Quant

ELEVATING TECHNOLOGY

Switch Layer 3 Function Configuration Manual

Switch Layer 3 Function Configuration Manual

Version V1.0

Q-M-4800-24P-L3-4S-V	Q-M-4800-48P-L3-4S-V	Q-IE-6600-28P-L3-4G-E	Q-IE-6600-48P-L3-4G-E
Q-EP-9300-24P-L3-4G	Q-EP-9300-48P-L3-4G	Q-IE-9600-24P-L3-4G-E	Q-IE-9600-48P-L3-4G-E

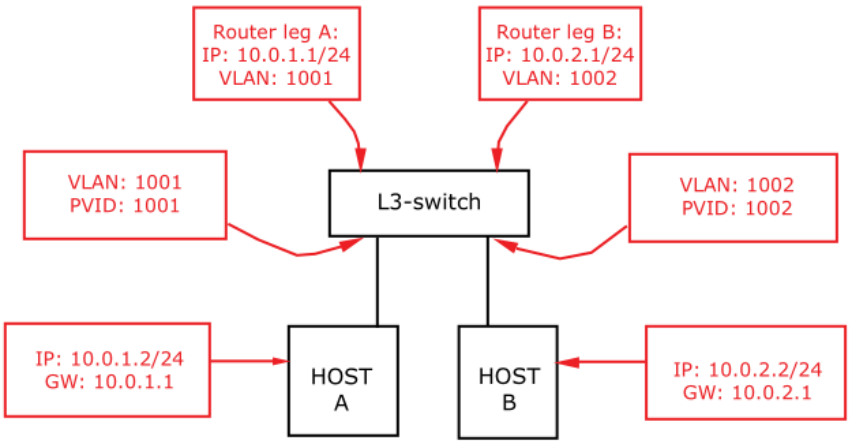
Table Of Contents

1. Layer 3 interface configuration

1.1. Overview

A Layer 3 sub-interface is a virtual interface. Its biggest feature is that Layer 3 attributes such as IP address can be configured so that the interface can be directly accessed by users through the IP address.

1.2. Networking Scenario



1.3. Configuration example

1.3.1. Create VLAN sub-interface

Action	Command	Description
Enter CONFIG mode	**configure terminal**	-
Create a Layer 3 VLAN sub-interface	**interface vlan** VLAN_ID	- VLAN_ID is an existing VID, the value range is <1-4095>

Note: Before applying a Layer 3 VLAN sub-interface, you must create a Layer 2 VLAN ID in CONFIG mode and add the corresponding port to the VLAN.

1.3.2. Deleting VLAN sub-interfaces

Action	Command	Description
Enter CONFIG mode	**configure terminal**	-
Delete VLAN sub-interface	**No interface VLAN** VLAN_ID	-VLAN_ID is an existing VID, the value range is <1-4095>

1.3.3. Configuring the IP address of the VLAN sub-interface

Action	Command	Description
Enter CONFIG mode	**configure terminal**	-
Enter Layer 3 VLAN sub-interface configuration mode	**Interface vlan** VLAN_ID	- VLAN_ID is an existing VID, and the value range is <1-4095>. Before entering VLAN sub-interface configuration mode, you need to execute Interface VLAN VLAN_ID to create a VLAN sub-interface. eg. Enter the VLAN 10 sub-interface configuration mode: Interface VLAN 10

Configure the IP address of the VLAN sub-interface	**Ip|ipv6 address [**<ipv4_addr> <ipv4_netmask>]|[<ipv6_addr > <ipv6_netmask>]	- <ipv4_addr>:The IP address of the Layer 3 VLAN interface, in dotted decimal format. - <ipv4_netmask>:Subnet mask of IP address.
Delete all IP addresses and their tags of vlan sub-interfaces	**no ip address**	

Note: Deleting all IP addresses of the VLAN sub-interface will cause the switch network to fail. Please use it with caution!

1.3.4. Display VLAN sub-interface information

Action	Command	Description
Display the summary of IP information for all interfaces	**show ip interface brief** **show ipv6 interface brief**	Indicates the status of the IPV4/IPV6 interface
Display address information of all VLAN sub-interfaces	**show interface vlan**	
Display the address information of the specified Layer 3 VLAN sub-interface	**show interface vlan** VLAN_ID	-VLAN_ID is an existing VID, the value range is <1-4095>

1.3.5. Create loopback

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Create a Layer 3 loop back	**int loopback** <1-2>	

1.3.7. Deleting loopback

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Delete loopback	no **int loopback** <1-2>	

1.3.8. Configuring the IP address of the loopback

Action	Command	Description
Enter CONFIG mode	**configure terminal**	-
Enter Layer 3 **loopback** configuration mode	**Interface loopback** <1-2>	
Configure the IP address of the **loopback**	**Ip|ipv6 address [**<ipv4_addr> <ipv4_netmask>]|[<ipv6_addr> <ipv6_netmask>]	- <ipv4_addr>:The IP address of the Layer 3 VLAN interface, in dotted decimal format. - <ipv4_netmask>:Subnet mask of IP address.
Delete all IP addresses and their tags of	**no ip address**	

1.3.4. Display loopback information

Action	Command	Description
Display the summary of IP information for all interfaces	**show ip interface brief** **show ipv6 interface brief**	Indicates the status of the IPV4/IPV6 interface
Display address information of all loopback	**show interface loopback**	
Display the address information of the specified loopback	**show interface loopback** <1-2>	

2. Layer 3 forwarding configuration

2.1. Overview

In a local area network, when a host or other network device has data to send to another host or device, it must know the IP address of the other host or device, but only having an IP address is not enough, because IP data packets must be encapsulated into frames to pass Physical network transmission, so the sending station must also have the physical address of the receiver, so a mapping from IP address to physical address is required. ARP is the protocol that implements this function.

2.2. Configuration example

2.2.1. ARP management

Action	Command	Description
clear arp dynamic cache	**clear ip arp**	-
Enter CONFIG mode	**configure terminal**	
Enter Layer 3 VLAN sub-interface configuration mode	**Interface vlan** VLAN_ID	

2.2.2. Display ARP information

Action	Command	Description
Display all arp list information	**clear ip arp**	-

2.2.3. ND management

Action	Command	Description
Clear ND dynamic information	**clear ipv6 neighbor**	-
Enter CONFIG mode	**configure terminal**	
Enter Layer 3 VLAN sub-interface configuration mode	**Interface vlan** VLAN_ID	

2.2.4. Display ND information

Action	Command	Description
Display all ND list information	**show ipv6 neighbor**	-

2.3. Static routing configuration

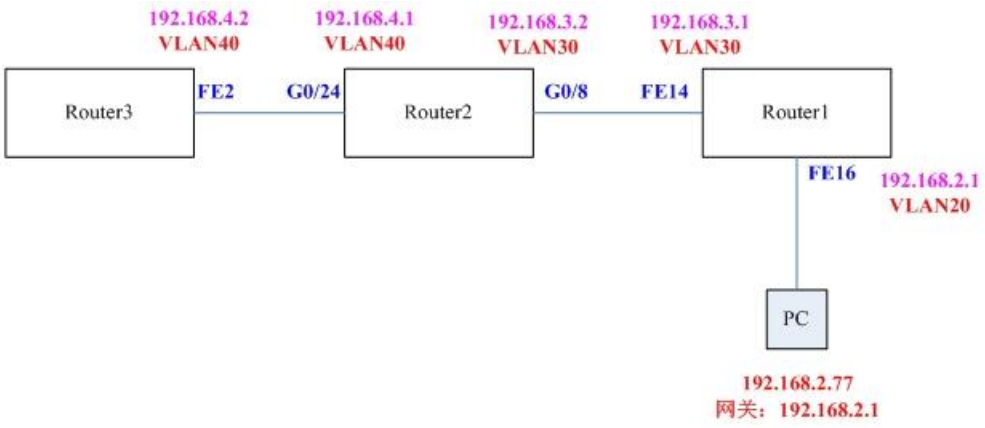
2.3.1. Overview

The static route is manually configured by the administrator. After the static route is configured, the data packets to the specified destination will be forwarded according to the path specified by the administrator.

In a network with a relatively simple network structure, only static routes can be configured to achieve network interoperability. Properly setting and using static routes can improve network performance and guarantee bandwidth for important network applications.

The disadvantage of static routing is that it cannot automatically adapt to changes in network topology. When a network failure or topology changes, routes may become unreachable, resulting in network interruption. At this time, the network administrator must manually modify the configuration of static routing.

2.3.2. Networking Scenario



2.3.3. Configuration example

2.3.3.1. Add static route

Action	Command	Description
Enter CONFIG mode	**configure terminal**	-
Add a static route to a destination network segment via a specified gateway	**ip route** <ipv4_addr> <ipv4_netmask> <ipv4_ucast> **(***distance***)**	-<ipv4_addr>: The destination network of the static route, in dotted decimal format, the last digit is 0. - <ipv4_netmask>: The subnet mask of the destination network, expressed in dotted decimal. - <ipv4_ucast>: The next hop address of the static route, in dotted decimal format. - distance: the administrative distance of the route, the value range is <1-255>, optional.
Add IPv6 static route	**ipv6 route** <ipv6_subnet> **{**<ipv6_ucast>	<ipv6_subnet> : IPv6 prefix x:x::y/z. <ipv6_ucast>: IPv6 unicast address (except link-local address) of

Note:

The destination address and mask are configured with all zeros (0.0.0.0/0), indicating

that the default route is configured.

