Content

Chapter 1 Routing Protocol Overview

Explanation：

The layer 3 switch in this chapter represents the a general sense of router or wireless controller which is running routing protocol.

To communicate with a remote host over the Internet, a host must choose a proper route via a set of routers or Layer3 switches.

Both routers and layer3 switches calculate the route using CPU, the difference is that layer3 switch adds the calculated route to the switch chip and forward by the chip at wire speed, while the router always store the calculated route in the route table or route buffer, and data forwarding is performed by the CPU. For this reason, although both routers and switches can perform route selection, layer3 switches have great advantage over routers in data forwarding. The following describes basic principle and methods used in layer3 switch route selection.

In route selection, the responsibility of each layer3 switch is to select a proper midway route according to the destination of the packet received; and send the packet to the next layer3 switch until the last layer3 switch in the route send the packet to the destination host. A route is the path selected by each layer3 switch to pass the packet to the next layer3 switch. Route can be grouped into direct route, static route and dynamic route.

Direct route refer to the path directly connects to the layer3 switch, and can be obtained with no calculation.

Static route is the manually specified path to a network or a host; static route cannot be changed freely. The advantage of static route is simple and consistent, and it can limit illegal route modification, and is convenient for load balance and route backup. However, as this is set manually, it is not suitable for mid- or large-scale networks for the route in such conditions are too huge and complex.

Dynamic route is the path to a network or a host calculated by the layer3 switch according to the routing protocols enabled. If the next hop layer3 switch in the path is not reachable, layer3 switch will automatically discard the path to that next hop layer3 switch and choose the path through other layer3 switches.

There are two dynamic routing protocols: Interior Gateway Protocol (IGP) and Exterior Gateway protocol (EGP). IGP is the protocol used to calculate the route to a destination inside an autonomous system. IGP supported by switch include RIP and OSPF, RIP and OSRF can be configured according to the requirement. Switch supports running several IGP dynamic routing protocols at the same time. Or, other dynamic routing protocols and static route can be introduced to a dynamic routing protocol, so that multiple routing protocols can be associated.

EGP is used to exchange routing information among different autonomous systems, such as BGP protocol. EGP supported by switch include BGP-4, BGP-4+.

1.1 Routing Table

As mentioned before, layer3 switch is mainly used to establish the route from the current layer3 switch to a network or a host, and to forward packets according to the route. Each layer3 switch has its own route table containing all routes used by that switch. Each route entry in the route table specifies the physical port should be used for forwarding packet to reach a destination host or the next hop layer3 switch to the host.

The route table mainly consists of the following:

- ☞ Destination address: used to identify the destination address or destination network of an IP packet.
- ☞ Network mask: used together with destination address to identify the destination host or the network the layer3 switch resides. Network mask consists of several consecutive binary 1's, and usually in the format of dotted decimal (an address consists of 1 to 4 255’s.) When “AND” the destination address with network mask, we can get the network address for the destination host or the network the layer3 switch resides. For example, the network address of a host or the segment the layer3 switch resides with a destination address of 200.1.1.1 and mask 255.255.255.0 is 200.1.1.0.
- ☞ Output interface: specify the interface of layer3 switch to forward IP packets.
- ☞ IP address of the next layer3 switch (next hop): specify the next layer3 switch the IP packet will pass.
- ☞ Route entry priority: There may be several different next hop routes leading to the same destination. Those routes may be discovered by different dynamic routing protocols or static routes manually configured. The entry with the highest priority (smallest value) becomes the current best route. The user can configure several routes of different priority to the same destination; layer3 switch will choose one route for IP packet forwarding according to the priority order.

To prevent too large route table, a default route can be set. Once route table look up fails, the default route will be chosen for forwarding packets.

The table below describes the routing protocols supported by switch and the default route look up priority value.

Routing Protocols or route type	Default priority value
Direct route	0
OSPF	110
Static route	1

RIP	120
OSPF ASE	150
IBGP	200
EBGP	20
Unknown route	255

1.2 IP Routing Policy

1.2.1 Introduction to Routing Policy

Some policies have to be applied when the router publishing and receiving routing messages so to filter routing messages, such as only receiving or publishing routing messages meets the specified conditions. A routing protocol maybe need redistribute other routing messages found by other protocols such as OSPF so to increase its own routing knowledge; when the router redistributing routing messages from other routing protocols there may be only part of the qualified routing messages is needed, and some properties may have to be configured to suit this protocol.

To achieve routing policy, first we have to define the characteristics of the routing messages to be applied with routing policies, namely define a group matching rules. We can configure by different properties in the routing messages such as destination address, the router address publishing the routing messages. The matching rules can be previously configured to be applied in the routing publishing, receiving and distributing policies.

Five filters are provided in switch: route-map, acl, as-path, community-list and ip-prefix for use. We will introduce each filter in following sections:

1. route-map

For matching certain properties of the specified routing information and setting some routing propertities when the conditions are fulfilled.

Route-map is for controlling and changing the routing messages while also controlling the redistribution among routes. A route-map consists of a series of match and set commands in which the match command specifies the conditions required matching, and the set command specifies the actions to be taken when matches. The route-map is also for controlling route publishing among different route process. It can also used on policy routing which select different routes for the messages other than the shortest route.

A group matches and set clauses make up a node. A route-map may consist of several nodes each of which is a unit for matching test. We match among nodes with by sequence-number. Match clauses define matching rules. The matching objects are some properties of routing messages. Different match clause in the same node is “and” relation logically, which means the matching test of a node, will not be passed until conditions in its entire match clause are matched. Set clause specifies actions, namely configure some properties of routing messages after the matching test is passed.

Different nodes in a route-map is an “or” relation logically. The system checks each node of the route-map in turn and once certain node test is passed the route-map test will be passed without taking the next node test.

2. access control list(acl)

ACL (Access Control Lists) is a data packet filter mechanism in the switch. The switch controls the network access and secure the network service by permitting or denying certain data packet transmtting out from or into the network. Users can establish a group of rules by certain messages in the packet, in which each rule to be applied on certain amount of matching messages: permit or deny. The users can apply these rules to the entrance or exit of specified switch, with which data stream in certain direction on certain port would have to follow the specified ACL rules in-and-out the switch. Please refer to chapter “ACL Configuration”.

3. Ip-prefix list

The ip-prefix list acts similarly to acl while more flexible and more understandable. The match object of ip-prefix is the destination address messages field of routing messages when applied in routing messages filtering.

An ip-prefix is identified by prefix list name. Each prefix list may contain multiple items, each of which specifies a matching range of a network prefix type and identifies with a sequence-number which specifies the matching check order of ip-prefix.

In the process of matching, the switch check each items identified by sequence-number in ascending order and the filter will be passed once certain items is matched(without checking rest items)

4. Autonomic system path information access-list as-path

The autonomic system path information access-list as-path is only used in BGP. In the BGP routing messages packet there is an autonomic system path field (in which autonomic system path the routing messages passes through is recorded). As-path is specially for specifying matching conditions for autonomic system path field.

As for relevant as-path configurations, please refer to the ip as-path command in BGP configuration.

5. community-list

Community-list is only for BGP. There is a community property field in the BGP routing messages packet for identifying a community. The community list is for specifying matching conditions for Community-list field.

As for relevant Community-list configuration, please refer to the ip as-path command in BGP configuration

1.2.2 IP Routing Policy Configuration Task List

1. Define route-map
2. Define the match clause in route-map
3. Define the set clause in route-map
4. Define address prefix list

1. Define route-map

Command	Explanation
Global mode	
route-map <*map_name*> {deny | permit} <*sequence_num*> **no route-map <*map_name*> [{deny | permit} <*sequence_num*>]**	Configure route-map; the **no route-map <*map_name*> [{deny | permit} <*sequence_num*>]** command deletes the route-map.

2. Define the match clause in route-map

Command	Explanation
Route-map configuration mode	
match as-path <*list-name*> **no match as-path [<*list-name*>]**	Match the autonomous system as path access-list the BGP route passes through; the **no match as-path [<*list-name*>]** command deletes match condition.
match community <*community-list-name* | *community-list-num* > [exact-match] **no match community [<*community-list-name* | *community-list-num* > [exact-match]]**	Match a community property access-list. The **no match community [<*community-list-name* | *community-list-num* > [exact-match]]** command deletes match condition.

match interface <*interface-name* > **no match interface [<*interface-name* >]**	Match by ports; The **no match interface [<*interface-name*e >]** command deletes match condition.
match ip <address | next-hop> <*ip-acl-name*e | *ip-acl-num* | prefix-list *list-name*> **no match ip <address | next-hop> [<*ip-acl-name*e | *ip-acl-num* | prefix-list [*list-name*]>]**	Match the address or next-hop; The **no match ip <address | next-hop> [<*ip-acl-name*e | *ip-acl-num* | prefix-list [*list-name*]>]** command deletes match condition.
match metric <*metric-val* > **no match metric [<*metric-val* >]**	Match the routing metric value; The **no match metric [<*metric-val* >]** command deletes match condition.
match origin <egp | igp | incomplete > **no match origin [<egp | igp | incomplete >]**	Match the route origin; The **no match origin [<egp | igp | incomplete >]** command deletes match condition.
match route-type external <type-1 | type-2 > **no match route-type external [<type-1 | type-2 >]**	Match the route type; The **no match route-type external [<type-1 | type-2 >]** command deletes match condition.
match tag <*tag-val* > **no match tag [<*tag-val* >]**	Match the route tag; The **no match tag [<*tag-val* >]** command deletes match condition.

3. Define the set clause in route-map

Command	Explanation
Route-map configuration mode	

set aggregator as <*as-number*> <*ip_addr*> **no set aggregator as [<*as-number*> <*ip_addr*>]**	Distribute an AS No. for BGP aggregator; The no command deletes the configuration
set as-path prepend <*as-num*> **no set as-path prepend [<*as-num*>]**	Add a specified AS No. before the BGP routing messages as-path series; The no command deletes the configuration
set atomic-aggregate **no set atomic-aggregate**	Configure the BGP atomic aggregate property; The no command deletes the configuration
set comm-list <*community-list-name* | *community-list-num* > delete **no set comm-list <*community-list-name* | *community-list-num* > delete**	Delete BGP community list value; The no command deletes the configuration
set community [*AA:NN*] [internet] [local-AS] [no-advertise] [no-export] [none] [additive] **no set community [*AA:NN*] [internet] [local-AS] [no-advertise] [no-export] [none] [additive]**	Configure BGP community list value; The no command deletes the configuration
set extcommunity <rt | soo> <*AA:NN*> **no set extcommunity <rt | soo> [<*AA:NN*>]**	Configure BGP extended community list property; The no command deletes the configuration
set ip next-hop <*ip_addr*> **no set ip next-hop [<*ip_addr*>]**	Set next-hop IP address; The no command deletes the configuration
set local-preference <*pre_val*> **no set local-preference [<*pre_val*>]**	Set local preference; The no command deletes the configuration
set metric < +/- *metric_val* | *metric_val*> **no set metric [+/- *metric_val* | *metric_val*]**	Set routing metric value; The no command deletes the configuration
set metric-type <type-1 | type-2> **no set metric-type [<type-1 | type-2>]**	Set OSPF metric type; The no command deletes the configuration

set origin <egp | igp | incomplete > **no set origin [<egp | igp | incomplete >]**	Set BGP routing origin; The no command deletes the configuration
set originator-id <*ip_addr*> **no set originator-id [<*ip_addr*>]**	Set routing originator ID; The no command deletes the configuration
set tag <*tag_val*> **no set tag [<*tag_val*>]**	Set OSPF routing tag value; The no command deletes the configuration
set vpnv4 next-hop <*ip_addr*> **no set vpnv4 next-hop [<*ip_addr*>]**	Set BGP VPNv4 next-hop address; the no command deletes the configuration
set weight < *weight_val*> **no set weight [<*weight_val*>]**	Set BGP routing weight; The no command deletes the configuration

4. Define address prefix list

Command	Explanation
Global mode	
ip prefix-list <*list_name*> description <*description*> **no ip prefix-list <*list_name*> description**	Describe the prefix list; The **no ip prefix-list <*list_name*> description** command deletes the configuration.
ip prefix-list <*list_name*> [seq <*sequence_number*>] <deny | permit> < any | *ip_addr/mask_length* [ge *min_prefix_len*] [le *max_prefix_len*]> **no ip prefix-list <*list_name*> [seq <*sequence_number*>] [<deny | permit> < any | *ip_addr/mask_length* [ge *min_prefix_len*] [le *max_prefix_len*]>]**	Set the prefix list; The **no ip prefix-list <*list_name*> [seq <*sequence_number*>] [<deny | permit> < any | *ip_addr/mask_length* [ge *min_prefix_len*] [le *max_prefix_len*]>]** command deletes the configuration.

1.2.3 Configuration Examples

The figure below shows a network consisting of four Layer 3 switches. This example demonstrates how to set the BGP as-path properties through route-map. BGP protocol is applied among the Layer 3 switches. As for switchC, the network 192.68.11.0/24 can be reached through two paths in which one is AS-PATH 1 by IBGP (going through SwitchD), the other one is AS-PATH 2 by EBGP (going through SwitchB). BGP selects the shortest path, so AS-PATH 1 is the preferred path. If the path 2 is wished, which is through EBGP path, we can add two extra AS path numbers into the AS-PATH messages from SwitchA to SwitchD so as to change the determination SwitchC take to 192.68.11.0/24.

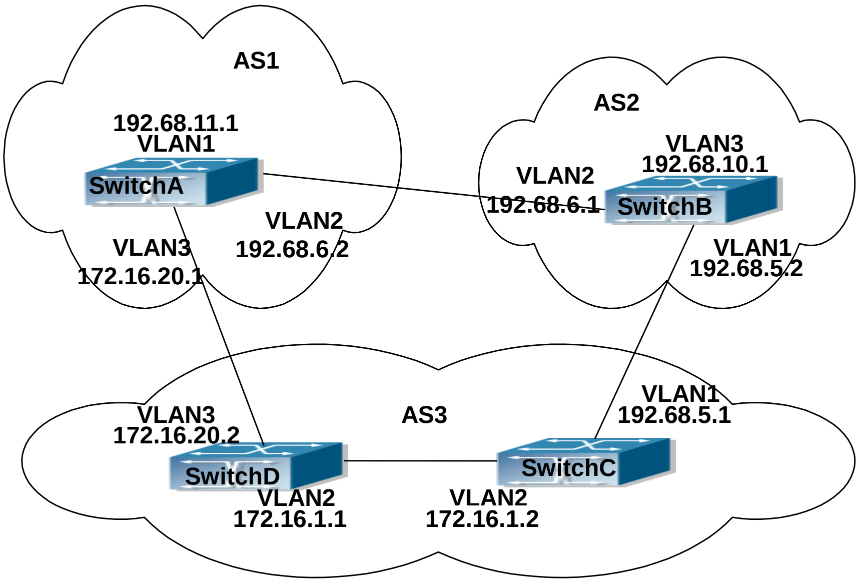

Fig 1-1 Policy routing Configuration

Configuration procedure: (only SwitchA is listed, configurations for other switches are omitted.)

The configuration of Layer 3 switchA:

```
SwitchA#config
SwitchA(config) #router bgp 1
SwitchA(config-router)#network 192.68.11.0 mask 255.255.255.0
SwitchA(config-router)#neighbor 172.16.20.2 remote-as 3
SwitchA(config-router)#neighbor 172.16.20.2 route-map AddAsNumbers out
SwitchA(config-router)#neighbor 192.68.6.1 remote-as 2
SwitchA(config-router)#exit
SwitchA(config)#route-map AddAsNumbers permit 10
SwitchA(config-route-map)#set as-path prepend 1 1
```

1.2.4 Troubleshooting

Faq: The routing protocol could not achieve the routing messages study under normal protocol running state

Troubleshooting: check following errors:

- ☞ Each node of route-map should at least has one node is permit match mode. When the route map is used in routing messages filtering, the routing messages will be considered not pass the routing messages filtering if certain routing messages does not pass the filtering of any nodes. When all nodes are set to deny mode, all routing messages will not pass the filtering in this route-map.
- ☞ Items in address prefix list should at least have one item set to permit mode. The deny mode items can be defined first to fast remove the unmatched routing messages, however if all the items are set to deny mode, any route will not be able to pass the filtering of this address prefix list. We can define a permit 0.0.0.0/0 le 32 item after several deny mode items are defined so to permit all other routing messages pass through. Only default route will be matched in less-equal 32 is not specified.

Chapter 2 Static Route

2.1 Introduction to Static Route

As mentioned earlier, the static route is the manually specified path to a network or a host. Static route is simple and consistent, and can prevent illegal route modification, and is convenient for load balance and route backup. However, it also has its own defects. Static route, as its name indicates, is static, it won't modify the route automatically on network failure, and manual configuration is required on such occasions, therefore it is not suitable for mid and large-scale networks.

Static route is mainly used in the following two conditions: 1) in stable networks to reduce load of route selection and routing data streams. For example, static route can be used in route to STUB network. 2) For route backup, configure static route in the backup line, with a lower priority than the main line.

Static route and dynamic route can coexist; layer3 switch will choose the route with the highest priority according to the priority of routing protocols. At the same time, static route can be introduced (redistribute) in dynamic route, and change the priority of the static route introduced as required.

