

Routing Protocol Configuration

Table of Contents

Chapter 1 Routing Protocol Overview	1
1.1 IP Routing Protocol.....	1
1.2 Choosing Routing Protocol.....	1
1.2.1 Interior Gateway Router Protocol.....	1
1.2.2 Exterior Gateway Routing Protocol	2
Chapter 2 Static routing Configuration.....	3
2.1 Overview.....	3
2.2 Static Routing Configuration Task List.....	3
2.3 Static Routing Configuration Task	4
2.3.1 Configure the Static Routing	4
2.4 Example of the Static Routing Configuration.....	4
Chapter 3 Configuring RIP.....	5
3.1 Overview.....	5
3.2 RIP Configuration Task List	5
3.3 RIP Configuration Task.....	6
3.3.1 Starting the RIP	6
3.3.2 Allowing the mono-broadcasting updaed and grouped by RIP Router.....	6
3.3.3 Using the Offsets on the Route metric	6
3.3.4 Regulating the Timer	7
3.3.5 Appointing the RIP Version Number.....	7
3.3.6 Enabling the RIP Authentication.....	8
3.3.7 Prohibitting the Route summary.....	8
3.3.8 Prohibitting the Authentication of Source IP Address	9
3.3.9 Maximum Number of Routes.....	9
3.3.10 Activating or Prohibit the Horizontal Split	9
3.3.11 Monitoring and Maintainance of RIP	10
3.4 Example of the RIP Configuration	10
Chapter 4 BEIGRP Configuration.....	12
4.1 Overview.....	12
4.2 BEIGRP Configuration Task List.....	13
4.2.1 Activating BEIGRP Protocol	13
4.2.2 Configuring the Sharable Percentage of Bandwidth	13
4.2.3 Adjusting the Arithmetic Coefficient of BEIGRP Composite Distance	13
4.2.4 Using "Offset" to Adjust the Composite Distance of the Router	14
4.2.5 Turning off Auto-Summary.....	14
4.2.6 Customizing Route Summary.....	15
4.2.7 Redistributing Other Routes into the BEIGRP Process.....	15
4.2.8 Configuring Other Parameters of BEIGRP	16
4.2.9 Monitoring and Maintaining BEIGRP.....	17
4.3 Examples of BEIGRP configuration.....	17

Chapter 5 Configuring OSPF	19
5.1 Overview.....	19
5.2 OSPF Configuration Task List	19
5.3 OSPF Configuration Task.....	20
5.3.1 Starting OSPF	20
5.3.2 Configuring the Interface Parameter of OSPF	20
5.3.3 Configuring OSPF Network Type	21
5.3.4 Configuring One-to-Multiple Broadcast Network.....	22
5.3.5 Configuring Non-Broadcasting Network.....	22
5.3.6 Configure OSPF domain	23
5.3.7 Configuring the NSSA Area of OSPF	24
5.3.8 Configuring Route Summary Within OSPF Domain.....	24
5.3.9 Configuring the Gathering of a Forwarding Router	25
5.3.10 Creating Default Route.....	25
5.3.11 Selecting Router ID Through Loopback Interface	25
5.3.12 Configuring the Management Distance of OSPF	26
5.3.13 Configuring the Route Calculation Timer	26
5.3.14 Configuring the On-Demand Link.....	26
5.3.15 Monitoring and Maintaining OSPF	27
5.4 Examples of OSPF Configuration.....	28
5.4.1 Examples of OSPF one-to-multi Point Configuration	28
5.4.2 Examples of OSPF point to multipoints, non-broadcasting configuration	29
5.4.3 Examples of the configuration of variable length sub-network masks.....	30
5.4.4 Examples of the configuration of OSPF route and route distribution	30
Chapter 6 Configure BGP	38
6.1 Overview.....	38
6.1.1 The BGP implementation of the router.....	38
6.1.2 How does BGP select the path	39
6.2 BGP Configuration Task List.....	39
6.2.1 Basic configuration task list of BGP	39
6.2.2 Advanced BGP configuration tasks list.....	40
6.3 Configure basic BGP features task	40
6.3.1 Configuring Basic BGP Features	40
6.3.2 Configure advanced BGP features.....	45
6.4 Monitoring and Maintaining BGP.....	50
6.4.1 Deleting the BGP Routing Table and the BGP Database.....	50
6.4.2 Displaying the Routing Table and the System Statistics Information	51
6.4.3 Tracking the BGP Information	51
6.5 Examples of BGP configuration.....	52
6.5.1 An example of BGP route-map.....	52
6.5.2 An example of neighbour configuration	53
6.5.3 An example of BGP route filtration based on the neighbor	53
6.5.4 Examples of BGP route filtration based on the interface.....	53
6.5.5 Examples of using prefix list to configure route filtration	54
6.5.6 Example of BGP route aggregation.....	55
6.5.7 Example of BGP route reflector.....	55

