

www.raisecom.com

RAX711-C-R (A)
Configuration Guide
(Rel_03)



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

Website: <http://www.raisecom.com>

Tel: 8610-82883305

Fax: 8610-82883056

Email: export@raisecom.com

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

Postal code: 100094

Notice

Copyright © 2021

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 RAX711-C-R, 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 RAX711-C-R systematically, as well as networking with the RAX711-C-R.

Versions

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

Product name	Product version	Hardware version
RAX711-C-R	P100R001	A.10 or later

Conventions

Symbol conventions

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

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

Symbol	Description
	Indicate a tip that may help you solve a problem or save time.

General conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Arial	Paragraphs in Warning, Caution, Notes, and Tip are in Arial.
Boldface	Names of files, directories, folders, and users are in boldface . For example, log in as user root .
<i>Italic</i>	Book titles are in <i>italics</i> .
Lucida Console	Terminal display is in Lucida Console.
Book Antiqua	Heading 1, Heading 2, Heading 3, and Block are in Book Antiqua.

Command conventions

Convention	Description
Boldface	The keywords of a command line are in boldface .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[]	Items (keywords or arguments) in square brackets [] are optional.
{ x y ... }	Alternative items are grouped in braces and separated by vertical bars. 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.
[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
<i>/*</i>	Indicate the interface ID/slot ID. For example, "Raisecom(config-eth/1)" indicates Ethernet interface 1 and "Raisecom(config-slot/4)" indicates slot 4.
<i>/*/*</i>	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

Convention	Description
<i>interface-type</i>	Interface type: • vlan: VLAN interface • loopback: Loopback interface • tunnel: Tunnel interface • tengigabitethernet or gigaethernet: Layer 2 physical interface/Layer 3 physical interface/sub-interface • fastethernet: out-of-band network management interface • port-channel: Trunk interface/sub-interface
<i>interface-number</i>	Interface ID based on the device model and interface type: • vlan: 1–4094 • loopback: 1–32 • tunnel: 1/1/1–1/1/40000 • tengigabitethernet or gigaethernet <i>unit/slot/port</i>: 1/1/1–1/1/4 or 1/2/1–1/2/12 (Layer 2/Layer 3 physical interface) • tengigabitethernet or gigaethernet <i>unit/slot/port.sub-interface</i>: 1/1/1.1–1/1/1.4094 or 1/1/2.1–1/1/2.4094 and so on (sub-interface) • fastethernet: 1/0/1 • port-channel: 1–16

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
<code>Raisecom(config-fastethernetunit/slot/port)#</code>	Entered out-of-band interface configuration mode. The interface ID is <i>unit/slot/port</i> , such as <code>Raisecom(config-fastethernet1/0/1)#</code> .
<code>Raisecom(config-gigaethernetunit/slot/port)#</code>	Entered Gigabit Ethernet interface configuration mode. The interface ID is <i>unit/slot/port</i> , such as <code>Raisecom(config-gigaethernet1/2/1)#</code> .
<code>Raisecom(config-gigaethernetunit/slot/port.sub)#</code>	Entered Gigabit Ethernet sub-interface configuration mode. The interface ID is <i>unit/slot/port.sub</i> , such as <code>Raisecom(config-gigaethernet1/2/1.1)#</code> .
<code>Raisecom(config-tengigabitethernetunit/slot/port)#</code>	Entered 10 Gbit/s Ethernet interface configuration mode. The interface ID is <i>unit/slot/port</i> , such as <code>Raisecom(config-gigaethernet1/2/1)#</code> .
<code>Raisecom(config-tengigabitethernetunit/slot/port.sub)#</code>	Entered 10 Gbit/s Ethernet sub-interface configuration mode. The interface ID is <i>unit/slot/port.sub</i> , such as <code>Raisecom(config-gigaethernet1/2/1.1)#</code> .
<code>Raisecom(config-vlan port)#</code>	Entered VLAN interface configuration mode. The interface ID is an integer, such as <code>Raisecom(config-vlan1)#</code> .
<code>Raisecom(config-port-channelport)#</code>	Entered Trunk interface configuration mode. The interface ID is an integer, such as <code>Raisecom(config-port-channel1)#</code> .
<code>Raisecom(config-port-channelport.sub)#</code>	Entered Trunk sub-interface configuration mode. The interface ID is <i>port.sub</i> , such as <code>Raisecom(config-port-channel1.1)#</code> .
<code>Raisecom(config-tunnelunit/slot/port)#</code>	Entered Tunnel interface configuration mode. The interface ID is <i>unit/slot/port</i> , such as <code>Raisecom(config-tunnel1/1/1)#</code> .
<code>Raisecom(config-loopbackport)#</code>	Entered Loopback interface configuration mode. The interface ID is an integer, such as <code>Raisecom(config-loopback1)#</code> .

Change history

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

Issue 03 (2021-12-31)

Third commercial release

- Fixed known bugs.

Issue 02 (2020-07-30)

Second commercial release

- Deleted BFD for link aggregation and MPLS load balancing.

Issue 01 (2020-06-12)

Initial commercial release

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 logging in	9
1.2.1 Connecting device	9
1.2.2 Accessing device through Console interface	10
1.2.3 Accessing device through Telnet	11
1.2.4 Accessing device through SSHv2	13
1.3 Backup and upgrade	14
1.3.1 Introduction	14
1.3.2 Backing up system	16
1.3.3 Upgrading system	17
1.3.4 Checking configurations	20
1.4 Device management	20
1.4.1 Introduction	20
1.4.2 Preparing for configurations	22
1.4.3 Configuring SNMP basic functions	22
1.4.4 Configuring Trap	23
1.4.5 Checking configurations	24
1.5 Configuring RMON	24
1.5.1 Introduction	24
1.5.2 Preparing for configurations	24
1.5.3 Configuring RMON alarm group	25
1.5.4 Configuring RMON event group	25
1.5.5 Configuring RMON statistics	25
1.5.6 Configuring RMON history statistics	26
1.5.7 Checking configurations	26
2 System management	27

2.1 User management.....	27
2.1.1 Configuring user management	27
2.1.2 Checking configurations	28
2.2 Fan management	28
2.3 Saving configurations.....	28
2.4 Time management	29
2.4.1 Configuring time and time zone.....	29
2.4.2 Configuring DST	29
2.4.3 Configuring NTP/SNTP.....	30
2.4.4 Checking configurations	31
2.5 Log management.....	31
2.5.1 Basic configurations of log management.....	31
2.5.2 Configuring log discriminator.....	32
2.5.3 Configuring log storage	32
2.5.4 Checking configurations	33
2.5.5 Maintenance.....	33
2.6 File management	33
2.6.1 Managing system files	33
2.7 Alarm management	33
2.7.1 Configuring alarm inhibition	36
2.7.2 Configuring alarm delay	36
2.7.3 Configuring alarm storage modes	37
2.7.4 Configuring alarm clearance.....	37
2.7.5 Configuring alarm report	37
2.7.6 Configuring alarm inverse	38
2.7.7 Configuring alarm monitoring	38
2.7.8 Configuring alarm output.....	39
2.7.9 Checking configurations	39
2.8 Key chain management	39
2.8.1 Introduction.....	39
2.8.2 Configuring key chain.....	40
2.8.3 Checking configurations	40
3 Zero-configuration.....	41
3.1 Configuring CO zero-configuration	41
3.1.1 Preparing for configurations	41
3.1.2 Configuring zero-configuration Server based on extended OAM.....	42
3.1.3 Configuring zero-configuration server based on DHCP	45
3.1.4 Checking configurations	49
4 Interface management.....	50
4.1 Basic configurations of interface.....	50
4.1.1 Configuring basic information of interface	50

4.1.2 Configuring interface working mode	51
4.1.3 Configuring Jumboframe on interface	51
4.1.4 Configuring MTU of interface	51
4.1.5 Configuring vibration suppression of interface.....	52
4.1.6 Configuring MAC address of interface	52
4.2 Configuring Ethernet interface	52
4.3 Configuring Ethernet sub-interface	53
4.4 Configuring VLAN interface	53
4.5 Configuring optical module DDM	54
4.5.1 Preparing for configurations	54
4.5.2 Enabling optical module DDM	54
4.5.3 Checking configurations	54
4.6 Configuring loopback interface.....	55
4.7.1 Preparing for configurations	55
4.7.2 Configuring IP address of out-of-band network management interface.....	55
4.8 Checking configurations	56
5 Ethernet	57
5.1 Configuring VLAN	57
5.1.1 Preparing for configurations	57
5.1.2 Configuring VLAN properties	58
5.1.3 Configuring VLANs based on Access interface.....	58
5.1.4 Configuring VLANs based on Trunk interface	59
5.1.5 Configuring VLAN based on MAC address	60
5.1.6 Configuring VLAN based on IP subnet	60
5.1.7 Configuring VLAN based on protocol.....	61
5.1.8 Checking configurations	61
5.2 Configuring MAC address table.....	61
5.2.1 Preparing for configurations	61
5.2.2 Configuring static MAC address table	62
5.2.3 Configuring dynamic MAC address table.....	62
5.2.4 Configuring blackhole MAC address.....	63
5.2.5 Filtering unknown L2 multicast packets	63
5.2.6 Checking configurations	64
5.2.7 Maintenance	64
5.3 Configuring QinQ	65
5.3.1 Preparing for configurations	65
5.3.2 Configuring basic QinQ.....	65
5.3.3 Configuring selective QinQ	66
5.3.4 Checking configurations	67
5.4 Configuring LLDP	67
5.4.1 Preparing for configurations	67

5.4.2 Enabling global LLDP	67
5.4.3 Enabling interface LLDP	67
5.4.4 Configuring LLDP basic functions	68
5.4.5 Configuring LLDP to send TLV packets	68
5.4.6 Configuring LLDP Trap	69
5.4.7 Checking configurations	69
5.5 Configuring loop detection	70
5.5.1 Preparing for configurations	70
5.5.2 Configuring loop detection	70
5.5.3 Checking configurations	70
5.5.4 Maintenance	71
5.6 Configuring L2CP	71
5.6.1 Preparing for configurations	71
5.6.2 Configuring L2CP to transparently transmit MAC address	71
5.6.3 Configuring L2CP profile	71
5.6.4 Applying L2CP profile to interface	72
5.6.5 Checking configurations	72
5.6.6 Maintenance	73
5.7 Configuring STP	73
5.7.1 Preparing for configurations	73
5.7.2 Enabling STP	73
5.7.3 Configuring STP parameters	73
5.7.4 Checking configurations	74
5.7.5 Maintenance	74
5.8 Configuring RSTP/MSTP	74
5.8.1 Preparing for configurations	74
5.8.2 Enabling MSTP	75
5.8.3 Configuring MST domain and its maximum number of hops	75
5.8.4 Configuring root/backup bridge	75
5.8.5 Configuring device interface and system priority	76
5.8.6 Configuring network diameter for switching network	77
5.8.7 Configuring internal path cost of interfaces	78
5.8.8 Configuring external path cost of interfaces	78
5.8.9 Configuring maximum transmission rate on interface	78
5.8.10 Configuring MSTP timer	79
5.8.11 Configuring edge interface	79
5.8.12 Configuring link type	80
5.8.13 Configuring root interface protection	81
5.8.14 Configuring interface loopguard	81
5.8.15 Executing mcheck operation	82
5.8.16 Checking configurations	82
5.9 Configuring MRSTP	82

5.9.1 Preparing for configurations	82
5.9.2 Enabling MRSTP	83
5.9.3 Configuring MRSTP parameter	83
5.9.4 Checking configurations	84
5.10 Configuring Super VLAN	84
5.10.1 Preparing for configurations	84
5.10.2 Configuring Super VLAN	84
5.10.3 Checking configurations	85
5.11 Configuring PVLAN	85
5.11.1 Preparing for configurations	85
5.11.2 Configuring PVLAN type	85
5.11.3 Configuring PVLAN association	85
5.11.4 Configuring PVLAN mode on interface	86
5.11.5 Checking configuration	87
5.12 Configuring GARP/GVRP	87
5.12.1 Configuring GARP	87
5.12.2 Configuring GVRP	88
5.12.3 Checking configurations	88
5.12.4 Maintenance	89
5.13 Configuring port security MAC	89
5.13.1 Configuring basic functions of port security MAC	89
5.13.2 Configuring static secure MAC address	90
5.13.3 Configuring dynamic secure MAC address	90
5.13.4 Configuring sticky secure MAC address on interface	91
5.13.5 Checking configurations	91
5.13.6 Maintenance	92
6 Clock synchronization	93
6.1 Configuring SyncE-based clock synchronization	93
6.1.1 Preparing for configurations	93
6.1.2 Configure the clock source of SyncE	93
6.1.3 Manually selecting SyncE clock source	94
6.1.4 Checking configurations	94
6.2 Configuring PTP-based clock synchronization	95
6.2.1 Preparing for configurations	95
6.2.2 Configuring PTP clock modes	95
6.2.3 Checking configurations	95
7 IP services	96
7.1 Configuring IPv4	96
7.1.1 Preparing for configurations	96
7.1.2 Configuring IPv4 address on interface	97
7.1.3 Configuring IPv4 PMTU	97

7.1.4 Checking configurations	97
7.2 Configuring IPv6.....	98
7.2.1 Preparing for configurations	98
7.2.2 Configuring IPv6 address on interface	98
7.2.3 Configuring IPv6 PMTU	98
7.2.4 Checking configurations	99
7.3 Configuring ARP.....	99
7.3.1 Preparing for configurations	99
7.3.2 Configuring static ARP	99
7.3.3 Configuring dynamic ARP	99
7.3.4 Configuring proxy ARP	100
7.3.5 Clearing ARP entries.....	100
7.3.6 Checking configurations	101
7.4 Configuring NDP	101
7.4.1 Preparing for configurations	101
7.4.2 Configuring static NDP entries	101
7.4.3 Configuring dynamic NDP entries.....	101
7.4.4 Configuring proxy NDP.....	103
7.5 Configuring ICMP	104
7.5.1 Configuring IPv4 ICMP.....	104
7.5.2 Configuring IPv6 ICMP.....	104
7.6 Configuring VRF.....	105
7.7 Configuring fault detection	105
7.7.1 PING	105
7.7.2 Traceroute	106
7.8 Configuring DHCPv4 Server	107
7.8.1 Preparing for configurations	107
7.8.2 Creating and configuring IPv4 address pool	107
7.8.3 Configuring DHCP v4 Server on interface	108
7.8.4 Checking configurations	108
7.9 Configuring DHCPv6 server	109
7.9.1 Enabling global DHCPv6 Server	109
7.9.2 Creating and configuring IPv6 address pool	109
7.9.3 Creating and configuring IPv6 prefix pool	109
7.9.4 Configuring DHCPv6 Server on interface	110
7.9.5 Checking configurations	110
7.10 Configuring DHCPv4 Client.....	111
7.10.5 Checking configurations	112
7.11 Configuring DHCPv6 client.....	112
7.11.1 Configuring DHCPv6 client.....	112
7.11.2 Checking configurations	113
7.12 Configuring DHCPv4 Relay	113

7.12.1 Preparing for configurations	113
7.12.2 Configuring global DHCPv4 Relay	113
7.12.3 Configuring DHCPv4 relay on interface.....	114
7.12.4 Configuring DHCPv4 relay Option 82.....	114
7.12.5 Checking configurations	114
7.13 Configuring DHCPv6 relay.....	115
7.14 Configuring DHCPv4 Snooping	115
7.14.1 Preparing for configurations	115
7.14.2 Configuring DHCPv4 Snooping	115
7.14.3 Configuring DHCPv4 Snooping Option 82	116
7.14.4 Checking configurations	116
7.15 Configuring DHCPv6 Snooping	117
7.15.1 Configuring DHCPv6 Snooping	117
7.15.2 Checking configurations	117
7.16 Configuring DHCPv4/DHCPv6 Option	117
7.16.1 Preparing for configurations	117
7.16.2 Configuring IPv4 DHCP Option 82	118
7.16.3 Configuring IPv4 DHCP Option 61	118
7.16.4 Configuring IPv4 self-defined DHCP Option	119
7.16.5 Configuring IPv6 DHCP Option 18	119
7.16.6 Configuring IPv6 DHCP Option 37	120
7.16.7 Configuring IPv6 DHCP Option 38	120
7.16.8 Configuring IPv6 self-defined DHCP Option	120
7.16.9 Checking configurations	120
8 IP routing.....	121
8.1 Configuring routing management	121
8.1.1 Configuring routing management	121
8.1.2 Configuring IP FRR	121
8.1.3 Checking configurations	122
8.2 Configuring static route.....	122
8.2.1 Preparing for configurations	122
8.2.2 IPv4 static route	122
8.2.3 IPv6 static route	123
8.2.4 Configuring BFD for static routes.....	123
8.2.5 Checking configurations	124
8.3 Configuring routing policy.....	125
8.3.1 Configuring IPv4 routing policy	125
8.3.2 Configuring IPv6 routing policy	128
8.3.3 Checking configurations	129
8.4 Configuring OSPFv2.....	130
8.4.1 Configuring OSPF basic functions.....	130

8.4.2 Configuring OSPF route properties	131
8.4.3 Configuring OSPF network type.....	132
8.4.4 Configuring OSPF area	134
8.4.5 Configuring load balancing.....	135
8.4.6 Maximizing LSA metric.....	135
8.4.7 Optimizing OSPF network.....	135
8.4.8 Configuring OSPF authentication policy	138
8.4.9 Controlling OSPF redistributed routes	138
8.4.10 Configuring OSPF routing policy	140
8.4.11 Configuring BFD for OSPF	142
8.4.12 Configuring OSPF for MPLS-TE	143
8.4.13 Checking configurations	143
8.4.14 Maintenance	144
8.5 Configuring OSPFv3.....	144
8.5.1 Starting OSPFv3 process	144
8.5.2 Configuring OSPFv3 network type.....	145
8.5.3 Configuring OSPFv3 area	145
8.5.4 Configuring OSPFv3 interface.....	146
8.5.5 Controlling OSPFv3 redistributed routes	147
8.5.6 Configuring timer of OSPFv3 packets	149
8.5.7 Configuring OSPFv3 route management	150
8.5.8 Configuring OSPFv3 routing policy	152
8.5.9 Configuring OSPFv3 authentication policy	154
8.5.10 Configuring BFD for OSPFv3	155
8.5.11 Checking configurations	155
8.5.12 Maintenance	156
8.6 Configuring ISIS	156
8.6.1 Configuring ISIS basic function.....	156
8.6.2 Configuring ISIS routing	157
8.6.3 Configuring ISIS network.....	158
8.6.4 Optimizing ISIS network	159
8.6.5 Configure ISIS authentication.....	161
8.6.6 Controlling ISIS routing information	162
8.6.7 Configuring ISIS BFD	164
8.6.8 Configuring ISIS GR	164
8.6.9 Configuring ISIS TE	165
8.6.10 Checking configurations	165
8.6.11 Maintenance	165
8.7 Configuring ISISv6	166
8.7.1 Configuring ISISv6 basic functions	166
8.7.2 Configuring ISISv6 authentication	167
8.7.3 Configuring ISISv6 route selection parameters	168

8.7.4 Controlling ISISv6 routing information	169
8.7.5 Configuring ISISv6 load balancing	171
8.7.6 Configuring ISISv6 BFD	171
8.7.7 Checking configurations	172
8.7.8 Maintenance	172
8.8 Configuring BGP	172
8.8.1 Configuring BGP basic functions.....	172
8.8.2 Configuring BGP redistributed routes.....	176
8.8.3 Configuring BGP to redistribute routes.....	177
8.8.4 Configuring BGP routing.....	178
8.8.5 Configuring BGP network	182
8.8.6 Configuring BFD for BGP	186
8.8.7 Configuring BGP authentication	187
8.8.8 Checking configurations	188
8.8.9 Maintenance.....	188
8.9 Configuring BGP4+	190
8.9.1 Configuring BGP4+ basic functions	190
8.9.2 Configuring BGP4+ advertised routes	191
8.9.3 Configuring BGP4+ redistributed routes	192
8.9.4 Configuring BGP4+ route attributes	192
8.9.5 Configuring BGP4+ network	194
8.9.6 Configuring BGP4+ authentication.....	196
8.9.7 Checking configurations	196
8.9.8 Maintenance.....	196
8.10 Configuring RIP	197
8.10.1 Configuring basic RIP functions	197
8.10.2 Configuring RIP version	197
8.10.3 Redistributing external routes	198
8.10.4 Configuring timer.....	198
8.10.5 Configuring loop suppression	199
8.10.6 Configuring RIP authentication	199
8.10.7 Configuring routing policy.....	199
8.10.8 Configuring route calculation	200
8.10.9 Checking configurations	200
8.11 Configuring RIPng	201
8.11.1 Configuring RIPng basic functions	201
8.11.2 Controlling routing information	201
8.11.3 Configuring timer.....	202
8.11.4 Configuring loop suppression	203
8.11.5 Configuring RIPng authentication.....	203
8.11.6 Configuring routing policy.....	203
8.11.7 Configuring route calculation.....	204

8.11.8 Checking configurations	204
9 MPLS	205
9.1.3 Checking configurations	206
9.2 Configuring MPLS Tunnel	206
9.4.9 Maintenance	216
9.5.3 Configuring RSVP-TE authentication	217
10 MPLS VPN	223
10.1.6 Configuring VPWS traffic label	230
10.2 Configuring CCC L2VPN	231
10.2.1 Preparing for configurations	231
10.2.2 Configuring CCC	233
10.2.3 Checking configurations	234
10.5 Configuring MPLS VPN fault detection	244
10.5.1 Preparing for configuration	244
10.5.2 Configuring MPLS VPN fault acknowledgement	244
10.5.3 Configuring MPLS VPN fault location	244
10.6 Maintenance	245
11 QoS	246
11.1 Configuring ACL	246
11.1.1 Preparing for configurations	246
11.1.2 Configuring ACL	246
11.1.3 Creating time period	249
11.1.4 Configuring filter	250
11.1.5 Checking configurations	250
11.2 Configuring priority trust and priority mapping	250
11.2.1 Preparing for configurations	250
11.2.2 Configuring priority trust	251
11.2.3 Configuring mapping between DSCP priority and local priority based on interface	251
11.2.4 Configuring mapping between CoS priority and local priority based on interface	252
11.2.5 Configuring Exp-to-local priority mapping	252
11.2.6 Configuring DSCP priority remarking	252
11.2.7 Configuring CoS priority remarking	253
11.2.8 Checking configurations	253
11.3 Configuring traffic classification and traffic policy	254
11.3.1 Preparing for configurations	254
11.3.2 Creating and configuring traffic classification	254
11.3.3 Creating and configuring traffic policing profile	255
11.3.4 Creating and configuring traffic policy	256
11.3.5 Checking configurations	257
11.4 Configuring congestion avoidance and queue shaping	257
11.4.1 Preparing for configurations	257

11.4.2 Configuring WRED profile	257
11.4.3 Configuring flow queue profile	258
11.4.4 Configuring queue shaping	258
11.4.5 Checking configurations	259
11.5 Configuring interface rate limiting	259
11.5.1 Preparing for configurations.....	259
11.5.2 Configuring interface-based rate limiting	259
11.5.3 Checking configurations	260
11.6 Configuring hierarchical bandwidth rate limiting	260
11.6.1 Preparing for configurations.....	260
11.6.2 Configuring bandwidth guarantee	260
11.6.3 Configuring hierarchical bandwidth guarantee	261
11.6.4 Checking configurations	262
11.7 Configuring traffic statistics	262
11.7.1 Configuring performance statistics	262
11.7.2 Checking configurations	263
11.8 Maintenance	263
12 Multicast	264
12.1 Configuring IGMP multicast basic functions	264
12.1.1 Configuring basic functions of L2 multicast.....	264
12.2 Configuring IGMP Snooping	266
12.2.1 Preparing for configurations	266
12.2.2 Configuring IGMP Snooping	266
12.2.3 Checking configurations	267
12.3 Configuring IGMP Querier	267
12.3.1 Preparing for configurations	267
12.3.2 Configuring IGMP Querier	268
12.3.3 Checking configurations	268
12.4 Configuring IGMP MVR	269
12.4.1 Preparing for configurations	269
12.4.2 Configuring IGMP MVR	269
12.4.3 Checking configurations	270
12.5 Configuring IGMP filtering.....	271
12.5.1 Preparing for configurations	271
12.5.2 Enabling IGMP filtering globally	271
12.5.3 Configuring IGMP filtering template.....	271
12.5.4 Configuring maximum number of groups.....	272
12.5.5 Checking configurations	273
12.6 Configuring multicast VLAN copy	273
12.6.2 Configuring multicast VLAN copy.....	274
12.6.3 Configuring static multicast members of VLAN-Copy	274

12.6.4 Configuring VLAN-Copy user VLAN.....	275
12.7 Configuring PIM	275
12.7.1 Preparing for configurations	275
12.7.2 Enabling PIM.....	276
12.7.3 Configuring PIM domain DR election.....	276
12.7.4 Configuring PIM domain RP election.....	277
12.7.5 Configuring PIM multicast source	278
12.7.6 Switching from RPT to SPT	278
12.7.7 Checking configurations	279
12.7.8 Maintenance.....	280
12.8 Configuring MLD L2 multicast	280
12.8.1 Preparing for configurations	280
12.8.2 Configuring MLD basic function.....	280
12.8.3 Configuring MLD Snooping.....	281
12.8.4 Adjusting MLD performance	281
12.8.5 Configuring MLD filtering	283
12.8.6 Checking configurations	285
12.8.7 Maintenance.....	285
12.9 Configuring MLD L3 multicast	286
12.9.1 Configuring MLD basic functions on interface	286
12.9.2 Adjusting MLD performance	287
12.9.3 Checking configurations	288
12.9.4 Maintenance.....	288
13 OAM	289
13.1 Configuring EFM	289
13.1.1 Preparing for configurations	289
13.1.2 Configuring EFM basic functions.....	289
13.1.3 Configuring EFM active functions.....	290
13.1.4 Configuring EFM passive functions	291
13.1.5 Configuring link monitoring and fault indication	292
13.1.6 Configuring extended OAM	293
13.1.7 Checking configurations	294
13.2 Configuring CFM.....	294
13.2.1 Preparing for configurations	294
13.2.2 Enabling CFM.....	295
13.2.3 Configuring CFM basic functions.....	295
13.2.4 Configuring fault detection	296
13.2.5 Configuring fault acknowledgement.....	297
13.2.6 Configuring fault location.....	298
13.2.7 Configuring AIS.....	299
13.2.8 Configuring LCK	300

13.2.9 Configuring CSF	300
13.2.10 Checking configurations	301
13.3 Configuring BFD	302
13.3.1 Preparing for configurations	302
13.3.2 Configuring BFD for IP	302
13.3.3 Configuring BFD for PW	303
13.3.4 Configuring BFD for VRF	304
13.3.5 Configuring BFD Trap	305
13.3.6 Checking configurations	305
13.4 Configuring SLA	305
13.4.1 Preparing for configurations	305
13.4.2 Configuring Y.1731-based SLA	306
13.4.3 Configuring SLA operation scheduling	307
13.4.4 Checking configurations	308
13.5 Configuring RFC2544	308
13.5.1 Configuring type of test packets	308
13.5.2 Configuring RFC2544 delay test	309
13.5.3 Configuring RFC2544 packet loss test	309
13.5.4 Configuring RFC2544 throughput test	310
13.5.5 Configuring RFC2544 operation scheduling	310
13.5.6 Checking configurations	311
13.6 Configuring Y.1564	311
13.6.1 Configuring service throughput test operation	311
13.6.2 Configuring service performance test operation	314
13.6.3 Configuring Y.1564 operation scheduling	317
13.6.4 Checking configurations	317
13.7 Configuring SLA test alarm	317
13.8 Configuring interface loopback	318
13.8.1 Preparing for configurations	318
13.8.3 Configuring loopback duration	319
13.8.4 Checking configurations	319
13.9 Configuring ULDP	319
13.10 Maintenance	320
14 Security	321
14.1 Configuring storm control	321
14.1.1 Preparing for configurations	321
14.1.2 Configuring storm control	322
14.1.3 Checking configurations	322
14.2 Configuring CPU protection	322
14.2.1 Preparing for configurations	322
14.2.2 Configuring global CPU CAR	323

14.2.3 Clear statistics	323
14.2.4 Checking configurations	323
14.3 Configuring CPU monitoring	323
14.3.1 Preparing for configurations	323
14.3.2 Configuring CPU monitoring alarm.....	324
14.4 Configuring RADIUS	324
14.4.1 Preparing for configurations	324
14.4.2 Configuring IPv4 RADIUS authentication	325
14.4.3 Configuring IPv6 RADIUS authentication	325
14.4.4 Configuring IPv4 RADIUS accounting	326
14.4.5 Configuring IPv6 RADIUS accounting	326
14.4.6 Checking configurations	327
14.5 Configuring TACACS+	327
14.5.1 Preparing for configurations	327
14.5.2 Configuring IPv4 TACACS+ authentication.....	327
14.5.3 Configuring IPv6 TACACS+ authentication.....	327
14.5.4 Configuring IPv4 TACACS+ accounting.....	328
14.5.5 Configuring IPv6 TACACS+ accounting.....	328
14.5.6 Checking configurations	329
14.6 Configuring RADIUS/TACACS+ accounting management	329
14.6.1 Configuring accounting policy.....	329
14.6.2 Configuring user management	330
14.6.3 Checking configurations	330
14.6.4 Configuring basic dot.1x.....	330
14.6.5 Configuring Dot.1X re-authentication	331
14.6.6 Configuring Dot.1X timer.....	332
14.6.7 Checking configurations	332
14.6.8 Maintenance	332
14.7 Configuring interface isolation.....	333
14.7.1 Preparing for configurations	333
14.7.2 Configuring interface isolation	333
14.7.3 Configuring VLAN isolation	333
14.7.4 Checking configurations	333
14.7.5 Checking configurations	334
14.8 Configuring port mirroring.....	334
14.8.1 Preparing for configurations	334
14.8.2 Configuring port mirroring	334
14.8.3 Checking configurations	335
14.9 Configuring PPPoE+	335
14.9.1 Preparing for configurations	335
14.9.2 Configuring PPPoE+ basic functions.....	336
14.9.3 Configuring PPPoE+ packet information.....	337

14.9.4 Checking configurations	339
14.9.5 Maintenance	339
14.10 Configuring dynamic ARP inspection	339
14.10.1 Preparing for configurations	339
14.10.2 Configuring trusted interface of dynamic ARP inspection.....	339
14.10.3 Configuring static binding of dynamic ARP inspection.....	340
14.10.4 Configuring dynamic binding of dynamic ARP inspection.....	340
14.10.5 Configuring protection VLAN of dynamic ARP inspection	340
14.10.6 Checking configurations	340
15 Reliability	341
15.1 Configuring link aggregation	341
15.1.1 Preparing for configurations	341
15.1.2 Configuring manual link aggregation	342
15.1.3 Configuring static LACP link aggregation.....	342
15.1.4 Configuring manual backup link aggregation.....	344
15.1.5 Configuring static LACP backup link aggregation	344
15.1.6 Configuring mLACP link aggregation.....	345
15.1.7 Checking configurations	347
15.2 Configuring interface backup	347
15.2.1 Preparing for configurations	347
15.2.2 Configuring interface backup group	348
15.2.3 Checking configurations	348
15.3 Configuring ELPS	349
15.3.1 Preparing for configurations	349
15.3.2 Creating protection pair	349
15.3.3 Configuring ELPS fault detection modes.....	350
15.3.4 (Optional) configuring ELPS switching control	351
15.3.5 Checking configurations	352
15.4 Configuring ERPS.....	352
15.4.1 Preparing for configurations	352
15.4.2 Creating ERPS protection ring.....	353
15.4.3 (Optional) creating ERPS protection tributary ring	354
15.4.4 Configuring ERPS fault detection modes	356
15.4.5 (Optional) configuring ERPS switching control	356
15.4.6 Checking configurations	357
15.5 Configuring VRRP	357
15.5.1 Preparing for configurations	357
15.5.2 Configuration procedure	357
15.5.3 Configuring VRRP backup group	358
15.5.4 Configuring VRRPv3 backup group	359
15.5.5 (Optional) configuring ping function of VRRP virtual IP address	360

15.5.6 Configuring VRRP/VRRPv3 monitoring interface	360
15.5.7 Configuring VRRP/VRRPv3 fast switching	360
15.5.8 Checking configurations	361
15.6 Configuring link-state tracking	361
15.6.1 Preparing for configurations	361
15.6.2 Creating a link-state group	361
15.6.3 Configuring fault processing action of link-state group	363
15.6.4 Checking configurations	363
15.7 Configuring PW redundancy protection	364
15.7.1 Preparing for configurations	364
15.7.2 Configuring PW redundancy protection	364
15.7.3 Binding service PW with management PW	364
15.7.4 Checking configurations	365
15.8 Maintenance	365
16 Appendix	367
16.1 Terms	367
16.2 Acronyms and abbreviations	369

Figures

Figure 1-1 Direct connection.....	9
Figure 1-2 USB connection.....	10
Figure 1-3 Out-of-band network management.....	10
Figure 1-4 Configuring parameters for Hyper Terminal	11
Figure 1-5 Working as the Telnet server.....	12
Figure 1-6 Working as the Telnet client	13
Figure 7-1 Proxy ARP application scenario	100
Figure 10-1 CCC local connection.....	231
Figure 12-1 IGMP Snooping scenario.....	266
Figure 12-2 IGMP MVR application	269
Figure 12-3 Multicast VLAN copy scenario	273
Figure 15-1 VRRP configuration procedure.....	358

1 Basic configurations

This chapter describes basic information and configuration procedures of the RAX711-C-R and provides related configuration examples, including following sections:

- CLI
- Connecting device and log
- Backup and upgrade
- Device management
- Configuring RMON

1.1 CLI

1.1.1 Overview

The Command Line Interface (CLI) is a medium for you to communicate with the RAX711-C-R. You can configure, monitor, and manage the RAX711-C-R through the CLI.

You can log in to the RAX711-C-R 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 RAX711-C-R locally through the Console interface.
- Configure the RAX711-C-R 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 RAX711-C-R.
- Enter a question mark (?) at the system prompt to obtain online help.
- The RAX711-C-R supports multiple intelligent analysis methods, such as fuzzy match and context association.

1.1.2 Levels

The RAX711-C-R 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

Entering user EXEC mode through user name

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 RAX711-C-R, if the RAX711-C-R adopts default configurations, a Login prompt will be displayed. Enter the default user name (raisecom) and password (raisecom) to enter the user EXEC mode, where the following command is displayed:

```
Raisecom>
```

Entering privileged EXEC mode through Enable command

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 prompt 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.
- 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 RAX711-C-R are listed in the following table.

Mode	Entry	Prompt
User EXEC	Log in to the RAX711-C-R, 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 gig Ethernet unit/slot/port command.	Raisecom(config-gigaethernetunit/slot/port)#
	In global configuration mode, use the interface tengigabitethernet unit/slot/port command.	Raisecom(config-tengigabitethernetunit/slot/port)#
Sub-interface configuration	In global configuration mode, use the interface gig Ethernet unit/slot/port.sub-interface command.	Raisecom(config-gigaethernetsubif)#
VLAN interface configuration	In global configuration mode, use the interface vlan vlan-id command.	Raisecom(config-vlanif)#
Tunnel interface configuration	In global configuration mode, use the interface tunnel tunnel-id command.	Raisecom(config-tunnel)#
Loopback interface configuration	In global configuration mode, use the interface loopback interface-number command.	Raisecom(config-loopback)#
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)#

Mode	Entry	Prompt
OSPFv3 configuration	In global configuration mode, use the ipv6 router ospf <i>process-id</i> [vrf <i>vrf-name</i>] command.	Raisecom(config-ospf6)#
BGP configuration	In global configuration mode, use the router bgp [<i>as-id</i>] command.	Raisecom(config-router)#
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 <i>vrf-name</i> command.	Raisecom(config-router-af)#
VLAN configuration	In global configuration mode, use the vlan <i>vlan-id</i> command.	Raisecom(config-vlan)#
Basic IP ACL configuration	In global configuration mode, use the access-list <i>acl-number</i> command. The <i>acl-number</i> parameter ranges from 1000 to 1999.	Raisecom(config-acl-ipv4-basic)#
Extended IP ACL configuration	In global configuration mode, use the access-list <i>acl-number</i> command. The <i>acl-number</i> parameter ranges from 2000 to 2999.	Raisecom(config-acl-ipv4-advanced)#
MAC ACL configuration	In global configuration mode, use the access-list <i>acl-number</i> command. The <i>acl-number</i> parameter ranges from 3000 to 3999.	Raisecom(config-acl-mac)#
User ACL configuration	In global configuration mode, use the access-list <i>acl-number</i> command. The <i>acl-number</i> parameter ranges from 5000 to 5999.	Raisecom(config-acl-map)#
cos-remark configuration	In global configuration mode, use the mls qos mapping cos-remark <i>profile-id</i> command.	Raisecom(cos-remark)#
cos-to-pri configuration	In global configuration mode, use the mls qos mapping cos-to-local-priority <i>profile-id</i> command.	Raisecom(cos-to-pri)#
dscp-mutation configuration	In global configuration mode, use the mls qos mapping dscp-mutation <i>profile-id</i> command.	Raisecom(dscp-mutation)#
dscp-to-pri configuration	In global configuration mode, use the mls qos mapping dscp-to-local-priority <i>profile-id</i> command.	Raisecom(dscp-to-pri)#

Mode	Entry	Prompt
exp-to-pri configuration	In global configuration mode, use the mls qos mapping exp-to-local-priority <i>profile-id</i> command.	Raisecom(exp-to-pri)#
pri-to-exp configuration	In global configuration mode, use the mls qos mapping local-priority-to-exp <i>profile-id</i> command.	Raisecom(pri-to-exp)#
WRED profile configuration	In global configuration mode, use the mls qos wred profile <i>profile-id</i> 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 <i>class-map-name</i> command.	Raisecom(config-cmap)#
Traffic monitoring profile configuration	In global configuration mode, use the mls qos policer-profile <i>policer-name</i> [single] command.	Raisecom(traffic-policer)#
PMP configuration	In global configuration mode, use the policy-map <i>policy-map-name</i> command.	Raisecom(config-pmap)#
Traffic policy bound with traffic classification configuration	In PMP configuration mode, use the class-map <i>class-map-name</i> command.	Raisecom(config-pmap-c)#
Service instance configuration	In global configuration mode, use the service <i>instance-name</i> level <i>md-level</i> command.	Raisecom(config-service)#
BFD session configuration	In global configuration mode, use the bfd <i>session-id</i> command.	Raisecom(config-bfd-session)#
	In global configuration mode, use the bfd <i>session-id</i> bind peer-ip <i>ip-address</i> [vrf-name <i>vrf-name</i>] command.	
	In global configuration mode, use the bfd <i>session-id</i> bind peer-ip <i>ip-address</i> interface gigaethernet <i>interface-number</i> command.	
	In global configuration mode, use the bfd <i>session-id</i> bind ldp-lsp peer-ip <i>ip-address</i> <i>ip-mask</i> command.	
	In global configuration mode, use the bfd <i>session-id</i> bind mpls interface tunnel <i>tunnel-if</i> cr-lsp command.	

Mode	Entry	Prompt
	In global configuration mode, use the bfd session-id bind pw vc-id peer-ip [pw-ttl ttl] command.	

1.1.4 Shortcut keys

The RAX711-C-R supports the following shortcut keys.

Shortcut key	Description
Up arrow (↑)	The previous command is displayed. If no previous command is available, no change is shown on the screen after you press the key.
Down arrow (↓)	The next command is displayed. If no previous command is available, no change is shown on the screen after you press the key.
Left arrow (←)	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.
Right arrow (→)	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.
Backspace	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.
Tab	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 keyword, you can press the Tab key to wrap, and then error information is displayed.
Ctrl+A.	Move the cursor to the beginning of the command line.
Ctrl+D or the Delete	Delete the character at the cursor.
Ctrl+E	Move the cursor to the end of the command line.
Ctrl+K	Delete all characters from the cursor to the end of the command line.

Shortcut key	Description
Ctrl+X	Delete all characters from the cursor to the beginning of the command line.
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
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
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 RAX711-C-R on the CLI.

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

1.2 Connecting device and logging in

1.2.1 Connecting device

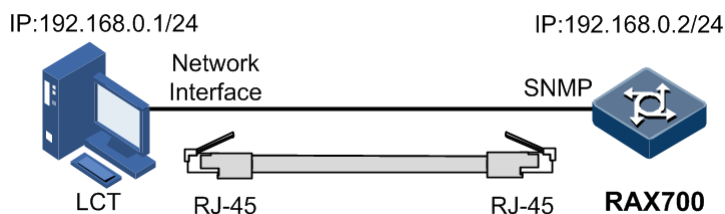
Users can log in to the device for configuration management through direct connection and network connection.

Direct connection

- Direction connection through a network cable

As shown in Figure 1-1, directly connect the SNMP 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.

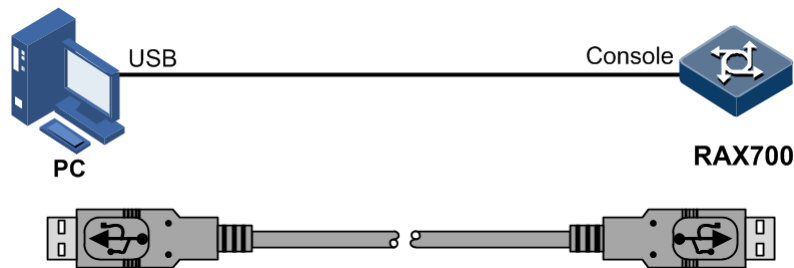
Figure 1-1 Direct connection



- 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

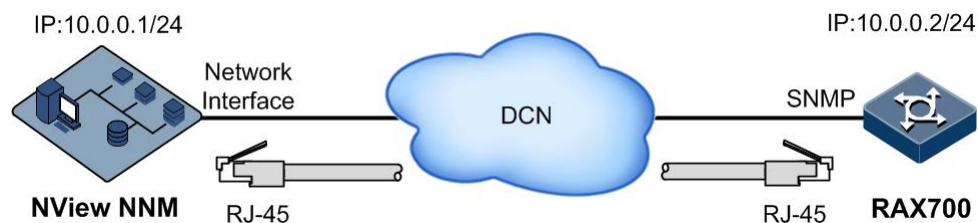


Network connection

The device supports out-of-band network management.

As shown in Figure 1-3, the device is connected to the DCN through the SNMP interface NEG, 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



1.2.2 Accessing device through Console interface



Note

The Console interface of the RAX711-C-R is a Universal Serial Bus (USB) A-shaped female interface, which is translated into a Universal Asynchronous Receiver/Transmitter (UART) in the device.

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 RAX711-C-R through this interface. This management method does not involve network communication.

You must log in to the RAX711-C-R through the Console interface under the following 2 conditions:

- The RAX711-C-R is powered on for the first time.
- You cannot log in to the RAX711-C-R through Telnet.

To log in to the RAX711-C-R through the Console interface, follow these steps:

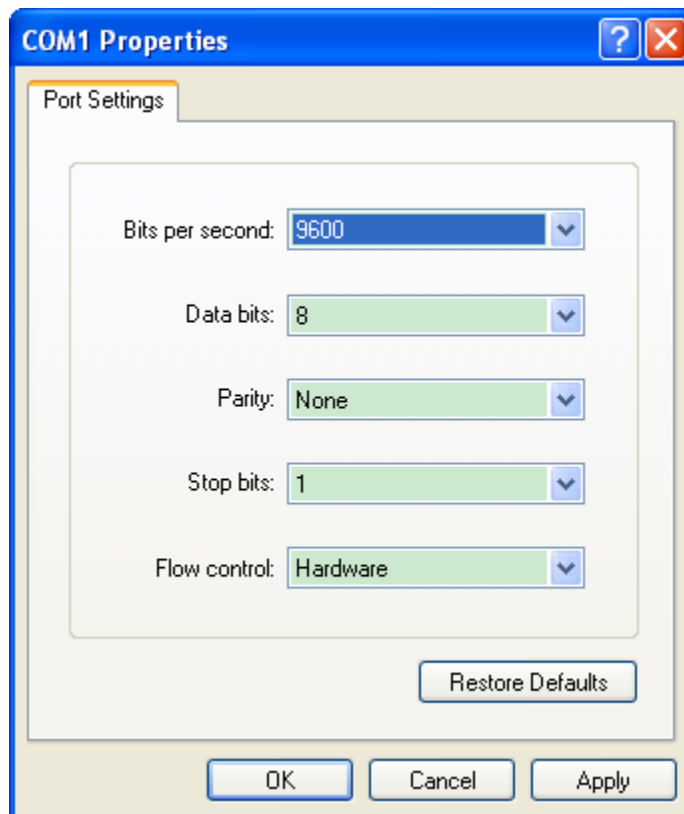


Note

Before logging in to the RAX711-C-R through the USB interface, install the driver for translating the USB interface into the UART interface to the PC.

- Step 1 Use an USB configuration cable to connect the Console interface of the RAX711-C-R 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**

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 RAX711-C-R. 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.

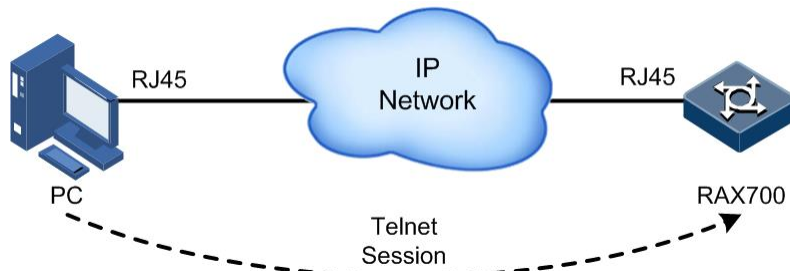
1.2.3 Accessing device through Telnet

Through Telnet, you can remotely log in to the RAX711-C-R through a PC and then log into other devices on the network through Telnet. In this way, it is not necessary to prepare a PC for each RAX711-C-R.

The RAX711-C-R provides the following Telnet services:

- Telnet Server: as shown in Figure 1-5, connect the PC and the RAX700 and start the terminal maintenance software on the PC. After selecting proper parameters, you can log in to the RAX700 for configuration and management.

Figure 1-5 Working as the Telnet server



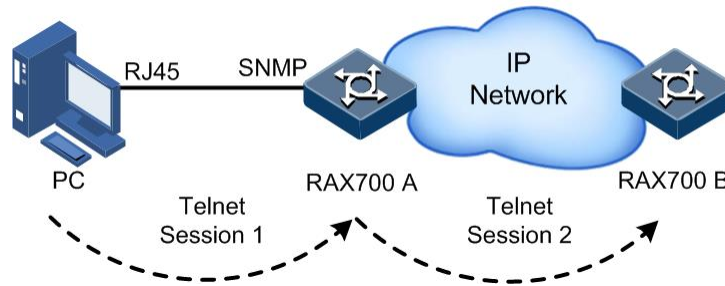
Note

For logging in to the RAX711-C-R through Telnet for the first time, you must log in to the RAX711-C-R 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)#interface fastethernet 1/0/1	Enter SNMP interface configuration mode.
3	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, it is 192.168.4.28.
4	Raisecom(config)#telnet-server accept interface-type interface-list	(Optional) configure the interface that supports Telnet.
5	Raisecom(config)#telnet-server close terminal-telnet session-number	(Optional) close the specified Telnet session.
6	Raisecom(config)#telnet-server max-session session-number	(Optional) configure the maximum number of Telnet sessions supported by the RAX711-C-R. By default, it is 10.
7	Raisecom(config)#telnet-server access-list acl-number	Configure Telnet server based on ACL.

- Telnet Client: after connecting the RAX711-C-R 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, RAX700 A works as Telnet Server and Telnet Client.

