

www.raisecom.com

Unicast Routing Configuration Guide

Legal Notices

Raisecom Technology Co., Ltd makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. **Raisecom Technology Co., Ltd** shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty.

A copy of the specific warranty terms applicable to your Raisecom product and replacement parts can be obtained from Service Office.

Restricted Rights Legend.

All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of **Raisecom Technology Co., Ltd.** The information contained in this document is subject to change without notice.

Copyright Notices.

Copyright ©2007 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.**

Trademark Notices

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

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows® XP is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Contact Information

Technical Assistance Center

The Raisecom TAC is available to all customers who need technical assistance with a Raisecom product, technology, or, solution. You can communicate with us through the following methods:

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road,
Haidian District, Beijing 100085

Tel: +86-10-82883305

Fax: +86-10-82883056

World Wide Web

You can access the most current Raisecom product information on the World Wide Web at the following URL:

<http://www.raisecom.com>

Feedback

Comments and questions about how the ... system software works are welcomed. Please review the FAQ in the related manual, and if your question is not covered, send email by using the following web page:

<http://www.raisecom.com/en/xcontactus/contactus.htm>.

If you have comments on the ... specification, instead of the web page above, please send comments to:

export@raisecom.com

We hope to hear from you!

CONTENTS

Release Notes	5
Chapter 1 Routing Overview	1
1.1 Overview	1
1.2 Enable routing transmission	2
Chapter 2 Static Routing Configuration	3
2.1 Static routing overview	3
2.1.1 Static routing	3
2.1.2 Default routing	3
2.2 Configure static routing	3
2.2.1 Default static routing configuration	3
2.2.2 Configure static routing	3
2.2.3 Default gateway configuration	4
2.3 Monitoring and maintenance	4
2.4 Typical configuration example	4
2.5 Static routing troubleshooting	6
Chapter 3 RIP Configuration	7
3.1 RIP overview	7
3.2 Configure RIP	7
3.2.1 Default RIP configuration	7
3.2.2 Start RIP	8
3.2.3 Enable the RIP protocol specified network	8
3.2.4 Configure RIP version	8
3.2.5 The authentication mode of port RIP protocol	9
3.2.6 Configure port additional metric value	9
3.2.7 Configure RIP timer	10
3.2.8 Configure RIP split-horizon	10
3.3 Monitoring and maintenance	11
3.4 Typical configuration example	13
3.5 RIP trouble shooting	14
Chapter 4 OSPF Configuration	15
4.1 OSPF overview	15
4.2 Configure OSPF	15
4.2.1 Default OSPF configuration	16
4.2.2 Enable OSPF	17
4.2.3 Enable the designed network OSPF protocol and appoint region ID	17
4.2.4 Configure OSPF interface parameter	17
4.2.5 Configure OSPF region parameters	19
4.2.6 Establish/configure virtual link	20
4.3 Monitoring and maintenance	20
4.4 Typical configuration example	22
4.5 OSPF trouble shooting	26

Release Notes

Date of Release	Manual Version	Software Version	Revisions

Preface

About This Manual

This manual introduces primary functions of the configuration management software for RC series products.

Who Should Read This Manual

This manual is a valuable reference for sales and marketing staff, after service staff and telecommunication network designers. For those who want to have an overview of the features, applications, structure and specifications of ... device, this is also a recommended document.

Relevant Manuals

《Raisecom NView System User Manual》

《Raisecom Nview System Installation and Deployment Manual》

《... User Manual》

《... Commands Notebook》

Organization

This manual is an introduction of the main functions of ... EMS. To have a quick grasp of the using of the EMS of ... , please read this manual carefully. The manual is composed of the following chapters

Chapter 1 Overview

This chapter briefly introduces the basic function of ...

Chapter 2 Configuration Management

This chapter mainly introduces the central site configuration management function of the

Chapter 3 Performance Management

This chapter focuses on performance management function of

Chapter 4 Device Maintenance Management

This chapter introduces the device maintenance management function of

Appendix A Alarm Type

The alarm types supported by

Compliance

The RC series products developed by Raisecom are strictly complied with the following standards as well as ITU-T, IEEE, IETF and related standards from other international telecommunication standard organizations:

YD/T900-1997 SDH Equipment Technical Requirements - Clock

YD/T973-1998 SDH 155Mb/s and 622Mb/s Technical conditions of optical transmitter module and receiver module

YD/T1017-1999 Network node interface for the Synchronous Digital Hierarchy (SDH)

YD/T1022-1999 Requirement of synchronous digital hierarchy (SDH) equipment function

YD/T1078-2000 SDH Transmission Network Technique Requirements-Interworking of Network Protection Architectures

YD/T1111.1-2001 Technical Requirements of SDH Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Receiver Modules

YD/T1111.2- 2001 Technical Requirements of SHD Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Transmitter Modules

YD/T1179- 2002 Technical Specification of Ethernet over SDH

G.703 Physical/electrical characteristics of hierarchical digital interfaces

G.704 Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels

G.707 Network node interface for the synchronous digital hierarchy (SDH)

G.774 Synchronous digital hierarchy (SDH) - Management information model for the network element view

G.781 Synchronization layer functions

G.783 Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks

G.784 Synchronous digital hierarchy (SDH) management

G.803 Architecture of transport networks based on the synchronous digital hierarchy (SDH)

G.813 Timing characteristics of SDH equipment slave clocks (SEC)

G.823 The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy

G.825 The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)

G.826 End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections

G.828 Error performance parameters and objectives for international, constant bit-rate synchronous digital paths

G.829 Error performance events for SDH multiplex and regenerator sections

G.831 Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)

G.841 Types and characteristics of SDH network protection architectures

G.842 Interworking of SDH network protection architectures

G.957 Optical interfaces for equipments and systems relating to the synchronous digital hierarchy

G.691 Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers

G.664 Optical safety procedures and requirements for optical transport systems

I.731 ATM Types and general characteristics of ATM equipment

I.732 ATM Functional characteristics of ATM equipment

IEEE 802.1Q Virtual Local Area Networks (LANs)

IEEE 802.1p Traffic Class Expediting and Dynamic Multicast Filtering

IEEE 802.3 CSMA/CD Access Method and Physical Layer Instruction

Chapter 1 Routing Overview

1.1 Overview

If there is no L3 device between VLANs, the devices which are in different VLAN can not communicate with each other. There are three kinds of routing.

- Default routing;
- Static routing;
- Dynamic routing.

A default routing is a special routing. You can configure a default routing using a static routing.

A static routing is a special routing configured manually by an administrator.

The advantage of static routing that it's safe and saves bandwidth, but can not adapt the dynamic change of network topology structure, like link invalidation and so on, so it may cause the destination unreachable. As network topology spreads, static routing will cost much time and energy.

Routing use dynamic routing protocol, which is able to compute the best routing for data stream. There are two types of dynamic routing protocol:

1. Use distance vector protocol to maintain routing table, it takes the distance of network resource as the computing evidence, and it can send routing table to neighbours periodically. Distance vector protocol uses one or one serious metric to compute the best routing, which makes it more convenient for configuration and usage.
2. Use link state protocol to maintain the data-base of network topology, that is to exchange link state announces (LSAs) among routings for maintenance. Sending LSAs is touched off by incidents, like constringency timer overtime or receiving request timer overtime. Link state protocol is able to answer the topology changes rapidly, but it needs more bandwidth and resources compared with distance vector protocol.