6.5.8 Example of BGP confederation	57
6.5.9 Example of route map with BGP group attribute	59
Chapter 7 Configure RSVP	62
7.1 Overview	62
7.2 RSVP Configuration Task List	62
7.3 RSVP Configuration Task	62
7.3.1 Enable a RSVP on a Router	62
7.3.2 Start RSVP in a IP Phone Module Configuration	63
7.3.3 Use RSVP to configure Command	63
7.3.4 Configure TOS and Precedence for RSVP flow	64
7.3.5 Use access-list in RSVP module	64
Chapter 8 Congiuring PBR	65
8.1 Overview	65
8.2 PBR Configuration Task List	65
8.3 PBR Configuration Task	65
8.3.1 Create standard access-list	65
8.3.2 Create route-map	66
8.3.3 Apply route-map on interface	66
8.3.4 Debug PBR	66
8.4 PBR configuion example	66
Chapter 9 Configuring DNS	68
9.1 Overview	68
9.1.1 DNS Application	68
9.1.2 DNS Term	68
9.2 DNS Configuration Task List	69
9.3 DNS Configuration Task	70
9.3.1 Enables DNS-based host name-to-address translation	70
9.3.2 Specify the IP address of a domain name server	70
9.3.3 Set a default domain name	71
9.3.4 Defines a list of domains	71
9.3.5 Defines static host name-to-address mapping	71
9.3.6 Specify times to retry a DNS query	72
9.3.7 Specify timeout waiting for response to a DNS query	72
9.3.8 Delete the mapping of a host name to IP address in cache	72
9.3.9 Specify the IP address of a primary server	72
9.3.10 Enable update function of dynamic DNS	73
9.3.11 Set the period of DNS update	73
9.3.12 Bind the domain name to a IP address or IP address of interface	73
9.3.13 The function of information showing or debug showing	74
9.4 Examples of BGP configuration	74
Chapter 10 PeanutHull Configuration	75
10.1 DHRP Overview	75
10.2 PeanutHull Commands	75
10.2.1 Entering DHRP Configuration State	75
10.2.2 Activating DHRP-Based DNS	75

10.2.3 Designating the Address of the Server.....	76
10.2.4 Designating a Default Domain Name.....	76
10.2.5 Configuring a Connection Port for DHRP Query.....	76
10.2.6 Setting a Username for Registration.....	76
10.2.7 Setting a Password for Registration.....	77
10.2.8 Binding IP Address and Domain Name.....	77
10.2.9 Software Module Display and Debug Display.....	77
10.2.10 PeanutHull Configuration Example.....	77

Chapter 1 Routing Protocol Overview

1.1 IP Routing Protocol

The router of the Company implements multiple IP dynamic routing protocol. They will be introduced in the description of each potocol in this Chapter.

IP routing protocols are classified into two categories: interior gateway router protocol (IGP) and exterior gateway router protocol (EGP). The routers of our Company support RIP, OSPF, BGP and BEIGRP. RIP、OSPF、BGP and BEIGRP can be configured separately on real needs. The router of our company supports simultaneous configuration of multiple routing protocol, including unlimited OSPF (if memory is sufficient) processes, a BGP process, a RIP progress and unlimited BEIGRP processes. Command “redistribute” can be used to inject other router protocols into the database of current routing protocol so that the multiple routing protocols can be associated.

In order to configure IP dynamic routing protocol, the corresponding process shall be started and the corresponding network interfaces and the specific dynamic routing process should be associated, to indicate on which interfaces where the routing process run. To this end, the relevant steps for configuration shall be referred to in the corresponding document of configuration commands.

1.2 Choosing Routing Protocol

The choice of routing protocol is a complicated process. When choosing a routing protocol, the following factors shall be taken into account:

- The size and complexity of the network
- Whether the support for VLSM is needed
- Network traffic
- Security requirement
- Reliability requirement
- Policy
- Others

The subject will not be detailed here. It is noted that the chosen routing protocol shall meet the real condition of network and comply with your requirements.