2.2 Introduction to Default Route

Default route is a kind of static route, which is used only when no matching route is found. In the route table, default route in is indicated by a destination address of 0.0.0.0 and a network mask of 0.0.0.0, too. If the route table does not have the destination of a packet and has no default route configured, the packet will be discarded, and an ICMP packet will be sent to the source address indicate the destination address or network is unreachable.

2.3 Static Route Configuration Task List

1. Static route configuration

1. Static route configuration

Command	Explanation
Global mode	

ip route {<*ip-prefix*> <*mask*> | <*ip-prefix*>/<*prefix-length*>} {<*gateway-address*> | <*gateway-interface*>} [<*distance*>] **no ip route {<*ip-prefix*> <*mask*> | <*ip-prefix*>/<*prefix-length*>} [<*gateway-address*> | <*gateway-interface*>] [<*distance*>]**	Set static routing; the **no ip route {<*ip-prefix*> <*mask*> | <*ip-prefix*>/<*prefix-length*>} [<*gateway-address*> | <*gateway-interface*>] [<*distance*>]** command deletes a static route entry

2.4 Static Route Configuration Examples

The figure shown below is a simple network consisting of three layer3 switches, the network mask for all switches and PC is 255.255.255.0. PC-A and PC-C are connected via the static route set in SwtichA and SwitchC; PC3 and PC-B are connected via the static route set in SwtichC to SwitchB; PC-B and PC-C is connected via the default route set in SwitchB.

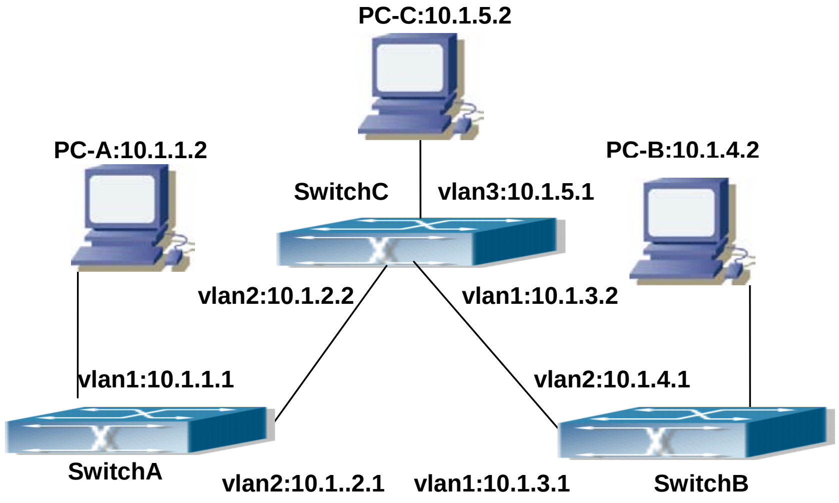

Fig 2-1 Static Route Configurations

Configuration steps:

Configuration of layer3 SwitchA

```
Switch#config
Switch (config) #ip route 10.1.5.0 255.255.255.0 10.1.2.2
```

Configuration of layer3 SwitchC

```
Switch#config
```

Next hop use the partner IP address

```
Switch(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.1
```

Next hop use the partner IP address

```
Switch(config)#ip route 10.1.4.0 255.255.255.0 10.1.3.1
```

Configuration of layer3 SwitchB

```
Switch#config
Switch(config)#ip route 0.0.0.0 0.0.0.0 10.1.3.2
```

In this way, ping connectivity can be established between PC-A and PC-C, and PC-B and PC-C.

Chapter 3 RIP

3.1 Introduction to RIP

RIP is first introduced in ARPANET, this is a protocol dedicated to small, simple networks. RIP is a distance vector routing protocol based on the Bellman-Ford algorithm. Network devices running vector routing protocol send two kind of information to the neighboring devices regularly:

- Number of hops to reach the destination network, or metrics to use or number of networks to pass.
- What is the next hop, or the director (vector) to use to reach the destination network.

The distance vector Layer 3 switch send all their route selecting tables to the neighbor layer3 switches at regular interval. A layer3 switch will build their own route selecting information table based on the information received from the neighbor layer3 switches. Then, it will send this information to its own neighbor layer3 switches. As a result, the route selection table is built on second hand information, route beyond 15 hops will be deemed as unreachable.

RIP protocol is an optional routing protocol based on UDP. Hosts using RIP send and receive packets on UDP port 520. All layer3 switches running RIP send their route table to all neighbor layer3 switches every 30 seconds for update. If no information from the partner is received in 180 seconds, then the device is deemed to have failed and the network connected to that device is considered to be unreachable. However, the route of that layer3 switch will be kept in the route table for another 120 seconds before deletion.

As layer3 switches running RIP built route table with second hand information, infinite count may occur. For a network running RIP routing protocol, when an RIP route becomes unreachable, the neighboring RIP layer3 switch will not send route update packets at once, instead, it waits until the update interval timeout (every 30 seconds) and sends the update packets containing that route. If before it receives the updated packet, its neighbors send packets containing the information about the failed neighbor, “infinite count” will be resulted. In other words, the route of unreachable layer3 switch will be selected with the metrics increasing progressively. This greatly affects the route selection and route aggregation time.

To prevent “infinite count”, RIP provides mechanism such as “split horizon” and “triggered update” to solve route loop. “Split horizon” is done by avoiding sending to a gateway routes leaned from that gateway. There are two split horizon methods: “simple split horizon” and “poison reverse split horizon”. Simple split horizon deletes from the route to be sent to the neighbor gateways the routes learnt from the neighbor gateways; poison reverse split horizon not only deletes the abovementioned routes, but set the costs of those routes to infinite. “Triggering update” mechanism defines whenever route metric changed by the gateway, the gateway advertise the update packets immediately, regardless of the 30 second update timer status.

There two versions of RIP, version 1 and version 2. RFC1058 introduces RIP-I protocol, RFC2453 introduces RIP-II, which is compatible with RFC1723 and RFC1388. RIP-I updates packets by packets broadcast, subnet mask and authentication is not supported. Some fields in the RIP-I packets are not used and are required to be all 0’s; for this reason, such all 0's fields should be checked when using RIP-I, the RIP-I packets should be discarded if such fields are non-zero. RIP-II is a more improved version than RIP-I. RIP-II sends route update packets by multicast packets (multicast address is 224.0.0.9). Subnet mask field and RIP authentication filed (simple plaintext password and MD5 password authentication are supported), and support variable length subnet mask. RIP-II used some of the zero field of RIP-I and require no zero field verification. switch send RIP-II packets in multicast by default, both RIP-I and RIP-II packets will be accepted.

Each layer3 switch running RIP has a route database, which contains all route entries for reachable destination, and route table is built based on this database. When a RIP layer3 switch sent route update packets to its neighbor devices, the complete route table is included in the packets. Therefore, in a large network, routing data to be transferred and processed for each layer3 switch is quite large, causing degraded network performance.

Besides the above mentioned, RIP protocol allows route information discovered by the other routing protocols to be introduced to the route table. It can also be as the protocol exchanging route messages with CE on PE routers, and supports the VPN route/transmitting examples.

The operation of RIP protocol is shown below:

1. Enable RIP. The switch sends request packets to the neighbor layer3 switches by broadcasting; on receiving the request, the neighbor devices reply with the packets containing their local routing information.
2. The Layer3 switch modifies its local route table on receiving the reply packets and sends triggered update packets to the neighbor devices to advertise route update information. On receiving the triggered update packet, the neighbor lay3 switches send triggered update packets to their neighbor lay3 switches. After a sequence of triggered update packet broadcast, all layer3 switches get and maintain the latest route information.

In addition, RIP layer3 switches will advertise its local route table to their neighbor devices every 30 seconds. On receiving the packets, neighbor devices maintain their local route table, select the best route and advertise the updated information to their own neighbor devices, so that the updated routes are globally valid. Moreover, RIP uses a timeout mechanism for outdated route, that is, if a switch does not receive regular update packets from a neighbor within a certain interval (invalid timer interval), it considers the route from that neighbor invalid, after holding the route fro a certain interval (holddown timer interval), it will delete that route.

3.2 RIP Configuration Task List

1. Enable RIP (required)
    (1) Enable/disable RIP module.
    (2) Enable interface to send/receive RIP packets
2. Configure RIP protocol parameters (optional)
    (1) Configure RIP sending mechanism
        1) Configure specified RIP packets transmission address
        2) Configure RIP interface broadcast
    (2) Configure the RIP routing parameters
        1) Configure route introduction (default route metric, configure routes of the other protocols to be introduced in RIP)
        2) Configure interface authentication mode and password
        3) Configure the route deviation
        4) Configure and apply route filter
        5) Configure Split Horizon
    (3) Configure other RIP protocol parameters
        1) Configure the managing distance of RIP route
        2) Configure the RIP route capacity limit in route table
        3) Configure the RIP update, timeout, holddown and other timer.
        4) Configure the receiving buffer size of RIP UDP
3. Configure RIP-I/RIP-II switch
    (1) Configure the RIP version to be used in all interfaces
    (2) Configure the RIP version to send/receive in all interfaces
    (3) Configure whether to enable RIP packets sending/receiving for interfaces
4. Delete the specified route in RIP route table
5. Configure the RIP routing aggregation
    (1) Configure aggregation route of IPv4 route mode
    (2) Configure aggregation route of IPv4 interface configuration mode
    (3) Display IPv4 aggregation route information
6. Configure redistribution of OSPF routing to RIP

(1) Enable Redistribution of OSPF routing to RIP

(2) Display and debug the information about configuration of redistribution of OSPF routing to RIP

1. Enable RIP protocol

Applying RIP route protocol with basic configuration in switch is simple. Normally you only have to open the RIP switch and configure the segments running RIP, namely send and receive the RIP data packet by default RIP configuration. The version of data packet sending and receiving is variable when needed, allow/deny sending, receiving RIP data packet. Refer to 3.

Command	Explanation
Global Mode	
router rip **no router rip**	Enables RIP; the **no router rip** command disables RIP.
Router and address family configuration mode	
network <*A.B.C.D/M* | *ifname*|*vlan*> **no network <*A.B.C.D/M* | *ifname*|*vlan*>**	Enables the segment running RIP protocol; the **no network <*A.B.C.D/M* | *ifname*|*vlan*>** command deletes the segment.

2. Configure RIP protocol parameters

（1）Configure RIP packet transmitting mechanism

1）Configure the RIP data packet point-transmitting

2）Configure the Rip broadcast

Command	Explanation
Router Configuration Mode	
neighbor <*A.B.C.D*> **no neighbor <*A.B.C.D*>**	Specify the IP address of the neighbor router needs point-transmitting; the **no neighbor <*A.B.C.D*>** command cancels the appointed router.
passive-interface<*ifname*|*vlan*> **no passive-interface<*ifname*|*vlan* >**	Block the RIP broadcast on specified pot and the RIP data packet is only transmittable among Layer 3 switch configured with neighbor. The **no passive-interface<*ifname*|*vlan* >** command cancels the function.

（2）Configure RIP route parameters

1）Configure route introduction (default route metric, configure routes of the other protocols to be introduced in RIP)

Command	Explanation
Router Configuration Mode	
default-metric <*value*> **no default-metric**	Sets the default route metric for route to be introduced; the **no default-metric** command restores the default setting.
redistribute {kernel |connected| static| ospf | isis| bgp} [metric<*value*>] [route-map<*word*>] **no redistribute {kernel |connected| static| ospf | isis| bgp} [metric<*value*>] [route-map<*word*>]**	Redistribute the routes distributed in other routing protocols into the RIP data packet; the **no redistribute {kernel |connected| static| ospf | isis| bgp} [metric<value>] [route-map<word>]** command cancels the distributed route of corresponding protocols.
default-information originate **no default-information originate**	Generate a default route to the RIP protocol; the **no default-information originate** command cancels the feature.

2）Configure interface authentication mode and password

Command	Explanation
Interface configuration mode	
ip rip authentication mode { text| md5} **no ip rip authentication mode [text| md5]**	Sets the authentication method; the **no ip rip authentication mode [text| md5]** command cancels the authentication action.
ip rip authentication string <*text*> **no ip rip authentication string**	Sets the authentication key; the **no ip rip authentication string** command means no key is needed.
ip rip authentication key-chain <*name-of-chain*> **no ip rip authentication key-chain [<*name-of-chain*>]**	Sets the key chain used in authentication, the **no ip rip authentication key-chain [<*name-of-chain*>]** command means the key chain is not used.
ip rip authentication cisco-compatible **no ip rip authentication cisco-compatible**	After configure this command, configure MD5 authentication, then can receive RIP packet of Cisco, the no command restores the default configuration.
Global mode	

key chain <*name-of-chain*> **no key chain < *name-of-chain* >**	Enter keychain mode, and configure a key chain, the **no key chain < *name-of-chain* >** command deletes the key chain.
Keychain mode	
key <*keyid*> **no key <*keyid*>**	Enter the keychain-key mode and configure a key of the keychain; the **no key <*keyid*>** command deletes one key.
Keychain-key mode	
key-string <*text*> **no key-string <*text*>**	Configure the password used by the key, the **no key-string <*text*>** command deletes the password.
accept-lifetime <*start-time*> {<*end-time*>| duration<*seconds*>| infinite} **no accept-lifetime**	Configure a key on the key chain and accept it as an authorized time; the **no accept-lifetime** command deletes it.
send-lifetime <*start-time*> {<*end-time*>| duration<*seconds*>| infinite} **no send-lifetime**	Configure the transmitting period of a key on the key chain; the **no send-lifetime** command deletes the send-lifetime.

3）Configure the route deviation

Command	Explanation
Router configuration mode	
offset-list <access-list-number | access-list-name> {in | out } <number> [<ifname>] **no offset-list <access-list-number |access-list-name> {in|out }<number >[<ifname>]**	Configure that provide a deviation value to the route metric value when the port sends or receives RIP data packet; the **no offset-list <access-list-number |access-list-name> {in|out } <number >[<ifname>]** command removes the deviation table.

4）Configure and apply the route filtering

Command	Explanation
Router configuration mode	

distribute-list {< ***access-list-number*** **|*access-list-name* >|prefix<*prefix-list-name*>}{in|out} [<*ifname*>]** **no distribute-list {<** ***access-list-number*** **|*access-list-name* >|prefix<*prefix-list-name*>}{in|out} [<*ifname*>]**	Configure and apply the access table and prefix table to filter the routes. The **no distribute-list {<** ***access-list-number*** **|*access-list-name*>|prefix<*prefix-list-name* >}{in|out} [<*ifname*>]** command means do not use the access table and prefix table.

5）Configure the split horizon

Command	Explanation
Interface configuration mode	
ip rip split-horizon [poisoned] **no ip rip split-horizon**	Configure that take the split horizon when the port sends data packets; poisoned for poison reverse the **no ip rip split-horizon** command cancels the split horizon.

（3）Configure other RIP protocol parameters

1）Configure RIP routing priority

2）Configure the RIP route capacity limit in route table

3）Configure timer for RIP update, timeout and hold-down

4）Configure RIP UDP receiving buffer size

Command	Explanation
Router configuration mode	
distance <*number*> [<*A.B.C.D/M*>] [<*access-list-name*|*access-list-number* >] **no distance [<*A.B.C.D/M*>]**	Specify the route administratively distance of RIP protocol; the **no distance [<*A.B.C.D/M*>]** command restores the default value 120.
maximum-prefix <*maximum-prefix*>[<*threshold*>] **no maximum-prefix <*maximum-prefix* >** **no maximum-prefix**	Configure the maximum of RIP route; the **no maximum-prefix <*maximum-prefix* >** **no maximum-prefix** command cancels the limit.
timers basic <*update*> <*invalid*> <*garbage*> **no timers basic**	Adjust the update, timeout and garbage collection time, the **no timers basic** command restores the default configuration.
recv-buffer-size <*size*> **no recv-buffer-size**	The command configures the UDP receiving buffer size of the RIP; the **no recv-buffer-size** command restores the system default values.

3. Configure RIP-I/RIP-II toggling

（1）Configure the RIP version to be used in all ports

Command	Explanation
RIP configuration mode	
version { 1 | 2 } **no version**	Configure the versions of all the RIP data packets transmitted/received by the Layer 3 switch port sending/receiving the **no version** command restores the default configuration, version 2.

（**2**）Configure the RIP version to send/receive in all ports.

（**3**）Configure whether to enable RIP packets sending/receiving for ports

Command	Explanation
Interface configuration mode	
ip rip send version { 1 | 1-compatible | 2 } **no ip rip send version**	Sets the version of RIP packets to send on all ports; the **no ip rip send version** command set the version to the one configured by the version command.
ip rip receive version {1 | 2 | } **no ip rip receive version**	Sets the version of RIP packets to receive on all ports; the no action of this command set the version to the one configured by the version command.
ip rip receive-packet **no ip rip receive-packet**	Enables receiving RIP packets on the interface; the **no ip rip receive-packet** command close data receiving on this port.
ip rip send-packet **no ip rip send-packet**	Enables sending RIP packets on the interface; the **no ip rip send-packet** command disables sending RIP packets on the interface.