The distance vector protocol that ISCOM three-layer switch supports is RIP, which uses metric to choose the best routing. At the same time, the switch also supports open frame shortest path first link state protocol.

In some network environment, VLAN connects to different network or subnet. In IP network, each subnet is mapped to a signal VLAN. VLAN configuration is about to control the size of broadcasting domain. However, when one VLAN end needs to communicate with the end in another terminal, the communication between VLAN- routing among VLAN is needed. You can configure one or more routing to transmit data stream to each destination VLAN.

Figure 1-1 shows basic routing topology structure, switch A is in VLAN 1, switch B is in VLAN 2, routing has a port in each VLANA. When host A in VLAN 1 needs to communicate with host Bin VLAN 1, it sends out a data packet, the destination address is host B, the switch will transmit the data packet directly to host B, without sending to routing. When host A sends data packet to host C in VLAN 2, switch A will transmit the data packet to routing. The routing will receive the packet on the port in VLAN 1, check out routing table, choose the correct outgress port, and send the data packet to the port of switch B on VLAN 2. Switch B will receive the data packet and transmit it to host C.

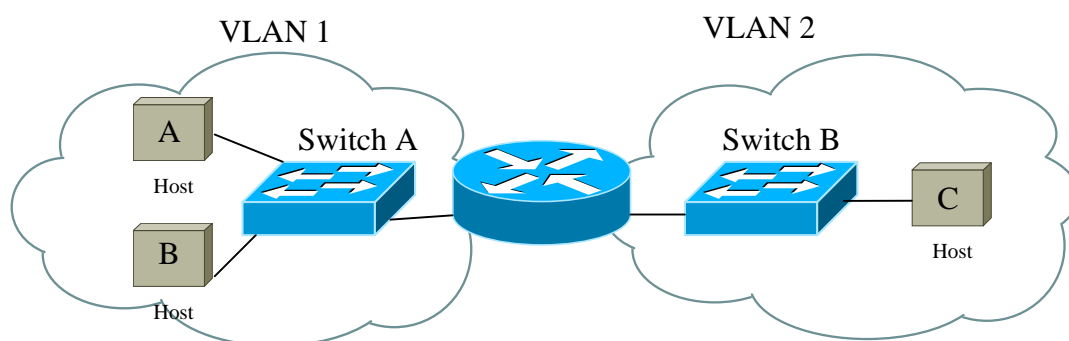


Fig 1-1 basic routing topology structure

1.2 Enable routing transmission

To realize three-layer routing transmission, **ip routing** is needed. By default the system forbids any software transmitting IP message. Enable IP transmission function, it is only needed to do the following configuration in global configuration mode. Use **no ip routing** to restore default configuration.

Step	Command	Description
1	config	Enter global configuration mode
2	ip routing	Enable/disable IP routing transmission function

⚠ Notice:

- Before you use the three layer function like static routing, dynamic routing and default gateway, IP routing transmission function must be opened first.

Chapter 2 Static Routing Configuration

2.1 Static routing overview

2.1.1 Static routing

Static routing is a special routing, it is manually configured by the administrator. By configuring static routing a communicating network can be established.

The advantage of static routing is safety and bandwidth saving. In the network with simple structure, it is only needed to configure static routing to make routing work, proper configuration and usage of static routing can improve the performance of network and offer enough bandwidth for important application. However, static routing can not adapt the dynamic change of network topology structure automatically, like unavailable link, so it may the destination is unreachable. As the growth of network topology, static routing will waste more and more time and energy.

2.1.2 Default routing

Default routing is a special routing. In brief, default routing is the routing that will be used only when there is no corresponding table item. That is, only when there is no proper routing, can default routing be used. In the routing table, default routing can appear with the address 0.0.0.0 (mask 0.0.0.0). Use **show ip routing** to check out if it is configured. If the destination address can not match up with any table item in the routing table, the message will be selected as default routing. If there is no default routing while the message destination is not in the routing table, then when the message is dropped, a ICMP message will be returned to the source end to report that the destination or network is unreachable.

2.2 Configure static routing

2.2.1 Default static routing configuration

Function	Default value
Static routing	Empty
Default routing	empty

2.2.2 Configure static routing

Sometimes, for simple network, the administrator can configure static routing manually. The process is as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	ip routing 10.0.0.0 255.0.0.0 192.168.1.1	Set the IP address of the next hop to destination network 10.0.0.0 is 192.168.1.1
3	exit	Return to privileged EXEC mode

4	show ip routing	Show routing table
5	config	Enter global configuration mode
6	no ip routing 10.0.0.0	Delete the routing in 10.0.0.0 network
7	exit	Return to privileged EXEC mode
8	show ip routing	Show routing table

When using **no ip routing**, network mask can be designated, and it can be undesignated to default mask. The next hop of routing must be the routing in the straight-through network.

2.2.3 Default gateway configuration

When a message that is needed for transmission do not find the destination network routing, use **ip default-gateway** to let the system transmit all the messages to default gateway. The steps are shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	ip default-gateway 192.168.1.1	Configure default gateway
3	exit	Return to privileged EXEC mode
4	show ip routing	Show routing table
5	config	Enter global configuration mode
6	no ip default-gateway	Cancel default gateway configuration
7	exit	Return to privileged EXEC mode
8	show ip routing	Show routing table

△ Notice

- For successful configuration, configure IP address is needed first, or configuring default gateway will be failed.

2.3 Monitoring and maintenance

Show routing table commands:

Command	Description
show ip routing	Show routing table

2.4 Typical configuration example

1) Network request

Configure static routing so that any two hosts or switches can PING through each other. The switch