Figure 1-6 Working as the Telnet client



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

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 RAX711-C-R supports SSHv2.

Before accessing the RAX711-C-R through SSHv2, you must log in to the RAX711-C-R through the Console interface and enable SSH service.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#generate ssh-key length</code>	Generate local SSHv2 key pair and designate its length.
3	<code>Raisecom(config)#ssh2 server</code>	Start the SSHv2 server.
4	<code>Raisecom(config)#ssh2 server authentication { password rsa-key }</code>	(Optional) configure SSHv2 authentication method.

Step	Command	Description
5	<code>Raisecom(config)#ssh2 server authentication-timeout <i>period</i></code>	(Optional) configure SSHv2 authentication timeout. The RAX711-C-R refuses to authenticate and open the connection when client authentication time exceeds the upper threshold.
6	<code>Raisecom(config)#ssh2 server authentication-retries <i>times</i></code>	(Optional) configure the allowable times for SSHv2 authentication failure. The RAX711-C-R refuses to authenticate and open the connection when client authentication failure times exceed the upper threshold.
7	<code>Raisecom(config)#ssh2 server port <i>port-id</i></code>	(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.
8	<code>Raisecom(config)#show ssh2 { server session }</code>	(Optional) show information about the SSHv2 server or the session end.
9	<code>Raisecom(config)#show ssh2 public-key [authentication]</code>	(Optional) show the public key for SSHv2 authentication on the device and the client.

1.3 Backup and upgrade

1.3.1 Introduction

The RAX711-C-R 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 RAX711-C-R, including the BootROM file, License file, Paf file, patch 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 RAX711-C-R, including the BootROM file, system configuration file, system startup file and FPGA file. These files are saved to the memory of the RAX711-C-R.

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

The system supports dual-system software, offering primary and backup systems.

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 RAX711-C-R. You can upgrade the BootROM software if a new version is available.

System startup file

The system startup file (with the .z suffix) is used to start and operate the RAX711-C-R, 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 RAX711-C-R 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, such as, local and remote zero-configuration mode. It is able to confirm specifications supported by the device according to the parameter range. The following examples show several important parameter ranges:

- ZERO_CONFIG_MODE_CLIENT: the value 0 indicates disabling remote zero-configuration while the value 1 indicates enabling remote zero-configuration.
- ZERO_CONFIG_MODE_CLIENT: if ZERO_CONFIG_MODE_CLIENT=1, the value 0 indicates disabling China Telecom zero-configuration while the value 1 indicates enabling China Telecom zero-configuration. The zero-configuration scheme for China Telecom is to request the IP address on the first uplink interface.
- ZERO_CONFIG_MANAGE_VLAN: the value 0 indicates that the VLAN management is not configured. All VLANs are covered when the IP address is automatically obtained.

After configuring parameters is complete, you could download parameters to the device through the **download** command and reboot the RAX711-C-R through the **reboot** command. Then the RAX711-C-R 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 suffix) is configuration items to be loaded when the device is booted at this time or next time.

After being powered on, the RAX711-C-R reads the configuration file from the memory for initialization. If there is no configuration file in the memory, the RAX711-C-R 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 RAX711-C-R 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 RAX711-C-R fails. By doing so, the RAX711-C-R will run normally as before. The pervious system file should be restored under the following conditions:

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

The RAX711-C-R 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 RAX711-C-R supports 2 upgrade modes:

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

1.3.2 Backing up system

You need to establish a FTP/TFTP environment before backing up system files. Generally, you can use a PC to serve as the FTP/TFTP server and the RAX711-C-R as the client, with the basic requirements as below:

- Connect the RAX711-C-R to the PC through the SNMP interface.
- Configure the IP address of the PC to interconnect with the RAX711-C-R.

IPv4-based network

Step	Command	Description
1	<code>Raisecom#upload { running-config startup-config backup-config } { ftp ip-address username password ftp-active ip-address username password tftp ip-address } [source source-address] filename</code>	Upload the system bootstrap files and system configuration files to the backup server.
2	<code>Raisecom#upload { accident-logfile command-logfile alarm-logfile running-logfile all-logfile } { ftp ip-address username password ftp-active ip-address username password tftp ip-address } [source source-address] filename</code>	Back up the log file to the server.

IPv6-based network

Step	Command	Description
1	Raisecom# upload { running-config startup-config backup-config } { ftp <i>ipv6-address username password</i> ftp-active <i>ipv6-address username password</i> tftp <i>ipv6-address</i> } [source <i>source-address</i>] <i>filename</i>	Upload the system bootstrap file and system configuration file to the backup server.
2	Raisecom# upload { accident-logfile command-logfile alarm-logfile running-logfile all-logfile } { ftp <i>ipv6-address username password</i> ftp-active <i>ipv6-address username password</i> tftp <i>ipv6-address</i> } [source <i>source-address</i>] <i>filename</i>	Back up the log system file to the server.

1.3.3 Upgrading system

Upgrading files in privileged EXEC mode

You need to establish a FTP/TFTP environment before upgrading system files. Generally, you can use a PC to serve as the FTP/TFTP server and the RAX711-C-R to be the client, with the basic requirements as below:

- Connect the RAX711-C-R to the PC through the SNMP interface.
- Configure the IP address of the PC to interconnect with the RAX711-C-R.

Step	Command	Description
1	Raisecom# download { system1 system2 bootstrap cp1d startup-config backup-config paf file } { ftp <i>ip-address username password</i> ftp-active <i>ip-address username password</i> tftp <i>ip-address</i> } [source <i>source-address</i>] <i>filename</i> [dir]	In IPv4-based networks, download system files through FTP or TFTP.
2	Raisecom# download { system1 system2 bootstrap cp1d startup-config backup-config paf file } { ftp <i>ipv6-address username password</i> ftp-active <i>ipv6-address username password</i> tftp <i>ipv6-address</i> } [source <i>source-address</i>] <i>filename</i> [dir]	In IPv6-based networks, download system files through FTP or TFTP.
3	Raisecom# boot next-startup { system1 system2 }	Specify the next bootstrap file for the device. The device supports dual-system software, offering primary and backup systems.
4	Raisecom# reboot [now] [in <i>minutes</i>]	Restart the device. The device will automatically load the downloaded system startup file.
5	Raisecom# show version	Show the device version.

Upgrading files in BootROM mode

Under the following conditions, you need to upgrade system software through BootROM mode.

- First startup
- System file damage
- Startup failure

You need to establish a FTP environment before upgrading system software in BootROM mode. Generally, you can use a PC to serve as the FTP server and the RAX711-C-R to be the client, with the basic requirements as below:

- Connect the RAX711-C-R to the FTP server through SNMP interface.
- Configure the FTP server to make it available.

Step	Operation
1	Log in to the device through the Console interface as an administrator and enter privileged EXEC mode, and then use the reboot command to restart the device. <pre> Raisecom#reboot Raisecom#reboot Please input 'yes' to confirm:yes 1970-01-01,08:02:42 [ros-scrnBg_0]System-4-SYSTEM_REBOOT:22 Reboot!!! 1970-01-01,08:02:54 [ros-scrnBg_0]System-4-SYSTEM_REBOOT:22 Reboot!!! booting... soc_pcie_hw_init : port->reg_base = 0x18012000 , its value = 0x1 PCIE port 0 in RC mode pos is 172 ==>PCIE: LINKSTA reg 0xbe val 0x1001 ***** port 0 is not active!! ***** GPIO:init Raisecom boot loader bootrom version 1.0.0 Raisecom Technology CO., LTD. Compiled Base Ethernet MAC address: 00:00:01:02:03:04 Press Ctrl+D to enter bootrom menu: 3 MBOOT MENU V1.1 1: Boot system from flash 2: Select default boot system 3: Update system from tftp 4: Update mboot from tftp 5: Update fpga from tftp 0: Reboot Press Up/Dwon or Number to move,Enter your choice: 3 Index Name Size ----- 1* system1.z_9.0.0.20200420 27994264 2 system2.z_9.0.0.20200420 27994264 Current selected version is 1 Please select a version to overwrite: Raisecom#rebootinput number error. sys - Download system image and update to flash </pre>
2	Enter the following information according to the prompt: Current selected version is 2

Step	Operation
	Please select a version to overwrite: 2 Local IP Address[192.168.4.28]:192.168.4.28 Server IP Address[192.168.4.172]:192.168.4.174 Filename [system.bin]:system1.z_9.0.0.20200420
3	After the downloading is completed, load the downloaded system software according to the prompt and start the new software version.

1.3.4 Checking configurations

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

1.4 Device management

1.4.1 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 NMS can manage all network devices that support SNMP, including monitoring network status, modifying configurations of a network device, and receiving network alarms. SNMP is the most widely used network management protocol in TCP/IP networks

Working mechanism

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

The RAX711-C-R communicates with the network management system through SNMP packets. Raisecom Nview NNM system can provide friendly Human Machine Interface (HMI) to facilitate network management. The following functions can be implemented through it:

- Send request packets to the RAX711-C-R.
- Receive reply packets and Trap packets from the RAX711-C-R, and show result.

The Agent is a program installed in the RAX711-C-R, implementing the following functions:

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

- 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 network management system through Agent to report current status of device.



Note

An Agent can be configured with several versions concurrently, and different versions communicate with different 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 RAX711-C-R, the packet will be dropped.
- Compatible with SNMPv1, SNMPv2c also uses community name authentication mechanism. SNMPv2c supports more operation types, data types, and error 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 RAX711-C-R supports SNMPv1, SNMPv2c, and SNMPv3.

MIB

Management Information Base (MIB) is the collection of all objects managed by NMS. It defines attributes for the managed objects:

- Name
- Access right
- Data type

The device-related statistic contents can be reached by accessing data items. Each proxy has its own MIB. MIB can be taken as an interface between NMS and Agent, through which NMS can read/write every managed object in Agent to manage and monitor the RAX711-C-R.

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 RAX711-C-R supports standard MIB and Raisecom-customized MIB.

1.4.2 Preparing for configurations

Scenario

To log in to the RAX711-C-R through the NMS, you should first configure SNMP basic functions.

Prerequisite

- Configure the IP addresses on the SNMP interface.
- Configure static router to link RAX711-C-R and NMS through the router.

1.4.3 Configuring SNMP basic functions

For SNMPv3, SNMPv1 or SNMPv2c, you should configure them respectively:

Configure SNMPv3 on the target device as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#snmp-server access <i>group-name</i> [read <i>view-name</i>] [write <i>view-name</i>] [notify <i>view-name</i>] [context <i>context-name</i> { exact prefix }] usm { noauthnopriv authnopriv authpriv }	Create and configure the SNMP access groups.
3	Raisecom(config)#snmp-server group <i>name</i> user <i>user</i> usm	(Optional) configure the mapping between users and access groups.
4	Raisecom(config)#snmp-server contact <i>syscontact</i>	(Optional) configure the ID and contact of network administrators.
5	Raisecom(config)#snmp-server host { <i>ip-address</i> <i>ipv6-address</i> } version 3 { noauthnopriv authnopriv authpriv } <i>user-name</i> [udpport <i>udpport</i>]	Configure the IP address of the SNMP target host.
6	Raisecom(config)#snmp-server location <i>sysLocation</i>	(Optional) specify the location for placing the RAX711-C-R.
7	Raisecom(config)#snmp-server user <i>user-name</i> [remote <i>engine-id</i>] authentication { md5 sha } <i>key-word</i> [privacy <i>privkey-value</i>]	Create a SNMP user name and configure the authentication algorithm, authentication password, and encryption password.
8	Raisecom(config)#snmp-server user <i>user-name</i> [remote <i>engine-id</i>] authkey { md5 sha } <i>authkey-word</i> [privkey <i>privkey-value</i>]	Add a SNMP user and specify the authentication algorithm, authentication password, and encryption password.
9	Raisecom(config)#snmp-server view <i>view-name</i> <i>oid-tree</i> [<i>mask</i>] { 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 <i>name [view view] { ro rw }</i>	Create a community name and configure its corresponding view and access priority.
3	Raisecom(config)#snmp-server contact <i>contact</i>	(Optional) configure the ID and contact of network administrators.
4	Raisecom(config)#snmp-server host { <i>ip-address</i> <i>ipv6-address</i> } version { <i>1</i> <i>2c</i> } <i>community-string [udpport port-id]</i>	Configure the IP address of the SNMP target host.
5	Raisecom(config)#snmp-server location <i>location</i>	(Optional) specify the location for placing the RAX711-C-R.

1.4.4 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 RAX711-C-R to send unrequested information to the network management system 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 RAX711-C-R and the network management system is available.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#ip address <i>ip-address</i> <i>vlan-id</i>	Configure the IP address of the RAX711-C-R.
4	Raisecom(config-port)#ipv6 address <i>ipv6-address/prefix-length</i> [<i>eui-64</i>]	Configure the IPv6 address of the interface.
5	Raisecom(config-port)#exit	Exit Layer 3 physical interface configuration mode. Enter global configuration mode.
6	Raisecom(config)#snmp-server host { <i>ip-address</i> <i>ipv6-address</i> } version <i>3</i> { <i>noauthnopriv</i> <i>authnopriv</i> <i>authpriv</i> } <i>name [udpport udpport]</i>	(Optional) configure the SNMPv3 Trap target host.
7	Raisecom(config)#snmp-server host { <i>ip-address</i> <i>ipv6-address</i> } version { <i>1</i> <i>2c</i> } <i>name [udpport udpport]</i>	(Optional) configure the SNMP v1 and SNMP v2c Trap target host.

1.4.5 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.

1.5 Configuring RMON

1.5.1 Introduction

Remote Network Monitoring (RMON) is a standard stipulated by IETF (Internet Engineering Task Force) for network data monitoring through different network Agent and 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 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.

1.5.2 Preparing for configurations

Scenario

RMON helps monitor and gather statistics about network traffics.

Compared with SNMP, RMON is a more high-efficient monitoring method. After you specify an alarm threshold, the RAX711-C-R 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 RAX711-C-R and the network management system is reachable.

1.5.3 Configuring RMON alarm group

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

1.5.4 Configuring RMON event group

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

1.5.5 Configuring RMON statistics

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

1.5.6 Configuring RMON history statistics

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#rmon history { <i>interface-type</i> <i>interface-number</i> ip <i>if-</i> <i>number</i> } [shortinterval <i>period</i>] [longinterval <i>period</i>] [buckets <i>buckets-number</i>] [ownerstring]	Enable RMON history statistics on an interface and configure related parameters. By default, RMON history statistics on all interfaces is disabled.

1.5.7 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 statisttics	Show information about the RMON statistics group.
5	Raisecom#show rmon history <i>interface-type interface-</i> <i>number</i>	Show information about the RMON history group.

2 System management

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

- User management
- Fan management
- Saving configurations
- Time management
- Log management
- File management
- Alarm management
- Key chain management

2.1 User management

When you start the RAX711-C-R 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 RAX711-C-R.



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 RAX711-C-R 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 RAX711-C-R and network. Creating user and setting password and privilege help to manage the login users and ensure network and device security.

2.1.1 Configuring user management

Step	Command	Description
1	<code>Raisecom#user name <i>user-name</i> password <i>password</i></code>	Create or modify the user name and password. You can delete a created user through the no username command.

Step	Command	Description
2	Raisecom#user name <i>user-name</i> privilege <i>privilege-level</i>	Configure the level and privilege of the user.

2.1.2 Checking configurations

No.	Command	Description
1	Raisecom#show user { active [onlineid <i>online-id</i> table [detail username <i>username</i>]	Show user information.

2.2 Fan management

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

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#fan-monitor mode { auto enforce }	Configure the working mode of the fan, including automatic mode and forced mode.
3	Raisecom(config)#fan-monitor enforce level <i>level-id</i>	Configure the fan rotating level in forced working mode.
4	Raisecom(config)#fan-monitor trap send enable	Enable fan monitoring.
5	Raisecom(config)#fan-monitor temperature-scale <i>temperature1 temperature2 temperature3</i>	Configure the critical temperature corresponding to the rotating level.
6	Raisecom#show fan-monitor information	Show the running information about the fan.
7	Raisecom#show fan-monitor status	Show the fan status.

2.3 Saving configurations

No.	Command	Description
1	Raisecom#write	Saving current configurations
2	Raisecom#auto-write enable	(Optional) enable auto-saving of configurations

No.	Command	Description
	<code>Raisecom#auto-write interval minutes</code>	

2.4 Time management

2.4.1 Configuring time and time zone

To ensure that the RAX711-C-R can cooperate with other devices, you need to configure system time and time zone precisely for the RAX711-C-R.

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

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	<code>Raisecom#clock summer-time enable</code>	Enable DST on the RAX711-C-R. By default, DST is disabled.
2	<code>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-min</code>	Configure the start time, end time, and offset of DST.



Note

- 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 adjusted forward 60 minutes. Thus, the 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 server { <i>ip-address</i> <i>ipv6-address</i> } [version <i>version-number</i>] [keyid <i>key-id</i>]	(Optional) configure the NTP server address for the client working in server/client mode.
3	Raisecom(config)#ntp peer { <i>ip-address</i> <i>ipv6-address</i> } [version <i>version-number</i>] [keyid <i>key-id</i>]	(Optional) configure the NTP peer address for the device working in peer mode.
4	Raisecom(config)#sntp server { <i>ip-address</i> <i>ipv6-address</i> } version { v1 v2 v3 v4 }	Configure the IP address of the SNTP server for the device working in SNTP client mode.
5	Raisecom(config)#ntp refclock-master <i>ip-address</i> [<i>stratum</i>]	Configure the local device as the NTP master clock, namely, the reference clock. By default, the local device is not a reference clock source.

Configuring NTP identity authentication

In networks with high security requirements, authentication is required when using NTP. After identity verification is enabled, the NTP client only synchronizes with the verified server to ensure the security of the network. The NTP client will authenticate the server only when authentication is enabled. If authentication is not enabled, the client will not perform authentication even if the server carries key information, and will directly synchronize the time with the server.

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

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



Note

- If the device is configured as the NTP reference clock source, the configuration of the NTP server or NTP peer fails and cannot be synchronized by other devices. If the NTP server or peer is configured, the device will fail to be configured as a clock reference source.
- SNTP and NTP are mutually exclusive. 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	<code>Raisecom#show clock [summer-time recurring]</code>	Show configurations of the system time, time zone, and DST.
2	<code>Raisecom#show sntp</code>	Show SNTP obtaining time and whether configurations are correct.
3	<code>Raisecom#show ntp status</code>	Show NTP configurations.
4	<code>Raisecom#show ntp associations [detail]</code>	Show NTP connections.
5	<code>Raisecom#show ntp authentication</code>	Show information about NTP security.

2.5 Log management

2.5.1 Basic configurations of log management

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

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

2.5.2 Configuring log discriminator

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

2.5.3 Configuring log storage

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#logging buffered size <i>size</i></code>	Configure the size of the log buffer. By default, it is 4 kBytes.
3	<code>Raisecom(config)#logging file</code>	Save logs to the log file.
4	<code>Raisecom(config)#logging [host <i>ip-address</i>] 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 }</code>	Configure the facility type of logs in the log host. By default, it is local7.
5	<code>Raisecom(config)#logging history</code>	Save logs to the historical log table.
6	<code>Raisecom(config)#logging history size <i>size</i></code>	Configure the size of the historical log table. By default, it is 1.

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	Show log statistics in the buffer.

2.6 File management

2.6.1 Managing system files

No.	Command	Description
1	Raisecom#erase [<i>file-name</i> backup-config]	Delete files from the memory.  Caution Use this command with caution.
2	Raisecom#dir	Show system files.
3	Raisecom#show startup	Show system startup files.

2.7 Alarm management

An alarm refers to information generated by the system based on module failures when a fault is generated on the RAX711-C-R or some working condition changes.

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 network management system is configured, the alarm will be sent to it through SNMP. The information sent to the network management system 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 network management system when the network management system is configured

Alarms will be broadcasted according to various terminals configured on the RAX711-C-R, including CLI terminal and network management system.

Related concepts

Related concepts about alarm management are displayed as below:

- Alarm inhibition

The RAX711-C-R only records root-cause alarms but incidental alarms when enabling alarm inhibition. For example, the generation of alarm A will inevitably produce alarm B, then alarm B is inhibited and does not appear in the alarm buffer when enabling alarm inhibition. By enabling alarm inhibition, the RAX711-C-R can effectively reduce the number of alarms.

The root-cause alarm and all other incidental alarms will be recorded on the RAX711-C-R when alarm inhibition is disabled.

- Alarm auto-report

Auto-report refers that an alarm will be reported to the network management system automatically with its generation and the network management system 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.



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 RAX711-C-R.

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 network management system after a delay but not immediately when alarms generate. Delay for recording and reporting alarms are identical.

By default, an alarm is reported 5s later after it is generated and an alarm is cleared 5s later after it is finished.

- 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 RAX711-C-R, 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

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 RAX711-C-R. If the RAX711-C-R is configured with the network management system, the administrator can monitor alarms on the network management system.

2.7.1 Configuring alarm inhibition

The RAX711-C-R only records root-cause alarms but incidental alarms when enabling alarm inhibition. For example, the generation of alarm A will inevitably produce alarm B, then alarm B is inhibited and does not appear in the alarm buffer or record the log information when enabling alarm inhibition. By enabling alarm inhibition, the RAX711-C-R can effectively reduce the number of alarms. The root-cause alarm and all other incidental alarms will be recorded on the RAX711-C-R when alarm inhibition is disabled.

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

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.

Step	Command	Description
2	<code>Raisecom(config)#alarm active delay second</code>	Configure the alarm generation delay. By default, it is 0s.
3	<code>Raisecom(config)#alarm clear delay second</code>	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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#alarm active storage-mode { loop stop }</code>	Configure the alarm storage mode. By default, it is stop.

2.7.4 Configuring alarm clearance

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#alarm clear type module_name</code>	Clear alarms of a specified functional module.

2.7.5 Configuring alarm report

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

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

Step	Command	Description
2	Raisecom(config)#alarm auto-report interface-type interface-number enable	Enable alarm auto-report based on various types of interfaces, including Ethernet interface, sub-interface, loopback interface, and link aggregation interface. By default, it is enabled.
3	Raisecom(config)#alarm auto-report type module_name [group-name] [interface- type interface-number] 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 inverse refers to that the actual alarms are shielded when the interface is disabled or without services. In other words, the interface does not report an alarm when there is an alarm but reports an alarm when there is no 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 functional 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.
- 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, it is enabled.
3	Raisecom(config)#alarm monitor module_name [group-name] [interface-type interface- number] enable	Enable alarm monitoring based on functional module. By default, it is enabled.

Step	Command	Description
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 output to syslog. By default, it is enabled.

2.7.9 Checking configurations

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

2.8 Key chain management

2.8.1 Introduction

For the sake of security, the authentication information of the application layer needs to be continuously changed on the network. The authentication algorithm and the shared security key together can be used to determine whether information is tampered when it is transmitted on an unsecured network. When this authentication method is used to authenticate data, it is necessary to share the security key and authentication algorithm 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), a large number of applications will use 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 requires the manual intervention of the administrator, which is complicated and cumbersome. In addition, it is very difficult to change the password of all routers without packet loss.

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

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

2.8.2 Configuring key chain

No.	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#key-chain <i>key-chain-name</i>	Create a key chain and enter Keychain configuration mode.
3	Raisecom(config-keychain)#accept-tolerance { <i>time-value</i> infinite }	Configure the receiving-tolerance time.
4	Raisecom(config-keychain)#key <i>key-id</i> key-string [0 7] <i>keystring</i>	Configure the key and password string.
5	Raisecom(config-keychain)#key <i>key-id</i> send-lifetime <i>start-time</i> { duration <i>duration-time</i> <i>end-time</i> infinite }	Configure the key sending lifetime.
6	Raisecom(config-keychain)#key <i>key-id</i> accept-lifetime <i>start-time</i> { duration <i>duration-time</i> <i>end-time</i> infinite }	Configure the key receiving lifetime.

2.8.3 Checking configurations

No.	Command	Description
1	Raisecom#show key-chain	Show key configurations and statistics.
2	Raisecom#show key-chain <i>key-chain-name</i> key <i>key-id</i>	Show configurations and statistics of a specified key.

3 Zero-configuration

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

- Configuring CO zero-configuration
- Checking configurations

3.1 Configuring CO zero-configuration

3.1.1 Preparing for configurations

Scenario

- When the CO device connects with remote devices, the RAX711-C-R can discover these remote devices by using the extended OAM protocol and configure the management IP address, management VLAN, and default route for them. Therefore, the network management system can quickly manage remote devices through the public IP address and global interface ID of the RAX711-C-R without being configured manually.
- When the CO and remote devices are connected directly/indirectly, both the CO and remote devices can provide zero-configuration through Dynamic Host Configuration Protocol (DHCP).

Prerequisite

- The RAX711-C-R is a CO device.
- The CO zero-configuration server is connected to the network management system and remote devices properly.
- Perform the following operations on the CO device based on extended OAM protocol:
 - Create and activate the management VLAN.
 - Manually enable the OAM active mode on the interface.

3.1.2 Configuring zero-configuration Server based on extended OAM

The IP RAN local device assigns private IP addresses for remote devices through extended OAM zero-configuration, ensuring that routes are available between the local and remote devices. To implement NMS path protection, the remote device is connected to the local device through dual uplinks.

Configuring management VLAN

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#create vlan <i>vlan-id</i> active	Create and activate a VLAN.
3	Raisecom(config)#oam mng-vlan <i>vlan-id</i>	Configure the remote management VLAN of zero-configuration. By default, it is VLAN 0.  Note After configuring the management VLAN through this command, do not modify the switching property of downlink interfaces of the CO device. Otherwise, it may cause the remote device to be out of management.
4	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
5	Raisecom(config-port)#oam enable	Enable OAM. By default, the interface is enabled with OAM.
6	Raisecom(config-port)#oam active	Configure the OAM active mode of the interface.

Configuring ACL

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#access-list <i>acl-number</i>	Create an ACL and enter ACL configuration mode.
3	Raisecom(config-acl-ipv4-advanced)#rule [<i>rule-id</i>] permit ip <i>source-ip-address source-ip-mask</i> any	Configure the ACL rules. Packets with source IP addresses meeting the ACL rule will be reported to the CPU.
	Raisecom(config-acl-ipv4-advanced)#exit	Exit ACL configuration mode.

Configuring traffic classification rules

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#class-map <i>class-map-name</i> match all</code>	Create a traffic classifier and enter CMAP configuration mode.
3	<code>Raisecom(config-cmap)#match access-list <i>acl-number</i></code> <code>Raisecom(config-cmap)#exit</code>	Define traffic classification which should match the ACL filtering rules.
4	<code>Raisecom(config)#policy-map <i>policy-map-name</i></code>	Create a traffic policy and enter PMAP configuration mode.
5	<code>Raisecom(config-pmap)#class-map <i>class-map-name</i></code>	Add a traffic classification policy to the traffic policy and enter traffic policy configuration mode which binds with traffic classification.
6	<code>Raisecom(config-pmap-c)#forward-to-cpu</code> <code>Raisecom(config-pmap-c)#exit</code> <code>Raisecom(config-pmap)#exit</code>	Forward the traffic to the CPU.

Applying traffic classification to interface

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical interface configuration mode. The interface is an uplink interface, for connecting the public network.
3	<code>Raisecom(config-port)#switchport mode trunk</code>	Configure the interface to Trunk mode.
4	<code>Raisecom(config-port)#switchport trunk allowed vlan <i>vlan-id</i> [confirm]</code>	Configure the VLANs allowed to pass in Trunk mode.
5	<code>Raisecom(config-port)#oam active</code>	Configure the OAM active mode.
6	<code>Raisecom(config-port)#service-policy ingress <i>policy-map-name</i></code>	Apply the traffic classification rule in the ingress direction of the interface.

Configuring address pool and gateway

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

Step	Command	Description
2	Raisecom(config)# ip oam server pool <i>pool-name</i>	Configure the address pool of the OAM property and enter address pool configuration mode.
3	Raisecom(config-pool)# address <i>start-ip-address end-ip-address mask { mask-address mask-length }</i>	Configure the IP address range and subnet mask of the address pool.
4	Raisecom(config-pool)# gateway ip-address	Configure the gateway of the address pool.
	Raisecom(config-pool)# exit	Exit address pool configuration mode.
5	Raisecom(config)# interface vlan <i>vlan-id</i>	Enter VLAN interface configuration mode. The VLAN ID is pre-activated.
6	Raisecom(config-vlanif)# ip address <i>ip-address [ip-mask] [sub]</i>	Configure the IP address of the VLAN interface, which is the IP address of the configured gateway of the address pool.

Configuring NAT

Network Address Translation (NAT) is used to convert the private management IP address of the remote device to the public IP address. Through zero-configuration, the remote device obtains a private IP address from the CO device. NAT can be used to translate the private IP address into the public IP address of the management network and distinguish different remote devices in a form of public IP address+global interface ID. Network management information transmitted between remote devices and the network management system is forwarded through the public IP address. Therefore, you should configure the public IP address and related management VLAN of the CO device.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface fastethernet <i>interface-number</i>	Enter network management interface configuration mode. The network management interface of the device is used to connect the network management server, which is also called the public network interface.
3	Raisecom(config-port)# nat outbound <i>acl-number</i>	Configure NAT. The ACL is created in the previous step.

(Optional) releasing IP address

When replacing a remote device that has applied for a management IP address, to prevent the IP address resource from being occupied for a long time, you need to manually configure the lease information about the IP address on the central office server.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#oam address <i>ip-address</i> release	Release the specified IP address.

3.1.3 Configuring zero-configuration server based on DHCP

Configuring ACL

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# access-list <i>acl-number</i>	Create an ACL and enter ACL configuration mode.
3	Raisecom(config-acl-ipv4-advanced)# rule [<i>rule-id</i>] permit ip <i>source-ip-address</i> <i>source-ip-mask</i> any	Configure the ACL filtering rule. The packets with the source IP address matching the ACL filtering rule will be reported to the CPU.
	Raisecom(config-acl-ipv4-advanced)# exit	Exit ACL configuration mode.

Configuring traffic classification rules

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# class-map <i>class-map-name</i> match all	Create a traffic classifier and enter CMAP configuration mode.
3	Raisecom(config-cmap)# match access-list <i>acl-number</i> Raisecom(config-cmap)# exit	Define traffic classification which should match the ACL filtering rules.
4	Raisecom(config)# policy-map <i>policy-map-name</i>	Create a traffic policy and enter PMAP configuration mode.
5	Raisecom(config-pmap)# class-map <i>class-map-name</i>	Add a traffic classification policy to the traffic policy and enter traffic policy configuration mode which binds with traffic classification.
6	Raisecom(config-pmap-c)# forward-to-cpu Raisecom(config-pmap-c)# exit Raisecom(config-pmap)# exit	Forward the traffic to the CPU.

Configuring DHCP server interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter uplink physical layer interface configuration mode. The interface is a DHCP gateway interface. The types of interface supported can be a VLAN interface, sub-interface, and physical interface.
	Raisecom(config-port)#no portswitch	Switch the interface mode to Layer 3 router mode.
	Raisecom(config-port)#encapsulation dot1q <i>vlan-id</i>	(Optional) when the DHCP gateway uses a sub-interface, configure the single-layer VLAN encapsulated by the Ethernet sub-interface. Configure the interface IP address.
3	Raisecom(config-port)#ip address <i>ip-address</i>	Configure the interface IP address. The address is consistent with the address of the address pool gateway.
4	Raisecom(config-port)#service-policy ingress <i>policy-map-name</i>	Apply the traffic classification rule to the ingress direction of the interface. Only physical layer interfaces support traffic classification rules.
5	Raisecom(config-port)#ip dhcp server	Enable DHCP Server on the interface. By default, the device is not enabled with DHCP Server.
	Raisecom(config-port)#exit	Exit interface configuration mode.

Configuring DHCP server address pool

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip dhcp server pool <i>pool-name</i>	Configure the address pool of the DHCP property and enter address pool configuration mode.
3	Raisecom(config-pool)#address <i>start-ip-address end-ip-address mask</i> { <i>mask-address</i> <i>mask-length</i> }	Configure the IP address range and subnet mask of the address pool.
4	Raisecom(config-pool)#gateway <i>ip-address</i>	Configure the default gateway of the address pool. The gateway is identical to the private IP address of the management IP address assigned to the remote device by the local device.
5	Raisecom(config-pool)#lease expired { <i>minute</i> infinite }	(Optional) configure the lease of the address pool. By default, it is 30min.

Step	Command	Description
6	Raisecom(config-pool)# option 60 <i>vendor-string</i>	(Optional) configure information carried by Option60.
7	Raisecom(config-pool)# option 43 [sub-option option-id] { hex ascii } <i>string</i>	(Optional) configure information about Option43.
8	Raisecom(config-pool)# trap server-ip <i>ip-address</i>	(Optional) configure the IP address of the SNMP server (network management system) to which the Trap is sent.
9	Raisecom(config-pool)# tftp-server <i>ip-address</i>	(Optional) configure the TFTP server related to the address pool.
10	Raisecom(config-pool)# exit	Exit address pool configuration mode.



Note

- If the zero-configuration server assigns management IP addresses to remote devices based on Layer 3 physical interface, the network management information exchanged between CO and remote devices is untagged packets.
- If the zero-configuration server assigns management IP addresses to remote devices based on sub-interface or VLAN interface, the network management information exchanged between CO and remote devices is Tagged packets with the management VLAN ID.

Configuring NAT

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter network management interface configuration mode.
3	Raisecom(config-port)# nat outbound <i>acl-number</i>	Configure NAT.

(Optional) releasing IP address

When changing a remote device, which has applied for a management IP address, to prevent the IP address from being occupied for a long time, you should manually release the IP address on the CO server.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ip dhcp address ip- address release	Release the specified IP address. This command is used to release the lease table and NAT table of the CO device only without influencing the IP address of the remote device.

(Optional) configuring lease file management



Note

The RAX711-C-R supports saving and synchronizing the lease file automatically, as well as deleting the lease file.

When changing the CO zero-configuration server, you can upload assigned IP addresses in a form of lease to the TFTP/FTP server (such as a PC) for backup. After changing the CO device, you can download the backup lease file to the local device to confirm that these assigned IP addresses are not lost.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip dhcp lease save	Save the lease file.
3	Raisecom(config)#ip dhcp lease erase	(Optional) delete the lease file from the DHCP server.
4	Raisecom(config)#ip dhcp address release [pool pool-name]	Release lease of specified address pool.
5	Raisecom(config)#ip dhcp address ip-address release	Release lease of the specified IP address.
6	Raisecom(config)#exit	Exit global configuration mode.
7	Raisecom#upload dhcpLease { ftp ip-address username password filename tftp ip-address filename }	Upload the lease file to the PC through TFTP/FTP.
8	Raisecom#download dhcpLease { ftp ip-address username password filename tftp ip-address filename }	Download the lease file from the PC through TFTP/FTP.

Configuring DHCP Relay

If the zero-configuration server and the remote device are in the same network segment, the remote device can obtain the IP address from the DHCP Server. Otherwise, the remote device can obtain the IP address from the DHCP Server through the device, which is enabled with DHCP Relay. The zero-configuration server can assign IP addresses to remote devices in different network segments.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip dhcp relay	Configure global DHCP Relay.
3	Raisecom(config)#interface interface-type interface-number	Enter Layer 3 physical interface configuration mode. Note The Layer 3 physical interface needs to be configured with the IP address.

Step	Command	Description
4	Raisecom(config-port)#ip dhcp relay	Enable DHCP Relay. Enable DHCP Relay on the interfaces connecting DHCP Server and DHCP Client.
5	Raisecom(config-port)#ip dhcp relay target-ip ip-address	Configure the destination IP address. The IP address can be either the IP address of DHCP Server or that of DHCP Relay.

3.1.4 Checking configurations

No.	Command	Description
1	Raisecom(config)#show ip dhcp server	Show configurations of interfaces of the DHCP server.
2	Raisecom(config)#show ip dhcp server lease	Show assigned IP addresses and information about remote devices.
3	Raisecom(config)#show ip server pool [pool-name]	Show configurations of the DHCP or OAM address pool.
4	Raisecom(config)#show ip dhcp server statistics	Show statistics of the DHCP server.
5	Raisecom(config)#show ip dhcp static-bind	Show static binding information about the IP address in the address pool and the MAC address.
6	Raisecom(config)#show oam zero config	Show configurations of directly-connected zero-configurations.
7	Raisecom(config)#show remote config-info all	Show configurations of remote devices in directly-connected zero-configuration server mode.
8	Raisecom(config)#show ip dhcp relay	Show configurations of DHCP Relay.
9	Raisecom(config)#show debugging ospf dcn_info [self]	Show NE information collected about the CO OSPF DCN zero-configuration server.
10	Raisecom(config)#show nat session [file] [count]	Show NAT entries of the CO OSPF DCN zero-configuration server.
11	Raisecom(config)#show nat outbound	Check the ACL information bound when NAT is performed in the outbound direction of the interface.
12	Raisecom(config)#show nat netstack-rule [dnat snat]	Show the protocol stack rules for NAT.

4 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

4.1 Basic configurations of interface

4.1.1 Configuring basic information of interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i> Raisecom(config-port)#no portswitch	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#ip address <i>ip-address</i> [<i>ip-mask</i>] [sub]	Configure the primary and secondary IP addresses, as well as subnet mask of the Layer 3 physical interface.
4	Raisecom(config-port)#description <i>string</i>	Configure interface descriptions.
5	Raisecom(config-port)#portswitch	Switch interface configuration mode. Switch the interface to Layer 2 physical interface configuration mode, namely, the switching mode.
6	Raisecom(config-port)#shutdown	(Optional) shut down the interface.

4.1.2 Configuring interface working mode

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#mode { 12 13 }	Configure Layer 3 physical interface working mode. • L2: access L2VPN. • L3: access L3VPN.

4.1.3 Configuring Jumboframe on interface

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 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 <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#jumboframe <i>frame-size</i>	Configure the interface to allow Jumbo frames to pass. By default, it is 9600 Bytes.

4.1.4 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 RAX711-C-R 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 <i>interface-type interface-number</i>	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#mtu <i>size</i>	Configure the MTU of the interface. By default, it is 1500 bytes.

4.1.5 Configuring vibration suppression of interface

When working on the network, the interface of the device may be alternately up and down due to various reasons, such as physical signal interference and configuration error in link layer. Frequent alternation causes repetitive vibration of routing protocols and unfavorably impacts the device and the network and even cause the network and some devices unavailable.

You can configure the vibration suppression period to reduce the switching frequency of interface Up and Down.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#vibration-suppress peroid <i>second</i>	Configure the suppression period of the interface. By default, the suppression period is 0s.

4.1.6 Configuring MAC address of interface

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

4.2 Configuring Ethernet interface

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

Step	Command	Description
3	Raisecom(config-port)# tpid { 8100 9100 88a8 }	Configure the TPID of the interface. By default, it is 0x8100.
4	Raisecom(config-port)# speed { auto 10 100 1000 10000 25000 40000 }	Configure the interface rate.
5	Raisecom(config-port)# duplex { auto full half }	Configure the interface duplex mode.

4.3 Configuring Ethernet sub-interface

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i> Raisecom(config-port)# no portswitch	Enter interface configuration mode.
3	Raisecom(config-port)# interface gigaethernet <i>unit/slot/port.sub-interface</i>	In Layer 3 physical interface configuration mode, enter Ethernet sub-interface configuration mode.
4	Raisecom(config-subif)# encapsulation dot1q <i>vlan-id</i>	Configure the single VLAN used for encapsulating the Ethernet sub-interface.
5	Raisecom(config-subif)# encapsulation qinq svlan <i>svlan-id cvlan cvlan-id</i>	Configure the double VLAN Tag used for encapsulating the Ethernet sub-interface.
6	Raisecom(config-subif)# mode { 12 13 }	Configure the sub-interface mode for accessing L2VPN or L2VPN.
7	Raisecom(config-subif)# vlan translate [svlan { untag <i>vlan-id</i> }] [cvlan { untag <i>vlan-id</i> }]	In L2VPN mode, configure VLAN mapping on the Ethernet sub-interface.

4.4 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 <i>vlan-id</i>	Enter VLAN interface configuration mode.
3	Raisecom(config-vlanif)# ip address <i>ip-address</i> [<i>ip-mask</i>] [sub]	Configure the primary and secondary IP addresses, and the subnet mask of the VLAN interface.

4.5 Configuring optical module DDM

4.5.1 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 by analyzing monitoring data.

Prerequisite

N/A

4.5.2 Enabling optical module DDM

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#transceiver ddm enable	Enable optical module DDM. By default, it is disabled.

4.5.3 Checking configurations

No.	Command	Description
1	Raisecom#show transceiver [<i>interface-type</i> <i>interface-number</i> history { 15m 24h }]	Show history information about optical module DDM.
2	Raisecom#show transceiver ddm <i>interface-type</i> <i>interface-list</i> [detail]	Show information about optical module DDM.
3	Raisecom#show transceiver information <i>interface-type</i> <i>interface-number</i>	Show information about optical module DDM.
4	Raisecom#show transceiver threshold-violations <i>interface-type</i> <i>interface-number</i>	Show transceiver threshold violations.
5	Raisecom#show transceiver ddm brief	Show brief information about optical module DDM.
6	Raisecom#show transceiver ddm poll-interval	Show information about optical module DDM at the poll interval.

4.6 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.

4.7 Configuring out-of-band network management interface

4.7.1 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 MCC of the device and uses the RJ45 interface. Management through out-of-band DCN has the following characteristics:

- Does not occupy service bandwidths.
- Does not affect the network management channel when the service channel and physical line are interrupted.
- Depend on a separate DCN.

Prerequisite

The network management IP address of the device is planned.

4.7.2 Configuring IP address of out-of-band network management 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 configuration mode.
3	Raisecom(config-port)#ip address ip-address [ip-mask] [sub]	Configure the IP address of the out-of-band network management interface.

4.8 Checking configurations

No.	Command	Description
1	Raisecom# show interface [rang] [<i>interface-type</i> <i>interface-number</i>] [configuration] [statistics]	Show interface configurations, status, and statistics.

5 Ethernet

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

- Configuring VLAN
- Configuring MAC address table
- Configuring QinQ
- Configuring LLDP
- Configuring loop detection
- Configuring L2CP
- Configuring STP
- Configuring RSTP/MSTP
- Configuring MRSTP
- Configuring Super VLAN
- Configuring PVLAN
- Configuring GARP/GVRP
- Configuring port security MAC

5.1 Configuring VLAN

5.1.1 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 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

5.1.2 Configuring VLAN properties

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#create vlan <i>vlan-list</i> active	Create a VLAN. By default, there is no VLAN and the interface is not added to any VLAN.
3	Raisecom(config)#vlan <i>vlan-id</i>	Enter VLAN configuration mode.
4	Raisecom(config-vlan)#name <i>vlan-name</i> Raisecom(config-vlan)#exit	(Optional) configure the VLAN name.
5	Raisecom(config)#interface <i>interface-type interface-number</i>	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 }	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.

5.1.3 Configuring VLANs based on Access interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#portswitch	Switch the interface to work in Layer 2 mode.

Step	Command	Description
4	<code>Raisecom(config-port)#switchport mode access</code>	Configure the interface mode to Access.
5	<code>Raisecom(config-port)#switchport access vlan <i>vlan-id</i></code>	Configure the interface Access VLAN.
6	<code>Raisecom(config-port)#switchport access egress-allowed vlan { all <i>vlan-list</i> } [confirm]</code>	Configure the VLAN list available for the Access interface.
7	<code>Raisecom(config-port)#switchport reject-frame { untagged tagged }</code>	(Optional) configure the untagged packets or tagged packets denied by the interface.

5.1.4 Configuring VLANs based on Trunk interface

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

- If the configured Native VLAN is not the default VLAN and there is no default VLAN in the VLAN list on the Trunk interface, the interface will not allow packets in the default VLAN to pass.
- When configuring a Trunk Untag VLAN list, the system automatically adds all Untagged VLAN to the Trunk allowed VLAN.
- Trunk allowed VLAN list and Trunk Untagged VLAN list are valid for the static VLAN only.

5.1.5 Configuring VLAN based on MAC address

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mac-vlan <i>mac-address</i> vlan <i>vlan-id</i> [priority <i>value</i>]	Associate the MAC address with the VLAN.
3	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
4	Raisecom(config-gigaethernet1/1/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.

5.1.6 Configuring VLAN based on IP subnet

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip-subnet-vlan <i>ip-address</i> [<i>ip-mask</i>] vlan <i>vlan-id</i> [priority <i>value</i>]	Associate the VLAN with the IP subnet address.
3	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
4	Raisecom(config-gigaethernet1/1/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.

5.1.7 Configuring VLAN based on protocol

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#protocol-vlan <i>protocol-index</i> { ipv4 ipv6 ethertype <i>protocol-id</i> }	Configure the association rules between the protocol VLAN and Ethernet packets.
3	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
4	Raisecom(config- gigaethernet1/1/port)#switchport protocol-vlan <i>protocol-index</i> vlan <i>vlan-id</i>	Configure the association rules between the protocol VLAN and the interface.

5.1.8 Checking configurations

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

5.2 Configuring MAC address table

5.2.1 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

5.2.2 Configuring static MAC address table

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

5.2.3 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 <i>interface-type</i> <i>interface-number</i>	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 <i>threshold-value</i>	(Optional) configure dynamic MAC address limit. By default, no dynamic MAC address limit is configured.
5	Raisecom(config)# vlan <i>vlan-id</i>	Enter VLAN configuration mode.
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 <i>second</i>	(Optional) configure the aging time of the MAC address. By default, it is 300s.

Step	Command	Description
8	Raisecom(config-port)#mac-address move-restrain enable Raisecom(config-port)#exit	(Optional) configure suppression over MAC address flapping. By default, it is disabled.
9	Raisecom(config)#vlan <i>vlan-id</i>	(Optional) enter VLAN configuration mode.
10	Raisecom(config-vlan)#mac-address threshold threshold-value	(Optional) configure dynamic MAC address limit. By default, no dynamic MAC address limit is configured.
11	Raisecom(config-vlan)#exit	(Optional) exit VLAN configuration mode and enter global configuration mode.
12	Raisecom(config)#mpls vsi <i>vsi-name</i> static	(Optional) create a VSI and enter VSI configuration mode.
13	Raisecom(config-vsi)#mac-address threshold threshold-value	(Optional) configure dynamic MAC learning limits. By default, it is not configured.

5.2.4 Configuring blackhole MAC address

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

5.2.5 Filtering unknown L2 multicast packets

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)#mac-address multicast drop-unknown { reserved-address vlan <i>vlan-list</i> }	Configure the mode of MAC address table multicast filtering to discard packets. • If reserved-address is selected, it indicates whether the discarded packets contain reserved addresses. • If vlan <i>vlan-list</i> is selected, it means filtering based on VLAN.

5.2.6 Checking configurations

No.	Command	Description
1	Raisecom# show mac-address count [<i>vlan vlan-id</i>] [<i>interface-type interface-number</i>]	Show the number of MAD address entries.
	Raisecom# show mac-address count vsi <i>vsi-name</i> [<i>interface-type interface-number</i>]	
	Raisecom# show mac-address count vsi <i>vsi-name</i> [vc-id <i>vc-id</i> peer <i>ip-address</i>]	
2	Raisecom# show mac-address { all static dynamic } [<i>vlan vlan-id</i>] [<i>interface-type interface-number</i>]	Show MAC address entries.
	Raisecom# show mac-address { all static dynamic } <i>vsi</i> <i>vsi-name</i> [<i>interface-type interface-number</i>]	
	Raisecom# show mac-address { all static dynamic } <i>vsi</i> <i>vsi-name</i> [vc-id <i>vc-id</i> peer <i>ip-address</i>]	
	Raisecom# show mac-address <i>mac-address</i> [<i>vlan vlan-id</i> <i>vsi</i> <i>vsi-name</i>]	
	Raisecom# show mac-address blackhole [<i>vlan vlan-id</i> <i>vsi</i> <i>vsi-name</i>]	
3	Raisecom# show mac-address learning <i>vlan</i>	Show automatic learning status of the MAC address table.
	Raisecom# show mac-address learning [<i>interface-type interface-number</i>]	
4	Raisecom# show mac-address multicast [<i>vlan vlan-id</i>] [count]	Show the L2 multicast table.