4. Delete the specified route in RIP route table

Command	Explanation
Admin Mode	
clear ip rip route {<*A.B.C.D/M*>|kernel|static|connected |rip|ospf|isis|bgp|all}	The command deletes a specified route from the RIP route table.

5. Configure the RIP routing aggregation

（1） Configure IPv4 aggregation route globally

Command	Explanation

Router Configuration Mode	
ip rip aggregate-address A.B.C.D/M **no ip rip aggregate-address A.B.C.D/M**	To configure or delete IPv4 aggregation route globally.

（2） Configure IPv4 aggregation route on interface

Command	Explanation
Interface Configuration Mode	
ip rip aggregate-address A.B.C.D/M **no ip rip aggregate-address A.B.C.D/M**	To configure or delete IPv4 aggregation route on interface.

（3） Display IPv4 aggregation route information

Command	Explanation
Admin Mode and Configuration Mode	
show ip rip aggregate	To display aggregation route information.

6. Configure redistribution of OSPF routing to RIP

(1) Enable Redistribution of OSPF routing to RIP

Command	Explanation
Router RIP Configuration Mode	
redistribute ospf [<*process-id*>] [metric <*value*>] [route-map <*word*>] **no redistribute ospf [<process-id>]**	To enable or disable the redistribution of OSPF routing to RIP.

(2) Display and debug the information about configuration of redistribution of OSPF routing to RIP

Command	Explanation
Admin Mode and Configuration Mode	
show ip rip redistribute	To display the information about configuration of redistribute from other routing.
Admin Mode	
debug rip redistribute message send **no debug rip redistribute message send** **debug rip redistribute route receive** **no debug rip redistribute route receive**	To enable or disable debugging messages sent by RIP for redistribution of OSPF routing. To enable or disable debugging messages received from NSM.

3.3 RIP Examples

3.3.1 Typical RIP Examples

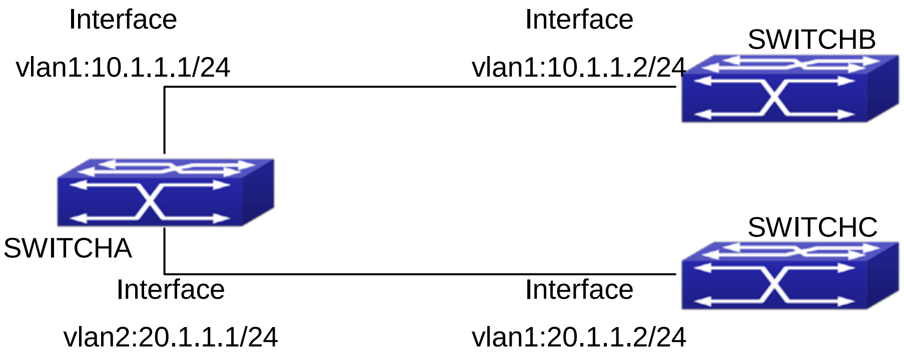

Fig 3-1 RIP example

In the figure shown above, a network consists of three Layer 3 switches, in which SwitchA connected with SwitchB and SwitchC, and RIP routing protocol is running in all of the three switches. SwitchA (interface vlan1：10.1.1.1,interface vlan2：20.1.1.1) exchanges Layer 3 switch update messages only with SwitchB (interface vlan1：10.1.1.2), but not with SwitchC (interface vlan 2: 20.1.1.2).

SwitchA, SwitchB, SwitchC configurations are as follows:

a) Layer 3 SwitchA：

Configure the IP address of interface vlan 1

```
SwitchA#config
SwitchA(config)# interface vlan 1
SwitchA(Config-if-Vlan1)# ip address 10.1.1.1 255.255.255.0
SwitchA(config-if-Vlan1)#
```

Configure the IP address of interface vlan 2

```
SwitchA(config)# vlan 2
SwitchA(Config-Vlan2)# switchport interface ethernet 1/0/2
Set the port Ethernet1/0/2 access vlan 2 successfully
SwitchA(Config-Vlan2)# exit
SwitchA(config)# interface vlan 2
SwitchA(Config-if-Vlan2)# ip address 20.1.1.1 255.255.255.0
```

Initiate RIP protocol and configure the RIP segments

```
SwitchA(config)#router rip
SwitchA(config-router)#network vlan 1
SwitchA(config-router)#network vlan 2
SwitchA(config-router)#exit
```

Configure that the interface vlan 2 do not transmit RIP messages to SwitchC

```
SwitchA(config)#router rip
SwitchA(config-router)#passive-interface vlan 2
SwitchA(config-router)#exit
SwitchA(config) #
```

b) Layer 3 SwitchB

Configure the IP address of interface vlan 1

```
SwitchB#config
SwitchB(config)# interface vlan 1
SwitchB(Config-if-Vlan1)# ip address 10.1.1.2 255.255.255.0
SwitchB(Config-if-Vlan1)exit
```

Initiate RIP protocol and configure the RIP segments

```
SwitchB(config)#router rip
SwitchB(config-router)#network vlan 1
SwitchB(config-router)#exit
```

c) Layer 3 SwitchC

```
SwitchC#config
SwitchC(config)# interface vlan 1
```

Configure the IP address of interface vlan 1

```
SwitchC(Config-if-Vlan1)# ip address 20.1.1.2 255.255.255.0
SwitchC(Config-if-Vlan1)#exit
```

Initiate RIP protocol and configure the RIP segments

```
SwitchC(config)#router rip
SwitchC(config-router)#network vlan 1
SwitchC(config-router)#exit
```

3.3.2 Typical Examples of RIP aggregation function

The application topology as follows：

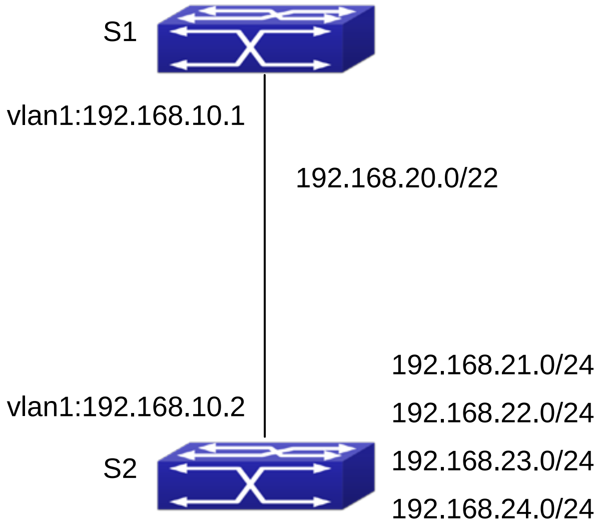

Fig 3-2 Typical application of RIP aggregation

As the above network topology, S2 is connected to S1 through interface vlan1, there are other 4 subnet routers of S2, which are 192.168.21.0/24, 192.168.22.0/24, 192.168.23.0/24, 192.168.24.0/24. S2 supports route aggregation, and to configure aggregation route 192.168.20.0/22 in interface vlan1 of S2, after that, sending router messages to S1 through vlan1, and put the four subnet routers aggregated to one router as 192.168.20.0/22, and send to S1, and not send subnet to neighbor. It can reduce the router table of S1, save the memory.

S1 configuration list:

```
S1(config)#router rip
S1(config-router) #network vlan 1
```

S2 configuration list:

```
S2(config)#router rip
S2(config-router) #network vlan 1
S2(config-router) #exit
S2(config)#in vlan 1
S2(Config-if-Vlan1)# ip rip agg 192.168.20.0/22
```

3.4 RIP Troubleshooting

The RIP protocol may not be working properly due to errors such as physical connection, configuration error when configuring and using the RIP protocol. So users should pay attention to following:

- ☞ First ensure the physic connection is correct
- ☞ Second, ensure the interface and chain protocol are UP (use **show interface** command)

- ☞ Then initiate the RIP protocol (use **router rip** command) and configure the segment (use **network** command) and set RIP protocol parameter on corresponding interfaces, such as the option between RIP-I and RIP-II
- ☞ After that, one feature of RIP protocol should be noticed ---the Layer 3 switch running RIP protocol sending route updating messages to all neighboring Layer 3 switches every 30 seconds. A Layer 3 switch is considered inaccessible if no route updating messages from the switch is received within 180 seconds, then the route to the switch will remains in the route table for 120 seconds before it is deleted. Therefore, if to delete a RIP route, this route item is assured to be deleted from route table after 300 seconds.
- ☞ When exchanging routing messages with CE using RIP protocol on the PE router, we should first create corresponding VPN routing/transmitting examples to associate with corresponding interfaces. Then enter the RIP address family mode configuring corresponding parameters. If the RIP routing problem remains unresolved, please use debug rip command to record the debug message in three minutes, and send them to our technical service center.

Chapter 4 RIPng

4.1 Introduction to RIPng

RIPng is first introduced in ARPANET, this is a protocol dedicated to small, simple networks. RIPng is a distance vector routing protocol based on the Bellman-Ford algorithm. Network devices running vector routing protocol send 2 kind of information to the neighboring devices regularly:

- Number of hops to reach the destination network, or metrics to use or number of networks to pass.
- What is the next hop, or the director (vector) to use to reach the destination network.

Distance vector layer3 switches send all their route selecting tables to the neighbor layer3 switches at regular interval. A layer3 switch will build their own route selecting information table based on the information received from the neighbor layer3 switches. Then, it will send this information to its own neighbor layer3 switches. As a result, the route selection table is built on second hand information, route beyond 15 hops will be deemed as unreachable.

RIPng is an optional routing protocol based on UDP. Hosts using RIPng send and receive packets on UDP port 521. All layer3 switches running RIP send their route table to all neighbor layer3 switches every 30 seconds for update. If no information from the partner is received in 180 seconds, then the device is deemed to have failed and the network connected to that device is considered to be unreachable. However, the route of that layer3 switch will be kept in the route table for another 120 seconds before deletion.

As layer3 switches running RIPng build route table with second hand information, infinite count may occur. For a network running RIPng routing protocol, when a RIPng route becomes unreachable, the neighboring RIPng layer3 switch will not send route update packets at once, instead, it waits until the update interval timeout (every 30 seconds) and sends the update packets containing that route. If before it receives the updated packet, its neighbors send packets containing the information about the failed neighbor, “infinite count” will be resulted. In other words, the route of unreachable layer3 switch will be selected with the metrics increasing progressively. This greatly affects the route selection and route aggregation time.

To avoid “infinite count”, RIPng provides mechanism such as “split horizon” and “triggered update” to solve route loop. “Split horizon” is done by avoiding sending to a gateway routes leaned from that gateway. There are two split horizon methods: “simple split horizon” and “poison reverse split horizon”. Simple split horizon deletes from the route to be sent to the neighbor gateways the routes learnt from the neighbor gateways; poison reverse split horizon not only deletes the abovementioned routes, but set the costs of those routes to infinite. “Triggering update” mechanism defines whenever route metric changed by the gateway, the gateway advertise the update packets immediately other than wait for the 30 sec timer.

So far the RIPng protocol has got only one version----Version1: RIPng protocol is introduced in RFC 2080. RIPng transmits updating data packet by multicast data packet (multicast address FF02::9)

Each layer3 switch running RIPng has a route database, which contains all route entries for reachable destination, and route table is built based on this database. When a RIPng layer3 switch sent route update packets to its neighbor devices, the complete route table is included in the packets. Therefore, in a large network, routing data to be transferred and processed for each layer3 switch is quite large, causing degraded network performance.

Besides the above mentioned, RIPng protocol allows IPv6 route information discovered by the other routing protocols to be introduced to the route table.

The operation of RIPng protocol is shown below:

1. Enable RIPng The switch sends request packets to the neighbor layer3 switches by broadcasting; on receiving the request, the neighbor devices reply with the packets containing their local routing information.
2. The Layer3 switch modifies its local route table on receiving the reply packets and sends triggered update packets to the neighbor devices to advertise route update information. On receiving the triggered update packet, the neighbor lay3 switches send triggered update packets to their neighbor lay3 switches. After a sequence of triggered update packet broadcast, all layer3 switches get and maintain the latest route information.

In addition, RIPng layer3 switches will advertise its local route table to their neighbor devices every 30 seconds. On receiving the packets, neighbor devices maintain their local route table, select the best route and advertise the updated information to their own neighbor devices, so that the updated routes are globally valid. Moreover, RIP uses a timeout mechanism for outdated route, that is, if a switch does not receive regular update packets from a neighbor within a certain interval (invalid timer interval), it considers the route from that neighbor invalid, after holding the route fro a certain interval (garbage collect timer interval), it will delete that route.

As a result of continuous development of IPv6 network, it has the network environment of nonsupport IPv6 sometimes, so it needs to do the IPv6 operation by tunnel. Therefore, our RIPng supports configuration on configure tunnel, and passes through nonsupport IPv6 network by unicast packet of IPv4 encapsulation.

4.2 RIPng Configuration Task List

RIPng Configuration Task List:

1. Enable RIPng protocol (required)
   （1） Enable/disable RIPng protocol
   （2） Configure the interfaces running RIPng protocol
2. Configure RIPng protocol parameters (optional)
   （1） Configure RIPng sending mechanism
      1) Configure specified RIPng packets transmission address
   （2） Configure RIP routing parameters
      1) Configure route introduction (default route metric, configure routes of the other protocols to be introduced in RIPng)
      2) Configure the route deviation
      3) Configure and apply route filter
      4) Configure split horizon
3. Configure other RIPng parameters
   (1) Configure timer for RIPng update, timeout and hold-down
4. Delete the specified route in RIPng route table
5. Configure RIPng route aggregation
   （1） Configure aggregation route of IPv6 route mode
   （2） Configure aggregation route of IPv6 interface configuration mode
   （3） Display IPv6 aggregation route information
6. Configure redistribution of OSPFv3 routing to RIPng
   （1） Enable redistribution of OSPFv3 routing to RIPng
   （2） Display and debug the information about configuration of redistribution of OSPFv3 routing to RIPng

1. Enable RIPng protocol

Applying RIPng route protocol with basic configuration in switch is simple. Normally you only have to open the RIPng switch and configure the segments running RIPng, namely send and receive the RIPng data packet by default RIPng configuration.

Command	Explanation
Global mode	
[no] router IPv6 rip	Enables the RIPng protocol; the **no router IPv6 rip** command shuts the RIPng protocol.
Interface configuration mode	

[no] IPv6 router rip	Configure the interface to run RIPng protocol; the **no IPv6 router rip** command set the interface not run RIPng protocol.

2. Configure RIPng protocol parameters

（1）Configure RIPng sending mechanism

1）Configure the RIPng data packets point-transmitting

Command	Explanation
Router configuration mode	
[no] neighbor *<IPv6-address>* *<ifname>*	Specify the IPv6 Link-local address and interface of the neighboring route needs point-transmitting; the **no neighbor *<IPv6-address>* *<ifname>*** command cancels the appointed router.
[no] passive-interface *<ifname>*	Block the RIPng multicast on specified port and the RIPng data packet is only transmittable among Layer 3 switch configured with neighbor. The **no passive-interface *<ifname>*** command cancels the function.

（2）Configure RIP routing parameters

1）Configure route introduction (default route metric, configure routes of the other protocols to be introduced in RIP)

Command	Explanation
Router configuration mode	
default-metric <*value*> **no default-metric**	Configure the default metric of distributed route; the **no default-metric** command restores the default configuration 1.
[no]redistribute {kernel |connected| static| ospf| isis| bgp} [metric<*value*>] [route-map<*word*>]	Redistribute the routes distributed in other route protocols into the RIPng data packet; the **no redistribute {kernel |connected| static| ospf| isis| bgp} [metric<*value*>] [route-map<*word*>]** command cancels the distributed route of corresponding protocols.
[no]default-information originate	Generate a default route to the RIPng protocol; the **no default-information originate** command cancels the feature.

2）Configure the route offset

Command	Explanation
Router configuration mode	
[no] offset-list <access-list-number |access-list-name> {in|out} <number > [<ifname>]	Configure that provide a deviation value to the route metric value when the port sends or receives RIPng data packet; the **no offset-list *<access-list-number* |*access-list-name>* {in|out} *<number* > [<*ifname*>]** command removes the deviation table.

3）Configure and apply route filter and route aggregation

Command	Explanation
Router configuration mode	
[no] distribute-list {<*access-list-number* |*access-list-name*> | prefix<*prefix-list-name*>} {in|out} [<*ifname*>]	Set to filter the route when the interface sends and receives RIPng data packets. The **no distribute-list {< *access-list-number* |*access-list-name* > | prefix<*prefix-list-name*>} {in|out} [<*ifname*>]** command means do not set the route filter.
[no]aggregate-address *<IPv6-address>*	Configure route aggregation, the **no aggregate-address *<IPv6-address*** command cancels the route aggregation.

4）Configure split horizon

Command	Explanation
Interface configuration mode	
IPv6 rip split-horizon [poisoned]	Configure that take the split-horizon when the port sends data packets, **poisoned** means with poison reverse.
no IPv6 rip split-horizon	Cancel the split-horizon.

3. Configure other RIPng protocol parameters

(1) Configure timer for RIPng update, timeout and hold-down

Command	Explanation
Router configuration mode	

timers basic ***<update> <invalid> <garbage>*** **no timers basic**	Adjust update, timeout and garbage recycle of RIPng timer, the **no timers basic** command restores the default configuration.