in the figure below is three layer switch

2) Topology

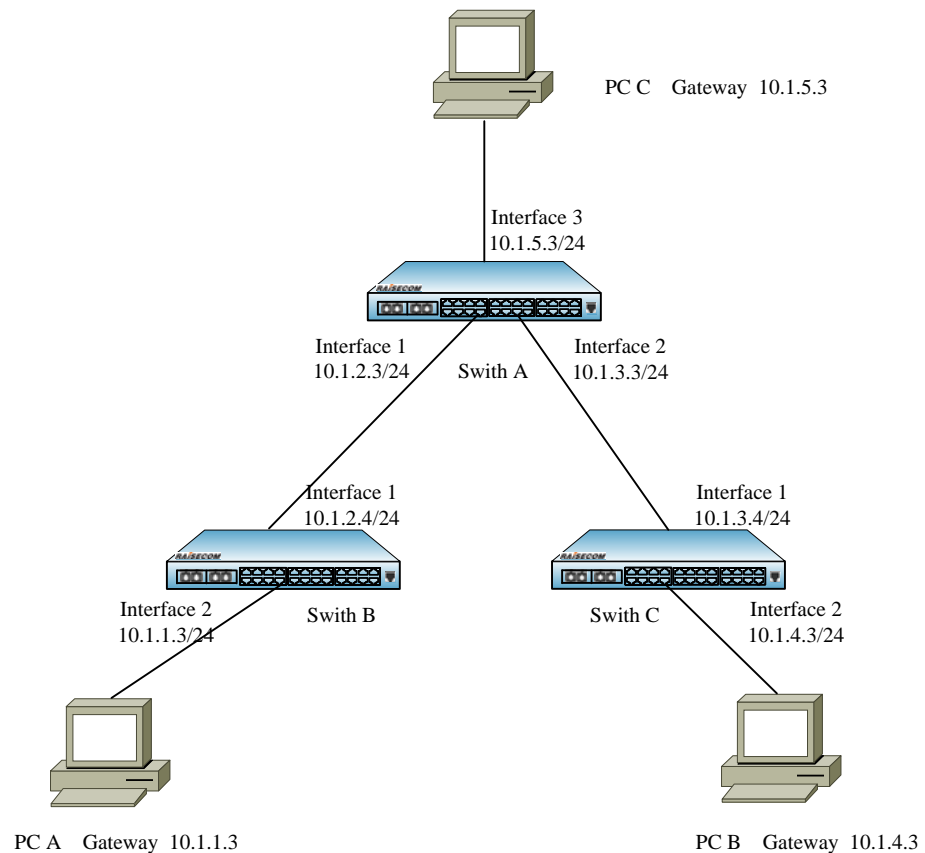


Fig 2-1 static routing configuration network structure

3) Configuration step

The precondition is to configure the IP address of each interface.

! Enable ip routing on Switch A and configure default gateway

```
Raisecom(config)# ip routing
```

```
Raisecom(config)# ip routing 10.1.1.0 255.255.255.0 10.1.2.4
```

```
Raisecom(config)# ip routing 10.1.4.0 255.255.255.0 10.1.3.4
```

! Enable ip routing on Switch B and configure default gateway

```
Raisecom(config)# ip routing
```

```
Raisecom(config)# ip default-gateway 10.1.2.3 255.255.255.0
```

! Enable ip routing on Switch C and configure default gateway

```
Raisecom(config)# ip routing
```

```
Raisecom(config)# ip default-gateway 10.1.3.3 255.255.255.0
```

! Configure default gateway to 10.1.1.3 on host A, the detailed configuration is omitted

! Configure default gateway to 10.1.4.3 on host B, the detailed configuration is omitted

! Configure default gateway to 10.1.5.3 on host C, the detailed configuration is omitted

Up till now any two hosts or Ethernet switches in figure 2-1 can make connection with each other.

2.5 Static routing troubling shooting

Trouble phenomena: the physical connection is correct, but they can not ping through each other

Trouble shooting:

Step 1: check out if the IP address of each port is correct.

Step 2: use **show ip routing** to check out if static routing or default gateway configuration is available.

Step 3: use **show running-config** to check out if routing transmission is enabled.

Chapter 3 RIP Configuration

3.1 RIP overview

Rip: Routing Information Protocol.

RIP is one of the most widely used interior gateway protocols now, which takes the famous distance vector algorithm. RIP is the simplest kind in distance vector protocol family, its routing choice is mainly based on the hop number before reaching destination spot, and usually this is weighed by the size of metric. RIP takes the distance from routing to its straight-through network is 0 hop, metric value is 1; the routing that needs to go through a routing is 1 hop, metric value is 2; the rest are like this. The maximum path cost that RIP supports is 15; when metric is larger than 16, RIP takes the path cost as infinite, and destination network is unreachable.

RIP is the protocol based on UDP (user datagram protocol) data message. The gateway or host that is running RIP needs to use 520 port of UDP to receive/send out messages when doing routing exchange. In RIP protocol, each routing that takes routing exchange will send out routing update messages to neighbour routings 6 after a certain period (30s by default). If the routing does not receive routing update information after about 6 update periods(180s by default), the link will be taken as unavailable. If in a certain time followed (300s by default) there is still no update information received from the link, it will be deleted from the routing table.

To improve the performance and make effective reflection in time to network topology structure, RIP protocol supports plant division, which saves a lot of shrinking time. At the same time, use trigger update for routing information change.

Raisecom three layer switches support both RIPv1 and RIPv2. RIPv2 supports clear text authentication, alterable long mask and classless inter-domain routing selection.

3.2 Configure RIP

To enable RIP three layer interface need to be configured for each network segments, use **ip routing** to realize three layer routing transmission function.

3.2.1 Default RIP configuration

Function	Default value
RIP routing protocol	Disabled
The given network RIP protocol	Disabled
RIP message receiving version	v1v2
RIP message sending version	broadcastv2
Port RIP protocol authentication mode	No authentication
Port add-ons measurement value configuration	1

RIP routing deleting timer exceed time	300 秒
RIP invalid timer	150 秒
RIP update timer	30 秒

3.2.2 Start RIP

Use **routing rip** to start RIP protocol. Enabling RIP protocol is the precondition of all the other RIP configuration. follows the commands below in global configuration mode.

Step	Command	Description
1	config	Enter global configuration mode
2	routing rip	Enable RIP

3.2.3 Enable the RIP protocol specified network

Use **network** to start RIP protocol of the given network, when the specified network and port IP address are in the same network, you can enable the port for RIP messages' receiving/sending. You can configure port IP address first, then use **network** to specify the network enabling port RIP protocol, and begin receiving/sending RIP messages; you can also use **network** to specify a network, then configure corresponding network IP address for the ports to enable port RIP protocol and begin receiving/sending RIP messages. When in a specified network, you need to specify the corresponding network mask at the same time. On a switch, the number of the network that is specified with **network** is unlimited. Use **no network** to clear the configuration. Follow the commands below for specified operation:

Step	Command	Description
1	config	Enter global configuration mode
2	routing rip	Enable RIP and turn to protocol configuration mode
3	network <i>network-number netmask</i>	Enable RIP protocol of the specified network

3.2.4 Configure RIP version

ISCOM allow you change some configuration parameters on the port, use **ip rip receive-version** to configure the version of RIP messages that be received by current port. You can ignore a certain version and do not handle it. When the port is configured to receive RIPv2, RIPv1 messages need not to be received. When the port is configured to receive *donotreceive*, the port will not receive rip messages. By default, the version of the RIP messages that can be received by current port can be configured as all. Use **no ip rip receive-version** to restore default configuration. Use **ip rip send-version** to configure the version of the RIP messages that current port can send out. By default,

only version 1 RIP message can be sent out from current port, and when the port is configure to receive *donotsend*, any RIP message can be sent out from the port. Use **no ip rip send-version** to restore current port sending version to default version.

Specified operation is shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip ifNum	Switch to three layer interface configuration mode
3	ip rip receive-version { v1 v2 v1v2 donotrecieve }	Configure the version of the RIP message that can be received by current port
4	ip rip send-version { v1 multicastv2 broadcastv2 donotsend }	Configure the version of the RIP message that can be received by current port

3.2.5 The authentication mode of port RIP protocol

ISCOM allows configure man to change the authentication method of RIP interface protocol, but to all the routings that is connected with the same network, the validation and password must keep the same, otherwise the routing may lose connection between each other. Use **ip rip auth-mode** to configure the authentication mode of current RIP protocol or it does not need authentication. Only RIPv2 supports authentication, while RIPv1 does not, but RIPv1 can be configured success. **No ip rip auth-mode** can help restore default configuration.