The specified next-hop address cannot be the IP address of the local interface.

eg:

#Add a static route to the network segment 192.168.4.0/24 via 192.168.3.2 on Router1(config)#ip route 192.168.4.0 255.255.255.0 192.168.3.2 #after that, the PC can ping 192.168.16.4.1

2.3.3.2. Deleting static routes

Action	Command	Description
Enter CONFIG mode	**configure terminal**	-
Delete a static route to a destination network segment	**no ip route** <ipv4_addr> <ipv4_netmask> <ipv4_ucast>	-<ipv4_addr>: The destination network of the static route, in dotted decimal format, the last digit is 0. -<ipv4_netmask>: The subnet mask of the destination network, expressed in dotted decimal. -<ipv4_ucast>: Specifies the next hop address of the static route to be deleted, in dotted decimal format, this parameter defaults to delete all static routes to a certain destination network segment.
Delete IPv6 static routes	**no ipv6 route** <ipv6_subnet> {<ipv6_ucast>}	<ipv6_subnet> :IPv6 prefix x:x::y/z. <ipv6_ucast> : IPv6 unicast address (except link-local address) of

eg:

#Delete a static route (config) on Router1 that reaches the 192.168.4.0/24 network segment via 192.168.3.2#no ip route 192.168.4.0 255.255.255.0 192.168.3.2#after the PC can no longer ping 192.168.16.4.1

3. RIP protocol

3.1. Protocol introduction

RIP is a distance vector protocol with hop count as a metric. RIP is widely used in global Internet routing and is an interior gateway protocol (IGP). It allows more information to be included in RIP packets and provides a simple MD5 authentication mechanism. RIP is a relatively simple interior gateway protocol. Because the implementation of RIP is relatively simple, and it is far easier than OSPF and IS-IS in terms of configuration, maintenance, and management, it is still widely used in actual networking. Mainly used in smaller networks, such as campus networks and regional networks with simpler structures.

3.1.1. Display routing information

Action	Command	Description
show routing information	show ip route	Indicates that all current routing information is displayed

3.2. Configuration preparation

Before configuring the basic functions of RIP, you need to complete the following tasks: Configure the network layer address of the interface to make the network layer of adjacent nodes reachable.

3.3. Configure the basic functions of RIP

3.3.1. Start RIP and configure the network segment range

Action	Command	Description
Enter CONFIG mode	**configure terminal**	-
Create a RIP process and enter RIP configuration mode	**router rip**	Required. By default, the RIP process is closed. Required. By default, the RIP function on an interface is disabled. - A.B.C.D: Specify the network segment - <wildcard-mask>: Inverse mask, such as 0.0.0.255
Enable RIP on the specified network segment interface	**network** *A.B.C.D* *<wildcard-mask>*	<ipv6_subnet> :IPv6 prefix x:x::y/z. <ipv6_ucast> : IPv6 unicast address (except link-local address) of

Note: If RIP-related commands are configured in interface mode before RIP is started, these configurations will take effect only after RIP is started.

RIP only runs on the interface of the specified network segment. For the interface that is not on the specified network segment, RIP neither receives and sends routes on it nor forwards its interface routes. Therefore, after the RIP is started, its working network segment must be specified.

3.3.2. Configure RIP version

Users can configure the RIP version in RIP mode, or configure the RIP version on the interface:

If an interface is not configured with a RIP version, the RIP version running on the interface will be based on the globally configured version.

If you want the RIP version configured on the interface to be different from the global configuration, enter the interface mode to configure the RIP version running on the interface.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter RIP configuration mode	**router rip**	-
Configure the global RIP version	**version** {**1**|**2**}	By default, if an interface is configured with a RIP version, the interface configuration shall prevail. If the interface is not configured, the interface only sends RIPv2 multicast packets.
Return to CONFIG mode	**exit**	-
Enter Layer 3 interface configuration mode	**interface vlan** <VLAN-ID>	- <VLAN-ID>: Layer 3 interface name
Configure the RIP version that the interface can receive	**ip rip receive version {1|2|all | none}**	Configure 1 and 2 to receive rip packets of version 1 and version 2, configure 1 to receive only 1, and configure 2 to receive only 2, otherwise, filter
Configure the RIP version sent by the interface	**ip rip send version {1|2|all | none}**	Configure 1 and 2 to send rip packets of version 1 and version 2, configure 1 to send only 1, configure 2 to send only 2, otherwise filter

3.4. Configuring RIP Routing Features

In practical applications, it is sometimes necessary to control the RIP routing information more precisely to meet the needs of complex network environments.
Before configuring the RIP routing feature, complete the following tasks:

Configure the network layer address of the interface to make the network layer of adjacent nodes reachable.
Configuring basic functions of RIP.

3.4.1. Configuring RIP to redistribute information from another routing protocol

If the router runs not only RIP but also other routing protocols, you can configure RIP to import routes generated by other protocols, such as OSPF static routes or directly connected routes.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter RIP configuration mode	**router rip**	-

Configure RIP to redistribute information from another routing protocol	**redistribute {bgp|connected|static | ospf} metric<0-16>**	By default, RIP does not import other routes bgp : The OSPF redistributed for the bgp routes. connected : The OSPF redistributed for the connected interfaces. Ospf: The OSPF redistributed for the ospf routes. Static: The OSPF redistributed for the static routes. Metric:<0-16>
Clear RIP to redistribute information from another routing protocol	**no redistribute {bgp|connect|static|ospf}**	
Configuring RIP to import default routes	**default-route originate**	
Clear RIP to import default routes	**no default-route originate**	
Configure the metric of routes imported by RIP	**default-metric<1-16>**	
Clear the metric of routes imported by RIP	**no default-metric<1-16>**	

3.4.2. Configure the distance of RIP routing

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter RIP configuration mode	**router rip**	-
Configure the distance of the RIP route	**distance <1-255>**	
Clear distance of RIP route	**no distance <1-255>**	

3.4.3. Configure passive-interface for RIP routing

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter RIP configuration mode	**router rip**	-
Configuring passive-interface for RIP routing	passive-interface**{default|vlan}** **<vlan_list>**	**default :all interfaces as passive-interface Vlan:VLAN interface**
Clear passive-interface for RIP routing	**no** passive-interface**{default|vlan}** **<vlan_list>**	

3.5. Adjust and optimize the RIP network

In some special network environments, the performance of the RIP network needs to be adjusted and optimized. Before adjusting the RIP, the following tasks need to be completed:

Configure the network layer address of the interface to make the network layer of adjacent nodes reachable

Configuring basic functions of RIP

3.5.1. Configuring split horizon and poison reversal

Note:

If both split horizon and poison reversal are configured, only the poison reversal function will take effect.

Routing loops can be prevented by configuring split horizon or poison reversal.

3.5.1.1. Configuring split horizon

By configuring split horizon, the routes learned from an interface cannot be advertised through this interface to avoid routing loops between adjacent routers.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter Layer 3 interface configuration mode	**interface vlan** <VLAN-ID>	- <VLAN-ID>: Layer 3 interface name
Enable split horizon	**ip rip split-horizon**	Optional. The split horizon function is enabled by default

Note: Turning off the split horizon function on a point-to-point link has no effect.

3.5.1.2. Configuring Poison Reversal

After poison reversal is configured, the routes learned from an interface can still be advertised from this interface, but the metric value of these routes will be set to 16 (that is, unreachable), which can be used to avoid routing loops between adjacent routers.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter Layer 3 interface configuration mode	**interface vlan** <VLAN-ID>	- <VLAN-ID>: Layer 3 interface name
Enable toxicity reversal function	**ip rip split-horizon poisoned-reverse**	Optional. By default, the poison reversal function is turned on

3.5.2. Configuring the Authentication Mode for RIPv2 Packets

In a network environment with high-security requirements, you can check and verify

the validity of RIPv2 packets by configuring the packet authentication mode.

RIPv2 supports two authentication methods: plaintext authentication and MD5 ciphertext authentication.

Plain text authentication cannot provide security, and the unencrypted authentication word is sent along with the message, so plain text authentication cannot be used in situations with high-security requirements.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter Layer 3 interface configuration mode	**interface vlan**<VLAN-ID>	- <VLAN-ID>: Layer 3 interface name
Configuring the Authentication Mode for RIPv2 Packets	**ip rip authentication mode {text | md5}**	- **text**: plaintext authentication method - **md5**: MD5 ciphertext authentication method No authentication by default
Configure the authentication key for RIPv2 packets	**ip rip authentication string** <word1-16>	- <word1-16>: Secret key, length 1-16

Note: When the RIP version is RIPv1, although the authentication mode can still be configured in interface mode, the configuration does not take effect because RIPv1 does not support authentication.

3.5.3. Configuring RIP Neighbors

Normally, RIP uses broadcast or multicast addresses to send packets. If RIP is run on a link that does not support broadcast or multicast packets, you must manually specify

RIP neighbors.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter RIP configuration mode	**router rip**	-
Configure RIP neighbors	**neighbor** *A.B.C.D*	- A.B.C.D: The IP address of the RIP adjacent routing switch, in dotted decimal format.