1.2.1 Interior Gateway Router Protocol

Interior Gateway Routing Protocol is used for the network in a single autonomous system. All the IP interior gateway routing protocol shall be associated with some

specific networks (such as configuring: *network*) when it is launched. Each routing process listens to update messages from other routers on the network and broadcasts its own routing information on the network at the same time. The inside gateway router protocol supported by the router of the Company includes:

- RIP
- OSPF
- BEIGRP

1.2.2 Exterior Gateway Routing Protocol

Exterior gateway routing protocol is used for exchange routing information between different autonomous systems. It is usually required to configure the corresponding neighbors for exchanging routes, the reachable networks and local autonomous system number. The exterior gateway routing protocol supported by the router of our company is BGP.

Chapter 2 Static routing Configuration

2.1 Overview

The chapter illustrates how to configure the Static routing. If you would like to have the detailed description on the Static routing commands in this section, you can refer to the Chapter of " Static routing " in the "Reference for the Network Protocol Commands". If you would like to search the document with other commands, you can use the master index for commands and conduct inline search.

Static routing is a special routing configuration ,and is configured by an administrator. In the network structure is relatively simple network, you only need to configure static routes on network interoperability. Properly setting up and using static routes can improve network performance and be guaranteed bandwidth for important network applications.

The shortcomings of the static route is: It can not automatically adapt to changes in network topology. When network failure or topology change may be the route is unreachable, resulting in network outages, then you must manually by the network administrator to modify the configuration of static routes.

Default route in the router can not find a matching routing table entry when routing:

- If the packet's destination address can not be any entries in the routing table to match, the packet will select the default routing;
- if no default route and destination of the packet is not in the routing table, the packet will be discarded.

Network 0.0.0.0/0.0.0.0 in the form of default route through the static routing configuration, in order to appear in the routing table.

2.2 Static Routing Configuration Task List

If you would like to configure the static routing, the following tasks are necessary.

- configure the relevant physical parameters of the interface
- configure the link layer attributes of the related interface
- configure the IP address of the relevant interface

2.3 Static Routing Configuration Task

2.3.1 Configure the Static Routing

To activate the static routing, the following steps shall be carried out under the global configuration mode:

Command	Purpose
<code>ip route A.B.C.C mask {next-hop interface} [distance] [tag tag] [global] [description]</code>	Configure the Static Routing

2.4 Example of the Static Routing Configuration

Assigned to the network segment 10.0.0.0/8 packets port is interface GigaEthernet3/0, the configuration is as follows:

```
ip route 10.0.0.0 255.0.0.0 gigaEthernet 3/0
```

Chapter 3 Configuring RIP

3.1 Overview

The chapter illustrates how to configure the RIP. If you would like to have the detailed description on the RIP commands in this section, you can refer to the Chapter of "RIP Commands" in the "Reference for the Network Protocol Commands". If you would like to search the document with other commands, you can use the master index for commands and conduct inline search.

The Route Information Protocol (RIP) is a relatively old but still commonly used Interior Gateway Protocol (IGP), which is mainly used in the small-sized network of the same kind.. And RIP is a traditional Distance Vector Routing Protocol, which occurs in the RFC 1058.

RIP exchanges Routing Information through broadcasting UDP Packets. In the Router, the update Route Information will be sent every 30 seconds. In case that no update information from the neighbor router has been received within 180 seconds, the Routes from that neighboring router in the Routing Table will then be labeled as "Unusable". And if there is still no updated information received in the next 120 seconds, these Routes will be deleted from the Routing Table.

The Hop Count is taken by the RIP as a metric to measure different routes. And the Hop Count refers to the number of the passed routers of packets from the Source to the destination. The metric of the Route that is directly connected to the Network is "0", the metric of the Route whose network is not able to reach is "16". As the Route metric used by the RIP is in a relatively small range, it is not applicable to large-scale network. .

If a router has a default route, RIP then will advertises the route to the false Network of 0.0.0.0. In fact, the 0.0.0.0 network does not exist, which is only used for realizing the function of default route in RIP.. If the RIP has learned a default route, or the default gateway is configured in router and configured with default metric, the router will then announce the default network.

The RIP will send the updates to the interface of the appointed network. If the network of the very interface is not appointed, the network then will not be announced in any RIP updating. .