In interface configuration mode, the authentication mode of interface RIP protocol can be change in the following way:

step	Command	Description
1	config	Enter global configuration mode
2	interface ip ifNum	Switch to three-layer interface configuration mode
3	ip rip auth-mode { none text }	Configure the interface RIP protocol validation access

3.2.6 Configure port additional metric value

Use **ip rip metric-default** to configure the additional metric value that current port gives to received RIP routing, which stands for the price that the routing needs to take when going through the node. User can change the configuration according to the need. Use **no ip rip default-metric** to restore it to default value.

Step	Command	Description
1	config	Enter global configuration mode

2	interface ip <i>ifNum</i>	Switch to three-layer interface configuration mode
3	ip rip metric-default <i>value</i>	Configure port additional metric value

3.2.7 Configure RIP timer

Use **timer flush** to configure the invalidation cycle of RIP routing that all the ports receive, which is the waiting time the routing changes from invalid to being deleted. Use **no timer flush** to restore it to default value.

Use **time invalid** to configure the life cycle of RIP routing that all the ports receive, which is the waiting time the routing changes from invalid to being deleted. Use **no timer invalid** to restore it to default value.

Use **timer update** to configure the update cycle of all the ports' sending RIP messages and change the frequency that current port sending cycle update messages. Use **no timer update** to restore it default value.

To configure RIP timer, follow the steps below:

Step	Command	Description
1	config	Enter global configuration mode
2	routing rip	Switch to RIP protocol configuration mode
3	timer flush <i>timeout</i>	Configure the waiting time that routing changes from invalid to being deleted
4	timer invalid <i>timeout</i>	Configure the waiting time that routing changes from received to invalid
5	timer update <i>timeout</i>	Configure the update cycle of all the port's sending RIP messages

⚠ Notice:

- When configuring RIP timer, notice the network performance before you change the value of timer, and make uniform configuration to all the routings that are running RIP, to avoid unnecessary network flow or network rout shake.

3.2.8 Configure RIP split-horizon

Split-horizon mechanism stops routing information from going back to the sending direction. You can describe split-horizon like this: if the port that sends RIP routing is the same one that receives RIP routing, then the routing metric value needs to be set infinite before being sent out. Thus, it can prevent network rip from coming into being., and tell neighbor equipments the information that what is unreachable in time, which saves the shrinking time. While broadcasting a invalid routing with 16 path cost will bring in additional information. By default, current port RIP has started split-horizon mechanism. Use **no ip rip split-horizon** to close port split-horizon mechanism.

To configure RIP timer, the operations are shown below:

Step	Command	Description
1	config	Enter global configuration mode
3	interface ip ifNum	Switch to three-layer interface configuration mode
3	no ip rip split-horizon	Disable port split-horizon mechanism

3.3 Monitoring and maintenance

Use some **show** commands to look over routing running situation, the content of routing table and the state of routing protocol and so on, for the convenience of monitoring and maintenance. Follow the commands below to make it:

Command	Description
show ip route	Show routing table
show ip protocol	Show routing protocol and the routing protocol configuration state under port
show ip rip statistics	Show RIP protocol and port static information

Use **show ip route** to check out if RIP connection is normal, and look over RIP routing state to check out if RIP communication is normal.

Raisecom# **show ip route**

Codes: C - Connected, S - Static, R - RIP, O - OSPF

```
-----
C   20.1.1.0[255.255.255.0],is directly connected , Interface 1
C   30.1.1.0[255.255.255.0],is directly connected , Interface 2
R   40.1.1.0[255.255.255.0],Via 30.1.1.4
R   50.1.1.0[255.255.255.0],Via 30.1.1.5
```

Total route count: 4

When RIP connection is established normally, the router will learn corresponding RIP routing, and two routes ahead with R will be shown in the routing table. A RIP routing contains the following information:

1. How router get information (R-from RIP protocol);
2. Destination network and the corresponding mask;
3. The next hop of router (across 30.1.1.4 or 30.1.1.5);

Use **show ip protocol** to look over the configuration information of the routing protocols like OSPF, RIP and so on. When RIP protocol get started, it will inform RIP protocol configuration information, the RIP configuration state of each port, appoint network list and protocol priority for RIP selection router; when RIP protocol is disabled, no information about RIP protocol will be shown. To help use the command, let's take RouterA in figure 3-1 for example an see how it works:

1. Raisecom#show ip protocol

The system will return:

Routing Protocol is 'RIP'

RIP global Enable

Default version control: send version 2(broadcast), receive any version

RIP supply interval is 30 (default 30)second

RIP router expire interval is 180 (default 180)second

RIP router flush interval is 300 (default 300)second

IF	Send	Recv	Metric	Split	Auth-mode	Auth-key	State

1	2(B)	1 2	1	Enable	none		UP
2	2(B)	1 2	1	Enable	none		UP

Routing for Networks:

20.1.1.0 0.0.0.255 active

30.1.1.0 0.0.0.255 active

Distance(default is 120):120

To the message and route send and received by RIP, use the command below for detail:

2、Raisecom#show ip rip statistics

The system will return:

Num of routes changed :8

Num of responses sent to RIP queries :0

interface 1:

The address of this interface is :20.1.1.3

Num of packets discarded :0

Num of routes discarded :0

Num of triggered updates :1

interface 2:

The address of this interface is :30.1.1.3

Num of packets discarded :0

Num of routes discarded :0

Num of triggered updates :1

3.4 Typical configuration example

1) Topology figure

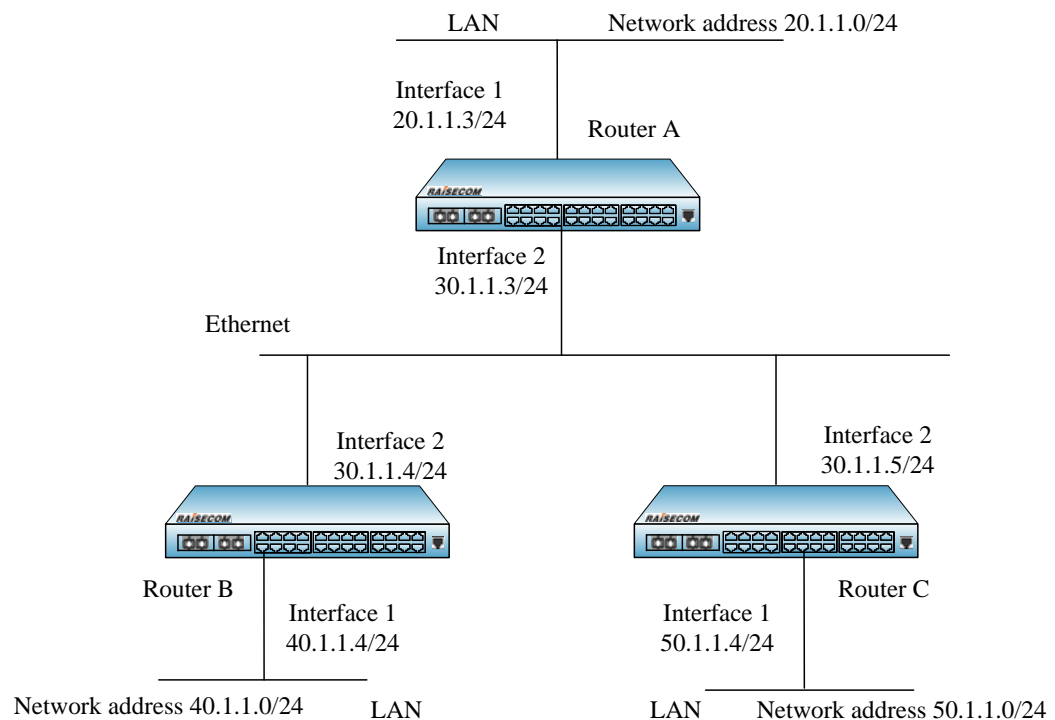


Fig 3-1 RIP configuration example (network structure show)