Note:

It is not recommended to use the neighbor A.B.C.D command when the RIP neighbor is directly connected to the current device, because this may cause the peer end to receive both multicast (or broadcast) and unicast packets with the same routing information.

When the specified neighbor is not directly connected to the local router, check the source address of the update message must be canceled.

3.6. Display RIP information

After completing the above configuration, run the show command to display the running status of RIP after the configuration, and verify the effect of the configuration by viewing the displayed information.

Action	Command	Description
Display the global RIP protocol to enable status and configuration parameter information	**show ip rip**	
Display RIP routing table information	**show ip route**	

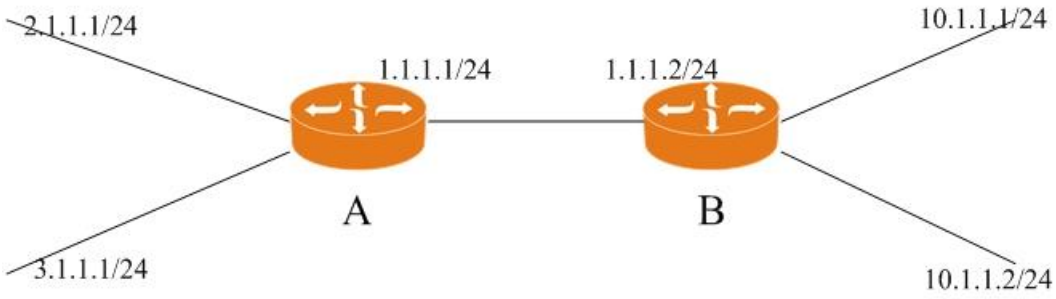
3.7. RIP typical configuration example

3.7.1. Configure the version of RIP

3.7.1.1. Networking Requirements

It is required to enable RIP on all interfaces of Router A and Router B, and use RIPv2 for network interconnection.

3.7.1.2. Network Diagram



3.7.1.3. Configuration steps

Step 1: Configure the IP address of each interface (omitted)

Step 2: Enable RIP function

#Configure Router A.

#configure terminal

(config)#router rip

(config-rip)#network 1.1.1.0 0.0.0.255

(config-rip)#network 2.1.1.0 0.0.0.255

(config-rip)#network 3.1.1.0 0.0.0.255

#Configure Router B.

#configure terminal

(config)#router rip

(config-rip)#network 1.1.1.0 0.0.0.255

(config-rip)#network 10.1.1.0 0.0.0.255

#View the RIP routing table of Router A.

#show ip route

Step 3: Configure the version of RIP

#Configure RIPv2 on Router A.

#configure terminal

(config)#router rip

(config-rip)#version 2

#Configure RIPv2 on Router B.

#configure terminal

(config)#router rip

(config-rip)#version 2

#View the RIP routing table of Router A.

#show ip route

Note: Because the aging time of RIP routing information is long, the routing information of RIPv1 will still exist in the routing table for a period of time after the RIPv2 version is configured.

3.8. Examples of Common Configuration Errors

3.8.1. Cannot Receive RIP Update Packets from Neighbors

3.8.1.1. Symptoms

When the link is normal, the RIP update message from the neighbor cannot be received.

3.8.1.2. Failure Analysis

After RIP is started, you must use the network command to enable the corresponding interface. If the working status of an interface is configured separately, make sure that the relevant interface is not suppressed or prohibited from sending and receiving RIP packets.

If the remote router is configured to send RIP packets in multicast mode, it should also be configured in multicast mode on the local router.

3.8.1.3. Troubleshooting

Step 1: Execute the show running-configuration command to check the RIP configuration.

Step 2: Run the show ip rip command to check whether the relevant RIP interface is enabled.

4. RIPng protocol

4.1. Protocol Introduction

RIPng is a distance vector protocol with hop count as metric. It is an extension of the RIPng-2 protocol in the original IPv4 network. Most RIPng concepts can be used for RIPng. RIPng is a relatively simple interior gateway protocol. Because the implementation of RIPng is relatively simple, and it is far easier to configure, maintain and manage than OSPFv3 and IS-IS for IPv6, it is still widely used in actual networking. Mainly used in smaller networks, such as campus networks and regional networks with simpler structures.

4.2. Configuration Preparation

Before configuring the basic functions of RIPng, you need to complete the following tasks: Configure the network layer address of the interface to make the network layer of adjacent nodes reachable.

4.3. Configure the basic functions of RIPng

4.3.1. Start RIPng and configure the network segment range

Action	Command	Description
Enter CONFIG mode	**configure terminal**	-
Create a RIPng process and enter RIPng configuration mode	**router RIPng**	Required. By default, the RIPng process is closed
Enable RIPng on the interface of the specified network segment	**network** x:x::y/z	Required. By default, the RIPng function on an interface is disabled - x:x::y: IPv6 specified network segment - z: mask length, such as 24
Add routes for RIPng	**route** x:x::y/z	- x:x::y: IPv6 specified network segment - z: mask length, such as 24

Note:

If RIPng-related commands are configured in interface mode before starting RIPng, these configurations will take effect only after RIPng is started.

RIPng only runs on the interface of the specified network segment; for the interface not on the specified network segment, RIPng neither receives and sends routes on it, nor forwards its interface routes. Therefore, after RIPng is started, its working network segment must be specified.

4.4. Configuring RIPng Routing Features

In practical applications, it is sometimes necessary to control the RIPng routing information more precisely to meet the needs of complex network environments.

Before configuring the RIPng routing feature, complete the following tasks:

Configure the network layer address of the interface to make the network layer of adjacent nodes reachable

Configuring basic functions of RIPng

4.4.1. Configuring RIPng to redistribute information from another routing protocol

If not only RIPng but also other routing protocols are running on the router, you can configure RIPng to import routes generated by other protocols, such as bgp routes or directly connected routes.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter RIPng configuration mode	**router ripng**	-
Configure RIPng to redistribute information from another routing protocol	**redistribute {bgp|connected|static| ospf6} metric<0-16>**	By default, RIPng does not import other routes
Clear RIPng to redistribute information from another routing protocol	**no redistribute {bgp|connected|static| ospf6} metric<0-16>**	
Configuring RIPng to import default routes	**default-information originate**	
Clear the default route imported by RIPng	**default-information originate**	
Configure the metric of routes imported by RIP	**default-metric<1-16>**	
Clear the metric of routes imported by RIP	**no default-metric<1-16>**	

4.4.2. Configure RIPng time parameters

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter RIPng configuration mode	**router ripng**	-
Configure RIPng time parameters	**timers 30 180 120**	By default, 30 180 120
Clear RIPng time parameter	no **timers 30 180 120**	

4.4.3. Configuring RIPng aggregation routes

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter RIPng configuration mode	**router ripng**	-
Configuring RIPng aggregation routes	**aggregate-address x:x::y/z**	
Clear RIPng Aggregation Routes	no **aggregate-address x:x::y/z**	

4.5. Adjust and optimize the RIPng network

In some special network environments, the performance of the RIPng network needs to be adjusted and optimized. Before adjusting RIPng, the following tasks need to be completed:

Configure the network layer address of the interface to make the network layer of adjacent nodes reachable

Configuring basic functions of RIPng

4.5.1. Configuring Split Horizon and Poison Reversal

Note:

If both split horizon and poison reversal are configured, only the poison reversal function will take effect.

Routing loops can be prevented by configuring split horizon or poison reversal.

4.5.1.1. Configuring split horizon

By configuring split horizon, the routes learned from an interface cannot be advertised through this interface to avoid routing loops between adjacent routers.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter Layer 3 interface configuration mode	**interface vlan** <VLAN-ID>	- <VLAN-ID>: Layer 3 interface name
Enable split horizon	**Ipv6 ripng split-horizon**	Optional. By default, the horizontal split function is enabled

Description: Turning off the split horizon function on a point-to-point link has no effect.

4.5.1.2. Configuring Poison Reversal

After poison reversal is configured, the routes learned from an interface can still be advertised from this interface, but the metric value of these routes will be set to 16 (that is, unreachable), which can be used to avoid routing loops between adjacent routers.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter Layer 3 interface configuration mode	**interface vlan** <VLAN-ID>	- <VLAN-ID>: Layer 3 interface name

Enable toxicity reversal function	**Ipv6 ripng split-horizon poisoned-reverse**	Optional. By default, poison reversal is turned on

4.6. Display RIPng information

After completing the above configuration, run the show command to display the running status of RIPng after the configuration, and verify the effect of the configuration by viewing the displayed information.

Action	Command	Description
Display the global RIPng protocol enable status and configuration parameter information	**show ipv6 ripng**	
Display RIPng routing table information	**show ipv6 route**	

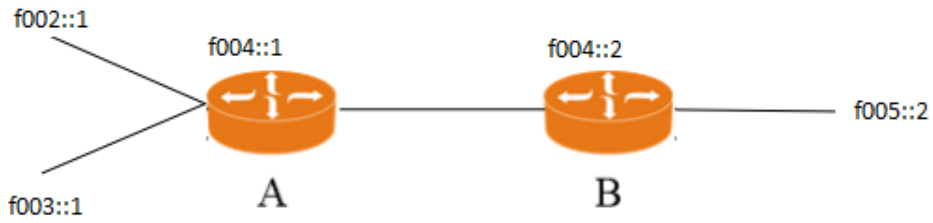
4.7. RIPng typical configuration example

4.7.1. Configure the version of RIPng

4.7.1.1. Networking requirements

It is required to enable RIPng on all interfaces of Router A and Router B, and use the RIPng protocol for network interconnection.

