VRF, and enter VRF configuration mode.
3	Raisecom(config-vrf)#**rd** *rd*	Configure the Route Distinguisher (RD) of VRF.
4	Raisecom(config-vrf)# **route-target** [**export** | **import** | **both**] *rt*	Configure the RT of the VRF.
5	Raisecom(config-vrf)#**multicast inband-signaling mldp**	Configure the iteration type of the multicast VPN tunnel.

13.6 Configuration examples

13.6.1 Example for applying IGMP filtering to interface

Networking requirements

Enable IGMP filtering on the device, and restrict multicast users by adding filtering rules to the interface.

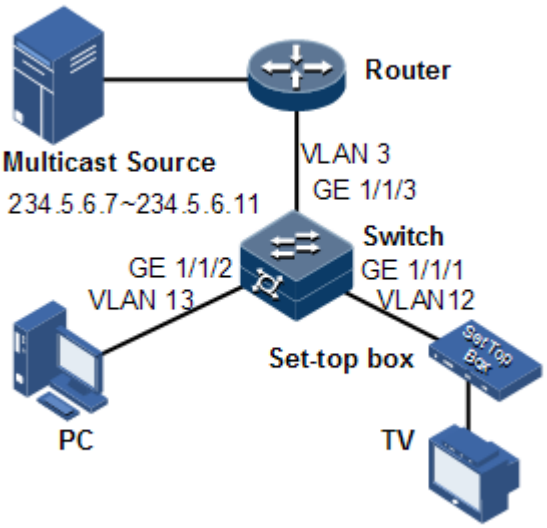
As shown in Figure 13-2, create the IGMP filter rule Profile 1, set the multicast group address range from 234.5.6.7 to 234.5.6.10 and the action to pass. Apply filtering rules to interface 1/1/1. The STBs can join the 234.5.6.7 multicast group, but cannot join the 234.5.6.11 multicast group. Interface 1/1/2 does not use the filtering rules. PCs can join the 234.5. 6.11 multicast group.

Set the maximum group limit on interface 1/1/1. After the STB joins 234.5.6.7 and then joins 234.5.6.8, it will exit the previous 234.5.6.7 multicast group.

As shown in Figure 13-2, IGMP MVR can be used to provide multicast services.

Copyright © Raisecom Technology Co., Ltd.

Figure 13-2 Applying IGMP filtering to the interface



Configuration steps

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

```
Raisecom#config
Raisecom(config)#create vlan 3,12,13 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan 12
Raisecom(config-gigaethernet1/1/1)#switchport trunk untagged vlan 3
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#switchport trunk native vlan 13
Raisecom(config-gigaethernet1/1/2)#switchport trunk untagged vlan 3
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#switchport mode trunk
Raisecom(config-gigaethernet1/1/3)#switchport trunk native vlan 3
Raisecom(config-gigaethernet1/1/3)#switchport trunk untagged vlan 12,13
Raisecom(config-gigaethernet1/1/3)#exit
```

Step 2 Configure the IGMP MVR.

```
Raisecom(config)#igmp mvr
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#igmp mvr
Raisecom(config-gigaethernet1/1/1)#igmp mvr user-vlan 12
Raisecom(config-gigaethernet1/1/1)#exit
```


Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#igmp mvr
Raisecom(config-gigaethernet1/1/2)#igmp mvr user-vlan 13
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#igmp mvr mcast-vlan 3 group any
```

Step 3 Configure the IGMP filtering template.

```
Raisecom(config)#igmp filter profile 1
Raisecom(config-igmp-profile)#permit
Raisecom(config-igmp-profile)#range 1 234.5.6.7 234.5.6.10
Raisecom(config-igmp-profile)#exit
```

Step 4 Apply the IGMP filtering template to the STB.

```
Raisecom(config)#igmp filter
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#igmp filter profile 1
```

Step 5 Configure the maximum number of groups on the STB.

```
Raisecom(config-gigaethernet1/1/1)#igmp filter max-groups 1
Raisecom(config-gigaethernet1/1/1)#igmp filter max-groups action replace
```

Checking results

Check whether the filtering configurations applied to the interface are correct.

```
Raisecom#show igmp filter gigaethernet 1/1/1
igmp profile:  1
max group:      1
current group:  0
action:       replace
```

13.6.2 Example for configuring IGMP MVR

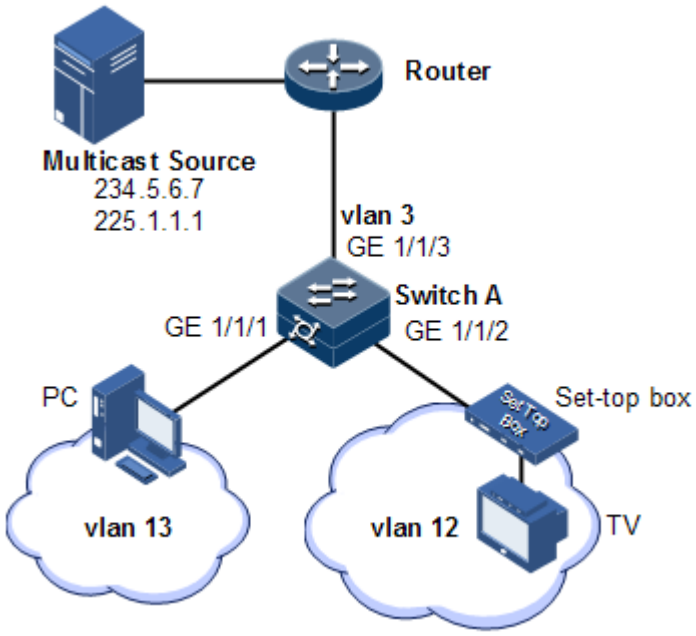
Networking requirements

As shown in Figure 13-3, GE 1/1/3 of Switch A is connected to a multicast router, interfaces 1/1/1 and 1/1/2 are connected to users in different VLANs, so that users can receive multicast data 234.5.6.7 and 225.1.1.1.

Copyright © Raisecom Technology Co., Ltd.

Configure IGMP MVR on Switch A and specify VLAN 3 as the multicast VLAN. In this way, the multicast data does not need to be copied in each user VLAN, but only in the multicast VLAN, which saves bandwidth.

Figure 13-3 IGMP MVR networking



Configuration steps

Step 1 Create a VLAN on Switch A and add the interface to the VLAN.

```
Raisecom#config
Raisecom(config)#create vlan 3,12,13 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan 13
Raisecom(config-gigaethernet1/1/1)#switchport trunk untagged vlan 12
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#switchport trunk native vlan 12
Raisecom(config-gigaethernet1/1/2)#switchport trunk untagged vlan 13
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#switchport mode trunk
Raisecom(config-gigaethernet1/1/3)#switchport trunk native vlan 3
Raisecom(config-gigaethernet1/1/3)#switchport trunk untagged vlan 12,13
Raisecom(config-gigaethernet1/1/3)#exit
```

Step 2 Configure IGMP MVR on Switch A.

Copyright © Raisecom Technology Co., Ltd.

```
Raisecom(config)#igmp mvr
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#igmp mvr
Raisecom(config-gigaethernet1/1/1)#igmp mvr user-vlan 13
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#igmp mvr
Raisecom(config-gigaethernet1/1/2)#igmp mvr user-vlan 12
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#igmp mvr mcast-vlan 3 group 234.5.6.7
Raisecom(config)#igmp mvr mcast-vlan 3 group 225.1.1.1
```

Checking results

Check whether IGMP MVR configurations on Switch A are correct.

```
Raisecom#show igmp mvr
igmp mvr running             :Enable
igmp mvr port               :1/1/1 1/1/2
igmp mvr multicast vlan(ref)   :3(2)
igmp aging time(s)           :260
```

Check whether the multicast VLAN and group address of Switch A are correct.