4. Delete the specified route in RIPng route table

Command	**Explanation**
Admin Mode	
clear IPv6 rip route {<*IPv6-address*>|kernel|static|connected|rip|ospf|isis|bgp|all}	The command deletes a specified route from the RIP route table.

5. Configure RIPng route aggregation

(1) Configure IPv6 aggregation route globally

Command	Explanation
Router Configuration Mode	
ipv6 rip aggregate-address X:X::X:X/M **no ipv6 rip aggregate-address X:X::X:X/M**	To configure or delete IPv6 aggregation route globally.

(2) Configure IPv6 aggregation route on interface

Command	Explanation
Interface Configuration Mode	
ipv6 rip aggregate-address X:X::X:X/M **no ipv6 rip aggregate-address X:X::X:X/M**	To configure or delete IPv6 aggregation route on interface.

(3) Display IPv6 aggregation route information

Command	Explanation
Admin Mode and Configuration Mode	
show ipv6 rip aggregate	To display IPv6 aggregation route information, such as aggregation interface, metric, numbers of aggregation route, times of aggregation.

6. Configure redistribution of OSPFv3 routing to RIPng

(1)Enable redistribution of OSPFv3 routing to RIPng

Command	Explanation

Router IPv6 RIP Configuration Mode	
redistribute ospf [<*process-tag*>] [metric<*value*>] [route-map<*word*>] **no redistribute ospf [<*process-tag*>]**	To enable or disable redistribution of OSPFv3 routing for RIPng.

(2) Display and debug the information about configuration of redistribution of OSPFv3 routing to RIPng

Command	Explanation
Admin Configuration Mode	
show ipv6 rip redistribute	To display RIPng routing which is redistributed from other routing protocols.
Admin Mode	
debug ipv6 rip redistribute message send **no debug ipv6 rip redistribute message send** **debug ipv6 rip redistribute route receive** **no debug ipv6 rip redistribute route receive**	To enable or disable debugging messages sent by RIPng for redistribution of OSPFv3 routing. To enable or disable debugging route messages received from NSM.

4.3 RIPng Configuration Examples

4.3.1 Typical RIPng Examples

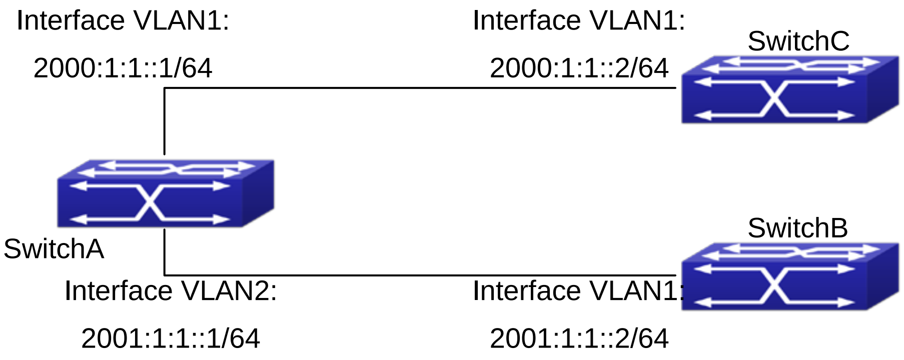

Fig 4-1 RIPng Example

As shown in the above figure, a network consists of three layer 3 switches. SwitchA and SwitchB connect to SwitchC through interface vlan1 and vlan2. All the three switches are running RIPng. Assume SwitchA (VLAN1：2001:1:1::1/64 and VLAN2：2001:1:1::1/64) exchange update information with SwitchB (VLAN1：2001:1:1::2/64) only, update information is not exchanged between SwitchA and SwitchC (VLAN1：2001:1:1::2/64).

The configuration for SwitchA, SwitchB and SwitchC is shown below:

Layer 3 SwitchA

Enable RIPng protocol

```
SwitchA(config)#router IPv6 rip
SwitchA(config-router)#exit
```

Configure the IPv6 address in vlan1 and configure vlan1 to run RIPng

```
SwitchA#config
SwitchA(config)# interface Vlan1
SwitchA(config-if-Vlan1)# IPv6 address 2000:1:1::1/64
SwitchA(config-if-Vlan1)#IPv6 router rip
SwitchA(config-if-Vlan1)#exit
```

Configure the IPv6 address in vlan2 and configure vlan2 to run RIPng

```
SwitchA(config)# interface Vlan2
SwitchA(config-if-Vlan2)#IPv6 address 2001:1:1::1/64
SwitchA(config-if-Vlan2)#IPv6 router rip
SwitchA(config-if-Vlan2)#exit
```

Configure the interface vlan1 do not send RIPng messages to SwitchC

```
SwitchA(config)#
SwitchA(config-router)#passive-interface Vlan1
SwitchA(config-router)#exit
```

Layer 3 SwitchB

Enable RIPng protocol

```
SwitchB (config)#router IPv6 rip
SwitchB (config-router-rip)#exit
```

Configure the IPv6 address and interfaces of Ethernet port vlan1 to run RIPng

```
SwitchB#config
SwitchB(config)# interface Vlan1
SwitchB(config-if)# IPv6 address 2001:1:1::2/64
SwitchB(config-if)#IPv6 router rip
SwitchB(config-if)exit
```

Layer 3 SwitchC

Enable RIPng protocol

```
SwitchC(config)#router IPv6 rip
SwitchC(config-router-rip)#exit
```

Configure the IPv6 address and interfaces of Ethernet port vlan1 to run RIPng

```
SwitchC#config
SwitchC(config)# interface Vlan1
SwitchC(config-if)# IPv6 address 2000:1:1::2/64
SwitchC(config-if)#IPv6 router rip
SwitchC(config-if)exit
```

4.3.2 RIPng Aggregation Route Function Typical Examples

The application topology as follows:

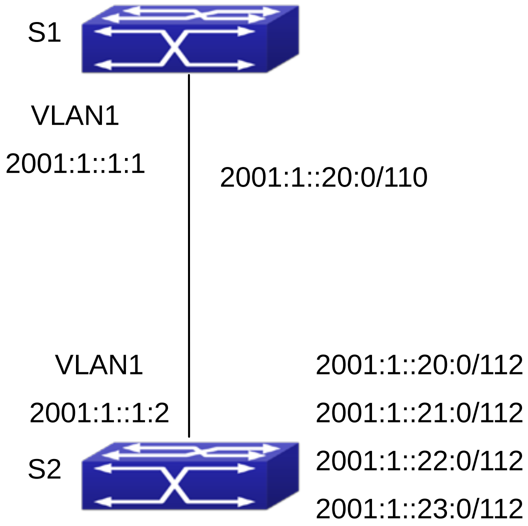

Fig 4-2 Typical application of RIPng aggregation

As the above network topology, S2 is connected to S1 through interface vlan1, there are other 4 subnet routers of S2, which are 2001:1::20:0/112, 2001:1::21:0/112, 2001:1::22:0/112, 2001:1::23:0/112. S2 supports route aggregation, and to configure aggregation route 2001:1::20:0/110 in interface vlan1 of S2, after that, sending router messages to S2 through vlan1, and put the four subnet routers aggregated to one router as 2001:1::20:0/110, and send to S1, and not send subnet to neighbor. It can reduce the router table of S1, save the memory.

S1 configuration list:

```
S1(config)#router ipv6 rip
S1(config)# interface Vlan1
S1(config-if-Vlan1)#IPv6 address 2001:1::1:1/112
S1(config-if-Vlan1)#IPv6 router rip
```

S2 configuration list:

```
S2(config)#router ipv6 rip
```

```
S2(config)#interface vlan 1
S2(config-if-Vlan1)#IPv6 address 2001:1::1:2/112
S2(config-if-Vlan1)#IPv6 router rip
S2(Config-if-Vlan1)#ipv6 rip agg 2001:1::20:0/110
```

4.4 RIPng Troubleshooting

The RIPng protocol may not be working properly due to errors such as physic connection, configuration error when configuring and using the RIPng protocol. So users should pay attention to the following:

- First ensure the physic connection is correct and the IP Forwarding command is open
- Second, ensure the interface and link layer protocol are UP (use **show interface** command)
- Then initiate the RIPng protocol (use **router IPv6 rip** command) and configure the port (use **IPv6 router** command), and set RIPng protocol parameter on corresponding interfaces.
- After that, a RIPng protocol feature should be noticed ---the Layer 3 switch running RIPng transmits the route updating messages every 30 seconds. A Layer 3 switch is considered inaccessible if no route updating messages from the switch are received within 180 seconds, then the route to the switch will remains in the route table for 120 seconds before it is deleted. Therefore, if to delete a RIPng route, this route item is assured to be deleted from route table after 300 seconds.
- If the RIP routing problem remains unresolved, please use **debug IPv6 rip** command to record the debug message in three minutes, and send them to our technical service center.

Chapter 5 OSPF

5.1 Introduction to OSPF

OSPF is abbreviation for Open Shortest Path First. It is an interior dynamic routing protocol for autonomous system based on link-state. The protocol creates a link-state database by exchanging link-states among layer3 switches, and then uses the Shortest Path First algorithm to generate a route table basing on that database.

Autonomous system (AS) is a self-managed interconnected network. In large networks, such as the Internet, a giant interconnected network is broken down to autonomous systems. Big enterprise networks connecting to the Internet are independent AS, since the other hosts on the Internet are not managed by those AS and they don’t share interior routing information with the layer3 switches on the Internet.

Each link-state Layer3 switch can provide information about the topology with its neighboring Layer3 switches.

- The network segment (link) connecting to the layer3 switch
- State of the connecting link

Link-state information is flooded throughout the network so that all Layer3 switches can get firsthand information. Link-state Layer3 switches will not broadcast all information contained in their route tables; instead, they only send changed link-state information. Link-state Layer3 switches establish neighborhood by sending “HELLO” to their neighbors, then link-state advertisements (LSA) will be sent among neighboring Layer3 switches. Neighboring Layer3 switch copy the LSA to their routing table and transfer the information to the rest part of the network. This process is referred to as “flooding”. In this way, firsthand information is sent throughout the network to provide accurate map for creating and updating routes in the network. Link-state routing protocols use cost instead of hops to decide the route. Cost is assigned automatically or manually. According to the algorithm in link-state protocol, cost can be used to calculate the hop number for packets to pass, link bandwidth, and current load of the link. The administrator can even add weight for better assessment of the link-state.

1) When a link-state layer3 switch enters a link-state interconnected network, it sends a HELLO packet to get to know its neighbors and establish neighborhood.

2) The neighbors respond with information about the links they are connecting and the related costs.

3) The originate layer3 switch uses this information to build its own routing table

4) Then, as part of the regular update, layer3 switch send link-state advertisement

(LSA) packets to its neighboring layer3 switches. The LSA include links and related costs of that layer3 switch.

5) Each neighboring layer3 switch copies the LSA packet and passes it to the next neighbor (i.e. flooding).

6) Since routing database is not recalculated before layer3 switch forwards LSA flooding, the converging time is greatly reduced.

One major advantage of link-state routing protocols is the fact that infinite counting is impossible, this is because of the way link-state routing protocols build up their routing table. The second advantage is that converging in a link-state interconnected network is very fast, once the routing topology changes, updates will be flooded throughout the network very soon. Those advantages release some layer3 switch resources, as the process ability and bandwidth used by bad route information are minor.

The features of OSPF protocol include the following: OSPF supports networks of various scales, several hundreds of layer3 switches can be supported in an OSPF network. Routing topology changes can be quickly found and updating LSAs can be sent immediately, so that routes converge quickly. Link-state information is used in shortest path algorithm for route calculation, eliminating loop route. OSPF divides the autonomous system into areas, reducing database size, bandwidth occupation and calculation load. (According to the position of layer3 switches in the autonomous system, they can be grouped as internal area switches, area border switches, AS border switches and backbone switches). OSPF supports load balance and multiple routes to the same destination of equal costs. OSPF supports 4 level routing mechanisms (process routing according to the order of intra-area path, inter-area path, type 1 external path and type 2 external path). OSPF supports IP subnet and redistribution of routes from the other routing protocols, and interface-based packet verification. OSPF supports sending packets in multicast.

Each OSPF layer3 switch maintains a database describing the topology of the whole autonomous system. Each layer3 switch gathers the local status information, such as available interface, reachable neighbors, and sends link-state advertisement (sending out link-state information) to exchange link-state information with other OSPF layer3 switches to form a link-state database describing the whole autonomous system. Each layer3 switch builds a shortest path tree rooted by itself according to the link-state database, this tree provides the routes to all nodes in an autonomous system. If two or more layer3 switches exist (i.e. multi-access network), "designated layer3 switch” and “backup designated layer3 switch” will be selected. Designated layer3 switch is responsible for spreading link-state of the network. This concept helps reducing the traffic among the Layer3 switches in multi-access network.

OSPF protocol requires the autonomous system to be divided into areas. That is to divide the autonomous system into 0 area (backbone area) and non-0 areas. Routing information between areas are further abstracted and summarized to reduce the bandwidth required in the network. OSPF uses four different kinds of routes; they are intra-area route, inter-area route, type 1 external route and type 2 external route, in the order of highest priority to lowest. The route inside an area and between areas describes the internal network structure of an autonomous system, while external routes describe how to select the routing information to destination outside the autonomous system. The first type of exterior route corresponds to the information introduced by OSPF from the other interior routing protocols, the costs of those routes are comparable with the costs of OSPF routes; the second type of exterior route corresponds to the information introduced by OSPF from the other exterior routing protocols, but the costs of those routes are far greater than that of OSPF routes, so OSPF route cost is ignored when calculating route costs.

OSPF areas are centered with the Backbone area, identified as Area 0, all the other areas must be connected to Area 0 logically, and Area 0 must be continuous. For this reason, the concept of virtual link is introduced to the backbone area, so that physically separated areas still have logical connectivity to the backbone area. The configurations of all the layer3 switches in the same area must be the same.

In conclusion, LSA can only be transferred between neighboring Layer3 switches, OSPF protocol includes 5 types of LSA: router LSA, network LSA, network summary LSA to the other areas, ASBR summary LSA and AS external LSA. They can also be called type1 LSA, type2 LSA, type3 LSA, type4 LSA, and type5 LSA. Router LSA is generated by each layer3 switch inside an OSPF area, and is sent to all the other neighboring layer3 switches in the same area; network LSA is generated by the designated layer3 switch in the OSPF area of multi-access network, and is sent to all other neighboring layer3 switches in this area. (In order to reduce traffic on layer3 switches in the multi-access network, “designated layer3 switch” and “backup designated layer3 switch” should be selected in the multi-access network, and the network link-state is broadcasted by the designated layer3 switch); network summary LSA is generated by border switches in an OSPF area , and is transferred among area border layer3 switches; AS external LSA is generated by layer3 switches on external border of AS, and is transferred throughout the AS.

As to autonomous systems mainly advertises exterior link-state, OSPF allow some areas to be configured as STUB areas to reduce the size of the topology database. Type4 LSA (ASBR summary LSA) and type5 LSA (AS external LSA) are not allowed to flood into/through STUB areas. STUB areas must use the default routes, the layer3 switches on STUB area edge advertise the default routes to STUB areas by type 3 summary LSA, those default routes only floods inside STUB area and will not get out of STUB area. Each

STUB area has a corresponding default route, the route from a STUB area to AS exterior destination must rely on the default route of that area.

The following simply outlines the route calculation process of OSPF protocol:

1） Each OSPF-enabled layer3 switch maintains a database (LS database) describing the link-state of the topology structure of the whole autonomous system. Each layer3 switch generates a link-state advertisement according to its surrounding network topology structure (router LSA), and sends the LSA to other layer3 switches through link-state update (LSU) packets. Thus each layer3 switches receives LSAs from other layer3 switches, and all LSAs are combined to the link-state database.

2） Since a LSA is the description of the network topology structure around a layer3 switch, the LS database is the description of the network topology structure of the whole network. The layer3 switches can easily create a weighted vector map according to the LS database. Obviously, all layer3 switches in the same autonomous system will have the same network topology map.

3） Each layer3 switch uses the shortest path first (SPF) algorithm to calculate a tree of shortest path rooted by itself. The tree provides the route to all the nodes in the autonomous system, leaf nodes consist of the exterior route information. The exterior route can be marked by the layer3 switch broadcast it, so that additional information about the autonomous system can be recorded. As a result, the route table of each layer3 switch is different.

OSPF protocol is developed by the IETF; the OSPF v2 widely used now is fulfilled according to the content described in RFC2328.