The RIP-2 of our company's router supports Plaintext and MD5 Authentication, Route Summary, CIDR and VLSM.

3.2 RIP Configuration Task List

If you would like to configure the RIP, the following tasks are necessary. While you have to first activate the RIP, the other tasks are optional.

- Starting the RIP
- Enabling Unicasting of RIP route update messages.

- Applying the offset on the route metric
- Regulating the Timer
- Designating the RIP Version Number
- Activating the RIP Authentication
- Prohibiting Route summary
- Prohibiting the Authentication on Source IP Address
- Activating or Prohibit the split-horizon

3.3 RIP Configuration Task

3.3.1 Starting the RIP

To activate the RIP, the following steps shall be carried out under the global configuration mode:

Command	Purpose
router rip	Activate the RIP Routing Process and enter the router configuration mode.
network <i>network-number</i> < <i>network-mask</i> >	Appoint the Network Number relevant to the RIP Routing Process

3.3.2 Allowing the mono-broadcasting updated and grouped by RIP Router

The RIP is a broadcasting-Type Protocol. If you would like the updating of routes to access to the non-broadcasting type network, the router shall be configured so as to enable information exchange. To this end, the following commands shall be used under router configuration mode:

Command	Purpose
neighbor <i>ip-address</i>	Define a neighbor router to exchange with it the Routing Information.

In addition, if you would like to control which interface(s) that can be used to exchange routing information, the command "ip rip passive" can be used to designate an interface or some interfaces prohibiting the sending of the update of routes. If necessary, please refer to the relevant discussion on the route filtration in the "Filtering the Routing Information" in the Chapter of "Protocol-Independent Commands in Configuring IP Router".

3.3.3 Using the Offsets on the Route metric

Offset List is taken to increase an offset on the Input and Output Routes, which have been learned with the RIP. On the other hand, you can use the Access List or the interface to limit the Offset List. In order to increase the Route metric, the following commands should be executed in the router configuration mode:

Command	Purpose
offset-list { <i>[[interface-type number]]* </i> } {in out} <i>access-list-name</i> offset	Increase an offset on the route metric.

3.3.4 Regulating the Timer

Routing protocols use several timers to determine the frequency for sending the updating of routes, how long the router will become invalid and other parameters. You can regulate these timers so as to make the performance of the Routing Protocols more suitable to the requirements of the network.

It is also possible to regulate the Route Protocol to accelerate the Convergence Time of all kinds of the IP Routing computation, to quickly backup to the redundant router so as to minimize the time of quick recovery. To regulate the Timer, the following commands should be used under router configuration model.

Command	Purpose
timers holddown <i>value</i>	Regulating the time (Unit: Second) it take to delete certain route from the Routing Table
timers expire <i>value</i>	Regulating the time (Unit: Second) that the router is announced to be invalid.
timers update <i>value</i>	Regulating the frequency for sending the updating of the Router (the time interval between sedning of the updating of routing, (unit: Second))

3.3.5 Appointing the RIP Version Number

The RIP-2 of our company's router supports Authentication, Password Management, Route summary, CIDR and VLSM.

Under the default circumstance, the router can receive the updates of RIPv1 and RIPv2, while it can only send the updates of RIP-1. By configuration, the router can be set to receive and send the updates of RIPv1 only, or receive and send the updates of RIPv2 only. For this purpose, the following commands should be taken in the router configuration mode:

Command	Purpose
version {1 2}	Configure the router to send and receive the updates of RIPv1 or RIPv2 only.

The above tasks are controlling the default behavior of the RIP. And you can also configure a certain interface to change this default behavior. In order to control the interface to send the RIP-1 updates or the RIP-2 updates, the following commands shall be used under interface configuration mode.

Command	Purpose
ip rip send version 1	Configure the interface to send the updates of RIP-1 only.
ip rip send version 2	Configure the interface to send the updates of RIP-2 only.
ip rip send version compatibility	Send by broadcasting t the Updating of RIP-2.message.

At the same time, to control the interface to receive the updates of RIP-1 and RIP-2, the following commands shall be used under the interface configuration mode:

Command	Purpose
ip rip receive version 1	Configure the interface to receive the updates of RIP-1 only.
ip rip receive version 2	Configure the interface to receive the updates of RIP-2 only.
ip rip receive version 1 2	Configure the interface to receive the updates of RIP-1 and RIP-2 only.

3.3.6 Enabling the RIP Authentication

RIP-1 does not support Authentication. If you would like to send and receive the updates of RIP-2, you can activate the function of RIP Authentication on the interface.