```
Raisecom#show igmp mvr vlan-group
Mcast-vlan     Start-group    End-group
-----------------------------------------
3            225.1.1.1      225.1.1.1
3            234.5.6.7      234.5.6.7
```


Copyright © Raisecom Technology Co., Ltd.

14 OAM

This chapter describes principles and configuration procedures of OAM, as well as related configuration examples, including following sections:

- Configuring EFM
- Configuring CFM
- Configuring BFD
- Configuring SLA
- Configuring MPLS-TP OAM
- Configuring RFC2544
- Configuring Y.1564
- Configuring SLA test alarm
- Configuring interface loopback
- Configuring smart probe
- Configuring ULDP
- Configuring Traceroute
- Configuring PING
- Maintenance

14.1 Configuring EFM

14.1.1 Preparing for configurations

Scenario

Deploying EFM between directly-connected devices can effectively improve the management and maintenance capability of Ethernet links and ensure network running smoothly.

Prerequisite

Connect interfaces and configure physical parameters of interfaces. Make the physical layer Up.

Copyright © Raisecom Technology Co., Ltd.

14.1.2 Configuring EFM basic functions

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**oam send-period** *period-ms* **timeout** *seconds*	(Optional) configure the OAM PDU delivery period and timeout. By default, the OAM PDU delivery time is 1s (the *period-ms* is 10, 10 × 100ms = 1s) and the timeout is 5s.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 2 or 3 physical interface configuration mode.
4	Raisecom(config-port)#oam { **active** | **passive** }	Configure the working mode of EFM. By default, it is passive.
5	Raisecom(config-port)#**oam enable**	Enable EFM OAM of the link. By default, it is disabled.

14.1.3 Configuring EFM active functions

Note

EFM active functions can be configured when the RAX721 is in active mode.

(Optional) configuring RAX721 to initiate EFM remote loopback

Note

- You can discover network faults in time by periodically detecting loopbacks. By detecting loopbacks in segments, you can locate exact areas where faults occur and you can troubleshoot these faults.
- When a link is in the loopback status, the RAX721 returns all packets but OAM packets received by the link to the peer. At this time, the user data packet cannot be forwarded properly. Therefore, disable this function immediately when detection is not required.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**oam remote-loopback**	Enable the interface to initiate remote loopback.
4	Raisecom(config-port)#**oam loopback timeout** *time*	(Optional) configure the timeout for the interface to initiate remote loopback. By default, it is 3s.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config-port)#**oam loopback retry** *times*	(Optional) configure the retry times for the interface to initiate remote loopback. By default, it is 2 times.

(Optional) viewing current variable values of peer device

Note

By getting the current variable values of the peer, you can get current link status. IEEE 802.3 Clause 30 defines and explains supported variables and their denotation gotten by OAM in details. The variable takes Object as the maximum unit. Each object contains Package and Attribute. A package contains several attributes. Attribute is the minimum unit of a variable. When an OAM variable is obtained, object, package, branch, and leaf description of attributes are defined by Clause 30 to describe requesting object, and the branch and leaf are followed by variable to denote object responds variable request. The RAX721 supports getting OAM information and interface statistics.
Peer variable cannot be obtained unless EFM connection is established.

Step	Command	Description
1	Raisecom#**show oam peer oam-info** [**gigaethernet** *interface-number*]	Show OAM basic information about the peer device.
	Raisecom#**show oam peer** [*interface-type interface-number*]	

14.1.4 Configuring EFM passive functions

Note

The passive functions of EFM can be configured regardless of the RAX721 is in active or passive mode.

(Optional) configuring RAX721 to respond to EFM remote loopback

Note

The peer EFM remote loopback will not take effect until the remote loopback response is configured on the local device.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *interface-number*	Enter GE interface configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**oam loopback** { **ignore** | **process** }	Configure the interface to ignore/respond to EFM remote loopback sent by the peer device. By default, the Layer 2 physical interface ignores EFM remote loopback.

14.1.5 Configuring link monitoring and fault indication

(Optional) configuring OAM link monitoring

OAM link monitoring is used to detect and report link errors in different conditions. When detecting a fault on a link, the RAX721 provides the peer with the generated time, window, and threshold, etc. by OAM event notification packets. The peer receives event notification and reports it to the network management system through SNMP Trap. Besides, the local device can directly report events to the network management system through SNMP Trap.
By default, the system sets default value for error generated time, window, and threshold.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *interface-number*	Enter GE interface configuration mode.
3	Raisecom(config-port)#**oam errored-frame window** *framewindow* **threshold** *framethreshold*	Configure the monitor window and threshold for an error frame event. By default, the monitor window is 1s and the threshold is 1 error frame.
4	Raisecom(config-port)#**oam errored-frame-period window** *frameperiodwindow* **threshold** *frameperiodthreshold*	Configure the monitor window and threshold for an error frame period event. By default, the monitor window is 1000ms and the threshold is 1 error frame.
5	Raisecom(config-port)#**oam errored-frame-seconds window** *framesecswindow* **threshold** *framesecsthreshold*	Configure the monitor window and threshold for an error frame seconds event. By default, the monitor window is 60s and the threshold is 1s.
6	Raisecom(config-port)#**oam errored-symbol-period window** *symperiodwindow* **threshold** *symperiodthreshold*	Configure the monitor window and threshold for an error symbol event. By default, the monitor window is 1s and the threshold is 1 error frame.

Copyright © Raisecom Technology Co., Ltd.

(Optional) configuring OAM fault indication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *interface-number*	Enter GE interface configuration mode.
3	Raisecom(config-port)#**oam notify** { **critical-event** | **dying-gasp** | **errored-frame** | **errored-frame-period** | **errored-frame-seconds** | **errored-symbol-period** } **enable**	Enable OAM notification of fault information and OAM link events. By default, OAM notification of all links is enabled.
4	Raisecom(config-port)#**oam event trap enable**	Enable OAM Trap of local OAM link events and fault events. By default, it is enabled.
5	Raisecom(config-port)#**oam peer event trap** { **enable** | **disable** }	Enable OAM Trap of peer OAM link events. By default, it is enabled.

14.1.6 Checking configurations

No.	Command	Description
1	Raisecom#**show oam** [*interface-type interface-number*]	Show configurations of OAM basic functions.
2	Raisecom#**show oam event** [*interface-type interface-number*] [**critical**]	Show local OAM link events.
3	Raisecom#**show oam loopback** [*interface-type interface-number*]	Show OAM remote loopback configurations.
4	Raisecom#**show oam notify** [*interface-type interface-number*]	Show OAM notification configurations.
5	Raisecom#**show oam peer event** [*interface-type interface-number*] [**critical**]	Show information about OAM peer events.
6	Raisecom#**show oam peer link-statistic** [*interface-type interface-number*]	Show peer OAM link statistics.
7	Raisecom#**show oam statistics** [*interface-type interface-number*]	Show OAM statistics.
8	Raisecom#**show oam trap** [*interface-type interface-number*]	Show OAM Trap information.

Copyright © Raisecom Technology Co., Ltd.

14.2 Configuring CFM

14.2.1 Preparing for configurations

Scenario

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

CFM can provide following OAM functions:

- Fault detection (Continuity Check, CC)
- Fault acknowledgement (LoopBack, LB)
- Fault location (LinkTrace, LT)
- Alarm Indication Signal (AIS)
- Client Signal Fail (CSF)

Prerequisite

- Connect interfaces and configure physical parameters of the interfaces. Make the physical layer Up.
- Create a VLAN.
- Add interfaces to the VLAN.

14.2.2 Enabling CFM

Note

- CFM fault detection and CFM fault location functions cannot take effect until the CFM is enabled.
- To enable CFM on an interface, you need to enable global CFM in global configuration mode and then enable CFM on the interface.
- When global CFM is disabled, interface CFM does not take effect.
- Ethernet LM cannot take effect unless CFM is enabled on the ingress interface of the service packet and MEP-related interfaces.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ethernet cfm enable`	Enable global CFM. By default, it is enabled.
3	`Raisecom(config)#interface gigaethernet` *`interface-number`*	Enter interface configuration mode.
	`Raisecom(config-port)#portswitch`	Switch the interface to L2 switching mode.
	`Raisecom(config-port)#mode l2`	Bind the interface with L2VPN. You need to configure this command for simulated Ethernet services.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-port)#**ethernet cfm enable**	Enable CFM on the interface. By default, it is disabled.

14.2.3 Configuring CFM basic functions

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet cfm domain** [**md-name** *domain-name*] **level** *md-level*	Create a MD. • If a MD name is assigned by the **md-name** parameter, it indicates that the MD is in 802.1ag style. And all MAs and CCMs in the MD are in 802.1ag style. • If a MD name is not assigned, the MD is in Y.1731 style and all MAs and CCMs in the MD are in Y.1731 style. • If the MD name is specified, it must be globally unique. • Levels of different MDs must be different.
3	Raisecom(config)#**service** *instance-name* **level** *md-level*	Create a service instance and enter service instance configuration mode.
4	Raisecom(config-service)#**service vlan-list** *vlan-list* [**primary** *vlan-id*]	(Optional) configure the VLAN related to the MA.
5	Raisecom(config-service)#**service mep** [**up** | **down**] **mpid** *mep-id interface-type interface-number* [**priority** *value*]	(Optional) configure the MEP based on service instance. Before configuring MEP, relating the service instance to the VLAN.
6	Raisecom(config-service)#**service remote-mep** *mep-list interface-type interface-number*	(Optional) add static remote MEP of the service instance manually. **Note** You need to manually add the static remote MEP and specify the interface. It fails to find the remote MEP automatically.
7	Raisecom(config-service)#**service tunnel tunnel** *interface-number* [**send** | **received**]	(Optional) configure OAM of the tunnel type.

Copyright © Raisecom Technology Co., Ltd.

14.2.4 Configuring fault detection

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet cfm errors archive-hold-time** *minutes*	(Optional) configure the archive-hold time of error CCMs. By default, it is 100min.
3	Raisecom(config)#**service** *instance-nameinstance-name* **level** *md-level*	Enter service instance configuration mode.
4	Raisecom(config-service)#**service cc interval** { **3ms** | **10ms** | **100ms** | **1** | **10** | **60** | **600** }	(Optional) configure the delivery period of CCMs.
5	Raisecom(config-service)#**service cvlan** *vlan-id*	(Optional) configure the CVLAN of the MA.
6	Raisecom(config-service)#**service priority** *priority*	(Optional) configure the priority of CFM OAM packets. By default, the priority is 7.
7	Raisecom(config-service)#**service cc enable mep** { *mep-list* | **all** }	(Optional) enable the MEP to send CCM packets.

14.2.5 Configuring fault acknowledgement

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service** *instance-name* **level** *md-level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**ping** *mac-address* [**count** *count-number*] [**size** *size*] [**source** *mep-id*] [**interval** *time*] [**timeout** *time*] [**padding** { **null** | **null-crc** | **prbs** | **prbs-crc** }] [**cos** *cos-value*] [**non-drop**] Raisecom(config-service)#**ping mep** *mep-id* [**count** *count-number*] [**size** *size*] [**source** *mep-id*] [**interval** *time*] [**timeout** *time*] [**padding** { **null** | **null-crc** | **prbs** | **prbs-crc** }] [**cos** *cos-value*] [**non-drop**]	Perform Layer 2 Ping for acknowledging faults. By default, 3 LBMs are sent. The TLV length of a packet is 64. The RAX721 automatically looks for an available source MEP.
4	Raisecom(config-service)#**ping ethernet multicast** [**cos** *cos-value*] [**non-drop**] [**size** *size*] [**timeout** *time*] [**padding** { **null** | **null-crc** | **prbs** | **prbs-crc** }]	Perform Layer 2 multicast Ping for acknowledging faults.

Copyright © Raisecom Technology Co., Ltd.

Note

- Before executing this command, ensure that global CFM is enabled. Otherwise, the Ping operation fails.
- If there is no MEP in a service instance, the Ping operation will fail because of failing to find source MEP.
- The Ping operation will fail if the specified source MEP is invalid. For example, the specified source MEP does not exist or CFM is disabled on the interface where the specified source MEP is.
- The Ping operation will fail if the Ping operation is performed based on specified destination MEP ID and the MAC address of destination is not found based on MEP ID.
- The Ping operation will fail if other users are using the specified source MEP to perform the Ping operation.
- If the service instance associates with the emulated Ethernet PW, when LB is performed, you need to enable global CFM and Ethernet CFM on the AC-side interface.

14.2.6 Configuring fault location

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#service` *instance-name* `level` *md-level*	Enter service instance configuration mode.
3	`Raisecom(config-service)#traceroute` *mac-address* [`ttl` *ttl*] [`source` *mep-id*] [`size` *size-value*] `Raisecom(config-service)#traceroute mep` *mep-id* [`ttl` *ttl*] [`source` *mep-id*] [`size` *size-value*]	Perform Layer 2 Traceroute for locating faults. By default, the TLV length of a packet is 64. The RAX721 automatically looks for an available source MEP.
4	`Raisecom(config)#ethernet cfm traceroute cache enable`	(Optional) enable LinkTrace cache. When LinkTrace cache is enabled, you can use the **show ethernet cfm traceroute cache** command to learn the routes discovered through the cache storage protocol. When LinkTrace cache is disabled, the result will be automatically erased by the **traceroute** command. By default, LinkTrace cache is disabled.
5	`Raisecom(config)#ethernet cfm traceroute cache` { `hold-time` *minute* | `size` *size* }	(Optional) configure the hold time of data in the LinkTrace cache and LinkTrace cache size. By default, the hold time is 100min and the LinkTrace cache size is 100.

Note

- Before executing this command, ensure that global CFM is enabled. Otherwise, the Traceroute operation fails.

Copyright © Raisecom Technology Co., Ltd.

- If there is no MEP in a service instance, the Traceroute operation will fail because of failing to find source MEP.
- The Traceroute operation will fail if the specified source MEP is invalid. For example, the specified source MEP does not exist or CFM is disabled on the interface where the specified source MEP is.
- The Traceroute operation will fail if the Ping operation is performed based on specified destination MEP ID and the MAC address of destination is not found based on MEP ID.
- If the CC feature is invalid, you can ensure Layer 2 Traceroute operation works normally by configuring static RMEP and specifying MAC address.
- The Traceroute operation will fail if other users are using the specified source MEP to perform the Traceroute operation.

14.2.7 Configuring Ethernet signal lock

Configure the server device as below:

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service** *cis-id* **level** *level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**service lck start mep** { *mep-id* | **all** }	Enable LCK packet sending. By default, it is not enabled.
4	Raisecom(config-service)#**service lck period** { **1** | **60** }	Configure the interval for sending LCK packets. By default, it is 1s.
5	Raisecom(config-service)#**service lck level** *level* [**vlan** v*lan-id*]	Configure the level of the client MD to which LCK is sent.

Configure the client device as below:

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service** *cis-id* **level** *level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**service suppress-alarms enable mep** { *mep-id* | **all** }	Enable alarm suppression. By default, it is enabled.

14.2.8 Configuring AIS

- Configure AIS on server devices.

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**ethernet cfm domain** [**md-name** *domain-name*] **level** *md-level*	Create a MD. **Note** When creating a high-level MA, you need to bind it with a vlan-list.
3	Raisecom(config)#**service** *instance-name* **level** *md-level*	Enter service instance configuration mode.
4	Raisecom(config-service)#**service ais level** *md-level*	Configure the level of the MD to which AIS is sent. **Note** The MD level must be higher than the service instance level.
5	Raisecom(config-service)#**service ais period** { **1** | **60** }	(Optional) configure the AIS delivery period. By default, the AIS delivery period is 1s.
6	Raisecom(config-service)#**service ais enable**	Enable AIS delivery. By default, AIS delivery is disabled.

- Configure AIS on client devices. Before configuring AIS, you need to configure MEP. For detailed configuration steps, see section 14.2.3 Configuring CFM basic functions.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet cfm domain** [**md-name** *domain-name*] **level** *md-level*	Create a MD.
3	Raisecom(config)#**service** *instance-name* **level** *md-level*	Enter service instance configuration mode.
4	Raisecom(config-service)#**service suppress-alarms enable mep** { *mep-list* | **all** }	Enable alarm inhibition. By default, alarm inhibition is enabled.

14.2.9 Configuring CSF

Configure LCK on server devices.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service** *instance-name* **level** *md-level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**service csf period** { **1** | **60** }	(Optional) configure the CSF packet delivery period. By default, the CSF packet delivery period is 1s.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-service)#**service csf enable mpid** *mep-id*	Enable the MEP to send the LCK packet.
5	Raisecom(config-service)#**service csf trap enable**	(Optional) enable CSF Trap.

14.2.10 Configuring LM statistics

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**service** *cis-id* **level** *level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**service lm-statistic priority-based enable**	Configure packet loss statistics based on priority. By default, it is enabled.

14.2.11 Configuring performance monitoring

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**service** *csi-id* **level** *ma-level*	Enter MA configuration mode.
3	Raisecom(config-service)#**service pm enable mep** { **all** | *mep-id* }	Enable MEP performance statistics.

14.2.12 Checking configurations

No.	Command	Description
1	Raisecom#**show cfm csf**	Show CSF information.
2	Raisecom#**show ethernet cfm**	Show CFM global configurations.
3	Raisecom#**show ethernet cfm full-detail**	Show CFM details globally.
4	Raisecom#**show ethernet cfm ais** [**level** *md-level*] [*source*]	Show AIS information. **Note** 802.1ag MDs do not support AIS.
5	Raisecom#**show ethernet cfm domain** [**level** *md-level*]	Show MD configurations.
6	Raisecom#**show ethernet cfm errors** [**level** *md-level*]	Show error CCM information.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
7	Raisecom#**show ethernet cfm lck** [**level** *md-level*] [**source**]	Show LCK information. **Note** The 802.1ag MDs do not support LCK.
8	Raisecom#**show ethernet cfm local-mp** [**interface** *interface-type interface-number*] Raisecom#**show ethernet cfm local-mp** [**level** *md-level*]	Show local MEP configurations.
9	Raisecom#**show ethernet cfm remote-mep** [**level** *md-level* [**service** *instance-name* [**mpid** *mep-id*]]]	Show remote MEP configurations.
10	Raisecom#**show ethernet cfm remote-mep static** [**level** *md-level*]	Show remote static MEP configurations.
11	Raisecom#**show ethernet cfm traceroute-cache**	Show information about routes in the LinkTrace cache.
12	Raisecom#**show ethernet cfm suppress-alarms**	Show CFM alarm suppression.
13	Raisecom#**show cfm lm ccm statistics**	Show CFM LM statistics.
14	Raisecom#**show cfm pm status**	Show status of performance statistics.

14.3 Configuring BFD

14.3.1 Preparing for configurations

Scenario

To reduce effect of faults on the device and improve network availability, the RAX721 needs to detect communication faults with adjacent devices. Therefore, it can take actions immediately to ensure service being transmitted properly.

BFD is a one-way detection. Therefore, both the local device and the peer device should be enabled with BFD. Otherwise, detection will fail.

Prerequisite

The DUT is configured with an IP address and routes between all devices are available.

14.3.2 Configuring BFD for IPv4

Creating BFD for IPv4 sessions

When you create the BFD binding:

Copyright © Raisecom Technology Co., Ltd.

- It indicates detecting multi-hop routes if you only specify the peer IP address.
- It indicates detecting the single-hop route if you specify both the local interface and the peer IP address, which refers to detecting the fixed route with the local interface as the egress interface and the peer IP address as the next-hop address.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**bfd** *session-id* **bind peer-ip** *ip-address* [**source-ip** *ip-address*]	Create multi-hop routes of BFD and enter BFD session mode. You must configure the source IP address when creating a multi-hop session.
3	Raisecom(config)#**bfd passive-create enable**	Enable passive creation of BFD sessions.

Configuring BFD session parameters

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**bfd** *session-id*	Enter BFD session mode. **Note** You cannot use this command to enter BFD session mode unless you create the BFD and bind the related path.
3	Raisecom(config-bfd-session)#**description** *description*	Configure descriptions of the BFD session.
4	Raisecom(config-bfd-session)#**local discriminator** *value*	(Optional) configure the local identifier of the BFD session. By default, the local identifier is displayed as 0, which indicates that no local identifier is configured. **Note** You need to configure this parameter for static BFD only. It is automatically generated by the system if not configured.
5	Raisecom(config-bfd-session)#**min send-interval** *interval*	Configure the minimum delivery interval of the BFD session. By default, it is 3ms.
6	Raisecom(config-bfd-session)#**min receive-interval** *interval*	Configure the minimum receiving interval of the BFD session. By default, it is 3ms.
7	Raisecom(config-bfd-session)#**detect-multiplier** *multiplier*	Configure the local detection times of the BFD session. By default, it is 3 times.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
8	Raisecom(config-bfd-session)#**remote discriminator** *value*	(Optional) configure the remote identifier of the BFD session. By default, the remote identifier is displayed as 0, which indicates that no remote identifier is configured. **Note** You need to configure this parameter for static BFD only. It is automatically generated by the system if not configured.
9	Raisecom(config-bfd-session)#**session enable** Raisecom(config-bfd-session)#**exit**	Enable BFD session. By default, it is disabled.
10	Raisecom(config)#**bfd** [**send-interval** *interval-value*] [**receive-interval** *interval-value*] [**detect-multiplier** *multiplier-value*]*	Configure the sending interval, receiving interval, and detection multiplier of dynamic BFD sessions.

14.3.3 Configuring BFD for PW

Creating BFD for PW sessions

After completing PW related configurations, you can configure PFD-based BFD. Create dynamic or semi-dynamic BFD for PW according to the following steps:

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**bfd** *session-id* **bind pw** *vc-id peer-address* [**pw-ttl** *ttl*]	Create a BFD for PW and enter BFD session configuration mode..

Configuring BFD session parameters

See section Configuring BFD session parameters in 14.3.2 Configuring BFD for IPv4.

Configuring full dynamic BFD for PW

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**mode l2**	Enter L2VPN configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-port)#**mpls l2vpn pw bfd** [**min-tx-interval** *tx-interval*] [**min-rx-interval** *rx-interval*] [**detect-multiplier** *multiplier*] [**backup**]	Configure PW-based full dynamic BFD.

14.3.4 Configuring BFD for VRF

Creating BFD for VRF

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**bfd** *session-id* **bind peer-ip** *ip-address* **vrf-name** *vrf-name* **interface** *interface-type interface-number* **source-ip** *ip-address*	Create single-hop BFD for IPv4 VRF and enter BFD session mode.
3	Raisecom(config)# **bfd** *session-id* **bind peer-ip** *ip-address* **vrf-name** *vrf-name* [**source-ip** *ip-address*]	Create multi-hop BFD for IPv4 VRF and enter BFD session mode.

Configuring BFD session parameters

See section Configuring BFD session parameters in 14.3.2 Configuring BFD for IPv4.

14.3.5 Configuring BFD for LAG member interfaces

Two devices are connected through a Layer 3 Ethernet LAG link, and the Ethernet LAG interface has multiple member interfaces. If BFD single hop session is bound width Ethernet LAG interfaces for link detection, the BFD single hop session randomly selects a member link. When the member interface fails (including link failure and interface failure), it will be considered that the entire Ethernet LAG is faulty; however, at this time, the Ethernet LAG link status may still be normal. To solve these problems, you can configure BFD for Link bundle sessions, which create a BFD sub-session for each member interface of Ethernet LAG for detection. Only when the status of all BFD sub-sessions is Down, the status of BFD for Link bundle sessions will be Down.

This command can be used to configure IPv4 LAG member interface detection.

Creating BFD for LAG member interface sessions

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**bfd** *session-id* **bind link-bundle peer-ip** *ip-address* [**vrf-name** *vrf-name*] **interface port-channel** *channel-number* [**source-ip** *ip-address*]	Create a single-hop BFD IPv4 LAG member interface, and enter BFD session configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config)#**bfd** *session-id* **bind link-bundle peer-ip default-ip interface port-channel** *channel-number*	

Configuring BFD session parameters

See section Configuring BFD session parameters in section 14.3.2 Configuring BFD for IPv4.

14.3.6 Configuring BFD Trap

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**bfd trap enable**	Enable BFD Trap. By default, BFD Trap is enabled.

14.3.7 Configuring SBFD

Seamless Bidirectional Forwarding Detection (SBFD) is used to detect peer operability in the SR scenario.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**sbfd destination peer-ip** *ipv4-address* **remote-discriminator** *value*	Configure the destination address and remote discriminator of SBFD.
3	Raisecom(config)#**sbfd destination peer-ipv6** *ipv6-address* **remote-discriminator** *value*	Configure the destination address (endpoint address for SRv6) and remote discriminator of SBFD for SRv6-TE Policy.
4	Raisecom(config)#**sbfd srv6-te-policy endpoint** *ipv6-address* **color** *value*	Configure the destination address (endpoint address for SRv6) and remote discriminator of SBFD and the color of the policy for SRv6-TE Policy.
5	Raisecom(config)#**sbfd reflector discriminator** { *value* | *ipv4-address* }	Configure the reflector discriminator of SBFD for the SBFD reflector.

14.3.8 Checking configurations

No.	Command	Description
1	Raisecom#**show bfd**	Show BFD global configurations.
2	Raisecom#**show bfd** *session-id* **config**	Show configurations about the specified BFD session.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
3	Raisecom#**show bfd** *session-id* **state**	Show status about the specified BFD session.
4	Raisecom#**show bfd** *session-id* **statistics**	Show statistics about the specified BFD session.
5	Raisecom#**show bfd** [*session-id*] **diagnostic-code**	Show the diagnostic code of BFD session.
6	Raisecom#**show mpls l2vpn pw bfd configuration**	Show PW BFD configurations.

14.4 Configuring SLA

14.4.1 Preparing for configurations

Scenario

To provide users with qualified network services, the carrier signs a SLA with users. To carry out SLA effectively, the ISP needs to deploy SLA feature on devices to measure the network performance, taking the measured results as an evidence for ensuring the network performance.

By selecting two detection points (source and destination devices), SLA configures and schedules SLA operations on a detection point. Therefore, network performance between these 2 detection points can be detected.

SLA takes statistics on round-trip packet loss ratio, round-trip/unidirectional (SD/DS) delay, jitter, throughput, and LM packet loss ratio test. In addition, it reports these data to the upper monitoring software (such as the network management system) to help analyze network performance for obtaining an expected result.

Note

When configuring SLA on the RAX721, note the following matters:

- The maximum number of operations allowed to be configured and concurrently scheduled is 128 (DM) + 128 (LM).
- Before scheduling a Y.1731 SLA operation, establish the CFM environment.
- Do not modify the scheduling information or re-schedule the SLA operation if the current scheduling does not stop.

Prerequisite

When you configure Layer 2 tests, deploy CFM between local and remote devices that need to be detected. Layer 2 Ping operation succeeds between local and remote devices.

Copyright © Raisecom Technology Co., Ltd.

14.4.2 Configuring Y.1731-based SLA

Configuring SLA delay test

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **y1731 latency remote-mep** *mep-id* **level** *level* **svlan** *vlan-id* [**cvlan** *cvlan-id*] [**cos** *cos-value*] [**interval** *interval-num*] [**size** *size-value*] **dm**	Configure Y1731 two-way delay or one-way delay test operations according to the destination MEP number. Configuring the one-way time delay requires that the test operation numbers created at both ends are the same.
3	Raisecom(config)#**sla** *oper-num* **y1731 latency remote-mac** *mac-address* **level** *level* **svlan** *vlan-id* [**cvlan** *cvlan-id*] [**cos** *cos-value*] [**interval** *interval-num*] [**size** *size-value*] **dm**	Configure the Y1731-delay test based on destination MAC address.
4	Raisecom(config)#**sla** *oper-num* **mpls-y1731 latency level** *level* **tunnel** *tunnel-number* [**interval** *period*] [**tc** *tc*] [**size** *size*]	Configure the Y.1731 delay test operation of the tunnel.

Configuring SLA packet loss test

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)# **sla** *oper-num* **y1731 pkt-loss remote-mep** *mep-id* **level** *level* **svlan** *vlan-id* [**cvlan** *cvlan-id*] [**cos** *cos-value*] { [**dlm**] | [**interval** *interval-num*] }	Configure the Y1731 packet loss test operation according to the destination MEP number.
3	Raisecom(config)#**sla** *oper-num* **y1731 pkt-loss remote-mac** *mac-address* **level** *level* **svlan** *vlan-id* [**cvlan** *cvlan-id*] [**cos** *cos-value*] { [**dlm**] | [**interval** *interval-num*] }	Configure the Y1731 packet loss test operation according to the destination MAC address.
4	Raisecom(config)#**sla** *oper-num* **mpls-y1731 pkt-loss level** *level* **tunnel** *tunnel-number* [**tc** *tc*] [**interval** *period*]	Configure the Y.1731 packet loss rate test operation of the tunnel.

14.4.3 Configuring SLA operation scheduling

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla schedule** { *oper-num* | **all** } [**life** { **forever** | *life-time* }] [**period** *second*]	Configure SLA scheduling information, including the lifetime period and executive interval, and enable SLA operation scheduling. By default, SLA operation scheduling is disabled.

Copyright © Raisecom Technology Co., Ltd.

The operation lifetime should not be shorter than the interval for scheduling the SLA operation.

14.4.4 Configuring SLA archive

After SLA archiving is enabled, the device will periodically (5 minutes) upload the performance data to the network management system via FTP. The performance data includes delay, jitter, packet loss rate, and availability indicators.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla archive upload**{ **enable** | **disable** }	Configure SLA archiving. By default, it is disabled.
3	Raisecom(config)#**sla** *oper-num* **report enable**	Configure SLA reporting.
4	Raisecom(config)#**sla** *oper-num* **archive enable**	Configure SLA archive.

14.4.5 Configuring iOAM

The in-band Operation, Administration, and Maintenance (iOAM) is to encapsulate OAM information to be carried and data into user data packets and send these packets with OAM information, without sending OAM information through the control plane packets.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **ioam** { **enable** | **disable** }	Enable iOAM in the egress direction. By default, it is disabled.
3	Raisecom(config)#**sla ioam device-id** *id*	Configure the device ID of the iOAM operation.
4	Raisecom(config)#**sla** *oper-num* **ioam interface** *interface-type interface-number* { **evpn-evpl** | **evpn-vpls** } *evpn-instance-value* **dest-mac** *mac-address* [**svlan** *vlan-id*] [**cos** *cos*] [**measure-mode** { **e2e** | **trace** }] [**interval** { **1s** | **10s** | **30s** | **60s** | **300s** }] [**disorder-measure enable**]	(Optional) configure the SLA operation of the iOAM type based on L2VPN.
5	Raisecom(config)#**sla** *oper-num* **ioam interface** *interface-type interface-number* **vrf** *vrf-name* **dest-ip** *ip-address* **source-ip** *ip-address* [**protocol** { **tcp** | **udp** | *protocol-id* }] [**dest-port** *port-number*] [**source-port** *port-number*] [**nexthop** *ip-address*] [**measure-mode** { **e2e** | **trace** }] [**interval** { **1s** | **10s** | **30s** | **60s** | **300s** }] [**disorder-measure enable**]	(Optional) configure the SLA operation of the iOAM type based on L3VPN.

Copyright © Raisecom Technology Co., Ltd.

14.4.6 Checking configurations

No.	Command	Description
1	`Raisecom#show sla`	Show SLA global information.
2	`Raisecom#show sla { all | oper-num } configuration`	Show information about SLA operation.
3	`Raisecom#show sla { all | oper-num } result { current-interval | current-period | history-period | latest-period | tests }`	Show test information about the operation.
4	`Raisecom#show sla { all | oper-num } threshold`	Show threshold alarms of operation scheduling.
5	`Raisecom#show sla { all | oper-num } ioam result`	Show the test result of the SLA operation of the iOAM type.

14.5 Configuring MPLS-TP OAM

14.5.1 Preparing for configurations

Scenario

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

CFM can provide following OAM functions based on the MPLS-TP network:

- Fault detection (Continuity Check, CC)
- Fault acknowledgement (LoopBack, LB)
- Fault location (LinkTrace, LT)
- Alarm Indication Signal (AIS)
- Client Signal Fail (CSF)
- Packet Delay and Packet Delay Variation Measurements (DM)
- Frame Loss Measurements (LM)

The implementation principle is similar to OAM based on Ethernet, but the ways for carrying related packets are different.

To ensure that users can enjoy a certain quality of network services, the carrier and customer will sign the Service Lever Agreement (SLA). To effectively fulfill SLA agreements, the carrier needs to deploy SLA features on devices to measure network performance, and use the measurement results as the basis for ensuring user performance.

Two checkpoints are selected to measure SLA features. One is configured with the SLA operations, which are scheduled and executed, so the network performance testing between two nodes is performed.

Copyright © Raisecom Technology Co., Ltd.

SLA calculates the round-trip packet loss rate, round-trip or one-way (SD/DS) delay, jitter, jitter variance, jitter distribution, and other data between two checkpoints, and notifies upper level monitoring software (such as network management software) of the data to analyze network performance and obtain the data that users want to see.

Prerequisites

- Connect interfaces and configure physical parameters of the interfaces. Make the physical layer Up.
- Configure basic functions of MPLS.
- Before configuring SLA, deploy CFM between the devices to be tested with network performance.

14.5.2 Enabling MPLS-TP CFM

By default, CFM is enabled.

14.5.3 Configuring MPLS-TP CFM

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp cfm domain level** *level*	Create an MPLS-TP MD.
3	Raisecom(config)#**mpls-tp service** *ma-name* **level** *ma-level*	Create a service instance, and enter service instance configuration mode.
4	Raisecom(config-service)#**service vc-id** *vc-id* **destination** *ip-address* [**ttl** *ttl*]	Configure the VC ID associated with the service instance.
5	Raisecom(config-service)#**service lsp** { **bidirection** *lsp-name* | **ingress** *lsp-in* **egress** *lsp-out* }	Configure the service instance to be associated with the specified ingress, egress, or bidirectional LSPs.
6	Raisecom(config-service)#**service lsp transit bidirection** *lsp-name* **lsr-id** *lsr-id* **ttl** *ttl* Raisecom(config-service)#**service lsp transit forward** *lsp-in* **backward** *lsp-out* **ttl** *ttl*	Create a service instance based on LSP subnet connection.
7	Raisecom(config-service)#**service mep** [**up** | **down**] **mpid** *mep-id*	Configure the MEP based on service instance.
8	Raisecom(config-service)#**service pw transit forward vc-id** *vc-id* **destination** *ip-address* **backward vc-id** *vc-id* **destination** *ip-address*	Configure the service instance to be associated with the subnet connection PW.
9	Raisecom(config-service)#**service section** { **dest-mac** *mac-address* | *interface-type interface-number* }	Configure the service instance to be associated with the section, and configure the destination MAC address of the section layer CC.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
10	Raisecom(config-service)#**service suppress-alarms enable mep** { **all** | *mep-list* }	Enable MEP alarm suppression.