5.2.7 Maintenance

No.	Command	Description
1	Raisecom(config)# clear mac-address dynamic	Clear MAC addresses.
	Raisecom(config)# clear mac-address dynamic [<i>vlan vlan-id</i>] [<i>interface-type interface-number</i>]	
	Raisecom(config)# clear mac-address dynamic vsi <i>vsi-name</i> [<i>interface-type interface-number</i>]	
	Raisecom(config)# clear mac-address dynamic vsi <i>vsi-name</i> [vc-id <i>vc-id</i> peer <i>ip-address</i>]	
	Raisecom(config)# clear mac-address dynamic <i>mac-address</i> [<i>vlan vlan-id</i> <i>vsi</i> <i>vsi-name</i>]	

5.3 Configuring QinQ

5.3.1 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 packets can be converted into single VLAN or double VLAN

Prerequisite

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

5.3.2 Configuring basic QinQ

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i></code> <code>Raisecom(config-port)#portswitch</code>	Enter Layer 2 interface configuration mode.
3	<code>Raisecom(config-port)#dot1q-tunnel</code>	Enable basic QinQ on the interface.
4	<code>Raisecom(config-port)#dot1q-tunnel cos override</code>	Enable CoS priority overriding on the interface.
5	<code>Raisecom(config-port)#switchport reject-frame { tagged untagged }</code>	Configure the type of packets denied by the interface.



Note

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

5.3.3 Configuring selective QinQ

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i> Raisecom(config-port)#portswitch	Enter Layer 2 interface configuration mode.
3	Raisecom(config-port)#switchport vlan-mapping-miss discard	Configure the interface to discard tagged messages that cannot match selective QinQ or VLAN translation rules.
4	Raisecom(config-port)#switchport vlan-mapping both priority-tagged [cos <i>cos-value</i>] add-outer <i>outer-vlan-id</i> [cos <i>cos-value</i>] [remove translate <i>vlan-id</i>]	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.
5	Raisecom(config-port)#switchport vlan-mapping both cvlan <i>custom-vlan-id</i> [cos <i>cos-value</i>] add-outer <i>outer-vlan-id</i> [cos <i>cos-value</i>] { remove translate <i>vlan-id</i> }	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.
6	Raisecom(config-port)#switchport vlan-mapping both inner <i>inner-vlan-list</i> add-outer <i>outer-vlan-id</i> [cos <i>cos-value</i>]	Add SVLAN based on CVLAN list configuration, you can add the specified SVLAN CoS value.
7	Raisecom(config-port)#switchport qinq default-cvlan <i>vlan-id</i>	Configure the default CVLAN for the interface.
	Raisecom(config-port)#switchport vlan-mapping both untag add-outer <i>outer-vlan-id</i> [cos <i>cos-value</i>]	Add SVLAN based on default CVLAN. You can add the specified SVLAN CoS value.
8	Raisecom(config-port)#switchport vlan-mapping both outer <i>outer-vlan-id</i> inner <i>inner-vlan-id</i> translate <i>outer-vlan-id</i> inner <i>inner-vlan-id</i> [cos <i>cos-value</i>]	Configure VLAN mapping rules based on SVLAN and CVLAN, and add the specified SVLAN CoS value.
9	Raisecom(config-port)#switchport vlan-mapping both outer <i>outer-vlan-id</i> translate <i>outer-vlan-id</i> [cos <i>cos-value</i>]	Configure VLAN mapping rules based on SVLAN, and add the specified SVLAN CoS value.
10	Raisecom(config-port)#switchport vlan-mapping both <i>vlan-list</i> translate <i>vlan-id</i>	Configure N:1 VLAN mapping rules.

5.3.4 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.

5.4 Configuring LLDP

5.4.1 Preparing for configurations

Scenario

When you obtain connection information between devices through the network management system for topology discovery, you need to enable LLDP on the RAX711-C-R. Therefore, the RAX711-C-R can notify its information to the neighbors mutually, and store neighbor information to facilitate the network management system querying information.

Prerequisite

N/A

5.4.2 Enabling global LLDP



Caution

After global LLDP is disabled, you cannot re-enable it immediately. Global LLDP cannot be enabled unless the restart timer times out.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#lldp enable	Enable global LLDP. By default, it is disabled.

5.4.3 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.

Step	Command	Description
3	Raisecom(config-port)#lldp enable	Enable interface LLDP. By default, interface LLDP is enabled.

5.4.4 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 <i>second</i>	(Optional) configure the delivery period timer of the LLDP packet. By default, it is 30s.
3	Raisecom(config)#lldp message-transmission delay <i>second</i>	(Optional) configure the delivery delay timer of the LLDP packet. By default, it is 2s.
4	Raisecom(config)#lldp message-transmission hold-multiplier <i>coefficient</i>	(Optional) configure the aging coefficient of the LLDP packet. By default, it is 4.
5	Raisecom(config)#lldp restart-delay <i>second</i>	(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.

5.4.5 Configuring LLDP to send TLV packets

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

Step	Command	Description
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.

5.4.6 Configuring LLDP Trap

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

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



Note

After enabled with LLDP Trap, the RAX711-C-R will send Traps after detecting aged neighbors, newly-added neighbors, and changed neighbor information.

5.4.7 Checking configurations

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

5.5 Configuring loop detection

5.5.1 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.

5.5.2 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 these 2 devices are blocked.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)# portswitch	Configure the interface to a switching interface or a Layer 3 interface working in L2 mode.
	Raisecom(config-port)# mode 12	
4	Raisecom(config-port)# loopback-detection [pkt-vlan { untag <i>vlan-id</i> }] [log-interval <i>minutes</i>] [hello-time <i>second</i>] [restore-time <i>second</i>] [action { block trap-only shutdown }]	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.

5.5.3 Checking configurations

No.	Command	Description
1	Raisecom# show loopback-detection [<i>interface-type</i> <i>interface-list</i>] [detail]	Show configurations of loop detection on interfaces.

5.5.4 Maintenance

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

5.6 Configuring L2CP

5.6.1 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

5.6.2 Configuring L2CP to transparently transmit MAC address

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

5.6.3 Configuring L2CP profile

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#l2cp-process profile profile-number</code>	Create a L2CP profile and enter L2CP profile mode.
3	<code>Raisecom(config-l2cp-profile)#name string</code>	(Optional) add profile descriptions.

Step	Command	Description
4	<code>Raisecom(config-l2cp-profile)#protocol { oam stp dot1x l2cp lldp cdp vtp pvst all } action { tunnel drop peer }</code>	(Optional) configure the processing action for L2CP packets.
5	<code>Raisecom(config-l2cp-profile)#tunnel vlan <i>vlan-id</i></code>	(Optional) configure the specified VLAN of transparent transmission.
6	<code>Raisecom(config-l2cp-profile)# port <i>interface-type interface-number</i></code>	(Optional) configure the specified egress interface of transparent transmission.
7	<code>Raisecom(config-l2cp-profile)#tunnel type mac</code>	(Optional) configure the tunnel type of transparent transmission.
8	<code>Raisecom(config-l2cp-profile)#usr-define <i>define-id</i> action { tunnel peer drop }</code>	Configure the action type of user-defined protocols.

5.6.4 Applying L2CP profile to interface

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

5.6.5 Checking configurations

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

5.6.6 Maintenance

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

5.7 Configuring STP

5.7.1 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 MAC address learning fault, and broadcast storm and network down caused by quick copy and transmission of data frame due to loops. STP calculation can block one interface in a broken loop and ensure that there is only one path from the data flow to the destination host, which is also the best path.

Prerequisite

Before configuring STP, you need to configure the physical parameters of the interface so that the physical layer status of the interface is Up.

5.7.2 Enabling STP

No.	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#spanning-tree mode stp</code>	Configure the spanning tree mode to STP.
3	<code>Raisecom(config)#spanning-tree enable</code>	Enable STP.

5.7.3 Configuring STP parameters

Configure STP parameters for the RAX711-C-R as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#spanning-tree priority priority-value</code>	(Optional) configure the device priority.
3	<code>Raisecom(config)#spanning-tree root { primary secondary }</code>	(Optional) configure the RAX711-C-R as the root or backup device.

Step	Command	Description
4	Raisecom(config)# interface <i>interface-type</i> <i>interface-number</i> Raisecom(config-port)# spanning-tree priority <i>priority-value</i> Raisecom(config-port)# exit	(Optional) configure the device interface priority.
5	Raisecom(config)# spanning-tree hello-time <i>value</i>	(Optional) configure the Hello Time.
6	Raisecom(config)# spanning-tree transit-limit <i>value</i>	(Optional) configure the maximum number of BPDU packets allowed to be sent within the Hello Time.
7	Raisecom(config)# spanning-tree forward-delay <i>value</i>	(Optional) configure the forward delay.
8	Raisecom(config)# spanning-tree max-age <i>value</i>	(Optional) configure the maximum age.

5.7.4 Checking configurations

No.	Command	Description
1	Raisecom# show spanning-tree	Show basic configurations of STP.
2	Raisecom# show spanning-tree <i>interface-type</i> <i>interface-number</i>	Show STP configurations on the interface.

5.7.5 Maintenance

Command	Description
Raisecom(config-port)# spanning-tree clear statistics	Clear statistics about interface spanning tree.

5.8 Configuring RSTP/MSTP

5.8.1 Preparing for configurations

Scenario

In big LAN or residential region aggregation, the aggregation devices form a ring for link backup, to avoid loops and meanwhile realize service load balancing. MSTP can select a different and unique forwarding path for each one or a group of VLANs.

Prerequisite

Configure interface physical parameters to make it Up.

5.8.2 Enabling MSTP

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree mode mstp	Configure the spanning tree mode to MSTP.
3	Raisecom(config)#spanning-tree enable	Enable STP.

5.8.3 Configuring MST domain and its maximum number of hops

You can configure domain information about the RAX711-C-R when it is running in MSTP mode. The device MST domain is decided by domain name, VLAN mapping table and configuration of MSTP revision level. You can configure the current device in a specific MST domain through the following configurations.

MST domain scale is restricted by the maximum number of hops. Starting from the root bridge of spanning tree in the domain, the configuration message (BPDU) reduces 1 hop count every time it passes a device. The RAX711-C-R discards the configuration message whose number of hops is 0. The device exceeding the maximum number of hops cannot join spanning tree calculation, thus restricting the MST domain scale.

Configure MSTP domain and its maximum number of hops for the RAX711-C-R as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree region-configuration	Enter MST domain configuration mode.
3	Raisecom(config-region)#name name	Configure MST domain name.
4	Raisecom(config-region)#revision-level level-value	Configure the revision level for MST domain. By default, it is 0.
5	Raisecom(config-region)#instance instance-id vlan vlan-list Raisecom(config-region)#exit	Configure mapping from the MST domain VLAN to the instance.
6	Raisecom(config)#spanning-tree max-hops hops-value	Configure the maximum number of hops for the MST domain.



Note

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

5.8.4 Configuring root/backup bridge

Two methods for MSTP root selection are as below:

- Configure the device priority to confirm STP root bridge or backup bridge through STP calculation.
- Assign the MSTP root directly with this command.

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



Caution

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

Configure root bridge or backup bridge for the RAX711-C-R as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree [instance <i>instance-id</i>] root { primary secondary }	Configure the RAX711-C-R as the root bridge or backup bridge for a STP instance.



Note

- You can confirm the effective instance of the root bridge or backup bridge through the **instance *instance-id*** command. The current device will be assigned as the root bridge or backup bridge of CIST if instance-id is 0 or parameter **instance *instance-id*** is omitted.
- The root types of the device in different instances are independent, that is, they not only can be the root bridge or the backup bridge of one instance, but also the root bridge or backup bridge of other spanning tree instances. However, in the same spanning tree instance, the same device cannot be used as the root bridge and backup bridge at the same time.
- 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 assigning one root bridge and several backup bridges for one spanning tree.

5.8.5 Configuring device interface and system priority

Whether the interface is selected as the root interface depends on the 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 decides whether the RAX711-C-R can be selected as the root of the spanning tree. Configuring smaller priority helps obtain a smaller Bridge ID to achieve the goal of designating certain device as the root. If the priority of two RAX711-C-R devices are identical, the RAX711-C-R with smaller MAC address will be selected as the root.

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

Configure interface priority and system priority for the RAX711-C-R as below.

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



Note

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

5.8.6 Configuring network diameter for switching network

The network diameter indicates the number of nodes on the path that has the most devices on a switching network. In MSTP, the network diameter is valid only to the CIST, and invalid to the MSTI instance. Regardless of the number of nodes in a path in one domain, it is considered as just one node. Actually, the network diameter should be defined as the number of domains in the path crossing the most domains. The network diameter is 1 if there is only one domain in the whole network.

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

Similar to the maximum number of hops of MST domain, only when the RAX711-C-R is configured as the CIST root device can this configuration take effect. MSTP will automatically configure the Hello Time, Forward Delay and Max Age parameters to a privileged value through calculation when you configure the network diameter.

Configure the network diameter for the switching network as below.

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

5.8.7 Configuring internal path cost of interfaces

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

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

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

Configure the internal path cost for the RAX711-C-R as below.

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

5.8.8 Configuring external path cost of interfaces

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

Configure the external path cost for the RAX711-C-R as below.

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

5.8.9 Configuring maximum transmission rate on interface

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

Configure maximum transmission rate on the interface for the RAX711-C-R as below.

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

5.8.10 Configuring MSTP timer

- **Hello Time:** the interval for the RAX711-C-R to send BPDUs. It is used to detect whether a link fails on the RAX711-C-R. The RAX711-C-R sends hello packets to other devices around in Hello Time to check if there is fault in the link. The default value is 2s. You can adjust the interval value according to network condition. You can reduce the interval when network link changes frequently to enhance the stability of STP. However, increasing the interval reduces CPU utilization rate for STP.
- **Forward Delay:** the time parameter to ensure the safe transit of device status. Link fault causes the network to recalculate spanning tree, but the new configuration message recalculated cannot be transmitted to the whole network immediately. There may be temporary loop if the new root interface and designated interface start transmitting data at once. This protocol adopts a status migration system: before the root interface and designated interface start forwarding data, it needs a medium status (learning status); after a Forward Delay, it enters forwarding status. The delay guarantees the new configuration message to be transmitted through the whole network. You can adjust the delay according to actual condition. That is, you can reduce it when the network topology changes infrequently and increase it under opposite conditions.
- **Max Age:** the bridge configurations used by STP have a life time that is used to judge whether the configurations are outdated. The RAX711-C-R will discard outdated configurations and STP will recalculate spanning tree. The default value is 20s. If the value is too small, it may cause frequent recalculation of the spanning tree. If the value is too larger, it will make STP unable to adapt to the network topology change timely.

All devices in the entire switching network use the three time parameters on the CIST root device, so only the configuration on the root device takes effect.

Configure the MSTP timer for the RAX711-C-R as below.

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

5.8.11 Configuring edge interface

The edge interface indicates that the interface neither directly connects to any devices nor indirectly connects to any device via the network where the interface is located.

If you configure the interface to an edge interface, its status can change into the forwarding status quickly without any waiting time. You can configure the Ethernet interface connected to the user client as an edge interface to fast change into the forwarding status.

When an interface is configured to edge interface auto detection (auto), the attributes of the edge interface are determined by the actual situation. When an interface is configured to an edge interface (force-true), the actual operating value of the interface becomes a non-edge interface after receiving the BPDU. When an interface is configured to a non-edge interface (force-false), similarly, regardless of whether it is an edge or non-edge interface, the interface will remain a non-edge interface until the configuration changes.

By default, all interfaces on the RAX711-C-R are configured in auto-detection attribute.

Configure the edge interface for the RAX711-C-R as below.

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

5.8.12 Configuring link type

Two interfaces connected by a point-to-point link can quickly transit to the forwarding 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 to 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 RAX711-C-R as below.

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

5.8.13 Configuring root interface protection

The bridge will re-elect a root interface when it receives a packet with higher priority, which influences network connectivity and also consumes CPU resources. For the MSTP network, if someone sends BPDUs with higher priority, the network may become unstable for the 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. Therefore, the downlink interface cannot receive the packets with priority higher than that of the bridge unless someone maliciously 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 damaging the upper layer link by other attacks from attacking sources.

Configure root interface protection for the RAX711-C-R as below.

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

5.8.14 Configuring interface loopguard

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

The spanning tree module exchanges packets periodically and it is considered that the link fails if it has not received a packet in a period. It will then select a new link and enable the backup interface. In actual networking, the cause to failure in receiving packets may not be the link fault. In this case, enabling the backup interface may generate loops.

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



Loopguard conflicts with link backup. That is, loopguard is implemented at the cost of disabling link backup.

Configure interface loop protection for the RAX711-C-R as below.

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

Step	Command	Description
3	Raisecom(config-port)#spanning-tree loopguard { enable disable }	Configure interface loopguard attributes.

5.8.15 Executing mcheck operation

Interface on the MSTP device has two working modes: STP compatible mode and MSTP mode. Suppose the interface of the MSTP device in a switch network is connected to the RAX711-C-R running STP, the interface will change to work in STP compatible mode automatically. The interface cannot change to work in MSTP mode if the RAX711-C-R running STP is removed, but the interface still works in STP compatible mode. You can execute the mcheck operation to force the interface to work in MSTP mode. If the interface receives new STP packets again, it will return to STP compatible mode.

Execute mcheck operation for the RAX711-C-R as below.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#spanning-tree mcheck	Execute the mcheck operation to force the interface back to the MSTP mode.

5.8.16 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] port-list port-list [detail]	Show configurations of spanning tree on the interface.
3	Raisecom#show spanning-tree region-operation	Show configurations of the MST domain.

5.9 Configuring MRSTP

5.9.1 Preparing for configurations

Scenario

When device A connects upstream to device B, if device B has a higher priority, it will be elected as the root bridge. However, if device A is connected downstream to multiple ring

networks and only STP/RSTP can run in the ring network. At this time, device A is expected to be designated as the root bridge of multiple ring network devices, all traffic is forwarded through device A, while device A can still select device B as the root bridge.

Prerequisite

N/A

5.9.2 Enabling MRSTP

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree enable	Enable global STP.
3	Raisecom(config)#spanning-treemode mrstp	Configure the spanning tree operation mode to MRSTP.
4	Raisecom(config)#spanning-tree mrstp pro-id	Create a MRSTP process.
5	Raisecom(config)#interface interface-type interface-number	Enter physical layer interface configuration mode or aggregation group interface configuration mode.
6	Raisecom(config-port)#spanning-tree mrstp pro-id	Bind the interface to the specified process.

5.9.3 Configuring MRSTP parameter

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#spanning-tree mrstp pro-id priority priority	(Optional) configure priority of the specified process.
3	Raisecom(config)#interface interface-type interface-number Raisecom(config-port)#spanning-tree priority priority-value	(Optional) configure the device interface priority.
4	Raisecom(config)#spanning-tree hello-time value	(Optional) configure the value of HelloTime.
5	Raisecom(config)#spanning-tree transit-limit value	(Optional) configure the maximum number of BPDU packets allowed to be sent within the Hello Time.
6	Raisecom(config)#spanning-tree forward-delay value	(Optional) configure the value of Forward Delay.
7	Raisecom(config)#spanning-tree max-age value	(Optional) configure the MaxAge.

5.9.4 Checking configurations

No.	Command	Description
1	<code>Raisecom#show spanning-tree mrstp pro-id</code>	Show basic information about MRSTP.

5.10 Configuring Super VLAN

5.10.1 Preparing for configurations

Scenario

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

Prerequisite

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

5.10.2 Configuring Super VLAN

Configure the super VLAN for the RAX711-C-R as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#create vlan vlan-id active</code> <code>Raisecom(config)#vlan vlan-id</code>	Create a VLAN, and enter VLAN configuration mode.
3	<code>Raisecom(config-vlan)#supervlan</code>	Configure the VLAN as a super VLAN.
4	<code>Raisecom(config-vlan)#subvlan [add remove] subvlan-list</code>	Configure sub-VLANs of the super VLAN.
5	<code>Raisecom(config-vlan)#exit</code>	Exit VLAN configuration mode.
6	<code>Raisecom(config)#interface vlan vlan-id</code>	Enter VLAN interface configuration mode.
7	<code>Raisecom(config-vlan)#arp local-proxy enable</code>	Enable local ARP proxy of the super VLAN.



Note

- After the interface of the super VLAN is configured, configure its IP address. The VLAN belonging to the super VLAN is a sub-VLAN.

- After being configured as a super VLAN, a VLAN cannot be configured with the VLAN interface and IP address.

5.10.3 Checking configurations

Use the following commands to check configuration results.

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

5.11 Configuring PVLAN

5.11.1 Preparing for configurations

Scenario

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

Prerequisite

- Create a static VLAN
- Activate it.

5.11.2 Configuring PVLAN type

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



Caution

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

5.11.3 Configuring PVLAN association

Configure PVLAN association for the RAX711-C-R as below.

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

Caution

- Before configuring VLAN association, create a VLAN and activate it, configure the PVLAN type, configure the primary VLAN and secondary VLANs, and choose the correct association type. Otherwise, VLAN association cannot be configured.
- The primary VLAN and secondary VLANs cannot be configured to the default VLAN. If VLAN2 is a cluster VLAN, it cannot be configured to PVLAN.
- A secondary VLAN can be added to only one PVLAN.
- A primary VLAN can be associated with only one isolated VLAN, or up to 64 secondary VLANs.

5.11.4 Configuring PVLAN mode on interface

The VLAN of the RAX711-C-R supports Access interface mode and Trunk interface mode, and the PVLAN supports promiscuous interface mode and host interface mode.

Caution

- The promiscuous interface mode and host interface mode support configuring association or mapping under the condition that PVLAN association or mapping already exists, otherwise the configuration will fail.
- When an interface is configured to the host interface mode or promiscuous interface mode without being associated with or mapped into a primary VLAN or secondary VLAN, the interface only allows untagged packets to enter.
- IGMP runs on the primary VLAN only. The VLANs that the data flow passes in the uplink and downlink of the PVLAN are different, so you cannot configure IGMP Snooping to implement multicast. Instead, you need to configure IGMP MVR.

Configure the PVLAN mode on the interface for the RAX711-C-R as below.

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

Step	Command	Description
3	<code>Raisecom(config-tengigabitethernet1/1/*)#switchport mode private-vlan { host promiscuous }</code>	Configure the PVLAN mode on the interface.
4	<code>Raisecom(config-tengigabitethernet1/1/*)#exit</code>	Return to global configuration mode.
5	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
6	<code>Raisecom(config-tengigabitethernet1/1/*)#switchport private-vlan host-association primary-vlan-id secondary-vlan-id</code>	Associate the primary VLAN and secondary VLANs on the host interface. You can use the no switchport private-vlan host-association command to delete the association between the primary VLAN and secondary VLANs on the host interface.
7	<code>Raisecom(config-tengigabitethernet1/1/*)#switchport private-vlan mapping primary-vlan-id [add remove] secondary-vlan-list</code>	Associate the primary VLAN and secondary VLANs on the promiscuous interface. You can use the no switchport private-vlan mapping command to delete the association between the primary VLAN and secondary VLANs on the promiscuous interface.

5.11.5 Checking configuration

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

5.12 Configuring GARP/GVRP

5.12.1 Configuring GARP

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

Step	Command	Description
2	Raisecom(config)# interface <i>interface-type</i> <i>interface-num</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-port)# garp timer { join leave leaveall } <i>time-value</i>	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).

5.12.2 Configuring GVRP

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# gvrp enable	Enable global GVRP.
3	Raisecom(config)# interface <i>interface-type</i> <i>interface-number</i>	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.



Caution

- You must configure the interface to Trunk mode before enabling interface GVRP.
- We do not recommend enabling GVRP on the member interfaces of the aggregation group.

5.12.3 Checking configurations

No.	Command	Description
1	Raisecom# show garp [<i>interface-type</i> <i>interface-number</i>]	Show configurations of the GARP timer.
2	Raisecom# show garp [<i>interface-type</i> <i>interface-number</i>] statistics	Show GARP statistics.
3	Raisecom# show gvrp [<i>interface-type</i> <i>interface-number</i>]	Show GVRP configurations.

No.	Command	Description
4	Raisecom# show gvrp [<i>interface-type interface-number</i>] statistics	Show GVRP statistics.
5	Raisecom# show gvrp local-vlan <i>interface-type interface-number</i>	Show the local VLAN of GVRP.

5.12.4 Maintenance

Command	Description
Raisecom(config)# clear gvrp [<i>interface-type interface-number</i>] statistics	Clear GVRP statistics.

5.13 Configuring port security MAC

5.13.1 Configuring basic functions of port security MAC



Caution

- We do not recommend enabling port security MAC on member interfaces of the LAG.
- We do not recommend using the MAC address management function to configure static MAC addresses when port security MAC is enabled on the same interface.
- When the 802.1x interface adopts a MAC address-based authentication mode, port security MAC conflicts with 802.1x. We do not recommend configuring them concurrently.
- Port security MAC conflicts with interface/interface+VLAN-based MAC address limit. We do not recommend configuring them concurrently.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-port)# switchport port-security	Enable port security MAC.
4	Raisecom(config-port)# switchport port-security maximum <i>maximum</i>	(Optional) configure the maximum number of secure MAC addresses.
5	Raisecom(config-port)# switchport port-security violation { protect restrict shutdown }	(Optional) configure the port security MAC violation mode.
6	Raisecom(config-port)# no port-security shutdown Raisecom(config-port)# exit	(Optional) re-enable the interface which is shut down due to violating port security MAC.

Step	Command	Description
7	Raisecom(config)#port-security recovery-time <i>second</i>	(Optional) configure the restoration time of port security MAC.



Note

- When the secure MAC violation policy is Shutdown, you can use this command to re-enable this interface which is shut down due to violating port security MAC.
- When the interface is Up, the configured secure MAC violation mode will remain valid.

5.13.2 Configuring static secure MAC address

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaetherne1/1/port)#switchport port-security	Enable port security MAC.
4	Raisecom(config-gigaetherne1/1/port)#switchport port-security mac-address <i>mac-address vlan vlan-id</i>	Configure the static secure MAC address.

5.13.3 Configuring dynamic secure MAC address

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#port-security aging-time <i>period</i>	(Optional) configure the aging time of dynamic secure MAC addresses.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
4	Raisecom(config-gigaetherne1/1/port)#switchport port-security aging-type { <i>absolute</i> <i>inactivity</i> }	(Optional) configure the aging type of secure MAC addresses.
5	Raisecom(config-gigaetherne1/1/port)#switchport port-security	(Optional) enable port dynamic security MAC learning.
6	Raisecom(config-gigaetherne1/1/port)#switchport port-security trap enable	(Optional) enable port security MAC Trap.
7	Raisecom(config-gigaetherne1/1/port)#switchport port-security trap period <i>value</i>	(Optional) configure the period for sending Traps for port security MAC.



Note

The **switchport port-security** command can enable port security MAC and dynamic secure MAC learning at the same time.

5.13.4 Configuring sticky secure MAC address on interface



Caution

We do not recommend configuring sticky secure MAC addresses when port sticky security MAC is disabled. Otherwise, port Sticky security MAC may be abnormal.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaetherne t1/1/port)#switchport port-security	Enable port security MAC.
4	Raisecom(config-gigaetherne t1/1/port)#switchport port-security mac-address sticky	Enable sticky secure MAC learning.
5	Raisecom(config-gigaetherne t1/1/port)#switchport port-security mac-address sticky <i>mac-address vlan vlan-id</i>	(Optional) manually configure sticky secure MAC addresses.



Note

After sticky secure MAC address learning is enabled, dynamic secure MAC addresses will be converted into sticky secure MAC addresses; manually configured sticky secure MAC addresses will take effect.

5.13.5 Checking configurations

No.	Command	Description
1	Raisecom# show port-security [<i>interface-type interface-list</i>]	Show configurations of port security MAC.
2	Raisecom# show port-security mac-address [<i>interface-type interface-list</i>]	Show configurations of secure MAC address and secure MAC address learning.

5.13.6 Maintenance

Command	Description
<code>Raisecom(config-gigaethernet1/1/port)#clear port-security { all configured dynamic sticky }</code>	Clear the secure MAC address of a specified type on a specified interface.

6 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
- Configuring PTP-based clock synchronization

6.1 Configuring SyncE-based clock synchronization

6.1.1 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

6.1.2 Configure the clock source of SyncE

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

No.	Command	Description
3	Raisecom(config)#sync operation-type { auto-select forced-freerun forced-holdover }	Configure the working status of SyncE. By default, forced-freerun is adopted.
4	Raisecom(config)#sync 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)#sync 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)#sync 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)#sync hold-off-time time	Configure the hold-off time of the clock source.

6.1.3 Manually selecting SyncE clock source

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

6.1.4 Checking configurations

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

6.2 Configuring PTP-based clock synchronization

6.2.1 Preparing for configurations

Scenario

SyncE only supports frequency synchronization instead of clock synchronization. However, mobile communication networks and power markets have strict requirements on the accuracy of clock synchronization. Therefore, PTP is adopted for time synchronization over the full-mesh network.

The RAX711-C-R only supports 1588 TC.

Prerequisite

N/A

6.2.2 Configuring PTP clock modes

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ptp enable	Enable global PTP. By default, global PTP is disabled.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter the switch interface configuration mode.
4	Raisecom(config-port)#portswitch	Configure the interface to switch mode.
5	Raisecom(config-port)#switchport access vlan <i>vlan-id</i>	Configure the interface VLAN.
6	Raisecom(config-port)#ptp enable	Enable PTP on the interface. By default, PTP on all interfaces is disabled.

6.2.3 Checking configurations

No.	Command	Description
1	Raisecom#show ptp	Show PTP information.

7 IP services

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

- Configuring IPv4
- Configuring IPv6
- Configuring ARP
- Configuring NDP
- Configuring ICMP
- Configuring VRF
- Configuring fault detection
- Configuring DHCPv4 Server
- Configuring DHCPv6 server
- Configuring DHCPv4 Client
- Configuring DHCPv6 client
- Configuring DHCPv4 Relay
- Configuring DHCPv6 relay
- Configuring DHCPv4 Snooping
- Configuring DHCPv6 Snooping
- Configuring DHCPv4/DHCPv6 Option

7.1 Configuring IPv4

7.1.1 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

7.1.2 Configuring IPv4 address on interface

No.	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i> Raisecom(config-port)#no portswitch	Enter Layer 3 physical interface configuration mode. In interface configuration mode, use the no portswitch command to switch the interface from Layer 2 switch mode to Layer 3 router mode.
3	Raisecom(config-port)#ip address <i>ip-address</i> [<i>ip-mask</i>] [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 <i>interface-type interface-number</i>	(Optional) configure the interface to borrow the IP address of other interfaces.
5	Raisecom(config-port)#mtu <i>max-frame-length</i>	Configure the maximum transmission unit of the interface.

7.1.3 Configuring IPv4 PMTU

No.	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ipv4 pathmtu <i>ip-address</i> <i>value</i>	Configure static PMTU entries.
3	Raisecom(config)#ipv4 pathmtu enable	Enable the IPv4 PMTU.
4	Raisecom(config)#ipv4 pathmtu age <i>age-time</i>	Configure the aging time of dynamic PMTU entries.

7.1.4 Checking configurations

No.	Command	Description
1	Raisecom#show ip interface brief	Show IP address configurations of the L3 interface.
2	Raisecom#show ipv4 pathmtu { <i>ip-address</i> all dynamic static }	Show IPv4 PMTU configurations.

7.2 Configuring IPv6

7.2.1 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

7.2.2 Configuring IPv6 address on interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter Layer 3 physical interface configuration mode. In interface configuration mode, use the no portswitch command to switch the interface from Layer 2 switch mode to Layer 3 router mode.
3	Raisecom(config-port)#ipv6 address <i>ipv6-address/prefix-length</i> [<i>eui-64</i>]	Configure the IPv6 address of the interface.
4	Raisecom(config-port)#ipv6 address <i>ipv6-address</i> link-local	Configure the IPv6 local link address of the interface.
5	Raisecom(config-port)#ipv6 address auto	Enable automatic configuration of IPv6 stateless address in interface mode.

7.2.3 Configuring IPv6 PMTU

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ipv6 pathmtu <i>ipv6-address value</i>	Configure static PMTU entries.
3	Raisecom(config)#ipv6 pathmtu enable	Enable IPv6 PMTU.
4	Raisecom(config)#ipv6 pathmtu age <i>age-time</i>	Configure the aging time of dynamic PMTU entries.

7.2.4 Checking configurations

Step	Command	Description
1	Raisecom# show ipv6 interface brief [<i>interface-type interface-number</i>]	Show IPv6 address configurations of the L3 interface.
2	Raisecom# show ipv6 address auto	Show information about the IPv6 address prefix.
3	Raisecom# show ipv6 pathmtu { all dynamic static <i>ipv6-address</i> }	Show information about the PMTU configured.

7.3 Configuring ARP

7.3.1 Preparing for configurations

Scenario

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

Prerequisite

Configure the interface IPv4 address.

7.3.2 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.

7.3.3 Configuring dynamic ARP

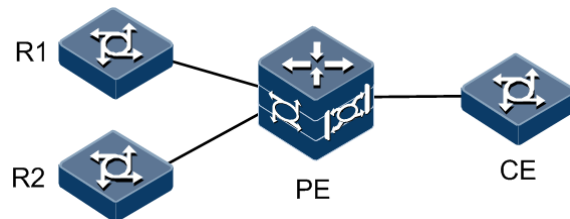
Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# arp mode { learn-all learn-reply-only }	Configure the ARP mode. By default, it learns the MAC address of all hosts.
3	Raisecom(config)# arp aging-time time	(Optional) configure the aging time of dynamic ARP. By default, the aging time is 1200 seconds.

Step	Command	Description
4	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter the 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 <i>number</i>	Configure the maximum number of ARP entries dynamically learned by the interface. By default, the number of ARP entries dynamically learned by the interface is 50000.
7	Raisecom(config-port)# gratuitous-arp-learning { enable disable }	Configure gratuitous ARP learning on the interface. By default, it is enabled.

7.3.4 Configuring proxy ARP

As shown in Figure 7-1, 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 7-1 Proxy ARP application scenario



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

7.3.5 Clearing ARP entries

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

7.3.6 Checking configurations

No.	Command	Description
1	<code>Raisecom#show arp [vrf vrf-name] [ip-address interface interface-type interface-number static]</code>	Show ARP information.

7.4 Configuring NDP

7.4.1 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.

7.4.2 Configuring static NDP entries

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

7.4.3 Configuring dynamic NDP entries

Configuring times of sending NS messages for detecting duplicated addresses

Configure times of sending NS messages for detecting duplicated addresses for the RAX711-C-R as below.

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

Step	Command	Description
2	<code>Raisecom(config)#ipv6 nd dad attempts <i>value</i></code>	Configure times of sending NS messages for detecting duplicated addresses.



Note

When the RAX711-C-R 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 RAX711-C-R as below.

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

Configuring aging time of dynamic NDP entries

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

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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical interface configuration mode.
3	<code>Raisecom(config-port)#ipv6 nd ra repression</code>	Enable RA repression. By default, RA suppression is enabled.

Step	Command	Description
4	Raisecom(config-port)# ipv6 nd ra interval <i>interval</i>	Configure the interval for advertising RA messages.
5	Raisecom(config-port)# ipv6 nd ra advlinkmtu <i>mtu-value</i>	Configure the MTU information carried in the RA message.
6	Raisecom(config-port)# ipv6 nd ra prefix <i>ipv6-prefix-address/prefix-length valid-lifetime preferred-lifetime</i> [no-autoconfig] [off-link]	Configure the prefix information carried in the RA message.
7	Raisecom(config-port)# ipv6 nd ra router-lifetime <i>lifetime</i>	Configure the lifetime of the router in the RA message.
8	Raisecom(config-port)# ipv6 nd ra hop-limit <i>hopsvalue</i>	Configure the hop limits in the RA message.
9	Raisecom(config-port)# ipv6 nd ra reachable-time <i>time</i>	Configure the peer reachable time in the RA message.
10	Raisecom(config-port)# ipv6 nd ra retrans-timer <i>value</i>	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.

7.4.4 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 <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-port)# ipv6 nd proxy { enable disable }	Enable or disable ordinary ND Proxy.

7.5 Configuring ICMP

7.5.1 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 ICMPv4 packet sending.
3	Raisecom(config)#ipv4 icmp send-rate bucket bucket-size ratelimit interval	Configure the limit of the sending rate for ICMPv4 packets.
4	Raisecom(config)#ipv4 icmp { type type-value code code-value name icmp-name all } receive	Enable ICMPv4 packet receiving.
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 ICMPv4 packets when the IP address is unavailable.
7	Raisecom(config-port)#ipv4 icmp port- unreachable send	Enable the function of sending ICMPv4 packets when the interface is unavailable.

7.5.2 Configuring IPv6 ICMP

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ipv6 icmp send-rate bucket bucket-size ratelimit interval	Configure the bucket size and rate limit of sending ICMPv6 error packets.
3	Raisecom(config)#ipv6 icmp { type type-value code icmpv6-code name icmpv6-name all } send	Enable the function of sending ICMPv6 packets.
4	Raisecom(config)#ipv6 icmp { type type-value code icmpv6-code name icmpv6-name all } receive	Enable the function of receiving ICMPv6 packets.
5	Raisecom(config)#ipv6 icmp redirect send	Enable the function of ICMPv6 packet redirection sending.
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 unavailable.
8	Raisecom(config-port)#ipv6 icmp port- unreachable send	Enable the function of sending ICMPv6 packets when the IPv6 interface is unavailable.

Step	Command	Description
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.

7.6 Configuring VRF

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.
5	Raisecom(config-vrf)# tunnel-policy policy-name	(Optional) configure the VRF tunnel policy and enter tunnel policy configuration mode.
6	Raisecom(config-tunnelpolicy)# tunnel select-seq { lsp cr-lsp } *	(Optional) configure the tunnel priority.

7.7 Configuring fault detection

7.7.1 PING

PING IPv4 network

Step	Command	Description
1	Raisecom# ping [vrf vpn-instance-name] ip-address [count count] [size size] [waittime period] [source ip-address] [df-bit]	Use the ping command to test the connectivity of the IPv4 network.



Note

The RAX711-C-R 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 [<i>vrf vpn-instance-name</i>] ipv6 <i>ipv6-address</i> [<i>count count</i>] [<i>size size</i>] [<i>waittime period</i>] [<i>source ipv6-address</i>]	Use the ping command to test the connectivity of the IPv6 network.

PING MPLS network

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

7.7.2 Traceroute

Traceroute IPv4 network

The interface is configured with an IPv4 address.

Step	Command	Description
1	Raisecom# traceroute [<i>vrf vpn-instance-name</i>] <i>ip-address</i> [<i>firstttl first-ttl</i>] [<i>maxttl max-ttl</i>] [<i>port port-number</i>] [<i>waittime period</i>] [<i>count times</i>] [<i>size size</i>]	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 <i>vpn-instance-name</i>] ipv6 <i>ipv6-address</i> [firstttl <i>first-ttl</i>] [maxttl <i>max-ttl</i>] [port <i>port-number</i>] [waittime <i>period</i>] [count <i>times</i>] [size <i>size</i>]	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 <i>ip-address/m</i> [next-hop <i>ip-address</i>] [maxttl <i>max-ttl</i>] [waittime <i>seconds</i>]	Use the traceroute command to test the MPLS network connectivity of a specified IPv4 address and check the network nodes that the packet has passed through.
2	Raisecom# traceroute mpls vc-id <i>vc-id</i> destination <i>ip-address</i> [maxttl <i>max-ttl</i>] [waittime <i>seconds</i>]	Use the traceroute command to test the MPLS network connectivity of a specified VC-ID and check the network nodes that the packet has passed through.

7.8 Configuring DHCPv4 Server

7.8.1 Preparing for configurations

Scenario

When the RAX711-C-R works as the DHCP v4 server, the DHCP v4 client can obtain the IP address from the server.

Prerequisite

The RAX711-C-R is not enabled with DHCP v4 Client. In addition, the DHCP v4 server works in common DHCP v4 server mode.

7.8.2 Creating and configuring IPv4 address pool

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

Step	Command	Description
2	Raisecom(config)# ip dhcp server pool <i>pool-name</i>	Create the IPv4 address pool and enter address pool configuration mode.
3	Raisecom(config-pool)# address <i>start-ip-address end-ip-address</i> mask { <i>mask</i> <i>mask-length</i> }	Configure the range of the IPv4 address pool.
4	Raisecom(config-pool)# lease expired { <i>minute</i> infinite }	Configure the lease of the IPv4 address pool.
5	Raisecom(config-pool)# dns-server <i>ip-address</i> [secondary]	Configure the DNS of the IPv4 address pool.
6	Raisecom(config-pool)# gateway <i>ip-address</i>	Configure the default gateway of the IPv4 address pool.
7	Raisecom(config-pool)# option 60 <i>vendor-string</i>	Configure information carried by Option 60.
8	Raisecom(config-pool)# option 43 [sub-option <i>option-id</i>] { hex ascii } <i>string</i>	Configure the information carried by Option43.
9	Raisecom(config-pool)# tftp-server <i>ip-address</i>	Configure the TFTP server of the IPv4 address pool.
10	Raisecom(config-pool)# trap server-ip <i>ip-address</i>	Configure the Trap server of the IPv4 address pool.

7.8.3 Configuring DHCP v4 Server on interface

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

7.8.4 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.

No.	Command	Description
5	Raisecom(config)# show ip server pool [<i>pool-name</i>]	Show configurations of the DHCPv4 address pool.

7.9 Configuring DHCPv6 server

7.9.1 Enabling global DHCPv6 Server

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ipv6 dhcp server	Enable global DHCPv6 Server.

7.9.2 Creating and configuring IPv6 address pool

To assign IPv6 addresses and network parameters to clients through DHCPv6 Server, an address pool must be created on the DHCPv6 Server.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ipv6 dhcp server pool <i>pool-name</i>	Create an address pool for assigning addresses and enter address pool mode.
3	Raisecom(dhcp-pool)# address prefix <i>ipv6-address/prefix-length</i>	Configure the prefix of the address pool.
4	Raisecom(dhcp-pool)# lifetime preferred-lifetime { <i>preferred-minute</i> infinite } valid-lifetime { <i>valid-minute</i> infinite }	(Optional) configure the lease time of the address pool, including the preferred time and effective time.
5	Raisecom(dhcp-pool)# dns-server <i>ipv6-address</i>	(Optional) configure the DNS server address of the address pool.

7.9.3 Creating and configuring IPv6 prefix pool

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ipv6 dhcp server prefix-pool <i>pool-name</i>	Create an address pool for assigning addresses and enter prefix address pool.
3	Raisecom(dhcp-prefix-pool)# prefix-delegation <i>ipv6-address/prefix-length</i>	Specify the address prefix of the IPv6 prefix pool.

7.9.4 Configuring DHCPv6 Server on interface

Only when DHCPv6 Server is enabled globally and on the interface, and the address pool is bound to the interface, can the interface receive and process the client's DHCPv6 request packets.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ipv6 dhcp server	Enable global DHCPv6 Server.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode or sub-interface configuration mode. By default, the interface is in router mode.
4	Raisecom(config-port)#ipv6 dhcp server	Enable DHCPv6 Server on the interface.
5	Raisecom(config-port)#ipv6 dhcp server rapid-commit	(Optional) enable rapid interaction on the interface.
6	Raisecom(config-port)#ipv6 dhcp server pool <i>pool-name</i>	Bind the address pool to the interface.
7	Raisecom(config-port)#ipv6 dhcp server prefix-pool <i>pool-name</i>	Bind the prefix pool to the interface.

7.9.5 Checking configurations

No.	Command	Description
1	Raisecom#show ipv6 dhcp server	Show DHCPv6 Server configurations.
2	Raisecom#show ipv6 dhcp server pool [<i>pool-name</i>]	Show configurations of the DHCPv6 Server address pool.
3	Raisecom#show ipv6 dhcp server prefix-pool [<i>pool-name</i>]	Show configurations of the DHCPv6 Server prefix pool.
4	Raisecom#show ipv6 dhcp server binding	Show information about the assigned IPv6 address and its clients.
5	Raisecom#show ipv6 dhcp pd server binding	Show binding information about the DHCPv6 prefix entrusting server.

7.10 Configuring DHCPv4 Client

7.10.1 Preparing for configurations

Scenario

When working as the DHCPv4 client, the RAX711-C-R can obtain an IP address from the DHCPv4 server. You can use the IP address to manage the RAX711-C-R.

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.

Prerequisite

The RAX711-C-R is not enabled with DHCPv4 Server and works in common DHCP Client mode.

7.10.2 (Optional) configuring DHCPv4 client information



Note

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)#interface <i>interface-type interface-number</i>	Enter Layer 3 interface configuration mode.
3	Raisecom(config-port)#ip dhcp client { class-id <i>class-id</i> client-id <i>client-id</i> hostname <i>hostname</i> }	Configure DHCPv4 Option 60 client, including the type identifier, client identifier, and host name. This command only takes effect on the Layer 3 interface.

7.10.3 Configuring DHCPv4 Client on Layer 3 interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 3 interface configuration mode.

Step	Command	Description
3	Raisecom(config-port)# ip address dhcp [server-ip <i>ip-address</i>]	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.

7.10.4 Renewing or releasing IPv4 address

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	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.
4	Raisecom(config-port)# no ip address dhcp	Release the IPv4 address. This command takes effect only on Layer 3 interface.

7.10.5 Checking configurations

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

7.11 Configuring DHCPv6 client

7.11.1 Configuring DHCPv6 client

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)# ipv6 address dhcp [server-ip <i>ipv6-address</i>]	Apply for the IPv6 address through DHCPv6.
4	Raisecom(config-port)# ipv6 dhcp client pd	Configure the prefix address pool of the DHCPv6 client.

Step	Command	Description
5	Raisecom(config-port)#ipv6 dhcp client renew	(Optional) renew the IP address. If the IP interface of the device has obtained an IP address through DHCP, the IP address will automatically renew when its lease time expires.
6	Raisecom(config-port)#ipv6 dhcp client rapid-commit	(Optional) enable the DHCPv6 Client to apply for fast interaction mode.
7	Raisecom(config-port)#ipv6 dhcp client information-request	(Optional) configure applying DNS, domain name, and other configurations through DHCPv6.

7.11.2 Checking configurations

No.	Command	Description
1	Raisecom#show ipv6 dhcp client	Show DHCPv6 Client configurations.

7.12 Configuring DHCPv4 Relay

7.12.1 Preparing for configurations

Scenario

When the RAX711-C-R 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 RAX711-C-R is not enabled with DHCPv4 Client or DHCPv4 Server.

7.12.2 Configuring global DHCPv4 Relay

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip dhcp relay	Enable global DHCPv4 relay.

7.12.3 Configuring DHCPv4 relay on interface

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

7.12.4 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 <i>interface-type interface-number</i>	Enter interface configuration mode.
5	Raisecom(config-port)#ip dhcp relay information trusted	Configure DHCPv4 relay trusted interface.

7.12.5 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.

7.13 Configuring DHCPv6 relay

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ipv6 dhcp relay	Enable global DHCPv6 relay.
3	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode. By default, the interface is in router mode.
4	Raisecom(config-port)#ipv6 dhcp relay	Enable interface DHCPv6 relay.
4	Raisecom(config-port)#ipv6 dhcp relay target- ip <i>ipv6-address</i>	Configure the destination IPv6 address for forwarding packets.