On the activated interface of RIP, we support 2 kinds of Authentication Modes: Plaintext Authentication and MD5 Authentication. the Plaintext authentication is used in each subgroups of BIP-2 under default status.

Notes:

Regarding the safety, please don't use Plaintext Authentication in the groups of RIP, because the unencrypted authentication key would be sent to each update of the RIP-2. If the safety is not a big question, (in case that it is guaranteed that the wrongly configured host can not take part in the route) the Plaintext Authentication can be used.

To configure the RIP Plaintext Authentication, the following steps should be taken under interface configuration mode:

Command	Purpose
ip rip authentication simple	Activate the RIP Authentication.
ip rip password <i>[string]</i>	Configure the Plaintext Authentication key for the interface.

In order to configure the MD5 Authentication, the steps below should be taken under interface configuration mode:

Command	Purpose
ip rip authentication <i>message-digest</i>	Activate the RIP MD5 Authentication
ip rip message-digest-key <i>[key-ID] md5</i> <i>[key]</i>	Configure the MD5 Authentication key for the interface

3.3.7 Prohibiting the Route summary

Under the default circumstance, the RIP-2 supports the automatic route summary, summarizing the RIP-2 Routes when crossing the boundary of the classified network. And the RIP-1 Automatic Route Gathering Function is always activated.

If there is a separated Sub-net, it is necessary to prohibit the Route summary to declare this Sub-net. If the Route Gathering is prohibited, when crossing the boundary of the classified network, the router will then send the route information of the sub-net and the host. Under the router configuration mode, the following command should be taken to prohibit the automatic gathering.

Command	Purpose
no auto-summary	Prohibit the Automatic summary

3.3.8 Prohibiting the Authentication of Source IP Address

Under the default circumstance, the router will authenticate the Authenticable Source IP Address of the received route update. If this address is illegal, the router update will then be rejected.

If you have a router in hope to receive the updating from it, but you have not configured the corresponding "network" or "neighbor" on the receiver, the function should be therefore prohibited. However in the common practice, this command is not recommended to use. Under router configuration mode, the following commands will prohibit the default function of authenticating the source IP address in incoming route updates.

Command	Purpose
no validate-update-source	Prohibit to authenticate the Source IP Address of the incoming RIP Router Updating.

3.3.9 Maximum Number of Routes

By default, the local RIP routing table can contain up to 1024 routes. When the number of routes in the routing table exceeds the maximum number, the route will not be added to the routing table any more. Meanwhile, the user will be notified that the number of routes in the routing table has reached the maximum number. Run the commands in the following table to configure the maximum number of the routes in the local RIP routing table in router configuration mode.

Command	Purpose
maximum-count <i>number</i>	Configures the maximum number of routes for the local RIP routing table.
no maximum-count	Resumes the default maximum number of the routes in the local RIP routing table.

3.3.10 Activating or Prohibit the Horizontal Split

Normally, the router, which is connected with IP Network and using the Distance Vector Routing Protocol, takes split-horizon to lower the possibility of route loops. The Split-Horizon prevents the announcements of route information to the receiving interface of this route information. In this way, communication within several routers (especially when the loop breaks) will be optimized. However, to Non-broadcasting Network (such as FR), things are not so easy. And maybe you have to prohibit the Horizontal Split.

If an interface has been configured with a supplementary IP Address and the Horizontal Split has been activated, the update-Source IP Address of the route update may not include every secondary IP address. The source IP address of one route update includes only one Network Number (unless the split-horizon is Prohibited).

In order to activate or prohibit the Horizontal Split, the following commands should be taken under interface configuration mode:

Command	Purpose
ip rip split-horizon	Activate the Split- Horizon
no ip rip split-horizon	Prohibit the Split- Horizon

Under the default circumstance, for the point to Point Interface, the Split-Horizon is activated; For Point-to multiple point Interface, the Split-Horizon is prohibited.

Please refer to the specific example of using Split-Horizon in the "Examples of Split-Horizon" in Section of this Chapter.

Notes:

Commonly, it is suggested that the default state remain unchanged unless you are sure that your application can't declare the route correctly until you change its state. Always remember: if the Split-Horizon is prohibited on a serial interface (and the interface is connected with a Packet-switched Network), you have to prohibit Split-Horizon to all routers in any relevant Multicast Group on that Network.