11	Raisecom(config-service)#**service priority** *priority*	Configure the priority of CFM packets.
12	Raisecom(config-service)#**service remote-mep** *mep-list* [*interface-type interface-number*]	Create a static remote MEP.
13	Raisecom(config-service)#**service lm-response enable**	Enable service instance frame loss rate measurement response.

Before enabling CFM packet sending, configure the association between the service instance and static L2VC.

14.5.4 Configuring MPLS-TP fault detection

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp cfm remote mep age-time** *minutes*	(Optional) configure the aging time of the remote MEP. By default, the aging time of the remote MEP learned by the device is 100min.
3	Raisecom(config)#**mpls-tp cfm errors archive-hold-time** *minutes*	(Optional) configure the storage time for CC messages with configuration errors. By default, the storage time for error CC messages is 100min. When the system is configured with a new storage time, it will immediately check the data in the database. If any data exceeds the time limit, it will be cleared immediately.
4	Raisecom(config)#**mpls-tp service** *ma-name* **level** *ma-level*	Enter service instance configuration mode.
5	Raisecom(config-service)#**service cc enable mep** { *mep-list* | **all** }	Enable the MEP to send CC messages. By default, the MEP does not send CC messages.
6	Raisecom(config-service)#**service cc interval** { **3ms** | **10ms** | **100ms** | **1** | **10** | **60** | **600** }	(Optional) configure the interval for sending CC messages of the service instance. By default, it is 1s. After CC packet sending is enabled, the configuration of the interval for sending CC messages does not take effect.
7	Raisecom(config-service)#**service remote-mep learning active**	Enable/Disable remote MEP learning, which adds dynamically learnt remote MEPs to the static remote MEP list.

Copyright © Raisecom Technology Co., Ltd.

14.5.5 Configuring MPLS-TP fault acknowledgement

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp service** *ma-name* **level** *ma-level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**ping** { **ingress** | **egress** } **ttl** *ttl* [**count** *count-number*] [**size** *size*] [**source** *mep-id*] [**timeout** *time*] [**padding** { **null** | **null-crc** | **prbs** | **prbs-crc** }]	Execute the MPLS-TP layer Ping function for fault acknowledgement. By default, the number of LBM messages sent is 5, the TLV length of the messages is 64, and an available source MEP is automatically found.
	Raisecom(config-service)#**ping mep** *mep-id* [**ttl** *ttl*] [**count** *count-number*] [**size** *size*] [**source** *mep-id*] [**timeout** *time*] [**padding** { **null** | **null-crc** | **prbs** | **prbs-crc** }]	
	Raisecom(config-service)#**ping mip icc** *icc-code code-id* [**interface-num** *interface-number*] **ttl** *ttl* [**count** *count-number*] [**size** *size*] [**source** *mep-id*] [**timeout** *time*] [**padding** { **null** | **null-crc** | **prbs** | **prbs-crc** }]	

Note

- If there is no MEP in a service instance, the Ping operation will fail because of failing to find source MEP.
- The Ping operation will fail if the specified source MEP is invalid. For example, the specified source MEP does not exist or CFM is disabled on the interface where the specified source MEP is.
- The Ping operation will fail if other users are using the specified source MEP to perform the Ping operation.

14.5.6 Configuring MPLS-TP fault location

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp service** *ma-name* **level** *ma-level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**traceroute ttl** *ttl* [**interface-mode**] [**timeout** *time*]	Execute the MPLS-TP layer Traceroute function for fault location.
	Raisecom(config-service)#**traceroute mep** *mep-id* [**ttl** *ttl*] [**source** *mep-id*] [**interface-mode**] [**timeout** *time*]	
	Raisecom(config-service)#**traceroute mip icc** *icc-code code-id* [**ttl** *ttl*] [**interface-num** *interface-number*] [**timeout** *time*]	

Copyright © Raisecom Technology Co., Ltd.

- If there is no MEP in a service instance, the Traceroute operation will fail because of failing to find source MEP.
- The Traceroute operation will fail if the specified source MEP is invalid. For example, the specified source MEP does not exist or CFM is disabled on the interface where the specified source MEP is.
- The Traceroute operation will fail if other users are using the specified source MEP to perform the Traceroute operation.

14.5.7 Configuring MPLS-TP AIS

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp service** *ma-name* **level** *ma-level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**service ais** { **level** *md-level* [**vlan** *vlan-id*] | **period** { **1** | **60** } }	Configure the level and AIS sending period of the client layer MD to which AIS is sent. • The VLAN needs to be specified only when the AIS Level under PW service instance is configured, and is not required in other cases. • When the service instance is PW OAM and Ethernet OAM is configured at the specified Level, a VLAN must be specified when the command is executed, and the specified VLAN must be the primary VLAN of Ethernet OAM. By default, the sending period is 1s.
4	Raisecom(config-service)#**service ais enable**	Enable AIS sending. By default, it is disabled.
5	Raisecom(config-service)#**service suppress-alarms enable mep** { *mep-list* | **all** }	Enable alarm suppression. By default, it is enabled.

14.5.8 Configuring MPLS-TP CSF

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp service** *ma-name* **level** *ma-level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**service csf enable mpid** *mep-id*	Enable CSF packet sending. This is applicable to PW OAM only. By default, it is disabled.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-service)#**service csf period** { **1** | **60** }	Configure the period for sending CSF packets. This is applicable to PW OAM only. By default, it is 1s.
5	Raisecom(config-service)#**service csf trap enable**	Enable CSF Trap sending. This is applicable to PW OAM only. By default, it is disabled.

14.5.9 Configuring MPLS-TP LCK

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp service** *ma-name* **level** *ma-level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**service lck level** *md-level* [**vlan** *vlan-id*]	Configure the level of LCK sending. By default, it is the MIP level which is higher than MEP level. The period is 1s.
4	Raisecom(config-service)#**service lck period** { **1** | **60** }	Configure the period for sending LCK packets.
5	Raisecom(config-service)#**service lck start mep** { *mep-list* | **all** }	Enable the MEP to send LCK packets.
6	Raisecom(config-service)#**service suppress-alarms enable mep** { *mep-list* | **all** }	Enable alarm suppression. By default, it is enabled.

14.5.10 Configuring basic information about MPLS-TP SLA operations

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **mpls-y1731** [**latency | pkt-loss**] **level** *md-level* { **l2vc** *l2vc-id* **peer-address** *ip-address* | **lsp-ingress** *lspingress-name* **lsp-egress** *lspegress-name* | **section** *interface-type interface-number* } [**interval** *period*] [**packets** *packets-num*] [**tc** *tc*]	Configure the SLA MPLS-Y1731-Jitter operation.

Copyright © Raisecom Technology Co., Ltd.

14.5.11 Configuring SLA scheduling information and enabling operation scheduling

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla schedule** *oper-num* [**life forever** | **life** *life-time*] [**period** *period*]	Configure SLA scheduling information, and enable operation scheduling. By default, operation scheduling is disabled.

14.5.12 Configuring fault relay based on association of MPLS-TP OAM and BFD alarms

By configuring fault relay based on association of MPLS-TP OAM and BFD alarms, the fault at the AC side can be transmitted to the PW side in time, and the fault that occurs at the PW side can also be transmitted to the AC side in time. In this way, protection switching is triggered, the traffic of the active link can be switched to the standby link in time, and the normal operation of the network is ensured. If the AC side does not support MPLS-TP OAM and BFD, the fault at the PW side can be transmitted to the CE device through the port Down status of the PE device, triggering the active/standby link switching.

The networking scenario with interconnection of PTN and IPRAN also supports fault relay across multiple PW segments, allowing faults at the PTN side to be transmitted to the IPRAN side in time, and vice versa, the fault at the IPRAN side can also be transmitted to the PTN side, triggering protection switching.

By default, fault relay based on association of MPLS-TP OAM and BFD alarms is enabled. If other related fault relay functions need to be implemented, see the following configuration steps.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**mode l2**	Configure the VPN mode of the Layer 3 physical interface to L2VPN. By default, it is L3VPN.
4	Raisecom(config-port)#**l2vpn fault-action if-down**	(Optional) configure fault relay as interface Down when the AC side does not support MPLS-TP OAM and BFD. This configuration takes effect on the physical interface only, rather than sub-interfaces.
	Raisecom(config-port)#**exit**	Exit interface configuration mode.
5	Raisecom(config)#**mpls switch-l2vc** *ip-address vc-id* **fault-relay**	Configure fault relay based on association of MPLS-TP OAM and BFD alarms in the multi-sectional PW application scenario.

Copyright © Raisecom Technology Co., Ltd.

14.5.13 Checking configurations

No.	Command	Description
1	Raisecom(config-service)#**show cfm mip**	Show global CFM configurations.
2	Raisecom(config)#**show mpls-tp cfm**	Show global CFM configurations of MPLS-TP.
3	Raisecom(config)#**show mpls-tp cfm ais** [**level** *md-level*] [**source**]	Show AIS configurations of MPLS-TP.
4	Raisecom(config)#**show mpls-tp cfm domain** [**level** *md-level*]	Show MD configurations
5	Raisecom(config)#**show mpls-tp cfm errors** [**level** *md-level*]	Show error CCM.
6	Raisecom(config)#**show mpls-tp cfm local-mp** [**level** *md-level*]	Show configurations of the local MEP.
7	Raisecom(config)#**show mpls-tp cfm remote-mep** [**level** *md-level* [**service** *csi-id* [**mpid** *mep-id*]]]	Show configurations of the remote MEP.
8	Raisecom(config)#**show mpls-tp cfm remote-mep static** [**level** *md-level*]	Show configurations of the static remote MEP.
9	Raisecom(config)#**show mpls-tp cfm suppress-alarms** [**level** *md-level*]	Show configurations of alarm suppression.
10	Raisecom(config)#**show mpls-tp cfm lck** [**level** *md-level*] [**source**]	Show LCK configurations of MPLS-TP.

14.6 Configuring RFC2544

The RFC2544-based test is generally used for testing the network performance before services provisioning or for testing services in the case of network interruption after the services are provisioned.

14.6.1 Configuring type of test packets

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla pkt-type** { **eth dest-mac** *mac-address* [**cvlan** *vlan-id*] [**svlan** *vlan-id*] [**cos** *cos*] [**cfi** *cfi-value*] | **ipv4 dest-ip** *ip-address* [**source-ip** *ip-address*] [**dest-udp-port** *port-id*] [**source-udp-port** *port-id*] [**tc** *tc*] [**ttl** *ttl*] }	Configure the type of SLA test packets.

Copyright © Raisecom Technology Co., Ltd.

14.6.2 Configuring RFC2544 delay test

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **rfc2544 latency interface** *interface-type interface-number* **eth dest-mac** *mac-address* [**cvlan** *vlan-id*] [**svlan** *vlan-id*] [**cos** *cos*] [**pkt-size** *pkt-size*] [**rate** *rate*]	Configure the delay test operation of a specified destination MAC address.
3	Raisecom(config)#**sla** *oper-num* **rfc2544 latency interface** *interface-type interface-number* **ipv4 dest-ip** *ip-address* [**source-ip** *ip-address*] [**dest-udp-port** *port-id*] [**source-udp-port** *port-id*] [**tc** *tc*] [**ttl** *ttl*] [**pkt-size** *pkt-size*] [**rate** *rate*]	Configure the delay test operation of a specified destination IP address.
4	Raisecom(config)#**sla** oper-num **rfc2544 latency interface** *interface-type interface-number* [**pkt-size** *pkt-size*] [**rate** *rate*]	Configure the delay test operation. Pre-configure the type of SLA test packets before using this command to configure the delay test operation.

14.6.3 Configuring RFC2544 packet loss test

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **rfc2544 pkt-loss interface** *interface-type interface-number* **eth dest-mac** *mac-address* [**cvlan** *vlan-id*] [**svlan** *vlan-id*] [**cos** *cos*] [**pkt-size** *pkt-size*] [**rate** *rate*]	Configure the packet loss test operation of a specified destination MAC address.
3	Raisecom(config)#**sla** *oper-num* **rfc2544 pkt-loss interface** *interface-type interface-number* **ipv4 dest-ip** *ip-address* [**source-ip** *ip-address*] [**dest-udp-port** *port-id*] [**source-udp-port** *port-id*] [**tc** *tc*] [**ttl** *ttl*] [**pkt-size** *pkt-size*] [**rate** *rate*]	Configure the packet loss test operation of a specified destination IP address.
4	Raisecom(config)#**sla** *oper-num* **rfc2544 pkt-loss interface** *interface-type interface-number* [**pkt-size** *pkt-size*] [**rate** *rate*]	Configure the packet loss test operation.

14.6.4 Configuring RFC2544 throughput test

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**sla** *oper-num* **rfc2544 throughput interface** *interface-type interface-number* **eth dest-mac** *mac-address* [**cvlan** *vlan-id*] [**svlan** *vlan-id*] [**cos** *cos*] [**pkt-size** *pkt-size*] [**threshold** *threshold*]	Configure the throughput test operation of a specified destination MAC address.
3	Raisecom(config)#**sla** *oper-num* **rfc2544 throughput interface** *interface-type interface-number* **ipv4 dest-ip** *ip-address* [**source-ip** *ip-address*] [**dest-udp-port** *port-id*] [**source-udp-port** *port-id*] [**tc** *tc*] [**ttl** *ttl*] [**pkt-size** *pkt-size*] [**threshold** *threshold*]	Configure the throughput test operation of a specified destination IP address.
4	Raisecom(config)#**sla** *oper-num* **rfc2544 throughput interface** *interface-type interface-number* [**pkt-size** *pkt-size*] [**threshold** *threshold*]	Configure the throughput test operation.

14.6.5 Configuring RFC2544 performance test

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **rfc2544 performance interface** *interface-type interface-number* **eth dest-mac** *mac-address* [**cvlan** *vlan-id*] [**svlan** *vlan-id*] [**pkt-size** *pkt-size*] **bandwidth** *bandwidth-value* **tc** *tc-value* **group-id** *group-id*	Configure the performance test operation for the specified destination MAC address.
3	Raisecom(config)#**sla** *oper-num* **rfc2544 performance interface** *interface-type interface-number* **ipv4 dest-ip** *ip-address* **source-ip** *ip-address* [**dest-udp-port** *port-id*] [**source-udp-port** *port-id*] [**cvlan** *vlan-id*] [**svlan** *vlan-id*] [**ttl** *ttl*] [**pkt-size** *pkt-size*] **bandwidth** *bandwidth-value* **tc** *tc-value* **group-id** *group-id*	Configure the performance test operation for the specified destination IP address.
4	Raisecom(config)#**sla** oper-num **rfc2544 performance interface** *interface-type interface-number* [**ttl** *ttl*] [**pkt-size** *pkt-size*] **bandwidth** *bandwidth-value* **tc** *tc-value* **group-id** *group-id*	Configure the performance test operation. Pre-configure the type of SLA test packets before using this command to configure the performance test operation.

14.6.6 Configuring RFC2544 operation scheduling

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla schedule** *oper-num* [**life** { **forever** | *life-time* }]	Enable the RFC2544 performance test operation scheduling, and configure the operation lifetime. By default, the scheduling is disabled.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**sla schedule** *oper-num* [**period** *second*]	Enable RFC2544 to configure test operation scheduling and configure the operation lifetime.

14.6.7 Checking configurations

No.	Command	Description
1	Raisecom#**show sla** { **all** | *oper-num* } **configuration**	Show configurations of the RFC2544 test operation.
2	Raisecom#**show sla** { **all** | *oper-num* } **result** { **current-period** | **tests** }	Show the RFC2544 performance test result.
3	Raisecom#**show sla** { **all** | *oper-num* } **result current-period**	Show the RFC2544 configuration test result.
4	Raisecom#**show sla group-id** *group-id* **configuration rfc2544**	Show the RFC2544 test operation group configurations.
5	Raisecom#**show sla group-id** *group-id* **result rfc2544** [**latest**]	Show the performance test results of the RFC2544 test operation group.
6	Raisecom#**show sla all** { **rfc2544** | **y1564_rfc2544** } **full-detail**	Show details of the SLA test.

14.7 Configuring Y.1564

14.7.1 Configuring service throughput test operation

Configuring IP service throughput test operation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **y1564 throughput interface** *interface-type interface-number* **service-ipv4 dest-ip** *ip-address* **source-ip** *ip-address* **mode cir step** *step-value*	Configure the throughput test operation based on IP services and enter the profile configuration mode.
	Raisecom(config)#**sla** *oper-num* **y1564 throughput interface** *interface-type interface-number* **service-video dest-ip** *ip-address* **source-ip** *ip-address* **mode cir step** *step-value*	Configure the throughput test operation based on video services and enter profile configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config)#**sla** *oper-num* **y1564 throughput interface** *interface-type interface-number* **service-voice dest-ip** *ip-address* **source-ip** *ip-address* **mode cir step** *step-value*	Configure the throughput test operation based on voice services and enter profile configuration mode.
	Raisecom(config)#**sla y1564** *oper-num*	Enter Y.1564 test operation template configuration mode.
3	Raisecom(config-y1564-thrgh-ip)#**svlan** *vlan-id*	Configure the SVLAN ID.
4	Raisecom(config-y1564-thrgh-ip)#**service-cos** *cos-value*	Configure the SVLAN CoS.
5	Raisecom(config-y1564-thrgh-ip)#**cvlan** *vlan-id*	Configure the CVLAN ID.
6	Raisecom(config-y1564-thrgh-ip)#**customer-cos** *cos-value*	Configure the CVLAN CoS.
7	Raisecom(config-y1564-thrgh-ip)#**pkt-size-mode** { **fix** | **increase** | **random** }	Configure the length mode of test packets. This configuration is not available for video services and voice services.
8	Raisecom(config-y1564-thrgh-ip)#**pkt-size fix** *pkt-size* Raisecom(config-y1564-thrgh-ip)#**pkt-size-range** *min-size max-size*	Configure the length for test packets. You can configure the fixed length or a length range according to the length mode of the test packets. This configuration is not available for video services and voice services.
9	Raisecom(config-y1564-thrgh-ip)#**frame-pattern** { **null** | **prbs** }	Configure the frame mode.
10	Raisecom(config-y1564-thrgh-ip)#**cir** *cir-value* **cbs** *cbs-value*	Configure the CIR and CBS.
11	Raisecom(config-y1564-thrgh-ip)#**eir** *eir-value* **ebs** *ebs-value*	Configure the EIR and EBS.
12	Raisecom(config-y1564-thrgh-ip)#**mode** { **eir** | **overload** }	Configure the traffic mode. There is no EIR configuration and Overload configuration is unavailable.
13	Raisecom(config-y1564-thrgh-ip)#**smac** *mac-address*	Configure the source MAC address.
14	Raisecom(config-y1564-thrgh-ip)#**dest-udp-port** *port-id*	Configure the destination UDP port. This configuration is not available for video services and voice services.
15	Raisecom(config-y1564-thrgh-ip)#**source-udp-port** *port-id*	Configure the source UDP port. This configuration is not available for video services and source services.
16	Raisecom(config-y1564-thrgh-ip)#**tc** *tc-value*	Configure the TC.
17	Raisecom(config-y1564-thrgh-ip)#**ttl** *ttl-value*	Configure the TTL.
18	Raisecom(config-y1564-thrgh-ip)#**nexthop-ip** *ip-address*	Configure the next-hop IP address.
19	Raisecom(config-y1564-thrgh-ip)#**group-id** *group-id*	Configure the group ID.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
20	Raisecom(config-y1564-thrgh-ip)#**bandwidth enable**	Enable bandwidth rate limiting.

Configuring Ethernet service throughput test operation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **y1564 throughput interface** *interface-type interface-number* **service-eth dest-mac** *mac-address* **mode cir step** *step-value*	Configure the throughput test operation based on Ethernet and enter the profile configuration mode.
	Raisecom(config)#**sla y1564** *oper-num*	Enter Y.1564 test operation profile configuration mode.
3	Raisecom(config-y1564-thrgh-eth)#**svlan** *vlan-id*	Configure the SVLAN ID.
4	Raisecom(config-y1564-thrgh-eth)#**service-cos** *cos-value*	Configure the SVLAN CoS.
5	Raisecom(config-y1564-thrgh-eth)#**service-tpid** *tpid-value*	Configure the SVLAN TPID.
6	Raisecom(config-y1564-thrgh-eth)#**service-cfi** *cfi-value*	Configure the SVLAN CFI.
7	Raisecom(config-y1564-thrgh-eth)#**cvlan** *vlan-id*	Configure the CVLAN ID.
8	Raisecom(config-y1564-thrgh-eth)#**customer-cos** *cos-value*	Configure the CVLAN CoS.
9	Raisecom(config-y1564-thrgh-eth)#**customer-tpid** *tpid-value*	Configure the CVLAN TPID.
10	Raisecom(config-y1564-thrgh-eth)#**customer-cfi** *cfi-value*	Configure the CVLAN CFI.
11	Raisecom(config-y1564-thrgh-eth)#**frame-pattern** { **null** | **prbs** }	Configure the frame mode.
12	Raisecom(config-y1564-thrgh-eth)#**cir** *cir-value* **cbs** *cbs-value*	Configure the CIR and CBS.
13	Raisecom(config-y1564-thrgh-eth)#**eir** *eir-value* **ebs** *ebs-value*	Configure the EIR and EBS.
14	Raisecom(config-y1564-thrgh-eth)#**mode** { **eir** | **overload** }	Configure the traffic mode.
15	Raisecom(config-y1564-thrgh-eth)#**group-id** *group-id*	Configure the group ID.
16	Raisecom(config-y1564-thrgh-eth)#**pkt-size-mode increase**	Configure the length mode of test packets. This configuration is not available for video services and voice services.
17	Raisecom(config-y1564-thrgh-eth)#**pkt-size fix** *pkt-size*	Configure the length of the test packets.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config-y1564-thrgh-eth)#**pkt-size-range** *min-size max-size*	You can configure the fixed length or length range according to the length mode of test packets. This configuration is not available for video services and voice services.
18	Raisecom(config-y1564-thrgh-eth)#**bandwidth enable**	Enable bandwidth rate limiting.

14.7.2 Configuring service performance test operation

Configuring IP service performance test operation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **y1564 performance interface** *interface-type interface-number* **service-ipv4 dest-ip** *ip-address* **source-ip** *ip-address* **bandwidth** *bandwidth-value* **group-id** *group-id*	Configure the performance test operation based on IP service and enter the profile configuration mode.
	Raisecom(config)#**sla** *oper-num* **y1564 performance interface** *interface-type interface-number* **service-video dest-ip** *ip-address* **source-ip** *ip-address* **bandwidth** *bandwidth-value*	Configure the performance test operation based on video service and enter the profile configuration mode.
	Raisecom(config)#**sla** *oper-num* **y1564 performance interface** *interface-type interface-number* **service-voice dest-ip** *ip-address* **source-ip** *ip-address* **bandwidth** *bandwidth-value*	Configure the performance test operation based on audio service and enter the profile configuration mode.
	Raisecom(config)#**sla y1564** *oper-num*	Enter Y.1564 test operation template configuration mode.
3	Raisecom(config-y1564-perf-ip)#**svlan** *vlan-id*	Configure the SVLAN ID.
4	Raisecom(config-y1564-perf-ip)#**service-cos** *cos-value*	Configure the SVLAN CoS.
5	Raisecom(config-y1564-perf-ip)#**cvlan** *vlan-id*	Configure the CVLAN ID.
6	Raisecom(config-y1564-perf-ip)#**customer-cos** *cos-value*	Configure the CVLAN CoS.
7	Raisecom(config-y1564-perf-ip)#**pkt-size-mode increase**	Configure the length mode of test packets. This configuration is not available for video services and voice services.
8	Raisecom(config-y1564-perf-ip)#**pkt-size fix** *pkt-size*	Configure the length of the test packets.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config-y1564-perf-ip)#**pkt-size-range** *min-size max-size*	You can configure the fixed length or length range according to the length mode of test packets. This configuration is not available for video services and voice services.
9	Raisecom(config-y1564-perf-ip)#**frame-pattern** { **null** | **prbs** }	Configure the frame mode.
10	Raisecom(config-y1564-perf-ip)#**smac** *mac-address*	Configure the source MAC address.
11	Raisecom(config-y1564-perf-ip)#**dest-udp-port** *port-id*	Configure the destination UDP port. This configuration is not available for video services and voice services.
12	Raisecom(config-y1564-perf-ip)#**source-udp-port** *port-id*	Configure the source UDP port. This configuration is not available for video services and source services.
13	Raisecom(config-y1564-perf-ip)#**tc** *tc-value*	Configure the TC.
14	Raisecom(config-y1564-perf-ip)#**ttl** *ttl-value*	Configure the TTL.
15	Raisecom(config-y1564-perf-ip)#**nexthop-ip** *ip-address*	Configure the next-hop IP address.
16	Raisecom(config-y1564-perf-ip)#**bandwidth enable**	Configure bandwidth rate limiting.

Configuring Ethernet service performance test operation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **y1564 performance interface** *interface-type interface-number* **service-eth dest-mac** *mac-address* **bandwidth** *bandwidth-value* **group-id** *group-id*	Configure the performance test operation based on Ethernet and enter the profile configuration mode.
	Raisecom(config)#**sla y1564** *oper-num*	Enter Y.1564 test operation profile configuration mode.
3	Raisecom(config-y1564-perf-eth)#**svlan** *vlan-id*	Configure the SVLAN ID.
4	Raisecom(config-y1564-perf-eth)#**service-cos** *cos-value*	Configure the SVLAN CoS.
5	Raisecom(config-y1564-perf-eth)#**service-tpid** *tpid-value*	Configure the SVLAN TPID.
6	Raisecom(config-y1564-perf-eth)#**service-cfi** *cfi-value*	Configure the SVLAN CFI.
7	Raisecom(config-y1564-perf-eth)#**cvlan** *vlan-id*	Configure the CVLAN ID.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
8	Raisecom(config-y1564-perf-eth)#**customer-cos** *cos-value*	Configure the CVLAN CoS.
9	Raisecom(config-y1564-perf-eth)#**customer-tpid** *tpid-value*	Configure the CVLAN TPID.
10	Raisecom(config-y1564-perf-eth)#**customer-cfi** *cfi-value*	Configure the CVLAN CFI.
11	Raisecom(config-y1564-perf-eth)#**frame-pattern** { **null** | **prbs** }	Configure the frame mode.
12	Raisecom(config-y1564-perf-eth)#**group-id** *group-id*	Configure the group ID.
13	Raisecom(config-y1564-perf-eth)#**pkt-size-mode increase**	Configure the length mode of test packets.
14	Raisecom(config-y1564-perf-eth)#**pkt-size-range** *pkt-size-1 pkt-size-2*	Configure the change range of the test packet length.
15	Raisecom(config-y1564-perf-eth)#**pkt-size fix** *pkt-size*	Configure the fix length of test packets.
16	Raisecom(config-y1564-perf-eth)#**bandwidth enable**	Enable bandwidth rate limiting.
17	Raisecom(config-y1564-perf-eth)#**sla y1564** *oper-num*	Enter Y.1564 test operation profile configuration mode.

14.7.3 Configuring Y.1564 operation recognition

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla y1564 service-identify type** { **vlan** [**cos** | **dscp**] | **untag** [**dscp** | **ip**] }	Configure Y.1564 test operation service recognition.

14.7.4 Configuring Y.1564 operation scheduling

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla schedule group-id** *group-id* [**life** { *life-time* | **forever** }] **performance**	Schedule the Y.1564 performance test operation.
3	Raisecom(config)#**sla schedule group-id** *group-id* [**period** *period*] **throughput**	Schedule the Y.1564 configuration test operation.
4	Raisecom(config)#**sla schedule** *oper-num* [**life** { **forever** | *life-time* }] [**period** *second*]	Schedule a certain Y.1564 test operations.

Copyright © Raisecom Technology Co., Ltd.

14.7.5 Checking configurations

No.	Command	Description
1	Raisecom#**show sla**	Check SLA global configurations.
2	Raisecom#**show sla** { **all** | *oper-num* | **group-id** *group-id* } **configuration**	Check Y.1564 operation configurations.
3	Raisecom#**show sla** { **all** | *oper-num* } **result test**	Show the latest test of a specified operation.
4	Raisecom#**show sla group-id** *group-id* **result** { **performance** | **throughput** }	Show test results of the performance or configuration test operation group.
5	Raisecom#**show sla group-id** *group-id* **result performance latest**	Show five-minute test results of the performance test operation group.
6	Raisecom#**show sla all y1564 full-detail**	Show information about all Y.1564 test operations.

14.8 Configuring SLA test alarm

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla alarm threshold** { **enable** | **disable** }	Enable threshold alarms.
3	Raisecom(config)#**sla** *oper-num* **loss-rate-threshold** { **current** | **average** } [**ds** | **sd** | **twoway**] *threshold*	Configure the packet loss alarm threshold to 10, in units of Hundred thousandth.
4	Raisecom(config)#**sla** *oper-num* **loss-pkt-trap** { **current** | **average** } **enable**	Enable packet loss rate alarm. By default, it is disabled.
5	Raisecom(config)#**sla** *oper-num* **delay-threshold** { **current** | **average** } [**ds** | **sd** | **two-way**] *threshold*	Configure the delay alarm threshold.
6	Raisecom(config)#**sla** *oper-num* **delay-trap** { **current** | **average** } [**ds** | **sd** | **two-way**] **enable**	Enable delay alarm. By default, it is disabled.
7	Raisecom(config)#**sla** *oper-num* **jitter-threshold** { **current** | **average** } [**ds** | **sd** | **twoway**] *threshold*	Configure the jitter alarm threshold. By default, the jitter alarm threshold is 50us.
8	Raisecom(config)#**sla** *oper-num* **jitter-threshold** { **current** | **average** } **enable**	Enable jitter alarm. By default, it is disabled.
9	Raisecom(config)#**sla** *oper-num* **availability-threshold** [**sd** | **ds**] *threshold*	Configure the threshold of the SLA availability test.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
10	Raisecom(config)#**sla** *oper-num* { **availabilitychange-trap** | **availability-trap** } [**sd** | **ds** | **two-way**] { **enable** | **disable** }	Enable alarm reporting for availability or availability change. By default, it is disabled.
11	Raisecom(config)#**sla maintenance** { **start** | **stop** }	Start or end the SLA maintenance window.
12	Raisecom(config)#**sla alarm availabilitychange enable**	Enable availability change alarms.
13	Raisecom(config)#**sla** *oper-num* **availability-flr-threshold** *threshold*	Configure the high packet loss rate threshold for the packet loss rate operation. If the current packet loss rate is less than the threshold, the current status is considered available, otherwise it is unavailable.
14	Raisecom(config)#**sla** *oper-num* **availability-num-consecutive-intervals** *availability-num*	Configure the number of operation consecutive availability indicators that measure the packet loss rate.
15	Raisecom(config)# **sla** *oper-num* **availability-num-consecutive-high-flr** *high-flr-num*	Configure the number of operation consecutive high packet loss indicators that measures the packet loss rate.

14.9 Configuring interface loopback

14.9.1 Preparing for configurations

Scenario

The network maintenance personnel can detect and analyse interface and network faults through interface loopback. The device supports physical interface loopback and LAG interface loopback.

Prerequisite

The interface status is Up.

14.9.2 Configuring interface loopback

Steps 2 and 3 are optional. To perform interface loopback, execute step 2. To perform link aggregation group loopback, execute step 3.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config-port)#**loopback** { **internal** | **external** } [**ipv4 access-list** *acl-number-ipv4* [**swap sip** *ipv4-addr*] | **ipv6 access-list** *acl-number-ipv6* [**swap sip** *ipv6-addr*]] [**swap smac** *mac-addr*] [**swap dip-disable**] [**swap dmac-disable**] [**swap upd-port-disable**] [**in-service** { **enable** | **disable** }] [**on-line** { **enable** | **disable** }]	mode and enable interface loopback. • internal: internal loopback • external: external loopback
3	Raisecom(config)#**interface port-channel** *channel-number*	Enter link aggregation configuration mode and enable loopback on the link aggregation group interface. • internal: internal loopback • external: external loopback
	Raisecom(config-port-channel*)#**loopback** { **internal** | **external** } [**ipv4 access-list** *acl-number-ipv4* [**swap sip** *ipv4-addr*] | **ipv6 access-list** *acl-number-ipv6* [**swap sip** *ipv6-addr*]] [**swap smac** *mac-addr*] [**swap dip-disable**] [**swap dmac-disable**] [**swap upd-port-disable**] [**in-service** { **enable** | **disable** }] [**on-line** { **enable** | **disable** }]	

14.9.3 Configuring loopback duration

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode and configure the loopback duration.
	Raisecom(config-port)#**loopback timeout** *minutes*	

14.9.4 Checking configurations

No.	Command	Description
1	Raisecom#**show interface** *interface-type interface-number*	Show interface status.
2	Raisecom#**show loopback** *interface-type interface-number*	Show configurations of the loopback interface.

Copyright © Raisecom Technology Co., Ltd.

14.10 Configuring smart probe

14.10.1 Preparing for configurations

Scenario

The RAX721 is usually used as the initiator of the smart probe system, and it is necessary to configure the connection of the smart probe TCP channel and the upload of the smart probe operation.

Prerequisite

N/A

14.10.2 Configuring smart probe TCP channel

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla iprobe tcp client-ip** *ip-address*	Configure the local IP address of the smart probe TCP channel.
3	Raisecom(config)#**sla iprobe tcp server-ip** *ip-address*	Configure the server IP address of the smart probe TCP channel.
4	Raisecom(config)#**sla iprobe tcp server-port** *port-id*	Configure the server port ID of the smart probe TCP channel.
5	Raisecom(config)#**sla iprobe tcp** { **enable** | **disable** }	Enable TCP channel connections.

14.10.3 Configuring the uploading of smart probe operation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla iprobe upload** { **1s** | **5m** | **both** }	Configure the type of csv file for uploading smart probe operations.
3	Raisecom(config)#**sla iprobe upload** { **starttime** | **endtime** } *hh mm ss year month day*	Configure the start time/end time for uploading the smart probe operation.
4	Raisecom(config)#**sla iprobe upload** { **user** *username* | **password** *password* }	Configure the user name/password for uploading the smart probe operation.
5	Raisecom(config)#**sla iprobe upload path** *dir*	Configure the file path for uploading the smart probe operation.
6	Raisecom(config)#**sla iprobe upload** { **primary** | **secondary** | **backup** } **server-port** *port-id*	Configure the service port number for uploading smart probe operations.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
7	Raisecom(config)#**sla iprobe upload { primary | secondary | backup } server-ip** *ip-address*	Configure the service IP address for uploading the smart probe operation.

14.10.4 Checking configurations

Step	Command	Description
1	Raisecom#**show sla iprobe configuration**	Show SLA smart probe configurations.

14.11 Configuring ULDP

14.11.1 Preparing for configurations

Scenario

When there is a unidirectional link (transmission in only one direction), ULDP can detect it, close the corresponding interface and send a warning message.

Prerequisite

Devices at both ends should support ULDP.

14.11.2 Default configurations of ULDP

Function	Default value
ULDP	Disable

14.11.3 Configuring ULDP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**uldp enable**	Enable global ULDP.
3	Raisecom(config)#**interface** *interface-type primary-interface-number*	Enter physical interface configuration mode.
4	Raisecom(config-port)#**uldp enable**	Enable interface ULDP.
5	Raisecom(config-port)#**exit**	Return to global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config)#**uldp recovery-time** *time*	(Optional) configure the recovery time of the unidirectional link.

14.11.4 Checking configurations

No.	Item	Description
1	Raisecom#**show uldp**	Show ULDP configurations.

14.12 Configuring Traceroute

14.12.1 Preparing for configurations

Scenario

- Traceroute test on the IPv4 destination address
- Traceroute test on the IPv6 destination address
- Traceroute test on the specified IPv6-SID
- Traceroute test on the specified SRv6 policy
- Traceroute test on the specified SR-MPLS
- Traceroute test on the specified MPLS

Prerequisite

N/A

14.12.2 Configuring Traceroute

Step	Command	Description
1	Raisecom#**traceroute** [**vrf** *vrf-name*] { *ip-address* | **dns** *dns-domain-name* } [**firstttl** *first-ttl*] [**maxttl** *max-ttl*] [**port** *port-number*] [**waittime** *period*] [**count** *packages*] [**size** *size*]	Perform the Traceroute test on the IPv4 destination address.
2	Raisecom#**traceroute** [**vrf** *vrf-name*] **ipv6** { *ipv6-address* | **dns** *dns-domain-name* } [**firstttl** *first-ttl*] [**maxttl** *max-ttl*] [**port** *port-number*] [**waittime** *period*] [**count** *packages*] [**size** *size*]	Perform the Traceroute test on the IPv6 destination address.
3	Raisecom#**traceroute ipv6-sid** [**overlay**] *sid1* [*sid2* [*sid3* [*sid4* [*sid5* [*sid6* [*sid7* [*sid8* [*sid9* [*sid10* [*sid11*]]]]]]]]]] [**firstttl** *first-ttl*] [**maxttl** *max-ttl*] [**port** *port-number*] [**waittime** *period*] [**count** *packages*] [**size** *size*] [**source** *ipv6-address*]	Perform the Traceroute test on the specified IPv6-SID.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom#**traceroute srv6-te policy endpoint-ip** *ipv6-address* **color** *color-id* **end-otp** *end-otp* [**firstttl** *first-ttl*] [**maxttl** *max-ttl*] [**port** *port-number*] [**waittime** *period*] [**count** *packages*] [**size** *size*] [**source** *ipv6-address*]	Perform the Traceroute test on the specified SRv6 policy.
5	Raisecom#**traceroute mpls segment-routing ipv4** *ipv4-address/mask-length*	Configure the Traceroute test on SR-MPLS-BE.
6	Raisecom#**traceroute mpls segment-routing te tunnel** *tunnel-number*	Configure the Traceroute test on SR-MPLS-TE.
7	Raisecom#**traceroute mpls ipv4** *ip-address/mask* [**generic**] [**nexthop** *ip-address*] [**waittime** *seconds*] [**maxttl** *ttl*] [**reply dscp** *dscp-value*] [**reply mode udp** | **reply mode udp-alert**] [**reply pad-tlv**] [**source** *ip-address*] [**tc** *tc-value*] [**flags fec**]	Configure the Traceroute test on MPLS LSP.