4.7.1.2. Network Diagram



RIPng version configuration network diagram

4.7.1.3. Configuration steps

Step 4: Configure the IP address of each interface (omitted)

Step 5: Enable RIPng function

#Configure Router A.

#configure terminal

(config)#router RIPng

(config-RIPng)#network f002::/24

(config-RIPng)#network f003::/24

(config-RIPng)#network f004::/24

#Configure Router B.

#configure terminal

(config)#router RIPng

(config-RIPng)#network f004::/24

(config-RIPng)#network f004::/24

#View the RIPng routing table of Router A.

#show ipv6 route

4.8. Examples of Common Configuration Errors

4.8.1. Cannot Receive RIPng Update Packets from Neighbors

4.8.1.1. Symptoms

When the link is normal, the RIPng update message from the neighbor cannot be received.

4.8.1.2. Failure Analysis

After RIPng is started, you must use the network command to enable the corresponding interface. If the working state of an interface is configured separately, make sure that the relevant interface is not suppressed or prohibited from sending and receiving RIPng packets.

4.8.1.3. Troubleshooting

Step 3: Run the show running-configuration command to check the RIPng configuration.

Step 4: Run the show ipv6 RIPng command to check whether the relevant RIPng interface is enabled.

5. OSPF protocol

5.1. Protocol Introduction

OSPF (Open Shortest Path First), as an interior gateway protocol (Interior Gateway Protocol, IGP), is used to advertise routing information between routers in the same autonomous area (AS). Different from the distance vector protocol (RIP), OSPF has the advantages of supporting large networks, fast route convergence, and occupying fewer network resources. It occupies a very important position in the currently applied routing protocols. The OSPF router collects the connection state information of each router in the network area where it is located, that is, the link state information (Link-State), and generates a link-state database (Link-State Database). The router

masters the link state information of all routers in the area, which is equivalent to understanding the topology of the entire network. OSPF routers use the Shortest Path First (SPF) algorithm to independently calculate routes to any destination. The OSPF daemon dynamically maintains the routing table, which realizes the value of the routing protocol.

5.2. Configuration Preparation

Before configuring the basic functions of OSPF, complete the following tasks:
Configure the network layer address of the interface to make the network layer of the adjacent node reachable.

5.3. Enable OSPF function

In each configuration task of OSPF, the OSPF function must be enabled before the configurations of other functions and features take effect.
To enable OSPF on a router, you must first create an OSPF process, specify the area associated with the process, and the network segment included in the area; for the current router, if the interface IP address of a router falls on the network segment of an area If the interface belongs to this area and the OSPF function is enabled, OSPF will advertise the directly connected route of this interface.
The Router ID is used to uniquely identify a router in an autonomous system. If a router is to run the OSPF protocol, the Router ID must exist.
Users can specify the Router ID when creating an OSPF process. During configuration, it must be ensured that the IDs of any two routers in the autonomous system are different. The usual practice is to configure the router ID to be the same as the IP address of an interface of the router.
If the router ID is not specified when the OSPF process is created, the global router ID is used by default. It is recommended that users specify the Router ID when creating an OSPF process.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Create OSPF and enter OSPF configuration mode	**router ospf**	By default, the system does not run OSPF
Set router-id	**router-id** *ip-address*	router-id in IP address format. By default, the system obtains the address of an interface according to a certain policy as router-id
Configure the network segment included in the OSPF area and enable OSPF on the interface of the specified network segment	**network** [*ip-address wildcard-mask*] **area** *area-id*	ip-address: the address of the network segment where the interface is located wildcard-mask: IP address inverse mask (similar to the form after the inversion of the IP address mask, where "1" means ignore the corresponding bit in the IP address; and "0" means that the bit must be reserved). area-id: is the ID number of the area to which this address range belongs. By default, the interface does not belong to any area, and the OSPF function is disabled

Note: A network segment can only belong to one area.

5.4. Configuring OSPF Areas

After the network administrator divides the entire network into multiple areas, they can be further configured as stub areas or NSSA areas according to networking requirements.

When the non-backbone area cannot maintain connectivity with the backbone area, or

the backbone area cannot maintain connectivity due to various situations, you can configure OSPF virtual links to solve the problem.

5.4.1. Configuring the Stub Area

For some non-backbone areas located at the edge of the AS, we can configure the stub command on all routers in the area to configure the area as a stub area. In this way, Type 5 LSAs describing external routes of the AS will not be flooded in the stub area, reducing the size of the routing table. The ABR generates a default route, and all packets reaching the outside of the AS are forwarded to the ABR.
If you want to further reduce the size of the routing table in the stub area and the number of routing information transmitted, you can configure the area as a Totally Stub area by specifying the no-summary parameter when configuring the stub command on the ABR. In this way, neither the routing information outside the autonomous system nor the routing information between areas will be transmitted to the local area, and all the packets destined outside the autonomous system and outside the area are sent to the ABR for forwarding.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter OSPF configuration mode	**router ospf**	
Set an OSPF area as a STUB area	**area** *area-id* **stub (no-summary)**	Required. By default, no area is set as a stub area. - area-id: OSPF domain ID. - no-summary: It is forbidden to import Interzone routes in the stub area, and configure the area as a Totally Stub (complete Stub) area.

Note:

All routing devices in a stub area must use the stub command to configure the area as a stub attribute.

The backbone area cannot be configured as a Totally Stub area.

ASBRs cannot exist in a Totally Stub area, that is, routes outside the AS cannot be propagated in this area.

Virtual connections cannot pass through the Totally Stub area.

5.4.2. Configuring NSSA Areas

A stub area cannot import external routes. In order to allow external routes to be advertised into the OSPF routing area while maintaining the characteristics of the rest of the stub area; network administrators can configure the area as an NSSA area.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	Enter CONFIG mode
Enter OSPF configuration mode	**router ospf**	Enter OSPF configuration mode
Configure an OSPF area as an NSSA area	**area** *area-id* **nssa** {no-summary | translator type7 (candidate | never | always) }	Required. By default, no area is set as an NSSA area. - area-id: OSPF area identifier, which can be in decimal integer or IP address format. The integer value range is <0-4294967295>. - **nssa**: This parameter is used to import the default route into the NSSA area, and is only used for the ABR or ASBR in the NSSA area. This parameter contains the following multiple options:

		- **no-summary**: Prohibits the import of Interzone routes into NSSA areas, which are also called Totally NSSA areas. - **translator**: This parameter is used to specify the translation role of the NSSA-ABR router. This parameter contains the following options: **candidate:** If this router is designated as a conversion router, it will convert NSSA-LSAs to Type-5 LSAs. **never:** This router will not translate NSSA-LSA. **always:** The router always converts NSSA-LSAs to Type-5 LSAs.

Note: All routers in the NSSA region must use the nssa command to configure the region as an NSSA attribute.

5.4.3. Configure Virtual Connection

After region division, OSPF routing updates between non backbone regions are exchanged through backbone regions. In this regard, OSPF requires that all non backbone areas must be connected to the backbone area, and the backbone area itself must also be connected.

However, in practical application, this requirement may not be met due to the limitations of various conditions. This can be solved by configuring the OSPF virtual connection on the ABR.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	Enter CONFIG mode
Enter OSPF	**router ospf**	Enter OSPF configuration mode

configuration mode		
Create and configure virtual connections	**area** *area-id* **virtual-link** *A.B.C.D* **[dead-interval** <1-65535> | **hello-interval** <1-65535> | **retransmit-interval** <1-65535> | **transmit-delay** <1-65535> | **authentication [message-digest | null] | authentication-key** *LINE* | **message-digest-key** *<1-255>* **md5** *LINE***]**	Required. -area-id: The identification of the virtual connection's translation area, either in decimal integer or IP address format. -A. B. C. D: ID of the neighbor router of the virtual connection, which must be in the format of IP address. **-dead-interval** <1-65535>: Specifies the interval, in seconds, for the death timer. **-hello-interval** <1-65535>: specifies the time interval for sending Hello message on the interface, and the unit is second. **-retransmit-interval** <1-65535>: specifies the time interval for retransmitting the LSA message on the interface, and the unit is second. **-transmit-delay**<1-65535>: specifies the time interval for delaying the sending of LSA message on the interface, and the unit is second. **-authentication [message-digest | null]**: Specify the authentication method of the virtual connection, where the parameter **message-digest** indicates that MD5 authentication is used, the parameter null indicates that no authentication is required, and the default parameter

		indicates that plaintext authentication is used. **-authentication-key** password: Specifies the plaintext authentication word for the interface, up to 8 characters. -message-digest-key keyid MD5 key: Specifies the MD5 authentication word identifier and the MD5 authentication word for the interface. The value range of keyid is 1 to 255, and key is a string of up to 16 characters.

Note

In order for the virtual connection to work, the routers at both ends of the virtual connection need to configure this command, and the hello-interval, dead-interval, authentication-key, and message-digest-key parameters configured at both ends must be consistent.

The default is 40 seconds for dead-interval, 10 seconds for hello-interval, 5 seconds for retransmit-interval, and 1 second for transmit-delay.

5.5. Configure routing information control for OSPF

Through the configuration in this section, you can control the publication and reception of OSPF routing information, and introduce the routing of other protocols.