7.14 Configuring DHCPv4 Snooping

7.14.1 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 switch configured with DHCP Snooping Option can process the packets according to whether the packet contains the Option field.

Prerequisite

N/A

7.14.2 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 <i>number</i>	Configure the maximum number of DHCPv4 Snooping binding tables.
4	Raisecom(config)#ip dhcp snooping option client-id	(Optional) configure DHCPv4 Snooping Option61.
5	Raisecom(config)#ip dhcp snooping option <i>optiong-code</i>	Configure DHCPv4 Snooping Option.

Step	Command	Description
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 <i>time</i>	(Optional) configure the interval for automatically saving the DHCPv4 Snooping binding table.
8	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
9	Raisecom(config-port)#ip dhcp snooping trust	Configure the interface to a DHCP Snooping trusted interface.
10	Raisecom(config-port)#ip dhcp snooping vlan <i>vlan-id</i>	Enable DHCP Snooping on a specified interface and a specified VLAN.

7.14.3 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 <i>interface-type interface-number</i>	Enter interface configuration mode.
4	Raisecom(config-port)#ip dhcp snooping information option vlan-list <i>vlan-list</i>	Configure the VLAN list of interface DHCP Snooping Option 82 VLAN.

7.14.4 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 [<i>max-learning-num</i>]	Show the DHCPv4 Snooping binding table.

7.15 Configuring DHCPv6 Snooping

7.15.1 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 <i>number</i>	Configure the maximum number of DHCPv6 Snooping binding tables.
4	Raisecom(config)#ipv6 dhcp snooping option <i>option-code</i>	Configure DHCPv6 Snooping Option.
5	Raisecom(config)#ipv6 dhcp snooping option remote-id	Configure DHCPv6 Snooping Option37.
6	Raisecom(config)#ipv6 dhcp snooping option interface-id	Configure DHCPv6 Snooping Option18.
7	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
8	Raisecom(config-port)#ipv6 dhcp snooping trust	Configure the interface to a DHCPv6 Snooping trusted interface.
9	Raisecom(config-port)#ipv6 dhcp snooping vlan <i>vlan-id</i>	Enable DHCPv6 Snooping on a specified interface and a specified VLAN.

7.15.2 Checking configurations

No.	Command	Description
1	Raisecom#show ipv6 dhcp snooping	Show DHCPv6 Snooping configurations.
2	Raisecom#show ipv6 dhcp snooping binding [max-learning-num]	Show information about the DHCPv6 Snooping binding table.

7.16 Configuring DHCPv4/DHCPv6 Option

7.16.1 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.

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.

Option 18 refers to the interface ID option. After receiving the request message sent by the DHCPv6 client to the DHCPv6 server, the DHCPv6 Snooping device adds the Option 18 option to the message and forwards it to the DHCPv6 server. The DHCPv6 server selects an appropriate address pool according to the client information carried in Option 18 and allocates an IPv6 addresses for the DHCPv6 client.

Option 37 refers to the remote ID option. After receiving the request message sent by the DHCPv6 client to the DHCPv6 server, the DHCPv6 Snooping device adds the Option 37 option to the message and forwards it to the DHCPv6 server. The DHCPv6 server can use the information in Option 37 to locate the DHCPv6 client, thus allocating IPv6 addresses.

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.

7.16.2 Configuring IPv4 DHCP Option 82

Option 82 should be used on the device with DHCP Snooping 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.

7.16.3 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.

Step	Command	Description
3	Raisecom(config)# interface <i>interface-type</i> <i>interface-number</i> Raisecom(config-port)# ipv4 dhcp option client-id { ascii <i>ascii-string</i> hex <i>hex-string</i> ip-address <i>ip-address</i> }	Configure Option 61 on the interface.

7.16.4 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.

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

7.16.5 Configuring IPv6 DHCP Option 18

Option 18 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)# ipv6 dhcp snooping option interface-id	Configure the Option device to support Option 18.
3	Raisecom(config)# interface <i>interface-type</i> <i>interface-number</i> Raisecom(config-port)# ipv6 dhcp option interface-id { ascii <i>ascii-string</i> hex <i>hex-string</i> ipv6-address <i>ip-address</i> }	(Optional) configure Option 18 on the interface.
4	Raisecom(config)# ipv6 dhcp option interface-id { ascii <i>ascii-string</i> hex <i>hex-string</i> ipv6-address <i>ip-address</i> }	(Optional) create IPv6-based Option 18.
5	Raisecom(config)# interface <i>interface-type</i> <i>interface-number</i> Raisecom(config-port)# ipv6 dhcp option interface-id { ascii <i>ascii-string</i> hex <i>hex-string</i> ipv6-address <i>ip-address</i> }	(Optional) create IPv6-based Option 18 on the interface.

7.16.6 Configuring IPv6 DHCP Option 37

Option 37 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)#ipv6 dhcp option remote-id { ascii <i>ascii-string</i> hex <i>hex-string</i> mac-format <i>mac-string</i> }	Configure Option 37.

7.16.7 Configuring IPv6 DHCP Option 38

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ipv6 dhcp client option38 enable	Enable Option 38.

7.16.8 Configuring IPv6 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.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ipv6 dhcp option { option-id interface-id } { ascii <i>ascii-string</i> hex <i>hex-string</i> ipv6-address <i>ip-address</i> }	(Optional) create a self-defined Option field based on IPv6.
3	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i> Raisecom(config-port)#ipv6 dhcp option option-id { ascii <i>ascii-string</i> hex <i>hex-string</i> ipv6-address <i>ip-address</i> }	(Optional) create a self-defined Option field based on IPv6 on the interface.

7.16.9 Checking configurations

No.	Command	Description
1	Raisecom#show ipv6 dhcp snooping	Show DHCPv6 Snooping configurations.
2	Raisecom#show ipv6 dhcp snooping binding [max-learning-num]	Show binding information about DHCPv6 Snooping.
3	Raisecom#show ip dhcp information option	Show configurations of DHCP Option.

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 <i>router-id</i>	Configure the Router ID. By default, the Router ID is 192.168.1.1.

8.1.2 Configuring IP FRR

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

Step	Command	Description
2	Raisecom(config)# ip frr route-map <i>map-name</i> [wtr-timer <i>timer</i>]	Configure IP FRR.

8.1.3 Checking configurations

No.	Command	Description
1	Raisecom# show router id	Show the Router ID.
2	Raisecom# show fib [vrf <i>vrf-name</i>] [<i>ip-address</i> <i>ipv6-address/m</i>]	Show the route forwarding table.
3	Raisecom# show fib [vrf <i>vrf-name</i>] [domain { ipv4 ipv6 }]	Show the domain of the route forwarding table.
4	Raisecom# show fib summary [all vrf <i>vrf-name</i>]	Show statistics of the route forwarding table.

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 IPv4 static route

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

Step	Command	Description
2	Raisecom(config)# ip route [vrf vrf-name] { <i>ip-address mask-address</i> <i>ip-address/m</i> } [vrf vrf-name] <i>next-hop</i> [<i>interface-type interface-number</i> port-channel <i>channel-number</i> vlan <i>vlan-id</i>] [distance <i>distance-value</i>] [description <i>words</i>] [tag <i>tag-value</i>]	Configure IPv4 static routes.
3	Raisecom(config)# ip route [vrf vrf-name] <i>ip-address mask-address</i> NULL 0 [distance <i>distance-value</i>] [description <i>words</i>] [tag <i>tag-value</i>]	(Optional) configure the IPv4 static route of the NULL interface.
4	Raisecom(config)# ip route static distance <i>distance</i>	(Optional) configure the default administrative distance of the IPv4 static route. The default administrative distance is 1.

8.2.3 IPv6 static route

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

8.2.4 Configuring BFD for static routes

BFD for IPv4 static route

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

Step	Command	Description
2	Raisecom(config)# ip route [vrf vrf-name] { <i>ip-address mask-address</i> <i>ip-address/m</i> } [vrf vrf-name] next-hop [<i>interface-type</i> <i>interface-number</i> port-channel <i>channel-</i> <i>number</i> vlan <i>vlan-id</i>] track bfd-session <i>bfd-session-id</i>	Bind static routes with BFD sessions. BFD can achieve fast response to faults and route switching.
	Raisecom(config)# ip route [vrf vrf-name] <i>ip-address mask-address</i> NULL 0 track bfd- session <i>bfd-session-id</i>	

BFD for IPv6 static route

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ipv6 route [vrf vrf-name] { <i>ipv6-address/0</i> <i>ipv6-address/m</i> } [vrf <i>vrf-name</i>] ipv6-next-hop [<i>interface-type</i> <i>interface-number</i> port-channel <i>channel-</i> <i>number</i>] track bfd-session <i>bfd-session-id</i>	Bind static routes with BFD sessions. BFD can achieve fast response to faults and route switching.
	Raisecom(config)# ipv6 route [vrf vrf-name] { <i>ipv6-address/0</i> <i>ipv6-address/m</i> } NULL 0 track bfd-session <i>bfd-session-id</i>	

8.2.5 Checking configurations

No.	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] <i>ip-</i> <i>address</i> [<i>mask-address</i>] [longer-prefixes] [detail]	Show the route to a destination IPv4 address.
3	Raisecom# show ip route [vrf vrf-name] <i>ip-</i> <i>address1</i> [<i>mask-address1</i>] <i>ip-address2</i> [<i>mask-</i> <i>address2</i>] [detail]	Show routing information between two IPv4 addresses.
4	Raisecom# show ipv6 route [all vrf vrf-name] [protocol { static connected bgp ospf isis rip }] [detail]	Show the IPv6 routing table.
5	Raisecom# show ip route [vrf vrf-name] summary	Show the IPv4 route summary.
6	Raisecom# show ipv6 route [vrf vrf-name] summary	Show the IPv6 route summary.
7	Raisecom# show ipv6 route [vrf vrf-name] { <i>start-ipv6-address/0</i> <i>start-ipv6-address/m</i> } { <i>end-ipv6-address/0</i> <i>end-ipv6-address/m</i> } [detail]	Show routing information between two IPv6 addresses.

No.	Command	Description
8	Raisecom# show ipv6 route [<i>vrf vrf-name</i>] <i>ipv6-address</i> [<i>prefix-length</i>] [longer-prefixes] [detail]	Show the route to a destination IPv6 address.

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 <i>prefix-name</i> [seq seq-number] { deny permit } { <i>ip-address/mask</i> any }	Create an IPv4 prefix-list or add a node to the IP prefix-list.
	Raisecom(config)# ip prefix-list <i>prefix-name</i> [seq seq-number] { deny permit } <i>ip-address/mask</i> { ge min-length ge min-length le max-length }	If no prefix-list ID (<i>seq-number</i>) is configured, the system will generate a prefix-list ID automatically. The generated pre-fix list ID has 5 digits.
	Raisecom(config)# ip prefix-list <i>prefix-name</i> [seq seq-number] { deny permit } <i>ip-address/mask</i> { le max-length le max-length ge min-length }	
3	Raisecom(config)# ip prefix-list <i>prefix-name</i> 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 filter

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

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip as-path access-list <i>access-list-number</i> { permit deny } <i>regex</i>	(Optional) configure the filter that is based on AS path of the BGP route.
3	Raisecom(config)#ip community-list { <i>standard-list-number</i> standard <i>standard-list-name</i> } { permit deny } <i>community-number</i> [internet] [local-as] [no-advertise] [no-export] Raisecom(config)#ip community-list { <i>expanded-list-number</i> expanded <i>expanded-list-name</i> } { permit deny } <i>regex</i>	(Optional) configure the filter that is based on standard or advanced community properties of the BGP route.
4	Raisecom(config)#ip extcommunity-list { <i>standard-list-number</i> standard <i>standard-list-name</i> } { permit deny } rt <i>route-target-number</i>	(Optional) configure the filter that is based on standard community properties of the BGP route.
5	Raisecom(config)#ip rd-filter <i>rd-filter-number</i> { permit deny } rd <i>rd-number</i>	(Optional) configure the filter that is based on RD property of the BGP route.

IPv4 routing table

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#route-map <i>map-name</i> { permit deny } <i>number</i>	Create the route mapping table and enter route mapping configuration mode.
3	Raisecom(config-route-map)#description <i>string</i>	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 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 <i>number</i>	Configure the on-match clause to continuing to match at some node. By default, the process is finished after matching.
6	Raisecom(config-route-map)#call <i>map-name</i>	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 <i>acl-number</i>	Configure the match clause to matching the next hop based on extended IP ACL.

8	Raisecom(config-route-map)# match ip next-hop prefix-list <i>prefix-name</i>	Configure the match clause to matching the next hop based on IP prefix-list.
9	Raisecom(config-route-map)# match ip address <i>acl-number</i>	Configure the match clause to matching the IP address based on extended IP ACL.
10	Raisecom(config-route-map)# match ip address prefix-list <i>prefix-name</i>	Configure the match clause to matching the IP address based on IP prefix-list.
11	Raisecom(config-route-map)# match interface <i>name</i>	Configure the match clause to matching the interface name.
12	Raisecom(config-route-map)# match metric <i>metric</i>	Configure the match clause to the matching rule that is based on route metric value.
13	Raisecom(config-route-map)# match tag <i>tag</i>	Configure the match clause to the matching rule that is based on Tag field of the route tagging.
14	Raisecom(config-route-map)# match as-path <i>path-list-number</i>	Configure the match clause to the BGP routing information matching rule that is based on AS-Path filter.
15	Raisecom(config-route-map)# match community { <i>community-list-number</i> <i>community-list-name</i> } [exact-match]	Configure the match clause to the BGP routing information matching rule that is based on community filter.
16	Raisecom(config-route-map)# extcommunity { <i>extcommunity-list-number</i> <i>extcommunity-list-name</i> }	Configure the match 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 <i>prefix-name</i>	Configure the match 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 <i>rd-filter-number</i>	Configure the match clause to the BGP routing information matching rule that is based on RD property filter.
19	Raisecom(config-route-map)# set metric [+ -] <i>metric</i>	Configure the set clause to modifying the route metric value after matching.
20	Raisecom(config-route-map)# set metric-type { type-1 type-2 }	Configure the set clause to modifying the route metric type after matching.
21	Raisecom(config-route-map)# set src ip-address	Configure the set clause to modifying the source IP address after matching.
22	Raisecom(config-route-map)# set ip next-hop ip-address	Configure the set clause to modifying the next-hop IP address of the route after matching.
23	Raisecom(config-route-map)# set tag <i>tag</i>	Configure the set clause to modifying the routing information tag after matching.
24	Raisecom(config-route-map)# set origin { egp <i>as-number</i> igp incomplete }	Configure the set clause to modifying the route source of the BGP routing information that matches with the routing policy.

25	Raisecom(config-route-map)#set as-path prepend <i>as-number</i>	Configure the set clause to modifying the as-path property of the BGP routing information that matches with the routing policy.
26	Raisecom(config-route-map)#set local-preference <i>preference</i>	Configure the set clause to modifying the local priority of the BGP routing information that matches with the routing policy.
27	Raisecom(config-route-map)#set community { <i>community-number</i> internet local-as no-advertise no-export } * [additive] Raisecom(config-route-map)# set community none	Configure the set clause to setting or deleting the community property of the BGP routing information that matches with the routing policy.
28	Raisecom(config-route-map)#set comm-list { <i>community-list-number</i> <i>community-list-name</i> } delete	Configure the set clause to deleting the community property of the BGP routing information that matches with the routing policy.
29	Raisecom(config-route-map)#set extcommunity rt <i>route-target-number</i> [additive]	Configure the set clause to adding or modifying the community property of the BGP routing information that matches with the routing policy.
30	Raisecom(config-route-map)#set ip backup-interface <i>interface-type interface-number</i>	Configure the set clause to modifying the backup egress interface after matching the policy.
31	Raisecom(config-route-map)#set ip backup-nexthop <i>nexthop-address</i>	Configure the set clause to modifying the backup next-hop address after matching the policy.

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 <i>prefix-name</i> [seq seq-number] { deny permit } { <i>ipv6-address/m</i> any } Raisecom(config)#ipv6 prefix-list <i>prefix-name</i> [seq seq-number] { deny permit } <i>ipv6-address/m</i> { ge min-length ge min-length 1e max-length } Raisecom(config)#ipv6 prefix-list <i>prefix-name</i> [seq seq-number] { deny permit } <i>ipv6-address/m</i> { 1e max-length 1e max-length ge min-length }	Create an IPv6 prefix list, or add a node to it. If you do not configure the prefix list <i>seq-number</i> , the sequence number be automatically generated by the system with a step of 5.

Step	Command	Description
3	Raisecom(config)# ipv6 prefix-list <i>prefix-name</i> description <i>string</i>	Configure description of the IPv6 prefix list. If the input description exceeds 80 characters, the first 80 characters will be applied.

IPv6 routing table

Step	Command	Description
1	Raisecom(config)# route-map <i>map-name</i> { permit deny } <i>number</i>	Create a routing table and enter routing table configuration mode.
2	Raisecom(config-route-map)# match ipv6 address <i>acl-number</i>	Configure a match clause to matching 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 <i>prefix-name</i>	Configure a match clause to matching the IP address based on IP prefix list.
4	Raisecom(config-route-map)# match ipv6 next-hop <i>acl-number</i>	Configure a match clause to matching 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 <i>prefix-name</i>	Configure a match clause to matching the next hop based on IP prefix list.
6	Raisecom(config-route-map)# match ipv6 route-source <i>prefix-list</i> <i>prefix-name</i>	Configure a match clause to matching routing source address based on prefix list for the BGP routing matching rules.
7	Raisecom(config-route-map)# set ipv6 next-hop { <i>ipv6-address</i> <i>peer-address</i> }	Configure the set clause to modifying the next-hop IP address after matching.
8	Raisecom(config-route-map)# set ipv6 backup-interface <i>interface-type</i> <i>interface-number</i>	Configure the set clause to modifying the egress interface after matching.
9	Raisecom(config-route-map)# set ipv6 backup-nexthop <i>ipv6-address</i>	Configure the set clause to modifying the next-hop address after matching.

8.3.3 Checking configurations

No.	Command	Description
1	Raisecom# show ip as-path access-list <i>access-list-number</i>	Show filtering information about the AS-path list.
2	Raisecom# show ip prefix-list [<i>prefix-name</i>] [seq <i>seq-number</i>]	Show information about the IP prefix list.

No.	Command	Description
3	Raisecom# show ip prefix-list <i>prefix-name</i> <i>ip-address/m</i> { longer first-match }	
4	Raisecom# show ip prefix-list summary [<i>prefix-name</i>]	Show summary of the IP prefix list.
5	Raisecom# show ip prefix-list detail [<i>prefix-name</i>]	Show statistics on the IP prefix list.
6	Raisecom# show ipv6 prefix-list [<i>prefix-name</i>] [seq <i>seq-number</i>]	Show information about the IPv6 prefix list.
7	Raisecom# show ipv6 prefix-list <i>prefix-name</i> <i>ipv6-address/m</i> { longer first-match }	
8	Raisecom# show ipv6 prefix-list summary [<i>prefix-name</i>]	Show summary of the IPv6 prefix list.
9	Raisecom# show ipv6 prefix-list detail [<i>prefix-name</i>]	Show statistics on the IPv6 prefix list.
10	Raisecom# show route-map <i>map-name</i>	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 [<i>community-list-number</i>] [<i>community-list-name</i>]	Show information about the group attribute list.
13	Raisecom# show ip extcommunity-list [<i>community-list-number</i>] [<i>community-list-name</i>]	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.

Step	Command	Description
2	Raisecom(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)# network <i>ip-address wild-card-mask</i> area <i>area-id</i>	Configure network segments included in the OSPF area.



Note

- 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 <i>process-id</i> [router-id <i>router-id</i>]	Enable 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.

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 <i>interface-type</i> <i>interface-number</i>	Enter Layer 3 interface configuration mode.
3	Raisecom(config-port)# ip ospf cost <i>cost</i>	Configure the OSPF cost of the IP interface.

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]	Enable 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]	Enable 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.

8.4.3 Configuring OSPF network type

Configuring OSPF network

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

Step	Command	Description
2	Raisecom(config)# interface <i>interface-type interface-number</i>	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 <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)# ip ospf priority <i>priority</i>	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 <i>interface-type interface-number</i>	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 <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
5	Raisecom(config-router-ospf)# neighbor <i>ip-address</i> [priority <i>priority</i>]	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.



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]	Enable 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.
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 paths of IP ECMP.

8.4.6 Maximizing LSA metric

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]	Configure maximum metric of the OSPF LSA packets. The metric of LSA packets 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.

Step	Command	Description
4	Raisecom(config-port)# ip ospf hello-interval <i>seconds</i>	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 <i>seconds</i>	Configure the OSPF Poll timer interval. By default, it is 120s.
6	Raisecom(config-port)# ip ospf retransmit-interval <i>seconds</i>	Configure the LAS retransmission interval on the IP interface. By default, it is 5s.
7	Raisecom(config-port)# ip ospf transmit-delay <i>seconds</i>	Configure the LSA retransmission delay on the IP interface. By default, it is 1s.



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 configure 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]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)# timers spf { <i>delay-time hold-time</i> 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.

Configuring OSPF passive interface

To make some OSPF routing information not obtained by some router on the network, you can configure 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 <i>interface-type interface-number</i>	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 <i>interface-type interface-number</i>	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 Hello packet.

Preventing Hello packet attacks

To prevent Hello 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 <i>process-id</i> [router-id <i>router-id</i>]	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.

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]	Enable 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.

8.4.9 Controlling OSPF redistributed routes

Configuring OSPF redistributed routes

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

Step	Command	Description
2	Raisecom(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)# redistribute { static connected isis bgp } [<i>metric metric</i>] [metric-type { 1 2 }] [tag <i>tag-value</i>] [route-map <i>map-name</i>] Raisecom(config-router-ospf)# redistribute ospf [<i>process-id</i>] [<i>metric metric</i>] [metric-type { 1 2 }] [tag <i>tag-value</i>] [route-map <i>map-name</i>]	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 <i>limit-number</i>	Configure the threshold of redistributed OSPF external routes. By default, no threshold is configured.

Configuring inter-area route aggregation

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

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

Aggregating redistributed external routes

After the external route is redistributed, configure route aggregation on the ASBR. The RAX711-C-R just puts the aggregated 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.

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

Advertising default route

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)# default-information originate [always] [metric <i>metric</i>] [type { 1 2 }]	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 <i>list-name</i> { permit deny } <i>ip-address mask-length</i> [ge <i>ge-length</i>] [le <i>le-length</i>]	Configure the IP prefix-list.
3	Raisecom(config)# access-list <i>acl-number</i>	Create an ACL and enter ACL configuration mode. Enter basic IP ACL configuration mode when the <i>acl-number</i> ranges from 1000 to 1999.
	Raisecom(config-ipv4-std)# rule [<i>rule-id</i>] { deny permit } { <i>source-ip-address</i> <i>source-ip-mask</i> any }	Configure basic IP ACL rules.
4	Raisecom(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.

Step	Command	Description
5	Raisecom(config-router-ospf)# distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> } 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 RAX711-C-R 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 <i>list-name</i> { permit deny } <i>ip-address mask-length</i> [ge <i>ge-length</i>] [le <i>le-length</i>]	Configure the IP prefix-list. You can use the no ip prefix-list list-name command to delete the configuration.
3	Raisecom(config)# access-list <i>acl-number</i>	Create an ACL and enter ACL configuration mode. Enter basic IP ACL configuration mode when the <i>acl-number</i> ranges from 1000 to 1999.
	Raisecom(config-acl-ip-std)# rule [<i>rule-id</i>] { deny permit } { <i>source-ip-address source-ip-mask</i> any }	Configure the basic IP ACL rule.
4	Raisecom(config)# router ospf <i>process-id</i> [router-id <i>router-id</i>]	Enable an OSPF process and enter OSPF configuration mode.
5	Raisecom(config-router-ospf)# distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> } 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 <i>acl-number</i> prefix-list <i>list-name</i> } out [static connected bgp rip]	Configure the OSPF releasing policy.
	Raisecom(config-router-ospf)# distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> } out ospf <i>process-id</i>	



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 Type3 LSA filtering policy

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip prefix-list list-name { permit deny } <i>ip-address mask-length</i> [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]	Enable 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.
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 <i>interface-number</i>	Enter interface configuration mode.

Step	Command	Description
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 <i>process-id</i> [router-id <i>router-id</i>]	Enable 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 <i>area-id</i>	Enable TE in the OSPF area. By default, it is disabled.
5	Raisecom(config-router-ospf)# mpls traffic-eng router-id <i>router-id</i>	Configure the Router ID of the MPLS-TE router.

8.4.13 Checking configurations

No.	Command	Description
1	Raisecom# show ip ospf [<i>process-id</i>]	Show OSPF basic information.
2	Raisecom# show ip ospf [<i>process-id</i>] route	Show OSPF routing information.
3	Raisecom# show ip ospf [<i>process-id</i>] interface [<i>interface-type</i> <i>interface-number</i>]	Show OSPF interface information.
4	Raisecom# show ip ospf [<i>process-id</i>] neighbor [<i>interface-type</i> <i>interface-number</i>] [<i>ip-address</i>]	Show OSPF neighbor information.
5	Raisecom# show ip ospf [<i>process-id</i>] neighbor statistics	Show OSPF neighbor statistics.
6	Raisecom# show ip ospf [<i>process-id</i>] database [max-age self-originate]	Show information about OSPF link status database.

No.	Command	Description
7	Raisecom# show ip ospf [<i>process-id</i>] database { asbr-summary external network router summary nssa-external opaque-link opaque-area opaque-as } [<i>ip-address</i>] [adv-router <i>ip-address</i> self-originate]	Show details about the OSPF link status database.
8	Raisecom# show ip ospf [<i>process-id</i>] database statistics	Show information about area border router and ASBR.
9	Raisecom# show ip ospf [<i>process-id</i>] border-routers	Show external statistics about OSPF ASBR.
10	Raisecom# show ip ospf [<i>process-id</i>] summay-address	Show summary about the OSPF ASBR external route.

8.4.14 Maintenance

Command	Description
Raisecom# clear ip ospf [<i>process-id</i>] 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 <i>process-id</i> [vrf <i>vrf-name</i>]	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)# router-id <i>router-id</i>	Configure the Router-ID of the OSPF process.

Configuring process IPsec authentication policy

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ipv6 router ospf <i>process-id [vrf vrf-name]</i>	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#ipsec policy <i>policy-name</i>	Configure the IPsec authentication policy of the OSPF process. The various parameters of the authentication policy must be valid so that the policy can be applied. By default, the process is not authenticated.

8.5.2 Configuring OSPFv3 network type

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#ipv6 ospf network { broadcast nbma ptmp ptp } [instance-id <i>instance-id</i>]	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 <i>process-id [vrf vrf-name]</i>	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.

Step	Command	Description
3	<code>Raisecom(config-ospf6)#area { area-id ip-format-area-id } stub [no-summary]</code>	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.

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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ipv6 router ospf process-id</code>	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	<code>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]</code>	Configure the virtual link.

8.5.4 Configuring OSPFv3 interface

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

Step	Command	Description
3	Raisecom(config-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.

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.  Note The device supports up to one OSPFv3 process, and one process can contain multiple OSPFv3 instances.

Step	Command	Description
3	<code>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]</code>	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 aggregation

If there are some continuous network segments in an area, you can configure route aggregation 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ipv6 router ospf process-id</code>	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	<code>Raisecom(config-ospf6)#area area-id range ipv6-address/mask [not-advertise]</code>	Configure inter-domain route aggregation.

Aggregating redistributed external routes

After ASBR imports external routes, if you configure route aggregation, the device only puts the aggregated routes in ASE LSA for announcement, reducing the number of LSAs in LSDB.

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

Step	Command	Description
2	<code>Raisecom(config)#ipv6 router ospf process-id</code>	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	<code>Raisecom(config-ospf6)#summary-address ipv6-address/mask [not-advertise]</code>	Configure external route aggregation. By default, external routes are not aggregated.

Advertising default route

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ipv6 router ospf process-id</code>	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	<code>Raisecom(config-ospf6)#default-information originate [always] [metric metric] [type { 1 2 }]</code>	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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.
3	<code>Raisecom(config-port)#ipv6 ospf hello-interval seconds [instance-id instance-id]</code>	Configure the interval for sending Hello packets on the OSPFv3 area interface. By default, the interval is 10s.
4	<code>Raisecom(config-port)#ipv6 ospf dead-interval seconds [instance-id instance-id]</code>	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	<code>Raisecom(config-port)#ipv6 ospf transmit-delay seconds [instance-id instance-id]</code>	Configure the transmission delay time of LSA on the OSPFv3 area interface. By default, it is 1s.

Step	Command	Description
6	Raisecom(config-port)# ipv6 ospf retransmit-interval <i>seconds</i> [instance-id <i>instance-id</i>]	Configure the interval for retransmitting the lost LSA packets on the OSPFv3 area interface. By default, it is 5s.

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 <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)# ipv6 ospf cost <i>value</i> [instance-id <i>instance-id</i>]	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 <i>value</i> [instance-id <i>instance-id</i>]	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 <i>process-id</i>	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)# distance <i>administrative-distance</i>	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.

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.
3	Raisecom(config-ospf6)#maximum load-balancing number	Configure the maximum number of IP ECMP paths supported by OSPFv3.

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 <i>acl-number</i> 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 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.

Step	Command	Description
3	Raisecom(config)# access-list <i>acl-number</i>	(Optional) create an ACL and enter ACL configuration mode. When the <i>acl-number</i> ranges from 7000 to 7999, the system will enter extended IPv6 ACL configuration mode.
	Raisecom(config-acl-ipv6-advanced)# rule [<i>rule-id</i>] { deny permit } { <i>protocol-id</i> ipv6 } { <i>source-ip-address/prefix-length</i> any } { <i>destination-ip-address/prefix-length</i> any } [dscp <i>dscp-value</i>]	(Optional) configure extended IPv6 ACL rules.
4	Raisecom(config)# ipv6 router ospf <i>process-id</i>	Start an OSPFv3 process and enter OSPFv3 configuration mode.
5	Raisecom(config-ospf6)# distribute-list { ipv6-access-list <i>acl-number</i> ipv6-prefix-list <i>list-name</i> } out [static connected bgp4+ ripng isisv6 <i>process-id</i>]	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 Type3 LSA filtering policy

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# ipv6 prefix-list <i>prefix-name</i> seq <i>seq-number</i> { deny permit } <i>ip-address/mask</i> [ge <i>min-length</i>] [le <i>max-length</i>]	(Optional) configure the address prefix list.
3	Raisecom(config)# ipv6 router ospf <i>process-id</i>	Start an OSPFv3 process and enter OSPFv3 configuration mode.

Step	Command	Description
4	<code>Raisecom(config-ospf6)#area { area-id ip-format-area-id } filter ipv6-prefix-list list-name { in out }</code>	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 Configuring OSPFv3 authentication policy

Configuring interface authentication policy

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.
3	<code>Raisecom(config-port)#ipv6 ospf ipsec policy policy-name [instance-id instance-id]</code>	Configure IPsec authentication policy on the OSPF interface. The priority of the interface authentication policy is higher than that of the process and area authentication policies. By default, the interface is not authenticated.

Configuring area IPsec authentication policy

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ipv6 router ospf process-id [vrf vrf-name]</code>	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	<code>Raisecom(config-ospf6)#area { area-id ip-format-area-id } ipsec policy policy-name</code>	Configure the IPsec authentication policy for OSPF areas. The parameters of the authentication policy must be valid so that the policy can be applied. The priority of the area authentication policy is higher than that of the process authentication policies. By default, the area is not authenticated.

8.5.10 Configuring BFD for OSPFv3

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ipv6 router ospf <i>process-id [router-id router-id]</i>	Enter OSPF configuration mode.
3	Raisecom((config-router-ospf))#bfd all-interfaces	Enable global BFD. By default, global BFD is not enabled.
4	Raisecom(config-router-ospf)#exit	Enter global configuration mode.
5	Raisecom(config)#interface <i>interface-</i> <i>type interface-number</i>	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 [<i>process-id</i>] [vrf <i>vrf-name</i>]	Show basic information about OSPFv3.
2	Raisecom#show ipv6 ospf [<i>process-id</i>] interface [<i>interface-type interface-number</i>]	Show information about the OSPFv3 interface.
3	Raisecom#show ipv6 ospf [<i>process-id</i>] neighbor [<i>neighbor-id</i>]	Show information about OSPFv3 neighbors.
4	Raisecom#show ipv6 ospf [<i>process-id</i>] 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 asbr	Show basic information about ASBR.
7	Raisecom#show ipv6 ospf [<i>process-id</i>] topology	Show information about the OSPFv3 topology.
8	Raisecom#show ipv6 ospf [<i>process-id</i>] vlink	Show information about OSPFv3 virtual links.

8.5.12 Maintenance

Command	Description
<code>Raisecom#clear ipv6 ospf [process-id] process [graceful]</code>	Restart the OSPFv3 process.
<code>Raisecom(config-ospf6)#ospf restart grace-period seconds</code>	Configure the graceful restart period of OSPFv3.
<code>Raisecom(config-ospf6)#capability restart { graceful signaling }</code>	Configure OSPFv3 GR. OSPFv3 GR can ensure that routers running OSPFv3 forward the service normally when the master/slave switchover starts or OSPFv3 restarts.
<code>Raisecom(config-ospf6)#ospf restart helper { never planned-only }</code>	Configure rules to enter help mode in OSPFv3 graceful restart mode.
<code>Raisecom(config-ospf6)#ospf restart helper [planned-only] max-grace-period seconds</code>	Configure the maximum restart period in OSPFv3 graceful restart help mode.

8.6 Configuring ISIS

8.6.1 Configuring ISIS basic function

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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router isis [area-tag] [vrf vrf-name]</code>	Start an ISIS process and enter ISIS configuration mode.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	(Optional) enter interface configuration mode.
4	<code>Raisecom(config-port)#ip router isis [area tag]</code> <code>Raisecom(config-port)#exit</code>	(Optional) start an ISIS process on the interface.
5	<code>Raisecom(config)#router isis [area-tag]</code>	Enter ISIS configuration mode.
6	<code>Raisecom(config-router-isis)#net network-entity</code>	Configure the network identifier entity of ISIS routing process.

8.6.2 Configuring ISIS routing

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.

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.

Step	Command	Description
6	Raisecom(config-port)# isis metric <i>metric [level-1 level-2]</i>	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 <i>[area-tag]</i>	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)# reference-bandwidth <i>bandwidth</i>	Configure reference rate referred to while calculating technical link overhead. By default, it is 100 Mbit/s.

Configuring ISIS administrative distance

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router isis <i>[area-tag]</i>	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)# distance <i>distance [ip-address mask-address]</i>	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 <i>interface-type interface-number</i>	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 <i>interface-type interface-number</i>	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:

- 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 <i>interface-type interface-number</i>	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 Holddown time. If the router cannot receive Hello packet sent by the peer router within the Holddown time, the peer router can be considered invalid. The Holddown time is configured based on interface and different router in the same area can set different the Holddown time.

By changing the time interval for sending Hello packet of ISIS or the invalid number of Hello packet, you can adjust the Holddown time.

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.

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 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 <i>interface-type</i> <i>interface-number</i>	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.
2	Raisecom(config)#router isis [<i>area-tag</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#hello padding	Enable Hello Packet padding. By default, all types of interface are padded with standard Hello packet.

8.6.5 Configure ISIS authentication

Configuring ISIS interface authentication

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#isis password { clear <i>password</i> md5 <i>password</i> } [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.

Step	Command	Description
2	Raisecom(config)# router isis [<i>area-tag</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)# area-password { <i>clear password</i> <i>md5 password</i> } [authenticate snp { <i>send-only</i> <i>validate</i> }]	Configure Level-1 area authentication.
4	Raisecom(config-router-isis)# domain-password { <i>clear password</i> <i>md5 password</i> } [authenticate snp { <i>send-only</i> <i>validate</i> }]	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 [<i>area-tag</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)# redistribute { connected static rip ospf process-id isis area-tag bgp } [route-map map-name] [level-1 level-2 level-1-2] [metric metric] [metric-type { external internal }]	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.

Configuring advertising default route

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router isis [<i>area-tag</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)# default-information originate	Configure advertising Level-2 default route.

Configuring ISIS route aggregation

Route aggregation can not only reduce the scale of routing table but also shrink the size of LSP packet generated by the local router and reduce the scale of LSDB.

- The aggregated route can be the route found by the ISIS and the route redistributed externally.
- The overload of aggregated route takes the minimum overload among all the routes aggregated.
- The router only aggregates the route generated in the local LSP.

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 aggregation among areas. By default, there is no route aggregation. The overload while configuring route aggregation is the maximum Metric in the LSA. And the route aggregation will be advertised.

Configuring ISIS equal-cost multi-path load balancing

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.

Step	Command	Description
4	Raisecom(config-router-isis)# distribute-list { ip access-list <i>acl-number</i> prefix-list <i>list-name</i> route-map <i>map-name</i> } 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 <i>interface-type</i> <i>interface-number</i>	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 [<i>area-tag</i>]	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.

8.6.8 Configuring ISIS GR

Configure ISIS graceful restart, that is, the switchover ensures no service interruption while the RAX711-C-R is rebooted.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router isis [<i>area-tag</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)# graceful-restart	Enable ISIS graceful restart. By default, it is disabled.
4	Raisecom(config-router-isis)# graceful-restart interval <i>seconds</i>	Enable the interval of ISIS graceful restart. By default, it is 300s.
5	Raisecom(config-router-isis)# graceful-restart sa enable	Enable ISIS graceful restart to restrain the neighbor device from advertising routes. By default, it is enabled.

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 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 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.
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

No.	Command	Description
1	Raisecom#clear isis process process-id [graceful-restart]	Clear ISIS.
2	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 [<i>area-tag</i>] [vrf <i>vrf-name</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
4	Raisecom(config-port)#ipv6 router isis [<i>area tag</i>] Raisecom(config-port)#exit	Enable ISISv6 capabilities on the interface. Establish ISIS neighbor relationship through the interface.
5	Raisecom(config)#router isis [<i>area-tag</i>]	Enter ISIS configuration mode.
6	Raisecom(config-router-isis)#net <i>network-entity</i>	Configure the network ID entity of the ISIS routing process.

Configuring 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 [<i>area-tag</i>] [vrf <i>vrf-name</i>]	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 [<i>area-tag</i>] [vrf <i>vrf-name</i>]	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 <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)# isis password { clear <i>password</i> md5 <i>password</i> } [level-1 level-2]	Configure the ISIS authentication mode and password of the interface.

Configuring area authentication

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router isis [<i>area-tag</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)# area-password { clear <i>password</i> md5 <i>password</i> } [authenticate snp { send-only validate }]	Configure Level-1 area authentication.
4	Raisecom(config-router-isis)# domain-password { clear <i>password</i> md5 <i>password</i> } [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.

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.

Step	Command	Description
3	<code>Raisecom(config-router-isis)#ipv6 distance distance [ip-address mask-address]</code>	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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router isis [area-tag]</code>	Start an ISIS process and enter ISIS configuration mode.
3	<code>Raisecom(config-router-isis)#ipv6 default-information originate</code>	Advertise Level-2 default routes.

Redistributing routes

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router isis [area-tag]</code>	Start an ISIS process and enter ISIS configuration mode.
3	<code>Raisecom(config-router-isis)#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]</code>	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.

Step	Command	Description
4	<code>Raisecom(config-router-isis)#ipv6 redistribute limit max-number [level-1 level-1-2 level-2]</code>	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	<code>Raisecom(config-router-isis)#redistribute isis ipv6 level-2 into level-1</code>	Configure routes in Level-2 area to be redistributed into Level-1 area. By default, the routing information in Level-2 area is not advertised to the Level-1 area.

Configuring ISISv6 route aggregation

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 aggregated route takes the minimum value of the cost of all aggregated routes.

The router only aggregates the routes in the locally generated LSP.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router isis [area-tag]</code>	Start an ISIS process and enter ISIS configuration mode.
3	<code>Raisecom(config-router-isis)#ipv6 summary-prefix ipv6-address/m [level-1 level-2 level-2-only]</code>	Configure IPv6 route aggregation. 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 [<i>area-tag</i>] [<i>vrf vrf-name</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#ipv6 distribute-list { ipv6-access-list <i>acl-number</i> ipv6-prefix-list <i>list-name</i> route-map <i>map-name</i> } out [connected static ripng ospfv3 <i>process-id</i> isisv6 <i>area-tag</i> 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 <i>acl-number</i> ipv6-prefix-list <i>list-name</i> route-map <i>map-name</i> } 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 [<i>area-tag</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#ipv6 maximum load-balancing <i>number</i>	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)#router isis [<i>area-tag</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#isis ipv6 bfd enable	Enable global ISISv6 BFD. By default, it is disabled.
4	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] [<i>interface-number</i>] [vrf <i>vrf-name</i>]	Show information about the ISIS interface.
2	Raisecom# show isis neighbor [<i>system-id</i> detail] [vrf <i>vrf-name</i>]	Show ISIS neighbor information.
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] [vrf <i>vrf-name</i>]	Show information about the ISIS topology.
5	Raisecom# show isis database [local] [level-1 level-2] [<i>lsp-id</i>] [detail] [vrf <i>vrf-name</i>]	Show ISIS link status database.
6	Raisecom# show isis summary	Show ISIS basic configurations.

8.7.8 Maintenance

Command	Description
Raisecom# clear isis process <i>process-id</i> [graceful-restart] [vrf <i>vrf-name</i>]	Clear ISISv6 information.
Raisecom# clear isis neighbor [<i>system-id</i>] [vrf <i>vrf-name</i>]	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 <i>as-id</i>	Enable BGP and create a BGP instance. Enter BGP configuration mode.
3	Raisecom(config-router)# bgp router-id <i>router-id</i>	(Optional) configure the BGP Router ID. By default, the BGP Router ID is the same as the global Router ID of the router.

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 neighborhood. To enhance stability of the BGP connection, we recommend using the loopback interface address to establish the connection.

Specified IP addresses of BGP neighbors are divided into 2 types:

- Interface IP address of the directly-connected BGP neighbor
- Loopback interface address of the BGP neighbor, where the route can reach. In this mode, you need to configure the route update source to ensure that the BGP neighbor is established properly.

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.

Step	Command	Description
8	<code>Raisecom(config-router)#neighbor ip-address description string</code>	(Optional) configure descriptions of the BGP neighbor. By default, there is no description of the BGP neighbor.
9	<code>Raisecom(config-router)#neighbor ip-address next-hop-self</code>	(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.
10	<code>Raisecom(config-router)#bgp log-neighbor-changes</code>	(Optional) enable the log which is used to inform the BGP neighbor of state change. By default, it is enabled.
11	<code>Raisecom(config-router)#neighbor ip-address shutdown</code>	(Optional) disallow the RAX711-C-R to establish the BGP connection with the specified BGP neighbor. By default, establishing the BGP connection with the BGP neighbor is allowed.
12	<code>Raisecom(config-router)#neighbor ip-address ebgp-multihop [ttl]</code>	(Optional) allow the RAX711-C-R to establish the EBGp connection with BGP neighbors in the indirectly-connected network. In addition, specify the maximum hops allowable for the specified EBGp connection. By default, only physically directly-connected BGP neighbors can establish the EBGp connection.
13	<code>Raisecom(config-router)#bgp redistribute-internal</code>	(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	<code>Raisecom(config-router)#bgp enforce-first-as</code>	Enforce the first AS number in the AS path received from an EBGp peer to be the AS where the EBGp peer is located.

Configuring BGP peer (IPv4 based on VPN instance)

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp as-id</code>	Enable BGP and create a BGP instance, and enter BGP configuration mode.
3	<code>Raisecom(config-router)#address-family ipv4 vrf vrf-name</code>	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	<code>Raisecom(config-router-af)#neighbor ip-address remote-as as-id</code>	Create the MP-BGP peer and specify the peer AS ID.

Step	Command	Description
5	<code>Raisecom(config-router-af)#neighbor ip-address activate</code>	Enable the exchange of routing information of the specified IPv6 address family between BGP peers.
6	<code>Raisecom(config-router-af)#neighbor ip-address1 update-source ipv6-address2</code> <code>Raisecom(config-router-af)#neighbor ip-address update-source interface-type interface-number</code>	Use 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 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	<code>Raisecom(config-router-af)#neighbor ip-address weight weight</code>	(Optional) configure the weight of routes learned from BGP peers. By default, the weight of routes learned from BGP peers is 0.
8	<code>Raisecom(config-router-af)#neighbor ip-address default-originate [route-map route-map-name]</code>	(Optional) enable the function of sending the default route to the peer. By default, no default route is sent to the peer.
9	<code>Raisecom(config-router-af)#neighbor ip-address next-hop-self</code>	(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	<code>Raisecom(config-router-af)#neighbor ip-address ebgp-multihop [ttl]</code>	(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	<code>Raisecom(config-router-af)#bgp log-neighbor-changes</code>	(Optional) enable logging for prompting the status change of BGP peers. By default, it is enabled.

Step	Command	Description
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.
2	Raisecom(config)# router bgp as-id	Enable BGP and 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 number 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.

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.

Step	Command	Description
3	Raisecom(config-router)# network <i>ip-address</i> [<i>mask-address</i>] [route-map <i>route-map-name</i>]	Inject static routes into the BGP routing table and advertise them to other ASs or local AS peers.

BGP redistributed routes(VPN-based IPv4)

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router bgp <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)# address-family ipv4 vrf <i>vrf-name</i>	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)# network <i>ip-address</i> [<i>mask-address</i>] [route-map <i>route-map-name</i>]	Inject static routes into the BGP routing table and advertise them to other ASs or local AS peers.

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 <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)# default-information originate	Configure the BGP to redistribute the default route.

Redistributing default route (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router bgp <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)# address-family ipv4 vrf <i>vrf-name</i>	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 <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)#redistribute { connected static rip ospf <i>process-id</i> isis <i>process-id</i> } [metric <i>metric</i>] [route-map <i>map</i>]	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 <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)#address-family ipv4 vrf <i>vrf-name</i>	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router)#redistribute { connected static rip ospf <i>process-id</i> isis <i>process-id</i> } [metric <i>metric</i>] [route-map <i>map</i>]	Configure BGP to redistribute routes of other protocols through re-advertising.

8.8.4 Configuring BGP routing

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 <i>as-id</i>	Enter BGP configuration mode.

Step	Command	Description
3	<code>Raisecom(config-router)#distance bgp ebgp distance1 ibgp distance2 local distance3</code>	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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp as-id</code>	Enter BGP configuration mode.
3	<code>Raisecom(config-router)#address-family ipv4 vrf vrf-name</code>	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	<code>Raisecom(config-router-af)#distance bgp ebgp distance1 ibgp distance2 local distance3</code>	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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp as-id</code>	Enter BGP configuration mode.
3	<code>Raisecom(config-router)#bgp deterministic-med</code>	(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	<code>Raisecom(config-router)#bgp always-compare-med</code>	Configure the BGP to compare the MED for all paths.
5	<code>Raisecom(config-router)#bgp bestpath compare-routerid</code>	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.

Step	Command	Description
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.
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 aggregated 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.
2	Raisecom(config)#router bgp <i>as-id</i>	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 <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)#bgp dampening <i>half-life reuse suppress max-suppress-time</i>	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	Enable the BGP-enabled device to send standard community attribute to the peer.

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.



Note

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.
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.

Configuring route reflector (VPNv4)

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 vpnv4	Enter BGP VPNv4 address family configuration mode.
4	Raisecom(config-router-af)#neighbor ip-address route-reflector-client	Configure the local device as the route reflector and configure the specified 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.