3.3.11 Monitoring and Maintenance of RIP

With the RIP monitored and maintained, the Network Statistics can be displayed, such as: RIP protocol Parameter Configuration, Network utilization, Real-time Tracing of Network Communication and so on. Such information can help you judge the use of Network Resource and further solve the network problems and know the reachability of network nodes .

The following commands can be used to display the statistics information of all kinds of routes under management statistics:

Command	Purpose
show ip rip	Display the present Status of RIP
show ip rip database	Display all routes of RIP
Show ip rip protocol	Display all the relevant information of RIP Protocol

Under the management mode, the following commands shall be used to trace route protocol information.

Command	Purpose
Debug ip rip database	Trace the procedure information of RIP Routing such as Insertion into the Routing Table, Deletion from the Routing Table, Changes of Routes and so on.
Debug ip rip protocol	Trace the RIP protocol messages.

3.4 Example of the RIP Configuration

Examples of the RIP Configuration is included in this section:

RouterA

```
interface ethernet 1/1
ip address 192.168.20.81 255.255.255.0
```

```
!  
interface loopback 0  
ip address 10.1.1.1 255.0.0.0  
!  
router rip  
network 192.168.20.0  
network 10.0.0.0  
!
```

RouterB

```
interface ethernet 1/1  
ip address 192.168.20.82 255.255.255.0  
interface loopback 0  
ip address 20.1.1.1 255.0.0.0  
!  
router rip  
network 192.168.20.0  
network 20.0.0.0  
!
```


Chapter 4 BEIGRP Configuration

This chapter will detail the configuration process of BEIGRP dynamic routing protocol.

4.1 Overview

Brief introduction of BEIGRP routing protocol.

The technology used by BEIGRP is similar to distance vector routing protocol:

- The router only makes routing decisions with the information provided by directly connected neighbours;
- The router only provides the routing information it uses to the directly connected neighbors. But, BEIGRP has some main differences with distance vector routing protocol, which entitles it to have more advantages:
- BEIGRP saves all routes from all neighbours in the topology table, not just the best routes so far;
- BEIGRP can make query to the neighbors when it is unable to access the destination and no alternative routes are available, so, the convergence speed of BEIGRP can compete with the best link-state protocol.

The introduction of DUAL---Diffused Update Algorithm is vital for BEIGRP's superiority to other traditional distance vector routing protocol. It always works actively and queries the neighbours when it is unable to access the destination and there is no alternative routes (feasible replacement). As the convergence process is active rather than negative (negatively waiting for the timeout of the routers), so the convergence speed of BEIGRP is very quick.

BEIGRP is a specific routing protocol designed to adapt to the requirements of EIGRP and is directly based on IP. It meets the following requirements of BEIGRP:

- Dynamically discover new neighbor and the disappearance of old neighbors through "Hello" message;
- So the transfer of data are all reliable;
- The transfer protocol permits unicast and multicast data transfer;
- The transfer protocol itself can adapt to the change of network condition and neighbor responding;
- BEIGRP can limit the percentage of its occupation of the bandwidth according to the requirements

4.2 BEIGRP Configuration Task List

To complete the configuration of BEIGRP the following tasks are required to be done, among them, the activation of BEIGRP is necessary while others can be decided according to the requirement.

- Activate BEIGRP protocol
- Configure the sharable percentage of bandwidth
- Adjust the arithmetic coefficient of BEIGRP composite distance
- Using “offset” to adjust the composite distance of the router
- Turn off auto-summary
- Customize route summary
- Configure other parameters of BEIGRP
- The supervision and maintenance of BEIGRP

4.2.1 Activating BEIGRP Protocol

In order to create a BEIGRP process, it is required to execute the following commands:

Command	Purpose
router beigrp <i>as-number</i>	Add a BEIGRP process under global configuration mode
network <i>network-number</i> <i>network-mask</i>	Add addresses to this BEIGRP process under router configuration mode

After finishing the above configuration, BEIGRP will start to run on all interfaces belonging to this address, discovers new neighbours through “Hello” and carries out initial routing interaction through “update”.