5.2 OSPF Configuration Task List

The OSPF configuration may be different from the configuration procedure to switches of the other manufacturers. It is a two-step process:

1、 Enable OSPF in the Global Mode;2、Configure OSPF area for the interfaces. The configuration task list is as follows:

1. Enable OSPF protocol (required)
    (1) Enable/disable OSPF protocol (required)
    (2) Configure the ID number of the layer3 switch running OSPF (optional)
    (3) Configure the network scope for running OSPF (optional)
    (4) Configure the area for the interface (required)
2. Configure OSPF protocol parameters (optional)

(1) Configure OSPF packet sending mechanism parameters
    1) Configure OSPF packet verification
    2) Set the OSPF interface to receive only
    3) Configure the cost for sending packets from the interface
    4) Configure OSPF packet sending timer parameter (timer of broadcast interface sending HELLO packet to poll, timer of neighboring layer3 switch invalid timeout, timer of LSA transmission delay and timer of LSA retransmission.
(2) Configure OSPF route introduction parameters
    1) Configure default parameters (default type, default tag value, default cost)
    2) Configure the routes of the other protocols to introduce to OSPF.
(3) Configure OSPF importing the routes of other OSPF processes
    1) Enable the function of OSPF importing the routes of other OSPF processes
    2) Display relative information
    3) Debug
(4) Configure other OSPF protocol parameters
    1) Configure OSPF routing protocol priority
    2) Configure cost for OSPF STUB area and default route
    3) Configure OSPF virtual link
    4) Configure the priority of the interface when electing designated layer3 switch (DR).
    5) Configure to keep a log for OSPF adjacency changes or not
    6) Filter the route obtained by OSPF

3. Disable OSPF protocol

1. Enable OSPF protocol

Basic configuration of OSPF routing protocol on switch is quite simple, usually only enabling OSPF and configuration of the OSPF area for the interface are required. The OSPF protocol parameters can use the default settings. If OSPF protocol parameters need to be modified, please refer to “2. Configure OSPF protocol parameters”.

Command	Explanation
Global Mode	
[no] router ospf [process <*id*>]	Enables OSPF protocol; the **no router ospf** command disables OSPF protocol. (required)
OSPF Protocol Configuration Mode	
router-id <*router_id*> **no router-id**	Configures the ID number for the layer3 switch running OSPF; the **no router id** command

	cancels the ID number. The IP address of an interface is selected to be the layer3 switch ID. (optional)
[no] network {**<*network*> <*mask*> |** **<*network*>/<*prefix*>}** **area <*area_id*>**	Configure certain segment to certain area, the **no network {<network> <*mask*> | <*network*>/<*prefix*>}** **area <area_*id*>** ***command*** cancels this configuration. (required)

2. Configure OSPF protocol parameters

（1）Configure OSPF packet sending mechanism parameters

1）Configure OSPF packet verification

2）Set the OSPF interface to receive only

3）Configure the cost for sending packets from the interface

Command	Explanation
Interface Configuration Mode	
ip ospf authentication { message-digest | null} **no ip ospf authentication**	Configures the authentication method by the interface to accept OSPF packets; the **no ip ospf authentication** command restores the default settings.
ip ospf [<*ip-address*>] authentication-key <*0 LINE* | *7 WORD* | *LINE*> **no ip ospf [<*ip-address*>] authentication**	Specify the authentication key required in sending and receiving OSPF packet on the interface; the no command cancels the authentication key.
[no] passive-interface <*ifname*> [<*ip-address*>]	Sets an interface to receive only, the **no passive-interface <*ifname*>[<*ip-address*>]** command cancels this configuration.
ip ospf cost <*cost* > **no ip ospf cost**	Sets the cost for running OSPF on the interface; the **no ip ospf cost** command restores the default setting.

4) Configure OSPF packet sending timer parameter (timer of broadcast interface sending HELLO packet to poll, timer of neighboring layer3 switch invalid timeout, timer of LSA transmission delay and timer of LSA retransmission).

Command	Explanation
Interface Configuration Mode	

ip ospf hello-interval <*time*> **no ip ospf hello-interval**	Sets interval for sending HELLO packets; the **no ip ospf hello-interval** command restores the default setting.
ip ospf dead-interval <*time* > **no ip ospf dead-interval**	Sets the interval before regarding a neighbor layer3 switch invalid; the **no ip ospf dead-interval** command restores the default setting.
ip ospf transit-delay <*time*> **no ip ospf transit-delay**	Sets the delay time before sending link-state broadcast; the **no ip ospf transmit-delay** command restores the default setting.
ip ospf retransmit <*time*> **no ip ospf retransmit**	Sets the interval for retransmission of link-state advertisement among neighbor layer3 switches; the **no ip ospf retransmit** command restores the default setting.

（2）Configure OSPF route introduction parameters

Configure the routes of the other protocols to introduce to OSPF.

Command	Explanation
OSPF Protocol Configuration Mode	
redistribute { bgp | connected | static | rip | kernel} [metric-type { 1 | 2 }] [tag <*tag*>] [metric <*cost_value*>] [router-map <*WORD*>] **no redistribute { bgp | connected | static | rip | kernel }**	Distribute other protocols to find routing and static routings as external routing messages the **no redistribute {bgp | connected | static | rip | kernel}** command cancels the distributed external messages.

（3）Configure OSPF importing the routes of other OSPF processes

1）Enable the function of OSPF importing the routes of other OSPF processes

Command	Explanation
Router OSPF Mode	
redistribute ospf [<*process-id*>] [metric<*value*>] [metric-type {1|2}][route-map<*word*>] **no redistribute ospf [<*process-id*>] [metric<*value*>] [metric-type {1|2}][route-map<*word*>]**	Enable or disable the function of OSPF importing the routes of other OSPF processes.

2）Display relative information

Command	Explanation
Admin Mode or Configure Mode	
show ip ospf [<*process-id*>] redistribute	Display the configuration information of the OSPF process importing other outside routes.

3）Debug

Command	Explanation
Admin Mode	
debug ospf redistribute message send **no debug ospf redistribute message send**	Enable or disable debugging of sending command from OSPF process redistributed to other OSPF process routing.
debug ospf redistribute route receive **no debug ospf redistribute route receive**	Enable or disable debugging of received routing message from NSM for OSPF process.

（4）Configure other OSPF protocol parameters

1）Configure how to calculate OSPF SPF algorithm time

2）Configure the LSA limit in the OSPF link state database

3）Configure various OSPF parameters

Command	Explanation
OSPF Protocol Configuration Mode	
timers spf <*interval*> **no timers spf**	Configure the SPF timer of OSPF; the **no timers spf** command restores the default settings.
overflow database {<*max-LSA*> [hard | soft] | external <*max-LSA*> <*recover time*>} **no overflow database [external <*max-LSA* > < *recover time* >]**	Configure the LSA limit in current OSPF process database; the **no overflow database [external < *max-LSA* > < *recover time* >]** command restores the default settings.

area <id> {authentication [message-digest] | default-cost <*cost*> | filter-list {access | prefix} <*WORD*> {in | out} | nssa [default-information-originate | no-redistribution | no-summary | translator-role] | range <*range*> | stub [no-summary] | virtual-link <*neighbor*>}
no area <id> {authentication | default-cost | filter-list {access | prefix} <*WORD*> {in | out} | nssa [default-information-originate | no-redistribution | no-summary | translator-role] | range <*range*> | stub [no-summary] | virtual-link <*neighbor*>}
	Configure the parameters in OSPF area (STUB area, NSSA area and virtual links); the **no area <id> {authentication | default-cost | filter-list {access | prefix} <*WORD*> {in | out} | nssa [default-information-originate | no-redistribution | no-summary | translator-role] | range <*range*> | stub [no-summary] | virtual-link <*neighbor*>}** command restores the default settings.

4）Configure the priority of the interface when electing designated layer3 switch (DR).

Command	Explanation
Interface Configuration Mode	
ip ospf priority <*priority*> **no ip ospf priority**	Sets the priority of the interface in “designated layer3 switch” election; the **no ip ospf priority** command restores the default setting.

5）Configure to keep a log for OSPF adjacency changes or not

Command	Explanation
OSPF Protocol Configuration Mode	
log-adjacency-changes detail **no log-adjacency-changes detail**	Configure to keep a log for OSPF adjacency changes or not.

6）Filter the route obtained by OSPF

Command	Explanation
OSPF Protocol Configuration Mode	
filter-policy <access-list-name> **no filter-policy**	Use access list to filter the route obtained by OSPF, the no command cancels the route filtering.

3. Disable OSPF protocol

Command	Explanation
Global Mode	

no router ospf [process <*id*>]	Disables OSPF routing protocol.

5.3 OSPF Examples

5.3.1 Configuration Example of OSPF

Scenario 1: OSPF autonomous system.

This scenario takes an OSPF autonomous system consists of five switch for example.

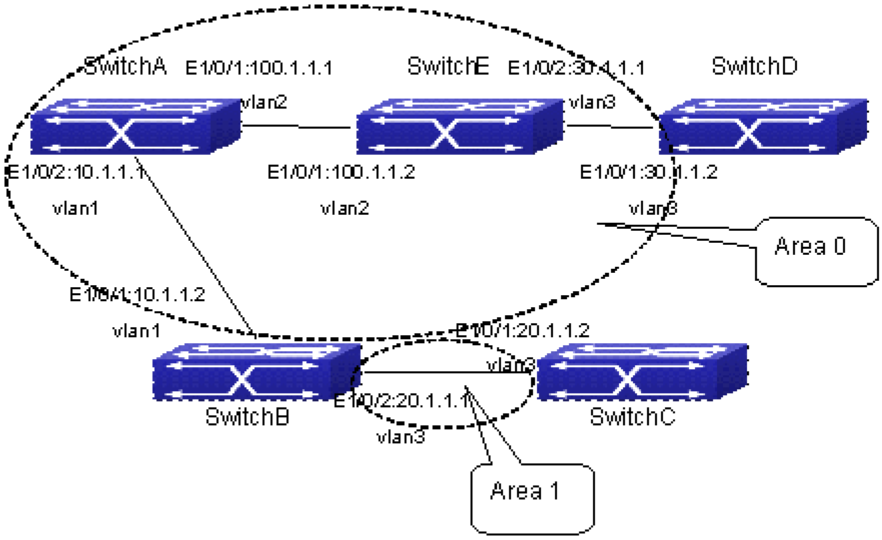

Fig 5-1 Network topology of OSPF autonomous system

The configuration for layer3 Switch1 and Switch5 is shown below:

Layer 3 Switch1

Configuration of the IP address for interface vlan1

```
Switch1#config
Switch1(config)# interface vlan 1
Switch1(config-if-vlan1)# ip address 10.1.1.1 255.255.255.0
Switch1(config-if-vlan1)#exit
```

Configuration of the IP address for interface vlan2

Configure the IP address of interface vlan2

```
Switch1(config)# interface vlan 2
Switch1(config-if-vlan2)# ip address 100.1.1.1 255.255.255.0
Switch1 (config-if-vlan2)#exit
```

Enable OSPF protocol, configure the area number for interface vlan1 and vlan2.

```
Switch1(config)#router ospf
Switch1(config-router)#network 10.1.1.0/24 area 0
Switch1(config-router)#network 100.1.1.0/24 area 0
Switch1(config-router)#exit
```

```
Switch1(config)#exit
Switch1#
```

Layer 3 Switch2:

Configure the IP address for interface vlan1 and vlan2.

```
Switch2#config
Switch2(config)# interface vlan 1
Switch2(config-if-vlan1)# ip address 10.1.1.2 255.255.255.0
Switch2(config-if-vlan1)#no shutdown
Switch2(config-if-vlan1)#exit
Switch2(config)# interface vlan 3
Switch2(config-if-vlan3)# ip address 20.1.1.1 255.255.255.0
Switch2(config-if-vlan3)#no shutdown
Switch2(config-if-vlan3)#exit
```

Enable OSPF protocol, configure the OSPF area interfaces vlan1 and vlan3 in

```
Switch2(config)#router ospf
Switch2(config-router)# network 10.1.1.0/24 area 0
Switch2(config-router)# network 20.1.1.0/24 area 1
Switch2(config-router)#exit
Switch2(config)#exit
Switch2#
```

Layer 3 Switch3:

Configuration of the IP address for interface vlan3.

```
Switch3#config
Switch3(config)# interface vlan 3
Switch3(config-if-vlan1)# ip address 20.1.1.2 255.255.255.0
Switch3(config-if-vlan3)#no shutdown
Switch3(config-if-vlan3)#exit
```

Initiate the OSPF protocol, configure the OSPF area to which interface vlan3 belongs

```
Switch3(config)#router ospf
Switch3(config-router)# network 20.1.1.0/24 area 1
Switch3(config-router)#exit
Switch3(config)#exit
Switch3#
```

Layer 3 Switch4:

Configuration of the IP address for interface vlan3

```
Switch4#config
Switch4(config)# interface vlan 3
Switch4(config-if-vlan3)# ip address30.1.1.2 255.255.255.0
```

```
Switch4(config-if-vlan3)#no shutdown
Switch4(config-if-vlan3)#exit
```

Enable OSPF protocol, configure the OSPF area interfaces vlan3 resides in.

```
Switch4(config)#router ospf
Switch4(config-router)# network 30.1.1.0/24 area 0
Switch4(config-router)#exit
Switch4(config)#exit
Switch4#
```

Layer 3 Switch5:

Configuration of the IP address for interface vlan2

```
Switch5#config
Switch5(config)# interface vlan 2
Switch5(config-if-vlan2)# ip address 100.1.1.2 255.255.255.0
Switch5(config-if-vlan2)#no shutdown
Switch5(config-if-vlan2)#exit
```

Configuration of the IP address for interface vlan3

```
Switch5(config)# interface vlan 3
Switch5(config-if-vlan3)# ip address 30.1.1.1 255.255.255.0
Switch5(config-if-vlan3)#no shutdown
Switch5(config-if-vlan3)#exit
```

Enable OSPF protocol, configure the number of the area in which interface vlan2 and vlan3 reside in.

```
Switch5(config)#router ospf
Switch5(config-router)# network 30.1.1.0/24 area 0
Switch5(config-router)# network 100.1.1.0/24 area 0
Switch5(config-router)#exit
Switch5(config)#exit
Switch5#
```

Scenario 2: Typical OSPF protocol complex topology.

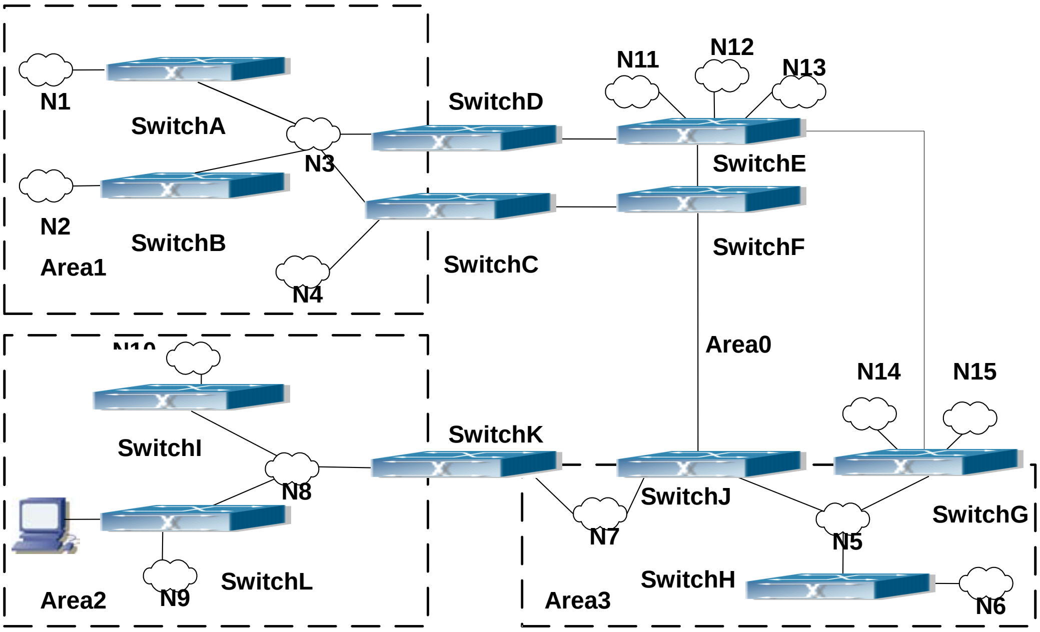

Fig 5-2 Typical complex OSPF autonomous system

This scenario is a typical complex OSPF autonomous system network topology. Area1 include network N1-N4 and layer3 SwitchA-SwitchD, area2 include network N8-N10, host H1 and layer3 SwitchH, area3 include N5-N7 and layer3 SwitchF, SwitchG SwitchA0 and Switch11, and network N8-N10 share a summary route with host H1(i.e. area3 is defined as a STUB area). Layer3 SwitchA, SwitchB, SwitchD, SwitchE, SwitchG, SwitchH, Switch12 are in-area layer3 switches, SwitchC, SwitchD, SwitchF, Switch10 and Switch11 are edge layer3 switches of the area, SwitchD and SwitchF are edge layer3 switches of the autonomous system.

To area1, layer3 switches SwitchA and SwitchB are both in-area switches, area edge switches SwitchC and SwitchD are responsible for reporting distance cost to all destination outside the area, while they are also responsible for reporting the position of the AS edge layer3 switches SwitchD and SwitchF, AS exterior link-state advertisement from SwitchD and SwitchF are flooded throughout the whole autonomous system. When ASE LSA floods in area 1, those LSAs are included in the area 1 database to get the routes to network N11 and N15.

In addition, layer3 SwitchC and SwitchD must summary the topology of area 1 to the backbone area (area 0, all non-0 areas must be connected via area 0, direct connections are not allowed), and advertise the networks in area 1 (N1-N4) and the costs from SwitchC and SwitchD to those networks. As the backbone area is required to keep connected, there must be a virtual link between backbone layer3 Switch10 and Switch11. The area edge layer3 switches exchange summary information via the backbone layer3 switch, each area edge layer3 switch listens to the summary information from the other edge layer3 switches.