Step	Command	Description
3	Raisecom(config-router)#bgp default local-preference <i>priority</i>	Configure BGP default local priority. By default, it is 100.

Configuring BGP timer

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router bgp <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)#bgp scan-time <i>time</i>	Configure the interval for scanning the BGP routing table. By default, it is 60s.
4	Raisecom(config-router)#timers bgp keep-alive-time <i>hold-time</i>	Configure the live and hold time of the global BGP connection. By default, the live and hold time of the global BGP connection are configured to 60s and 180s respectively.
5	Raisecom(config-router)#neighbor <i>ip-address</i> timers keep-alive-time <i>hold-time</i>	Configure the live and hold time of the neighbor. By default, the live and hold time of the neighbor are identical to the ones of the global BGP connection.

Configuring BGP route aggregation

- At present, the RAX711-C-R supports BGP manual aggregation. Manual aggregation is only valid for existing routes in the BGP local routing table. If there is no route, whose mask size is greater than 16 bytes, in the BGP routing table, the BGP will not release the aggregated route even you use the aggregate 10.1.1.1 255.255.0.0 command to aggregate the route.
- The aggregated route cannot be set to the default route (0.0.0.0/0).

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router bgp <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)#aggregate-address <i>ip-address mask-address</i>	Configure BGP route aggregation and release the aggregated route and detail route.
4	Raisecom(config-router)#aggregate-address <i>ip-address mask-address summary-only</i>	Configure BGP route aggregation, release the aggregated route only and dampens the detail route.
5	Raisecom(config-router)#aggregate-address <i>ip-address mask-address as-set</i>	Configure BGP route aggregation and set the AS_SET option. The generated aggregated route includes all AS IDs in the AS_PATH and takes them as an AS_SET to prevent the route loop.

Configuring BGP route aggregation (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#router bgp <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)#address-family <i>ipv4 vrf vrf-name</i>	Enter IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#aggregate-address <i>ip-address mask-address</i>	Configure BGP route aggregation and advertise aggregated routes and detailed routes.
5	Raisecom(config-router-af)#aggregate-address <i>ip-address mask-address summary-only</i>	Configure BGP route aggregation. Advertise aggregated routes but suppress detailed routes.
6	Raisecom(config-router-af)#aggregate-address <i>ip-address mask-address as-set</i>	Configure BGP route aggregation and configure the AS_SET option. The generated aggregated route includes all AS numbers 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 <i>access-list-number</i> { permit deny } <i>regex</i>	Configure the filter of the AS_PATH list.
3	Raisecom(config)#router bgp [<i>as-id</i>]	Enter BGP configuration mode.
4	Raisecom(config-router)#neighbor <i>ip-address</i> filter-list <i>access-list-number</i> { 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 <i>ip-address</i> route-map <i>map-name</i> { in out }	Apply the routing policy to the specified neighbor to filter or release the route.
6	Raisecom(config-router)#neighbor <i>ip-address</i> prefix-list <i>prefix-list-name</i> { in out }	Configure the specified neighbor to filter received or released 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.

Step	Command	Description
2	<code>Raisecom(config)#ip as-path access-list access-list-number { permint deny } regexp</code>	Configure the filter of AS path list.
3	<code>Raisecom(config)#router bgp [as-id]</code>	Enter BGP configuration mode.
4	<code>Raisecom(config-router)#address-family ipv4 vrf vrf-name</code>	Enter IPv4 address family configuration mode of the BGP VPN instance.
5	<code>Raisecom(config-router-af)#neighbor ip- address filter-list access-list-number { in out }</code>	Configure the BGP route filtering policy based on AS path list.
6	<code>Raisecom(config-router-af)#neighbor ip- address route-map map-name { in out }</code>	Apply the routing policy to a specified peer to filter the received or advertised routes.
7	<code>Raisecom(config-router-af)#neighbor ip- address prefix-list prefix-list-name { in out }</code>	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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip as-path access-list access-list-number { permint deny } regexp</code>	Configure the filter of AS path list.
3	<code>Raisecom(config)#router bgp [as-id]</code>	Enter BGP configuration mode.
4	<code>Raisecom(config-router)#address-family vpnv4</code>	Enter BGP VPNv4 address family configuration mode.
5	<code>Raisecom(config-router-af)#neighbor ip- address filter-list access-list-number { in out }</code>	Configure the BGP route filtering policy based on AS path list.
6	<code>Raisecom(config-router-af)#neighbor ip- address route-map map-name { in out }</code>	Apply the routing policy to a specified peer to filter the received or advertised routes.
7	<code>Raisecom(config-router-af)#neighbor ip- address prefix-list prefix-list-name { in out }</code>	Configure a specified peer to filter the received or advertised routes based on IP prefix list.

8.8.6 Configuring BFD for BGP

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

Step	Command	Description
2	Raisecom(config)# router bgp <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)# neighbor <i>ip-address</i> 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 <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)# address-family ipv4 vrf <i>vrf-name</i>	Enter IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)# neighbor <i>ip-address</i> fall-over bfd	Enable BFD for peer BGP connections. By default, it is disabled.

8.8.7 Configuring BGP authentication

Configuring BGP authentication

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router bgp <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)# neighbor <i>ip-address</i> password <i>password</i>	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 <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)# address-family ipv4 vrf <i>vrf-name</i>	Enter IPv4 address family configuration mode of the BGP VPN instance.

Step	Command	Description
4	<code>Raisecom(config-router-af)#neighbor ip-address password password</code>	Enable MD5 authentication on BGP messages when the BGP peer establishes TCP connections. By default, it is disabled.

8.8.8 Checking configurations

No.	Command	Description
1	<code>Raisecom#show ip bgp</code>	Show contents of the local BGP routing table.
2	<code>Raisecom#show ip bgp ip-address [ip-mask]</code>	Show information about the specified network in the local BGP routing table.
3	<code>Raisecom#show ip bgp dampening dampened-paths</code>	Show information about the dampened routes.
4	<code>Raisecom#show ip bgp dampening parameters</code>	Show route dampening parameters.
5	<code>Raisecom#show ip bgp dampening flap-statistics</code>	Show route flapping statistics.
6	<code>Raisecom#show ip bgp summary</code>	Show summary of the BGP peer.
7	<code>Raisecom#show ip bgp neighbors [ip-address]</code>	Show detailed status of the BGP peer.
8	<code>Raisecom#show ip bgp vpnv4 { all rd rd vrf vrf-name }</code>	Show routing information about all or the specified BGP VPNv4.
9	<code>Raisecom#show ip bgp vpnv4 { all vrf vrf-name } ip-address [mask-address]</code>	Show routing information in the specified network segment of the BGP VPNv4 address family.
10	<code>Raisecom#show ip bgp vpnv4 { all vrf vrf-name } summary</code>	Show summary routing information about the BGP VPNv4 address family.
11	<code>Raisecom#show ip bgp vpnv4 { all vrf vrf-name } neighbors router-id [routes]</code>	Show routing information about the specified BGP VPNv4 peer.
12	<code>Raisecom#show ip bgp vpnv4 all labels</code>	Show label information about the BGP VPNv4 route prefix.

8.8.9 Maintenance

Command	Description
<code>Raisecom#clear ip bgp dampening [network-address [network-mask]]</code>	Clear information about routing attenuation.

Command	Description
Rasiecom#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.
Rasiecom#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.
Rasiecom#clear ip bgp internal [ipv4 unicast ipv6 unicast vpnv4 unicast]	Hard reset all or specified IBGP connections, and the connection is interrupted.
Rasiecom#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.
Rasiecom#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.
Rasiecom#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.
Rasiecom#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.
Rasiecom#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.
Rasiecom#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.
Rasiecom#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.
Rasiecom#clear ip bgp ipv6 unicast ipv6-address	Hard reset the BGP connection with the specified IPv6 address, and the connection is interrupted.

Command	Description
<code>Raisecom#clear ip bgp ipv6 unicast <i>ipv6-address</i> { in out soft }</code>	Soft reset the BGP connection of the specified IPv6 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp <i>as-id</i></code>	Enable BGP and create a BGP instance. Enter BGP configuration mode.
3	<code>Raisecom(config-router)#bgp router-id <i>router-id</i></code>	(Optional) configure BGP Router ID. By default, the BGP Router ID is the same as the global Router ID of the router.

Configuring BGP+ peer

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp <i>as-id</i></code>	Enable BGP and create a BGP instance. Enter BGP configuration mode.
3	<code>Raisecom(config-router)#address-family ipv6</code>	Enter BGP IPv6 address family configuration mode.
4	<code>Raisecom(config-router-af)#neighbor <i>ipv6-address</i> remote-as <i>as-id</i></code>	Create a BGP peer and specify the AS ID of the peer.
5	<code>Raisecom(config-router-af)#neighbor <i>ipv6-address1</i> update-source <i>ipv6-address2</i></code>	Use the specified source IPv6 address or local source interface when establishing a BGP

Step	Command	Description
	<code>Raisecom(config-router-af)#neighbor ipv6-address update-source interface- type interface-number</code>	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	<code>Raisecom(config-router-af)#neighbor ipv6-address weight weight</code>	(Optional) configure the weight of routes learned from BGP peers. By default, the weight of routes learned from BGP peers is 0.
7	<code>Raisecom(config-router-af)#neighbor ipv6-address default-originate [route- map route-map-name]</code>	(Optional) enable the function of sending the default route to the peer. By default, no default route is sent to the peer.
8	<code>Raisecom(config-router-af)#neighbor ipv6-address next-hop-self</code>	(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	<code>Raisecom(config-router-af)#neighbor ipv6-address ebgp-multihop [tt1]</code>	(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	<code>Raisecom(config-router-af)#neighbor ipv6-address route-update-interval second</code>	(Optional) configure the interval for sending packets with the same route prefix to the peer.

8.9.2 Configuring BGP4+ advertised routes

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp as-id</code>	Enter BGP configuration mode.
3	<code>Raisecom(config-router)#address-family ipv6</code>	Enter BGP IPv6 address family configuration mode.

Step	Command	Description
4	<code>Raisecom(config-router-af)#network ipv6-address [route-map route-map- name]</code>	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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp as-id</code>	Enter BGP configuration mode.
3	<code>Raisecom(config-router)#address-family ipv6</code>	Enter BGP IPv6 address family configuration mode.
4	<code>Raisecom(config-router-af)#default-information originate</code>	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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp as-id</code>	Enter BGP configuration mode.
3	<code>Raisecom(config-router)#address-family ipv6</code>	Enter BGP IPv6 address family configuration mode.
4	<code>Raisecom(config-router-af)#redistribute { connected static ripng ospfv3 1 isisv6 process-id } [metric metric] [route-map map]</code>	Configure BGP to redistribute routes of other protocols into the BGP routing table through re-advertising.

8.9.4 Configuring BGP4+ route attributes

Configuring BGP4+ administrative distance

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp as-id</code>	Enter BGP configuration mode.

Step	Command	Description
3	Raisecom(config-router)#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 aggregated 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.

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 aggregation

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 aggregation, and advertise aggregated routes and detailed routes.
5	Raisecom(config-router-af)#aggregate-address ipv6-address/prefix-length summary-only	Configure BGP route aggregation and only advertise aggregated routes to suppress detailed routes.
6	Raisecom(config-router-af)#aggregate-address ipv6-address/prefix-length as-set	Configure BGP route aggregation and set the AS_SET option so that the aggregated 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.

Step	Command	Description
3	Raisecom(config-router)#address-family ipv6	Enter BGP IPv6 address family configuration mode.
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 { permint 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.

Step	Command	Description
7	<code>Raisecom(config-router-af)#neighbor ipv6-address prefix-list prefix-list-name { in out }</code>	Configure the specified peer to filter the received or advertised routes based on IP prefix list.

8.9.6 Configuring BGP4+ authentication

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router bgp as-id</code>	Enter BGP configuration mode.
3	<code>Raisecom(config-router)#address-family ipv6</code>	Enter BGP IPv6 address family configuration mode.
4	<code>Raisecom(config-router-af)#neighbor ipv6-address password password</code>	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	<code>Raisecom#show ip bgp ipv6 unicast summary</code>	Show summary information about IPv6 BGP peers.
23	<code>Raisecom#show ip bgp ipv6 unicast neighbors [ipv6-address]</code>	Show the status information about IPv6 BGP peers.
3	<code>Raisecom#show ip bgp ipv6 unicast dampening dampened-paths</code>	Show suppressed routing information in the IPv6 unicast routing table.
4	<code>Raisecom#show ip bgp ipv6 unicast dampening flap-statistics</code>	Show the statistics of route flapping in the IPv6 unicast routing table.
5	<code>Raisecom#show ip bgp ipv6 unicast [ipv6-address ipv6-address/prefix-length]</code>	Show information about the specified network in the BGP routing table.

8.9.8 Maintenance

For BGP4+ maintenance commands, refer to section 8.8.9 Maintenance.

8.10 Configuring RIP

8.10.1 Configuring basic RIP 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.
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 RAX711-C-R. 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.
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 area-tag 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 invalid-time holddown-time flush-time	Configure the RIP timer. By default, the update interval is 30s. The invalid interval is 180s. The suppression interval is 120s. The refreshing interval is 120s.

8.10.5 Configuring loop suppression

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



Note

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 <i>interface-type interface-number</i>	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 RIP packets on the interface is no authentication.
4	Raisecom(config-port)#ip rip authentication string <i>password-string</i>	Configure the interface-associated password.
5	Raisecom(config-port)#ip rip authentication key-chain <i>key-chain-name</i>	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.

Step	Command	Description
3	<code>Raisecom(config-rip)#distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> route-map <i>rmap-name</i> } in [<i>interface-type interface-number</i>]</code>	Configure RIP ingress routing policy.
4	<code>Raisecom(config-rip)#distribute-list { ip-access-list <i>acl-number</i> prefix-list <i>list-name</i> route-map <i>rmap-name</i> } out [<i>interface-type interface-number</i>]</code>	Configure RIP egress routing policy.
5	<code>Raisecom(config-rip)#distribute-list gateway <i>list-name</i> in [<i>interface-type interface-number</i>]</code>	Execute routing policies on the source address of the received packets through RIP.

8.10.8 Configuring route calculation

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router rip</code>	Enable RIP, and enter RIP configuration mode.
3	<code>Raisecom(config-rip)#distance <i>distance-value</i> [<i>ip-address wild-card-mask</i>]</code>	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	<code>Raisecom(config-rip)#maximum load-balancing <i>number</i></code>	Configure the maximum number of IP equal-cost multi-path load balancing paths.

8.10.9 Checking configurations

No.	Command	Description
1	<code>Raisecom#show ip rip</code>	Show basic information about RIP.
2	<code>Raisecom#show ip rip database</code>	Show information about RIP routing database.
3	<code>Raisecom#show ip rip interface [<i>interface-type interface-number</i>]</code>	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.
2	Raisecom(config)#router ripng	Start the RIPng process and enter RIPng configuration mode.
3	Raisecom(config-ripng)#network interface-type interface-number	Configure the network where RIPng direct connection is valid.
4	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.
5	Raisecom(config)#interface interface- type interface-number	Enter interface configuration mode.
6	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 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.

Step	Command	Description
3	<code>Raisecom(config-ripng)#redistribute { static connected isisv6 area-tag bgp4+ ospfv3 process-id } [metric metric] [route-map map-name] [tag tag-value]</code>	Configure the RIPng route redistributing policy.
4	<code>Raisecom(config-ripng)#default-metric metric</code>	Configure the default metric for the redistributed external routes. By default, the metric of the redistributed external routes is 1.

Configuring broadcast default route

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ripng</code>	Start the RIPng process and enter RIPng configuration mode.
3	<code>Raisecom(config-ripng)#default-information originate</code> <code>Raisecom(config-ripng)#exit</code>	Enable broadcast default route. By default, it is disabled.

Advertising aggregated routes

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
4	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.
5	<code>Raisecom(config-port)#ipv6 ripng summary-address ipv6-address/m</code>	Advertise the aggregated IPv6 prefix information on the interface.

8.11.3 Configuring timer

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ripng</code>	Start the RIPng process and enter RIPng configuration mode.
3	<code>Raisecom(config-ripng)#timers basic update-time invalid-time holddown-time flush-time</code>	Configure the RIPng timer. By default, the update interval is 30s, the failure interval is 180s, the suppression interval is 120s, and the refresh interval is 120s.

8.11.4 Configuring loop suppression

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-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 set to 16, which is unreachable. By default, poison reverse is disabled.



Note

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 <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#ipv6 ripng ipsec policy <i>policy-name</i> 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 <i>policy-name</i>	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.

Step	Command	Description
3	Raisecom(config-ripng)# distribute-list { ipv6-access-list <i>acl-number</i> prefix-list <i>list-name</i> route-map <i>rmap-name</i> } in [<i>interface-type interface-number</i>]	Configure the routing policy of RIPng in the ingress direction.
4	Raisecom(config-ripng)# distribute-list { ipv6-access-list <i>acl-number</i> prefix-list <i>list-name</i> route-map <i>rmap-name</i> } out [<i>interface-type interface-number</i>]	Configure the routing policy of RIPng in the egress direction.

8.11.7 Configuring route calculation

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)# distance <i>distance-value</i>	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 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 [<i>interface-type interface-number</i>]	Show configurations and status of the interface running RIPng.

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

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 function, 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.
3	Raisecom(config)#mpls enable	Enable global MPLS function.

Step	Command	Description
4	<code>Raisecom(config)#mpls label-advertise { implicit-null non-null explicit-null }</code>	(Optional) configure the label distribution mode for the last but one hop.

9.1.3 Checking configurations

Step	Command	Description
1	<code>Raisecom#show mpls</code>	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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface tunnel interface-number</code>	Enter Tunnel interface configuration mode.
3	<code>Raisecom(config-tunnelif)#tunnel mode { gre mpls ipv4-ipv6 [ds-lite] ipv6-ipv4 [6rd 6to4] vxlan }</code>	Configure the Tunnel mode.
4	<code>Raisecom(config-tunnelif)#description description</code>	(Optional) configure descriptions of the Tunnel interface.
5	<code>Raisecom(config-tunnelif)#mtu mtu-value</code>	Configure the Tunnel MTU.
6	<code>Raisecom(config-tunnelif)#statistics enable</code>	(Optional) configure Tunnel statistics.
7	<code>Raisecom(config-tunnelif)#traffic-statistics enable</code>	(Optional) enable Tunnel traffic statistics.

Configuring Tunnel destination IPv4 address

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

Step	Command	Description
3	Raisecom(config-tunnelif)# ip address <i>ip-address</i> [sub]	Configure the destination IPv4 address of the Tunnel interface.

Configuring Tunnel destination IPv6 address

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface tunnel <i>interface-number</i>	Enter Tunnel interface configuration mode.
3	Raisecom(config-tunnelif)# ipv6 address <i>ipv6-address/m</i> [eui-64]	Configure the destination IPv6 address of the Tunnel interface.
	Raisecom(config-tunnelif)# ipv6 address <i>ipv6-address/m</i> anycast	

Configuring Tunnel type

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface tunnel <i>interface-number</i>	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 }	Configure the protocol type of the Tunnel interface. By default, it is static.
5	Raisecom(config-tunnelif)# mpls tunnel- id <i>tunnel-id</i>	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)# mpls te hot- standby wtr <i>wtr-time</i>	(Optional) configure the WTR time of the Tunnel interface hot backup. By default, the WTR time is 10s.

9.2.2 Configuring MPLS Tunnel policy

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#tunnel-policy <i>policy-name</i>	Enter Tunnel policy configuration mode.
3	Raisecom(config-tunnelpolicy)#tunnel select-seq { lsp [cr-lsp] cr-lsp [lsp] gre } Raisecom(config-tunnelpolicy)#tunnel select-seq lsp [cr-lsp] [load-balance-number <i>number</i>]	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.

9.2.3 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.

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 node.

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 <i>lsp-name dest-network mask nexthop ip-address out-label out-label lsr-id egress-lsr-id tunnel-id tunnel-id</i>	Configure the static unidirectional LSP Ingress node.
3	Raisecom(config)#mpls static-lsp transit <i>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</i>	Configure the static unidirectional LSP Transit node.
4	Raisecom(config)#mpls static-lsp egress <i>lsp-name in-label in-label lsr-id ingress-lsr-id tunnel-id tunnel-id</i>	Configure the static unidirectional LSP Egress node.
5	Raisecom(config)#mpls static-lsp egress <i>lsp-name</i> diffserv-mode { pipe uniform [exp-to-local-priority <i>profile-number</i>] }	(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 <i>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</i>	Configure the static unidirectional LSP Ingress node.
3	Raisecom(config)#mpls static-lsp transit <i>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</i>	Configure the static unidirectional LSP Transit node.
4	Raisecom(config)#mpls static-lsp egress <i>lsp-name in-label in-label lsr-id ingress-lsr-id tunnel-id tunnel-id</i>	Configure the static unidirectional LSP Egress node.
5	Raisecom(config)#mpls static-lsp egress <i>lsp-name</i> diffserv-mode { pipe uniform [exp-to-local-priority <i>profile-number</i>] }	(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 <i>lsp-name lsr-id egress-lsr-id tunnel-id tunnel-id</i>	Create the static bidirectional corouted LSP and enter Ingress LSP (ILSP) configuration mode.
3	Raisecom(config-ingress-lsp)#forward <i>dest-network mask nexthop ip-address out-label out-label</i>	Configure the next hop of the ingress node (with IP capability) forward LSP.
	Raisecom(config-ingress-lsp)#forward <i>dest-network [mask] nexthop-mac mac-address interface-type interface-number out-label out-label</i>	Configure the next hop of the ingress node (without IP capability) forward LSP.
4	Raisecom(config-ingress-lsp)#backward <i>in-label in-label</i>	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 <i>lsp-name lsr-id ingress-lsr-id egress-lsr-id tunnel-id tunnel-id</i>	Create the static bidirectional corouted LSP and enter TLSP configuration mode.
3	Raisecom(config-transit-lsp)#forward <i>in-label in-label nexthop ip-address out-label out-label</i>	Configure the next hop of the Transit node forward LSP.
4	Raisecom(config-transit-lsp)#backward <i>in-label in-label nexthop ip-address out-label out-label</i>	Configure the incoming label 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 <i>lsp-name lsr-id ingress-lsr-id tunnel-id tunnel-id</i>	Create the static bidirectional corouted LSP and enter ELSP (ELSP) configuration mode.

Step	Command	Description
3	<code>Raisecom(config-egress-lsp)#forward in-label in-label</code>	Configure the incoming label of the Egress node forward LSP.
4	<code>Raisecom(config-ingress-lsp)#backward dest-network mask nexthop ip-address out-label out-label</code>	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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mpls bidirectional static-lsp ingress lsp-name lsr-id egress-lsr-id tunnel-id tunnel-id</code>	Create the static bidirectional corouted LSP and enter ILSP configuration mode.
3	<code>Raisecom(config-ingress-lsp)#forward dest-network [mask] nexthop-mac mac-address interface-type interface-number out-label out-label</code>	Configure the next hop of the Ingress node forward LSP.
4	<code>Raisecom(config-ingress-lsp)#backward in-label in-label</code>	Configure the incoming label of the Ingress node backward LSP.

Configuring static bidirectional LSP Transit node

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mpls bidirectional static-lsp transit lsp-name lsr-id ingress-lsr-id egress-lsr-id tunnel-id tunnel-id</code>	Create the static bidirectional corouted LSP and enter Transit LSP (TLSP) configuration mode.
3	<code>Raisecom(config-transit-lsp)#forward in-label in-label nexthop-mac mac-address interface-type interface-number out-label out-label</code>	Configure the next hop of the Transit node forward LSP.
4	<code>Raisecom(config-transit-lsp)#backward in-label in-label nexthop-mac mac-address interface-type interface-number out-label out-label</code>	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 <i>lsp-name lsr-id ingress-lsr-id tunnel-id tunnel-id</i>	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 <i>dest-network</i> <i>[mask] nexthop-mac mac-address interface-type</i> <i>interface-number out-label out-label</i>	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 <i>[lsp-name]</i>	Show static bidirectional LSP configurations.
3	Raisecom#show mpls static-lsp <i>[lsp-name]</i> Raisecom#show mpls static-lsp <i>[egress ingress</i> <i> transit]</i>	Show static unidirectional LSP configurations.
4	Raisecom#show mpls lsp static <i>[ingress transit</i> <i> egress]</i>	Show configurations of static LSP.

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.
4	Raisecom(config)#mpls label-advertise { implicit-null non-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 <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#mpls ldp	Enable LDP on the interface.
4	Raisecom(config-port)#mpls ldp transport-address <i>interface</i>	(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 <i>hello-time</i>	(Optional) configure the Hello-hold timer of the LDP remote session. By default, the Hello-hold timer of the LDP remote session is 45s.
6	Raisecom(config-port)#mpls ldp timer keepalive-hold <i>keepalive-time</i>	(Optional) configure the Keepalive-hold timer of the LDP remote session. By default, the Keepalive-hold timer of the LDP remote session is 45s.

9.4.4 Configuring LDP remote session

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mpls ldp targeted neighbour <i>ip-address</i>	Enable LDP remote discovery and enter remote neighbor configuration mode.

Step	Command	Description
3	<code>Raisecom(config-ldp-remote-peer)#mpls ldp timer hello-hold <i>hello-time</i></code>	Configure the Hello-hold timer of the LDP remote session. By default, the Hello-hold timer of the LDP remote session is 45s.
4	<code>Raisecom(config-ldp-remote-peer)#mpls ldp timer keepalive-hold <i>keepalive-time</i></code>	Configure the Keepalive-hold timer of the LDP remote session. By default, the Hello-hold timer of the LDP remote session is 45s.

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 iTN8800 as below. Step 2 and step 3 can implement different encryption functions respectively. Choose one as required.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mpls ldp md5-password plain <i>peer-ip-address password</i></code>	Configure LDP MD5 cleartext password. Use the show running-config command to show the cleartext password.
3	<code>Raisecom(config)#mpls ldp md5-password cipher <i>peer-ip-address [encrpty] password</i></code>	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 BFD for TLDP

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mpls ldp targeted neighbour <i>ip-address</i></code>	Enable LDP remote discovery and enter remote symmetric configuration mode.
3	<code>Raisecom(config-ldp-remote-peer)#mpls ldp bfd enable</code>	Enable BFD for TLDP.

9.4.7 Configuring LDP FRR

Automatic LDP FRR

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	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 <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#mpls ldp frr nexthop <i>nexthop-address</i>	Enable LDP FRR and specify the IP address of the next hop. By default, LDP FRR is disabled.

9.4.8 Checking configurations

No.	Command	Description
1	Raisecom#show mpls ldp	Show LDP global information.
2	Raisecom#show mpls ldp history [<i>ip-address</i>]	Show LDP history information.
3	Raisecom#show mpls ldp interface [<i>interface-type interface-number</i>] [detail]	Show LDP interface information.
4	Raisecom#show mpls ldp targeted neighbour <i>ip-address</i>	Show remote neighbor information.
5	Raisecom#show mpls ldp session [detail] [peer <i>peer-address</i>]	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 <i>peer-address</i>]	Show LDP adjacency information.
9	Raisecom#show mpls ldp lsp record [<i>ip-address</i>] [detail] [{ libra1 lsp }]	Show details about LDP LSP.
10	Raisecom#show mpls ldp lsp record last <i>number</i> [detail]	Show LDP LSP records.

No.	Command	Description
11	Raisecom#show mpls ldp policy [{ inbound outbound }] [{ peer-id <i>ip-address</i> peer-group <i>group-name</i> }]	Show LDP strategies.
12	Raisecom#show mpls lsp [ldp] [ingress transit egress]	Show master or backup LSP configurations.
13	Raisecom#show mpls ldp lsp record [<i>ip-address</i>] [detail] [{ libra1 lsp }]	Show details about LDP LSP.

9.4.9 Maintenance

Command	Description
Raisecom#clear mpls ldp lsp record	Clear LDP LSP records.
Raisecom#mpls ldp graceful-restart	Configure LDP LSP graceful restart.

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.

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.
5	Raisecom(config-port)#mpls rsvp-te authentication window-size size-value	Configure the RSVP-TE authentication window.

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.

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.
3	Raisecom(config)# router ospf <i>process-id</i> [vrf <i>vrf-name</i>] [router-id <i>router-id</i>]	Start an OSPF process and enter OSPF configuration mode.
4	Raisecom(config-router-ospf)# capability opaque	Enable OSPF opaque LSA. By default, it is disabled.
5	Raisecom(config-router-ospf)# mpls traffic-eng area <i>area-id</i>	Enable OSPF TE. By default, it is disabled.
6	Raisecom(config-router-ospf)# mpls traffic-eng router-id <i>router-id</i>	Configure the ID of the MPLS-TE router.

Configuring OSPF TE

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# router ospf <i>process-id</i> [vrf <i>vrf-name</i>] [router-id <i>router-id</i>]	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 <i>area-id</i>	Enable TE for the OSPF area. By default, it is not enabled.
5	Raisecom(config-router-ospf)# mpls traffic-eng router-id <i>router-id</i>	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 <i>area-tag</i> [vrf <i>vrf-name</i>]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)# mpls traffic-eng { level-1 level-2 }	Enable TE for the ISIS area.

Step	Command	Description
4	Raisecom(config-router-isis)#mpls traffic-eng router-id <i>router-id</i>	Configure the Router ID of the MPLS-TE router.

9.5.5 Configuring explicit path and Tunnel

step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mpls explicit-path <i>path-name</i>	Create MPLS-TE explicit path and enter explicit path configuration mode.
3	Raisecom(config-mpls-exp-path)#next-hop <i>ip-address</i> { 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 <i>interface-number</i>	Enter tunnel interface configuration mode.
5	Raisecom(config-tunnel)#description <i>description</i>	(Optional) configure the description information about Tunnel interface.
6	Raisecom(config-tunnel)#ip address <i>ip-address</i> [sub]	Configure the destination IP address on the Tunnel interface.
7	Raisecom(config-tunnel)#mpls signal-protocol { rsvp-te static }	Configure the protocol type of Tunnel interface and choose RSVP-TE. By default, it is static protocol.
8	Raisecom(config-tunnel)#mpls tunnel-id <i>tunnel-id</i>	Configure Tunnel ID on the Tunnel interface.
9	Raisecom(config-tunnelif)#mpls explicit-path <i>path-name</i> [secondary]	Configure binding Tunnel interface with explicit path or with backup explicit path. Backup explicit path is used for LSP hot backup protection.
10	Raisecom(config-tunnelif)#mpls te commit	Hand configuration information about MPLS Tunnel interface, including Tunnel ID and destination IP address.
11	Raisecom(config)#mpls label-advertise { 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

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 <i>interface-number</i>	Enter Tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#tunnel mode mpls	Configure the Tunnel interface mode to MPLS.
4	Raisecom(config-tunnel)#mpls signal-protocol { rsvp-te static }	Configure the protocol type of the Tunnel interface to RSVP-TE. By default, it is static.
5	Raisecom(config-tunnelif)#mpls te fast-reroute [node-protect]	Enable FRR on the Tunnel interface. By default, it is disabled.
6	Raisecom(config-tunnel)#mpls te bypass-tunnel	(Optical) configure the current Tunnel as a bypass Tunnel.
7	Raisecom(config-tunnelif)#exit	Exit Tunnel interface configuration mode.
8	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 3 physical interface configuration mode.
	Raisecom(config-port)#mpls te backup-path tunnel <i>interface-number</i>	Configure FRR bypass Tunnel on the Layer 3 physical interface.

Configuring LSP hot backup

The RSVP-TE is enabled and the explicit path and related function of Tunnel is configured.

Both step 3 and step 4 are for configuring hot backup. However, step 3 is for specifying explicit path and step 4 is for automatic generation mode. If step 3 and step 4 are configured together, step 3 will prevail.

step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface tunnel <i>interface-number</i>	Enter tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#tunnel mode mpls	Configure the Tunnel interface mode to MPLS.
4	Raisecom(config-tunnelif)#mpls explicit-path <i>path-name secondary</i>	Specify the explicit path as the hot backup LSP and enable hot backup protection.
5	Raisecom(config-tunnelif)#mpls te hot-standby wtr <i>interval</i>	(Optional) configure hot backup switch-back time on MPLS tunnel interface. This function only takes effect on RSVP-TE. By default, the WTR is 10s.

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 [detect-multiplier <i>detect-multiplier</i> min-rx-interval <i>min-rx-interval</i> min-tx-interval <i>min-tx-interval</i>]	Enable BFD based on RSVP-TE globally.
3	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
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 [<i>interface-type interface-number</i>]	Show status of RSVP-TE on the interface.
3	Raisecom#show mpls rsvp-te session [destination <i>ip-address</i> tunnel-id <i>tunnel-id</i>]	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 hot-standby state { all interface tunnel <i>interface-number</i> }	Show hot backup on Tunnel interface.
7	Raisecom)#show mpls te bypass-tunnel [<i>interface-number</i>]	Show the bypass Tunnel.
8	Raisecom#show mpls explicit-path [<i>path-name</i>]	Show explicit path.
9	Raisecom#show mpls te frr protecting [bypass-tunnel tunnel <i>interface-number</i>]	Show FRR protection.
10	Raisecom#show cspf tedb [detail <i>ip-address</i>]	Show TEDB database.
11	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.

9.6.2 Configuring MPLS Tunnel fault acknowledgment

Step	Command	Description
1	<code>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]</code>	Configure the MPLS LSP Ping test.
2	<code>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]</code>	Configure the MPLS Tunnel Ping test.

9.6.3 Configuring MPLS Tunnel fault location

Step	Command	Description
1	<code>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]</code>	Configure the MPLS LSP Traceroute test.
2	<code>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]</code>	Configure the MPLS Tunnel Traceroute test.

10 MPLS VPN

This chapter describes principles and configuration procedures of MPLS-TP, including following sections:

- Configuring VPWS
- Configuring CCC L2VPN
- Configuring VPLS
- Configuring MPLS L3VPN
- Configuring MPLS VPN fault detection
- Maintenance

10.1 Configuring VPWS

10.1.1 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 10-1 and Table 10-2.

Table 10-1 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.

Type of sub-interface	Function	VPWS/VSI	
		Raw encapsulation	Tagged encapsulation
	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	Replace 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 10-2 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. Use the vlan translation svlan untag command to enable the interface to remove the outer Tag. Otherwise, the Tag cannot be removed.	Remove the outer Tag of the packet first and then add outer Tag according to the interface configurations. Use the vlan translation svlan untag command to enable the interface to remove the outer 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	Add the outer Tag to the packet. Use the vlan translation svlan untag command to enable the interface to add the outer Tag. Otherwise, the Tag cannot be added. The added Tag is the SVLAN encapsulated by the sub-interface.	Replace the outer Tag of the packet. Use the vlan translation svlan untag command to enable the interface to add the outer Tag. Otherwise, the Tag cannot be added. The added Tag is the SVLAN encapsulated by the sub-interface.

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 command to enable the interface to remove the outer Tag. Otherwise, the Tag cannot be removed.	Remove the outer Tag of the packet first and then add outer Tag according to the interface configurations. Use the vlan translation svlan untag command to enable the interface to remove the outer 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.
		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	Add the outer Tag to the packet. Use the vlan translation svlan untag command to enable the interface to add the outer Tag. Otherwise, the Tag cannot be added. The added Tag is the SVLAN encapsulated by the sub-interface.	Replace the outer Tag of the packet. Use the vlan translation svlan untag command to enable the interface to add the outer Tag. Otherwise, the Tag cannot be added. The added Tag is the SVLAN encapsulated by the sub-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.

10.1.2 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 <i>interface-type</i> <i>interface-number</i>	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 12	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 <i>interface-type</i> <i>interface-number.subif</i>	Enter sub-interface configuration mode.
	Raisecom(config-subif)#encapsulation { dot1q qinq }	Configure the sub-interface encapsulation mode.
	Raisecom(config-subif)#mode 12	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.
	Raisecom(config-subif)#vlan translation svlan untag	(Optional) configure the outer VLAN tag for the sub-interface.
	Raisecom(config-subif)#vlan translation svlan untag cvlan untag	(Optional) configure the outer double-layer VLAN tag for the sub-interface.

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 <i>ip-address</i> raw <i>vc-id</i> <i>vc-id</i> in-label <i>in-label</i> out-label <i>out-label</i> [tunnel-policy <i>policy-name</i> tunnel <i>tunnel-number</i>] [no-control-word] [mtu <i>mtu</i>] [backup bypass]	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 <i>ip-address</i> [tagged] <i>vc-id</i> <i>vc-id</i> in-label <i>in-label</i> out-label <i>out-label</i> [tunnel-policy <i>policy-name</i> tunnel <i>interface-number</i>] [no-control-word] [mtu <i>mtu</i>] [tpid <i>tpid</i>] [svlan <i>vlan-id</i>] [backup bypass]	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.

10.1.3 Configuring dynamic L2VC

Configuring service extraction interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
	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 12	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 <i>interface-type</i> <i>interface-number</i>.<i>subif</i>	Enter sub-interface configuration mode.
	Raisecom(config-subif)#encapsulation { dot1.q qinq }	Configure the sub-interface encapsulation mode.
	Raisecom(config-subif)#mode 12	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.
	Raisecom(config-subif)#vlan translation svlan untag	(Optional) configure the outer VLAN tag for the sub-interface.

Step	Command	Description
	Raisecom(config-subif)#vlan translation svlan untag cvlan untag	(Optional) configure the outer double-layer VLAN tag for the sub-interface.

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 bypass]	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] [svlan vlan-id] [backup bypass]	Configure dynamic L2VC. The encapsulation mode of PW packets is Tagged. You can choose to configure the client VLAN ID.

10.1.4 Configuring MS-PW

Configuring static-to-static PW switching

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
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 static-to-static MS-PW, which is encapsulated based on Ethernet.
3	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] backup ip-address vc-id in-label in-label out-label out-label [tunnel-policy policy-name tunnel tunnel-number]	(Optional) configure static-to-static MS PW with backup protection. The PW is encapsulated based on Ethernet.

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, which is encapsulated based on Ethernet.
3	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] backup ip-address vc-id in-label in-label out-label out-label [tunnel-policy policy-name tunnel tunnel-number]	(Optional) configure dynamic-to-static MS PW with backup protection. The PW is encapsulated based on Ethernet.
4	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 [tunnel-policy policy-name tunnel tunnel-number] { raw tagged } [no-control-word] [mtu mtu] backup ip-address vc-id [tunnel-policy policy-name tunnel tunnel-number]	Configure static-to-dynamic MS-PW with backup protection.

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-interface tunnel-number] between ip-address vc-id [tunnel-policy policy-name tunnel-interface tunnel-number] { raw tagged }	Configure dynamic-to-dynamic MS-PW, which is encapsulated based on Ethernet.
3	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 } backup ip-address vc-id [tunnel-policy policy-name tunnel tunnel-number]	(Optional) configure dynamic-to-dynamic MS PW with backup protection. The PW 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.

10.1.5 (Optional) configuring BFD for PW

After configuring PW, you can configure PW-based BFD.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#mpls l2vpn pw bfd [<i>min-tx-interval tx-interval</i>] [<i>min-rx-interval rx-interval</i>] [<i>detect-multiplier multiplier</i>] [<i>backup</i>]	Configure PW-based BFD.

10.1.6 Configuring VPWS traffic label

Configuring L2VPN traffic label

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#mpls l2vpn flow-label { both send receive } [<i>static</i>] [<i>backup</i>]	Configure the L2VPN label.

Configuring MS PW traffic label

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mpls switch-l2vc <i>ip-address vc-id vc-id</i> flow-label { both send receive }	Enable traffic label for a specified PW in the MS PW.

Configuring load balancing based on traffic label

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mpls l2vpn flow-label hash-fields { 12 13 14 }	Configure the HASH factor for traffic label load balancing: • Based on MAC address • Based on IP address • Based on quintuple

10.1.7 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.

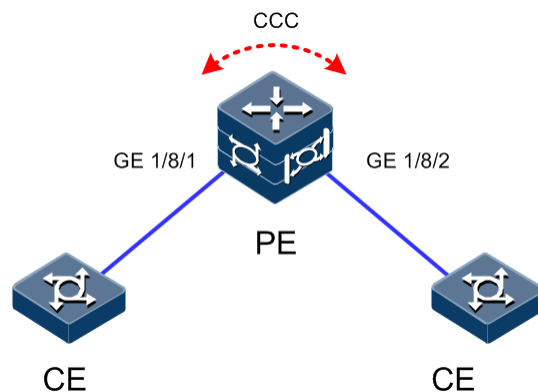
10.2 Configuring CCC L2VPN

10.2.1 Preparing for configurations

Scenario

Circuit Cross Connect (CCC) is a method to implement MPLS L2VPN through static LSP. As shown in Figure 10-1, CCC is applied to the local connection scenario. CE1 and CE2 are connected to the same PE. The PE acts as a Layer 2 switch. Data exchange is implemented by configuring the interface type and encapsulation mode.

Figure 10-1 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.

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.

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.

10.2.2 Configuring CCC

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

Step	Command	Description
2	<pre>Raisecom(config)#ccc ccc-name interface interface-type interface-number [access-port] [raw tagged] out-interface interface-type interface-number [access-port] [raw tagged]</pre>	Configure CCC. • interface interface-type interface-number: configure the CCC ingress interface. The interface-type is the interface type, including GE physical interfaces, 10GE physical interfaces, and sub-interfaces. The interface-number is the interface number, which depends on the interface type. • access-port: configure the physical interface mode. In the incoming direction of the interface, only untagged packets are allowed to pass and tagged packets are discarded. This mode is invalid when configured on the sub-interface. • raw: configure the encapsulation mode of the physical interface or sub-interface to raw, namely, the operation of the interface about VLAN translation. • tagged: configure the encapsulation mode of the physical interface or sub-interface to tagged, namely, the operation of the interface about VLAN translation. • out-interface interface-type interface-number: configure the CCC egress interface.

10.2.3 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show 12vpn ccc ccc-name</pre>	Show CCC configurations.

10.3 Configuring VPLS

10.3.1 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.

10.3.2 Configuring VSI



Note

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.
5	Raisecom(config-vsi)#encapsulation { raw tagged }	Configure the encapsulation mode of VSI services.
6	Raisecom(config-vsi)#l2vpn access-mode asymmetry	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 [isolate]] [backup [recv-block] bypass]	Configure the VSI static peer. Create a PW and specify the Tunnel for the PW to isolate ACs.
8	Raisecom(config-vsi)#mpls peer ip-address [vc-id vc-id] [tunnel-policy policy-name tunnel tunnel-number] [no-control-word] [upe [isolate]]	Configure the MPLS dynamic peer. Create a PW and specify a Tunnel for the PW to implement AC isolation.
9	Raisecom(config-vsi)#ratelimit { broadcast unknown-multicast dlf } cir cir-value [cbs cbs-value]	Configure rate limiting.
10	Raisecom(config-vsi)#exit	Exit VSI configuration mode.
	Raisecom(config)#interface interface-type interface-number	Enter interface configuration mode.
11	Raisecom(config-port)#mpls l2binding vsi vsi-name [isolate]	Bind VPLS services.

Configuring VSI MAC address rules

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

Step	Command	Description
2	Raisecom(config)# mpls vsi <i>vsi-name</i> 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 <i>threshold-value</i>	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)# interface <i>interface-type interface-number</i>	Enter interface configuration mode.
7	Raisecom(config-port)# mac-address static unicast <i>mac-address vsi vsi-name</i> [<i>interface-type interface-number</i>]	Configure the unicast MAC address of the VSI.
8	Raisecom(config-port)# mac-address blackhole <i>mac-address vsi vsi-name</i>	Configure the blackhole MAC address of the VSI.

Configuring VSI storm control

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# mpls vsi <i>vsi-name</i> static	Create a VSI and enter VSI configuration mode.
3	Raisecom(config-vsi)# storm-control { broadcast unknown-multicast d1f all } enable	Enable storm control.

Configuring VSI traffic statistics

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# mpls vsi <i>vsi-name</i> static	Create a VSI and enter VSI configuration mode.
3	Raisecom(config-vsi)# traffic-statistics [peer <i>ip-address vc-id vc-id</i>] enable	Enable VSI traffic statistics.

10.3.3 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.

10.3.4 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.

10.4 Configuring MPLS L3VPN

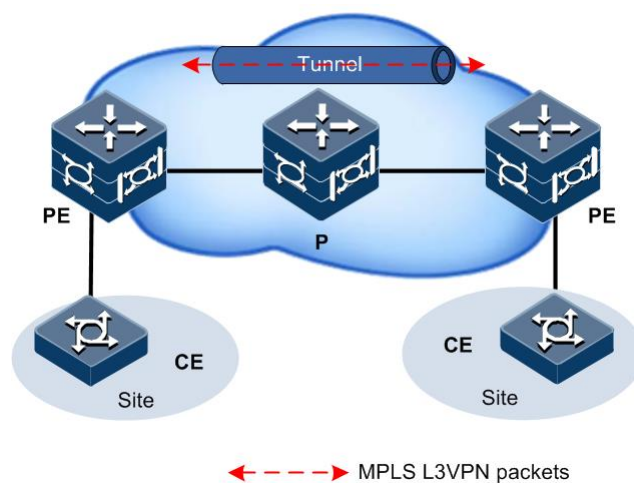
10.4.1 Preparing for configurations

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 10-2, in MPLS L3 VPN topology, the PE device and CE device exchange routes through EBGP.

Figure 10-2 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.
- Configure MPLS basic functions.
- Configure Tunnel related functions.

10.4.2 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 <i>vrf-name</i>	Create a VRF and enter VRF configuration mode.
3	Raisecom(config-vrf)#rd <i>rd</i>	Configure the VRF RD.
4	Raisecom(config-vrf)#route-target [export import both] <i>rt</i> [evpn]	Configure the VRF RT.

10.4.3 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 <i>interface-type interface-number</i>	Enter Layer 3 physical interface, VLAN sub-interface, and sub-interface configuration modes.
3	Raisecom(config-port)#ip vrf forwarding <i>vrf-name</i>	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.

10.4.4 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.
2	Raisecom(config)#router ospf <i>process-id</i> [vrf <i>vrf-name</i>] [router-id <i>router-id</i>]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#network <i>ip-address wild-card-mask area</i> <i>area-id</i>	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.

10.4.5 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 <i>policy-name</i>	Configure a Tunnel policy and enter Tunnel policy configuration mode.
3	Raisecom(config-tunnelpolicy)#tunnel select-seq { lsp cr-lsp } *	Configure the Tunnel selection sequence.

10.4.6 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 <i>as-id</i>	Enable BGP and create a BGP instance and enter BGP configuration mode.
3	Raisecom(config-router)#bgp router-id <i>router-id</i>	Configure BGP router ID.
4	Raisecom(config-router)#neighbor ip-address remote-as <i>as-id</i>	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 <i>ip-address2</i>	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 <i>vrf-name</i>	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.

Step	Command	Description
13	<code>Raisecom(config-router-af)#exit-address-family</code>	Exit IPv4 address family configuration mode based on BGP VPN instance.

10.4.7 Configuring PE-CE route switching

Static routes, EBGp 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip route vrf vrf-name destination-address mask-address { next-hop NULL 0 } * [distance distance] [description text] [tag tag]</code>	Configure static routes in the specified VRF.
3	<code>Raisecom(config)#router bgp as-id</code>	Enable BGP. Create a BGP instance and enter BGP configuration mode.
4	<code>Raisecom(config-router)#address-family ipv4 vrf vrf-name</code>	Specify the IPv4 unicast address family routing table of the specified VPN instance and enter VPN instance IPv4 unicast address family configuration mode.
5	<code>Raisecom(config-router-af)#redistribute static</code>	Redistribute routes to the IPv4 unicast address family routing table of the VPN instance.