2) Configuration instruction

As is shown in figure 3-1, RouterA connects to subnet 20.1.1.1/24 using ethernet port. RouterB, RouterC ethernet ports connect to 40.1.1.0/24 and 50.1.1.0/24 respectively. RouterC, Router A and Router B are connected using ethernet 30.1.1.0/24. Follow the figure to configure IP port and port address.

3) Configuration steps

The steps below are only about the operation related with RIP.

! Enable ip routing

Raisecom(config)# **ip routing**

! Configure Router A

Raisecom(config)# **router rip**

Raisecom (config-router-rip)# **network 20.1.1.0 0.0.0.255**

Raisecom (config-router-rip)# **network 30.1.1.0 0.0.0.255**

! Configure Router B

```
Raisecom(config)# router rip

Raisecom (config-router-rip)# network 30.1.1.0 0.0.0.255

Raisecom (config-router-rip)# network 40.1.1.0 0.0.0.255

! Configure Router C

Raisecom(config)# router rip

Raisecom (config-router-rip)# network 30.1.1.0 0.0.0.255

Raisecom (config-router-rip)# network 50.1.1.0 0.0.0.255
```

3.5 RIP trouble shooting

Fault: the physical connection is normal, but the RIP protocol communication between each other is incorrect.

Fault shooting:

Step 1 use **ping** to test if network connection is normal.

Step 2 if it is normal, use **show ip protocols** to examine if RIP has been started normally on both sides, and check out if RIP protocol is valid, if port RIP protocol has been started, that is to check out if the network that port IP address belongs to is in the list appointed by **network**.

Step 3 check out if the configuration about validation on both sides are consistent. If there are validations on both sides, check out if the passwords are same.

Step 4 check out the version limit of sending & receiving RIP messages on connect-through port

Chapter 4 OSPF Configuration

4.1 OSPF overview

OSPF (open shortest path first) is a kind of inner gateway protocol, developed by OSPF work group from Internet Engineering Task Force. This protocol is designed for IP network, which receives outer routing information. All kinds of OSPF messages are encapsulated directly in IP, relays not on other protocols (like TCP, UDP). OSPF supports message validation.

OSPF routing protocol is a kind of link state routing protocol, work on a Autonomous System, which means a group of network that exchange routing information using the uniform routing strategy or routing protocol. In this AS, all the OSPF routers maintain a link state database that describes the topology structure of the whole autonomous system. The link state bulletin in the database describes the state information of corresponding link in the routing domain, like its available interfaces and reachable neighbor routers. Using flooding, the router can broadcast the information to the whole autonomous system.

All the routers run the same algorithm, and establish each other's shortest path tree according to the link state. The shortest path tree gives the shortest route from the router to each destination address in its AS.

OSPF allows several network aggregate to a region, and the structure of the region is invisible to other parts of AS. Using this information hiding, much routing communication can be saved. Beside, because the routing inside the region is decided only by the topology structure of its own, so the region can be protected from the fault routing data. OSPF allows configuring several regions in one AS, but when several regions exist, there must be one backbone region (ID: 0), so that all the regions keep logical connectivity.

OSPF running process:

1. When OSPF protocol is started on router active port, other routers in the same network send out HELLO packets, if there exist two or more routers in all kinds of network that allows multi-addresses visit, 'Designed Router' and 'Backup Designed Router' must be selected in the network. The designed router sees to broadcasting network link state. This concept helps reduce the neighbor relationship number between each switch in the multi-addresses visit network. When the two routers that share the same data link fulfill some designed parameters from the HELLO packets they received, they will become neighbor.
2. The neighbor relationship forms between the routers that exchange routing information.
3. Send LSA among all the routers that have neighbor relationship. LSA describes all the information on router linking, port and link state. These links can reach to STUB network, other OSPF routers, other area's network and outer network (the network that learns routing from another routing process, or the network outside AS). Because there is different types of link state information, OSPF defines several LSA types.
4. HELLO is used to keep the activity state between the neighbors. If the network topology is static, and there are no other activities that raise LSA, it will be sent every 30 minutes.

4.2 Configure OSPF

ISCOM obeys OSPFv2, and supports the following features:

- Stub region – supports stub region concept;
- Certification – supports plain text and MD5 certification among the neighbor routers in the same region;
- Router port parameter configuration – on OSPF port the following parameters can be configured: port output cost, re-sending LSA interval, port transmission delay, router priority, hello time interval, dead time interval, certification, certification key word;
- Virtual-link – virtual link is supported;
- Not-so-stubby-area (NSSA) – RFC 1587;

One of OSPF features is that, the coordination among many inside-the-domain routers, domain edge routers (connected with many regions) and AS edge router is needed. Without any configuration, the state of the router based on OSPF and visiting server is default parameter value, no validation and the port belongs not to any region. If some configuration parameters have been modified, all the switches' configuration must keep the same.

4.2.1 Default OSPF configuration

Function	Default value
OSPF routing protocol	Disable
Designed network RIP protocol	Disable
OSPF interface parameter	Cost : 1 Hello interval: 10s Priority: 1 Retransmit interval: 5s Transmit delay: 1s Dead interval: 4 times hello interval Authentication type: none Authentication password: empty MD5 key: empty
OSPF region parameter	Default cost: 1 Range: disable. Stub: no definition NSSA: no definition
Virtual-link	No definition area ID and Router ID

	<p>Hello interval: 10s</p> <p>Retransmit interval: 5s</p> <p>Transmit delay: 1s</p> <p>Dead interval: 4 times hello interval</p> <p>Authentication type: none</p> <p>Authentication password: empty</p> <p>MD5 key: empty</p>
--	---

4.2.2 Enable OSPF

Use **router ospf** to enable OSPF protocol. Enabling OSPF protocol is the precondition of all the other OSPF configuration tasks. In global configuration mode, type the following commands:

Step	Command	Description
1	config	Enter global configuration mode
2	router ospf	Enable OSPF

Use **no router ospf** to disable OSPF protocol.

4.2.3 Enable the designed network OSPF protocol and appoint region ID

All the ports of the switches that is running OSPF need to be configured into the same region, if there exist several regions in the autonomous system, BackBone (region ID is 0) must be configured.