8	Raisecom#**traceroute mpls te tunnel** *tunnel-interface* [**waittime** *seconds*] [**maxttl** *ttl*] [**reply dscp** *dscp-value*] [**reply mode udp** | **reply mode udp-alert**] [**reply pad-tlv**] [**source** *ip-address*] [**tc** *tc-value*] [**flags fec**]	Configure the Traceroute test on the MPLS Tunnel.

14.13 Configuring PING

14.13.1 Preparing for configurations

Scenario

PING is used to detect whether the network is connected properly.

Prerequisite

N/A

14.13.2 PING IPv4 network

Step	Command	Description
1	Raisecom#**ping** [**vrf** *vpn-instance-name*] { *ip-address* | **dns** *dns-domain-name* } [**count** *count*] [**interface** *interface-type interface-number*] [**interval** *time*] [**size** *size*] [**waittime** *period*] [**source** *ip-address*] [**df-bit**]	Use the **ping** command to test the connectivity of the IPv4 network.

Copyright © Raisecom Technology Co., Ltd.

You cannot perform other operations in the process of PING until PING is finished or Ping is interrupted by pressing **Ctrl**+**C**.

14.13.3 PING IPv6 network

Step	Command	Description
1	Raisecom#**ping** [**vrf** *vpn-instance-name*] **ipv6** { *ipv6-address* | **dns** *dns-domain-name* } [**count** *count*] [**interface** *interface-type interface-number*] [**interval** *time*] [**size** *size*] [**waittime** *period*] [**source** *ipv6-address*]	Use the **ping** command to test the connectivity of the IPv6 network.

14.13.4 PING MPLS network

Step	Command	Description
1	Raisecom#**ping mpls ipv4** *ip-address/m* [**nexthop** *ip-address*] [**count** *count*] [**size** *size*] [**waittime** *period*] [**source** *ipv-address*] [**ttl**] [**tc**]	Use the **ping** command to test the MPLS network connectivity of a specified IPv4 address.
2	Raisecom#**ping mpls vc-id** *vc-id* **destination** *ip-address* [**count** *count*] [**size** *size*] [**waittime** *period*] [**source** *ipv-address*] [**ttl**] [**tc**]	Use the **ping** command to test the MPLS network connectivity of a specified VC-ID.
3	Raisecom#**ping mpls ipv4** *ip-address/mask* [**generic**] [**nexthop** *ip-address*] [**interval** *interval*] [**count** *count*] [**waittime** *seconds*] [**ttl** *ttl*] [**reply dscp** *dscp-value*] [**reply mode udp** | **reply mode udp-alert**] [**reply pad-tlv**] [**size** *size*] [**source** *ip-address*] [**tc** *tc-value*]	Configure the PING test on MPLS LSP.
4	Raisecom#**ping mpls te tunnel** *tunnel-interface* [**interval** *interval*] [**count** *count*] [**waittime** *seconds*] [**ttl** *ttl*] [**reply dscp** *dscp-value*] [**reply mode udp** | **reply mode udp-alert**] [**reply pad-tlv**] [**size** *size*] [**source** *ip-address*] [**tc** *tc-value*]	Configure the PING test on the MPLS Tunnel.

14.13.5 PING DHCP Server

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp server ping** { **packet** *packet-num* | **timeout** *time* }	Configure the network connectivity with the DHCPv4 server.

Copyright © Raisecom Technology Co., Ltd.

14.13.6 PING the SR network

Step	Command	Description
1	Raisecom#**ping ipv6-sid** [**segment-by-segment**] *sid1* [*sid2* [*sid3* [*sid4* [*sid5* [*sid6* [*sid7* [*sid8* [*sid9* [*sid10* [*sid11*]]]]]]]]]] [**interval** *time*] [**count** *packages*] [**size** *size*] [**waittime** *period*] [**source** *ipv6-address*]	Configure the PING SRv6 test, specify the PING SID stack, and configure the packet sending interval, number of sent packets, byte size, waiting timeout, and source IP address.
2	Raisecom#**ping srv6-te policy endpoint-ip** *ipv6-address* **color** *color-id* [**interval** *time*] [**waittime** *period*] [**count** *packages*] [**size** *size*] [**source** *ipv6-address*]	Configure the PING SRv6 policy test, specify the endpoint and color, and configure the packet sending interval, number of sent packets, byte size, waiting timeout, and source IP address.
3	Raisecom#**ping mpls segment-routing** { **ipv4** *ipv4-address/mask-length* | **te tunnel** *interface-number* }	Configure the PING test on MPLS SR.

14.14 Maintenance

Command	Description
Raisecom(config)#**clear oam config**	Clear OAM configurations.
Raisecom(config-port)#**clear oam event**	Clear OAM event statistics.
Raisecom(config-port)#**clear oam statistics**	Clear OAM statistics.
Raisecom(config)#**clear ethernet cfm errors** [**level** *md-level*]	Clear error CCM records.
Raisecom(config)#**clear ethernet cfm suppress-alarm source**	Clear alarm inhibition information about MEPs.
Raisecom(config)#**clear ethernet cfm traceroute-cache**	Clear LinkTrace cache configurations.
Raisecom(config)#**clear bfd** *session-id* **statistics**	Clear statistics about specified BFD sessions.
Raisecom(config-service)#**clear cfm suppress-alarm source**	Clear alarm inhibition information about MPLS-TP MEPs.
Raisecom(config-service)#**clear ais packet statistic**	Clear AIS packet statistics.
Raisecom(config-service)#**clear csf packet statistic**	Clear CSF packet statistics.

Copyright © Raisecom Technology Co., Ltd.

15 Security

This chapter describes principles and configuration procedures of security, as well as related configuration examples, including following sections:

- Configuring AAA
- Configuring storm control
- Configuring CPU protection
- Configuring CPU monitoring
- Configuring port mirroring
- Configuring attack prevention
- Configuring ARP attack prevention
- Configuring dynamic ARP inspection
- Configuring URPF
- Configuring 802.1x
- Configuring password management
- Configuration examples

15.1 Configuring AAA

15.1.1 Preparing for configurations

Scenario

In order to control user access to the device and network, you can deploy a RADIUS/TACACS+ server in the network to authenticate and account for users. The RAX721 can be used as a proxy device of the RADIUS/TACACS+ server to authorize user access based on the feedback results from the RADIUS/TACACS+ server. TACACS+ is more secure and reliable than RADIUS.

Prerequisite

N/A

Copyright © Raisecom Technology Co., Ltd.

15.1.2 Default configurations

Function	Default value
RADIUS authentication port number/backup authentication port number	1812
RADIUS accounting port number/backup accounting port number	1813
TACACS+ authentication port number/backup authentication port number	49
TACACS+ accounting port number/backup accounting port	49
Billing failure handling strategy	**online**
Sending period of update packets	0
Command line authorization status	Disable

15.1.3 Configuring AAA

Configuring AAA basic functions

Step	Command	Description
1	`Raisecom#aaa`	Enter AAA configuration mode.
2	`Raisecom(aaa)#aaa accounting login enable`	Enable AAA accounting.
3	`Raisecom(aaa)#aaa accounting fail { offline | online }`	Configure the accounting failure handling policy.
4	`Raisecom(aaa)#aaa accounting update` *minute*	Configure the interval for sending accounting update packets. If it is configured to 0, it means no accounting update packet will be sent. **Note** Through the accounting start packet, accounting-Update packet, and accounting-End packet, the RADIUS accounting server can record the access time and operations of each user.
5	`Raisecom(aaa)#aaa command authorize { enable | disable }`	Enable/Disable AAA authentication through the command line.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(aaa)#**user special-characters** *charlist*	(Optional) configure the special characters that can be used in the user name and password. By default, the following 32 special characters are supported: `~!@#$%^&*()_-+={}[]|\:;'<>",.?.
6	Raisecom(aaa)#**domain** { *domain-name* | **default** | **default_admin** }	Create a user domain and enter domain configuration mode.
7	Raisecom(aaa-*)#**user login** { **local-radius** | **local-user** | **radius-local** [**server-no-response**] | **radius-user** | **local-tacacs** | **tacacs-local** [**server-no-response**] | **tacacs-user** }	Configure the user login mode.

Configuring AAA service template

Step	Command	Description
1	Raisecom#**aaa**	Enter AAA configuration mode.
2	Raisecom(aaa)#**service-scheme** *scheme-name*	Create a service template and enter service template configuration mode.
3	Raisecom(service-scheme-*)#**service car** { **ingress** | **egress** } **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*]	Configure service template rate limiting.

15.1.4 Configuring RADIUS

Configuring RADIUS authentication

Step	Command	Description
1	Raisecom#**radius** [**backup**] { *ipv4-address* | *ipv6-address* } [**auth-port** *port-number*] [**sourceip** { *sip-address* | *sipv6-address* }]	Specify the IP address of the RADIUS authentication server. Configure the **backup** parameter to specify the backup RADIUS authentication server.
2	Raisecom#**radius-key** *string*	Configure the shared plaintext key of the RADIUS authentication server.
3	Raisecom#**radius-encrypt-key** *string*	Configure the shared ciphertext key of the RADIUS authentication server.
4	Raisecom#**radius backup key** *string*	Configure the shared plaintext key of the RADIUS backup authentication server.
5	Raisecom#**radius backup encrypt-key** *string*	Configure the shared ciphertext key of the RADIUS backup authentication server.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom#**radius response-timeout** *time*	Configure the response timeout period of the RADIUS authentication server.
7	Raisecom#**radius authentication fail trap** { **enable** | **disable** }	Configure alarm trap for reporting RADIUS authentication failures.
8	Raisecom#**user login** { **local-user** | **radius-user** | **local-radius** | **radius-local** [**server-no-response**] }	Configure the authentication mode for user login in RADIUS authentication.
9	Raisecom#**enable login** { **local-user** | **radius-user** | **local-radius** | **radius-local** [**server-no-response**] }	Configure the authentication mode for user entering privileged EXEC mode in RADIUS authentication.

Configuring RADIUS accounting

Step	Command	Description
1	Raisecom#**radius** [**backup**] **accounting-server** { *ipv4-address* | *ipv6-address* } [**acct-port** *port-number*] [**sourceip** { *sip-address* | *sipv6-address* }]	Specify the IP address and UDP port number of the RADIUS accounting server. Configure the **backup** parameter to specify the backup RADIUS accounting server.
2	Raisecom#**radius** [**backup**] **accounting-server key** *string*	Configure the shared plaintext key for communication with the RADIUS accounting server. The key must be the same as the shared key set on the RADIUS accounting server, otherwise accounting will fail.
3	Raisecom#**radius** [**backup**] **accounting-server encrypt-key** *string*	Configure the shared ciphertext key for communication with the RADIUS accounting server. The key must be the same as the shared key set on the RADIUS accounting server, otherwise accounting will fail.

15.1.5 Configuring TACACS+

Configuring TACACS+ authentication

Step	Command	Description
1	Raisecom#**tacacs-server** [**backup**] { *ipv4-address* | *ipv6-address* } [**sourceip** { *sip-address* | *sipv6-address* }] [**auth-port** *port-number*]	Specify the IP address of the TACACS+ authentication server. Configure the **backup** parameter to specify the backup TACACS+ authentication server.
2	Raisecom#**tacacs-server** [**backup**] **key** *string*	Configure the shared plaintext key for TACACS+ authentication. Configure the **backup** parameter to specify the backup TACACS+ authentication server.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom#**tacacs-server** [**backup**] **encrypt-key** *string*	Configure the shared ciphertext key for TACACS+ authentication. Configure the **backup** parameter to specify the backup TACACS+ authentication server.
4	Raisecom#**user login** { **local-user** | **radius-user** | **local-radius** | **radius-local** [**server-no-response**] }	Configure the authentication mode for user login in TACACS+ authentication.
5	Raisecom#**enable login** { **local-user** | **radius-user** | **local-radius** | **radius-local** [**server-no-response**] }	Configure the authentication mode for user entering privileged EXEC mode in TACACS+ authentication.

Configuring TACACS+ accounting

Step	Command	Description
1	Raisecom#**tacacs** [**backup**] **accounting-server** { *ipv4-address* | *ipv6-address* } [**sourceip** { *sip-address* | *sipv6-address* }] [**acct-port** *port-number*]	Specify the IP address of the TACACS+ accounting server. Configure the **backup** parameter to specify the backup TACACS+ accounting server.
2	Raisecom#**tacacs** [**backup**] **accounting-server key** *string*	Configure the shared plaintext key for communication with the TACACS+ accounting server.
3	Raisecom#**tacacs** [**backup**] **accounting-server encrypt-key** *string*	Configure the shared ciphertext key for communication with the TACACS+ accounting server.

15.1.6 Checking configurations

No.	Command	Description
1	Raisecom#**show radius-server**	Show configurations of the RADIUS server.
2	Raisecom#**show tacacs-server**	Show configurations of the TACACS+ server.
3	Raisecom#**show aaa**	Show AAA configurations.
4	Raisecom#**show service-scheme** { **all-scheme** | **name** *scheme-name* }	Show service profile configurations.

15.1.7 Maintenance

Command	Description
Raisecom#**clear tacacs statistics**	Clear TACACS+ statistics

Copyright © Raisecom Technology Co., Ltd.

15.2 Configuring storm control

15.2.1 Preparing for configurations

Scenario

In the Layer 2 network, after storm control is configured, it can inhabit generation of broadcast storm, when unknown multicast, unknown unicast, and broadcast packets increase, to ensure forwarding normal packets.

Prerequisite

Configure physical parameters on an interface and make the physical layer Up.

15.2.2 Configuring storm control

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**portswitch**	Enter interface configuration mode and switch it to Layer 2 interface mode.
3	Raisecom(config-port)#**storm-control mode** { **kbps** | **pps** }	Configure the storm control mode. By default, it is kbps.
4	Raisecom(config-port)#**storm-control** { **broadcast** | **unknown-multicast** | **dlf** | **all** } **kbps** *kbps-value* [**burst** *burst-value*]	Configure the rate limiting threshold of storm control.
	Raisecom(config-port)#**storm-control** { **broadcast** | **unknown-multicast** | **dlf** | **all** } **pps** *value*	
5	Raisecom(config-port)#**storm-control action** { **shutdown** | **drop** }	Configure the storm control action of the interface. By default, it is drop.

Note

When storm control is enabled, you can configure rate limiting. However, configurations cannot take effect. When storm control is disabled, rate limiting configurations take effect automatically.

15.2.3 Checking configurations

No.	Command	Description
1	Raisecom#**show storm-control** {**interface** [*interface-type interface-number*] | **status** | **vlan** *vlanid* }	Show configurations of storm control.

Copyright © Raisecom Technology Co., Ltd.

15.3 Configuring CPU protection

15.3.1 Preparing for configurations

Scenario

When the device receives a great number of attack packets in a short period, the CPU will run with full load and the CPU utilization rate reaches to 100%. This will cause the normal functions of the device to fail. CPU CAR helps to efficiently limit the speed of packets, which enters the CPU.

Prerequisite

N/A

15.3.2 Configuring global CPU CAR

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#cpu-protect car **global pps** *pps-value*	Configure the rate limiting mode for global CPU packets protection.
3	Raisecom(config)#**cpu-protect car queue** *queue-number* **pps** *pps-value*	Configure the rate limiting mode of the CPU protection queue.

15.3.3 Clearing statistics

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**clear** cpu-protect car **global statistics**	Clear global statistics on CPU protection.
3	Raisecom(config)#**clear** cpu-protect car **queue** *queue-id* **statistics**	Clear statistics on the specified queue of CPU protection.

15.3.4 Checking configurations

No.	Command	Description
1	Raisecom#**show cpu-protect car statistics**	Show CPU CAR statistics.

Copyright © Raisecom Technology Co., Ltd.

15.4 Configuring CPU monitoring

15.4.1 Preparing for configurations

Scenario

CPU monitoring is used to monitor task status, CPU utilization rate, and stack usage in real time. It provides CPU utilization threshold alarm to facilitate discovering and eliminating a hidden danger, helping the administrator locate the fault quickly.

Prerequisite

To output CPU monitoring alarms in a Trap form. You need to configure the IP address of Trap target host on the RAX721, that is, the IP address of the network management system.

15.4.2 Configuring CPU monitoring alarm

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**cpu threshold recovering** *recovering-threshold-value* **rising** *rising-threshold-value*	Configure the CPU alarm rising threshold and recovery threshold.
3	Raisecom(config)#**cpu interval** *interval-value* Raisecom(config)#**exit**	(Optional) configure the CPU alarm sampling interval. By default, the sampling interval of CPU alarm is 60s.
4	Raisecom#**show cpu-utilization** [**dynamic**]	Show the CPU utilization rate.
5	Raisecom#**show cpu-utilization** *code-cpu-id*	
6	Raisecom#**show cpu-utilization history** { **10min** | **1min** | **2hour** | **5sec** }	
7	Raisecom#**show process** [**dead** | **sorted** { **priority** | **name** } | *taskname*]	Show status of each task.
	Raisecom#**show process pid** *id-range*	
	Raisecom#**show process cpu** [**sorted** [**10min** | **1min** | **5sec** | **invoked**]]	

15.5 Configuring port mirroring

15.5.1 Preparing for configurations

Scenario

Port mirroring refers to mirroring packets of the specified mirroring port to the destination port or aggregation group without affecting packet forwarding. With port mirroring, users can

Copyright © Raisecom Technology Co., Ltd.

monitor transmitting and receiving status of one or more interfaces for analyzing network status.

Prerequisite

N/A

15.5.2 Configuring port mirroring

The same interface/link aggregation group cannot be a monitoring interface and a mirroring source interface concurrently. Therefore, the interface/link aggregation group in step 3 and step 4 cannot be the same one.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mirror-group** *group-id*	Create a port mirroring group.
3	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**mirror-group** *group-id* **monitor-port** Raisecom(config-port)#**exit**	(Optional) enter interface configuration mode. Configure the interface as a monitoring interface.
	Raisecom(config)#**interface port-channel** *channel-number* Raisecom(config-port-channel*)#**mirror-group** *group-id* **monitor-port** Raisecom(config-port-channel*)#**exit**	(Optional) enter link aggregation configuration mode. Configure the link aggregation group as the monitoring interface.
4	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**mirror-group** *group-id* **source-port** [**ingress** | **egress**]	(Optional) enter interface configuration mode. Configure the interface as a mirroring source interface and configure mirroring rules to mirror the packets in the ingress direction, egress direction, or both directions of the source interface.
	Raisecom(config)#**interface port-channel** *channel-number* Raisecom(config-port-channel*)#**mirror-group** *group-id* **source-port** [**ingress** | **egress**]	(Optional) enter link aggregation configuration mode. Configure the link aggregation group as a mirroring source interface and configure mirroring rules to mirror the packets in the ingress direction, egress direction, or both directions of the source interface.
5	Raisecom(config-port)#**exit** Raisecom(config)#**mirror-group** *group-id* **source-cpu** [**ingress** | **egress**]	Configure the mirroring of CPU packets.

15.5.3 Configuring RSPAN

The Remote Switched Port Analyzer (RSPAN) is a port mirroring technology on the switch, used to provide network data traffic for the network analyzer and to provide remote monitoring across networks.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mirror-group** *group-id*	Create a port mirroring group.
3	Raisecom(config)#**mirror-group** *group-id* { **remote-source** | **remote-destination** }	Configure the device as the source end or destination end of remote mirroring.
4	Raisecom(config)#**mirror-group** *group-id* **remote-vlan** *vlan-id*	Configure the remote mirroring VLAN.
5	Raisecom(config)#**mirror-group** *group-id* **reflector-port** *interface-type interface-number*	Configure the reflector port of remote mirroring. The reflector port should be added to the mirroring VLAN. For related configurations, see section 4.1 Configuring VLAN.

15.5.4 Checking configurations

No.	Command	Description
1	Raisecom#**show mirror-group** *group-id*	Show basic information about port mirroring.

15.6 Configuring attack prevention

15.6.1 Preparing for configurations

Scenario

With the gradual increase in the scale of the network and the increasing popularity of applications, the requirements for network security and the security of network equipment are becoming higher and higher. In the network, there are a large number of malicious attack packets targeting network devices, causing excessive CPU usage of the device, degrading device performance, affecting normal services, and even causing system interruption. These messages need to be restricted to ensure the safe operation of the device.

Prerequisite

The interface is enabled.

15.6.2 Enabling attack prevention

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**defend ping-of-death enable**	Enable death prevention of Ping packet attacks.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config)#**defend land enable**	Enable attack prevention against TCP synchronization packets with the loopback address.
4	Raisecom(config)#**defend tcp-flag enable**	Enable prevention against TCP malformed packet attacks.
5	Raisecom(config)#**defend teardrop enable**	Enable prevention against teardrop packet attacks.
6	Raisecom(config)#**defend winnuke enable**	Enable prevention against WinNuke packet attacks.
7	Raisecom(config)#**defend icmp-redirect enable**	Enable prevention against ICMP redirection packet attacks.
8	Raisecom(config)#**defend icmp-unreachable enable**	Enable prevention against ICMP unreachable packet attacks.
9	Raisecom(config)#**defend icmp-forward enable**	Enable prevention against ICMP forwarding packet attacks.
10	Raisecom(config)#**defend fraggle enable**	Enable prevention against Fraggle packets attacks.
11	Raisecom(config)#**defend ip-source-route enable**	Enable prevention against Fraggle packets attacks.
12	Raisecom(config)#**defend trace enable**	Enable anti-Trace attacks.
13	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
14	Raisecom(config-port)#**defend ip-fragment enable**	Enable prevention against IP fragmented packet attacks.
15	Raisecom(config-port)#**defend smurf enable**	Enable prevention against smurf packet attacks on the interface.

15.6.3 Configuring prevention against traffic attacks

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**defend flood** { **tcp** | **udp** } { *source-ip-address mask-address* | **any** } [*source-port*] { *destination-ip-address mask-address* | **any** } [*dest-port*] *interface-type interface-number* { **to-cpu** | **forward** | **drop** }	Configure prevention against TCP/UDP traffic attacks based on IPv4 address.
3	Raisecom(config)#**defend flood** { **tcp** | **udp** } { *source-ipv6-address/m* | **any** } [*source-port*] { *destination-ipv6-address/m* | **any** } [*dest-port*] *interface-type interface-number* { **to-cpu** | **forward** | **drop** }	Configure prevention against TCP/UDP traffic attacks based on IPv6.
4	Raisecom(config)#**defend flood arp** { *source-mac mask-address* | **any** } { *dest-mac mask-address* | **any** } *interface-type interface-number* { **to-cpu** | **forward** | **drop** }	Configure prevention against ARP traffic attacks.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config)#**defend flood** *protocol-id* { *source-ip-address mask-address* | **any** } { *destination-ip-address mask-address* | **any** } { **to-cpu** | **forward** | **drop** }	Configure prevention against traffic attacks based on IPv4.
6	Raisecom(config)#**defend flood** *protocol-id* { *source-ip-address mask-address* | **any** } { *destination-ip-address mask-address* | **any** } { *interface-type interface-number* | **port-channel** *port-number* } { **to-cpu** | **forward** | **drop** }	Configure prevention against traffic attacks based on the interface and IPv4 address.
7	Raisecom(config)#**defend flood** *protocol-id* { *source-ipv6-addressn/mask* | **any** } { *destination-ipv6-address/mask* | **any** } { **to-cpu** | **forward** | **drop** }	Configure prevention against traffic attacks based on IPv6.
8	Raisecom(config)#**defend flood** *protocol-id* { *source-ipv6-address/mask* | **any** } { *destination-ipv6-address/mask* | **any** } { *interface-type interface-number* | **port-channel** *port-number* } { **to-cpu** | **forward** | **drop** }	Configure prevention against traffic attacks based on the interface and IPv6.
9	Raisecom(config)#**defend flood icmp** { *source-ip-address mask-address* | **any** } { *destination-ip-address mask-address* | **any** } [**type** *type-value*] [**code** *code-value*] [*interface-type interface-number* | **port-channel** *port-number*] { **to-cpu** | **forward** | **drop** }	Configure prevention against IPv4 ICMP traffic attacks.
10	Raisecom(config)#**defend flood icmp** { *source-ipv6-address/mask* | **any** } { *destination-ipv6-address/mask* | **any** } [**type** *type-value*] [**code** *code-value*] [*interface-type interface-number* | **port-channel** *port-number*] { **to-cpu** | **forward** | **drop** }	Configure prevention against IPv6 ICMP traffic attacks.
11	Raisecom(config)#**tcp syn-ack limit num** *number*	Limit the number of syn-ack packets in TCP connections.

15.7 Configuring ARP attack prevention

15.7.1 Preparing for configurations

Scenario

ARP anti-attack prevents attackers from sending fake ARP packets by impersonating users and gateways, and attacking devices by sending a large number of IP packets whose target IP addresses cannot be resolved.

Prerequisite

N/A

Copyright © Raisecom Technology Co., Ltd.

15.7.2 Default configurations

Function	Default value
The device only learns the status of the ARP entry requested by itself	Disable
ARP destination address check	Disable
ARP filtering	Disable
ARP solidification	Disable

15.7.3 Configuring ARP attack prevention

ARP attack prevention supports the configuration of Layer 3 Ethernet interfaces, sub-interfaces, and VLAN interfaces. This chapter only uses Layer 3 Ethernet interfaces for example to describe the configuration steps.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *unit-id/slot-id/port-id*	Enter Layer 3 Ethernet interface configuration mode.
3	Raisecom(config-port)#**arp learning strict enable**	Enable the device to learn the ARP table entry requested by itself only.
4	Raisecom(config-port)#**arp check-destination-ip enable**	Enable ARP destination address check.
5	Raisecom(config-port)#**arp filter** { **gratuitous** | **mac-illegal** | **tha-filled-request** }	Configure ARP filtering.
6	Raisecom(config-port)#**arp anti-attack entry-check** { **fixed-all** | **fixed-mac** | **send-ack** }	Fix ARP entries.
7	Raisecom(config-port)#**arp rate-limit** *value*	Configure the ARP rate limit.
8	Raisecom(config-port)#**arp validate mac** { **dest** | **source** [**dest**] }	Configure the MAC address for ARP validation.
9	Raisecom(config-port)#**exit**	Return to the global configuration mode.
10	Raisecom(config)#**arp active-ack enable**	Enable ARP active acknowledgement.
11	Raisecom(config)#**arp safe-guard enable**	Enable ARP bidirectional separation.
12	Raisecom(config)#**arp solicit-count** *value*	Configure the upper limit of sending broadcast ARP requests.

Copyright © Raisecom Technology Co., Ltd.

15.7.4 Checking configurations

No.	Command	Description
1	Raisecom#**show arp**	Show ARP configurations.
2	Raisecom#**show ip arp filter**	Show configurations of ARP filtering.

15.8 Configuring dynamic ARP inspection

15.8.1 Preparing for configurations

Scenario

Dynamic ARP inspection is used to prevent common ARP spoofing attacks in the network, and to isolate ARP packets from unsafe sources. Whether to trust ARP packets is achieved through the trust status of the interface, and whether it meets the requirements is achieved through the binding table.

Prerequisite

Before configuring dynamic ARP inspection, if there are DHCP users, you need to enable DHCP snooping.

15.8.2 Configuring trusted interface of dynamic ARP inspection

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**ip arp-inspection trust**	Configure the interface as a trusted interface. You can use the **no ip arp-inspection trust** command to configure the interface to a non-trusted interface.

15.8.3 Configuring static binding of dynamic ARP inspection

Dynamic ARP inspection is used to prevent common ARP spoofing attacks on the network, and to isolate ARP packets from unsafe sources. Whether it meets the requirements is achieved through the binding table.

The static binding method refers to manually configuring the binding relationship. After static ARP binding is enabled, static ARP detection binding rules configured on the device take effect immediately.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip arp-inspection static-config**	Enable global static binding.
3	Raisecom(config)#**ip arp-inspection binding** *ip-address* [*mac-address*] [**vlan** *vlan-id*] *interface-type interface-number*	Configure static binding rules.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
5	Raisecom(config-port)#**ip arp-inspection binding-number** *binding-number*	Configure the number of static ARP binding tables on the interface.

15.8.4 Configuring dynamic binding of dynamic ARP inspection

Dynamic ARP inspection is used to prevent common ARP spoofing attacks on the network. Dynamic ARP inspection isolates ARP packets from insecure sources.

In dynamic binding mode, a dynamic binding relationship is generated through cooperation with DHCP Snooping. When the DHCP Snooping entry changes, the dynamic ARP inspection will also update the dynamic binding entry synchronously. After dynamic DHCP Snooping binding is enabled, the content of the DHCP Snooping binding table will be learned into the dynamic ARP detection binding table, and the content of the DHCP Snooping binding table will be learned later.

To enable dynamic binding of dynamic ARP inspection, use the **ip dhcp snooping** command to enable DHCP snooping.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip arp-inspection dhcp-snooping**	Enable global dynamic binding.

15.8.5 Configuring protection VLAN of dynamic ARP inspection

Configure dynamic ARP inspection to protect the specified VLAN. ARP packets in the untrusted interface VLAN will be protected. Only ARP packets that meet the binding table rules are allowed to pass, and the rest are discarded.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip arp-inspection dhcp-snooping**	Enable global dynamic binding.

Copyright © Raisecom Technology Co., Ltd.

15.8.6 Checking configurations

Step	Command	Description
1	Raisecom#**show ip arp-inspection**	Show configurations of dynamic ARP.
2	Raisecom#**show ip arp-inspection binding** [*interface-type interface-number*]	Show configurations of the dynamic ARP binding table.

15.9 Configuring URPF

15.9.1 Preparing for configurations

Scenario

URPF checks the validity of the source address of the message to prevent network attacks based on source address spoofing. If the check passes, the message is allowed to pass; otherwise, the source address is considered to be forged and the message is discarded.

Prerequisite

N/A

15.9.2 Configuring URPF

URPF supports the configuration of Layer 3 Ethernet interfaces, VLAN interfaces and Ethernet sub-interfaces. This chapter only uses Layer 3 Ethernet interfaces for example to describe

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *unit-id/slot-id/port-id*	Enter Layer 3 Ethernet interface configuration mode.
3	Raisecom(config-gigaethernet*/*/*)#{ **ip** | **ipv6** } **urpf** { **loose** | **strict** } [**allow-default-route**]	Configure URPF on the interface.

15.9.3 Checking configurations

N/A

Copyright © Raisecom Technology Co., Ltd.

15.10 Configuring 802.1x

15.10.1 Preparing for configurations

Scenario

To achieve access authentication for LAN users and solve the security problems of access users, you need to configure 802.1x authentication on the device.

For users who have passed authentication, they are allowed to access network resources; if authentication fails, the user cannot access network resources. Through the authentication control of the user access interface, the purpose of user management is achieved.

Prerequisite

Before configuring 802.1x authentication, if you use a RADIUS authentication server, you need to complete the following tasks:

- Configure the RADIUS server IP address and RADIUS public key.
- The device can Ping with the RADIUS server.

15.10.2 Default configurations

Function	Default value
Global 802.1x	Disable
Interface 802.1x	Disable
Global authentication mode	**chap**
Interface access control mode	**auto**
Interface authentication method	**portbased**
RADIUS server expiration timer	5s
802.1x re-authentication	Disable
802.1x re-authentication timer	3600s
802.1x quiet timer	60s
Retransmission timer for request packets	30s
Requester timeout timer	30s
Maximum number of users	512

Copyright © Raisecom Technology Co., Ltd.

15.10.3 Configuring basic functions of 802.1x

- 802.1x conflicts with STP on the same interface. You cannot enable them concurrently.
- Only one user authentication request is processed on an interface at a time.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**dot1x enable**	Enable global 802.1x.
3	Raisecom(config)#**dot1x authentication-method** { **chap** | **pap** | **eap** }	Configure global authentication mode.
4	Raisecom(config)#**dot1x auth-mode** { **radius** | **local** | **tacacs+** }	Configure 802.1x authentication mode.
5	Raisecom(config)#**dot1x free-ip** *ip-address* [*ip-mask* | *mask-length*]	Configure the IP address range that can be accessed by 802.1x terminal users who fail to be authenticated or exits authorization.
6	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 2 physical interface configuration mode.
7	Raisecom(config-gigaethernet1/1/*)#**dot1x enable**	Enable interface 802.1x.
8	Raisecom(config-gigaethernet1/1/*)#**dot1x auth-control** { **auto** | **authorized-force** | **unauthorized-force** }	Configure the interface access control mode.
9	Raisecom(config-gigaethernet1/1/*)#**dot1x auth-method** { **gigaethernet1/1/*based** | **macbased** }	Configure the interface authentication mode.
10	Raisecom(config-gigaethernet1/1/*)#**dot1x keepalive** { **enable** | **disable** }	Enable/Disable port 802.1x handshake.
11	Raisecom(config-gigaethernet1/1/*)#**dot1x max-user** *user-number*	Configure the maximum number of users that can be authenticated on the 802.1x port.
12	Raisecom(config-gigaethernet1/1/*)#**dot1x guest-vlan** *vlan-id*	Configure the 802.1x Guest VLAN for the specified port.
13	Raisecom(config-gigaethernet1/1/*)#**dot1x auth-free voice-vlan**	Configure the authentication-free function for voice terminals on designated ports.

If 802.1x is not enabled in the global or interface mode, the interface control mode of the 802.1x is the mandatory interface authorization mode.

Copyright © Raisecom Technology Co., Ltd.

15.10.4 Configuring 802.1x re-authentication

The re-authentication function is initiated for authorized users, so before enabling the re-authentication function, you should ensure that global and interface 802.1x are enabled. The interface in authorized state remains in the authorized state during the re-authentication process. If the re-authentication fails, it enters the non-authorized state.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config-gigaethernet1/1/*)#**dot1x reauthentication enable**	Enable 802.1x re-authentication.

15.10.5 Configuring 802.1x timer

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config-gigaethernet1/1/*)#**dot1x timer reauth-period** *reauth-period*	Configure the re-authentication timer.
4	Raisecom(config-gigaethernet1/1/*)#**dot1x timer quiet-period** *second*	Configure the silent timer time.
5	Raisecom(config-gigaethernet1/1/*)#**dot1x timer supp-timeout** *supp-timeout*	Configure the applicant authentication timeout timer.
6	Raisecom(config-gigaethernet1/1/*)#**dot1x timer server-timeout** *server-timeout*	Configure the timeout timer of the authentication server.
7	Raisecom(config-gigaethernet1/1/*)#**dot1x timer keepalive-period** *second*	Configure the port 802.1x retransmission interval of Keepalive packets.
8	Raisecom(config-gigaethernet1/1/*)#**dot1x timer tx-period** *second*	Configure the Request/Identity request packet timeout timer.

15.10.6 Checking configurations

Step	Command	Description
1	Raisecom#**show dot1x** *interface-type interface-number*	Show interface 802.1x configurations.
2	Raisecom#**show dot1x** *interface-type interface-number* **statistics**	Show interface 802.1x statistics.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom#**show dot1x** *interface-type interface-number* **user**	Show user information for interface 802.1x authentication.
4	Raisecom#**show dot1x free-ip**	Show the IP address segment that can be accessed by 802.1x terminal users who have failed authentication or have exited authorization.

15.10.7 Maintenance

Command	Description
Raisecom(config)#**clear dot1x** *interface-type interface-number* **statistics**	Clear interface 802.1x statistics.

15.11 Configuring password management

15.11.1 Preparing for configurations

Scenario

The MD5 encryption key is assisted by offline encryption tools, and is used for protocols such as OSPF that need to support MD5 encryption.

Prerequisite

N/A

15.11.2 Configuring MD5 encryption keys

You need to enter the plain text for MD5 authentication on the device and the cipher text can be directly generated by encryption on the device.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**md5 encrypt keystring** *string*	Configure the MD5 encryption key to encrypt the plaintext into ciphertext.

15.11.3 Checking configurations

N/A

Copyright © Raisecom Technology Co., Ltd.

15.12 Configuration examples

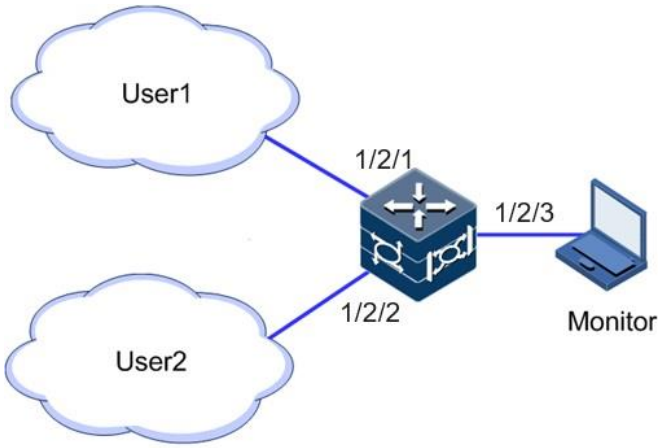
15.12.1 Example for configuring port mirroring

Networking requirements

As shown in Figure 15-1, user network 1 is connected to RAX721 through GE interface 1/2/1, and user network 2 is connected to GE interface 1/2/2. The network maintenance personnel hope to monitor user network 1 through the monitoring equipment and capture abnormal data flow to analyze the cause of the problem and solve it in time.

The data monitoring equipment is connected to the RAX721 through GE interface 1/2/3.

Figure 15-1 Configuring port mirroring



Configuration steps

Step 1 Create port mirroring group 1.