Configure the CE device as below.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ip route destination-address { mask-address mask-length } { next-hop NULL 0 } * [distance distance] [description text] [tag tag]</code>	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 <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)#address-family ipv4 vrf <i>vrf-name</i>	Create BGP VRF and enter IPv4 unicast address family configuration mode.
4	Raisecom(config-router-af)#neighbor <i>ip-address</i> remote-as <i>as-id</i>	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 <i>ip-address</i> 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.
6	Raisecom(config-router-af)#redistribute { connected static ospf } [metric <i>metric</i>] [route-map <i>map</i>]	Redistribute CE routes. Redistribute the CE routes to the VPN routing table to advertise them to the peer PE on the network.
	Raisecom(config-router-af)#network <i>ip-address</i> [mask-address] [route-map <i>route-map-name</i>]	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 <i>as-id</i>	Enter BGP configuration mode.
3	Raisecom(config-router)#neighbor <i>ip-address</i> remote-as <i>as-id</i>	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 <i>metric</i>] [route-map <i>map</i>]	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 <i>ip-address</i> [mask-address] [route-map <i>route-map-name</i>]	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.

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.

10.4.8 Checking configurations

No.	Command	Description
1	Raisecom# show ip vrf 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] [vrf vrf-name] route	Show information about OSPF routes.
7	Raisecom# show ip bgp [ip-address [ip-mask]]	Show information about BGP routes.

10.5 Configuring MPLS VPN fault detection

10.5.1 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.

10.5.2 Configuring MPLS VPN fault acknowledgement

Step	Command	Description
1	<code>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]</code>	Configure the MPLS PW Ping test.
2	<code>Raisecom#ping mpls vsi vsi-name mac mac-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]</code>	Configure the MPLS VPLS Ping test.
3	<code>Raisecom#ping vrf vpn-name ip-address [count count] [df-bit] [size size] [source ip-address] [waittime seconds]</code>	Configure the MPLS VRF PING detection.

10.5.3 Configuring MPLS VPN fault location

Step	Command	Description
1	<code>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]</code>	Configure the MPLS PW Traceroute test.
2	<code>Raisecom#traceroute [vrf instance-name] ip-address [firstttl first-ttl] [maxttl max-ttl] [port port-number] [waittime second] [count times] [size size]</code>	Configure the MPLS L3VPN Traceroute test.

10.6 Maintenance

Command	Description
<code>Rasiecom#clear ip bgp [all ip-address external] vrf vrf-name [as-id]</code>	Reset all BGP connections or a specified BGP connection in the VRF.
<code>Rasiecom#clear ip bgp [all ip-address external] vrf vrf-name [as-id] { in out soft }</code>	Upgrade all BGP routes or a specified BGP route in the VRF instead of disconnecting BGP connections, namely, soft reset.
<code>Rasiecom#clear traffic-statistics vrf vrf-name</code>	Clear VRF traffic statistics.

11 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 traffic statistics
- Maintenance

11.1 Configuring ACL

11.1.1 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

11.1.2 Configuring ACL

Select Steps 3–7 as required.

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

Step	Command	Description
2	<code>Raisecom(config)#access-list <i>acl-number</i></code>	Create an ACL, select an ACL value, and enter the corresponding ACL configuration mode. The value of <i>acl-number</i> 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
3	<code>Raisecom(config-acl-ip-std)#rule [<i>rule-id</i>] { deny permit } { <i>source-ip-address source-ip-mask</i> any } [time-range <i>time-range-name</i>]</code>	Configure the basic IP ACL rule in basic IP ACL configuration mode.
4	<code>Raisecom(config-acl-ip-ext)#rule [<i>rule-id</i>] { deny permit } { <i>protocol-id</i> icmp ip } { <i>source-ip-address source-ip-mask</i> any } { <i>destination-ip-address destination-ip-mask</i> any } [dscp <i>dscp-value</i> precedence <i>precedence-value</i> tos <i>tos-value</i>] [ttl <i>ttl-value</i>] [vrf <i>vrf-name</i>] [vni <i>vni-value</i>] [fragment] [time-range <i>time-range-name</i>]</code> <code>Raisecom(config-acl-ip-ext)#rule [<i>rule-id</i>] { deny permit } udp { <i>source-ip-address source-ip-mask</i> any } [<i>source-port</i>] { <i>destination-ip-address destination-ip-mask</i> any } [<i>destination-port</i>] [dscp <i>dscp-value</i> precedence <i>precedence-value</i> tos <i>tos-value</i>] [ttl <i>ttl-value</i>] [vrf <i>vrf-name</i>] [vni <i>vni-value</i>] [fragment] [time-range <i>time-range-name</i>]</code> <code>Raisecom(config-acl-ip-ext)#rule [<i>rule-id</i>] { deny permit } tcp { <i>source-ip-address source-ip-mask</i> any } [<i>source-port</i>] { <i>destination-ip-address destination-ip-mask</i> any } [<i>destination-port</i>] [tcpflag <i>flag-value tcpflagmask mask-value</i>] [dscp <i>dscp-value</i> precedence <i>precedence-value</i> tos <i>tos-value</i>] [ttl <i>ttl-value</i>] [vrf <i>vrf-name</i>] [vni <i>vni-value</i>] [url-group <i>group-value</i>] [fragment] [time-range <i>time-range-name</i>]</code>	(Optional) configure the extended IP ACL rule in IP ACL configuration mode.

Step	Command	Description
	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 type-value [type-value] [dscp dscp-value precedence precedence-value tos tos-value] [ttl ttl-value] [vrf vrf-name] [vni vni-value] [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-mps)#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 } [ethertype { ethertype [ethertype-mask] ip arp }] layer2 rule-string rule-mask offset [second rule-string rule-mask offset] [third { 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 } [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] [flow-label label-value] [fragment] [time-range time-range-name]	(Optional) configure the extended IPv6 ACL rules in extended IPv6 ACL configuration mode.

Step	Command	Description
	<pre>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] [flow-label label-value] [fragment] [time-range time-range-name]</pre>	
	<pre>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] [flow-label label-value] [fragment] [time-range time-range-name]</pre>	
10	<pre>Raisecom(config-acl-advanced)#rule [rule-id] { deny permit } { source-mac-address source-mac-mask any } { destination-mac-address destination-mac-mask any } [svlan svlanid] [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]</pre>	Configure Advanced ACL rules.
11	<pre>Raisecom(config)#access-list copy dest-acl-number source-acl-number</pre>	Copy to generate the same ACL rule.

11.1.3 Creating time period

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#time-range time-range-name start-time to end-time { weekday-list mon tue wed thu fri sta sun off-day working-day daily } [from time date [to time date] to time date]</pre>	Create the time period, which can be referred to by the ACL rule.
	<pre>Raisecom(config)#time-range time-range-name { from time date [to time date] to time date }</pre>	

11.1.4 Configuring filter

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

11.1.5 Checking configurations

No.	Command	Description
1	Raisecom#show access-list [<i>acl-number</i> name acl-name]	Show ACL information.
2	Raisecom#show filter interface	Show filter information.
	Raisecom#show filter interface <i>interface-type</i> <i>interface-number</i> [ingress egress]	
	Raisecom#show filter statistics interface <i>interface-</i> <i>type interface-number { ingress egress } access-</i> <i>list acl-number { acl-number name acl-name }</i>	
3	Raisecom#show time-range [<i>time-range-name</i>]	Show configurations of the time period.

11.2 Configuring priority trust and priority mapping

11.2.1 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 RAX711-C-R can perform different operations on packets with different priorities, providing related services.

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

11.2.2 Configuring priority trust

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-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 ipp	Configure the interface to trust IPP.
5	Raisecom(config-port)#mls qos trust port-priority	Configure the interface to trust interface priority.
6	Raisecom(config-port)#mls qos priority <i>priority</i>	Configure the interface priority. By default, it is 5.

11.2.3 Configuring mapping between DSCP priority and local priority based on interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mls qos mapping dscp-to- local-priority <i>profile-id</i>	Create the DSCP-to-local priority (color) mapping profile and enter dscp-to-pri configuration mode.
3	Raisecom(dscp-to-pri)#dscp <i>dscp-value</i> to local-priority <i>localpri-value</i> [color { green red yellow }]	Configure mapping between the DSCP priority and local priority (color).
4	Raisecom(dscp-to-pri)#exit Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Exit dscp-to-pri configuration mode. Enter interface configuration mode.

Step	Command	Description
5	Raisecom(config-port)#mls qos dscp-to-local-priority <i>profile-id</i>	Apply the DSCP-to-local priority (color) mapping profile to an interface.

11.2.4 Configuring mapping between CoS priority and local priority based on interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mls qos mapping cos-to-local-priority <i>profile-id</i>	Create the CoS-to-local priority (color) mapping profile and enter cos-to-pri configuration mode.
3	Raisecom(dscp-to-pri)#cos <i>cos-value</i> to local-priority <i>localpri-value</i> [color { green red yellow }]	Configure mapping between the CoS priority and local priority (color).
4	Raisecom(dscp-to-pri)#exit Raisecom(config)#interface <i>interface-type interface-number</i>	Exit cos-to-pri configuration mode. Enter interface configuration mode.
5	Raisecom(config-port)#mls qos cos-to-local-priority <i>profile-id</i> [dei enable]	Apply the CoS-to-local priority (color) mapping profile to an interface or enable color marking for outgoing packets on the interface.

11.2.5 Configuring Exp-to-local priority mapping

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mls qos mapping exp-to-local-priority <i>profile-id</i>	Create an Exp-to-local priority (color) mapping profile and enter exp-to-pri configuration mode.
3	Raisecom(exp-to-pri)#exp <i>exp-value</i> to local-priority <i>localpri-value</i> [color { green red yellow }]	Configure Exp-to-local priority (color) mapping.

11.2.6 Configuring DSCP priority remarking

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mls qos mapping dscp-mutation <i>profile-id</i>	Create the DSCP remarking profile and enter dscp-mutation configuration mode.

Step	Command	Description
3	Raisecom(dscp-mutation)#dscp <i>dscp-value</i> to new-dscp <i>dscp-value</i>	Remark the DSCP priority of specified packets.
4	Raisecom(dscp-mutation)#exit Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Exit dscp-mutation configuration mode. Enter interface configuration mode.
5	Raisecom(config-port)#mls qos dscp-mutation <i>profile-id</i>	Apply the DSCP remarking profile to an interface.

11.2.7 Configuring CoS priority remarking

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mls qos mapping cos-remark <i>profile-id</i>	Create the CoS remarking profile and enter dscp-remark configuration mode.
3	Raisecom(cos-remark)#local-priority <i>localpri-value</i> to cos <i>cos-value</i>	Configure the mapping between the local priority and CoS priority.
4	Raisecom(cos-remark)#exit Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Exit cos-remark configuration mode. Enter interface configuration mode.
5	Raisecom(config-port)# mls qos cos-remark-mapping enable [<i>dei enable</i>]	Enable local priority-to-CoS mapping or enable color marking for outgoing packets on the interface.
6	Raisecom(config-port)#mls qos cos-remark <i>profile-id</i>	Apply the CoS remarking profile to an interface.

11.2.8 Checking configurations

No.	Command	Description
1	Raisecom#show mls qos mapping dscp-to-local-priority [<i>default</i> <i>profile-id</i>]	Show information about the DSCP-to-local priority (color) mapping profile.
2	Raisecom#show mls qos mapping cos-to-local-priority [<i>default</i> <i>profile-id</i>]	Show information about the CoS-to-local priority (color) mapping profile.
3	Raisecom#show mls qos mapping exp-to-local-priority [<i>default</i> <i>profile-id</i>]	Show information about Exp-to-local priority (color) mapping.
4	Raisecom#show mls qos mapping dscp-mutation [<i>default</i> <i>profile-id</i>]	Show information about the DSCP remarking profile.
5	Raisecom#show mls qos mapping cos-remark [<i>default</i> <i>profile-id</i>]	Show information about the CoS remarking profile.

No.	Command	Description
6	Raisecom#show mls qos mapping local-priority-to-exp [default <i>profile-id</i>]	Show information about the local priority-to-Exp mapping profile.
7	Raisecom#show mls qos mapping ipp-to-local-priority [default <i>profile-id</i>]	Show information about the IPP-to-local priority mapping profile.
8	Raisecom#show mls qos interface [<i>interface-type</i> <i>interface-number</i>]	Show QoS information on the interface.

11.3 Configuring traffic classification and traffic policy

11.3.1 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

11.3.2 Creating and configuring traffic classification

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#class-map <i>class-map-name</i> [match all match any]	Create traffic classification and enter CMAP configuration mode.
3	Raisecom(config-cmap)#match access-list { <i>acl-number</i> name <i>acl-name</i> }	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.

Step	Command	Description
	<pre>Raisecom(config- cmap)#match { dscp dscp- list cos cos-list inner-cos cos-list inner-vlan inner-vlan- list ip precedence ipp-list ip tos tos- list ipv6 dscp dscp- list label lable-list second-label lable- list vlan vlan-list }</pre>	Configure the rule lists of various types that match the traffic classification rule. • dscp dscp-list: match the DSCP value. • cos cos-list: match the CoS. • inner-cos cos-list: match the inner CoS. • inner-vlan inner-vlan-list: match the inner VLAN list. • ip precedence ipp-list: match the IP priority. • ip tos tos-list: match the ToS. • ipv6 dscp dscp-list: match the IPv6 DSCP value. • label lable-list: match the label value. • second-label lable-list: match the second-label value. • vlan vlan-list: match the VLAN list.

11.3.3 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)#drop-color { red yellow } *	(Optional) discard packets with specified color.
4	Raisecom(traffic-policer)#set-cos { green green-value [red red-value] [yellow yellow-value] red red-value }	(Optional) configure the mapping between packet color and CoS priority.
5	Raisecom(traffic-policer)#set-dscp { green green-value [red red-value] [yellow yellow-value] red red-value }	(Optional) configure the mapping between packet color and DHCP priority.
6	Raisecom(traffic-policer)#recolor { green-recolor { red yellow } red-recolor { green yellow } yellow-recolor { green red } } *	(Optional) re-color the packet. QoS use the CAR to classify and color the packet. The downstream network can accept the color result of the upstream network or re-color the packet based on its classification standard.
7	Raisecom(traffic-policer)#cir cir cbs cbs [ebs ebs] Raisecom(traffic-policer)#cir cir cbs cbs eir eir ebs ebs [coupling] Raisecom(traffic-policer)#cir cir cbs cbs pir pir pbs pbs	(Optional) configure rate limiting parameters.

11.3.4 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 <i>policy-map-name</i>	Create a traffic policy and enter PMAP configuration mode.
3	Raisecom(config-pmap)#class-map <i>class-map-name</i>	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 <i>policer-name</i>	Import a traffic policing profile (policer) into the traffic policy.
5	Raisecom(config-pmap-c)#set { cos <i>cos-value</i> local-priority <i>value</i> } Raisecom(config-pmap-c)#set { inner-vlan <i>inner-vlan-id</i> vlan <i>vlan-id</i> }	(Optional) configure packet remarking.
6	Raisecom(config-pmap-c)#add outer-vlan <i>vlan-id</i>	(Optional) configure the VLAN ID of the added outer VLAN Tag.
7	Raisecom(config-pmap-c)#redirect-to <i>interface-type interface-number</i>	(Optional) configure the redirection rule to forward matched packets through the specified interface.
8	Raisecom(config-pmap-c)#copy-to-mirror mirror-group <i>group-id</i>	(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 <i>interface-type interface-number</i>	Exit CMAP configuration mode. Exit PMAP configuration mode. Enter interface configuration mode.
12	Raisecom(config-port)#service-policy { ingress egress } <i>policy-map-name</i>	Apply the traffic policy to an interface.

11.3.5 Checking configurations

No.	Command	Description
1	<code>Raisecom#show class-map [class-map-name]</code>	Show traffic classification information.
2	<code>Raisecom#show mls qos policer [policer-name]</code>	Show traffic policing rules.
3	<code>Raisecom#show policy-map [policy-map-name] [class-map class-map-name]</code>	Show traffic policy information.
4	<code>Raisecom#show service-policy interface</code> <code>Raisecom#show service-policy interface interface-type interface-number [egress ingress]</code>	Show information about applied policies.
5	<code>Raisecom#show service-policy statistics interface interface-type interface-number { egress ingress } policy-map policy-map-name [class-map class-map-name]</code>	Show statistics about applied traffic policies.

11.4 Configuring congestion avoidance and queue shaping

11.4.1 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 RAX711-C-R 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

11.4.2 Configuring WRED profile

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mls qos wred profile profile-id</code>	Create the WRED profile and enter WRED profile configuration mode.

Step	Command	Description
3	<code>Raisecom(wred)#wred [color { green red yellow }] start-drop-threshold start-drop end-drop-threshold end-drop max-drop-probability max-drop</code>	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	<code>Raisecom(wred)#wred start-drop-threshold start-value end-drop-threshold end-value max-drop-probability max-value</code>	Configure the drop threshold of the WRED profile.

11.4.3 Configuring flow queue profile

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mls qos flow-queue profile flow-profile-id</code>	Create a flow profile and enter flow profile configuration mode.
3	<code>Raisecom(flow-queue)#scheduler wrr</code>	Configure the queue scheduling policy. By default, it is SP.
4	<code>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]</code>	Configure the queue, weight, shaping, and WRED information of the flow profile. If no weight is configured, SP scheduling mode is adopted.
5	<code>Raisecom(flow-queue)#exit</code> <code>Raisecom(config)#interface interface-type interface-number</code>	Exit flow profile configuration mode. Enter interface configuration mode.
6	<code>Raisecom(config-port)# mls qos flow-queue profile-id</code>	Apply the flow profile to an interface.

11.4.4 Configuring queue shaping

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.
3	<code>Raisecom(config-port)#mls qos shaping egress pir pir-value [pbs pbs-value]</code>	Configure queue shaping for queues of the interface.

11.4.5 Checking configurations

No.	Command	Description
1	<code>Raisecom#show mls qos wred profile [profile-list]</code>	Show WRED profile configurations.
2	<code>Raisecom#show mls qos flow-queue profile flow-profile-list</code>	Show flow profile configurations.
3	<code>Raisecom#show mls qos shaping interface [interface-type interface-number egress]</code>	Show queue shaping information.
4	<code>Raisecom#show mls qos queue statistics interface interface-type interface-number</code>	Show queue statistics of the interface.

11.5 Configuring interface rate limiting

11.5.1 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

11.5.2 Configuring interface-based rate limiting

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.
3	<code>Raisecom(config-port)#rate-limit { egress ingress } cir cir-value cbs cbs-value [pir pir-value pbs pbs-value]</code> <code>Raisecom(config-port)#exit</code>	Configure rate limiting in the ingress and egress directions of the interface. Rate limiting can be based on the following interfaces: • Layer 3 physical interface of the VLAN interface • Layer 2 physical interface • Sub-interface • Link aggregation interface
4	<code>Raisecom(config)#rate-limit mode { 11 12 }</code>	(Optional) configure the rate limiting mode. • 11: physical layer mode • 12: data link layer mode

11.5.3 Checking configurations

No.	Command	Description
1	Raisecom# show rate-limit interface	Show interface-based rate limiting.
	Raisecom# show rate-limit interface <i>interface-type interface-number [ingress egress]</i>	

11.6 Configuring hierarchical bandwidth rate limiting

11.6.1 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 guarantee profile and a hierarchical bandwidth guarantee profile to match the packets received on the interface with the profile to ensure the normal transmission of special services.

Prerequisite

N/A

11.6.2 Configuring bandwidth guarantee

Creating bandwidth guarantee template

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# bandwidth-profile <i>bwp-profile-id</i> <i>cir cir cbs cbs [pir pir-value pbs pbs-value]</i> <i>[color-aware]</i>	Create a bandwidth guarantee template.
	Raisecom(config)# bandwidth-profile <i>bwp-profile-id</i> <i>cir cir cbs cbs eir eir ebs ebs [color-aware</i> <i>[coupling]]</i>	
3	Raisecom(config)# bandwidth-profile <i>bwp-profile-id</i> description <i>word</i>	Configure the description of the bandwidth guarantee template.



Note

If the bandwidth guarantee template is quoted by other hierarchical templates or is applied, you will fail to delete it.

11.6.3 Configuring hierarchical bandwidth guarantee

Configuring hierarchical VLAN bandwidth guarantee

No.	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#bandwidth-profile <i>profile-id</i> cir <i>cir cbs cbs [eir eir ebs ebs] [color-aware]</i>	Create a bandwidth guarantee template.
3	Raisecom(config)#hierarchy-vlan bandwidth-profile <i>hc-profile-id</i>	Create a hierarchical VLAN template and enter hierarchical VLAN configuration mode.
4	Raisecom(config-hvlan)#bandwidth vlanlist <i>vlan-list bwp-profile-id</i> Raisecom(config-hcos)#exit	Configure a hierarchical VLAN template.
5	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
6	Raisecom(config-port)#bandwidth { ingress egress } vlan <i>vlan-id bwp-profile-id</i>	Apply the VLAN bandwidth rate-limiting template to the interface.
7	Raisecom(config-port)#bandwidth ingress vlan <i>vlan-id coslist cos-value bwp-profile-id</i>	Apply the VLAN+CoS bandwidth rate-limiting template to the interface.

Configuring hierarchical CoS bandwidth guarantee

No.	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#bandwidth-profile <i>profile-id</i> cir <i>cir cbs cbs [eir eir ebs ebs] [color-aware]</i>	Create a bandwidth guarantee template.
3	Raisecom(config)#hierarchy-cos bandwidth-profile <i>hc-profile-id</i>	Create a hierarchical CoS template and enter HCoS configuration mode.
4	Raisecom(config-hcos)#bandwidth coslist <i>cos-list bwp-profile-id</i> Raisecom(config-hcos)#exit	Configure a hierarchical CoS template.
5	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
6	Raisecom(config-port)#bandwidth { ingress egress } vlan <i>vlan-id coslist cos-value bwp-profile-id</i>	Apply the VLAN+CoS bandwidth rate-limiting template to the interface.

No.	Command	Description
7	<code>Raisecom(config-port)#bandwidth ingress vlan <i>vlan-id bwp-profile-id hierarchy-cos hcos-profile-id</i></code>	Apply the VLAN+CoS hierarchical bandwidth rate-limiting template to the interface.

11.6.4 Checking configurations

No.	Command	Description
1	<code>Raisecom#show bandwidth-profile [<i>bwp-profile-id</i>]</code>	Show information about the bandwidth guarantee template.
2	<code>Raisecom#show bandwidth interface <i>interface-type interface-number</i></code>	Show bandwidth guarantee configurations on the interface.
3	<code>Raisecom#show hierarchy-cos-bandwidth profile [<i>hc-profile-id</i>]</code>	Show information about the hierarchical CoS bandwidth guarantee template.
4	<code>Raisecom#show hierarchy-vlan-bandwidth profile [<i>hd-profile-id</i>]</code>	Show information about hierarchical VLAN bandwidth guarantee template.

11.7 Configuring traffic statistics

11.7.1 Configuring performance statistics

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter interface configuration mode. By default, it is routing mode.
3	<code>Raisecom(config-port)#portswitch</code>	Configure the interface to switch mode.
4	<code>Raisecom(config-port)#performance statistics enable</code>	Enable performance statistics on the interface.
5	<code>Raisecom(config-port)#performance statistics vlan <i>vlan-list [cos cos-value] enable</i></code> <code>Raisecom(config-port)#exit</code>	Enable interface+VLAN or interface+VLAN+CoS performance statistics.
6	<code>Raisecom(config)#performance statistics interval buckets <i>buckets-value</i></code>	Configure the interval buckets of performance statistics.

11.7.2 Checking configurations

No.	Command	Description
1	Raisecom#show performance statistics interval buckets	Show global performance statistics.
2	Raisecom#show performance statistics interface <i>interface-type interface-number [vlan vlan-list [cos cos-value]] { current history }</i>	Show current or history performance statistics on the interface, interface + VLAN, or interface + VLAN + CoS.

11.8 Maintenance

Command	Description
Raisecom(config)#clear service-policy statistics interface <i>interface-type interface-number { egress ingress }</i>	Clearing traffic policy statistics.
Raisecom(config)#clear service-policy statistics interface <i>interface-type interface-number { egress ingress } policy-map policy-map-name [class-map class-map-name]</i>	
Raisecom(config)#clear mls qos queue statistics interface <i>interface-type interface-number [queueid queue-id]</i>	Clear queue statistics of interfaces.
Raisecom(config)#clear filter statistics interface <i>interface-type interface-number { ingress egress } [access-list acl-number]</i>	Clear ACL statistics.
Raisecom(config)#clear performance statistics histroy	Clear performance statistics on all history groups.

12 Multicast

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

- Configuring IGMP multicast basic functions
- Configuring IGMP Snooping
- Configuring IGMP Querier
- Configuring IGMP MVR
- Configuring IGMP filtering
- Configuring multicast VLAN copy
- Configuring PIM
- Configuring MLD L2 multicast
- Configuring MLD L3 multicast

12.1 Configuring IGMP multicast basic functions

12.1.1 Configuring basic functions of L2 multicast

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#igmp mrouter vlan <i>vlan-id interface-type interface-number</i>	(Optional) configure the multicast routing interface.
3	Raisecom(config)#igmp member-timeout { seconds infinite }	(Optional) configure the aging time of IGMP members.
4	Raisecom(config)#igmp ring <i>interface-type interface-number</i>	(Optional) enable IGMP ring network forwarding on the interface.
5	Raisecom(config)#igmp report-suppression	(Optional) enable Report suppression. Packet suppression and Proxy conflict with each other.
6	Raisecom(config)#igmp version { 2 3 }	(Optional) configure the IGMP version.

7	<code>Raisecom(config)#igmp mrouter vlan vlan-list priority priority-number</code>	(Optional) configure the CoS priority of the IGMP routing VLAN.
8	<code>Raisecom(config-port)#igmp immediate- leave vlan vlan-list</code>	Configure immediate leave. If the downstream interface is not enabled with immediate leave, the routing interface will calculate the aging time according to the robust coefficient when receiving the leave packet. The group timeout timer is configured to GMI (Group Membership Interval), $GMI = (robust-value * lastmember-queryinterval)$.

12.1.2 Checking configurations

No.	Command	Description
1	<code>Raisecom#show igmp configuration</code>	Show IGMP basic configurations.
2	<code>Raisecom#show igmp mrouter</code>	Show configurations of the multicast routing interface.
3	<code>Raisecom#show igmp immediate-leave [interface-type interface-number]</code>	Show configurations of L2 multicast immediate leave.
4	<code>Raisecom#show igmp statistics [interface-type interface-number]</code>	Show L2 multicast statistics.
5	<code>Raisecom#show igmp mrouter vlan-priority</code>	Show the CoS priority of the IGMP routing VLAN.
6	<code>Raisecom#show igmp ring</code>	Show information about the IGMP ring network interface.

12.1.3 Maintenance

Command	Description
<code>Raisecom(config)#clear igmp statistics [interface-type interface-number]</code>	Clear statistics on L2 multicast IGMP.
<code>Raisecom(config)#no igmp member interface-type interface-number</code>	Delete the specified multicast forwarding entry.

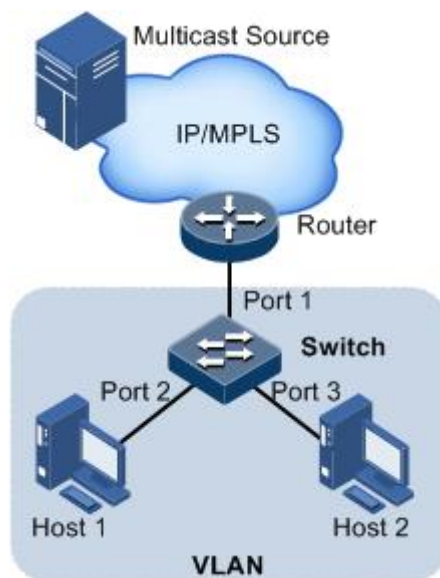
12.2 Configuring IGMP Snooping

12.2.1 Preparing for configurations

Scenario

As shown in Figure 12-1, multiple hosts receive data from the multicast source, and multiple hosts belong to the same VLAN. You can run IGMP Snooping on the switch between the multicast router and the host. You can establish and maintain a multicast forwarding table by monitoring IGMP packets between the multicast router and the host to implement Layer 2 multicast.

Figure 12-1 IGMP Snooping scenario



Prerequisite

Before configuring IGMP Snooping, complete the following tasks:

- Disable multicast VLAN copy on the device.
- Create a VLAN and add the corresponding interface to the VLAN.

12.2.2 Configuring IGMP Snooping

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#igmp snooping	Enable global IGMP Snooping.
3	Raisecom(config)#igmp member-timeout { seconds infinite }	(Optional) configure the aging time of IGMP members.
4	Raisecom(config)#igmp snooping vlan vlan-list	(Optional) enable IGMP Snooping in global VLAN.

Step	Command	Description
5	<pre>Raisecom(config)#vlan <i>vlan-id</i> Raisecom(config-vlan)#igmp snooping static ip-address [<i>interface-type</i> <i>interface-number</i>]</pre>	(Optional) configure the static members of IGMP Snooping in VLAN mode.



Note

- IGMP snooping and IGMP MVR cannot be enabled at the same time in the same multicast VLAN, otherwise the configuration fails.
- IGMP Snooping and multicast VLAN copy cannot be enabled at the same time in the same multicast VLAN, otherwise the configuration fails.

12.2.3 Checking configurations

No.	Command	Description
1	<pre>Raisecom#show igmp snooping [vlan <i>vlan-id</i> member vlan <i>vlan-list</i> mrouter vlan-priority]</pre>	Show IGMP Snooping configurations.
2	<pre>Raisecom#show igmp snooping member [<i>interface-type interface-number</i> vlan <i>vlan-id</i>]</pre>	Show multicast members of IGMP Snooping.
3	<pre>Raisecom#show igmp snooping member count [<i>interface-type interface-number</i> vlan <i>vlan-id</i>]</pre>	Show the number of IGMP Snooping multicast group members.
4	<pre>Raisecom#show igmp snooping vlan <i>vlan-id</i></pre>	Show configurations of IGMP Snooping in the specified VLAN.

12.3 Configuring IGMP Querier

12.3.1 Preparing for configurations

Scenario

In a network with multicast routing protocols widely applied, there are multiple hosts or client subnets that receive multicast information. You can configure IGMP Querier on the switch connected to the multicast router and the host to intercept the IGMP packets between the host and the router, thus reducing the network burden.

Configuring IGMP Querier can reduce the configuration and management of the client subnet by the multicast router, and at the same time realize the multicast connection of the client subnet.

IGMP Querier is generally used in conjunction with IGMP Snooping or IGMP MVR.

Prerequisite

Before configuring IGMP Querier, perform the following tasks:

- Create a VLAN.
- Add the corresponding interface to the VLAN.

12.3.2 Configuring IGMP Querier

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#igmp querier	Enable IGMP Querier.
3	Raisecom(config)#igmp source-ip <i>ip-address</i>	(Optional) configure the source IP address for IGMP queriers to send Query packets.
4	Raisecom(config)#igmp query-interval <i>period</i>	(Optional) configure the IGMP query interval.
5	Raisecom(config)#igmp query-max-response-time <i>period</i>	(Optional) configure the maximum response time of Query packets.
6	Raisecom(config)#igmp last-member-query-interval <i>period</i>	(Optional) configure the interval for the last group member to send Query packets.
7	Raisecom(config)#igmp proxy	Configure IGMP proxy.



Note

- If IGMP Querier is not enabled, you can configure IGMP Querier, including configuring the source IP address, query interval, maximum response time for sending Query packets, and the interval for the last member to send Query packets. When IGMP Querier is enabled, these configurations take effect immediately.
- IGMP Querier can be activated when IGMP Snooping or IGMP MVR is enabled.
- IGMP Proxy conflicts with IGMP Querier. IGMP Proxy conflicts with IGMP Report-Suppression.

12.3.3 Checking configurations

No.	Item	Description
1	Raisecom#show igmp querier	Show configurations of IGMP querier.

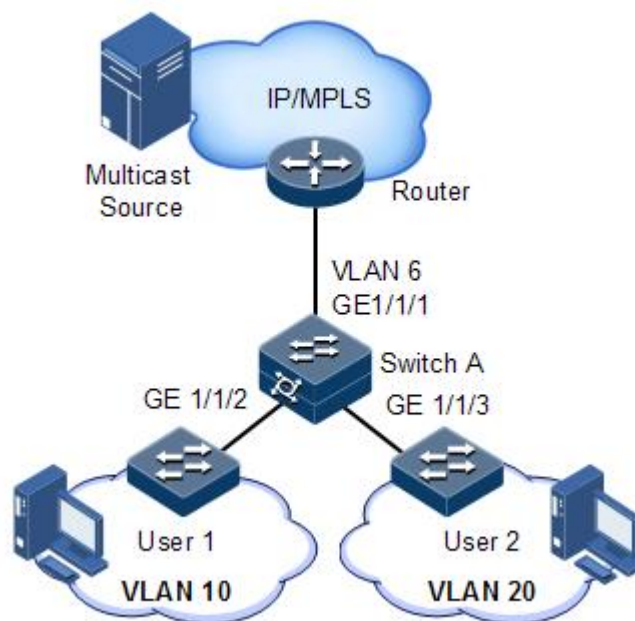
12.4 Configuring IGMP MVR

12.4.1 Preparing for configurations

Scenario

As shown in Figure 12-2, 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.

Figure 12-2 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.

12.4.2 Configuring IGMP MVR

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#igmp mvr</code>	Enable IGMP MVR.

Step	Command	Description
3	<code>Raisecom(config)#igmp mvr mcast-vlan <i>vlan-id</i> group { <i>start-ip-address</i> [<i>end-ip-address</i>] any }</code>	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	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter interface configuration mode.
5	<code>Raisecom(config-gigaethernet1/1/port)#igmp mvr mcast-vlan <i>vlan-id</i> static <i>ip-address user-vlan vlan-id</i></code>	(Optional) configure the MVR static multicast member.
6	<code>Raisecom(config-gigaethernet1/1/port)#igmp mvr user-vlan <i>vlan-id</i></code>	(Optional) configure the effective range of multicast cross VLAN copy.
7	<code>Raisecom(config-gigaethernet1/1/port)#igmp mvr mcast-vlan <i>vlan-id</i> static <i>ip-address</i></code>	(Optional) configure the static multicast members of MVR.



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.

12.4.3 Checking configurations

Step	Command	Description
1	<code>Raisecom# show igmp mvr { interface <i>interface-type interface-number</i> }</code>	Show configurations of the IGMP MVR of the specified interface.
2	<code>Raisecom#show igmp mvr member [<i>interface-type interface-number</i> <i>user-vlan vlan-id</i>]</code>	Show information about IGMP MVR multicast group members.
3	<code>Raisecom#show igmp mvr member count { <i>interface-type interface-number</i> <i>user-vlan vlan-id</i> }</code>	Show the number of members in the IGMP MVR multicast group.
4	<code>Raisecom#show igmp mvr vlan-group [<i>mcast-vlan vlan-id</i>]</code>	Show the multicast VLAN and its group address set.

12.5 Configuring IGMP filtering

12.5.1 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 switch 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.

12.5.2 Enabling IGMP filtering globally

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#igmp filter</code>	Enable IGMP filtering globally.



Note

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.

12.5.3 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#igmp filter profile profile-number</code>	Create an IGMP profile and enter profile configuration mode.
3	<code>Raisecom(config-igmp-profile)#{ permit deny }</code>	Configure IGMP profile actions.
4	<code>Raisecom(config-igmp-profile)#range range-id start-ip-address [end-ip-address]</code>	Configure the IP multicast address or range of control access.

Step	Command	Description
5	<code>Raisecom(config-igmp-profile)#exit</code> <code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode or aggregation group configuration mode.
6	<code>Raisecom(config-port)#igmp filter profile profile-number [vlan vlan-list]</code> <code>Raisecom(config-port)#exit</code>	Apply the IGMP profile filtering template to the physical layer interface or "interface+VLAN".
	<code>Raisecom(config-port-channel)#igmp filter profile profile-number [vlan vlan-list]</code> <code>Raisecom(config-port-channel)#exit</code>	Apply the IGMP profile filtering template to the aggregation group interface or "interface+VLAN".



Note

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.

12.5.4 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter the physical layer interface configuration mode or aggregation group configuration mode.
3	<code>Raisecom(config-port)#igmp filter max-groups group-number [vlan vlan-list]</code>	Configure the maximum number of groups allowed on the physical layer interface or "interface + VLAN".
	<code>Raisecom(config-portchannel)#igmp filter max-groups group-number [vlan vlan-list]</code>	Configure the maximum number of groups allowed to be added to an aggregation group interface or "interface + VLAN".
4	<code>Raisecom(config-port)#igmp filter max-groups action { drop replace } [vlan vlan-list]</code>	(Optional) configure actions to be taken when the number of physical layer interfaces or "interface + VLAN" groups exceeds the maximum number of groups.
	<code>Raisecom(config-portchannel)#igmp filter max-groups action { drop replace } [vlan vlan-list]</code>	(Optional) configure actions to be taken when the number of groups added to an aggregation group interface or "interface + VLAN" exceeds the maximum number.

12.5.5 Checking configurations

No.	Command	Description
1	<code>Raisecom#show igmp filter [interface interface-type interface-number [vlan vlan-id]]</code>	Show configurations of IGMP filtering.
2	<code>Raisecom#show igmp filter profile [profile-number]</code>	Show information about the IGMP Profile.

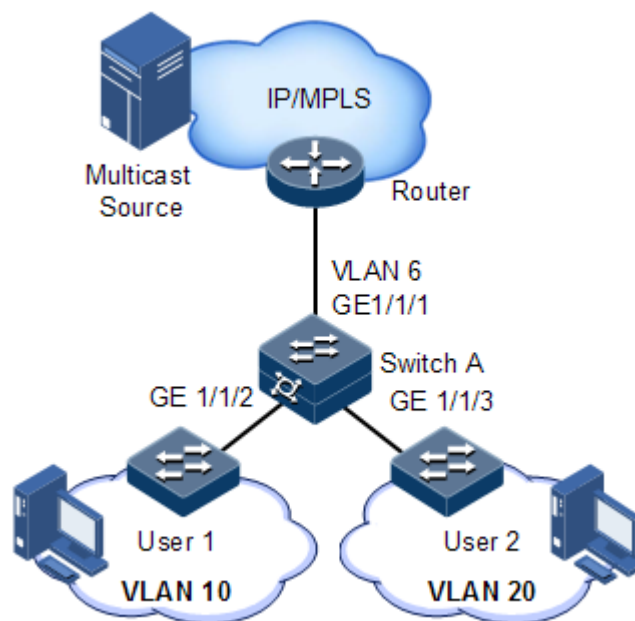
12.6 Configurng multicast VLAN copy

12.6.1 Preparing for configurations

Scenario

As shown in Figure 12-1, multiple hosts receive data from the multicast source, and multiple hosts belong to different VLANs. You can run multicast VLAN copy on Switch A, configure the multicast VLAN, and copy the multicast data to the user VLAN on the receiving interface, so that users in different VLANs share the same multicast VLAN to receive the same multicast data, and can also reduce bandwidth waste.

Figure 12-3 Multicast VLAN copy scenario



Prerequisite

Before configuring multicast VLAN copy, perform the following task:

- Create a VLAN and add the corresponding interface to the VLAN.



Note

- When N: 1 VLAN conversion and VLAN copy are configured at the same time, you need to configure VLAN copy first, and then configure N: 1 VLAN mapping.
- When N: 1 VLAN conversion and PIM are configured at the same time, you need to configure PIM first, and then configure N: 1 VLAN mapping.

12.6.2 Configuring multicast VLAN copy

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#igmp vlan-copy	Enable global multicast VLAN copy.
3	Raisecom(config)#igmp vlan-copy mcast-vlan <i>vlan-id</i> group { <i>start-ip</i> [<i>end-ip</i>] any }	Configure the group address set of the multicast VLAN. Note After multicast VLAN copy 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 message will not be processed and the user cannot receive multicast streaming.

12.6.3 Configuring static multicast members of VLAN-Copy

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-port)#igmp vlan-copy mcast-vlan <i>vlan-id</i> static <i>ip-address</i> user-vlan <i>vlan-id</i>	Configure static multicast members of VLAN-Copy.



Note

- Multicast VLAN copy and IGMP MVR cannot be enabled at the same time in the same multicast VLAN, otherwise the configuration fails.
- Multicast VLAN copy and IGMP Snooping cannot be enabled simultaneously in the same multicast VLAN, otherwise the configuration fails.

12.6.4 Configuring VLAN-Copy user VLAN

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical interface configuration mode.
3	Raisecom(config-port)#igmp vlan-copy user-vlan <i>vlan-id</i>	Configure the user VLAN of multicast VLAN copy.

12.6.5 Checking configurations

No.	Command	Description
1	Raisecom#show igmp vlan-copy	Show related configurations of multicast VLAN copy.
2	Raisecom#show igmp vlan-copy <i>interface-type interface-number</i>	Show configurations of multicast VLAN copy on a specified interface.
3	Raisecom#show igmp vlan-copy member	Show multicast group members of multicast VLAN copy.
4	Raisecom#show igmp vlan-copy member <i>interface-type interface-number</i>	Show multicast group members of multicast VLAN copy on a specified interface.
5	Raisecom#show igmp vlan-copy member user-vlan <i>vlan-id</i>	Show multicast group members of multicast VLAN copy of the specified user VLAN.
6	Raisecom#show igmp vlan-copy vlan-group [mcast-vlan <i>vlan-id</i>]	Show the multicast VLAN and the bound address set of multicast VLAN copy.

12.7 Configuring PIM

12.7.1 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

12.7.2 Enabling PIM

Enabling IPv4 PIM

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#ip pim sparse-mode	Enable IPv4 PIM-SM on the interface. By default, PIM-SM is disabled on the interface.

Enabling IPv6 PIM

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#ipv6 pim sparse-mode	Enable IPv6 PIM-SM on the interface. By default, PIM-SM is disabled.

12.7.3 Configuring PIM domain DR election

Configuring IPv4 PIM domain DR

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#ip pim dr-priority <i>priority-value</i>	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.

Configuring IPv6 PIM domain DR

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

Step	Command	Description
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode.
3	<code>Raisecom(config-port)#ipv6 pim dr-priority priority-value</code>	In the IPv6-based PIM domain, configure the priority of interfaces participating in DR elections. By default, the DR priority on the interface is 1.

12.7.4 Configuring PIM domain RP election

Configuring IPv4-based PIM domain RP election

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router pim</code>	Enter IPv4 PIM configuration mode.
3	<code>Raisecom(config-router-pim6)#bsr-candidate interface-type interface-number [hash-mask-length [priority]]</code>	Configure the candidate election router of the PIM domain.
4	<code>Raisecom(config-router-pim6)#rp-candidate interface-type interface-number [group-policy acl-number]</code>	Configure the candidate RP parameter of the PIM domain.

Configuring IPv6-based PIM domain RP election

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ipv6 pim</code>	Enter IPv6-based PIM configuration mode.
3	<code>Raisecom(config-router-pim6)#bsr-candidate ipv6-address [hash-mask-length [priority]]</code>	Configure the candidate election router of the PIM domain.
4	<code>Raisecom(config-router-pim6)#rp-candidate ipv6-address [group-policy acl-number]</code>	Configure the candidate RP parameter of the PIM domain.

12.7.5 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 multicast source survival time. By default, the lifetime of a multicast source is 210s.
4	Raisecom(config-router-pim)#ssm-policy acl-number	Configure the SSM source address range. This configuration needs to be used in conjunction with IP ACL.

Configuring IPv6 multicast source

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)#source-lifetime interval	Configure the multicast source survival time. By default, the lifetime of a multicast source is 210s.
4	Raisecom(config-router-pim6)#ssm-policy acl-number	Configure the SSM source address range. This configuration needs to be used in conjunction with IP ACL.

12.7.6 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.

Step	Command	Description
3	<code>Raisecom(config-router-pim)#spt-threshold { traffic-rate infinity } [group-policy acl-number]</code>	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	<code>Raisecom(config-router-pim)#timer spt-switch interval</code>	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.

Configuring IPv6-based switching

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#router ipv6 pim</code>	Enter IPv6 PIM configuration mode.
3	<code>Raisecom(config-router-pim6)#spt-threshold { traffic-rate infinity } [group-policy acl-number]</code>	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	<code>Raisecom(config-router-pim6)#timer spt-switch interval</code>	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.

12.7.7 Checking configurations

No.	Command	Description
1	<code>Raisecom#show { ip ipv6 } pim bsr-router</code>	Show election router of the PIM domain.
2	<code>Raisecom#show { ip ipv6 } pim interface</code>	Show information about the PIM interface.
3	<code>Raisecom#show { ip ipv6 } pim routing-table</code>	Show information about the PIM routing table.
4	<code>Raisecom#show { ip ipv6 } pim rp</code>	Show RP information about the PIM.

No.	Command	Description
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.

12.7.8 Maintenance

Command	Description
Raisecom#clear { ip ipv6 } pim process	Reconfigure IPv4/IPv6 PIM multicast and clear PIM configurations on the current device.

12.8 Configuring MLD L2 multicast

12.8.1 Preparing for configurations

Scenario

The multicast technology that appeared in the IPv4 era effectively solved the problems of single-point transmission and multi-point reception, and realized efficient data transmission from point to multipoint in the network, which can greatly save network bandwidth and reduce network load. In IPv6 networks, the application of multicast technology has been further enriched and strengthened. The device establishes a forwarding table of multicast packets by listening to MLD packets, thereby managing and controlling the forwarding of multicast data packets, and forwarding the multicast data packets to the host that needs to receive the data.

Prerequisite

N/A

12.8.2 Configuring MLD basic function

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mld mrouter vlan <i>vlan-id</i> interface-type interface-number	Create a multicast router interface in the specified VLAN.
3	Raisecom(config)#mld ring interface-type interface-number	Enable MLD ring network forwarding on the interface.

Step	Command	Description
4	<pre>Raisecom(config)#interface interface-type interface-number Raisecom(config-port)#prtswtich Raisecom(config-port)#mld immediate-leave [vlan vlan-list] Raisecom(config-port)#exit</pre>	Enable MLD immediate leave on the interface or "interface + VLAN". If immediate leave is not enabled on the downstream interface, the routing interface will calculate the aging time according to the robust coefficient when it receives leave packets. The group timeout timer is set to GMI (Group Membership Interval), GMI = (robust-value * lastmember-queryinterval).
5	<pre>Raisecom(config)#mld report-suppression</pre>	(Optional) enable Report suppression. The device receives multiple report packets of the same group within a certain period of time, and only forwards one report packet to the routing port. Other packets will be suppressed.
6	<pre>Raisecom(config)#mld member-timeout { second infinite }</pre>	(Optional) configure the aging time of MLD members.
7	<pre>Raisecom(config)#mld version { 1 2 }</pre>	Configure the MLD version.

12.8.3 Configuring MLD Snooping

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#mld snooping</pre>	Enable MLD Snooping.
3	<pre>Raisecom(config)#mld snooping vlan vlan-list</pre>	(Optional) enable MLD Snooping in global VLAN.
4	<pre>Raisecom(config)#vlan vlan-id Raisecom(config-vlan)#mld snooping static ip-address [interface-type interface-number]</pre>	(Optional) configure the static members of MLD Snooping in VLAN mode.

12.8.4 Adjusting MLD performance

Configuring MLD Querier

Step	Command	Description
1	<pre>Raisecom#config</pre>	Enter global configuration mode.
2	<pre>Raisecom(config)#mld querier</pre>	Enable MLD querier.