5.5.1. Configure OSPF route aggregation

Configure route aggregation: Aggregate OSPF routes on area boundaries.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter OSPF	**router ospf**	

configuration model		
Configure route aggregation for OSPF	**area {***ip-address* |<0-4294967295>**} range** *ip-address-mask* **[not-advertise|advertise|cost]**	By default, routes are not aggregated

5.5.2. Configure the cost value of the OSPF interface

OSPF has two ways to configure the cost values for an interface:

The overhead value is directly configured in the interface mode;

Configure the bandwidth reference value of the interface. OSPF automatically calculates the cost value of the interface according to the bandwidth reference value. The calculation formula is: Interface Cost be equal to Bandwidth Reference Value divide Interface Bandwidth. When the calculated cost value is greater than the 65535, the cost takes the maximum value 65535; when the calculated cost value is less than 1, the cost takes the minimum value 1.

If you do not configure the cost value for this interface in interface mode, OSPF automatically calculates the cost value based on the bandwidth of the interface.

5.5.2.1. Configure cost values for the interface

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter OSPF configuration model	**router ospf**	
Enter interface mode	**interface** vlan <VLAN-ID>	
Set the cost value of the OSPF interface	**ip ospf cost** *cost*	1-65535 By default, the interface automatically calculates the cost based on the current bandwidth.

5.5.3. Configure the administrative priority of the OSPF protocol

Because a router may run multiple dynamic routing protocols at the same time, there is a problem of sharing and selecting routing information among various routing protocols. The system sets a priority for each routing protocol. When different protocols find the same route, the route with higher priority will be selected first.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter interface mode	**interface** vlan <VLAN-ID>	
Configure the routing priority of the OSPF protocol	**ip ospf priority** <0-255>	

5.5.4. Configure OSPF to bring in external routines

5.5.4.1. Configure OSPF to introduce routing for other protocol

If not only OSPF but also other routing protocols are running on the router, OSPF can be configured to introduce routes generated by other protocols, such as RIP, static routes, or directly connected routes, and announce these routing information through Type5 LSA or Type7 LSA.

OSPF can also filter incoming routes, converting only external routes that meet the filter criteria to Type5 LSA or Type7 LSA for publication.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter OSPF configuration model	**router ospf**	
Configure OSPF to introduce routing for	**[no] redistribute {bgp|connected|static|rip}**	Required. By default, no other protocol routing information is

other protocol	**[metric** <0-16777214>**]** **[metric-type** {1|2} **]**	introduced. **bgp | connected | static | rip:** The type of source routing protocol that can be introduced. **Metric** <0-16777214>: (Optional) Configures the metric value for the route. The default is 1. **Metric-type** { 1 | 2 }: (Optional) Configures the metric type. 1 for Type-1 external routing and 2 for Type-2 external routing. The default is 2.

5.5.4.2. Configure OSPF to introduce a default rout

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter OSPF configuration model	**router ospf**	
Configure OSPF Default Routine	**[no] default-information originate [always] [metric** <0-16777214>**] [metric-type** {1|2}**]**	0ptional. By default, there is no default route. a**lways:** (optional) If the local machine is not configured with a default route, use this parameter to generate an ase LSA that describes the default route and publish it; if this keyword is not specified, the local machine must be configured with a default route to introduce the ase LSA that generates the default route. **metric** <0-16777214>: (Optional) Sets the metric value of this ase LSA.

		The value range is 0-16777214. The default value is 1. **metric-type** {1 | 2}: (Optional) Sets the metric type for this ase LSA. The value range is Type-1 or Type-2. The default value is 2.

5.6. Configure OSPF Network Tuning Optimization

Users can adjust and optimize the OSPF network from the following aspects:
By changing the OSPF packet timer, the convergence speed of the OSPF network and the network load brought by the protocol packets can be adjusted. On some low-speed links, it is necessary to consider the delay time for the interface to transmit the LSA.
By adjusting the SPF calculation interval, the problem of resource consumption caused by frequent changes in the network can be suppressed.
In a network with high security requirements, the security of the OSPF network can be improved by configuring the OSPF authentication feature.
At the same time, OSPF supports the network management function. You can configure the OSPF MIB to bind to a certain process and send Trap messages and logs.

5.6.1. Configure OSPF message timer

The user can configure the following OSPF message timers on the interface:
Hello timer: The time interval for the interface to send Hello messages to the neighbors. The value of the Hello timer between OSPF neighbors shall be consistent, and shall be inversely proportional to the route convergence speed and the network load.
Poll timer: In NBMA network, the time interval for a router to send a polling Hello message to a neighbor router whose status is down.
Neighbor invalidation time: During the neighbor invalidation time, if the interface

has not received the Hello message sent by the neighbor, the router will declare the neighbor invalid.

Time interval for interface retransmission of LSA: After the router announces an LSA to its neighbor, the neighbor needs to confirm it. If no acknowledgement message is received from the other party within the retransmission interval, the LSA will be retransmitted to the neighbor.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter interface mode	**Interface vlan** <VLAN-ID>	-
Configure Hello Timer	**ip ospf hello-interval** <1-65535>	By default, the time interval for P2P and Broadcast interfaces to send Hello messages is 10 seconds, and the time interval for P2MP and NBMA interfaces to send Hello messages is 30 seconds.
Configure neighbor expiration time	**ip ospf dead-interval** <1-65535>	The length of time for a neighboring routing switch on an interface to die defaults to 40 seconds.
Configure the time interval of interface retransmission LSA	**ip ospf retransmit-interval** <1-65535>	By default, the interface retransmits LSAs every 5 seconds.

Note: The value of the retransmission LSA interval between adjacent routers should not be set too small, or unnecessary retransmissions will occur. Generally, it should be longer than the time for a message to be transmitted between two routers for a round trip.

5.6.2. Configure distance

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Create OSPF and enter OSPF mode	**router ospf**	
Configure distance	**distance**{<1-255>|ospf <1-255>}	Configuration management distance
Unconfigure distance	**no distance**{<1-255>|ospf <1-255>}	Unconfigure the management distance

5.6.3. Configure default-metric

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Create OSPF and enter OSPF model	**router ospf**	
Configure default-metric	**default-metric** <0-16777214>	Configure the metric value for the route
Unconfigure default-metric	**[no] default-metric** <0-16777214>	Unconfigure the metric value for the rout

5.6.4. Configure the forbidden interface to send OSPF message

If you want OSPF routing information not to be available to routers in a network, you can disable the interface from sending OSPF messages.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Create OSPF and enter OSPF model	**router ospf**	
Prohibit the interface from	**passive-interface[default|vlan]**	By default, the interface

sending OSPF message		is allowed to send OSPF message

5.6.5. Configure OSPF authentication

From the security point of view, in order to avoid the leakage of routing information or malicious attacks on OSPF routers, OSPF provides packet authentication.

When an OSPF router establishes a neighbor relationship, the configured password is carried in the sent message, and the password is verified when the message is received. Only the message that passes the verification can be received, otherwise, the message will not be received, and the neighbor cannot be established normally.

To configure OSPF packet authentication, all routers in the same area need to configure the area authentication mode, and the configured authentication mode must be the same. Routers in the same network segment need to configure the same interface authentication mode and password.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Create OSPF and enter OSPF model	**router ospf**	
Configure the authentication mode for the OSPF area	**area** {A.B.C.D|<0-4294967295>} **authentication (message-digest)**	-message-digest: with this parameter, MD5 ciphertext authentication mode is used; without this parameter, simple plaintext authentication mode is used. By default, the zone authentication mode is not configured.
Return to CONFIG mode	**exit**	-

Enter VLAN interface model	**interface vlan** <VLAN-ID>	-
Configure the verification mode of OSPF interface as simple plaintext verification	**ip ospf authentication**	By default, the interface does not authenticate OSPF packets.
Configure the verification mode of OSPF interface as MD5 ciphertext verification	**ip ospf authentication message-digest**	By default, the interface does not authenticate OSPF packets.
No validation is performed on the OSPF interface	IP OSPF authentication null, equivalent to no IP OSPF authentication.	By default, the interface does not authenticate OSPF packets.
Configure simple plaintext authentication key of OSPF interface	**ip ospf authentication-key [encrypted|unencrypted]** <word1-8>	-ip -addres: OSPF interface IP -< word 1-8 >: simple plaintext authentication key, maximum character length 8
Configure MD5 ciphertext authentication key for OSPF interface	**ip ospf message-digest-key** <1-255> **md5 [encrypted|unencrypted]** <word1-8>	-< word 1-8 >: MD5 ciphertext authentication key, maximum character length 16

5.7. OSPF Display and Maintenance

After the above configuration is completed, execute the show command to display the operation of OSPF after configuration, and verify the effect of the configuration by viewing the displayed information.