```
Raisecom#config
Raisecom(config)#mirror-group 1
```

Step 2 Configure GE interface 1/2/3 as a monitoring interface.

```
Raisecom(config)#interface gigaethernet 1/2/3
Raisecom(config-gigaethernet1/2/3)#mirror-group 1 monitor-port
Set successfully.
```

Step 3 Configure GE interface 1/2/1 as the mirroring source interface, and the mirroring rule is to mirror incoming packets.

```
Raisecom(config)#interface gigaethernet 1/2/1
```


Copyright © Raisecom Technology Co., Ltd.

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

Checking results

Use the **show mirror-group** command to see whether port mirroring configurations are correct.

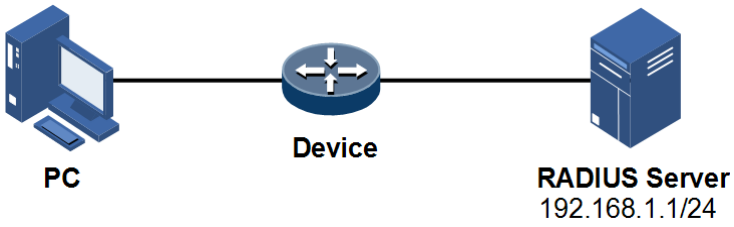
```
Raisecom#show mirror-group
Mirror Group 1:
Monitor Port:
   gigaethernet1/2/3
Source Port:
   gigaethernet1/2/1            : ingress
Reflector Port:
Remote Vlan:
```

15.12.2 Example for configuring RADIUS

Networking requirements

As shown in Figure 15-2, to control user access to the device, you need to deploy RADIUS authentication and accounting on the Device to authenticate users who log in to the Device and record their operations. It is required that the update message sending interval is 2 minutes and the user will be offline when accounting fails.

Figure 15-2 RADIUS application



Configuration steps

Step 1 Configure AAA.