In OSPF routing protocol configuration mode, use **network** to enable the port that belongs to the command designed network, create a region and add the port to the region. If there is no port that belongs to the command designed network, use the command and the system will create region for only. Specific operations are as follows:

Step	Command	Description
1	config	Enter global configuration
2	router ospf	Enable OSPF, and turn to protocol configuration mode
3	network <i>network-number netmask area</i> <i>area-id</i>	Enable the port that is running OSPF, and define the port region ID

4.2.4 Configure OSPF interface parameter

ISCOM allows configure-man change some configuration parameters, but to all the routers that connect to the same network, some specific parameters must be kept the same. These parameters includes: hello-interval, dead-interval, authentication mode and password. If these parameters had been configured in one of the routers in the network, the other routers' configuration must be kept the

same with the first one, or the routers will lose connection.

In interface configuration mode, follow the steps below to configure port parameters:

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip <i>ifNum</i>	Turn to three-layer interface configuration mode
3 (optical)	ip ospf cost <i>cost</i>	Configure transmission cost for the port
4 (optical)	ip ospf dead-interval <i>seconds</i>	Configure neighbor dead time interval, that is if there is no HELLO message received from a neighbor in the time interval, then the node will take it as losing connection with the neighbor
5 (optical)	ip ospf hello-interval <i>seconds</i>	Configure the time interval of sending HELL message
6 (optical)	ip ospf priority <i>priority</i>	Configure router priority, which is used for DR/DBR polling.
7 (optical)	ip ospf retransmit-interval <i>seconds</i>	Configure the time interval of port re-sending link state broadcast, the unit is second.
8 (optical)	ip ospf transmit-delay <i>seconds</i>	Configure the delay value of port transmitting link state broadcast.
9 (optical)	ip ospf authentication-type { simple-password message-digest none }	Configure port authentication mode.
10 (optical)	ip ospf authentication-password <i>string</i>	Configure port authentication mode to simple password authentication.
11 (optical)	ip ospf message-digest-key <i>keyid</i> md5 <i>key</i>	Configure port MD5 authentication

△ Notice:

- By default dead-interval is four times of hello-interval, when hello-interval is modified, dead-interval will be modified automatically with four times relationship. But if only dead-interval is modified, hello-interval will not be changed.

4.2.5 Configure OSPF region parameters

Configure-man can configure stub region, NSSA region, ABR to stub or the cost of NSSA region default router, aggregate region routing.

Stub region is a region that the outer routing information of the router will not flood to, which decreases the size of link state database, and saves the resource cost of each router processing outer routing information inside the region. The Area Border Router that connects to stub region must use summary-LSAs to proclaim a default link to stub region, these default routing flood in stub region. To decrease more LSA, you can install **no-summary** on stub region border router to configure stub region to totally stubby region, totally stubby region stops not only autonomous system outer routing information flooding but also all summary-LSAs flooding, except summary-LSAs by default.

NSSA (Not-So-Stubby area) is region that does not accept any routing information outside autonomous system, except the routing information sent with LSA TYPE 7. You can also install **no-summary** on border routers of NSSA region, so that the NSSA region stops not only the routing information flood outside LSA TYPE 7 but also all the summary-LSAs flood, except summary-LSAs by default.

Area default-cost command is used only in ABR that is connected to stub or NSSA region. The command configures the cost from ABR to stub/NSSA region default routing.

Border region router can be region centralized or aggregation router. Single aggregation routing uses ABR for other regions' broadcasting, so that routing information can be reduced at region border. Outside the region, each address range will aggregate a routing broadcasting, so that routing table can be reduced. Command parameter means if aggregation routing will be broadcasted.

Step	Command	Description
1	config	Enter global configuration mode
2	router ospf	Enable OSPF, and turn to protocol configuration mode
3 (optical)	area area-id stub [no-summary]	Configure the region to stub region
4 (optical)	area area-id nssa [no-summary]	Configure the region to NSSA region
5 (optical)	area area-id default-cost cost	Configure the default routing cost from ABR to stub or NSSA region
6 (optical)	area area-id range ip-address mask [[advertise not-advertise]]	Aggregate the designed region to designed network routing, if there is advise in the command, then a type 3, aggregated LSA affiche aggregation routing will form. If not-advertise exists in the command, then it will not form.

⚠ Notice:

- Only when both routers are in the same stub region can they form neighbor relationship, if two routers are within the same network, but one is in stub region while the other one is not, then the two router can not form neighbor relationship, nor can they exchange link state information.

4.2.6 Establish/configure virtual link

Virtual link is used to restore or enhance backbone connection, which can be configured between the two ABR in the same region and each of which has a port. Because backbone region must keep logical connection, so if the two nodes in the backbone region have no region routing, or if there is backbone region logical abruption, virtual link must be configured to keep the backbone connection. What's else, by configuring a virtual link from not-backbone region to backbone region, the redundancy rate of backbone region can be enhanced to raise its connection.

Virtual link is marked by the opposite side router ID, the region that provides routing for virtual link is Transmit Area, it is needed to designate Transmit Area when configuring virtual link. A virtual link will be enabled when router finds out its virtual neighbor routing, which can be seen as a unnumbered port to port link in backbone region. So you can configure virtual port parameter.

Virtual link configuration is in OSPF routing protocol configuration mode

Step	Command	Description
1	config	Enter global configuration mode
2	router ospf	Enable OSPF and turn to protocol configuration mode
3 (optical)	area area-id virtual-link router-id [hello-interval hello-interval] [retransmit-interval retransmit-interval] [transmit-delay transmit-delay] [dead-interval dead-interval] [authentication-type {simple-password message-digest none}] [authentication-key authentication-key] [message-digest-key message-digest-key md5 md5]	Create and configure virtual link

⚠ Notice:

- Virtual link can not be configured to cross stub region, and it must be configured between two ABR. It will change from state DOWN to up before it finds out ABR routing.

4.3 Monitoring and maintenance

Use **show** to show some special data , it helps watching OSPF running state, and handling the running problem. In privileged mode run the commands below:

Command	Description
show ip route	Show routing table
show ip protocol	Show routing protocol and port routing protocol configuration
show ip ospf	Show OSPF collective information
show ip ospf database	Show link state information bank
show ip ospf interface	Show port information in designed port mode
show ip ospf neighbor [router-id]	Show neighbor information
show ip ospf virtual-link	Show virtual link information

1. Show OSPF main information

For example: RAISECOM# **show ip ospf**

OSPF region				
Region ID	port number	SPF running times	region type	
1	2	180	neither Stub nor NSSA	
2	1	35	neither Stub nor NSSA	
3	1	11	Stub	
4	1	25	NSSA	

2. Show all the OSPF region link state database information

For example: Raisecom# **show ip ospf database**

Router ID 20.0.0.1

Region: 1

LSA type	Link state ID	Affiche router	Time	Serious number	Checksum
1	10.0.0.1	10.0.0.1	481	0x80000007	0x86C0
1	13.0.0.2	13.0.0.2	743	0x80000002	0x61AD
3	10.0.0.0	10.0.0.1	732	0x8000000B	0xF63F
3	13.0.0.0	10.0.0.1	2103	0x80000002	0xE359
3	172.22.0.0	13.0.0.2	743	0x80000002	0x4249

Region: 2

LSA type	Link state ID	Affiche router	time	serious number	Checksum
1	10.0.0.1	10.0.0.1	936	0x800000011	0x49F1
1	10.0.0.2	10.0.0.2	538	0x80000008	0x6B86
2	10.0.0.2	10.0.0.2	538	0x80000003	0x7593
3	13.0.0.0	10.0.0.2	923	0x80000001	0x42CD
3	12.0.0.0	10.0.0.2	880	0x80000001	0xEA30

3 172.22.0.0 10.0.0.2 738 0x80000001 0x2831

4.4 Typical configuration example

The following are some OSPF configuration examples:

- OSPF router configuration with different identities.
- Virtual link configuration;

Example 1: OSPF router configuration with different identities.