4.2.2 Configuring the Sharable Percentage of Bandwidth

Under default circumstances, BEIGRP can occupy 50% of the bandwidth at most. You may wish to change this default value in order to guarantee the normal interaction of other data, or wishes to adjust the actually usable bandwidth of BEIGRP through the command when the interface is configured with a bandwidth not fit for actual situation. Under these conditions, you can use the following commands under interface configuration mode:

Command	Purpose
ip beigrp bandwidth-percent <i>percent</i>	Configure the maximum percentage of BEIGRP messages' occupation of the bandwidth

4.2.3 Adjusting the Arithmetic Coefficient of BEIGRP Composite Distance

Under certain situations, the arithmetic co-efficient of BEIGRP composite distance may need to be adjusted, and finally influences the routing policy of the router. Although the

default arithmetic co-efficient of BEIGRP can satisfy most networks, but it may still need to be adjusted under some particular conditions. But this adjust may bring great change to the whole network, so it must be performed by the most experienced engineers.

Use the following command under router configuration mode:

Command	Purpose
metric weights <i>k1 k2 k3 k4 k5</i>	Adjust the arithmetic co-efficient of BEIGRP composite distance.

4.2.4 Using "Offset" to Adjust the Composite Distance of the Router

We use offset list to purposely add all incoming and outgoing routes according to the requirement, or the composite distance of certain routes meeting the requirements. The aim of this approach is to finally influence the routing result of the router, and meets our expected result. During the process of configuration, the user can designate access list or application interface in the offset list selectively and according to your requirements, in order to more clearly notify which routes to carry out operations to increase offset. Looking at the following command:

Command	Purpose
offset {type number *} {in out} access-list-name offset	Apply an offset list.

4.2.5 Turning off Auto-Summary

The auto-summary of BEIGRP is different with other dynamic routing protocols, and it obeys the following rules:

- When a BEIGRP process defines several networks, as long as there is at least one sub-net of this networks exists in the BEIGRP topology list, it creates the summary route of the defined network.
- The established summary route points to interface Null0, and has the distance as the minimum distance of all the sub-nets of the network included in the route. The summary route is also injected into the main IP routing table with the management distance of 5 (unable to be configured)
- When sending update to the neighbors in different main IP network, the sub-nets summarized by rule1 and rule 2 is cancelled and only a summary route will be sent.
- Do not perform summary towards the sub-nets of any networks not listed in BEIGRP process definition.

Under certain network situations, you may wish to report every detailed route to the neighbor, and you may use the following commands:

Command	Purpose
no auto-summary	Turn off auto-summary of the route.

4.2.6 Customizing Route Summary

When auto-summary cannot meet the requirements, you may configure route summary on each interface running BEIGRP and designate the destination addresses that need performing summary. The interfaces configured for summary will not send the concrete update information of the sub -nets belonging this summary address, while other interfaces are not affected.

Here, the summary operation follows the following rules:

- After an interface is configured for summary, it creates the summary route of the defined network as long as this network has at least one sub-net in BEIGRP topology list;
- The summary route points to interface Null0, and has the distance as the minimum distance of all the sub-nets of the network included in the route. The summary route is also injected into the main IP routing table with the management distance of 5 (unable to be configured)
- When sending route update on the interface configured with summary range, the concrete route belonging to the summary address will be canceled. The update to other interfaces are not affected.

Command	Purpose
ip beigrp <i>summary-address</i> <i>as-number address mask</i>	Configure route summary on an interface.

4.2.7 Redistributing Other Routes into the BEIGRP Process

The **redistribute** operation follows the below rules:

- It isn't have to configure the command "default-metric" when redistribute the static routes and the connected routes. The related parameter(such as: bandwidth, delay, reliability , load and MTU) is attained from the related interface.
- It isn't necessary to configure the command "default-metric" when redistribute the routes of other beigrp process. The related parameter is attained from the BEIGRP process redistributed.
- It is necessary to configure the command "default-metric" when redistribute the routes of others protocol (such as: rip, ospf). The related parameter is validated by the configuration of "default-metric". If we redistribute the routes of these types without the command "default-metric", the redistribution doesn't work.

In a router running the BEIGRP protocol and the RIP protocol, the following commands must be configured when we need obtain the routes from RIP protocol to BEIGRP protocol.

Command	Purpose
default-metric bandwidth delay reliability loading mtu	configure the default parameter of redistribute
redistribute protocol [process] [route-map name]	redistribute the routes to BEIGRP protocol.