Action	Command	Description
Displays summary information for OSPF	**show ip ospf**	
Displays information about OSPF neighbor	**show ip ospf neighbor (detail)**	
Displays information about all routing tables for the OSPF proces	**show ip ospf route**	
Displays virtual connection information for a process in OSPF	**show ip ospf interface vlink** <vlink_list>	
Display OSPF interface information	**show ip ospf interface (vlan** <vlan_list>**)**	

5.8. Example of a typical configuration

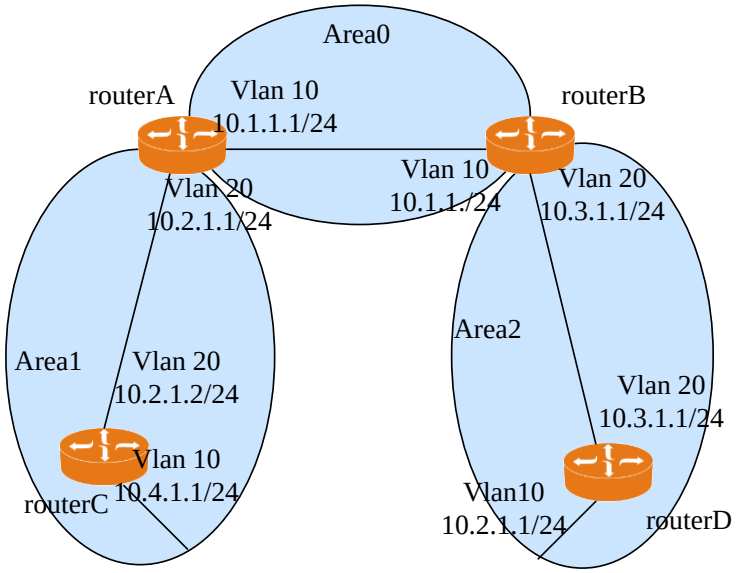
Note: In the configuration example, only the commands related to OSPF configuration are listed.

5.8.1. Configure OSPF Basic Features

5.8.1.1. Networking requirements

All routers run OSPF and divide the entire autonomous system into three areas. Where Router A and Router B act as ABR to forward routes between areas. Once configured, each router should learn routes to all network segments within the AS.

5.8.1.2. Network diagram



5.8.1.3. Configuration Steps

Step 1: Configure the IP address of each interface (omitted)

Step 2: Configure OSPF basic functions

#Configure Router A.

#configure terminal

(config)#router ospf

(config-ospf)#network 10.1.1.0 0.0.0.255 area 0

(config-ospf)#network 10.2.1.0 0.0.0.255 area 1

(config-ospf)#exit

#Configure Router B.

#configure terminal

(config)#router ospf

(config-ospf)#network 10.1.1.0 0.0.0.255 area 0

(config-ospf)#network 10.3.1.0 0.0.0.255 area 2

(config-ospf)#exit

#Configure Router C.

#configure terminal

(config)#router ospf

(config-ospf)#network 10.2.1.0 0.0.0.255 area 1

(config-ospf)#network 10.4.1.0 0.0.0.255 area 1

(config-ospf)#exit

#Configure Router D.

#configure terminal

(config)#router ospf

(config-ospf)#network 10.3.1.0 0.0.0.255 area 2

(config-ospf)#network 10.5.1.0 0.0.0.255 area 2

(config-ospf)#exit

Step 3: Verify the configuration results

#View Router A's OSPF neighbors.

#show ip ospf neighbor

#Displays the OSPF routing information of Router A.

#show ip ospf route

#Use Ping on Router D to test connectivity.

#ping 10.4.1.1

ping ip 10.4.1.1

PING 10.4.1.1 (10.4.1.1): 56 data bytes

64 bytes from 10.4.1.1: seq=0 ttl=64 time=4.299 ms

64 bytes from 10.4.1.1: seq=1 ttl=64 time=1.776 ms

64 bytes from 10.4.1.1: seq=2 ttl=64 time=1.804 ms

64 bytes from 10.4.1.1: seq=3 ttl=64 time=1.694 ms

64 bytes from 10.4.1.1: seq=4 ttl=64 time=1.824 ms

--- 10.4.1.1 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 1.694/2.279/4.299 ms

6. OSPFv3 protocol

6.1. Protocol introduction

OSPF (Open Shortest Path First), as an Internal Gateway Protocol (IGP), is used to publish routing information between routers in the same autonomous domain (AS). Different from distance vector protocol (RIP), OSPF has the advantages of supporting large networks, fast routing convergence, and taking up less network resources. It plays an important role in the current routing protocols. The OSPF router collects the connection status information of each router in its network area, that is, link state information, and generates a link state database. The router has mastered the link status information of all routers in the region, which is equivalent to understanding the topology of the entire network. The OSPF router uses the Shortest Path First (SPF) algorithm to independently calculate the route to any destination. The OSPF daemon dynamically maintains the routing table, which realizes the value of the routing protocol.

OSPFv3 is the abbreviation of OSPF Version 3. Through the establishment of OSPFv3 network, routing information is found and calculated in the autonomous domain. OSPFv3 can be applied to large-scale networks, and can support up to hundreds of industrial routing switching all-in-one machines.

The main purpose of OSPFv3 is to develop a routing protocol independent of any specific network layer. For this purpose, the internal router information of OSPFv3 has been redesigned.

OSPFv3 differs from OSPFv2 in that:

OSPFv3 does not insert IP based data into the message header at the beginning of the data packet and link status announcement (LSA).

OSPFv3 uses information independent of network protocols to perform key tasks that used to require IP packet header data, such as identifying the LSA that published routing data.

6.2. Configuration preparation

Before configuring the basic functions of OSPFv3, you need to complete the following tasks: enable IPv6 capabilities to make the network layer of adjacent nodes accessible.

6.3. Enable OSPF function

OSPFv3 supports multiple processes. Multiple OSPFv3 processes started on an industrial router are distinguished by different process numbers. The OSPFv3 process number is set when OSPFv3 is started. It is only valid locally and does not affect the message exchange with other industrial routing switching all-in-one machines.
Router ID is a 32 bit unsigned integer in the form of IPv4 address. It is the unique identification of an industrial routing and switching machine in the autonomous system. The Router ID of OSPFv3 must be manually configured. If the ID number is not configured, OSPFv3 cannot operate normally.
When configuring the Router ID manually, it must be ensured that the Router ID of any two industrial router switches in the autonomous system is different. If multiple OSPFv3 processes are running on the same industrial routing and switching all-in-one machine, different Router IDs must be specified for different processes.
To ensure the stability of OSPFv3 operation, the division of Router ID should be determined and manually configured during network planning.
Please perform the following configuration on each industrial routing switching all-in-one machine that needs to run OSPFv3 protocol.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Create OSPF and enter OSPF configuration mode	**router ospf6**	Start OSPFv3 and enter the OSPFv3 view.
Set router id	**router-id A.B.C.D**	Configure Router ID.

Configure the network segment included in the OSPF area, and enable OSPF on the interface of the specified network segment	**area** area-id **interface** IFNAME	Area id: the ID number of the area to which this address range belongs, which can be 0. By default, the interface does not belong to any region, and the OSPFv3 function is turned off. IFNAME: Enable OSPFv3 on the interface

6.4. Configure OSPF routing information control

Through the configuration in this section, you can control the release and receipt of OSPFv3 routing information, and introduce routes of other protocols.

6.4.1. Configure the OSPFv3 interface overhead value

OSPF has two ways to configure the interface cost value:
Directly configure the cost value in interface mode,
Configure the bandwidth reference value of the interface. OSPF automatically calculates the cost value of the interface according to the bandwidth reference value. The calculation formula is: interface cost be equal to bandwidth reference value divide interface bandwidth. When the calculated cost value is greater than 65535, the maximum cost value is 65535, When the calculated cost is less than 1, the minimum cost is 1.
If the cost value of this interface is not configured in interface mode, OSPFv3 will automatically calculate the cost value based on the bandwidth of the interface.

6.4.1.1. Configure the cost value of the interface

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter interface mode	**interface** vlan <VLAN-ID>	
Set the cost value of OSPFv3 interface	**ipv6 ospf cost** *cost*	1-65535. By default, the interface automatically calculates the cost based on the current bandwidth.

6.4.2. Configure the management priority of OSPFv3 protocol

Since multiple dynamic routing protocols may be running on the router at the same time, there is a problem of sharing and selecting routing information among various routing protocols. The system sets a priority for each routing protocol. When different protocols find the same route, the route with higher priority will be selected first.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter interface mode	**interface** vlan <VLAN-ID>	
Configure the routing priority of OSPFv3 protocol	**ipv6 ospf6 priority** <0-255>	

6.4.3. Configure OSPFv3 to Import External Routes

6.4.3.1. Configure routes for OSPFv3 to introduce other protocols

If OSPFv3 is not only running on the router, but also running other routing protocols, you can configure OSPFv3 to introduce routes generated by other protocols, such as RIPng, static routes, or direct connect routes. Because OSPFv3 is a routing protocol based on link status, you cannot directly filter the published LSA, so you can only

filter when OSPFv3 introduces routes, and only qualified routes can become LSAs and be published.

Please perform the following configuration on the industrial routing switching all-in-one machine running OSPFv3 protocol.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter OSPFv3 configuration mode	**router ospf6**	
Configure routes for OSPFv3 to introduce other protocols	**redistribute{connected|static|ripng|bgp}**	By default, no other protocol routing information is introduced. Connected | static | ripng: the type of source routing protocol that can be imported.

6.5. Configure OSPFv3 network adjustment and optimization

Configure some features and functions of OSPFv3 in some special network environments to adjust and optimize the performance of OSPFv3 network.

By changing the message timer of OSPFv3, the convergence speed of OSPFv3 network and the network load brought by protocol messages can be adjusted. In some low-speed links, the delay time of interface transmitting LSA needs to be considered.