```
Raisecom#aaa
Raisecom(aaa)#aaa accounting login enable
Raisecom(aaa)#aaa accounting fail offline
Raisecom(aaa)#aaa accounting update 2
Raisecom(aaa)#domain default
Raisecom(aaa-default)#user login radius-user
Raisecom(aaa-default)#end
```


Copyright © Raisecom Technology Co., Ltd.

Step 2 Authenticate login users through RADIUS.

```
Raisecom#radius 192.168.1.1
Raisecom#radius-key raisecom
```

Step 3 Account login users through RADIUS.

```
Raisecom#radius accounting-server 192.168.1.1
Raisecom#radius accounting-server key raisecom
```

Checking results

Use the **show radius-server** command to show whether RADIUS configurations are correct.

```
Raisecom#show radius-server
Radius timeout(second)            :3
Authentication server IP          : 192.168.1.1
Authentication port              :1812
Backup authentication server IP     :
Backup authentication port         :1812
Authentication Server Key          : I+NNa9uluaix
Backup authentication server Key    :--
Accounting server IP              :
Accounting server port            :1813
Backup accounting server IP        :
Backup accounting port            :1813
Accounting server Key             : orMCKszV2X38
Backup Accounting server Key       :--
Authentation source ip            :
Authentation backup source ip      :
Accounting source ip              :
Accounting backup source ip        :
NAS IP Address                   :--
Accounting NAS IP Address          :--
```

Use the **show aaa** command to show whether RADIUS accounting configurations are correct.

```
Raisecom#show aaa
Accounting login            : enable
Accounting Mode        :--
Update interval(minute)      :2
Accounting fail policy       :offline
authorization fail policy    :15
Command authorization       :disable
```


Copyright © Raisecom Technology Co., Ltd.

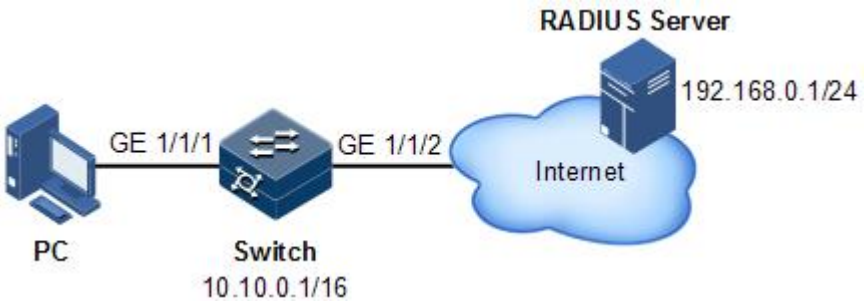
15.12.3 Example for configuring 802.1x

Networking requirements

To enable users to access the external network, as shown in Figure 15-3, configure 802.1x authentication on the device. The specific requirements are as follows:

- The IP address of the device is 10.10.0.1, the mask is 255.255.0.0, and the default gateway address is 10.10.0.2.
- The RADIUS server is used for authentication and authorization. The IP address of the RADIUS server is 192.168.0.1, and the password is raisecom.
- The interface control mode is the protocol authorization mode.
- After the authentication is passed, the re-authentication process can be initiated automatically after 600s.

Figure 15-3 802.1x networking



Configuration steps

Step 1 Configure the IP address and RADIUS server address of the device.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 10.10.0.1 255.255.0.0
Raisecom(config-vlan1)#exit
Raisecom(config)#ip route 0.0.0.0 0.0.0.0 10.10.0.2
Raisecom(config)#exit
Raisecom#radius 192.168.0.1
Raisecom#radius-key Raisecom
```

Step 2 Enable global and interface 802.1x authentication.

```
Raisecom#config
Raisecom(config)#dot1x enable
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#dot1x enable
```


Copyright © Raisecom Technology Co., Ltd.

Step 3 (Optional) configure the authorization mode as protocol authorization. By default, authentication is required and no configuration is required.

```
Raisecom(config-gigaethernet1/1/1)#dot1x auth-control auto
```

Step 4 Enable re-authentication and set the re-authentication time to 600s

```
Raisecom(config-gigaethernet1/1/1)#dot1x reauthentication enable
Raisecom(config-gigaethernet1/1/1)#dot1x timer reauth-period 600
```

Checking results

Use the **show dot1x** command to show 802.1x configurations.

```
Raisecom#show dot1x gigaethernet 1/1/1
802.1x Global Admin State: enable
802.1x Authentication Method: chap
802.1x Authentication Mode: radius
802.1x allowed max user number: 512
-------------------------------------------------------
Port gigaethernet 1/1/1
-------------------------------------------------------
802.1X Port Admin State: Enable
PAE: Authenticator
PortMethod: Portbased
PortControl: Auto
ReAuthentication: Enable
KeepAlive: Enable
QuietPeriod: 60(s)
ServerTimeout: 5(s)
SuppTimeout: 30(s)
ReAuthPeriod: 600(s)
TxPeriod: 30(s)
KeepalivePeriod: 60(s)
MaxUserNum: 512
```


Copyright © Raisecom Technology Co., Ltd.

16 Reliability

This chapter describes principles and configuration procedures of network reliability, as well as related configuration examples, including following sections:

- Configuring link aggregation
- Configuring interface backup
- Configuring PW redundancy
- Configuring VRRP
- Configuring VRRPv3
- Configuring ERPS
- Configuring MPLS linear protection
- Configuring HA hot backup
- Configuring EVPL dual-homing protection
- Maintenance
- Configuration examples

16.1 Configuring link aggregation

16.1.1 Preparing for configurations

Scenario

When greater bandwidth and high reliability are needed for network links, you can configure manual or static LACP link aggregation.

Link aggregation aggregates multiple physical Ethernet interfaces into a logical link to provide load sharing of uplink and downlink traffic among member interfaces. This helps increase the bandwidth. In addition, connection reliability is enhanced when member interfaces back up for each other dynamically.

Prerequisite

Configure physical parameters of the interface and make the physical layer Up.

Copyright © Raisecom Technology Co., Ltd.

16.1.2 Configuring manual link aggregation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**link-aggregation** load-sharing mode { **all** | **dip** | **dmac** | **sip** | **smac** | **sip** | **sxordip** | **sxordmac** }	Configuring the load-sharing mode of the link aggregation. By default, the system adopts the **all** mode.
3	Raisecom(config)#interface **port-channel** *channel-number* Raisecom(config-port)#**mode manual**	Create a link aggregation group. Configure the working mode of the link aggregation group to manual aggregation.
4	Raisecom(config)#interface *interface-type interface-number* Raisecom(config-port)#**portswitch**	Enter physical interface configuration mode.
5	Raisecom(config-port)#**port-channel** *group-id*	Add member interfaces to the LAG.
6	Raisecom(config-port)#**exit**	Return to global configuration mode.

Note

Do not configure services on interfaces, which are added to the LAG.

16.1.3 Configuring static LACP link aggregation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lacp system-priority** *priority*	(Optional) configure the system LACP priority. The smaller the value is, the higher the system LACP priority is. The end with a higher system LACP priority is the active end. LACP selects the active interface and standby interface based on configurations on the active end. If the system LACP priorities are identical, select the one with a smaller MAC address as the active end. By default, the system LACP priority is 32768.
3	Raisecom(config)#**lacp timeout** { **fast** | **slow** }	(Optional) configure the LACP timeout mode.
4	Raisecom(config)#**interface port-channel** *channel-number*	Enter LAG configuration mode.
5	Raisecom(config-port-channel*)#**mode lacp**	Configure the working mode of the LAG to static LACP link aggregation.
6	Raisecom(config-port-channel*)#{ **max-active** | **min-active** } **links** *threshold*	(Optional) configure the maximum/minimum number of active links of the LACP LAG.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
7	Raisecom(config-port-channel1)#**lacp priority preempt enable**	(Optional) enable priority preemption of the link aggregation group.
8	Raisecom(config-port-channel*)#**exit**	Return to global configuration mode.
9	Raisecom(config)#**link-aggregation load-sharing mode** { **all** | **dip** | **dmac** | **sip** | **smac** | **sip** | **lable** | **sxordip** | **sxordmac** }	Configure load balancing mode of link aggregation. By default, the system adopts the **all** mode.
10	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.
11	Raisecom(config-port)#**portswitch**	Configure the interface to switch mode.
12	Raisecom(config-port)#**port-channel** *channel-number*	Add the interface to the LAG.
13	Raisecom(config-port)#**lacp mode** { **active** | **passive** }	(Optional) configure the LACP mode of member interfaces. By default, the LACP mode is active. LACP connection fails if both ends of a link are in passive mode.
14	Raisecom(config-port)#**lacp port-priority** *priority*	(Optional) configure the interface LACP priority. The interface LACP priority affects the selection of LACP default interface. The smaller the number is, the higher the priority is. By default, it is 32768.
15	Raisecom(config-port)#**exit**	Exit 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 selects a default interface based on following conditions in order: whether the neighbor is discovered, maximum interface speed, the highest interface LACP priority, and the smallest interface ID. The default interface is in active status. Interfaces, which have the same speed, peer device, and operation key of the operation key with the default interface, are in active status. Other interfaces are in standby status.
- When the number of member interfaces in the static LAG reaches the maximum number of active interfaces, the later-added interfaces cannot become member interfaces even they meet all requirements on member interfaces. This helps make traffic of current member interfaces continuous.

Copyright © Raisecom Technology Co., Ltd.

16.1.4 Configuring manual backup link aggregation

Configuring backup link aggregation group interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port-channel** *channel-number*	Enter aggregation group configuration mode.
3	Raisecom(config-port-channel*)#**mode manual backup**	Configure the working mode of the link aggregation group interface to backup.
4	Raisecom(config-port-channel*)#**manual backup action** { **block** | **shutdown** } Raisecom(config-port-channel*)#**exit**	Configure the backup interface status of the link aggregation group to block or shutdown.

Configuring active link aggregation group interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port-channel** *channel-number*	Enter aggregation group configuration mode.
3	Raisecom(config-port-channel*)#**master-port** *interface-type interface-number*	Configure the active interface of link aggregation.
4	Raisecom(config-port-channel*)#**restore-mode** { **non-revertive** | **revertive** [**restore-delay** *second*] }	Configure the restoration mode and restoration delay of the LAG. By default, the restoration mode is non-revertive.
5	Raisecom(config-port-channel*)#**exit**	Return to global configuration mode.

Adding member interfaces

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**portswitch**	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config-port)#**port-channel** *channel-number*	Add member interfaces to the link aggregation group.
4	Raisecom(config-port)#**exit**	Return to global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

16.1.5 Configuring static LACP active/standby link aggregation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lacp system-priority** *system-priority*	(Optional) configure the system LACP priority. The smaller the value is, the higher the system LACP priority is. The end with a higher system LACP priority is the active end. LACP selects the active interface and standby interface based on configurations on the active end. If the system LACP priorities are identical, select the one with a smaller MAC address as the active end. By default, it is configured to 32768.
3	Raisecom(config)#**lacp timeout** { **fast** | **slow** }	(Optional) configure the LACP timeout mode.
4	Raisecom(config)#**interface port-channel** *channel-number*	Enter aggregation group configuration mode.
5	Raisecom(config-port-channelif)#**mode lacp backup**	Configure the working mode of the LAG to static LACP backup link aggregation.
6	Raisecom(config-port-channelif)#**master-port** *interface-type interface-number*	Configure the master interface of link aggregation.
7	Raisecom(config-port-channelif)#**restore-mode** { **non-revertive** | **revertive** [**restore-delay** *second*] }	Configure the restoration mode and restoration delay of the LAG. By default, the restoration mode is non-revertive.
8	Raisecom(config-port-channelif)#**exit**	Return to global configuration mode.
9	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**portswitch**	Enter Layer 2 physical interface configuration mode.
10	Raisecom(config-port)#**port-channel** *channel-number*	Add Layer 2 physical interfaces to the LAG.
11	Raisecom(config-port)#**lacp mode** { **active** | **passive** }	(Optional) configure the LACP mode of member interfaces. By default, the LACP mode is active. LACP connection fails if both ends of a link are in passive mode.
12	Raisecom(config-port)#**lacp port-priority** *port-priority*	(Optional) configure the interface LACP priority. The interface LACP priority affects the selection of the default LACP interface. The smaller the number is, the higher the priority is. By default, it is 32768.
13	Raisecom(config-port)#**exit**	Return to global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

16.1.6 Checking configurations

No.	Command	Description
1	Raisecom#**show lacp internal** [**detail**]	Show local system LACP interface status, identifier, interface priority, management key, operation key, and interface status machine.
2	Raisecom#**show lacp neighbor** [**detail**]	Show neighbor LACP information, including the identifier, interface priority, device ID, Age, operation key ID, interface ID, and interface status machine.
3	Raisecom#**show lacp statistics** [*interface-type interface-number*]	Show interface LACP statistics, including the total number of received LACP packets, number of received and transmitted Marker packets, number of received and transmitted Marker Response packets, and number of error packets.
4	Raisecom#**show lacp sys-id**	Show global status of local system LACP, device ID, LACP priority, and MAC address.
5	Raisecom#**show port-channel**	Show whether the current system is enabled with link aggregation mode or load balancing mode, and show the information about member interfaces and currently-active member interfaces in all current LAGs. **Note** Currently active member interfaces refers to interfaces in Active status in the LAG.

16.2 Configuring interface backup

16.2.1 Preparing for configurations

Scenarios

In a dual-uplink networking scenario, you can realize redundancy backup of the active/standby link and fast switching of services through interface backup, thus improving service reliability.

Prerequisite

N/A

16.2.2 Configuring interface backup group

Creating port or port + VLAN port backup group

No.	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**portswitch**	Enter interface configuration mode.
3	Raisecom(config-port)#**port backup** *interface-type interface-number* [**vlanlist** *vlanlist* [**primaryvlan** *vlanid*] [**md-level** *level-value*]] Raisecom(config-port)#**exit**	Create a backup interface based on interface or interface + VLAN for the primary interface. Interface-based interface backup supports switching or restoring services of the specified VLAN or all services on the interface.
4	Raisecom(config-port)#**port backup restore-mode** { **non-revertive** | **revertive** [**restore-delay** *delay-time*] }	Configure the restoration mode and restoration delay of interface backup.
5	Raisecom(config-port)#**port backup fault-detect cfm**	Configure the fault detection mode of interface backup. CFM detection is not supported for port backup in port + VLAN separate delivery mode.
6	Raisecom(config-port)#**port backup** *interface-type interface-number* **force-switch** [**vlan** *vlan-id*]	(Optional) forcedly switch services to the backup link. The forced switching of the specified VLAN is only applicable to the port backup group in single delivery mode.

Creating port backup group in port + VLAN separate delivery mode

No.	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**portswitch**	Enter interface configuration mode.
3	Raisecom(config-port)#**port backup** *interface-type interface-number* **vlanlist** *vlanlist* **separate**	Under the primary interface, create a port backup group based on port + VLAN in a separate delivery mode.
4	Raisecom(config-port)#**port backup restore-mode** { **non-revertive** | **revertive** [**restore-delay** *delay-time*] }	Configure port backup recovery mode and recovery delay.
5	Raisecom(config-port)#**port backup** *interface-type interface-number* **force-switch** [**vlan** *vlan-id*]	(Optional) forcedly switch services to the backup link. The forced switching of the specified VLAN is only applicable to the port backup group in the single delivery mode.

16.2.3 Checking configurations

No.	Item	Description
1	Raisecom#**show port backup**	Show basic information about interface backup.

Copyright © Raisecom Technology Co., Ltd.

No.	Item	Description
2	Raisecom#**show port backup pb**	Show information about the interface backup group.
3	Raisecom#**show port backup group**	Show interface status of the interface backup group.

16.3 Configuring PW redundancy

16.3.1 Preparing for configurations

Scenario

PW redundancy is used on the networking scenario of CE connecting to 3 PEs asymmetrically, multiple CEs connecting to multiple PEs, and CE accessing a networking with MS-PW, and so on.

Prerequisite

A PW is created.

16.3.2 Configuring PW redundancy

Both Layer 3 physical interface and sub-interface support PW redundancy. When the Layer 3 physical interface or sub-interface at the AC end fails, it will trigger the PW redundancy protection switching. The following contents describe the configuration steps based on Layer 3 physical interfaces.

Creating primary/secondary PW

For details, refer to section 11.1 Configuring VPWS.

Configuring dynamic BFD

For details, refer to section 14.3.3 Configuring BFD for PW.

Configuring PW redundancy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**mode l2**	Configure the VPN mode on Layer 3 physical interface to L2VPN. By default, it is L3VPN.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
4	Raisecom(config-port)#**mpls l2vpn redundancy** { **independent** | **master** [**switch-mode** { **non-revertive** | **revertive** [**wtr-time** *wtr-time*] }]	Configure L2VPN to support PW redundancy protection based on VPWS.
5	Raisecom(config-port)#**mpls l2vpn switchover**	(Optional) manually switch the service flow from the primary PW to the secondary PW.