Virtual link can not only maintain the connectivity of the backbone area, but also strengthen the backbone area. For example, if the connection between backbone layer3 SwitchG and Switch10 is cut down, the backbone area will become incontinuous. The backbone area can become more robust by establishing a virtual link between backbone layer3 switches SwitchF and Switch10. In addition, the virtual link between SwitchF and Switch10 provide a short path from area 3 to layer3 SwitchF.

Take area 1 as an example. Assume the IP address of layer3 SwitchA is 10.1.1.1, IP address of layer3 SwitchB interface VLAN2 is 10.1.1.2, IP address of layer3 SwitchC interface VLAN2 is 10.1.1.3, IP address of layer3 SwitchD interface VLAN2 is 10.1.1.4. SwitchA is connecting to network N1 through Ethernet interface VLAN1 (IP address 20.1.1.1); SwitchB is connecting to network N2 through Ethernet interface VLAN1 (IP address 20.1.2.1); SwitchC is connecting to network N4 through Ethernet interface VLAN3 (IP address 20.1.3.1). All the three addresses belong to area 1. SwitchC is connecting to layer3 SwitchE through Ethernet interface VLAN1 (IP address 10.1.5.1); SwitchD is connecting to layer3 SwitchD through Ethernet interface VLAN1 (IP address 10.1.6.1); both two addresses belong to area 1. Simple authentication is implemented among layer3 switches in area1, edge layer3 switches of area 1 authenticate with the area 0 backbone layer3 switches by MD5 authentication.

The followings are just configurations for all layer3 switches in area 1, configurations for layer3 switches of the other areas are omitted. The following are the configurations of SwitchA SwitchB.SwitchC and SwitchD:

1)SwitchA:

Configure IP address for interface vlan2

```
SwitchA#config
SwitchA(config)# interface vlan 2
SwitchA(config-If-Vlan2)# ip address 10.1.1.1 255.255.255.0
SwitchA(config-If-Vlan2)#exit
```

Enable OSPF protocol, configure the area number for interface vlan2.

```
SwitchA(config)#router ospf
SwitchA(config-router)#network 10.1.1.0/24 area 1
SwitchA(config-router)#exit
```

Configure simple key authentication.

```
SwitchA(config)#interface vlan 2
SwitchA(config-If-Vlan2)#ip ospf authentication
SwitchA(config-If-Vlan2)#ip ospf authentication-key test
SwitchA(config-If-Vlan2)exit
```

Configure IP address and area number for interface vlan1.

```
SwitchA(config)# interface vlan 1
SwitchA(config-If-Vlan1)#ip address 20.1.1.1 255.255.255.0
SwitchA(config-If-Vlan1)#exit
SwitchA(config)#router ospf
SwitchA(config-router)#network 20.1.1.0/24 area 1
SwitchA(config-router)#exit
```

2)SwitchB:

Configure IP address for interface vlan2

```
SwitchB#config
SwitchB(config)# interface vlan 2
SwitchB(config-If-Vlan2)# ip address 10.1.1.2 255.255.255.0
SwitchB(config-If-Vlan2)#exit
```

Enable OSPF protocol, configure the area number for interface vlan2.

```
SwitchB(config)#router ospf
SwitchB(config-router)#network 10.1.1.0/24 area 1
SwitchB(config-router)#exit
SwitchB(config)#interface vlan 2
```

Configure simple key authentication.

```
SwitchB(config)#interface vlan 2
SwitchB(config-If-Vlan2)#ip ospf authentication
SwitchB(config-If-Vlan2)#ip ospf authentication-key test
SwitchB(config-If-Vlan2)#exit
```

Configure IP address and area number for interface vlan1.

```
SwitchB(config)# interface vlan 1
SwitchB(config-If-Vlan1)#ip address 20.1.2.1 255.255.255.0
SwitchB(config-If-Vlan1)#exit
SwitchB(config)#router ospf
SwitchB(config-router)#network 20.1.2.0/24 area 1
SwitchB(config-router)#exit
SwitchB(config)#exit
```

3)SwitchC:

Configure IP address for interface vlan2

```
SwitchC#config
SwitchC(config)# interface vlan 2
SwitchC(config-If-Vlan2)# ip address 10.1.1.3 255.255.255.0
SwitchC(config-If-Vlan2)#exit
```

Enable OSPF protocol, configure the area number for interface vlan2

```
SwitchC(config)#router ospf
SwitchC(config-router)#network 10.1.1.0/24 area 1
SwitchC(config-router)#exit
```

Configure simple key authentication

```
SwitchC(config)#interface vlan 2
SwitchC(config-If-Vlan2)#ip ospf authentication
SwitchC(config-If-Vlan2)#ip ospf authentication-key test
SwitchC(config-If-Vlan2)#exit
```

Configure IP address and area number for interface vlan3

```
SwitchC(config)# interface vlan 3
SwitchC(config-If-Vlan3)#ip address 20.1.3.1 255.255.255.0
SwitchC(config-If-Vlan3)#exit
SwitchC(config)#router ospf
SwitchC(config-router)#network 20.1.3.0/24 area 1
SwitchC(config-router)#exit
```

Configure IP address and area number for interface vlan 1

```
SwitchC(config)# interface vlan 1
SwitchC(config-If-Vlan1)#ip address 10.1.5.1 255.255.255.0
SwitchC(config-If-Vlan1)#exit
SwitchC(config)#router ospf
SwitchC(config-router)#network 10.1.5.0/24 area 0
SwitchC(config-router)#exit
```

Configure MD5 key authentication.

```
SwitchC(config)#interface vlan 1
SwitchC (config-If-Vlan1)#ip ospf authentication message-digest
SwitchC (config-If-Vlan1)#ip ospf authentication-key test
SwitchC (config-If-Vlan1)#exit
SwitchC(config)#exit
SwitchC#
```

4)SwitchD:

Configure IP address for interface vlan2

```
SwitchD#config
SwitchD(config)# interface vlan 2
SwitchD(config-If-Vlan2)# ip address 10.1.1.4 255.255.255.0
SwitchD(config-If-Vlan2)#exit
```

Enable OSPF protocol, configure the area number for interface vlan2.

```
SwitchD(config)#router ospf
SwitchD(config-router)#network 10.1.1.0/24 area 1
SwitchD(config-router)#exit
```

Configure simple key authentication.

```
SwitchD(config)#interface vlan 2
SwitchD(config-If-Vlan2)#ip ospf authentication
SwitchD(config-If-Vlan2)#ip ospf authentication-key test
SwitchD(config-If-Vlan2)#exit
```

Configure the IP address and the area number for the interface vlan 1

```
SwitchD(config)# interface vlan 1
SwitchD(config-If-Vlan1)# ip address 10.1.6.1 255.255.255.0
SwitchD(config-If-Vlan1)exit
SwitchD(config)#router ospf
SwitchD(config-router)#network 10.1.6.0/24 area 0
SwitchD(config-router)#exit
```

Configure MD5 key authentication

```
SwitchD(config)#interface vlan 1
SwitchD(config-If-Vlan1)#ip ospf authentication message-digest
SwitchD(config-If-Vlan1)#ip ospf authentication-key test
SwitchD(config-If-Vlan1)exit
SwitchD(config)#exit
SwitchD#
```

Scenario 3: The function of OSPF importing the routers of other OSPF processes

As shown in the following graph, a switch running the OSPF routing protocol connects two networks: network A and network B. Because of some reason, it is required that network A should be able to learn the routers of network B, but network B should not be able to learn the routers of network A. According to that, two OSPF processes can be started respectively on interface vlan 1 and interface vlan 2. the OSPF process which interface vlan 1 belongs to is configured to import the routers of the OSPF process which interface vlan 2 belongs to, while the OSPF process which interface vlan 2 belongs to should not be configured to import the routers of the OSPF process which interface vlan 1 belongs to.

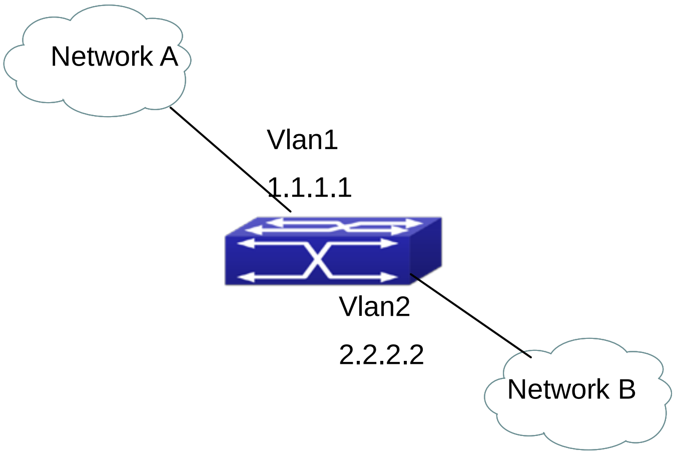

Fig 5-3 Function of OSPF importing the routers of other OSPF processes example

We can configure as follows:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 1.1.1.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ip address 2.2.2.2 255.255.255.0
Switch(Config-if-Vlan2)#exit
Switch(config)#router ospf 10
Switch(config-router)#network 2.2.2.0/24 area 1
Switch(config-router)#exit
Switch(config)#router ospf 20
Switch(config-router)#network 1.1.1.0/24 area 1
Switch(config-router)#redistribute ospf 10
Switch(config-router)#exit
```

5.3.2 Configuration Examples of OSPF VPN

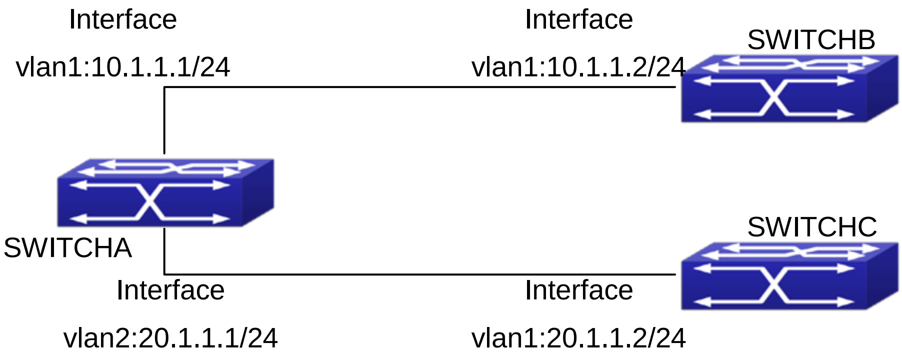

Fig 5-4 OSPF VPN Example

The above figure shows that a network consists of three Layer 3 switches in which the switchA as PE, SwitchB and SwitchC as CE1 and CE2. The PE is connected to CE1 and CE2 through vlan1 and vlan2. The routing messages are exchanged between PE and CE through OSPF protocol.

a) SwitchA, the Layer 3 switch as PE

Configure VPN route/transmitting examples vpnb and vpnc

```
SwitchA#config
SwitchA(config)#ip vrf vpnb
SwitchA(config-vrf)#
SwitchA(config-vrf)#exit
SwitchA#(config)
SwitchA(config)#ip vrf vpnc
SwitchA(config-vrf)#
SwitchA(config-vrf)#exit
```

Associate the vlan 1 and vlan 2 respectively with vpnb and vpnc while configuring IP address

```
SwitchA(config)#in vlan1
SwitchA(config-if-Vlan1)#ip vrf forwarding vpnb
SwitchA(config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0
SwitchA(config-if-Vlan1)#exit
SwitchA(config)#in vlan2
SwitchA(config-if-Vlan2)#ip vrf forwarding vpnc
SwitchA(config-if-Vlan2)#ip address 20.1.1.1 255.255.255.0
SwitchA(config-if-Vlan2)#exit
```

Configure OSPF examples associated with vpnb and vpnc respectively

```
SwitchA(config)#
SwitchA(config)#router ospf 100 vpnb
SwitchA(config-router)#network 10.1.1.0/24 area 0
SwitchA(config-router)#redistribute bgp
SwitchA(config-router)#exit
SwitchA(config)#router ospf 200 vpnc
SwitchA(config-router)#network 20.1.1.0/24 area 0
SwitchA(config-router)#redistribute bgp
```

b) The Layer 3 SwitchB of CE1：

Configure the IP address of Ethernet E 1/0/2

```
SwitchB#config
SwitchB(config)# interface Vlan1
SwitchB(config-if-vlan1)# ip address 10.1.1.2 255.255.255.0
```

```
SwitchB (config-if-vlan1)exit
```

Enable OSPF protocol and configuring OSPF segments

```
SwitchB(config)#router ospf
SwitchB(config-router-rip)#network 10.1.1.0/24 area 0
SwitchB(config-router-rip)#exit
```

c) The Layer 3 SwitchC of CE2

Configure the IP address of Ethernet E 1/0/2

```
SwitchC#config
SwitchC(config)# interface Vlan1
SwitchC(config-if-vlan1)# ip address 20.1.1.2 255.255.255.0
SwitchC(config-if-vlan1)#exit
```

Initiate OSPF protocol and configuring OSPF segments