Step	Command	Description
3	Raisecom(config)# mld source-ip <i>ip-address</i>	(Optional) configure the source IP address for MLD queriers to send Query packets.
4	Raisecom(config)# mld query-interval <i>period</i>	(Optional) configure the MLD query interval.
5	Raisecom(config)# mld query-max-response-time <i>period</i>	(Optional) configure the maximum response time of Query packets.
6	Raisecom(config)# mld last-member-query-interval <i>period</i>	(Optional) configure the interval for the last group member to send Query packets.
7	Raisecom(config)# mld robust-count <i>value</i>	Configure the MLD robust coefficient.
8	Raisecom(config)# mld proxy	Enable MLD Proxy.



Note

- If MLD Querier is not enabled, you can configure MLD Querier, including the source IP address, query of the interval, and the maximum response time for the sent Query packets, and the interval for the last member to send Query packets. When MLD Querier is enabled, these configurations take effect immediately.
- MLD proxy conflicts with MLD querier. MLD proxy conflicts with MLD report-suppression.

Configuring interface MLD robust coefficient

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode. By default, the interface is in Layer 3 router mode.
3	Raisecom(config-port)# ipv6 mld robustness-variable <i>value</i>	Configure the MLD robust coefficient on the interface. By default, the MLD robust coefficient is 2.

Configuring interface MLD query and response

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type interface-number</i>	Enter interface configuration mode. By default, the interface is in Layer 3 router mode.

Step	Command	Description
3	<code>Raisecom(config-port)#ipv6 mld query-max-response-time seconds</code>	Configure the maximum MLD query response time on the interface. By default, the maximum query response time is 12s.
4	<code>Raisecom(config-port)#ipv6 mld query-interval seconds</code>	Configure the general MLD query interval of the interface. By default, the general MLD query interval is 125s.
5	<code>Raisecom(config-port)#ipv6 mld last-member-query-interval seconds</code>	Configure the last member query interval of MLD on the interface. By default, the last member query interval is 1s.

Configuring immediate leave of multicast members

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter interface configuration mode. By default, the interface is in Layer 3 router mode.
3	<code>Raisecom(config-port)#ipv6 mld immediate-leave</code>	Enable immediate leave of MLD members. By default, it is disabled.

12.8.5 Configuring MLD filtering

Enabling MLD filtering globally

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#mld filter</code>	Enable global MLD filtering.



Note

When configuring the application of the MLD filter template or the maximum number of groups, you need to execute the **mld filter** command to enable MLD filtering globally.

Configuring MLD filtering template

The MLD filtering template can be applied to the interface or interface + VLAN.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#mld filter profile <i>profile-number</i>	Create a MLD profile and enter profile configuration mode.
3	Raisecom(config-mld-profile)# { permit deny }	Configure the action of the MLD profile.
4	Raisecom(config-mld-profile)#range <i>range-id start-ip-address [end-ip-address]</i>	Configure the IPv6 multicast address or range of access control.
5	Raisecom(config-mld-profile)#exit Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode or aggregation group configuration mode.
6	Raisecom(config-port)#mld filter profile <i>profile-number [vlan vlan-list]</i>	Apply the MLD filtering profile to the physical layer interface or interface + VLAN.
	Raisecom(config-portchannel)#mld filter profile <i>profile-number [vlan vlan-list]</i>	Apply the MLD filtering profile to the aggregation group interface or interface + VLAN.
	Raisecom(config-portchannel)#exit	



Note

By executing the **mld filter profile** *profile-number* command in interface configuration mode, you can apply the created MLD Profile to the specified interface. An MLD Profile can be applied to multiple interfaces, but each interface can only have one MLD Profile.

Configuring maximum number of groups

You can configure the maximum number of groups that can be joined by users. You can apply it to the interface or interface + VLAN.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode or aggregation group configuration mode.
3	Raisecom(config-port)#mld filter max-groups <i>group-number [vlan vlan-list]</i>	Configure the maximum number of groups allowed on the physical layer interface, aggregation group interface, or "interface + VLAN".
4	Raisecom(config-port)#mld filter max-groups action { drop replace } <i>[vlan vlan-list]</i>	(Optional) configure actions to be taken when the number of physical layer interfaces, aggregation group interfaces, or "interface + VLAN" groups exceeds the maximum number of groups.

12.8.6 Checking configurations

Step	Command	Description
1	Raisecom#show mld immediate-leave [<i>interface-type interface-number</i> port-channel port-channel-id]	Show configurations of MLD immediate leave.
2	Raisecom#show mld mrouter	Show information about MLD multicast router interface.
3	Raisecom#show mld snooping [vlan vlan-id]	Show configurations of MLD Snooping.
4	Raisecom#show mld snooping member [<i>interface-type interface-number</i> vlan vlan-id]	Show multicast group members of MLD Snooping.
5	Raisecom#show mld snooping member count [<i>interface-type interface-number</i> vlan vlan-id]	Show the number of multicast group members of MLD Snooping.
6	Raisecom#show mld statistics [<i>interface-type interface-number</i>]	Show MLD packet statistics.
7	Raisecom# show mld filter [interface gigaheternet interface-number [vlan vlan-id]]	Show configurations of MLD filtering.
8	Raisecom# show mld filter profile [<i>profile-number</i>]	Show configurations of the MLD filtering profile.
9	Raisecom#show mld configuration	Show MLD basic configurations.

12.8.7 Maintenance

Command	Description
Rasiecom#clear mld statistics [<i>interface-type interface-number</i>]	Clear MLD statistics.
Rasiecom#no mld member <i>interface-type interface-number</i>	Delete the multicast forwarding entries of a specified interface.

12.9 Configuring MLD L3 multicast

12.9.1 Configuring MLD basic functions on interface

Enabling MLD

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode. By default, the interface is in L3 router mode.
3	Raisecom(config-port)#ipv6 mld enable	Enable interface MLD. By default, interface MLD is disabled.

Configuring MLD version

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode. By default, the interface is in L3 router mode.
3	Raisecom(config-port)#ipv6 mld version { 1 2 }	Configure the MLD version on the interface. By default, the MLD version is version 2.

Statically joining multicast group

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode. By default, the interface is in L3 router mode.
3	Raisecom(config-port)#ipv6 mld static group <i>ipv6-address</i>	Configure the static multicast group members on the interface.

Configuring access control for multicast group and multicast source

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

Step	Command	Description
2	Raisecom(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)# ipv6 mld group-policy <i>acl-number</i>	Configure the range of multicast groups for interfaces to join.
4	Raisecom(config-port)# ipv6 mld source-ip-policy <i>acl-number</i>	Configure the source address range of the VOD of the interface.
5	Raisecom(config-port)# ipv6 mld limit <i>limit-number</i>	Configure the maximum number of multicast groups that an interface can join.

12.9.2 Adjusting MLD performance

Configuring MLD robustness coefficient

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)# ipv6 mld robustness-variable <i>value</i>	Configure the MLD robustness coefficient on the interface.

Configuring MLD query and response

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)# ipv6 mld query-max-response-time <i>value</i>	Configure the maximum MLD query response time on the interface.
4	Raisecom(config-port)# ipv6 mld query-interval <i>value</i>	Configure the general MLD query interval on the interface.
5	Raisecom(config-port)# ipv6 mld last-member-query-interval <i>value</i>	Configure the MLD last member query interval on the interface.

Configure immediate leave of multicast group members

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

Step	Command	Description
2	Raisecom(config)#interface interface-type interface-number	Enter interface configuration mode.
3	Raisecom(config-port)#ipv6 mld immediate-leave	Enable immediate leave of MLD members.

12.9.3 Checking configurations

No.	Command	Description
1	Raisecom#show ipv6 mld group [ipv6-address interface-type interface-number]	Show MLD group member relationship.
2	Raisecom#show ipv6 mld interface [interface-type interface-number]	Show MLD configurations on the interface.
3	Raisecom#show ipv6 mld statistics [interface-type interface-number]	Show MLD packet statistics on the interface.
4	Raisecom#show ipv6 mld mroute	Show the IPv6 multicast routing table.
5	Rasiecom#show ipv6 mld ssm-mapping group	Show mapping relationship.

12.9.4 Maintenance

Command	Description
Rasiecom#clear ipv6 mld group [ipv6-address interface-type interface-number]	Clear the MLD dynamic forwarding table.
Rasiecom#clear ipv6 mld statistics [interface-type interface-number]	Clear MLD statistics.
Rasiecom#clear ipv6 mfib statistics	Clear statistics of the IPv6 multicast forwarding table.

13 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 RFC2544
- Configuring Y.1564
- Configuring SLA test alarm
- Configuring interface loopback
- Configuring ULDP
- Maintenance

13.1 Configuring EFM

13.1.1 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.

13.1.2 Configuring EFM basic functions

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

Step	Command	Description
2	<code>Raisecom(config)#oam send-period period-ms timeout seconds</code>	(Optional) configure the OAM PDU delivery period and timeout. By default, the OAM PDU delivery time is 1s (the parameter is 10, $10 \times 100\text{ms} = 1\text{s}$) and the timeout is 5s.
3	<code>Raisecom(config)#interface gigaethernet interface-number</code>	Enter Layer 2 or 3 physical interface configuration mode.
4	<code>Raisecom(config-port)#oam { active passive }</code>	Configure the working mode of EFM. By default, it is passive.
5	<code>Raisecom(config-port)#oam enable</code>	Enable EFM OAM of the link. By default, it is enabled.

13.1.3 Configuring EFM active functions



Note

EFM active functions can be configured when the RAX711-C-R is in active mode.

(Optional) configuring RAX711-C-R 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 RAX711-C-R 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface gigaethernet interface-number</code>	Enter GE interface configuration mode.
3	<code>Raisecom(config-port)#oam remote-loopback</code>	Enable the interface to initiate remote loopback.
4	<code>Raisecom(config-port)#oam loopback timeout time</code>	(Optional) configure the timeout for the interface to initiate remote loopback. By default, it is 3s.
5	<code>Raisecom(config-port)#oam loopback retry times</code>	(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 RAX711-C-R supports getting OAM information and interface statistics.

Peer variable cannot be obtained unless EFM connection is established.

Step	Command	Description
1	<code>Raisecom#show oam peer oam-info [gigaethernet <i>interface-number</i>]</code>	Show OAM basic information about the peer device.
	<code>Raisecom#show oam peer [gigaethernet <i>interface-number</i>]</code>	

13.1.4 Configuring EFM passive functions



Note

The passive functions of EFM can be configured regardless of the RAX711-C-R is in active or passive mode.

(Optional) configuring RAX711-C-R 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface gigaethernet <i>interface-number</i></code>	Enter GE interface configuration mode.
3	<code>Raisecom(config)#oam loopback { ignore process }</code>	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.

13.1.5 Configuring link monitoring and fault indication

(Optional) configuring OAM link monitoring



Note

OAM link monitoring is used to detect and report link errors in different conditions. When detecting a fault on a link, the RAX711-C-R 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 <i>interface-number</i>	Enter GE interface configuration mode.
3	Raisecom(config-port)#oam errored-frame window <i>framewindow threshold</i> <i>framethreshold</i>	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 <i>frameperiodwindow threshold</i> <i>frameperiodthreshold</i>	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 <i>framesecswindow threshold</i> <i>framesecsthreshold</i>	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 <i>symperiodwindow threshold</i> <i>symperiodthreshold</i>	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.

(Optional) configuring OAM fault indication

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

Step	Command	Description
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. By default, it is disabled.
5	Raisecom(config-port)#oam peer event trap { enable disable }	Enable OAM Trap of peer OAM link events. By default, it is disabled.

13.1.6 Configuring extended OAM

Both Layer 2 and Layer 3 interfaces on the RAX711-C-R support extended OAM.
Configuring OAM on Layer 3 interface does not affect configurations of its sub-interfaces.

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)#oam enable	Enable OAM on the interface.
4	Raisecom(config-port)#oam { active passive }	Configure the working mode of OAM. By default, it is passive.
5	Raisecom(config-port)#remote-device	Enter remote configuration mode.
6	Raisecom(config-remote)#hostname hostname	Configure the host name of the remote device.
7	Raisecom(config-remote)#ip address ip-address [ip-mask] [vlan-id]	Configure the IP address of the remote device.  Note • We recommend that you not use this command together with zero-configuration, because it may cause the remote device out of control. • When the remote device is an IP RAN device, its IP address should be configured on interface Loopback 1. If you configure the management VLAN ID, the sub-interface (the parent interface is enabled with OAM) will use the IP address of interface Loopback 1, otherwise, it will not. • When the remote device is a PTN device, you should configure its IP address on IP interface 0. If you configure the management VLAN ID, the VLAN will be associated with IP interface 0.



Note

After entering remote configuration mode, you can show the command list supported by the remote device by using the **list** command. Then you can manage the remote device by using those commands. For example:

- Use the `snmp-server community` command to configure the network management for the remote device.
- Use the `switch-mode dot1q-vlan native-vlan` command to configure VLAN for the remote device.
- Use the `reboot` command to reboot the remote device.
- Use the `erase` command to delete configuration files from the remote device.

There are multiple commands available for you to monitor and manage the remote device through extended OAM. They are not listed here one by one, and you can use them as required. Using some commands remotely on the remote device has the same effect as using these commands locally on the remote device.

13.1.7 Checking configurations

No.	Command	Description
1	<code>Raisecom#show oam [interface-type interface-number]</code>	Show configurations of OAM basic functions.
2	<code>Raisecom#show oam event [interface-type interface-number] [critical]</code>	Show local OAM link events.
3	<code>Raisecom#show oam loopback [interface-type interface-number]</code>	Show OAM remote loopback configurations.
4	<code>Raisecom#show oam notify [interface-type interface-number]</code>	Show OAM notification configurations.
5	<code>Raisecom#show oam peer event [interface-type interface-number] [critical]</code>	Show information about OAM peer events.
6	<code>Raisecom#show oam peer link-statistic [interface-type interface-number]</code>	Show peer OAM link statistics.
7	<code>Raisecom#show oam statistics [interface-type interface-number]</code>	Show OAM statistics.
8	<code>Raisecom#show oam trap [interface-type interface-number]</code>	Show OAM Trap information.

13.2 Configuring CFM

13.2.1 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)
- Ethernet lock signal (Lock, LCK)
- 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.

13.2.2 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, it does not affect enabling/disabling EFM on the interface.
- 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 disabled.
3	Raisecom(config)#interface gigaethernet interface-number	Enter GE interface configuration mode.
	Raisecom(config-port)#portswitch	Switch the interface to L2 switching mode.
4	Raisecom(config-port)#ethernet cfm enable	Enable CFM on the interface. By default, it is disabled.

13.2.3 Configuring CFM basic functions

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

Step	Command	Description
2	<code>Raisecom(config)#ethernet cfm domain [md-name domain-name] level md-level</code>	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. • Do not support configuring Y.1731 and 802.1ag CFM concurrently. • If the MD name is specified, it must be globally unique. • Levels of different MDs must be different.
3	<code>Raisecom(config)#service instance-name level md-level</code>	Create a service instance and enter service instance configuration mode.
4	<code>Raisecom(config-service)#service vlan-list vlan-list [primary vlan-id]</code>	Configure the VLAN related to the MA.
5	<code>Raisecom(config-service)#service mep [up down] mpid mep-id [interface-type interface-number] [priority value]</code>	Configure the MEP based on service instance. Before configuring MEP, relating the service instance to the VLAN.
6	<code>Raisecom(config-service)#service remote-mep mep-list interface-type interface-number</code>	Add static remote MEP of the service instance manually.  Note 802.1ag down MEP needs to manually add the remote MEP and specify the interface. It fails to find the remote MEP automatically.
7	<code>Raisecom(config-service)#service suppress-alarms enable mep { mep-list all }</code>	Enable alarm inhibition. By default, it is enabled.

13.2.4 Configuring fault detection

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ethernet cfm errors archive-hold-time minutes</code>	(Optional) configure the archive-hold time of error CCMs. By default, it is 100min.
3	<code>Raisecom(config)#service instance-name instance-name level md-level</code>	Enter service instance configuration mode.

Step	Command	Description
4	<code>Raisecom(config-service)#service cc interval { 3ms 10ms 100ms 1 10 60 600 }</code>	(Optional) configure the delivery period of CCMs.
5	<code>Raisecom(config-service)#service cc enable mep { mep-list all }</code>	Enable MEP to send CCMs.
6	<code>Raisecom(config-service)#service cvlan vlan-id</code>	(Optional) configure the CVLAN of the MA.
7	<code>Raisecom(config-service)#service priority priority</code>	(Optional) configure the priority of CFM OAM packets. By default, it is 7.

13.2.5 Configuring fault acknowledgement

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#service instance-name level md-level</code>	Enter service instance configuration mode.
3	<code>Raisecom(config-service)#ping mac-address [count count-number] [size size] [source mep-id] [timeout time] [padding { null null-crc prbs prbs-crc }]</code> <code>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 }]</code>	Perform Layer 2 Ping for acknowledging faults. By default, 3 LBMs are sent. The TLV length of a packet is 64. The RAX711-C-R automatically looks for an available source MEP.  Note To perform Ping MEP operation, 802.1ag down MEP needs to be configured with the static remote MAC address.
4	<code>Raisecom(config-service)#ping ethernet multicast [size size] [timeout time] [padding { null null-crc prbs prbs-crc }]</code>	Perform Layer 2 multicast Ping for acknowledging faults.



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, Ping operation will fail because of failing to find source MEP.
- 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.

- 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.
- Ping operation will fail if other users are using the specified source MEP to perform 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.

13.2.6 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] Raisecom(config- service)#traceroute mep mep-id [ttl ttl] [source mep-id] [interface-mode] [timeout time size size-value]	Perform Layer 2 Traceroute for locating faults. By default, the TLV length of a packet is 64. The RAX711-C-R automatically looks for an available source MEP.  Note To perform Traceroute MEP operation, 802.1ag down MEP needs to be configured with the static remote MAC address.
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.
- If there is no MEP in a service instance, Traceroute operation will fail because of failing to find source MEP.
- 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.
- 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.
- Traceroute operation will fail if other users are using the specified source MEP to perform Traceroute operation.

13.2.7 Configuring AIS

- Configure AIS on server devices.

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 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.

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.

13.2.8 Configuring LCK

Configuring LCK on server-layer devices

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 lck level md-level [vlan vlan-id]	Configure the level for sending the LCK packet. The level must be higher than the service instance level. By default, the level of the MIP is used, which is higher than the MEP level, to send the LCK packet.
5	Raisecom(config-service)#service lck period { 1 60 }	(Optional) configure the LCK packet delivery period. By default, it is 1s.
6	Raisecom(config-service)#service lck start mep { mep-list all }	Configure the MEP to send the LCK packet. By default, the MEP does not send the LCK packet.

Configuring LCK on client-layer devices

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.

13.2.9 Configuring CSF

- Configure LCK on server devices.

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.

Step	Command	Description
3	Raisecom(config)# service <i>instance-name level md-level</i>	Enter service instance configuration mode.
4	Raisecom(config-service)# service csf period { 1 60 }	(Optional) configure the CSF packet delivery period. By default, the CSF packet delivery period is 1s.
5	Raisecom(config-service)# service csf enable mpid <i>mep-id</i>	Enable the MEP to send the LCK packet.
6	Raisecom(config-service)# service csf trap enable	(Optional) enable CSF Trap.

13.2.10 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 ais [<i>level md-level</i>] [<i>source</i>]	Show AIS information.  Note 802.1ag MDs do not support AIS.
4	Raisecom# show ethernet cfm domain [<i>level md-level</i>]	Show MD configurations.
5	Raisecom# show ethernet cfm errors [<i>level md-level</i>]	Show error CCM information.
6	Raisecom# show ethernet cfm lck [<i>level md-level</i>] [<i>source</i>]	Show LCK information.  Note The 802.1ag MDs do not support LCK.
7	Raisecom# show ethernet cfm local-mp [<i>interface interface-type interface-number</i>] Raisecom# show ethernet cfm local-mp [<i>level md-level</i>]	Show local MEP configurations.
8	Raisecom# show ethernet cfm remote-mep [<i>level md-level</i>] [<i>service instance-name instance-name</i>] [<i>mpid mep-id</i>] []	Show remote MEP configurations.
9	Raisecom# show ethernet cfm remote-mep static [<i>level md-level</i>]	Show remote static MEP configurations.
10	Raisecom# show ethernet cfm traceroute-cache	Show information about routes in the LinkTrace cache.

13.3 Configuring BFD

13.3.1 Preparing for configurations

Scenario

To reduce effect of faults on the device and improve network availability, the RAX711-C-R 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.

13.3.2 Configuring BFD for IP

Creating BFD for IP sessions

When you create the BFD binding:

- 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#bfd session-id bind peer-ip ip-address [source-ip ip-address]</code>	Create multi-hop routes of BFD session detection and enter BFD session mode. You must configure the source IP address when creating a multi-hop session.
3	<code>Raisecom(config)#bfd session-id bind peer-ip ip-address interface interface-type interface-number</code>	Create a single-hop route of static BFD session detection, bind Layer 3 physical interface, sub-interface, VLAN interface or Layer 3 LAG interface, and enter BFD session mode.

Configuring BFD session parameters

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

Step	Command	Description
2	<code>Raisecom(config)#bfd session-id</code>	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	<code>Raisecom(config-bfd- session)#description description</code>	Configure descriptions of the BFD session.
4	<code>Raisecom(config-bfd- session)#local discriminator value</code>	(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	<code>Raisecom(config-bfd- session)#min send- interval interval</code>	Configure the minimum delivery interval of the BFD session. By default, it is 10ms.
6	<code>Raisecom(config-bfd- session)#min receive- interval interval</code>	Configure the minimum receiving interval of the BFD session. By default, it is 10ms.
7	<code>Raisecom(config-bfd- session)#detect- multiplier multiplier</code>	Configure the local detection times of the BFD session. By default, it is 3 times.
8	<code>Raisecom(config-bfd- session)#remote discriminator value</code>	(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	<code>Raisecom(config-bfd- session)#session enable</code>	Enable BFD session. By default, it is disabled.
10	<code>Raisecom(config-bfd- session)#vid vlan-id</code>	Configure the VLAN ID of Default-IP session packets.

13.3.3 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 13.3.2 Configuring BFD for IP.

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.
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.

13.3.4 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 13.3.2 Configuring BFD for IP.

13.3.5 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.

13.3.6 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.
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.
	Raisecom#show bfd [sessionid] diagnostic-code	Show the diagnostic code of BFD session.

13.4 Configuring SLA

13.4.1 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 iTN 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 RAX711-C-R, note the following matters:

- Up to 16 operations can be configured and scheduled concurrently.
- Before scheduling a 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.
- Up to 20 detections are available for one test and up to 5 pieces of statistics records are shown.

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.
- When you configure Layer 3 tests (icmp-echo and icmp-jitter), Layer 3 Ping operation succeeds between local and remote devices.

13.4.2 Configuring Y.1731-based SLA

When conducting delay test based on Ethernet, LSP, and PW, you can conduct delay compensation according to the interface rate and packet length, obtaining a delay/jitter value close to the actual value. This function can be user-defined.

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] 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 the Y1731-echo delay test based on destination MEP ID.
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] 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.

Configuring SLA packet loss test

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

Step	Command	Description
2	<code>Raisecom(config)#sla oper-num y1731 pkt-loss remote-mep mep-id level level svlan vlan-id [cvlan cvlan-id] [cos cos-value] [interval interval-num] size size-value] slm</code>	Configure the Y1731 packet loss test operation according to the destination MEP ID.  Note When testing the packet loss rate according to the MEP ID, it is recommended that the user specify the MAC address when using the service remote-mep command to configure the remote MEP.
3	<code>Raisecom(config)#sla oper-num y1731 pkt-loss remote-mac mac-address level level svlan vlan-id [cvlan cvlan-id] [cos cos-value] [interval interval-num] size size-value] slm</code>	Configure the Y1731 packet loss test operation according to the destination MAC address.



Note

- After configuring one operation (differed by operation ID), you cannot modify or configure it again. You need to delete the operation in advance if you need to configure it again.
- SLA supports scheduling up to 16 operations at a time. Before you stop scheduling the same operation, you cannot modify scheduling information or re-schedule the operation. If you need to reschedule the operation, you need to finish the scheduling (reach scheduling life time or stop scheduling) before performing the next scheduling.
- When configuring LSP-based SLA operation, note the name of lsp-ingress (LSP Ingress node) is the one of the LSP Ingress node for creating the LSP and the name of the LSP Egress node is the one of the LSP Egress node for creating the LSP.

Enabling SLA packets to encapsulate TLV

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#sla private-tlv enable</code>	Enable SLA test packets to encapsulate private TLV.

13.4.3 Configuring SLA operation scheduling

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

Step	Command	Description
2	<code>Raisecom(config)#sla schedule { oper-num all } [life { forever lifetime }] [period second] [begin]</code>	Configure SLA scheduling information, including the lifetime period and executive interval, and enable SLA operation scheduling. By default, SLA operation scheduling is disabled.



Note

- The operation lifetime should not be shorter than the interval for scheduling the SLA operation.
- The interval for scheduling the SLA operation should not be shorter than 20s.

13.4.4 Checking configurations

No.	Command	Description
1	<code>Raisecom#show sla</code>	Show SLA global information.
2	<code>Raisecom#show sla { all oper-num } configuration</code>	Show information about SLA operation.
3	<code>Raisecom#show sla { all oper-num } result { current-interval current-period history-period latest-period tests }</code>	Show test information about the operation.
4	<code>Raisecom#show sla { all oper-num } threshold</code>	Show threshold alarms of operation scheduling.

13.5 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.

13.5.1 Configuring type of test packets

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#sla pkt-type eth dest-mac mac-address [cvlan vlan-id] [cos cos] [cfi cfi-value] [svlan vlan-id] [tpid tpid-value] [cos cos] [cfi cfi-value]</code>	Configure the type of SLA test packets.

Step	Command	Description
	<pre>Raisecom(config)#sla pkt-type ipv4 dest-ip ip-address [source-ip ip-address] [dest-udp-port port-id] [source-udp-port port-id] [tc tc] [cvlan vlan-id [cos cos]] [svlan vlan-id [cos cos]] [ttl ttl]</pre>	

13.5.2 Configuring RFC2544 delay test

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#sla oper-num rfc2544 latency interface { interface-type interface-number port-channel port- channel } eth dest-mac mac-address [cos cos] [cvlan vlan-id] [svlan vlan-id] [pkt-size pkt-size] [rate rate]</pre>	Configure the delay test operation of a specified destination MAC address.
3	<pre>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]</pre>	Configure the delay test operation of a specified destination IP address.
4	<pre>Raisecom(config)#sla oper-num rfc2544 latency interface interface-type interface-number [pkt-size pkt-size] [rate rate]</pre>	Configure the delay test operation. You need to pre-configure the type of SLA test packets before using this command to configure the delay test operation.

13.5.3 Configuring RFC2544 packet loss test

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	<pre>Raisecom(config)#sla oper-num rfc2544 pkt-loss interface { interface-type interface-number port- channel port-channel } eth dest-mac mac-address [cvlan vlan-id] [svlan vlan-id] [cos cos] [pkt-size pkt-size] [rate rate]</pre>	Configure the packet loss test operation of a specified destination MAC address.

Step	Command	Description
3	Raisecom(config)#sla oper-num rfc2544 pkt-loss interface { interface-type interface-number port-channel port-channel } 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 port-channel port-channel } [pkt-size pkt-size] [rate rate]	Configure the packet loss test operation.

13.5.4 Configuring RFC2544 throughput test

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#sla oper-num rfc2544 throughput interface { interface-type interface-number port-channel port-channel } 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 port-channel port-channel } { 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 port-channel port-channel } [pkt-size pkt-size] [threshold threshold]	Configure the throughput test operation.

13.5.5 Configuring RFC2544 operation scheduling

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#sla schedule { oper-num all } [life { forever lifetime }] [period second] [begin]	Enable the RFC2544 test operation scheduling, and configure the operation lifetime and the execution interval. By default, the scheduling is disabled.

13.5.6 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	Show the latest test of the operation.

13.6 Configuring Y.1564



Note

In the MPLS network environment, both the initiating end and the loopback end of the Y.1564 test are PE devices, which are responsible for encapsulating and decapsulating Y.1564 test packets. The test process is as below:

- The initiating PE encapsulates the Y.1564 test packet into a PW packet and forwards it to the loopback PE in the MPLS network.
- After receiving the PW packet, the loopback PE decapsulates the packet and restores it to the Y.1564 test packet.
- After the Y.1564 test packet exchanges source and destination IP addresses, and source and destination MAC addresses at the loopback PE, it is encapsulated as a PW packet again.
- The PW packet is forwarded to the initiating PE through the MPLS network, decapsulated, and restored to the Y.1564 test packet.
- The initiating PE collects and processes the test packets and completes the Y.1564 test.

13.6.1 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.

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 profile 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 fix pkt-size	Configure a fixed length for test packets. This configuration is not available for video services and voice services.
8	Raisecom(config-y1564-thrgh-ip)# pkt-size-mode { fix increase random }	Configure the length mode of test packets. By default, it is fix.
9	Raisecom(config-y1564-thrgh-ip)# pkt-size-range pkt-size-1 pkt-size-2	Configure the change range of the test packet length.
10	Raisecom(config-y1564-thrgh-ip)# frame-pattern { null prbs }	Configure the frame mode.
11	Raisecom(config-y1564-thrgh-ip)# bandwidth { enable disable }	Enable bandwidth limit.
12	Raisecom(config-y1564-thrgh-ip)# cir cir-value cbs cbs-value	Configure the CIR and CBS.
13	Raisecom(config-y1564-thrgh-ip)# eir eir-value ebs ebs-value	Configure the EIR and EBS.
14	Raisecom(config-y1564-thrgh-ip)# mode { eir overload }	Configure the traffic mode. There is no EIR configuration and Overload configuration is unavailable.
15	Raisecom(config-y1564-thrgh-ip)# smac mac-address	Configure the source MAC address.
16	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.
17	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.

Step	Command	Description
18	Raisecom(config-y1564-thrgh-ip)#swap-udp-port { enable disable }	Enable swapping the source UDP port.
19	Raisecom(config-y1564-thrgh-ip)#tc tc-value	Configure the TC.
20	Raisecom(config-y1564-thrgh-ip)#ttl ttl-value	Configure the TTL.
21	Raisecom(config-y1564-thrgh-ip)#interface-role { uni nni }	Configure the role of the interface which initiates the test. By default, the interface is an UNI.
22	Raisecom(config-y1564-thrgh-ip)#nexthop-ip ip-address	Configure the next-hop IP address.
23	Raisecom(config-y1564-thrgh-ip)#group-id group-id	Configure the group ID.

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-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)#service-tpid tpid-value	Configure the SVLAN TPID.
6	Raisecom(config-y1564-thrgh-ip)#service-cfi cfi-value	Configure the SVLAN CFI.
7	Raisecom(config-y1564-thrgh-ip)#cvlan vlan-id	Configure the CVLAN ID.
8	Raisecom(config-y1564-thrgh-ip)#customer-cos cos-value	Configure the CVLAN CoS.
9	Raisecom(config-y1564-thrgh-ip)#customer-tpid tpid-value	Configure the CVLAN TPID.
10	Raisecom(config-y1564-thrgh-ip)#customer-cfi cfi-value	Configure the CVLAN CFI.
11	Raisecom(config-y1564-thrgh-ip)#frame-pattern { null prbs }	Configure the frame mode.

Step	Command	Description
12	<code>Raisecom(config-y1564-thrgh-ip)#cir <i>cir-value</i> cbs <i>cbs-value</i></code>	Configure the CIR and CBS.
13	<code>Raisecom(config-y1564-thrgh-ip)#eir <i>eir-value</i> ebs <i>ebs-value</i></code>	Configure the EIR and EBS.
14	<code>Raisecom(config-y1564-thrgh-ip)#mode { eir overload }</code>	Configure the traffic mode.
15	<code>Raisecom(config-y1564-thrgh-ip)#group-id <i>group-id</i></code>	Configure the group ID.
16	<code>Raisecom(config-y1564-thrgh-ip)#interface- role { uni nni }</code>	Configure the role of the interface which initiates the test. By default, the interface is an UNI.
17	<code>Raisecom(config-y1564-thrgh-ip)#pkt-size-mode { fix increase random }</code>	Configure the length mode of test packets.
18	<code>Raisecom(config-y1564-thrgh-ip)#pkt-size- range <i>pkt-size-1</i> <i>pkt-size-2</i></code>	Configure the change range of the test packet length.
19	<code>Raisecom(config-y1564-thrgh-ip)#pkt-size fix <i>pkt-size</i></code>	Configure the fix length of test packets.
20	<code>Raisecom(config-y1564-thrgh-ip)#sla y1564 <i>oper-num</i></code>	Enter Y.1564 test operation profile configuration mode.

13.6.2 Configuring service performance test operation

Configuring IP service performance test operation

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#sla <i>oper-num</i> y1564 performance interface <i>interface-type</i> <i>interface-number</i> service-ipv4 dest-ip <i>ip-</i> <i>address</i> source-ip <i>ip-address</i> bandwidth <i>bandwidth-value</i> group-id <i>group-id</i></code>	Configure the performance test operation based on IP service and enter the profile configuration mode.
	<code>Raisecom(config)#sla <i>oper-num</i> y1564 performance interface <i>interface-type</i> <i>interface-number</i> service-video dest-ip <i>ip-</i> <i>address</i> source-ip <i>ip-address</i> bandwidth <i>bandwidth-value</i></code>	Configure the performance test operation based on video service and enter the profile configuration mode.
	<code>Raisecom(config)#sla <i>oper-num</i> y1564 performance interface <i>interface-type</i> <i>interface-number</i> service-voice dest-ip <i>ip-</i> <i>address</i> source-ip <i>ip-address</i> bandwidth <i>bandwidth-value</i></code>	Configure the performance test operation based on voice service and enter the profile configuration mode.

Step	Command	Description
	Raisecom(config)# sla y1564 oper-num	Enter Y.1564 test operation profile 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 fix pkt-size	Configure the fix length of the test packet. This configuration is not available for the video services and voice services.
8	Raisecom(config-y1564-perf-ip)# pkt-size-mode { fix increase random }	Configure the length mode of test packets. By default, it is fix.
9	Raisecom(config-y1564-perf-ip)# pkt-size-range pkt-size-1 pkt-size-2	Configure the change range of the test packet length.
10	Raisecom(config-y1564-perf-ip)# frame-pattern { null prbs }	Configure the frame mode.
11	Raisecom(config-y1564-perf-ip)# bandwidth { enable disable }	Enable bandwidth limit.
12	Raisecom(config-y1564-perf-ip)# mode { eir overload }	Configure the traffic mode. There is no EIR configuration and Overload configuration is unavailable.
13	Raisecom(config-y1564-perf-ip)# smac mac-address	Configure the source MAC address.
14	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.
15	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.
16	Raisecom(config-y1564-perf-ip)# swap-udp-port { enable disable }	Enable swapping the source UDP port.
17	Raisecom(config-y1564-perf-ip)# tc tc-value	Configure the TC.
18	Raisecom(config-y1564-perf-ip)# ttl ttl-value	Configure the TTL.
19	Raisecom(config-y1564-perf-ip)# interface-role { uni nni }	Configure the role of the interface which initiates the test. By default, the interface is an UNI.

Step	Command	Description
20	<code>Raisecom(config-y1564-perf-ip)#nexthop-ip ip-address</code>	Configure the next-hop IP address.

Configuring Ethernet service performance test operation

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>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</code>	Configure the performance test operation based on Ethernet and enter the profile configuration mode.
	<code>Raisecom(config)#sla y1564 oper-num</code>	Enter Y.1564 test operation profile configuration mode.
3	<code>Raisecom(config-y1564-perf-eth)#svlan vlan-id</code>	Configure the SVLAN ID.
4	<code>Raisecom(config-y1564-perf-eth)#service-cos cos-value</code>	Configure the SVLAN CoS.
5	<code>Raisecom(config-y1564-perf-eth)#service-tpid tpid-value</code>	Configure the SVLAN TPID.
6	<code>Raisecom(config-y1564-perf-eth)#service-cfi cfi-value</code>	Configure the SVLAN CFI.
7	<code>Raisecom(config-y1564-perf-eth)#cvlan vlan-id</code>	Configure the CVLAN ID.
8	<code>Raisecom(config-y1564-perf-eth)#customer-cos cos-value</code>	Configure the CVLAN CoS.
9	<code>Raisecom(config-y1564-perf-eth)#customer-tpid tpid-value</code>	Configure the CVLAN TPID.
10	<code>Raisecom(config-y1564-perf-eth)#customer-cfi cfi-value</code>	Configure the CVLAN CFI.
11	<code>Raisecom(config-y1564-perf-eth)#frame-pattern { null prbs }</code>	Configure the frame mode.
12	<code>Raisecom(config-y1564-perf-eth)#group-id group-id</code>	Configure the group ID.
13	<code>Raisecom(config-y1564-perf-eth)#interface-role { uni nni }</code>	Configure the role of the interface which initiates the test. By default, the interface is an UNI.
14	<code>Raisecom(config-y1564-perf-eth)#pkt-size-mode { fix increase random }</code>	Configure the length mode of test packets.
15	<code>Raisecom(config-y1564-perf-eth)#pkt-size-range pkt-size-1 pkt-size-2</code>	Configure the change range of the test packet length.

Step	Command	Description
16	Raisecom(config-y1564-perf-eth)# pkt-size fix <i>pkt-size</i>	Configure the fix length of test packets.
17	Raisecom(config-y1564-perf-eth)# sla y1564 <i>oper-num</i>	Enter Y.1564 test operation profile configuration mode.

13.6.3 Configuring Y.1564 operation scheduling

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# sla schedule group-id <i>group-id</i> [life { <i>life-time</i> forever }] performance	Schedule the Y.1564 performance test operation.
3	Raisecom(config)# sla schedule group-id <i>group-id</i> [period <i>period</i>] throughput	Schedule the Y.1564 configuration test operation.
4	Raisecom(config)# sla schedule { <i>oper-num</i> all }	Schedule a certain or all Y.1564 test operations.

13.6.4 Checking configurations

No.	Command	Description
1	Raisecom# show sla	Check SLA global configurations.
2	Raisecom# show sla { all <i>oper-num</i> group-id <i>group-id</i> } configuration	Check Y.1564 operation configurations.
3	Raisecom# show sla { all <i>oper-num</i> } result	Show the latest test of a specified operation.
4	Raisecom# show sla group-id <i>group-id</i> result { performance throughput }	Show test results of the performance or configuration test operation group.
5	Raisecom# show sla group-id <i>group-id</i> result performance latest	Show five-minute test results of the performance test operation group.

13.7 Configuring SLA test alarm

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

Step	Command	Description
2	<code>Raisecom(config)#sla oper-num loss-rate-threshold { current average } [ds sd twoway] threshold</code>	Configure the packet loss alarm threshold. By default, it is 999999.
3	<code>Raisecom(config)#sla oper-num loss-pkt-trap { current average } enable</code>	Enable packet loss rate alarm. By default, it is disabled.
4	<code>Raisecom(config)#sla oper-num delay-threshold { current average } [ds sd two-way] threshold</code>	Configure the delay alarm threshold. By default, it is 5000000us.
5	<code>Raisecom(config)#sla oper-num delay-trap { current average } [ds sd two-way] enable</code>	Enable delay alarm. By default, it is disabled.

13.8 Configuring interface loopback

13.8.1 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.

13.8.2 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	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code> <code>Raisecom(config-port)#loopback external [access-list acl-number rc-sam] swap smac mac-address swap dmac- mac-address</code>	Enter interface configuration mode and enable interface loopback.
3	<code>Raisecom(config)#interface port-channel channel-number</code>	Enter link aggregation configuration mode and enable loopback on the link aggregation group

Step	Command	Description
	Raisecom(config-port-channel*)# loopback external [access-list <i>acl-number</i> rc-sam] swap smac <i>mac-address</i> swap dmac- <i>mac-address</i>	interface.

13.8.3 Configuring loopback duration

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type</i> <i>interface-number</i> Raisecom(config-port)# loopback timeout <i>minutes</i>	Enter interface configuration mode and configure the loopback duration.



Note

- The first 3 bytes of the destination MAC address cannot be configured to 0x0180C2.
- The source MAC address cannot be a multicast or broadcast MAC address.

13.8.4 Checking configurations

No.	Command	Description
1	Raisecom# show interface <i>interface-type</i> <i>interface-number</i>	Show interface status.
2	Raisecom# show loopback <i>interface-type</i> <i>interface-number</i>	Show configurations of the loopback interface.

13.9 Configuring ULDP

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# uldp enable	Enable ULDP. By default, ULDP is disabled.

Step	Command	Description
3	Raisecom(config)#uldp recovery-time <i>seconds</i>	Configure the ULDP recovery time. By default, the recovery time is 15s.
4	Raisecom(config)#show uldp	Show ULDP configurations.
5	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
6	Raisecom(config-port)#uldp enable	Enable ULDP.

13.10 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 [<i>level md-level</i>]	Clear error CCM records.
Raisecom(config)#clear ethernet cfm remote-mep [<i>level md-level</i>]	Clear information about discovered remote MEPs.
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)#clear cfm suppress-alarm source	Clear alarm inhibition information about MPLS-TP MEPs.

14 Security

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

- Configuring storm control
- Configuring CPU protection
- Configuring CPU monitoring
- Configuring RADIUS
- Configuring TACACS+
- Configuring RADIUS/TACACS+ accounting management
- Configuring interface isolation
- Configuring port mirroring
- Configuring PPPoE+
- Configuring dynamic ARP inspection

14.1 Configuring storm control

14.1.1 Preparing for configurations

Scenario

In the Layer 2 network, after storm control is configured, it can inhibit 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.

14.1.2 Configuring storm control

Configuring storm control on physical interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#storm-control { broadcast unknown-multicast d1f all } enable	Enable storm control. By default, storm control of broadcast packets, unknown multicast packets, and unknown unicast packets is disabled.
4	Raisecom(config-port)#storm-control mode { kpps pps ratio }	Configure the storm control mode to kpps.
5	Raisecom(config-port)#storm-control { broadcast unknown-multicast d1f } { kpps <i>kpps-value</i> pps <i>pps-value</i> ratio <i>ratio-value</i> } [burst <i>burst-value</i>]	Configure the rate limiting threshold of storm control.



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.

14.1.3 Checking configurations

No.	Command	Description
1	Raisecom#show storm-control interface [<i>interface-type interface-number</i>]	Show storm control configurations.

14.2 Configuring CPU protection

14.2.1 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

14.2.2 Configuring global CPU CAR

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#cpu-protect car type { arp bpdu dhcp icmp igmp mld ndp oam } queue queue-id	Configure the protocol binding queue of CPU protection.
3	Raisecom(config)#cpu-protect car global kbps cir cir cbs cbs	Configure the rate limiting mode of global CPU packet protection.
4	Raisecom(config)#cpu-protect car queue queue-id kbps cir cir cbs cbs	Configure the rate limiting mode of CPU protection queue.

14.2.3 Clear statistics

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#clear cpu-protect car global statistics	Clear statistics about 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.

14.2.4 Checking configurations

No.	Command	Description
1	Raisecom#show cpu-protect car statistics	Show CPU CAR statistics.

14.3 Configuring CPU monitoring

14.3.1 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 RAX711-C-R, that is, the IP address of the network management system.

14.3.2 Configuring CPU monitoring alarm

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)# cpu threshold recovering <i>recovering-threshold- value</i> rising <i>rising-threshold- value</i>	Configure the CPU alarm rising threshold and recovery threshold.
3	Raisecom(config)#cpu interval <i>interval-value</i>	(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 history { 10min 1min 2hour 5sec }	
6	Raisecom#show process [dead sorted { priority name } <i>taskname</i>]	Show status of each task.
7	Raisecom#show process cpu [sorted [10min 1min 5sec invoked]]	

14.4 Configuring RADIUS

14.4.1 Preparing for configurations

Scenario

To control users accessing devices and network, you can deploy the RADIUS server at the network to authenticate and account users. The RAX711-C-R can be used as a Proxy of the RADIUS server to authenticate users based on results returned by the RADIUS server.

Prerequisite

N/A

14.4.2 Configuring IPv4 RADIUS authentication

Step	Command	Description
1	Raisecom#radius [backup] <i>ip-address</i> [auth-port <i>port-id</i>]	Specify the IP address and port ID of the RADIUS authentication server. The backup parameter is used to specify a backup RADIUS authentication server.
2	Raisecom#radius-key <i>string</i>	Configure the shared key of the RADIUS authentication server.
3	Raisecom#radius-encrypt-key <i>string</i>	Configure the shared ciphertext key of the RADIUS authentication server.
4	Raisecom#radius backup key <i>string</i>	Configure the shared key of the backup RADIUS authentication server.
5	Raisecom#radius backup encrypt-key <i>string</i>	Configure the ciphertext shared key of the backup RADIUS authentication server.
6	Raisecom#radius response-timeout <i>seconds</i>	(Optional) configure the response timeout time of the RADIUS server.
7	Raisecom#radius authentication fail trap enable	Enable authentication failure alarm reporting.

14.4.3 Configuring IPv6 RADIUS authentication

Step	Command	Description
1	Raisecom#radius [backup] <i>ipv6-address</i> [auth-port <i>port-id</i>]	Specify the IPv6 address and authentication interface ID of the RADIUS authentication server. Configure the backup parameter to specify the backup RADIUS authentication server.
3	Raisecom#radius-key <i>string</i>	Configure the shared key of the RADIUS authentication server.
4	Raisecom#radius-encrypt-key <i>string</i>	Configure the ciphertext shared secret key of the RADIUS authentication server.
5	Raisecom#radius backup key <i>string</i>	Configure the shared key of the backup RADIUS authentication server.
6	Raisecom#radius backup encrypt-key <i>string</i>	Configure the ciphertext shared secret key of the backup RADIUS authentication server.
7	Raisecom#radius response-timeout <i>seconds</i>	(Optional) configure the response timeout time of the RADIUS server.
8	Raisecom#radius authentication fail trap enable	Enable alarm reporting for authentication failure.

Step	Command	Description
1	Raisecom#radius [backup] ipv6-address [auth-port port-id]	Specify the IPv6 address and authentication interface ID of the RADIUS authentication server. Configure the backup parameter to specify the backup RADIUS authentication server.

14.4.4 Configuring IPv4 RADIUS accounting

Step	Command	Description
1	Raisecom#radius [backup] accounting-server ip-address [acct-port port-id]	Specify the IP address and accounting interface ID of the RADIUS accounting server. By default, the interface ID is 1813. Configure the backup parameter to specify the backup RADIUS accounting server.
2	Raisecom#radius accounting-server key string	Configure the shared key to communicate with the RADIUS accounting server.
3	Raisecom#radius accounting-server encrypt-key string	Configure the encrypted shared key to communicate with the RADIUS accounting server.
4	Raisecom#radius authorization no-privilege { offline priority-value }	Configure the processing policy for accounting authorization failure. • offline: force offline. If the authorization fails, the user is forced to go offline. • priority-value: user priority. If authorization fails, the user uses the specified priority.

14.4.5 Configuring IPv6 RADIUS accounting

Step	Command	Description
1	Raisecom#radius [backup] accounting-server ipv6-address [acct-port port-id]	Specify the IPv6 address and accounting interface ID of the RADIUS accounting server. By default, the interface ID is 1813. Configure the backup parameter to specify the backup RADIUS accounting server.
2	Raisecom#radius accounting-server key string	Configure the shared key to communicate with the RADIUS accounting server.
3	Raisecom#radius accounting-server encrypt-key string	Configure the encrypted shared key to communicate with the RADIUS accounting server.
4	Raisecom#radius authorization no-privilege { offline priority-value }	Configure the processing policy for accounting authorization failure. • offline: force offline. If the authorization fails, the user is forced to go offline. • priority-value: user priority. If authorization fails, the user uses the specified priority.

14.4.6 Checking configurations

No.	Command	Description
1	Raisecom# show radius-server	Show configurations of the RADIUS server.