16.3.3 Configuring VPLS PW Redundancy

VPLS PW Redundancy is the PW Redundancy in the VPLS scenario, used to implement fast convergence of the VPLS network and to shorten the service interruption time due to faults.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls vsi** *vsi-name* **static**	Create a VSI, and enter VIS configuration mode.
3	Raisecom(config-vsi)#**pw protect-group** *groupname*	Create a VPLS PW Redundancy protection group, and enter protection group configuration mode.
4	Raisecom(config-vsi-protect-group)#**mpls peer** *peer-ip* [**vcid** *vc-id*] [**backup**]	Configure the master/slave PW in the protection group.
5	Raisecom(config-vsi-protect-group)#**pw-redundancy** { **master** [**switch-mode** { **non-revertive** | **revertive** [**wtr-time** *time*] }] | **independent** }	Configure the redundancy mode, switching mode, and WTR time.
6	Raisecom(config-vsi-protect-group)#**mpls l2vpn switchover**	(Optional) manually perform master/salve PW switching.

16.3.4 Checking configurations

No.	Command	Description
1	Raisecom#**show mpls l2vc**	Show configurations of PW redundancy.
2	Raisecom#**show vsi** [*vsiname*] **protect-group** [*groupname*]	Show configurations of the VPLS PW Redundancy protection group.

Copyright © Raisecom Technology Co., Ltd.

16.4 Configuring VRRP

16.4.1 Preparing for configurations

Scenario

VRRP forms a virtual routing device by adding devices with gateway functions to the backup group, and selects the Master device to undertake the forwarding task through VRRP election. The host in the network only needs to configure the virtual routing device as the default gateway.

VRRP effectively improves the reliability of the network and simplifies the host configuration. You can also implement load sharing of network traffic by configuring multiple VRRP backup groups.

Prerequisite

Before configuring VRRP, you need to configure the network layer attributes of the interface to connect the network.

16.4.2 Creating and enabling VRRP

The VRRP backup group supports Layer 3 Ethernet interfaces, VLAN interfaces, aggregation group interface, and Layer 3 Ethernet sub-interfaces. This chapter only uses Layer 3 Ethernet interfaces for example to describe the configuration steps.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type unit-id/slot-id/port-id*	Enter Layer 3 Ethernet interface configuration mode.
3	Raisecom(config-gigaethernet1/1/*)#**vrrp** *group-id* **ip** *ip-address*	Create a VRRP backup group and add a virtual IP address to the backup group.
4	Raisecom(config-gigaethernet1/1/*)#**vrrp** *group-id* **enable**	Enable the VRRP backup group.

Caution

- The virtual IP addresses of devices in the same backup group must be the same.
- Only one virtual IPv4 address can be configured for one backup group.
- one backup group can only be configured under one interface of the device.

16.4.3 Configuring VRRP backup group

The VRRP backup group supports Layer 3 Ethernet interfaces, aggregation group interfaces, VLAN interfaces, and Layer 3 Ethernet sub-interfaces. This chapter only uses Layer 3 Ethernet interfaces for example to describe the configuration steps.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *unit-id/slot-id/port-id*	Enter Layer 3 Ethernet interface configuration mode.
3	Raisecom(config-gigaethernet1/1/*)#**vrrp** *group-id* **description** *string*	Configure the description of the VRRP backup group.
4	Raisecom(config-gigaethernet1/1/*)#**vrrp** *group-id* **priority** *value*	Configure the priority of the VRRP backup group.
5	Raisecom(config-gigaethernet1/1/*)#**vrrp** *group-id* **preempt** [**delay-time** *second*]	Configure the VRRP backup group to preempt mode and configure the preemption delay time.
6	Raisecom(config-gigaethernet1/1/*)#**vrrp** *group-id* **timers advertise-interval** *period*	Configure the interval for the VRRP backup group to send packets.

Caution

- Devices in the same VRRP backup group must be consistent in the interval for sending VRRP notification messages. If the time interval is inconsistent, it will cause a configuration error, the devices in the group will not communicate with each other, and will migrate to the Master state, resulting in VRRP failure.
- In the backup group, the device that provides the virtual IP address, namely, the IP owner, has a priority of 255, and its priority is not configurable.

16.4.4 Configuring VRRP Ping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**vrrp ping**	Enable VRRP Ping, that is, the virtual IP address of the VRRP backup group can be pinged.

16.4.5 Configuring VRRP Trap

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**vrrp-traps enable**	Enable VRRP Trap.

Copyright © Raisecom Technology Co., Ltd.

16.4.6 Configuring VRRP monitoring interface

The VRRP monitoring interface supports Layer 3 Ethernet interfaces, aggregation group interfaces, VLAN interfaces, and Layer 3 Ethernet sub-interfaces. This chapter only uses Layer 3 Ethernet interfaces for example to describe the configuration steps.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *unit-id/slot-id/port-id*	Enter Layer 3 Ethernet interface configuration mode.
3	Raisecom(config-gigaethernet1/1/*)#**vrrp** *group-id* **bfd-session** *session-id*	Bind sessions to VRRP backup groups.
4	Raisecom(config-gigaethernet1/1/*)#**vrrp** *group-id* **track** *interface-type interface-number* [**reduced** *priority*]	Configure the track function of the VRRP backup group.

16.4.7 Configuring BFD for VRRP

VRRP fast switching supports Layer 3 Ethernet interfaces, aggregation group interfaces, VLAN interfaces, and Layer 3 Ethernet sub-interfaces. This chapter only uses Layer 3 Ethernet interfaces for example to describe the configuration steps.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type unit-id/slot-id/port-id*	Enter Layer 3 Ethernet interface configuration mode.
3	Raisecom(config-gigaethernet*/*/*)#**vrrp** *group-id* **track bfd-session** *session-id* [**increased** *priority* | **reduced** *priority*]	Configure the VRRP backup group to monitor the BFD session to achieve the purpose of fast switching.

16.4.8 Checking configurations

No.	Command	Description
1	Raisecom#**show vrrp interface** { *interface-type unit-id/slot-id/port-id* | **vlan** *vlan-id* | **port-channel** *channel-number* } [*group-id*]	Show VRRP configurations and status on the interface.
2	Raisecom#**show vrrp interface** { *interface-type unit-id/slot-id/port-id* | **vlan** *vlan-id* | **port-channel** *channel-number* } [*group-id*] **statistics**	Show global statistics and VRRP statistics on the interface.
3	Raisecom#**show vrrp** [*group-id*]	Show configurations of all VRRP backup groups or a specified VRRP backup group.
4	Raisecom#**show vrrp** [*group-id*] **track**	Show VRRP fault tracking information.

Copyright © Raisecom Technology Co., Ltd.

16.4.9 Maintenance

Command	Description
Raisecom#**clear vrrp** [**interface** { *interface-type unit-id/slot-id/port-id* | **vlan** *vlan-id* | **port-channel** *channel-number* } [*group-id*]] **statistics**	Clear statistics of all VRRP backup groups or a specified VRRP backup group.

16.5 Configuring VRRPv3

16.5.1 Preparing for configurations

Scenario

VRRPv3 forms a virtual routing device by adding devices with a gateway function to the backup group, and selects the Master device to undertake the forwarding task through the VRRPv3 mechanism. The host in the network only needs to configure the virtual routing device as the default gateway.

VRRPv3 effectively improves the reliability of the network and simplifies the host configuration. You can also implement load sharing of network traffic by configuring multiple VRRP backup groups.

Prerequisite

Before configuring VRRPv3, you need to configure the network layer attributes of the interface to connect the network.

16.5.2 Default configurations

VRRPv3 default configurations:

Function	Default value
VRRP trap status	Enable
VRRP group on the interface	no
VRRP backup group description	no
VRRP backup group status	Enable
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
VRRP trap status under the IP interface	Enable

Copyright © Raisecom Technology Co., Ltd.

Function	Default value
Ping status of the virtual IP address of the VRRP backup group	Enable

16.5.3 Creating and enabling VRRPv3

The VRRPv3 backup group supports Layer 3 Ethernet interfaces, aggregation group interfaces, VLAN interfaces, and Layer 3 Ethernet sub-interfaces. This chapter only uses Layer 3 Ethernet interfaces for example to describe the configuration steps.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type unit-id/slot-id/port-id*	Enter Layer 3 Ethernet interface configuration mode.
3	`Raisecom(config-gigaethernet1/1/*)#vrrp6` *group-id* `ipv6` *ipv6-address*	Create a VRRPv3 backup group and add a virtual IPv6 address to the backup group. The virtual IPv6 address must be in the same network segment as the interface IPv6 address.
4	`Raisecom(config-gigaethernet1/1/*)#vrrp6` *group-id* `enable`	Enable the VRRPv3 backup group.

Caution

- The virtual IPv6 addresses of devices in the same backup group must be the same.
- One backup group can only be configured with one virtual IPv6 link-local address, and 15 virtual IPv6 global unicast addresses can be configured.
- One backup group can only be configured under one interface of the device.

16.5.4 Configuring VRRPv3 backup group

The VRRPv3 backup group supports Layer 3 Ethernet interfaces, aggregation group interfaces, VLAN interfaces, and Layer 3 Ethernet sub-interfaces. This chapter only takes Layer 3 Ethernet interfaces for example to describe the configuration steps.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type unit-id/slot-id/port-id*	Enter Layer 3 Ethernet interface configuration mode.
3	`Raisecom(config-gigaethernet1/1/*)#vrrp6` *group-id* `description` *string*	Configure the description of the VRRPv3 backup group.
4	`Raisecom(config-gigaethernet1/1/*)#vrrp6` *group-id* `priority` *priority*	Configure the priority of the VRRPv3 backup group.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
5	Raisecom(config-gigaethernet1/1/*)#**vrrp6** *group-id* **preempt** [**delay-time** *time*]	Configure the VRRPv3 backup group to preempt mode and configure the preemption delay time.
6	Raisecom(config-gigaethernet1/1/*)#**vrrp6** *group-id* **timers advertise-interval** *period*	Configure the interval for the VRRPv3 backup group to send packets.

Caution

- Devices in the same VRRPv3 backup group must be consistent in the interval for sending VRRPv3 notification messages. If the time interval is inconsistent, it will cause a configuration error, the devices in the group will not communicate with each other, and will migrate to the Master state, resulting in VRRPv3 failure.
- In the backup group, the device that provides the virtual IPv6 address, namely, the IP owner, has a priority of 255, and its priority is not configurable.

16.5.5 Configuring VRRPv3 PING

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**vrrp ping**	Enable VRRPv3 PING, that is, the virtual IPv6 address of the VRRPv3 backup group can be pinged.

16.5.6 Configuring VRRPv3 Trap

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**vrrp-traps enable**	Enable VRRPv3 Trap.

16.5.7 Configuring VRRPv3 monitoring interface

The VRRP monitoring interface supports Layer 3 Ethernet interfaces, aggregation group interfaces, VLAN interfaces, and Layer 3 Ethernet sub-interfaces. This chapter only uses Layer 3 Ethernet interfaces for example to describe the configuration steps.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type unit-id/slot-id/port-id*	Enter Layer 3 Ethernet interface configuration mode.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
3	Raisecom(config-gigaethernet*/*/*)#**vrrp6** *group-id* **track** { *interface-type unit-id/slot-id/port-id* | **vlan** *vlan-id* } [**reduced** *priority*]	Configure the tracking function of the VRRP backup group.

16.5.8 Configuring BFD for VRRPv3

The BFD for VRRPv3 supports Layer 3 Ethernet interfaces, aggregation group interfaces, VLAN interfaces, and Layer 3 Ethernet sub-interfaces. This chapter only uses Layer 3 Ethernet interfaces for example to describe the configuration steps.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type unit-id/slot-id/port-id*	Enter Layer 3 Ethernet interface configuration mode.
3	Raisecom(config-gigaethernet1/1/*)#**vrrp6** *group-id* **bfd-session** *session-id*	Bind sessions to VRRPv3 backup groups.
4	Raisecom(config-gigaethernet1/1/*)#**vrrp6** *group-id* **track bfd-session** *session-id* [**increased** *priority* | **reduce** *priority*]	Configure the VRRPv3 backup group to monitor BFD sessions to implement fast switching.

16.5.9 Checking configurations

No.	Command	Description
1	Raisecom#**show vrrp interface** { *interface-type unit-id/slot-id/port-id* | **vlan** *vlan-id* | **port-channel** *channel-number* } [*group-id*]	Show VRRP configurations and status on the interface.
2	Raisecom#**show vrrp interface** { *interface-type unit-id/slot-id/port-id* | **vlan** *vlan-id* | **port-channel** *channel-number* } [*group-id*] **statistics**	Show VRRP statistics globally and on the interface.
3	Raisecom#**show vrrp** [*group-id*]	Show configurations of all VRRP backup groups or a specified VRRP backup group.
4	Raisecom#**show vrrp** [*group-id*] **track**	Show the fault tracking function of VRRP.

16.5.10 Maintenance

Command	Description
Raisecom#**clear vrrp** [**interface** { *interface-type unit-id/slot-id/port-id* | **vlan** *vlan-id* | **port-channel** *channel-number* } [*group-id*]] **statistics**	Clear statistics of all backup groups or a specified backup group.

Copyright © Raisecom Technology Co., Ltd.

16.6 Configuring ERPS

16.6.1 Preparing for configurations

Scenario

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

By defining different roles for nodes on a ring, ERPS 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 loopback, perform protection switching, and automatically recover from faults. In addition, the switching time is shorter than 50ms.

The RAX721 supports the single ring, intersecting ring, and tangent ring.

ERPS provides 2 modes to detect a fault:

- Detect faults based on physical interface status: learning link fault quickly and switching services immediately, suitable for detecting the fault between neighbor devices.
- Detect faults based on CFM: suitable for unidirectional detection or multi-device crossing detection.
- Detect faults based on physical interface and CFM.

Prerequisite

- Connect interfaces and configure physical parameters for them. Make the physical layer Up.
- Create a VLAN.
- Add the interface to the VLAN.
- Create the management VLAN and VLANs of the working and protection interfaces.
- Configure CFM detection between devices and form a neighbor relationship (preparing for CFM detection mode).

16.6.2 Creating ERPS protection ring

Caution

- Only one device on the protection ring can be set to the Ring Protection Link (RPL) Owner and one device is configured to RPL Neighbor. Other devices are set to ring forwarding nodes.
- In actual, the tangent ring consists of 2 independent single rings. Configurations on the tangent ring are identical to the ones on the common single ring. The intersecting ring consists of a main ring and a tributary ring. Configurations on the main ring are identical to the ones on the common single ring.

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

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
2	Raisecom(config)#**ethernet ring-protection** *ring-number* **east** *interface-type interface-number* **west** *interface-type interface-number* **node-type rpl-owner rpl** { **east** | **west** } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a protection ring and set the node to the RPL Owner. By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094. If you configure the not-revertive mode, the protection ring is in non-revertive mode. In revertive mode, the traffic is switched from the protection line back to the working line when the working line recovers from a fault. However, in non-revertive mode, the traffic is not switched. By default, the protection ring is in revertive mode. **Note** The east and west interfaces cannot be the same one.
	Raisecom(config)#**ethernet ring-protection** *ring-number* **east** *interface-type interface-number* **west** *interface-type interface-number* **node-type rpl-neighbour rpl** { **east** | **west** } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a protection ring and set the node to the RPL Neighbour. By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094.
	Raisecom(config)#**ethernet ring-protection** *ring-number* **east** *interface-type interface-number* **west** *interface-type interface-number* [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a protection line and set the node to the RPL forwarding node. By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094.
3	Raisecom(config)#**ethernet ring-protection** *ring-number* **name** *string*	(Optional) configure a name for the protection ring.
4	Raisecom(config)#**ethernet ring-protection** *ring-number* **version** { **1** | **2** }	(Optional) configure the protocol version. Protocol versions of all nodes on a ring should be consistent. Version 1 distinguishes rings through the protocol VLAN. Therefore, you should configure different protocol VLANs for these rings. We recommend configuring different protocol VLANs for these rings, even you use version 2. By default, version 2 is used.
5	Raisecom(config)#**ethernet ring-protection** *ring-number* **guard-time** *guard-time*	(Optional) after the ring Guard timer is configured, the failed node does not process APS packets during a period. In a larger ring network, after the failed node is recovered, the node may be in down status again because it receives fault notifications sent by neighbor nodes. The ring Guard timer can resolve this problem. By default, the ring Guard timer is 200ms.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
6	Raisecom(config)#**ethernet ring-protection** *ring-number* **wtr-time** *wtr-time*	(Optional) configure the ring WTR timer. In revertive mode, when the working line recovers from a fault, traffic is not switched to the working line unless the WTR timer times out. By default, the ring WTR time value is 5min.
7	Raisecom(config)#**ethernet ring-protection** *ring-number* **holdoff-time** *holdoff-time*	(Optional) configure the Holdoff timer. After the Holdoff timer is configured, when the working line fails, the system will delay to report the fault. It means that services will be delayed to be switched to the protection line. This can prevent frequent switching caused by flapping of the working line. By default, the Holdoff timer value is 100ms. **Note** If the Holdoff timer value is over great, it may influence 50ms switching performance. Therefore, we recommend configuring the Holdoff timer value to 0ms.

16.6.3 (Optional) creating ERPS protection tributary ring

Caution

- Only the intersecting ring consists of a main ring and a tributary ring. The main ring is a complete ring and all its nodes should be configured with double interfaces. The sub-interface is an incomplete ring and you must configure the single interface on the intersecting node.
- Configurations on the main ring are identical to the ones on the single ring/tangent ring.
- Configurations of non-intersecting nodes of the intersecting ring are identical to the ones on the single ring/tangent ring.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-number* **east** *interface-type interface-number* [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create the tributary ring on the intersecting node and set the intersecting node to the forwarding node.
	Raisecom(config)#**ethernet ring-protection** *ring-number* **east** *interface-type interface-number* **node-type** { **rpl-neighbour** | **rpl-owner** } **rpl** { **east** | **west** } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create the tributary ring on the intersecting node and set the intersecting node to the RPL Neighbour or RPL Owner. By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config)#**ethernet ring-protection** *ring-number* **west** *interface-type interface-number* [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create the tributary ring on the intersecting node and set the intersecting node to the forwarding node.
3	Raisecom(config)#**ethernet ring-protection** *ring-number* **west** *interface-type interface-number* **node-type** { **rpl-neighbour** | **rpl-owner** } **rpl** { **east** | **west** } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create the tributary ring on the intersecting node and set the intersecting node to the RPL Neighbour or RPL Owner By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094.
4	Raisecom(config)#**ethernet ring-protection** *ring-number* **raps-vc** { **with** | **without** }	(Optional) configure the tributary ring virtual channel mode on the intersecting node. Because the link between intersecting nodes belong to the main ring, the transmission mode of protocol packets of the tributary ring is different from the one of the main ring. It is divided into with and without modes. By default, the tributary ring virtual channel adopts the with mode. Transmission modes on 2 intersecting nodes must be identical.
5	Raisecom(config)#**ethernet ring-protection** *ring-number* **propagate enable**	Enable the ring Propagate switch on the intersecting node. Because data of the tributary ring need to be forwarded through the main ring, there is the MAC address table of the tributary ring on the main ring. When the topology of the tributary ring changes, the tributary ring should use the Propagate switch to inform the main ring to refresh the MAC address table to avoid traffic loss. By default, the ring Propagate switch is disabled. We recommend enabling ring Propagate switch.

16.6.4 Configuring ERPS fault detection modes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-number* { **east** | **west** } **failure-detect physical-link**	Configure the ERPS fault detection mode to failure-detect physical-link. By default, the ERPS fault detection mode is failure-detect physical-link.

Copyright © Raisecom Technology Co., Ltd.

Step	Command	Description
	Raisecom(config)#**ethernet ring-protection** *ring-number* { **east** | **west** } **failure-detect cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Configure the ERPS fault detection mode to failure-detect cc. This ERPL fault detection mode cannot take effect unless you finish related configurations on CFM. If you configure the MD, the MA should be below the configured md-level.
	Raisecom(config)#**ethernet ring-protection** *ring-number* { **east**| **west** } **failure-detect physical-link-or-cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Configure the ERPS fault detection mode to failure-detect physical-link-or-cc. In this mode, it believes that the link fails when a fault is detected on the physical link/CC. This ERPL fault detection mode cannot take effect unless you finish related configurations on CFM. If you configure the MD, the MA should be below the configured md-level.

16.6.5 (Optional) configuring ERPS switching control

Note

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

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-number* **force-switch** { **east** | **west** }	Switch the traffic on the protection ring to the west/east interface forcedly.
3	Raisecom(config)#**ethernet ring-protection** *ring-number* **manual-switch** { **east** | **west** }	Switch the traffic on the protection ring to the west/east interface manually. Its priority is lower than the one of forced switch and APS.

16.6.6 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show ethernet ring-protection**	Show ERPS protection ring configurations.
2	Raisecom(config)#**show ethernet ring-protection status**	Show ERPS protection ring status.
3	Raisecom(config)#**show ethernet ring-protection statistics**	Show ERPS protection ring statistics.

Copyright © Raisecom Technology Co., Ltd.

16.6.7 Maintenance

Command	Description
Raisecom(config)#**clear ethernet ring-protection** *ring-number* **command**	Clear the switching control command of the protection ring, including the **force-switch** and **manual-switch** commands.
Raisecom(config)#**clear ethernet ring-protection** *ring-number* **statistics**	Clear protection ring statistics, including the number of sent APS packets, the number of received APS packets, the latest switching time, and the fault detection mode.

16.7 Configuring MPLS linear protection

16.7.1 Preparing for configurations

Scenario

MPLS linear protection switching protects the primary link by providing a backup link. Therefore, it provides end-to-end protection for LSP links and PW links between devices.

Prerequisite

Configure MPLS basic functions.

16.7.2 Configuring MPLS linear protection switching

Creating LSP 1:1 linear protection pair

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls line-protection** *aps-id* { **lsp** | **transit-lsp** } **working** *lsp-ingress-name lsp-egress-name* **protection** *lsp-ingress-name lsp-egress-name* [**ttl** *ttl*] **one-to-one** [**non-revertive**]	Create a MPLS LSP linear protection pair and configure the working line, protection line, and protection mode.

Creating PW 1:1 linear protection pair

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls line-protection** *aps-id* { **pw** | **ms-pw** } **working vc-id** *vc-id* **destination** *ip-address* **protection vc-id** *vc-id* **destination** *ip-address* [**ttl** *ttl*] **one-to-one** [**non-revertive**]	Create a MPLS PW linear protection pair and configure the working line, protection line, and protection mode.

Copyright © Raisecom Technology Co., Ltd.

Configuring basic properties of protection pair

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls line-protection** *aps-id* **name** *string*	(Optional) configure the name of the MPLS linear protection pair.
3	Raisecom(config)#**mpls line-protection** *aps-id* **hold-off-timer** *hold-off-timer*	Configure the Hold off timer. By default, it is 0.
4	Raisecom(config)#**mpls line-protection** *aps-id* **wtr-timer** *wtr-timer*	Configure the WTR timer. By default, it is 5min.
5	Raisecom(config)#**mpls line-protection trap enable**	Enable MPLS linear protection Trap. By default, it is enabled.