```
SwitchC(config)#router ospf
SwitchC(config-router)#network 20.1.1.0/24 area 0
SwitchC(config-router)#exit
```

5.4 OSPF Troubleshooting

The OSPF protocol may not be working properly due to errors such as physic connection, configuration error when configuring and using the OSPF protocol. So users should pay attention to following:

- First ensure the physic connection is correct
- Second, ensure the interface and link protocol are UP (use **show interface** command)
- Configure different IP address from different segment on each interface
- Then initiate OSPF protocol (use **router-ospf** command) and configure the OSPF area on corresponding interface
- After that, a OSPF protocol feature should be checked---the OSPF backbone area should be continuous and apply virtual link to ensure it is continuous. if not; all non 0 areas should only be connected to other non 0 area through 0 area; a border Layer 3 switch means that one part of the interfaces of this switch belongs to 0 area, the other part belongs to non 0 area; Layer 3 switch DR should be specified for multi-access network such as broadcast network.

Chapter 6 OSPFv3

6.1 Introduction to OSPFv3

OSPFv3 (Open Shortest Path First) is the third version for Open Shortest Path First, and it is the IPv6 version of OSPF Protocol. It is an interior dynamic routing protocol for autonomous system based on link-state. The protocol creates a link-state database by exchanging link-states among layer3 switches, and then uses the Shortest Path First algorithm to generate a route table basing on that database.

Autonomous system (AS) is a self-managed interconnected network. In large networks, such as the Internet, a giant interconnected network is broken down to autonomous systems. Big enterprise networks connecting to the Internet are independent AS, since the other hosts on the Internet are not managed by those AS and they don’t share interior routing information with the layer3 switches on the Internet.

Each link-state layer3 switch can provide information about the topology with its neighboring layer3 switches.

- The network segment (link) connecting to the layer3 switch
- State of the connecting link

Link-state information is flooded throughout the network so that all layer3 switches can get first hand information. Link-state layer3 switches will not broadcast all information contained in their route tables; instead, they only send changed link-state information. Link-state layer3 switches establish neighborhood by sending “HELLO” to their neighbors, then link-state advertisements (LSA) will be sent among neighboring layer3 switches. Neighboring layer3 switch copy the LSA to their routing table and transfer the information to the rest part of the network. This process is referred to as “flooding”. In this way, firsthand information is sent throughout the network to provide accurate map for creating and updating routes in the network. Link-state routing protocols use cost instead of hops to decide the route. Cost is assigned automatically or manually. According to the algorithm in link-state protocol, cost can be used to calculate the hop number for packets to pass, link bandwidth, and current load of the link, the administrator can even add weight for better assessment of the link-state.

1) When a link-state layer3 switch enters a link-state interconnected network, it sends a HELLO packet to get to know its neighbors and establish neighborhood.

2) The neighbors respond with information about the links they are connecting and the related costs.

3) The originate layer3 switch uses this information to build its own routing table.

4) Then, as part of the regular update, layer3 switch send link-state advertisement (LSA) packets to its neighboring layer3 switches. The LSA include links and related costs of that layer3 switch.

5) Each neighboring layer3 switch copies the LSA packet and passes it to the next neighbor (i.e. flooding).

6) Since routing database is not recalculated before layer3 switch forwards LSA flooding, the converging time is greatly reduced.

One major advantage of link-state routing protocols is the fact that infinite counting is impossible, this is because of the way link-state routing protocols build up their routing table. The second advantage is that converging in a link-state interconnected network is very fast, once the routing topology changes, updates will be flooded throughout the network very soon. Those advantages release some layer3 switch resources, as the process ability and bandwidth used by bad route information are minor.

The features of OSPFv3 protocol include the following: OSPFv3 supports networks of various scales, several hundreds of layer3 switches can be supported in an OSPFv3 network. Routing topology changes can be quickly found and updating LSAs can be sent immediately, so that routes converge quickly. Link-state information is used in shortest path algorithm for route calculation, eliminating loop route. OSPFv3 divides the autonomous system intro areas, reducing database size, bandwidth occupation and calculation load. (According to the position of layer3 switches in the autonomous system, they can be grouped as internal area switches, area edge switches, AS edge switches and backbone switches). OSPFv3 supports load balance and multiple routes to the same destination of equal costs. OSPFv3 supports 4 level routing mechanisms (process routing according to the order of route inside an area, route between areas, type 1 external route and type 2 external route). OSPFv3 support IP subnet and redistribution of routes from the other routing protocols, and interface-based packet verification. OSPFv3 supports sending packets in multicast.

Each OSPFV3 layer3 switch maintains a database describing the topology of the whole autonomous system. Each layer3 switch gathers the local status information, such as available interface, reachable neighbors, and sends link-state advertisement (sending out link-state information) to exchange link-state information with other OSPFv3 layer3 switches to form a link-state database describing the whole autonomous system. Each layer3 switch builds a shortest path tree rooted by itself according to the link-state database, this tree provide the routes to all nodes in an autonomous system. If two or more layer3 switches exist (i.e. multi-access network), "designated layer3 switch” and “backup designated layer3 switch” will be selected. Designated layer3 switch is responsible for spreading link-state of the network. This concept helps reducing the traffic among the Layer3 switches in multi-access network.

OSPFv3 protocol requires the autonomous system to be divided into areas. That is to divide the autonomous system into 0 area (backbone area) and non-0 areas. Routing information between areas are further abstracted and summarized to reduce the bandwidth required in the network. OSPFv3 uses four different kinds of routes: they are the route inside the area, route between areas, type 1 external route and type 2 external route, in the order of highest priority to lowest. The route inside an area and between areas describe the internal network structure of an autonomous system, while external routes describe external routes describe how to select the routing information to destination outside the autonomous system. The first type of exterior route corresponds to the information introduced by OSPFv3 from the other interior routing protocols, the costs of those routes are comparable with the costs of OSPFv3 routes; the second type of exterior route corresponds to the information introduced by OSPFv3 from the other exterior routing protocols, but the costs of those routes are far greater than that of OSPFv3 routes, so OSPFv3 route cost is ignored when calculating route costs.

OSPFv3 areas are centered with the Backbone area, identified as the Area 0, all the other areas must be connected to Area 0 logically, and Area 0 must be continuous. For this reason, the concept of virtual link is introduced to the backbone area, so that physically separated areas still have logical connectivity to the backbone area. The configurations of all the layer3 switches in the same area must be the same.

In one word, LSA can only be transferred between neighboring Layer3 switches, and OSPFv3 protocol includes seven kinds of LSA: link LSA, internal-area prefix LSA, router LSA, network LSA, inter-area prefix LSA, inter-area router LSA and autonomic system exterior LSA. Router LSA is generated by each Layer 3 switch in an OSPF area, and is sent to all other neighboring Layer 3 switch in this area; network LSA is generated by designated Layer 3 switch in the OSPF area of multi-access network and is sent to all other neighboring layer3 switches in this area.(To reduce data traffic among each Layer 3 switches in the multi-access network, “designated layer3 switch” and “backup designated layer3 switch” should be selected in the multi-access network, and the network link-state is broadcasted by designated Layer 3 switch); the inter-area prefix LSA and inter-area router LSA are generated by OSPF area border Layer 3 switches and transferred among those switches. The autonomic system exterior LSA is generated by autonomic system exterior border Layer 3 switches and transferred in the whole autonomic system. Link LSA is generated by Layer 3 switch on the link and sent to other Layer 3 switches on the link. Internal-area prefix LSA is generated by designated layer3 switch of each link in this area, and flooded to the whole area.

For autonomous system focused on exterior link-state announcement, OSPFv3 allow some areas to be configured as STUB areas in order to reduce the size of topological database. Router LSA, network LSA, inter-area prefix LSA, link LSA, internal-area prefix

LSA are permitted to advertise to STUB area. Default route must be used in STUB area, Layer 3 switches on the area border of STUB area announces to default routes of STUB area by inter-area prefix LSA; these default routes only flood in STUB area, not outside of STUB area. Each STUB area has a corresponding default route, the route from STUB area to AS exterior destination depends only on default route of this area.

The following simply outlines the route calculation process of OSPFv3 protocol:

1) Each OSPF-enabled layer3 switch maintains a database (LS database) describing the link-state of the topology structure of the whole autonomous system. Each layer3 switch generates a link-state advertisement according to its surrounding network topology structure (router LSA), and sends the LSA to other layer3 switches through link-state update (LSU) packets. Thus, each layer3 switches receives LSAs from other layer3 switches, and all LSAs combined to the link-state database.
2) Since a LSA is the description of the network topology structure around a layer3 switch, the LS database is the description of the network topology structure of the whole network. The layer3 switches can easily create a weighted vector map according to the LS database. Obviously, all layer3 switches in the same autonomous system will have the same network topology map.
3) Each layer3 switch uses the shortest path first (SPF) algorithm to calculate a tree of shortest path rooted by itself. The tree provides the route to all the nodes in the autonomous system, leaf nodes consist of the exterior route information. The exterior route can be marked by the layer3 switch broadcast it, so that additional information about the autonomous system can be recorded. As a result, the route table of each layer3 switch is different.

OSPFv3 protocol is developed by the IETF, the OSPF v3 used now is fulfilled according to the content described in RFC2328 and RFC2740.

As a result of continuous development of IPv6 network, it has the network environment of nonsupport IPv6 sometimes, so it needs to do the IPv6 operation by tunnel. Therefore, our OSPFv3 supports configuration on configure tunnel, and passes through nonsupport IPv6 network by unicast packet of IPv4 encapsulation.

6.2 OSPFv3 Configuration Task List

OSPFv3 Configuration Task List:

1. Enable OSPFv3 (required)
   （1） Enable/disable OSPFv3 (required)
   （2） Configure the router-id number of the layer3 switch running OSPFv3 (optional)

（3） Configure the network scope for running OSPFv3 (optional)
（4） Enable OSPFv3 on the interface (required)

2. Configure OSPFv3 auxiliary parameters (optional)
  （1） Configure OSPFv3 packet sending mechanism parameters
    1) Set the OSPFv3 interface to receive only
    2) Configure the cost for sending packets from the interface
    3) Configure OSPFv3 packet sending timer parameter (timer of broadcast interface sending HELLO packet to poll, timer of neighboring layer3 switch invalid timeout, timer of LSA transmission delay and timer of LSA retransmission).
  （2） Configure OSPFv3 route introduction parameters
    1) Configure default parameters (default type, default tag value, default cost)
    2) Configure the routes of the other protocols to introduce to OSPFv3
  （3） Configure OSPFv3 importing the routes of other OSPFv3 processes
    1) Enable the function of OSPFv3 importing the routes of other OSPFv3 processes
    2) Display relative information
    3) Debug
  （4） Configure other OSPFv3 protocol parameters
    1) Configure OSPFv3 routing protocol priority
    2) Configure cost for OSPFv3 STUB area and default route
    3) Configure OSPFv3 virtual link
    4) Configure the priority of the interface when electing designated layer3 switch
3. Close OSPFv3 Protocol

1. Enable OSPFv3 Protocol

It is very simple to run the basic configurations of OSPFv3 routing protocol on the Layer 3 switch, normally only enabling OSPFv3, implement OSPFv3 interface, the default value is defined to OSPFv3 protocol parameters. Refer to 2. Configure OSPF auxiliary parameters, if the OSPFv3 protocol parameters need to be modified.

Commands	Explanation
Global Mode	
[no] router IPv6 ospf <*tag*>	The command initializes OSPFv3 routing process and enter OSPFv3 mode to configure OSPFv3 routing process. The **no router IPv6 ospf <*tag*>** command stops relative process. (required)
OSPFv3 Protocol Configure Mode	

router-id <*router_id*> **no router-id**	Configure router for OSPFv3 process. The **no router-id** command returns ID to 0.0.0.0 .(required)
[no] passive-interface<*ifname*>	Configure an interface receiving without sending. The **no passive-interface<*ifname*>** command cancels configuration.
Interface Configuration Mode	
[no] IPv6 router ospf {area <*area-id*> [instance-id <*instance-id*> | tag <*tag*> [instance-id <*instance-id*>]] | tag <*tag*> area <*area-id*> [instance-id <*instance-id*>]}	Implement OSPFv3 routing on the interface. The **no IPv6 router ospf {area <*area-id*> [instance-id <*instance-id*> | tag <*tag*> [instance-id <*instance-id*>]] | tag <*tag*> area <*area-id*> [instance-id <*instance-id*>]}** command cancels configuration.

2. Configure OSPFv3 parameters

（1）Configure OSPFv3 packet sending mechanism parameters

1）Set the OSPF interface to receive only

2）Configure the cost for sending packets from the interface

Commands	Explanation
Interface Configuration Mode	
IPv6 ospf cost <*cost*> [instance-id <*id*>] **no IPv6 ospf cost [instance-id <*id*>]**	Appoint interface to implement required cost of OSPFv3 protocol. The **no IPv6 OSPF cost [instance-id <*id*>]** restores the default setting.

3）Configure OSPFv3 packet sending timer parameter (timer of broadcast interface sending HELLO packet to poll, timer of neighboring layer3 switch invalid timeout, timer of LSA transmission delay and timer of LSA retransmission).

Commands	Explanation
Interface Configuration Mode	
IPv6 ospf hello-interval <*time*> [instance-id <*id*>] **no IPv6 ospf hello-interval [instance-id <*id*>]**	Sets interval for sending HELLO packets; the **no IPv6 ospf hello-interval [instance-id <*id*>]** command restores the default setting.

IPv6 ospf dead-interval <*time*> [instance-id <*id*>] **no IPv6 ospf dead-interval [instance-id <*id*>]**	Sets the interval before regarding a neighbor layer3 switch invalid; the **no IPv6 ospf dead-interval [instance-id <*id*>]** command restores the default setting.
IPv6 ospf transit-delay <*time*> [instance-id <*id*>] **no IPv6 ospf transit-delay [instance-id <*id*>]**	Sets the delay time before sending link-state broadcast; the **no IPv6 ospf transit-delay [instance-id <*id*>]** command restores the default setting.
IPv6 ospf retransmit <*time*> [instance-id <*id*>] **no IPv6 ospf retransmit [instance-id <*id*>]**	.Sets the interval for retransmission of link-state advertisement among neighbor layer3 switches; the **no IPv6 ospf retransmit [instance-id <*id*>]** command restores the default setting.

（2）Configure OSPFv3 route introduction parameters

Configure OSPFv3 route introduction parameters

Commands	Explanation
OSPF Protocol Mode	
[no]redistribute {kernel |connected| static| rip| isis| bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>]	Introduces other protocol discovery routing and static routing regarded as external routing message. The **no redistribute {kernel |connected| static| rip| isis| bgp} [metric<*value*>] [metric-type {1|2}][route-map<*word*>]** command cancels imported external routing message.

（3）Configure OSPFv3 importing the routes of other OSPFv3 processes

1）Enable the function of OSPFv3 importing the routes of other OSPFv3 processes

Command	Explanation
Router IPv6 OSPF Mode	
redistribute ospf [<*process-id*>] [metric<*value*>] [metric-type {1|2}][route-map<*word*>] **no redistribute ospf [<*process-id*>] [metric<*value*>] [metric-type {1|2}][route-map<*word*>]**	Enable or disable the function of OSPFv3 importing the routes of other OSPFv3 processes.

2）Display relative information

Command	Explanation
Admin Mode or Configure Mode	
show ipv6 ospf [<*process-id*>] redistribute	Display the configuration information of the OSPFv3 process importing other outside routes.

3）Debug

Command	Explanation
Admin Mode	
debug ipv6 ospf redistribute message send **no debug ipv6 ospf redistribute message send** **debug ipv6 ospf redistribute route receive** **no debug ipv6 ospf redistribute route receive**	Enable or disable debugging of sending command from OSPFv3 process redistributed to other OSPFv3 process routing. Enable or disable debugging of received routing message from NSM for OSPFv3 process.

（4） Configure Other Parameters of OSPFv3 Protocol

1） Configure OSPFv3 STUB Area & Default Routing Cost

2） Configure OSPFv3 Virtual Link

Commands	Explanation
OSPFv3 Protocol Configuration Mode	
timers spf <*spf-delay*> <*spf-holdtime*> **no timers spf**	Configure OSPFv3 SPF timer. The **no timers spf** command recovers default value.
area <*id*> stub [no-summary] **no area <*id*> stub [no-summary]** **area <*id*> default-cost <*cost*>** **no area <*id*> default-cost** **area <*id*> virtual-link A.B.C.D [instance-id <*instance-id*> INTERVAL]** **no area <*id*> virtual-link A.B.C.D [|INTERVAL]**	Configure parameters in OSPFv3 area (STUB area, Virtual link). The no command restores default value.

4）Configure the priority of the interface when electing designated layer3 switch (DR).

Commands	Explanation
Interface Configuration Mode	
IPv6 ospf priority *<priority>* [instance-id <*id*>] **no IPv6 ospf priority [instance-id <*id*>]**	Sets the priority of the interface in "designated layer3 switch" election; the "**no IPv6 ospf priority [instance-id <*id*>]**" command restores the default setting.

3. Disable OSPFv3 Protocol

Commands	Explanation
Global Mode	
no router IPv6 ospf ospf [<*tag*>]	Disable OSPFv3 Routing Protocol.

6.3 OSPFv3 Examples

Examples 1: OSPF autonomous system.

This scenario takes an OSPF autonomous system consists of five switch for example.

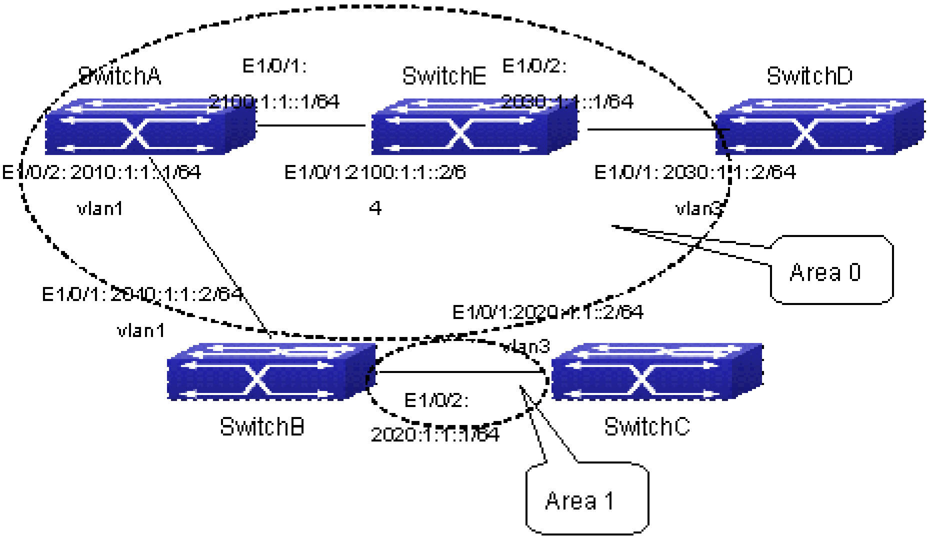

Fig 6-1 Network topology of OSPF autonomous system

The configuration for layer3 SwitchA and SwitchE is shown below:

Layer3 SwitchA:

Enable OSPFv3 protocol, configure router ID

```
SwitchA(config)#router IPv6 ospf
SwitchA (config-router)#router-id 192.168.2.1
```

Configure interface vlan1 IPv6 address and affiliated OSPFv3 area

```
SwitchA#config
```

```
SwitchA(config)# interface vlan 1
SwitchA(config-if-vlan1)# IPv6 address 2010:1:1::1/64
SwitchA(config-if-vlan1)# IPv6 router ospf area 0
SwitchA(config-if-vlan1)#exit
```

Configure interface vlan2 IP address and affiliated OSPFv3 area

```
SwitchA(config)# interface vlan 2
SwitchA(config-if-vlan2)# IPv6 address 2100:1:1::1/64
SwitchA(config-if-vlan2)# IPv6 router ospf area 0
SwitchA (config-if-vlan2)#exit
SwitchA(config)#exit
SwitchA#
```

Layer 3 SwitchB:

Enable OSPFv3 protocol, configure router ID

```
SwitchB(config)#router IPv6 ospf
SwitchB (config-router)#router-id 192.168.2.2
```

Configure interface vlan1 address, VLAN2 IPv6 address and affiliated OSPFv3 area

```
SwitchB#config
SwitchB(config)# interface vlan 1
SwitchB(config-if-vlan1)# IPv6 address 2010:1:1::2/64
SwitchB(config-if-vlan1)# IPv6 router ospf area 0
SwitchB(config-if-vlan1)#exit
SwitchB(config)# interface vlan 3
SwitchB(config-if-vlan3)# IPv6 address 2020:1:1::1/64
SwitchB(config-if-vlan3)# IPv6 router ospf area 1
SwitchB(config-if-vlan3)#exit
SwitchB(config)#exit
SwitchB#
```

Layer 3 SwitchC:

Enable OSPFv3 protocol, configure router ID

```
SwitchC(config)#router IPv6 ospf
SwitchC(config-router)#router-id 192.168.2.3
```

Configure interface vlan3 IPv6 address and affiliated OSPFv3 area