1) Topology figure, as is shown in 4-1

Figure 4-1 shows the network figure of a OSPF configuration example. You can see that there exists several OSPF regions and router, inner router, affiche border router with several identities.

2) Configuration explanation

OSPF basic configuration needs 3 necessary steps:

- Confirm which region each router port is bind to.
- Use **router ospf** to start OSPF protocol.
- Use **network** to add the designated port to specific region and run OSPF protocol.

Notice: **area** areaid **stub no-summary** can be configured on stub region border router for only. **area** areaid **nssa no-summary** can be configured on nssa region border router for only.

3) Configuration step

Configure router A – inner router

! Configure interface 0

Raisecom(config)# **interface ip 0**

Raisecom (config-if)# **ip address 192.108.1.1 255.255.255.0 1**

! Configure OSPF protocol

Raisecom (config)#**router ospf**

Raisecom (config-router-ospf)#**network 192.108.1.0 0.0.0.255 area 1**

Configure router B – inner router

! Configure interface 6

Raisecom (config)#**interface ip 6**

Raisecom(config-if)#**ip address 192.108.1.2 255.255.255.0 2**

! Configure OSPF

Raisecom (config)#**router ospf**

Raisecom (config-router-ospf)#**network 192.108.1.0 0.0.0.255 area 1**

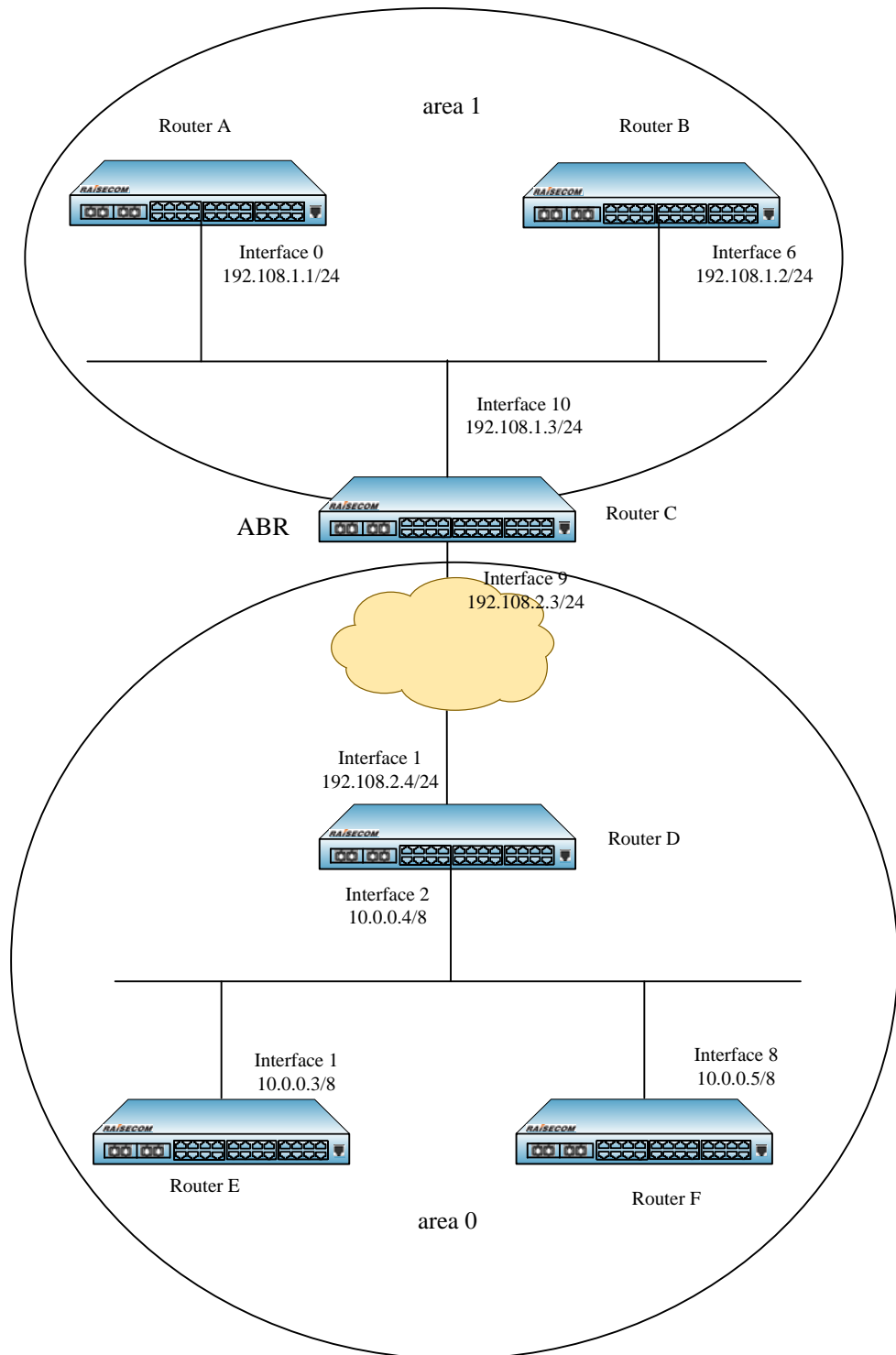


Fig 4-1 OSPF different identities router configuration

Configure router C – ABR

! Configure interface 10

```
Raisecom (config)#interface ip 10
```

```
Raisecom (config-if)#ip address 192.108.1.3 255.255.255.0 1
```

! Configure OSPF protocol

```
Raisecom (config)#router ospf
```

```
Raisecom (config-router-ospf)#network 192.108.1.0 0.0.0.255 area 1
! Configure interface 9
Raisecom (config)#interface ip 9
Raisecom (config-if)#ip address 192.108.2.3 255.255.255.0 1
! Configure OSPF protocol
Raisecom (config)#router ospf
Raisecom (config-router-ospf)#network 192.108.2.0 0.0.0.255 area 0

Configure router D – inner router
! Configure interface 1
Raisecom (config)#interface ip 1
Raisecom (config-if)#ip address 192.108.2.4 255.255.255.0 1
! Configure OSPF protocol
Raisecom (config)#router ospf
Raisecom (config-router-ospf)#network 192.108.2.0 0.0.0.255 area 0
! Configure interface 2
Raisecom (config)#interface ip 2
Raisecom (config-if)#ip address 10.0.0.4 255.0.0.0 2
! Configure OSPF protocol
Raisecom (config)#router ospf
Raisecom (config-router-ospf)#network 10.0.0.0 0.255.255.255 area 0

Configure router E – inner router
! Configure interface 1
Raisecom (config)#interface ip 1
Raisecom (config-if)#ip address 10.0.0.3 255.0.0.0 1
! Configure OSPF protocol
Raisecom (config)#router ospf
Raisecom (config-router-ospf)#network 10.0.0.0 0.255.255.255 area 0

Configure router F – inner router
! Configure interface 8
Raisecom (config)#interface ip 8
Raisecom (config-if)#ip address 10.0.0.5 255.0.0.0 2
```