14.5 Configuring TACACS+

14.5.1 Preparing for configurations

Scenario

To control users accessing devices and network, you can deploy the RADIUS server on the network to authenticate and account users. Compared with RADIUS, TACACS+ is more secure and reliable. The RAX711-C-R can be used as a Proxy of the TACACS+ server to authenticate users based on results returned by the TACACS+ server.

Prerequisite

N/A

14.5.2 Configuring IPv4 TACACS+ authentication

Step	Command	Description
1	Raisecom# tacacs-server [backup] <i>ip-address</i> [auth-port <i>port-id</i>]	Specify the IP address and port ID of the TACACS+ authentication server. The backup parameter is used to specify a backup TACACS+ authentication server.
2	Raisecom# tacacs-server [backup] key <i>string</i>	Configure the shared key of TACACS+ authentication. The backup parameter refers to the backup server.
3	Raisecom# tacacs-server [backup] encrypt-key <i>string</i>	Configure the ciphertext shared key of the TACACS+ authentication server. The backup parameter refers to the backup server.

14.5.3 Configuring IPv6 TACACS+ authentication

Step	Command	Description
1	Raisecom# tacacs-server [backup] <i>ipv6-address</i> [auth-port <i>port-id</i>]	Specify the IPv6 address of the TACACS+ authentication server. Configure the backup parameter to specify the backup TACACS+ authentication server.

Step	Command	Description
2	Raisecom# tacacs-server key <i>string</i>	Configure the shared key of TACACS+ authentication.
3	Raisecom# tacacs-server [backup] key <i>string</i>	Configure the shared key of TACACS+ authentication. The backup parameter refers to the backup server.
4	Raisecom# tacacs-server [backup] encrypt-key <i>string</i>	Configure the ciphertext shared key of the TACACS+ authentication server. The backup parameter refers to the backup server.

14.5.4 Configuring IPv4 TACACS+ accounting

Step	Command	Description
1	Raisecom# tacacs [backup] accounting-server <i>ip-address</i>	Configure the IPv4 address of the TACACS+ accounting server. Select the backup parameter to configure the IP address of the backup server.
2	Raisecom# tacacs accounting-server key <i>string</i>	Configure the shared key for communicating with the TACACS+ accounting server.
4	Raisecom# tacacs accounting-server encrypt-key <i>string</i>	Configure the encrypted shared key for communicating with the TACACS+ accounting server.

14.5.5 Configuring IPv6 TACACS+ accounting

Step	Command	Description
1	Raisecom# tacacs [backup] accounting-server <i>ipv6-address</i>	Configure the IPv6 address of the TACACS+ accounting server. Select the backup parameter to configure the IP address of the backup server.
2	Raisecom# tacacs accounting-server key <i>string</i>	Configure the shared key for communicating with the TACACS+ accounting server.
4	Raisecom# tacacs accounting-server encrypt-key <i>string</i>	Configure the encrypted shared key for communicating with the TACACS+ accounting server.

14.5.6 Checking configurations

No.	Command	Description
1	Raisecom#show tacacs-server	Show configurations of the TACACS+ server.

14.6 Configuring RADIUS/TACACS+ accounting management

14.6.1 Configuring accounting policy

Step	Command	Description
1	Raisecom#aaa	Enter the charging configuration mode.
2	Raisecom(aaa)#domain { default default_admin domain-name }	Configure the accounting domain.
3	Raisecom(aaa)#aaa accounting login enable	Enable accounting. By default, the system is not enabled with accounting.
4	Raisecom(aaa)#aaa command authorize enable	Enable authentication of accounting command line.
5	Raisecom(aaa)#login-trap enable	Enable accounting login Trap.
6	Raisecom(aaa)#aaa accounting fail { online offline }	Configure the processing policy for accounting failure. By default, it is online, that is, login is allowed after accounting fails.
7	Raisecom(aaa)#aaa accounting update period	Configure the sending interval for accounting update packets. If it is configured to 0, no accounting update packet is sent. By default, the sending interval is 0. Note The RADIUS accounting server can record each user's access time and operation by receiving the accounting start packet, accounting update packet, and accounting end packet.

14.6.2 Configuring user management

Step	Command	Description
1	Raisecom#aaa	Enter accounting configuration mode.
2	Raisecom(aaa)#user name user-name password [plain] [cipher] <i>password</i>	Configure the user name and password.
3	Raisecom(aaa)#user name user-name privilege <i>priority-value</i>	Configure the user priority.
4	Raisecom(aaa)#user name user-name state { active inactive }	Configure the user status.
5	Raisecom(aaa)#user user-name bind-ip ip-address	(Optional) bind the user with an IPv4 address.
	Raisecom(aaa)#user user-name bind-ipv6 ipv6-address	(Optional) bind the user with an IPv6 address.
6	Raisecom(aaa)#user_group group-id	Create a user group.
7	Raisecom(aaa)#user user-name user_group group-id	Configure the members of the user group.
8	Raisecom(aaa)#user user-name { allow-exec disallow-exec } first-keyword [second- keyword]	Configure the user naming conventions.
9	Raisecom(aaa)#user user-name service-scheme <i>scheme-name</i>	Configure the user service plan.

14.6.3 Checking configurations

No.	Command	Description
1	Raisecom#show aaa	Show AAA configurations.

14.6.4 Configuring basic dot.1x



Caution

- Dot.1X and STP are mutually exclusive on the interface and cannot be used at the same time.
- An interface can only handle one user authentication request at a time.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#dot1x enable	Enable global Dot.1X.
3	Raisecom(config)#dot1x authentication-method { chap pap eap }	Configure the global authentication method.

Step	Command	Description
4	Raisecom(config)# dot1x auth-mode { radius local tacacs+ }	Configure the authentication mode for Dot.1X authentication.
5	Raisecom(config)# dot1x free-ip <i>ip-address</i> [<i>ip-mask</i> <i>mask-length</i>]	Configure an IP address segment that can be accessed by Dot.1X terminal users who fail authentication or exit authorization.
6	Raisecom(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
7	Raisecom(config-port)# dot1x enable	Enable Dot.1X on the interface.
8	Raisecom(config-port)# dot1x auth-control { auto authorized-force unauthorized-force }	Configure the interface access control mode.
9	Raisecom(config-port)# dot1x auth-method { portbased macbased }	Configure the interface access control mode.
10	Raisecom(config-port)# dot1x keepalive { enable disable }	Enable/Disable Dot.1X handshake on the interface.
11	Raisecom(config-port)# dot1x max-user <i>user-number</i>	Configure the maximum number of users allowed for Dot.1X port authentication.



Note

If Dot.1X is not enabled in global or interface mode, the interface control mode of Dot.1X is the mandatory authorization.

14.6.5 Configuring Dot.1X re-authentication



Caution

Re-authentication is initiated for authorized users, so before enabling re-authentication, you should ensure that global and interface Dot.1X are enabled. The interface in authorized state still maintains the authorized state during the re-authentication process. If re-authentication fails, it enters the unauthorized state.

Step	Command	Description
1	Raisecom# config	Enter global configuration mode.
2	Raisecom(config)# interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-port)# dot1x reauthentication enable	Enable Dot.1X re-authentication.

14.6.6 Configuring Dot.1X timer

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#dot1x timer reauth-period <i>reauth-period</i>	Configure the re-authentication timer.
4	Raisecom(config-port)#dot1x timer quiet-period <i>second</i>	Configure the silent timer.
5	Raisecom(config-port)#dot1x timer supp-timeout <i>supp-timeout</i>	Configure the authentication timeout timer for applicants.
6	Raisecom(config-port)#dot1x timer server-timeout <i>server-timeout</i>	Configure the authentication server timeout timer.
7	Raisecom(config-port)#dot1x timer keepalive-period <i>second</i>	Configure the interval for Dot.1X to retransmit Keepalive packets on the interface.
8	Raisecom(config-port)#dot1x timer tx-period <i>second</i>	Configure the Request/Identity request packet timeout timer.

14.6.7 Checking configurations

No.	Command	Description
1	Raisecom#show dot1x <i>interface-type</i> <i>interface-list</i>	Show Dot.1X configurations on the interface.
2	Raisecom#show dot1x <i>interface-type</i> <i>interface-list</i> statistics	Show Dot.1X statistics on the interface.
3	Raisecom#show dot1x <i>interface-type</i> <i>interface-list</i> user	Show user information for Dot.1X authentication on the interface.
4	Raisecom#show dot1x free-ip	Show the IP address segments that can be accessed by Dot.1X terminal users who fail authentication or exit authorization.

14.6.8 Maintenance

Command	Description
Raisecom(config)#clear dot1x <i>interface-type</i> <i>interface-list</i> statistics	Clear Dot.1X statistics on the interface.

14.7 Configuring interface isolation

14.7.1 Preparing for configurations

Scenario

To isolate Layer 2 data of interfaces in a VLAN and provide physical isolation between interfaces, you need to configure interface isolation.

By adding interfaces that need to be controlled to a VLAN protection group, you can enhance network security and provide flexible networking scheme for users.

Interface isolation helps isolate interfaces in a VLAN, enhance network security, and provide flexible networking schemes.

Prerequisite

N/A

14.7.2 Configuring interface isolation

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

14.7.3 Configuring VLAN isolation

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

14.7.4 Checking configurations

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

14.7.5 Checking configurations

No.	Command	Description
1	Raisecom# show switchport protect	Show configurations of interface isolation.

14.8 Configuring port mirroring

14.8.1 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 monitor transmitting and receiving status of one or more interfaces for analyzing network status.

Prerequisite

N/A

14.8.2 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 <i>group-id</i>	Create a port mirroring group.
3	Raisecom(config)# mirror-group <i>group-id</i> remote-vlan <i>vlan-id</i>	Configure the remote mirroring VLAN of the mirroring group.
4	Raisecom(config)# mirror-group <i>group-id</i> reflector-port <i>interface-type interface-number</i>	Configure the reflector interface of the mirroring group.
5	Raisecom(config)# interface <i>interface-type interface-number</i> Raisecom(config-port)# mirror-group <i>group-id</i> monitor-port Raisecom(config-port)# exit	(Optional) enter interface configuration mode. Configure the interface as a monitoring interface.
	Raisecom(config)# interface port-channel <i>channel-number</i> Raisecom(config-port-channel*)# mirror-group <i>group-id</i> monitor-port Raisecom(config-port-channel*)# exit	(Optional) enter link aggregation configuration mode. Configure the link aggregation group as the monitoring interface.

Step	Command	Description
6	Raisecom(config)# interface <i>interface-type</i> <i>interface-number</i> Raisecom(config-port)# mirror-group <i>group-id</i> 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 <i>channel-number</i> Raisecom(config-port-channel*)# mirror-group <i>group-id</i> 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.
7	Raisecom(config-port)# exit Raisecom(config)# mirror-group <i>group-id</i> source-cpu [ingress egress]	Configure the CPU as the source of the mirror group.

14.8.3 Checking configurations

No.	Command	Description
1	Raisecom# show mirror-group [<i>group-id</i>]	Show basic information about port mirroring.

14.9 Configuring PPPoE+

14.9.1 Preparing for configurations

Scenario

To prevent illegal users from accessing during the PPPoE authentication process, you need to configure PPPoE + and add additional user identification information to the PPPoE packets.

Since the added user identification information is related to the specific switch and interface, the authentication server can bind the user to the switch and interface and other information. Therefore, the problems of account sharing and account theft can be effectively prevented, and users can be better positioned to ensure network security.

Prerequisite

N/A

14.9.2 Configuring PPPoE+ basic functions



Caution

PPPoE + is used to process PADI and PADR messages, and only targets at PPPoE clients. Generally, only the interface connected to the client is enabled with PPPoE +, and the trusted interface refers to the interface connecting the switch and the PPPoE server. The roles of these two interfaces are mutually exclusive, that is, an interface cannot be both a PPPoE+ enabled interface and a trusted interface.

Enabling PPPoE+

After PPPoE + is enabled globally and on the interface of the device, the PPPoE authentication packet sent to the interface will be added with user information and then sent to the trusted interface.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#pppoeagent enable	Enable global PPPoE+.
3	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#portswitch	Configure the interface mode to switch mode.
5	Raisecom(config-port)#pppoeagent enable	Enable PPPoE+ on the interface.

Configuring PPPoE+ trusted interface

The PPPoE + trusted interface is configured to prevent PPPoE server spoofing and security risks caused by PPPoE packets being forwarded to other non-service interfaces. Generally, the interface connected to the PPPoE server is configured as the trusted interface. PPPoE packets from the PPPoE client to the server will only be forwarded by the trusted interface, and only PPPoE packets received from the trusted interface will be forwarded to the PPPoE client.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type</i> <i>interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#portswitch	Configure the interface mode to switching mode.
4	Raisecom(config-port)#pppoeagent trust	Configure the PPPoE+ trusted interface.



Because PPPoE + is aimed at the PPPoE client instead of the server, the downstream interface of the device cannot receive PADO and PADS packets, which means that the PPPoE + enabled interface cannot receive PADO and PADS packets. If the interface receives these packets, it indicates that there are error packets and the interface should discard them. However, the interface can forward PADO and PADS packets from the trusted interface. At the same time, PADI and PADR packets should only be forwarded to the trusted interface.

14.9.3 Configuring PPPoE+ packet information

PPPoE + mainly processes a specific Tag in PPPoE packets. This Tag contains two fields: Circuit ID and Remote ID:

- Circuit ID is filled with the VLAN ID, interface number and host name of the interface that receives the client request packets.
- Remote ID is filled with the MAC address of the client or the MAC address of the switch.

Configuring Circuit ID

Circuit ID has two filling modes: switch mode and ONU mode. The default is Switch mode. In ONU mode, the format of Circuit ID is fixed, and there is no customized format. These commands are used to configure the padding content of the Circuit ID in Switch mode.

In Switch mode, Circuit ID has two filling formats:

- Default format: when no custom Circuit ID is configured, it is filled with VLAN ID /interface number/additional string (if no additional string is defined, the default is the hostname).
- Customized format: when a customized Circuit ID is configured, it is filled with the configured Circuit ID string.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#pppoeagent circuit-id mode { onu switch olt }	Configure the padding mode of Circuit ID.
3	Raisecom(config)#interface interface-type interface-number	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#portswitch	Configure the interface mode to switching mode.
5	Raisecom(config-port)#pppoeagent circuit-id string	(Optional) configure the Circuit ID as a customized character string.

Circuit ID contains an additional string in the default format. The additional string is the hostname of the switch by default. You can configure it as a customized string.

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

Step	Command	Description
2	Raisecom(config)#pppoeagent circuit-id attach-string <i>string</i>	(Optional) configure the additional string of the Circuit ID. If the Circuit ID is the default format, the contents configured by this command will be added to the Circuit ID.

Configuring Remote ID

Remote ID is filled with a MAC address, you can choose to fill in the MAC address of the switch or the MAC address of the client, and you can choose to fill in the Remote ID in binary or ASCII form.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#portswitch	Configure the interface mode to switching mode.
4	Raisecom(config-port)#pppoeagent remote-id { client-mac switch-mac }	(Optional) fill in the Remote ID of the interface PPPoE+ with the MAC address.
5	Raisecom(config-port)#pppoeagent remote-id format { ascii binary }	(Optional) configure the Remote ID padding mode of the interface PPPoE+.

Configuring Tag overwriting

For some reasons, such as the tag of some information fields may be forged by the client, the original Tag of the packet needs to be overwritten. After Tag overwriting is enabled, if PPPoE packets already carry the information field Tag, the tag will be overwritten. If not, a tag will be added.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#portswitch	Configure the interface mode to switching.
4	Raisecom(config-port)#pppoeagent vendor-specific-tag overwrite enable	Enable Tag overwriting.

14.9.4 Checking configurations

No.	Command	Description
1	<code>Raisecom#show pppoeagent [interface-type interface-list]</code>	Show PPPoE+ configurations.
2	<code>Raisecom#show pppoeagent statistic [interface-type interface-list]</code>	Show PPPoE+ statistics.

14.9.5 Maintenance

Command	Description
<code>Raisecom(config)#clear pppoeagent statistic</code>	Clear PPPoE+ statistics.

14.10 Configuring dynamic ARP inspection

14.10.1 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.

14.10.2 Configuring trusted interface of dynamic ARP inspection

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.
3	<code>Raisecom(config-port)#ip arp-inspection trust</code>	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, which means that the interface does not trust ARP packets.

14.10.3 Configuring static binding of dynamic ARP inspection

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] port port-id	Configure static binding relationship.

14.10.4 Configuring dynamic binding of dynamic ARP inspection



Caution

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.

14.10.5 Configuring protection VLAN of dynamic ARP inspection

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ip arp-inspection dhcp-snooping	Enable global dynamic binding.
3	Raisecom(config)#ip arp-inspection vlan vlan-list	Configure the protection VLAN of dynamic ARP inspection.

14.10.6 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 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 ELPS
- Configuring ERPS
- Configuring VRRP
- Configuring link-state tracking
- Configuring PW redundancy protection
- Maintenance

15.1 Configuring link aggregation

15.1.1 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.

mLACP link aggregation is used for the AC-side link in dual-homed PW protection to provide communication between the DHD and 2 destination modes, as well as selection of active interfaces. It is used to resolve the problem for selecting the path, prevent the loop, and enhance the network availability.

Prerequisite

Configure physical parameters of the interface and make the physical layer Up.

15.1.2 Configuring manual link aggregation

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface port-channel - port-channel-number	Enter LAG configuration mode.
3	Raisecom(config-port-channel*)#mode manual	Configure the manual link aggregation mode.
4	Raisecom(config-port-channel*)#load- sharing mode { dst-ip dst-mac src- dst-ip src-dst-mac src-ip src-mac }	Configuring the load-sharing mode of the link aggregation. By default, load sharing mode is rc-dst-mac , which means selecting the forwarding interface according to OR operation result of source MAC address and destination MAC address.
5	Raisecom(config-port-channel*)#exit	Return to global configuration mode.
6	Raisecom(config)#interface interface-type interface-number	Enter physical interface configuration mode.
7	Raisecom(config-port)#port-channel group- id	Add member interfaces to the LAG.
8	Raisecom(config-port)#exit	Return to global configuration mode.



Note

Do not configure services on interfaces, which are added to the LAG. In a LAG, member interfaces that share loads must be identically configured. Otherwise, data cannot be forwarded properly. For example, packets may be lost. These configurations include STP, QoS, QinQ, VLAN, interface properties, and MAC address learning.

- STP status on the interface, properties (point-to-point/non point-to-point) of the link connected to the interface, path cost of the interface, STP priority, packet Tx speed limit, whether the interface is configured with loopback protection, root protection, and whether the interface is an edge interface.
- QoS: traffic policing, traffic shaping, congestion avoidance, rate limiting, SP queue, WRR queue scheduling, WFQ queue, interface priority, and interface trust mode.
- QinQ: QinQ status on the interface, added outer VLAN tag, policies for adding outer VLAN Tags for different inner VLAN IDs.
- VLAN: the allowed VLAN, default VLAN, and the link type (Trunk, Hybrid, and Access) on the interface, and whether VLAN packets carry Tag.
- Interface properties: speed, duplex mode, and link Up/Down status.
- MAC address learning: MAC address learning status, MAC address limit, and whether to forward and control data after the MAC address table is full.

15.1.3 Configuring static LACP link aggregation

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

Step	Command	Description
2	<code>Raisecom(config)#lacp system-priority <i>priority</i></code>	(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	<code>Raisecom(config)#lacp timeout { fast slow }</code>	(Optional) configure the LACP timeout mode.
4	<code>Raisecom(config)#interface port-channel <i>channel-number</i></code>	Enter LAG configuration mode.
5	<code>Raisecom(config-port-channel*)#mode lacp</code>	Configure the working mode of the LAG to static LACP link aggregation.
6	<code>Raisecom(config-port-channel*)#{ max-active min-active } links <i>threshold</i></code>	(Optional) configure the maximum/minimum number of active links of the LACP LAG.
7	<code>Raisecom(config-port-channel1)#lacp priority preempt enable</code>	(Optional) enable priority preemption of the link aggregation group.
8	<code>Raisecom(config-port-channel*)#load-sharing mode { dst-ip dst-mac src-dst-ip src-dst-mac src-ip src-mac }</code>	(Optional) configure the load balancing mode of link aggregation. By default, the system uses the src-dst-mac mode, which selects the forwarding interface based on logical OR of the source and destination MAC addresses.
9	<code>Raisecom(config-port-channel*)#exit</code>	Return to global configuration mode.
10	<code>Raisecom(config)#interface <i>interface-type interface-number</i></code>	Enter physical interface configuration mode.
11	<code>Raisecom(config-port)#portswitch</code>	Configure the interface to switch mode.
12	<code>Raisecom(config-port)#port-channel <i>channel-number</i></code>	Add the interface to the LAG.
13	<code>Raisecom(config-port)#lacp mode { active passive }</code>	(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	<code>Raisecom(config-port)#lacp port-priority <i>priority</i></code>	(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	<code>Raisecom(config-port)#exit</code>	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 active interfaces even they meet all requirements on active interfaces. This helps make traffic of current member interfaces continuous.

15.1.4 Configuring manual backup link aggregation

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 LAG to manual backup link aggregation.
4	Raisecom(config-port-channel*)#master- port interface-type interface-number	Configure the master interface of link aggregation.
5	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.
6	Raisecom(config-port-channel*)#exit	Return to global configuration mode.
7	Raisecom(config)#interface interface- type interface-number	Enter Layer 2 physical interface configuration mode.
8	Raisecom(config-port)#port-channel channel-number	Add member interfaces to the LAG.
9	Raisecom(config-port)#exit	Return to global configuration mode.

15.1.5 Configuring static LACP backup link aggregation

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

Step	Command	Description
2	Raisecom(config)#lacp system-priority <i>system-priority</i>	(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 <i>channel-number</i>	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 <i>interface-type interface-number</i>	Configure the master interface of link aggregation.
7	Raisecom(config-port-channelif)#restore-mode { non-revertive revertive [restore-delay <i>second</i>] }	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 <i>interface-type interface-number</i>	Enter Layer 2 physical interface configuration mode.
10	Raisecom(config-port)#port-channel <i>channel-number</i>	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 <i>port-priority</i>	(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.

15.1.6 Configuring mLACP link aggregation

Configuring ICCP channel

In the application scenario of PW dual-homing protection, the user equipment accesses the network through two PE devices. An ICCP channel needs to be established between the two PE devices in order to carry DNI-PW (bypass PW).

Perform the following configurations on the MC-PW working node and protection node respectively.

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 IP address generally uses the IP address of the channel physical interface or channel aggregation interface.
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 IP address of the peer device 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 a chassis group and enter chassis group configuration mode.
3	Raisecom(config-ic-group)#iccp-channel channel-id	Bind an ICCP channel to the chassis group.
4	Raisecom(config-ic-group)#mlacp { master slave }	Configure the mLACP role of the local device in the chassis group.
5	Raisecom(config-ic-group)#port-channel group-id	Bind a LAG to the chassis group.
6	Raisecom(config-ic-group)#restore-mode { non-revertive revertive [restore-delay seconds] }	Configure the fault restoration mode and delay of the LAG in the chassis group.
7	Raisecom(config-ic-group)#mlacp system-priority system-priority	Configure the mLACP system priority of the local device in the 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 chassis group.

15.1.7 Checking configurations

No.	Command	Description
1	<code>Raisecom#show lacp internal</code>	Show local system LACP interface status, identifier, interface priority, management key, operation key, and interface status machine.
2	<code>Raisecom#show lacp neighbor [detail]</code>	Show neighbor LACP information, including the identifier, interface priority, device ID, Age, operation key ID, interface ID, and interface status machine.
3	<code>Raisecom#show lacp statistics</code>	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	<code>Raisecom#show lacp sys-id</code>	Show global enabling status of local system LACP, device ID, LACP priority, and MAC address.
5	<code>Raisecom#show port-channel</code>	Show whether the current system is enabled with link aggregation, link aggregation load-sharing mode, member interfaces and currently-active member interfaces in all current LAGs.  Note Currently active member interfaces refers to interfaces in UP status in the LAG.
6	<code>Raisecom#show mlacp-group [icg-list]</code>	Show configurations and running information about the MLACP group.
7	<code>Raisecom#show mlacp-group [icg-list] statistics</code>	Show packet receiving/sending statistics of the MLACP group.

15.2 Configuring interface backup

15.2.1 Preparing for configurations

Scenarios

In a dual-uplink networking scenario, you can realize redundancy backup of the primary/slave link and fast switching of services through interface backup, thus improving service reliability.

Prerequisite

N/A

15.2.2 Configuring interface backup group

The RAX711-C-R supports interface backup based on interface or interface+VLAN. Choose one from Step 3 and Step 4. By configuring optional parameters of the command, you can switch services of the specified VLAN or all services on the interface when faults occur based on interface backup.

No.	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#port backup <i>interface-type interface-number</i> [vlanlist vlanlist primaryvlan <i>vlanid [md-level level-value]</i> Raisecom(config-port)#exit	(Optional) create a backup interface based on interface 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 <i>interface-type interface-number</i> vlanlist vlanlist separate	(Optional) create a backup interface based on interface+VLAN for the primary interface.
5	Raisecom(config-port)#port backup restore-mode { non-revertive revertive [restore-delay delay- <i>time] }</i>	Configure the restoration mode and restoration delay of interface backup.
6	Raisecom(config-port)#port backup fault-detect cfm	Configure the fault detection mode of interface backup.
7	Raisecom(config-port)#port backup <i>interface-type interface-number</i> force-switch [vlan vlan-id]	(Optional) forcedly switch services to the backup link.

15.2.3 Checking configurations

No.	Item	Description
1	Raisecom#show port backup	Show basic information about interface backup.
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.

15.3 Configuring ELPS

15.3.1 Preparing for configurations

Scenario

To make the Ethernet reliability up to Telecom-grade (network self-heal time less than 50ms), you can deploy ELPS at Ethernet. ELPS is used to protect the Ethernet connection. It is an end-to-end protection technology.

ELPS supports 1+1 and 1:1 protection switching modes. It is divided into unidirectional protection switching and bidirectional protection switching based on the fact that whether services of both ends are switched concurrently when the link fails. Unidirectional and bidirectional protection switching are available in 1+1 protection switching mode only. 1:1 protection switching mode supports bidirectional protection switching only.

ELPS provides 3 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 CC: suitable for unidirectional detection or multi-device crossing detection.
- Detect faults based on physical interface status and CC.

Prerequisite

- Connect interfaces and configure physical parameters for them. Make the physical layer Up.
- Create a VLAN.
- Add the interface to the VLAN.
- Configure CFM detection and form a neighbor relationship (preparing for CC mode).

15.3.2 Creating protection pair

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ethernet line-protection line- number working interface- type interface-number vlan-list protection interface-type interface- number vlan-list one-to- one [non-revertive] protocol-vlan vlan-id	Create the ELPS protection pair and configure the protection mode. The protection group is in non-revertive mode if you configure the non-revertive parameter. • In revertive mode, when the working line recovers from a fault, traffic is switched from the protection line to the working line. • In non-revertive mode, when the working line recovers from a fault, traffic is not switched from the protection line to the working line. By default, there is no ELPS protection pair.
3	Raisecom(config)#ethernet line-protection line- number name string	(Optional) configure a name for the ELPS protection pair. By default, there is no name for the ELPS protection pair.

Step	Command	Description
4	<code>Raisecom(config)#ethernet line-protection line-number wtr-timer wtr-timer</code>	(Optional) configure the WTR timer. In revertive mode, when the working line recovers from a fault, traffic is not switched to the working line unless the WTR timer times out. By default the WTR timer value is 5min.  Note We recommend that WTR timer configurations on both ends keep consistent. Otherwise, we cannot ensure 50ms quick switching.
5	<code>Raisecom(config)#ethernet line-protection line-number hold-off-timer hold-off-timer</code>	(Optional) configure the Holdoff timer. After the Holdoff timer is configured, when the working line fails, the system will delay to process 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 0.  Note If the Holdoff timer value is over great, it may influence 50ms switching performance. Therefore, we recommend configuring the Holdoff timer value to 0.

15.3.3 Configuring ELPS fault detection modes



Note

Fault detection modes of the working line and protection line can be different. However, we recommend that fault detection mode configurations of the working line and protection line keep consistent.

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#ethernet line-protection line-number { working protection } failure-detect physical-link</code>	Configure the fault detection mode of the working line/protection line to failure-detect physical-link. By default, the fault detection mode is failure-detect physical-link.
	<code>Raisecom(config)#ethernet line-protection line-number { working protection } failure-detect cc [md md-name] ma ma-name level level mep local-mep-id remote-mep-id</code>	Configure the fault detection mode of the working line/protection line to failure-detect cc. This fault detection mode cannot take effect unless you finish related configurations on CFM.

Step	Command	Description
	Raisecom(config)#ethernet line-protection line-number { working protection } failure-detect physical-link-or-cc [md md-name] ma ma-name level level mep local-mep-id remote-mep-id	Configure the fault detection mode of the working line/protection line 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 fault detection mode cannot take effect unless you finish related configurations on CFM.

15.3.4 (Optional) configuring ELPS switching control



Note

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

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#ethernet line-protection line-number lockout	Lock protection switching. After this configuration, the traffic is not switched to the protection line even the working line fails. By default, the traffic is automatically switched to the protection line when the working line fails.
3	Raisecom(config)#ethernet line-protection line-number force-switch	Switch the traffic from the working line to the protection line forcedly. By default, the traffic is automatically switched to the protection line when the working line fails.
4	Raisecom(config)#ethernet line-protection line-number manual-switch	Switch the traffic from the working line to the protection line manually. Its priority is lower than the one of forced switch and APS. By default, the traffic is automatically switched to the protection line when the working line fails.
5	Raisecom(config)#ethernet line-protection line-number manual-switch-to-work	In non-revertive mode, switch the traffic from the protection line to the working line.  Note After you execute a protection group command, if a fault/recovery event occurs or if other protection group commands, both ends of the protection group may select different lines. In this case, you should use the clear ethernet line-protection end-to-end command to delete the configured protection group command to make both ends of the protection group select the identical line.

15.3.5 Checking configurations

No.	Command	Description
1	Raisecom(config)#show ethernet line-protection [<i>line-number</i>]	Show configurations of the protection pair.
2	Raisecom(config)#show ethernet line-protection [<i>line-number</i>] statistics	Show statistics of the protection pair.
3	Raisecom(config)#show ethernet line-protection [<i>line-number</i>] aps	Show APS information about the protection pair.

15.4 Configuring ERPS

15.4.1 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 RAX711-C-R 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).

15.4.2 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.
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.

Step	Command	Description
4	<code>Raisecom(config)#ethernet ring-protection ring-number version { 1 2 }</code>	(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	<code>Raisecom(config)#ethernet ring-protection ring-number guard-time guard-time</code>	(Optional) after the ring Guard timer is configured, the failed node does not process APS packets during a period. In a 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.
6	<code>Raisecom(config)#ethernet ring-protection ring-number wtr-time wtr-time</code>	(Optional) configure the ring WTR timer. In revertive mode, when the working line recovers from a fault, traffic is not switched to the working line unless the WTR timer times out. By default, the ring WTR time value is 5min.
7	<code>Raisecom(config)#ethernet ring-protection ring-number holdoff-time holdoff-time</code>	(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.

15.4.3 (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	<code>Raisecom#config</code>	Enter global configuration mode.

Step	Command	Description
2	<pre>Raisecom(config)#ethernet ring-protection <i>ring-number</i> east <i>interface-type</i> <i>interface-</i> <i>number</i> west <i>interface-type</i> <i>interface-number</i> node-type rpl-owner rpl { east west } [not-revertive] [protocol- vlan <i>vlan-id</i>] [block- vlanlist <i>vlan-list</i>]</pre>	Create the tributary ring on the intersecting node and set the intersecting node to the RPL Owner. 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 links between 2 intersecting nodes belong to the main ring. Therefore, when you configure the tributary ring on the intersecting node, you can only configure the west or east interface. By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094.
	<pre>Raisecom(config)#ethernet ring-protection <i>ring-number</i> east <i>interface-type</i> <i>interface-</i> <i>number</i> west <i>interface-type</i> <i>interface-number</i> node-type rpl-neighbour rpl { east west } [not-revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-list</i>]</pre>	Create the tributary ring on the intersecting node and set the intersecting node to the RPL Neighbour. By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094.
	<pre>Raisecom(config)#ethernet ring-protection <i>ring-number</i> east <i>interface-type</i> <i>interface-</i> <i>number</i> west <i>interface-type</i> <i>interface-number</i> [not- revertive] [protocol-vlan <i>vlan-id</i>] [block-vlanlist <i>vlan-list</i>]</pre>	Create the tributary ring on the intersecting node and set the intersecting node to the RPL forwarding node. By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094.
3	<pre>Raisecom(config)#ethernet ring-protection <i>ring-number</i> raps-vc { with without }</pre>	(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.

Step	Command	Description
4	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.

15.4.4 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.
	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.

15.4.5 (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 forcibly.
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.

15.4.6 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.

15.5 Configuring VRRP

15.5.1 Preparing for configurations

Scenario

In general, we configure a default route to the breakout gateway for all devices in a LAN. Therefore, these devices can communicate with the external network. If the gateway fails, devices in the LAN fail to communicate with the external network.

The VRRP technology combines multiple routers to form a backup group. By configuring a virtual IP address for the backup group, you can set the default gateway to the virtual IP address of the backup group to make devices in the LAN communicate with the external network.

VRRP helps improve network reliability. It facilitates avoiding network interruption caused by failure of a single link and prevents changing routing configurations because of link failure.

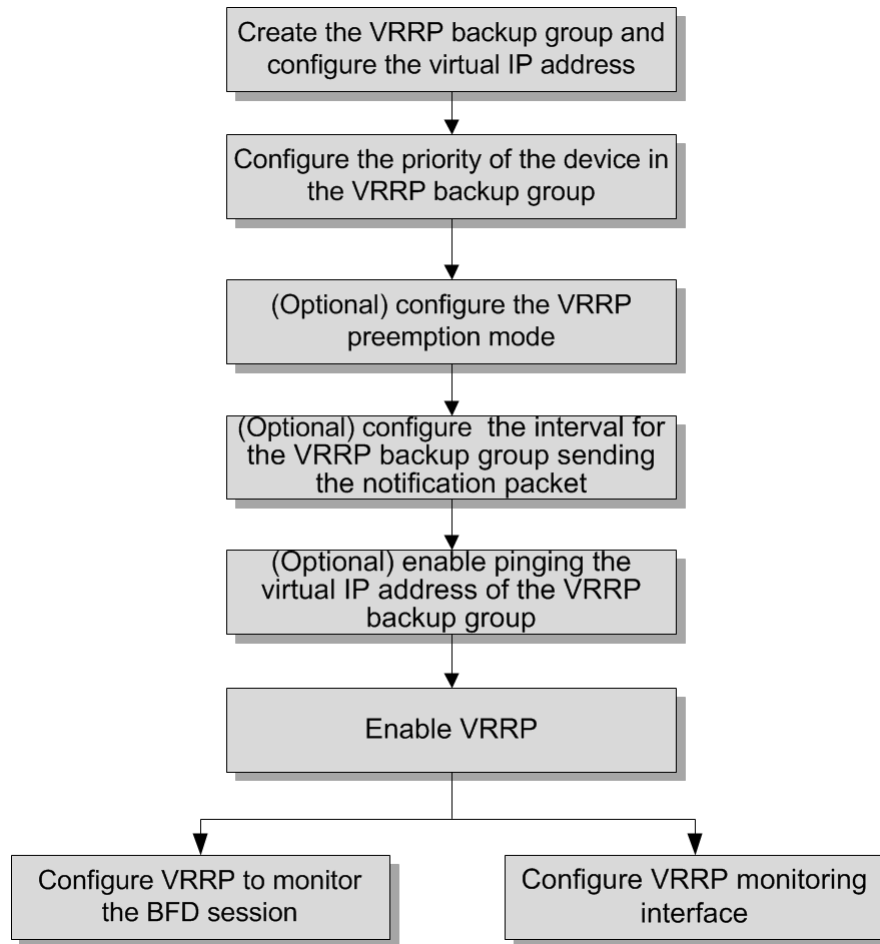
Prerequisite

The interface is in Layer 3 router mode and the IP address is configured.

15.5.2 Configuration procedure

Figure 15-1 shows the VRRP configuration procedure.

Figure 15-1 VRRP configuration procedure



15.5.3 Configuring VRRP backup group

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter interface configuration mode.
3	Raisecom(config-port)#vrrp group-id ip <i>ip-address</i>	Create a VRRP backup group and configure a virtual IP address for the VRRP backup group. The virtual IP address must be at the same network segment with the interface IP address.
4	Raisecom(config-port)#vrrp group-id description <i>description</i>	(Optional) configure descriptions of the VRRP backup group.
5	Raisecom(config-port)#vrrp group-id preempt [<i>delay-time second</i>]	(Optional) enable the preemption mode of the VRRP backup group. By default, the newly-created VRRP backup group is in preemption mode. The preemption delay is 0s.

Step	Command	Description
6	<code>Raisecom(config-port)#vrrp group-id priority priority</code>	Configure the priority of the device in the VRRP backup group. By default, the priority of the newly-created VRRP backup group is 100.
7	<code>Raisecom(config-port)#vrrp group-id timers advertise-interval seconds</code>	(Optional) configure the interval for the VRRP backup group sending the notification packet. By default, it is 1s.
8	<code>Raisecom(config-port)#vrrp group-id enable</code>	Enable VRRP. By default, it is enabled.

15.5.4 Configuring VRRPv3 backup group

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#interface interface-type interface-number</code> <code>Raisecom(config-port)#no portswitch</code>	Enter interface configuration mode.
3	<code>Raisecom(config-port)#vrrp6 group-id ipv6 ipv6-address</code>	Create a VRRPv3 backup group and configure the virtual IPv6 address for it. One VRRPv3 backup group can be configured with only 1 virtual IPv6 local link address and 15 virtual IPv6 global unicast address.
4	<code>Raisecom(config-port)#vrrp6 group-id description description</code>	(Optional) configure the description of the VRRPv3 backup group.
5	<code>Raisecom(config-port)#vrrp6 group-id preempt [delay-time second]</code>	(Optional) enable VRRPv3 backup group preemption mode. By default, the newly created VRRPv3 backup group is in preemption mode, and the preemption delay is 0s.
6	<code>Raisecom(config-port)#vrrp6 group-id priority priority</code>	Configure the priority of the device in the VRRPv3 backup group. By default, the priority of a newly created VRRPv3 backup group is 100.
7	<code>Raisecom(config-port)#vrrp6 group-id timers advertise-interval second</code>	(Optional) configure the interval for VRRPv3 backup groups to send advertisement packets. By default, the interval for sending advertisement packets is 1 second.
8	<code>Raisecom(config-port)#vrrp6 group-id enable</code>	Enable VRRPv3. By default, VRRPv3 of the newly created backup group is enabled.

15.5.5 (Optional) configuring ping function of VRRP virtual IP address

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#vrrp ping	Ping the virtual IP address of the VRRP backup group. By default, pinging the virtual IP address of the newly-created VRRP backup group is enabled.

15.5.6 Configuring VRRP/VRRPv3 monitoring interface

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i> Raisecom(config-port)#no portswitch	Enter interface configuration mode.
3	Raisecom(config-port)#vrrp group-id track <i>interface-type interface-number [reduce priority]</i>	Configure VRRP monitoring interface.
4	Raisecom(config-port)#vrrp6 group-id track <i>interface-type interface-number [reduce priority]</i>	Configure the VRRPv3 monitor interface.

15.5.7 Configuring VRRP/VRRPv3 fast switching

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i> Raisecom(config-port)#no portswitch	Enter interface configuration mode.
3	Raisecom(config-port)#vrrp group-id track bfd-session <i>session-id [increased priority reduce priority]</i>	Configure the VRRP backup group to monitor the BFD session to realize fast switching.
4	Raisecom(config-port)#vrrp6 group-id track bfd-session <i>session-id [increased priority reduce priority]</i>	Configure the VRRPv3 backup group to monitor the BFD session to realize fast switching.

15.5.8 Checking configurations

No.	Command	Description
1	<code>Raisecom#show vrrp group-id</code>	Show VRRP backup group configurations.
2	<code>Raisecom#show vrrp interface interface-type interface-number [group-id]</code>	Show VRRP backup group configurations on the interface.
3	<code>Raisecom#show vrrp interface interface-type interface-number [group-id] statistics</code>	Show VRRP backup group statistics on the interface.
4	<code>Raisecom#show vrrp [group-id] track</code>	Show monitoring information about the VRRP backup group.

15.6 Configuring link-state tracking

15.6.1 Preparing for configurations

Scenario

When the uplink of the intermediate device fails, if the lower-layer device cannot be notified in time, the traffic cannot be switched to the backup path, resulting in traffic interruption.

The main function of link-state tracking is to perform pre-configured fault handling actions when the fault source fails, so that the fault of the upper layer device is quickly delivered to the lower layer devices, thereby triggering the active-standby switchover.

Prerequisite

Before configuring link-state tracking, you need to connect the interface and configure the physical parameters of the interface to make the interface Up.

15.6.2 Creating a link-state group

Creating interface-based link-state group

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#link-state-tracking group group-number</code>	Create a link-state group and configure link-state tracking.
3	<code>Raisecom(config)#interface interface-type interface-number</code>	Enter physical layer interface configuration mode.

Step	Command	Description
4	<code>Raisecom(config-port)#link-state-tracking group group-number { downstream upstream }</code>	Configure the link-state group of the interface and the interface type. One interface only belongs to one link-state group and can only be configured to an uplink interface or a downlink interface.



Note

- There can be multiple upstream interfaces in one link-state group. As long as one upstream interface is Up, no link-state tracking will occur. Link-state tracking will occur only when all upstream interfaces are Down.
- In global mode, when you use the **no link-state-tracking group group-number** command to disable link-state tracking, the link-state group will be deleted.
- In physical layer interface mode, you can use the **no link-state-tracking group** command to delete an interface from the link-state group. If you delete an interface and there are no other interfaces under the link-state group and the link-state group is not enabled, deleting the interface will also delete the link-state group.

Creating link-state group based on remote MEP

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#link-state-tracking group group-number upstream ma-name name cfm-mepid mep-id level level-id</code>	Create a link-state group based on remote MEP and enable link-state tracking.

Creating link-state group based on ELPS

Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#link-state-tracking group group-number upstream elps-8031-link value</code>	Create an ELPS-based link-state group and enable link-state tracking.



Caution

When creating an ELPS-based link-state group, if you configure the next action to shutting down interface list, you need to ensure that these interfaces are not the interfaces associated with ELPS protection.

Creating link-state group based on mLACP group

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#link-state-tracking group <i>group-number upstream mlacp mlacp-id</i>	Create a link-state group based on link aggregation and enable link-state tracking.

15.6.3 Configuring fault processing action of link-state group

Interface fault processing mode

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#link-state-tracking group <i>group-number action</i> { blockvlanlist <i>vlan-list</i> modify-pvid <i>vlan-id</i> }	Configure the fault processing mode on the link-state interface.

Global fault processing mode

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#link-state-tracking group <i>group-number action</i> { delete-vlan <i>vlan-id</i> flush-erps <i>rind-id</i> }	Configure link-state tracking global fault processing mode.

15.6.4 Checking configurations

Step	Command	Description
1	Raisecom#show link-state-tracking group [<i>group-number</i>]	Show configurations and status of the link-state group.

15.7 Configuring PW redundancy protection

15.7.1 Preparing for configurations

Scenario

PW redundancy protection 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, etc.

Prerequisite

- The AC link between the dual-homed CE and PE supports E-Trunk or E-APS link protection.
- PEs can access each other through IGP.
- PW or MS-PW is created.

15.7.2 Configuring PW redundancy protection

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.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#mode 12	Configure the VPN mode on Layer 3 physical interface to L2VPN. By default, it is L3VPN.
4	Raisecom(config-port)#mpls 12vpn 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 12vpn switchover	Manually switch the service flow from the master PW to the slave PW.

15.7.3 Binding service PW with management PW

The master/slave PW status detection in the PW redundancy protection group is based on BFD. During BFD for PW, each service PW is bound with BFD packets and sessions, which increases the number of BFD sessions, thus wasting resources. By configuring the management PW, you can create only one BFD session for PWs with the same destination address, thus saving network resources.

Ensure that the management PW is created on the corresponding loopback interface before binding the service PW with the management PW.

No.	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#interface <i>interface-type interface-number</i>	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#mode 12	Configure the VPN mode on the Layer 3 physical interface to L2VPN. By default, it is L3VPN.
4	Raisecom(config-port)#mpls 12vc [backup bypass] track admin-pw loopback loopback-number	Bind the service PW with the management PW.

15.7.4 Checking configurations

No.	Command	Description
1	Raisecom#show mpls 12vc	Show configurations of PW redundancy protection.

15.8 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 statistics of received and transmitted packets of the chassis group.
Raisecom(config)#clear ethernet line-protection statistics	Clear statistics of the protection group.
Raisecom(config)#clear ethernet line-protection aps-id end-to-end command	Clear end-to-end switching control commands.
Raisecom(config)#clear ethernet ring-protection ring-number statistics	Clear statistics of the protection ring, including the number of transmitted APS packets, the number of received APS packets, the last switching time, and the fault detection mode.
Raisecom(config)#clear ethernet ring-protection ring-number command	Clear switching control commands of the protection ring, including the force-switch and manual-switch commands.
Raisecom(config)#clear mpls line-protection aps-id command	Clear control commands of the MPLS linear protection pair.
Raisecom(config)#clear mpls line-protection [aps-id] statistics	Clear statistics about the MPLS linear protection pair.

Command	Description
Raisecom(config)# clear iccp channel [<i>channel-id</i>] statistics	Clear statistics of ICC received and transmitted packets.
Raisecom(config)# clear vrrp statistics	Clear packet statistics of all VRRP backup groups.

16 Appendix

This chapter lists terms, acronyms, and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

16.1 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.

A

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.
-----------------------------------	--

A

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.

16.2 Acronyms and abbreviations

A

ACL	Access Control List
APS	Automatic Protection Switching

C

CE	Customer Edge
CFM	Connectivity Fault Management
CoS	Class of Service

D

DHD	Dual Home Device
DSCP	Differentiated Services Code Point

E

EFM	Ethernet in the First Mile
-----	----------------------------

F

FTP	File Transfer Protocol
-----	------------------------

G

GPS	Global Positioning System
GSM	Global System for Mobile Communications

H

HA	High Availability
I	
ICCP	Inter-Chassis Communication Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector
L	
LACP	Link Aggregation Control Protocol
LBM	LoopBack Message
LBR	LoopBack Reply
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LTM	LinkTrace Message
LTR	LinkTrace Reply
M	
MA	Maintenance Association
MAC	Medium Access Control
MD	Maintenance Domain
MEG	Maintenance Entity Group
MEP	Maintenance associations End Point
MIB	Management Information Base
MIP	Maintenance association Intermediate Point
MTU	Maximum Transmission Unit
N	
NTP	Network Time Protocol
O	

OAM Operation, Administration and Maintenance

P

PDU Protocol Data Unit

PE Provider Edge

PSN Packet Switched Network

PTN Packet Transport Network

PW Pseudo Wire

PWE3 Pseudo Wire Emulation Edge-to-Edge

Q

QoS Quality of Service

R

RMEP Remote Maintenance association End Point

RMON Remote Network Monitoring

S

SAToP Structure-Agnostic TDM over Packet

SFP Small Form-factor Pluggables

SLA Service Level Agreement

SNMP Simple Network Management Protocol

SNTP Simple Network Time Protocol

SP Strict-Priority

SSH Secure Shell

T

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

V

VPN	Virtual Private Network
VLAN	Virtual Local Area Network

W

WRR	Weight Round Robin
-----	--------------------