```
SwitchC#config
SwitchC(config)# interface vlan 3
SwitchC(config-if-vlan3)# IPv6 address 2020:1:1::2/64
SwitchC(config-if-vlan3)# IPv6 router ospf area 1
SwitchC(config-if-vlan3)#exit
SwitchC(config)#exit
```

```
SwitchC#
```

Layer 3 SwitchD:

Enable OSPFv3 protocol, configure router ID

```
SwitchD(config)#router IPv6 ospf
SwitchD(config-router)#router-id 192.168.2.4
```

Configure interface vlan3 IPv6 address and affiliated OSPFv3 area

```
SwitchD#config
SwitchD(config)# interface vlan 3
SwitchD(config-if-vlan3)# IPv6 address 2030:1:1::2/64
SwitchD(config-if-vlan3)# IPv6 router ospf area 0
SwitchD(config-if-vlan3)#exit
SwitchD(config)#exit
SwitchD#
```

Layer 3 SwitchE:

Startup OSPFv3 protocol, configure router ID

```
SwitchE(config)#router IPv6 ospf
SwitchE(config-router)#router-id 192.168.2.5
```

Configure interface IPv6 address and affiliated OSPFv3 area

```
SwitchE#config
SwitchE(config)# interface vlan 2
SwitchE(config-if-vlan2)# IPv6 address 2100:1:1::2/64
SwitchE(config-if-vlan2)# IPv6 router ospf area 0
SwitchE(config-if-vlan2)#exit
```

Configure interface VLAN3 IPv6 address and affiliated area

```
SwitchE(config)# interface vlan 3
SwitchE(config-if-vlan3)# IPv6 address 2030:1:1::1/64
SwitchE(config-if-vlan3)# IPv6 router ospf area 0
SwitchE(config-if-vlan3)#exit
SwitchE(config)#exit
SwitchE#
```

6.4 OSPFv3 Troubleshooting

In the process of configuring and implementing OSPFv3, physical connection, configuration false probably leads to OSPFv3 protocol doesn’t work. Therefore, the customers should give their attention to it:

- First of all, to ensure correct physical connection;
- Secondly, to ensure interface and link protocol are UP (execute **show interface**

instruction);

- And configure IPv6 address of the different net segment on every interface.
- To startup OSPFv3 protocol (execute **router IPv6 OSPF** instruction), and configure affiliated OSPFv3 area on relative interface.
- And then, consider OSPFv3 protocol characteristic —— OSPFv3 backbone area (area 0) must be continuous. If it doesn't ensure that virtual link is implemented continuously, all of not area 0 only can be connected by area 0 and other not area 0, not directly connected by not area 0; The border Layer 3 switch is a part of this Layer 3 switch interface belongs to area 0, and another part of interface belongs to not area 0; for multi-access net etc like broadcast, Layer 3 switch DR needs vote and appoint; for each OSPFv3 process must not configure router ID of 0.0.0.0 address.

Chapter 7 Black Hole Routing Manual

7.1 Introduction to Black Hole Routing

Black Hole Routing is a special kind of static routing which drops all the datagrams that match the routing rule.

7.2 IPv4 Black Hole Routing Configuration Task

1. Configure IPv4 Black Hole Routing

1. Configure IPv4 Black Hole Routing

Command	Explaination
Global Configuration Mode	
ip route {<*ip-prefix*> <*mask*>|<*ip-prefix*>/<*prefix-length*>} null0 [<*distance*>] **no ip route {<*ip-prefix*> <*mask*>|<*ip-prefix*>/<*prefix-length*>} null0**	To configure the static Black Hole Routing. The no form of this command will remove the specified Black Hole Routing configuration.

7.3 IPv6 Black Hole Routing Configuration Task

1. Enable the IPv6 function
2. Configure the IPv6 Black Hole Routing

1. Enable the IPv6 function

Command	Explaination
Global Configuration Mode	
ipv6 enable	To enable the IPv6 function on the switch.

2. Configure IPv6 Black Hole Routing

Command	Explaination
Global Configuration Mode	

ipv6 route *<ipv6-prefix/prefix-length>* null0 [<*precedence*>] **no ipv6 route *<ipv6-prefix/prefix-length>* null0**	To configure static IPv6 Black Hole Routing. The no form of this command will remove the specified configuration.

7.4 Black Hole Routing Configuration Exmaples

Example 1: IPv4 Black Hole Routing function.

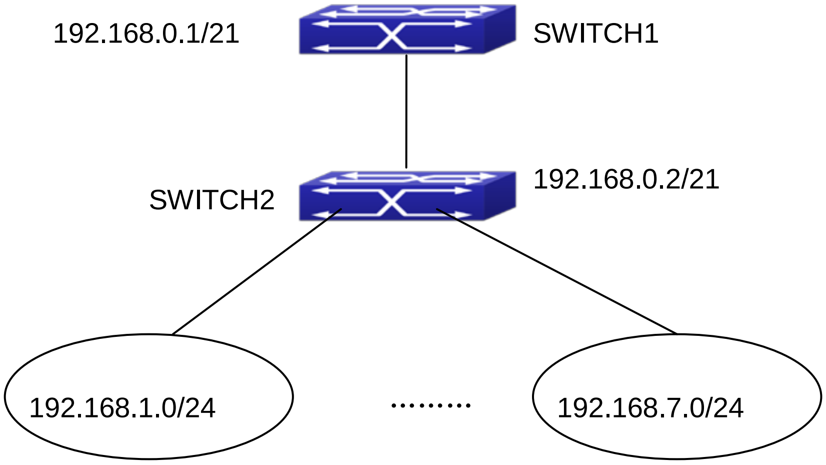

Fig 9-1 IPv4 Black Hole Routing Configuration Example

As it is shown in the figure, in Switch 2, eight in all interfaces are configured as Layer 3 VLAN interfaces for access interfaces. The network addresses are 192.168.1.0/24 ~ 192.268.7.0/24. A default routing is configured on Switch 2 to connect to Switch 1. And a backward default routing is configured on Switch 1 to Switch 2, whose network address is 192.168.0.0/21. Commonly, this configuration will work well. However, if one of the Layer 3 interfaces in Switch 2 goes down, for example, the interface belonged to 192.168.1.0/24. When datagrams arrives at VLAN1 in Switch 2, there will be no routing rules for these datagrams. The switch then will forward these datagrams according to the default routing, back to Switch 1. When Switch 1 receives these datagrams, it will forward them back to Switch 2. Thus, loopback exists. To solve this problem, Black Hole Routing can be introduced on Switch 2.

```
ip route 192.168.0.0/21 null0 50
```

Then Switch 2 will drop the datagrams from interface VLAN1 that match the Black

Hole Routing rule. And loopback routing is prevented.

Configuration steps are listed as below:

```
Switch#config
Switch(config)#ip route 192.168.0.0/21 null0 50
```

Example 2: IPv6 Black Hole Routing function.

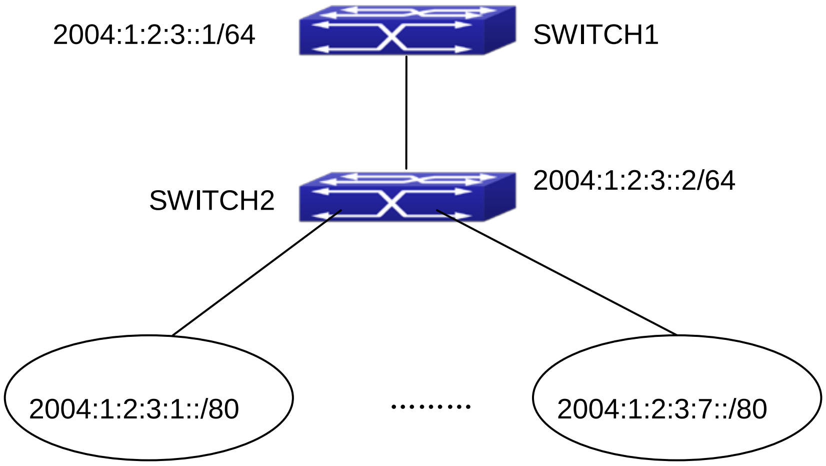

Fig 9-2 IPv6 Black Hole Routing Configuration Example

As it is shown in the figure, in Switch 2, eight in all interfaces are configured as Layer 3 VLAN interfaces for access interfaces. The network addresses are 2004:1:2:3:1/80~2004:1:2:3:7/80. A default routing is configured on Switch 2 to connect to Switch 1. And a backward default routing is configured on Switch 1 to Switch 2, whose network address is 2004:1:2:3::/64. Commonly, this configuration will work well. However, if one of the Layer 3 interfaces in Switch 2 goes down, for example, the interface belonged to 2004:1:2:3:1/80. When datagrams arrives at VLAN1 in Switch 2, there will be no routing rules for these datagrams. The switch then will forward these datagrams according to the default routing, back to Switch 1. When Switch 1 receives these datagrams, it will forward them back to Switch 2. Thus, loopback exists. To solve this problem, Black Hole Routing can be introduced on Switch 2.

```
ipv6 route 2004:1:2:3::/64 null0 50
```

Then Switch 2 will drop the datagrams from interface VLAN1 that match the Black Hole Routing rule. And loopback routing is prevented.

Configuration steps are listed as below:

```
Switch#config
Switch(config)#ipv6 route 2004:1:2:3::/64 null0 50
```

7.5 Black Hole Routing Troubleshooting

When configuring the Black Hole Routing function, the configuration may not work due to some reasons such as incorrect network address mask, and incorrect management distance. Attention should be paid to the following items:

☞ IPv6 should be enabled before IPv6 Black Hole Routing can work.

☞ It is suggested that the length of the network address mask should be longer than that of normal routing configuration, in order to prevent the Black Hole Routing from intervening other routing configuration.

☞ When the network address mask of Black Hole Routing configuration is the same with some other configuration, it is suggested that the distance of Black Hole Routing is set lower.

For problems that cannot be fixed through above methods, please issue the command show ip route distance and show ip route fib, and show l3. And copy and paste the output of the commands, and send to the technical service center of our company.

Chapter 8 ECMP Configuration

8.1 Introduction to ECMP

ECMP (Equal-cost Multi-path Routing) works in the network environment where there are many different links to arrive at the same destination address. If using the traditional routing technique, only a link can be used to send the data packets to the destination address, other links at the backup state or the invalidation state, and it needs some times to process the mutual switchover under the static routing environment. However, ECMP protocol can use multi-links under such network environment, it not only implements the load balance, increases the transport bandwidth, but also can completely backup the data transport of the invalidation links without delay and packet loss.

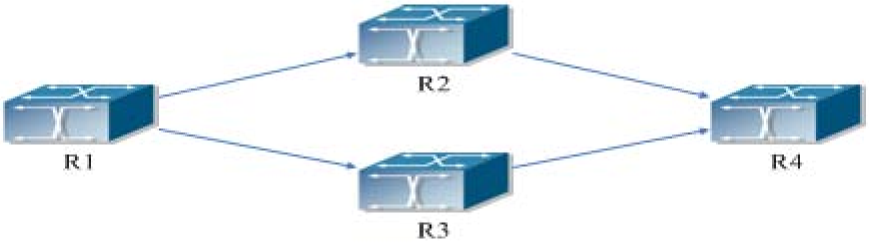

Fig 10-1 the application environment of ECMP

As it is shown in the figure, there are two paths can be selected from R1 to R4, they are R1-R2-R4 and R1-R3-R4. If the route type and the cost are same, then it can forms two routes from R1 to R4, but the next hop is different. If two routes are selected as the best, then they form the equal-cost route.

8.2 ECMP Configuration Task List

1. Configure the max number of equal-cost route

1. Configure the max number of equal-cost route

Command	Explanation
Global mode	

maximum-paths <1-32> **no maximum-paths**	Configure the max number of equal-cost route.

8.3 ECMP Typical Example

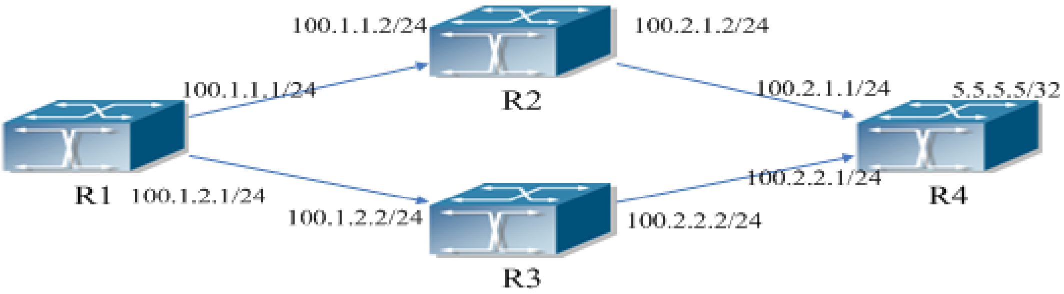

Fig 10-2 the application environment of ECMP

As it is shown in the figure, the R1 connect to R2 and R3 with the interface address 100.1.1.1/24 and 100.1.2.1/24. The R2 and R3 connect to R1 with the interface address 100.1.1.2/24 and 100.1.2.2/24. The R4 connect to R2 and R3 with interface address 100.2.1.1/24 and 100.2.2.1/24. The R2 and R3 connect to R4 with the interface address 100.2.1.2/24, 100.2.2.2/24. The loopback address of R4 is 5.5.5.5/32.

8.3.1 Static Route Implements ECMP

```
R1(config)#ip route 5.5.5.5/32 100.1.1.2
R1(config)#ip route 5.5.5.5/32 100.1.2.2
```

On R1, show ip route, the following is displayed:

```
R1(config)#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
C        1.1.1.1/32 is directly connected, Loopback1    tag:0
S        5.5.5.5/32 [1/0] via 100.1.1.2, Vlan100    tag:0
                    [1/0] via 100.1.2.2, Vlan200    tag:0
C        100.1.1.0/24 is directly connected, Vlan100    tag:0
```

```
C          100.1.2.0/24 is directly connected, Vlan200 tag:0
C          127.0.0.0/8 is directly connected, Loopback    tag:0
                                      Total routes are : 6 item(s)
```

8.3.2 OSPF Implements ECMP

R1 configuration:

```
R1(config)#interface Vlan100
R1(Config-if-Vlan100)# ip address 100.1.1.1 255.255.255.0
R1(config)#interface Vlan200
R1(Config-if-Vlan200)# ip address 100.1.2.1 255.255.255.0
R1(config)#interface loopback 1
R1(Config-if-loopback1)# ip address 1.1.1.1 255.255.255.255
R1(config)#router ospf 1
R1(config-router)# ospf router-id 1.1.1.1
R1(config-router)# network 100.1.1.0/24 area 0
R1(config-router)# network 100.1.2.0/24 area 0
```

R2 configuration:

```
R2(config)#interface Vlan100
R2(Config-if-Vlan100)# ip address 100.1.1.2 255.255.255.0
R2(config)#interface Vlan200
R2(Config-if-Vlan200)# ip address 100.2.1.2 255.255.255.0
R2(config)#interface loopback 1
R2(Config-if-loopback1)# ip address 2.2.2.2 255.255.255.255
R2(config)#router ospf 1
R2(config-router)# ospf router-id 2.2.2.2
R2(config-router)# network 100.1.1.0/24 area 0
R2(config-router)# network 100.2.1.0/24 area 0
```

R3 configuration:

```
R3(config)#interface Vlan100
R3(Config-if-Vlan100)# ip address 100.1.2.2 255.255.255.0
R3(config)#interface Vlan200
R3(Config-if-Vlan200)# ip address 100.2.2.2 255.255.255.0
R3(config)#interface loopback 1
R3(Config-if-loopback1)# ip address 3.3.3.3 255.255.255.255
R3(config)#router ospf 1
R3(config-router)# ospf router-id 3.3.3.3
```

```
R3(config-router)# network 100.1.2.0/24 area 0
R3(config-router)# network 100.2.2.0/24 area 0
```

R4 configuration:

```
R4(config)#interface Vlan100
R4(Config-if-Vlan100)# ip address 100.2.1.1 255.255.255.0
R4(config)#interface Vlan200
R4(Config-if-Vlan200)# ip address 100.2.2.1 255.255.255.0
R4(config)#interface loopback 1
R4(Config-if-loopback1)# ip address 5.5.5.5 255.255.255.255
R4(config)#router ospf 1
R4(config-router)# ospf router-id 4.4.4.4
R4(config-router)# network 100.2.1.0/24 area 0
R4(config-router)# network 100.2.2.0/24 area 0
```

On R1, show ip route, the following is displayed:

```
R1(config)#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
C        1.1.1.1/32 is directly connected, Loopback1   tag:0
O        5.5.5.5/32 [110/3] via 100.1.1.2, Vlan100, 00:00:05   tag:0
                    [110/3] via 100.1.2.2, Vlan200, 00:00:05   tag:0
C        100.1.1.0/24 is directly connected, Vlan100   tag:0
C        100.1.2.0/24 is directly connected, Vlan200   tag:0
O        100.2.1.0/24 [110/2] via 100.1.1.2, Vlan100, 00:02:25   tag:0
O        100.2.2.0/24 [110/2] via 100.1.2.2, Vlan200, 00:02:25   tag:0
C        127.0.0.0/8 is directly connected, Loopback   tag:0
                         Total routes are : 8 item(s)
```