By adjusting the SPF calculation interval, the resource consumption problem caused by frequent network changes can be suppressed.

For the broadcast network, the DR priority of the interface is configured to affect the selection of DR/BDR.

6.5.1. Configure OSPFv3 message timer

The user can configure the following OSPF message timers on the interface:

Hello timer: The time interval for the interface to send Hello messages to neighbors. The value of the Hello timer between OSPF neighbors should be consistent and inversely proportional to the route convergence speed and network load.

Poll timer: In the NBMA network, the time interval for a router to send a polling Hello message to a neighbor router whose status is down.

Neighbor expiration time: If the interface has not received the Hello message sent by the neighbor within the neighbor expiration time, the router will declare the neighbor invalid.

Time interval for interface retransmission of LSA: After the router announces an LSA to its neighbor, the neighbor needs to confirm it. If no acknowledgement message is received from the other party within the retransmission interval, the LSA will be retransmitted to the neighbor.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter interface mode	**Interface vlan** <VLAN-ID>	-
Configure Hello Timer	**Ipv6 ospf6 hello-interval** <1-65535>	By default, the time interval between P2P and Broadcast interfaces sending Hello messages is 10 seconds, and the time interval between P2P and NBMA interfaces sending Hello messages is 30 seconds.
Configure neighbor expiration time	**Ipv6 ospf6 dead-interval** <1-65535>	The length of time for adjacent routing switches on the

		interface to die is 40 seconds by default.
Configure the time interval of interface retransmission LSA	**Ipv6 ospf6 retransmit-interval** <1-65535>	By default, the interface retransmits LSA every 5 seconds.

Note: The value of the retransmission LSA interval between adjacent routers should not be set too small, or unnecessary retransmissions will occur. It usually takes longer than one round trip time for a message to be transmitted between two routers.

Users can adjust and optimize the OSPF network from the following aspects:

By changing the message timer of OSPF, the convergence speed of OSPF network and the network load brought by protocol message can be adjusted. In some low-speed links, the delay time of interface transmitting LSA needs to be considered.

By adjusting the SPF calculation interval, the resource consumption problem caused by frequent network changes can be suppressed.

In the network with high security requirements, the security of the OSPF network can be improved by configuring the OSPF authentication feature.

OSPF also supports the network management function. You can configure the OSPF MIB to bind to a process, and send Trap messages and logs.

6.5.2. Configure distance

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Create OSPF6 and enter OSPF6 mode	**router ospf6**	
Configure distance	**distance**{<1-255>|ospf6<1-255}	Configuration management distance
Unconfigure distance	**no distance**{<1-255>|ospf6<1-255}	Unconfigure the management distance

6.5.3. Configure to prohibit the interface from sending OSPF message

If you want to prevent OSPF routing information from being obtained by routers in a network, you can prohibit the interface from sending OSPF messages.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Create OSPF6 and enter OSPF6 mode	**router ospf6**	
Forbid the interface to send OSPF6 message	**passive-interface [default|vlan]**	By default, the interface is allowed to send OSPF6 messages

6.6. OSPF6 display and maintenance

After completing the above configuration, execute the show command to display the operation of OSPF6 after configuration. Verify the configuration effect by viewing the display information.

Action	Command	Description
Display the summary information of OSPF6	**show ip ospf6**	
Display OSPF6 neighbor information	**show ip ospf6 neighbor (detail)**	
Displays information about all routing tables of OSPF6 processes	**show ip ospf6 route**	
Display the virtual connection	**show ip ospf6 interface**	

information of a process in OSPF6	**vlink** <vlink_list>	
Display OSPF6 interface information	**show ip ospf6 interface (vlan**<vlan_list>**)**	

7. BGP4 and BGP4+

7.1. Protocol introduction

Border Gateway Protocol (BGP) is a distance vector routing protocol that realizes route reachability between AS (Autonomous System) and selects the best route. The three versions released earlier are BGP-1, BGP-2 and BGP-3. BGP-4 was used in 1994. After 2006, the version used by unicast IPv4 networks is BGP-4. The version used by other networks (such as IPv6) is MP-BGP.

MP-BGP is an extension of BGP-4 to achieve the purpose of application in different networks. The original message mechanism and routing mechanism of BGP-4 have not changed. The application of MP-BGP on IPv6 unicast network is called BGP4+, and the application on IPv4 multicast network is called MBGP (Multicast BGP).

To facilitate the management of the expanding network, the network is divided into different autonomous systems. In 1982, the External Gateway Protocol (EGP) was used to dynamically exchange routing information between AS. However, EGP is relatively simple in design. It only publishes the routing information that can be reached by the network, but does not optimize the routing information. At the same time, it does not consider the problems such as loop avoidance, which will soon be unable to meet the requirements of network management.

BGP is another external gateway protocol designed to replace the original EGP. Unlike the original EGP, BGP can perform routing optimization, avoid routing loops, deliver routes more efficiently, and maintain a large amount of routing information. Although BGP is used to transfer routing information between ASs, not all ASs need to run BGP to transfer routing information. For example, on the upstream outlet of the data center connected to the Internet, in order to avoid the impact of massive Internet

routing on the internal network of the data center, the device uses static routing instead of BGP to communicate with the external network.

7.2. Configuration preparation

Before configuring the basic functions of BGP, you need to complete the following tasks: configure the network layer address of the interface to make the network layer of adjacent nodes reachable.

7.3. Configure the basic functions of BGP

7.3.1. Start BGP and enter BGP view

Action	Command	Description
Enter CONFIG mode	**configure terminal**	-
Create BGP process and enter BGP configuration mode	**router bgp** <*as-number*>	Required. By default, the BGP process is down. After a BGP peer is established, changing the BGP Router ID causes the BGP peer relationship to be reset.
Configure BGP Router ID	**router-id** <*ipv4-address*>	

Note: By default, BGP will automatically select the Router ID in the system view as the Router ID of the BGP protocol. If the selected Router ID is the IP address of the physical interface, when the IP address changes, the routing will oscillate. To improve the stability of the network, the Router ID can be manually configured as the Loopback interface address.

7.3.2. Configure BGP Peer

When configuring a BGP peer, if the AS number of the specified peer is the same as the local AS number, the IBGP peer is configured. If the AS number of the specified peer is different from the local AS number, the EBGP peer is configured. In order to

enhance the stability of the BGP connection, it is recommended to use the Loopback interface address that can be reached by the route to establish the BGP connection.

When using the IP address of the Loopback interface to establish a BGP connection, it is recommended that the peer connect interface command be configured at both ends of the peer to ensure the correctness of the interface and address of the TCP connection at both ends. If the command is configured on only one end, the BGP connection may fail.

When using the IP address of the Loopback interface to establish an EBGP connection, you must configure the command peer ebgp max hop (where hop count ≥ 2), otherwise the EBGP connection cannot be established.

If you need to configure a large number of peers in the same way, you can reduce the configuration workload by configuring BGP peer groups.

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter BGP view	**router bgp**<*as-number*>	-
Create BGP peer	**neighbor**<*ipv4_addr*>| <*ipv6_addr*> **remote-as** <*as-number*>	-
Enable address clusters for neighbors	**neighbor** <*ipv4_addr*>| <*ipv6_addr*> ***multicast*** | **Unicast enable**	
Set timer	***times bgp <KeepAlive time> <holdtime>***	***<KeepAlive time>:<1-65535> <holdtime>:<1-65535>***
Add Subnet	**network [**<*ipv4_addr*> **<wildcard-mask>**]|[<*ipv6_addr*> **<ipv6-mask>**	-<ipv6 mask>: ffff: ffff: ffff: ffff: ffff: ffff: ffff: ffff means the mask length is 128, and ffff: ffff: ffff: ffff:: 0 means the mask length is 64
Set next hop	**next-hop-local**	

	neighbor<*ipv4_addr*>| <*ipv6_addr*>	
Activate peer	**activate neighbor {<ipv4_address>| <ipv6_address>} [multicast]**	
Redistribute Routes	**redistribute {connected | static|rip| ospf} address-family {ipv4 | ipv6} [metric <metric>]**	
Redistribute Default Routes	**default local-preference <local_prf>**	
Set deterministic med	**deterministic-med**	
Configure Distance	**distance<distance_ebgp> <distance_ibgp> <distance_local>**	
Configure route reflection	**reflector-client neighbor {<ipv4_address>| <ipv6_address>} [multicast]**	

7.4. Configuring BGP Routing Aggregation

Action	Command	Description
Enter CONFIG mode	**configure terminal**	
Enter RIP configuration mode	**router BGP**	-
Configure Routing Aggregation	**aggregate-address{{<ipv4_address><ipv4_mask>[multicast]}|<subnet>}**	

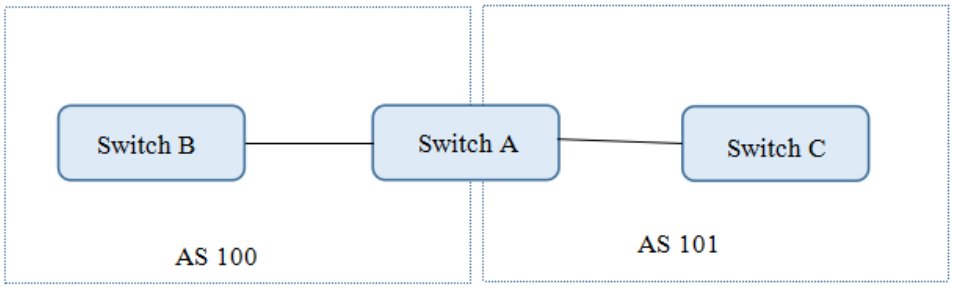
Note: Manual aggregation is effective for the existing routing table entries in the BGP local routing table. For example, there are no routes in the BGP routing table with a mask length greater than 16, such as 10.1.1.1/24. Even if the command aggregate 10.1.1.1 16 is configured, BGP will not generate aggregation routes.