! Configure OSPF protocol

```
Raisecom (config)#router ospf
```

```
Raisecom (config-router-ospf)#network 10.0.0.0 0.255.255.255 area 0
```

Example 2: virtual link configuration

1) Topology figure 4-2

2) Configuration instructure

Figure 4-2 shows a network topology structure that is not so well designed. Suppose there is no Router E in the figure, and there are four routers in the backbone region, suppose the link between A and B has been broken, then it will lead to backbone region abruption. Router C and D can not communicate with each other. If the two router are the only ABR of each other's region, it will lead to routing information block between the regions. The best way for this problem is to add a redundant actual physical link, but to some reason, the physical link between C and D can not be established. Then we can take a compromising way: establish a virtual link between A and B to keep the connection. Notice, you'd better not use virtual link in actual working, because the existence of virtual link show the shortage of the network design, and the network is not in good state.

3) Configuration steps:

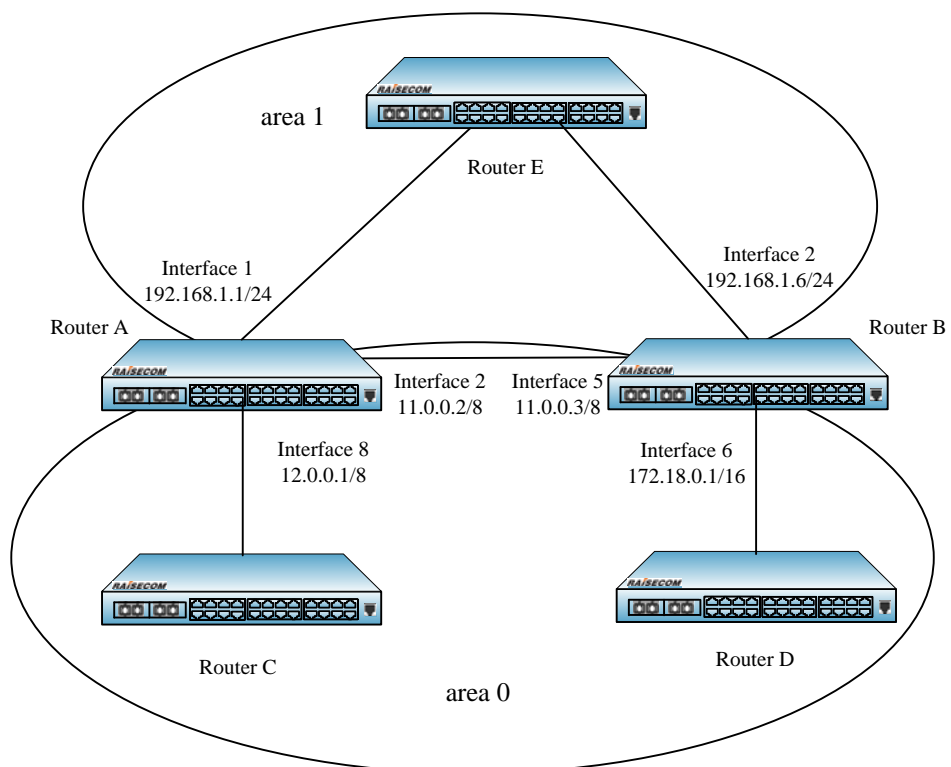


Fig 4-2 Virtual link configuration

Configure router A

! Configure interface 1

```
Raisecom(config)#interface ip 1
```

```
Raisecom(config-if)#ip address 192.168.1.1 255.255.255.0 1
```

```
! Configure interface 8
Raisecom(config)#interface ip 8
Raisecom(config-if)#ip address 12.0.0.1 255.0.0.0 4

! Configure interface 2
Raisecom(config)#interface ip 2
Raisecom(config-if)#ip address 11.0.0.2 255.0.0.0 3

! Configure OSPF protocol
Raisecom(config)#router ospf
Raisecom(config-router-ospf)#network 12.0.0.0 0.255.255.255 area 0
Raisecom(config-router-ospf)#network 11.0.0.0 0.255.255.255 area 0
Raisecom(config-router-ospf)# network 192.168.1.0 0.0.0.255 area 1
Raisecom(config-router-ospf)# area 1 virtual-link 192.168.1.6


Configure router B

! Configure interface 5
Raisecom(config)#interface ip 5
Raisecom(config-if)#ip address 11.0.0.3 255.0.0.0 1

! Configure interface 6
Raisecom(config)#interface ip 6
Raisecom(config-if)#ip address 172.18.0.1 255.255.0.0 4

! Configure interface 2
Raisecom(config)#interface ip 2
Raisecom(config-if)#ip address 192.168.1.6 255.255.255.0 3

! Configure OSPF protocol
Raisecom(config)#router ospf
Raisecom(config-router-ospf)#network 11.0.0.0 0.255.255.255 area 0
Raisecom(config-router-ospf)#network 172.18.0.0 0.0.255.255 area 0
Raisecom(config-router-ospf)# network 192.168.1.0 0.0.0.255 area 1
Raisecom(config-router-ospf)#area 1 virtual-link 192.168.1.1
```

4.5 OSPF trouble shooting

Fault case 1:

Two straight connecting router have all been configured OSPF protocol on the same network port, but the protocol can not work well, and the two sides can not reach FULL state.

Trouble shooting:

Step 1: check out if all the ports have correct address and mask.

Step 2: check out if each port has been configured to the correct region, the two ports needs to be in the same region.

Step 3: check out if the physical connection and underlayer protocol is running normally. Use **ping** to examine it, if local router can not ping the opposite router through, it means that the physical connection and underlayer protocol have problems. In addition, if the port is POS type, check out if PPP protocol has been encapsulated, that is to run **encapsulation PPP**.

Step 4: check out if the interface parameter of each router is the same type, which includes hello-interval, dead-interval and authentication type and password.

Step 5: if one area is configured to stub region, then all the routers connected to the region should configure the region to stub region, or the communication can not be established.

Fault 2:

When there are several regions configured in the network, the routing information of each region is incomplete.

Trouble shooting:

When 2 or more regions exists, backbone region (region ID: 0) must be configured to ensure the region connection.

Fault 3:

When virtual link is configured, use **show ip ospf virtual-link** and find that virtual port is not in active state.

Trouble shooting:

Step 1: check out the cross region of virtual link, it can not go through stub region

Step 2: check out ABR routing, if there is not then virtual port can not be in active state.



北京瑞斯康达科技发展有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road,
Haidian District, Beijing Postcode: 100085 Tel: +86-10-82883305 Fax: +86-10-82883056
Email: export@raisecom.com <http://www.raisecom.com>