Configuring switching control commands

Select any step from steps 2–5 as required. Use the **clear mpls line-protection** command to clear switching control commands of the protection pair immediately.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls line-protection** *aps-id* **force-switch**	(Optional) switch the traffic to the protection line forcedly. By default, the traffic is automatically switched to the protection line when the working line fails.
3	Raisecom(config)#**mpls line-protection** *aps-id* **lockout**	(Optional) configure MPLS linear protection switching lockout. By default, the traffic is automatically switched to the protection line when the working line fails.
4	Raisecom(config)#**mpls line-protection** *aps-id* **manual-switch**	(Optional) switch the traffic to the protection line manually. By default, the traffic is automatically switched to the protection line when the working line fails.
5	Raisecom(config)#**mpls line-protection** *aps-id* **manual-switch-to-work**	(Optional) switch the traffic back to the working line manually.

16.7.3 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show mpls line-protection** [*aps-id*] **config**	Show MPLS linear protection pair configurations.
2	Raisecom(config)#**show mpls line-protection** [*aps-id*] **statistic**	Show MPLS linear protection pair statistics.

Copyright © Raisecom Technology Co., Ltd.

No.	Command	Description
3	Raisecom(config)#**show mpls line-protection** [*aps-id*] **status**	Show MPLS linear protection pair status.

16.8 Configuring HA hot backup

16.8.1 Preparing for configurations

Scenario

High Availability (HA) includes hot backup, batch backup, and realtime backup, used to implement high system reliability. A device supporting HA hot backup requires two cards, one is the master card working in the master mode, and the other is the slave card working in the slave mode. Whenever the master card fails, the slave card will become active and take over work to ensure the normal operation of the system.

Prerequisite

The master and slave cards are inserted.

16.8.2 Configuring HA switching

Step	Command	Description
1	Raisecom#**ha switchover**	Manually switch services between the master card and slave card.

16.8.3 Checking configurations

No.	Command	Description
1	Raisecom#**show ha state**	Show the HA hot backup status.

16.9 Configuring EVPL dual-homing protection

16.9.1 Preparing for configurations

Scenario

A multi-home site refers to the site connected to multiple PEs through different Ethernet links, which form an Ethernet Segment (ES) and are identified by the same ES Identifier (ESI) as belonging to the same ES. Multiple connected PEs form a redundant backup group, which can avoid the impact by PE single point failures on the network and improve its reliability.

Copyright © Raisecom Technology Co., Ltd.

Prerequisites

N/A

16.9.2 Configuring mLACP link aggregation

Configuring the ICCP channel

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**iccp local-ip** *ip-address*	Configure the local IP address of the ICCP channel. The local IP address is usually the IP address of the physical interface or LAG interface of the channel.
3	Raisecom(config)#**iccp channel** *channel-id*	Create an ICCP channel, and enter ICCP configuration mode.
4	Raisecom(config-iccp)#**member-ip** *ip-address*	Configure the peer IP address of the ICCP channel.
5	Raisecom(config-iccp)#**iccp enable**	Enable the ICCP channel.

Configuring mLACP link aggregation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mlacp-group** *icg-id*	Create an inter-chassis group, and enter inter-chassis group configuration mode.
3	Raisecom(config-ic-group)#**iccp-channel** *channel-id*	Configure the inter-chassis group to be bound with an ICCP channel.
4	Raisecom(config-ic-group)#**mlacp** { **master** | **slave** }	Configure the mLACP role of the local device in the inter-chassis group.
5	Raisecom(config-ic-group)#**port-channel** *group-id*	Configure the inter-chassis group to be bound with a LAG.
6	Raisecom(config-ic-group)#**restore-mode** { **non-revertive** | **revertive** [**restore-delay** *seconds*] }	Configure the revertive mode and restore-delay time of the LAG in the inter-chassis group.
7	Raisecom(config-ic-group)#**mlacp system-priority** *system-priority*	Configure the system priority of the local device in the inter-chassis group. By default, it is 32768.
8	Raisecom(config-ic-group)#**track pw** *pw-id* **peer** *ip-address*	Configure the PW to be monitored in the inter-chassis group.

Copyright © Raisecom Technology Co., Ltd.

16.9.3 Configuring EVPL dual-homing

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode.
3	`Raisecom(config-port)#evpn esi` *esi*	Configure the ESI on the PE interface that is connected to the CE. Then, the PE can obtain the ESI of other Pes through route advertisement so that it can learn those PEs that are connected to the same CE as the PE.
4	`Raisecom(config-port)#evpn ignore-ac-state`	Configure the PE interface to ignore the AC status in the EVPN multi-homed single-active networking.

5	`Raisecom(config-port)#evpn redundancy-mode single-active`
	`Raisecom(config-port)#exit`
	`Raisecom(config)#exit`
		Configure the EVPL redundancy mode to single-active on the interface.
		By default, it is dual-active.

16.10 Maintenance

Command	Description
`Raisecom(config)#clear lacp statistics [` *interface-type interface-number* `]`	Clear LACP statistics.
`Raisecom(config)#clear mlacp mlacp-group [` *icg-id* `] statistics`	Clear the statistics about the packets sent and received by the inter-chassis group.
`Raisecom(config)#clear iccp channel [` *channel-id* `] statistics`	Clear statistics about the packets sent and received by ICC.
`Raisecom#clear vrrp statistics`	Clear packet statistics of all VRRP backup groups.

16.11 Configuration examples

16.11.1 Example for configuring VRRP single backup group

Networking requirements

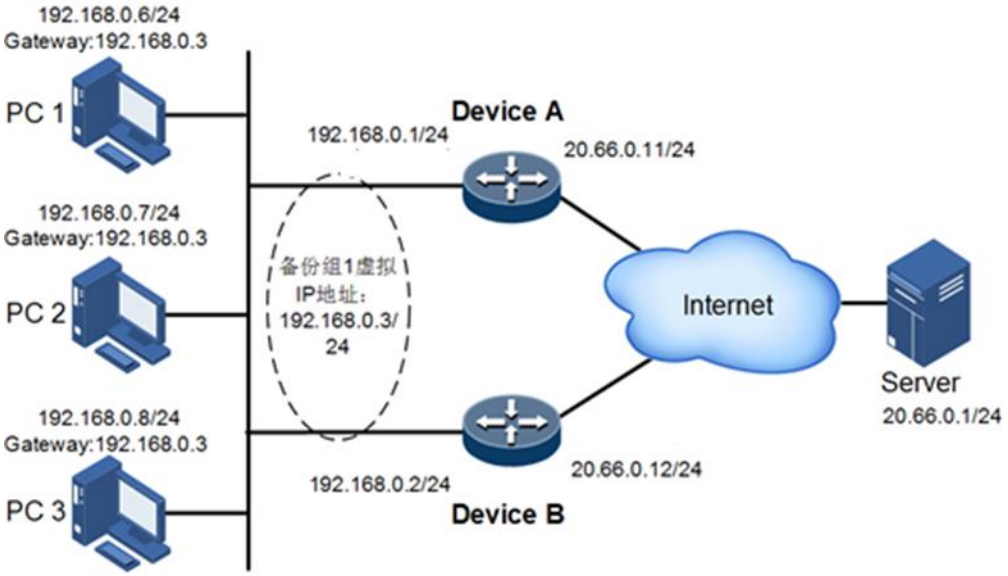
PC 1, PC 2, and PC 3 use the VRRP backup group composed of Device A and Device B as their default gateway, that is, 192.168.0.3, with a subnet mask of 255.255.255.0, to access servers on the Internet, as shown in Figure 16-1. The composition of the VRRP backup group is as follows:

- The backup group number is 1.

Copyright © Raisecom Technology Co., Ltd.

- The IP address of the virtual router of the backup group is 192.168.0.3, and the subnet mask is 255.255.255.0.
- Router A serves as the master device, with a priority of 150.
- Router B is a backup device, allowing preemption, and the preemption delay time is 20s.

Figure 16-1 VRRP single backup group networking



Configuration steps

Step 1 Configure the virtual IP address 192.168.0.3 of backup group 1 as the default gateway of PC 1, PC 2 and PC 3. The specific configuration is omitted.

Step 2 Configure the IP address.

Configure Device A.

```
Raisecom#hostname DeviceA
DeviceA#config
DeviceA(config)#interface gigaethernet 1/2/1
DeviceA(config-gigaethernet1/2/1)#ip address 192.168.0.1 1 255.255.255.0
```

Configure Device B.

```
Raisecom#hostname DeviceB
DeviceB#config
DeviceB(config)#interface gigaethernet 1/2/1
DeviceB(config-gigaethernet1/2/1)#ip address 192.168.0.2 1 255.255.255.0
```

Step 3 Create a VRRP backup group and start it.

Configure Device A.

Copyright © Raisecom Technology Co., Ltd.

```
DeviceA(config-gigaethernet1/2/1)#vrrp 1 ip 192.168.0.3
DeviceA(config-gigaethernet1/2/1)#vrrp 1 priority 150
DeviceA(config-gigaethernet1/2/1)#vrrp 1 enable
```

Configure Device B.

```
DeviceB(config-gigaethernet1/2/1)#vrrp 1 ip 192.168.0.3
DeviceB(config-gigaethernet1/2/1)#vrrp 1 enable
```

Checking results

Use the **show vrrp** command to show VRRP configurations on Device A.

```
DeviceA#show vrrp
VRRP Trap: Enabled
Ping Enable: Enabled
Interface: gigaethernet1/2/1 - Group: 1 - Enabled
  State: Master
  Description:
  Virtual IP Address: 192.168.0.3
  Virtual MAC Address: 0000.5e00.0101
  Advertisement Interval: 1(sec)
  Preemption: Enabled
  Delay Time: 0(sec)
  Cfg Priority: 150
  Run Priority: 150
  Master Router: 192.168.0.1 (local)
  Master Priority: 150
  Master Advertisement Interval: 1(sec)
  Master Down Interval: 15.609(sec)
```

Use the **show vrrp** command to show VRRP configurations on Device B.

```
DeviceB#show vrrp
VRRP Trap: Enabled
Ping Enable: Enabled
Interface: gigaethernet1/2/1 - Group: 1 - Enabled
  State: Backup
  Description:
  Virtual IP Address: 192.168.0.3
  Virtual MAC Address: 0000.5e00.0103
  Advertisement Interval: 1.000(sec)
  Preemption: Enabled
  Delay time: 0.000(sec)
  Bfd-sesion: --
  Cfg Priority: 100
  Run Priority: 100
```


Copyright © Raisecom Technology Co., Ltd.

```
Master Router: 192.168.0.1
Master Priority: 100
Master Advertisement Interval: 1.000(sec)
Master Down Interval: 3.609(sec)
```

16.11.2 Example for configuring VRRP multiple backup groups

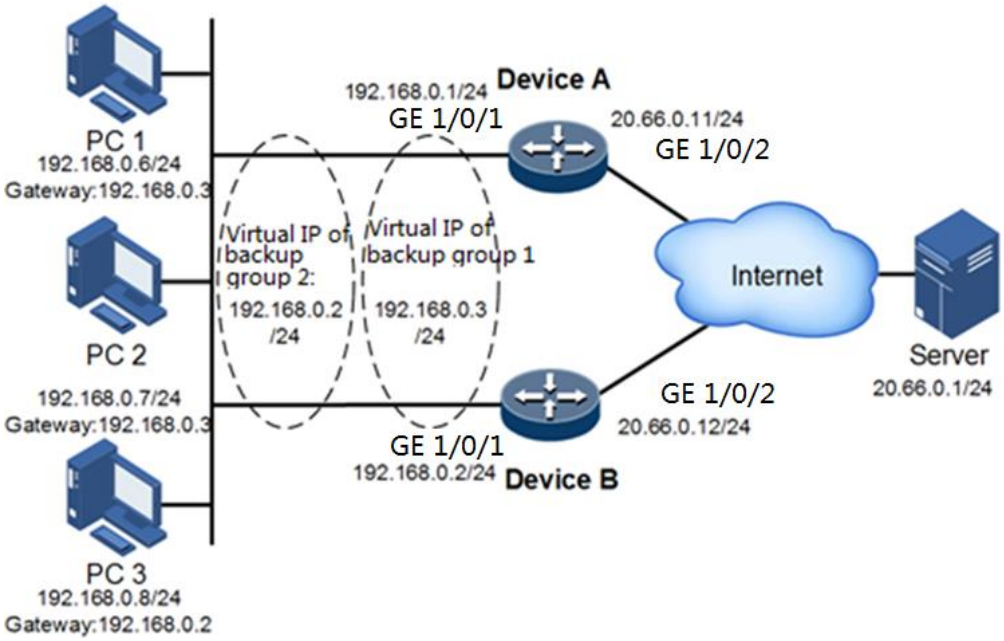
Networking requirements

To implement load sharing of network traffic and the purpose of mutual backup, you can configure one device as a backup for multiple backup groups. As shown in Figure 16-2, the specific requirements are as follows:

- Device A serves as the master device of backup group 1 and at the same time as the backup device of backup group 2.
- Device B serves as the master device of backup group 2 and at the same time as the backup device of backup group 1.
- The virtual IP address of backup group 1 is 192.168.0.3, the subnet mask is 255.255.255.0; the virtual IP address of backup group 2 is 192.168.0.2, and the subnet mask is 255.255.255.0.

To access servers on the Internet, PC 1 and PC 2 use backup group 1 as the default gateway, and PC 3 uses backup group 2 as the default gateway.

Figure 16-2 VRRP multiple backup groups networking



Configuration steps

Step 1 Configure the virtual IP address 192.168.0.3 of the backup group 1 as the default gateway of PC 1 and PC 2, and configure the default gateway of PC 3 to 192.168.0.2. The specific configuration is omitted.

Copyright © Raisecom Technology Co., Ltd.

Step 2 Configure the IP address.

Configure Device A.

```
Raisecom#hostname DeviceA
DeviceA#config
DeviceA(config)#interface gigaethernet 1/2/1
DeviceA(config-gigaethernet1/2/1)#ip address 192.168.0.1 1 255.255.255.0
```

Configure Device B.

```
Raisecom#hostname DeviceB
DeviceB#config
DeviceB(config)#interface gigaethernet 1/2/1
DeviceB(config-gigaethernet1/2/1)#ip address 192.168.0.2 1 255.255.255.0
```

Step 3 Create a VRRP backup group and start it.

Configure Device A.

```
DeviceA(config-gigaethernet1/2/1)#vrrp 1 ip 192.168.0.3
DeviceA(config-gigaethernet1/2/1)#vrrp 1 priority 150
DeviceA(config-gigaethernet1/2/1)#vrrp 1 enable
DeviceA(config-gigaethernet1/2/1)#vrrp 2 ip 192.168.0.2
DeviceA(config-gigaethernet1/2/1)#vrrp 2 enable
```

Configure Device B.

```
DeviceB(config-gigaethernet1/2/1)#vrrp 1 ip 192.168.0.3
DeviceB(config-gigaethernet1/2/1)#vrrp 1 enable
DeviceB(config-gigaethernet1/2/1)#vrrp 2 ip 192.168.0.2
DeviceB(config-gigaethernet1/2/1)#vrrp 2 priority 150
DeviceB(config-gigaethernet1/2/1)#vrrp 2 enable
```

Checking results

Use the **show vrrp** command to show VRRP configurations of Device A.

```
DeviceA#show vrrp
VRRP Trap: Enabled
Ping Enable: Enabled
Interface: gigaethernet1/2/1 - Group: 1 - Enabled
  State: Master
```


Copyright © Raisecom Technology Co., Ltd.

```
  Description:
  Virtual IP Address: 192.168.0.3
  Virtual MAC Address: 0000.5e00.0103
  Advertisement Interval: 1.000(sec)
  Preemption: Enabled
  Min Delay: 0.000(sec)
  Cfg Priority: 150
  Run Priority: 150
  Master Router: 192.168.0.1 (local)
  Master Priority: 150
  Master Advertisement Interval: 1.000(sec)
  Master Down Interval: 3. 414 (sec)

Interface: gigaethernet1/2/1 - Group: 2 - Enabled
  State: Backup
  Description:
  Virtual IP Address: 192.168.0.2
  Virtual MAC Address: 0000.5e00.0102
  Advertisement Interval: 1.000(sec)
  Preemption: Enabled
  Min Delay: 0.000(sec)
  Cfg Priority: 100
  Run Priority: 100
  Master Router: 192.168.0.2
  Master Priority: 255
  Master Advertisement Interval: 1.000(sec)
Master Down Interval: 3.609(sec)
```

Use the **show vrrp** command to show VRRP configurations of Device B.

```
DeviceB#show vrrp
VRRP Trap: Enabled
Ping Enable: Enabled
Interface: gigaethernet1/2/1 - Group: 1 - Enabled
  State: Backup
  Description:
  Virtual IP Address: 192.168.0.3
  Virtual MAC Address: 0000.5e00.0103
  Advertisement Interval: 1.000(sec)
  Preemption: Enabled
  Min Delay: 0.000(sec)
  Cfg Priority: 100
  Run Priority: 100
  Master Router: 192.168.0.1
  Master Priority: 150
  Master Advertisement Interval: 1.000(sec)
  Master Down Interval: 3.609(sec)

Interface: gigaethernet1/2/1 - Group: 2 - Enabled
  State: Master
  Description:
  Virtual IP Address: 192.168.0.2
  Virtual MAC Address: 0000.5e00.0102
```


Copyright © Raisecom Technology Co., Ltd.

```
  Advertisement Interval: 1.000(sec)
  Preemption: Enabled
  Min Delay: 0.000(sec)
  Cfg Priority: 255
  Run Priority: 100
  Master Router: 192.168.0.2 (local)
  Master Priority: 255
  Master Advertisement Interval: 1.000(sec)
Master Down Interval: 3.000(sec)
```


Copyright © Raisecom Technology Co., Ltd.

17 Appendix

This chapter lists terms, acronyms, and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

17.1 Terms

A

Access Control List (ACL)	A series of ordered rules composed of permit | deny sentences. These rules are based on source MAC address, destination MAC address, source IP address, destination IP address, interface ID, etc. The device decides to receive or refuse the packets based on these rules.

C

Connectivity Fault Management (CFM)	A standard defined by IEEE. It defines protocols and practices for OAM (Operations, Administration, and Maintenance) for paths through 802.1 bridges and local area networks (LANs). Used to diagnose fault for EVC (Ethernet Virtual Connection). Cost-effective by fault management function and improve Ethernet maintenance.

E

Encapsulation	A technology used by the layered protocol. When the lower protocol receives packets from the upper layer, it will map packets to the data of the lower protocol. The outer layer of the data is encapsulated with the lower layer overhead to form a lower protocol packet structure. For example, an IP packet from the IP protocol is mapped to the data of 802.1Q protocol. The outer layer is encapsulated by the 802.1Q frame header to form a VLAN frame structure.

Copyright © Raisecom Technology Co., Ltd.

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, etc. for a link between two directly-connected devices. EFM is mainly used for the Ethernet link on edges of the network accessed by users.

L

Link Aggregation	A computer networking term which describes using multiple network cables/ports in parallel to increase the link speed beyond the limits of any one single cable or port, and to increase the redundancy for higher availability.

P

Packet	In data communication field, packet is the data unit for switching and transmitting information. In transmission, it will be continuously encapsulated and decapsulated. The header is used to define the destination address and source address. The trailer contains information indicating the end of the packet. The payload data in between is the actual packet.
Packet switching	In packet switching network, data is partitioned into multiple data segments. The data segment is encapsulated by control information, such as, destination address, to form the switching packet. The switching packet is transmitted to the destination in the way of storage-forwarding on the network. Packet switching is developed based on storage-forwarding method and has merits of both circuit switching and packet switching.

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.

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.

Copyright © Raisecom Technology Co., Ltd.

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.

17.2 Acronyms and abbreviations

A

ACL	Access Control List
APS	Automatic Protection Switching
AS	Autonomous System
ASM	Any-Source Multicast

B

BGP	Border Gateway Protocol

C

CAR	Committed Access Rate
CCC	Circuit Cross Connect
CE	Customer Edge
CIDR	Classless Inter-Domain Routing
CFM	Connectivity Fault Management
CoS	Class of Service
CLNP	Connectionless Network Protocol
CR-LDP	Constraint-Routing Label Distribution Protocol

D

DRR	Deficit Round Robin
DSCP	Differentiated Services Code Point
DM	Dense Mode

Copyright © Raisecom Technology Co., Ltd.

E

EFM	Ethernet in the First Mile
EBGP	External Border Gateway Protocol

F

FTP	File Transfer Protocol

G

GPS	Global Positioning System

H

HA	High Availability

I

IANA	Internet Assigned Numbers Authority
IBGP	Internal Border Gateway Protocol
ICCP	Inter-Chassis Communication Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocols
IP	Internet Protocol
ISIS	Intermediate System to Intermediate System
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector
IGMP	Internet Group Management Protocol

L

L2PDU	Layer2 Protocol Data Unit
L2VC	Layer 2 Virtual connection
L2VPN	Layer2 Virtual Private Network
L3VPN	Layer3 Virtual Private Network
LACP	Link Aggregation Control Protocol
LBM	LoopBack Message

Copyright © Raisecom Technology Co., Ltd.

LBR	LoopBack Reply
LDP	Label Distribution Protocol
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LSR	Label Switching Router
LTM	LinkTrace Message
LTR	LinkTrace Reply

M

MA	Maintenance Association
MAC	Medium Access Control
MBGP	Multicast Border Gateway Protocol
MD	Maintenance Domain
MEG	Maintenance Entity Group
MEP	Maintenance associations End Point
MIB	Management Information Base
MIP	Maintenance association Intermediate Point
MLD	Multicast Listener Discover
MPLS	Multiprotocol Label Switching
MP-BGP	Multiprotocol Extensions for Border Gateway Protocol
MSDP	Multicast Source Discovery Protocol
MTU	Maximum Transfered Unit

N

NHLFE	Next Hop Label Forwarding Entry
NTP	Network Time Protocol

O

OSPF	Open Shortest Path First
OAM	Operation, Administration and Maintenance

P

PDU	Protocol Data Unit

Copyright © Raisecom Technology Co., Ltd.

PE	Provider Edge
PIM	Protocol Independent Multicast
PW	Pseudo Wire
PWE3	Pseudo Wire Emulation Edge-to-Edge

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
RPT	Rendezvous Point Tree
RMON	Remote Network Monitoring
RSVP-TE	Resource Reservation Protocol Traffic Engineering

S

SFP	Small Form-factor Pluggables
SLA	Service Level Agreement
SM	Sparse Mode
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SSH	Secure Shell
SSM	Source-Specific Multicast

T

TACACS+	Terminal Access Controller Access Control System
TCI	Tag Control Information
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service
TPID	Tag Protocol Identifier

Copyright © Raisecom Technology Co., Ltd.

V

VPN	Virtual Private Network
VLAN	Virtual Local Area Network

W

WRR	Weight Round Robin

Copyright © Raisecom Technology Co., Ltd.

瑞斯康达科技发展股份有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: Raisecom Building, No. 11, East Area, No. 10 Block, East Xibeiwang Road, Haidian District, Beijing, P.R.China Postal code: 100094 Tel: +86-10-82883305
Fax: 8610-82883056 http://www.raisecom.com Email: export@raisecom.com