7.5. Display BGP information

After completing the above configuration, execute the show command to display the operation of the BGP after configuration. Verify the configuration effect by viewing the display information.

Action	Command	Description
Display BGP protocol information	show ip bgp neighbor	
Display bgp information	show ip bgp summary	-

7.6. Example of BGP typical configuration



SwitchA:

router bgp

as-number 100

network 192.168.0.1 0.0.0.255

neigbor 192.168.0.100 remote-as 100

neigbor 192.168.0.101 remote-as 101

activate neighbor 192.168.0.100

activate neighbor 192.168.0.101

router-id 2.2.2.2

!

SwitchB:

192.168.0.100

router bgp

as-number 100

network 192.168.0.1 0.0.0.255

neigbor 192.168.0.99 remote-as 100

activate neighbor 192.168.0.99

router-id 3.3.3.3

!

SwitchC:

192.168.0.101

router bgp

as-number 101

network 192.168.0.1 0.0.0.255

neigbor 192.168.0.99 remote-as 100

activate neighbor 192.168.0.99

router-id 4.4.4.4

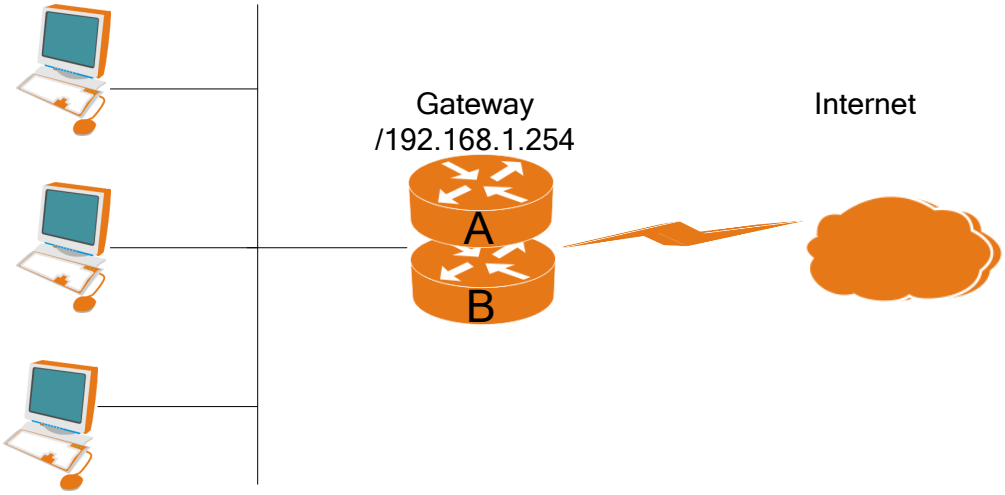
!

8.VRRP

8.1. Protocol Introduction

With the development of Internet, the reliability of network is getting higher and higher. In particular, terminal devices need to be connected to the network at all times. The terminal connects to the network by setting the default gateway. To solve the problem of gateway stability, you can increase the number of gateways, but the terminal host usually can only set one gateway. The VRRP protocol can be used to realize the backup of devices and minimize the time of network interruption. The general networking device A and device B negotiate to form a VRRP group. At the same time, only the devices in the master state can forward data. The terminal device is represented as a virtual IP address 192.168.1.254, as shown in the following figure.

The VRRP function of this device supports IPv4 and IPv6 protocols.



8.2. Configuration preparation

Before configuring the basic functions of VRRP, you need to complete the following tasks: configure the network layer address of the interface to make the network layer of adjacent nodes accessible.

8.3. Configure the basic functions of VRRP

Action	Command	Description
Enter CONFIG mode	**configure terminal**	-
Enter interface mode	**interface** vlan<VLAN-ID>	-
Create vrrp group and configure virtual IP address	**vrrp**<1-255>**virtual-address** <ipv4_addr>|<ipv6_addr>	-The vrrp group number identifies an interactive vrrp group. There is no default value -<ipv4_ Addr>The configured IP address must be in the same network segment as the specified

		interface address. If the virtual IP is the actual IP of the interface, configure the master. Otherwise, configure the backup
Configure the priority of vrrp	**vrrp** <1-255> **priority**<*1-254*>	The priority is 100 by default. If the virtual IP is the actual IP of the interface, it defaults and is automatically promoted to 255
Configure the preemption mode of vrrp	**{no}vrrp** <1-255> **preempt**	By default, the preemption mode is enable
Configure the time interval of sending advertisement message by vrrp	**vrrp** <1-255> version <2-3>	3 by default
Configure the shutdown of vrrp	**vrrp** <1-255> shutdown	

8.4. Display VRRP information

After completing the above configuration, execute the show command to display the running status of VRRP after configuration, and verify the configuration effect by viewing the display information.

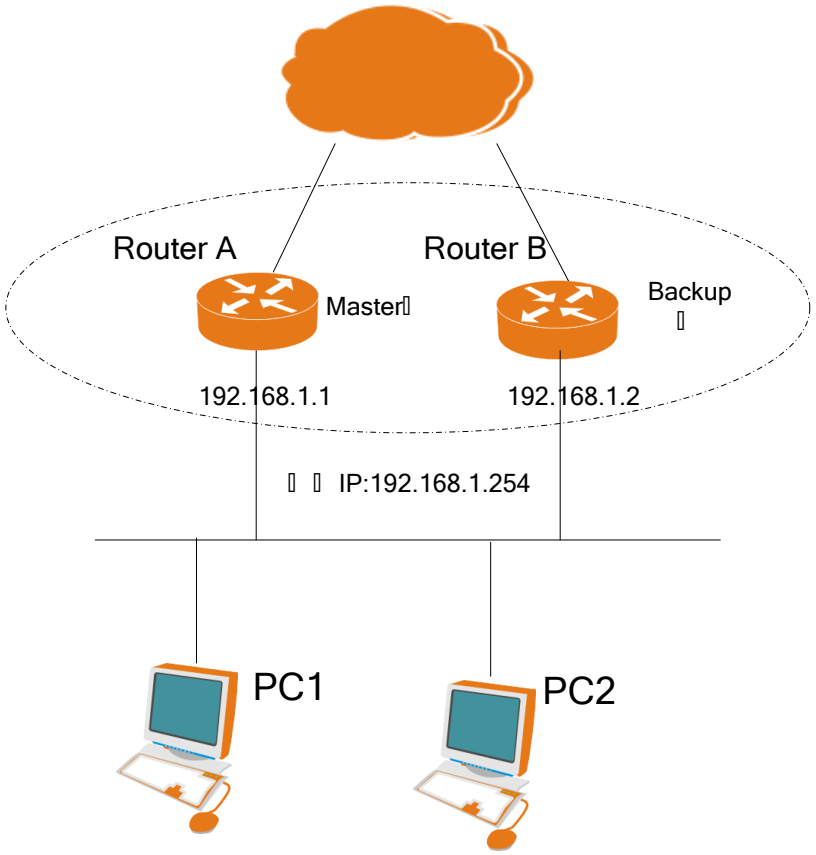
Action	Command	Description
Display the status information of VRRP	**show vrrp [interface vlan** <vlan_id>|**vrid]**	-Vrid: (optional) VRRP backup group ID, ranging from 1 to 255. With this parameter, VRRP status information of the specified group ID will be displayed.

		Without this parameter, VRRP status information of all group IDs will be displayed.
Display the basic information of VRRP	**show vrrp summary**	

8.5. VRRP Typical Configuration Example

8.5.1. Networking requirements

8.5.2. Networking Diagram



8.5.3. Configuration steps

Step 1: Configure the IP address of each interface (omitted)

Step 2: Configure the basic content of vrrp

#Configure Router A.

#configure terminal

(config)#interface vlan 1

(config-vrrp)#interface vlan1

(config-if-vlan)# vrrp 1 virtual-address 192.168.1.254

(config-if-vlan)# vrrp 1 priority 120

(config-if-vlan)#end

#Configure Router B.

#configure terminal

(config)#interface vlan 1

(config-vrrp)#interface vlan1

(config-if-vlan)# vrrp 1 virtual-address 192.168.1.254

(config-if-vlan)# vrrp 1 priority 100

(config-if-vlan)#end

#View the vrrp status of Router A.

MBN8000#show vrrp

The display is as follows:

VLAN1 - Vrid 1

VRRP State is Master

Virtual IP address:192.168.1.254

Virtual Mac address: 00-00-5E-00-01-01

Current Priority: 100

VRRP timer: Advertise 1s

Authentication string is not set

Preempt is enable

Note: RouterA and routerB need to be configured with the same VRRP group number and virtual IP. Currently, it supports up to 255 VRRP groups, and only one VRRP group can be configured on an interface.