4.2.8 Configuring Other Parameters of BEIGRP

In order to adapt to different network environments, and to make BEIGRP be more effectively and fully functions, we may need to adjust the following parameters:

- Adjust the time interval of BEIGRP to send “hello” messages and the timeout death time of the neighbours
- Turn off split-horizon

1. Adjusting the time interval of BEIGRP to send "hello" messages and the timeout death time of the neighbors

BEIGRP hello protocol achieves 3 objectives to enable correct BEIGRP operation:

- It discovers accessible new neighbors. The discovery is automatic and requires no manual configuration;
- It checks neighbors' configuration and only permits communication with the neighbours configured with compatible mode.
- It continues to maintain the availability of the neighbors and detects the disappearance of the neighbors.

The router sends “hello” multicast packet on all interfaces running BEIGRP. All routers support BEIGRP receive these multicast groups, so that it can discover all neighbours.

“Hello” protocol uses two timers to detect the disappearance of the neighbours: hello interval defines the frequency of sending BEIGRP hello messages on the interface of the router, while hold timer defines the interval of time the router has to wait for the communication data from the designated neighbor before the declaration of the neighbour's death. We ordered that every time it receives BEIGRP packet from the neighbour router, it resets the hold timer.

Different network type or network bandwidth will use different default value of hello timer:

Interface type encapsulation		Hello timer (second)	Hold timer (second)
LAN interface	Any	5	15
WAN interface	HDLC or PPP	5	15
	NBMA interface, bandwidth<=T1	60	180
	NBMA interface, bandwidth>T1	5	15
	The point-to-point sub-interface of NBMA interface	5	15

The difference of the default value of the timer in Hello protocol may induce the result that the BEIGRP neighbours connected to different IP sub-network use different hello and hold timer. To resolve the problem, the hello packet of every router designates its own hold timer, every BEIGRP router uses neighbour's the designated hold timer of the hello group to decide the timeout of this neighbour. Here, it can enable the

appearance of different neighbour error detection timers in the different stands of the same WAN nephogram. But under some particular situation, the default value of the timer cannot be met, so if you want to adjust the time interval of sending hello messages, use the following command:

Command	Purpose
ip beigrp hello-interval <i>seconds</i>	Adjust the time interval of sending hello message from this interface

If you wish to adjust the timeout timer of the neighbour, use the following command:

Command	Purpose
ip beigrp hold-time <i>seconds</i>	Adjust the timeout death time of the neighbor

2. Shutting down the horizon split

Commonly, we wish to use split-horizon. It will prevent the routing information from one interface to be broadcasted back to the same interface, so as to avoid route loop. But under certain circumstances, this is not the optimized choice, and then we can use the following command to disable split-horizon:

Command	Purpose
no ip beigrp split-horizon	Turn off horizontal split

4.2.9 Monitoring and Maintaining BEIGRP

To clear the neighbourship with all neighbours, use the following command:

Command	Purpose
clear ip beigrp neighbors [<i>as-number</i> <i>interface</i>]	To clear the neighborhood with all neighbours

In order to show various statistics information of BEIGRP, execute the following commands:

Command	Purpose
show ip beigrp interfaces [<i>interface</i>] [<i>as-number</i>]	show interface information
show ip beigrp neighbors [<i>as-number</i> <i>interface</i>]	show neighbor information
show ip beigrp topology [<i>as-number</i> <i>all-link</i> <i>summary</i> <i>active</i>]	show topology information

4.3 Examples of BEIGRP configuration

In the following example, the interface ethernet1/1 is configured to send a summary route to address 10.0.0.0/8, and all subnets routes belonging to this address will not be advertised to the neighbors from the interface. Meanwhile, we turn off the auto-summary of BEIGRP process.

```
interface Ethernet 1/1
ip beigrp summary-address 1 10.0.0.0 255.0.0.0
```

```
!  
router beigrp 1  
network 172.16.0.0 255.255.0.0  
no auto-summary
```

Chapter 5 Configuring OSPF

5.1 Overview

The OSPF Configuration will be introduced in this chapter. For more specific detailed information about all the OSPF commands, please refer to the relevant sections about OSPF Commanders in the Reference for Network Protocol Configuration.

OSPF is an IGP Route protocol developed by the OSPF Working Group of IETF. The OSPF, which is designed for the IP Network, supports the IP Sub-network and the External Route Information Label and at the same time allows the authentication of message and supports the IP Multicast.

The Implementation of OSPF of our company complies with the OSPF V2 specification (Refers to RFC2328). Some key features in the implementation are listed in the following:

- Stub Area--Supporting the Stub Area
- Route redistribution--Any route, formed by and learned a routing protocol, can always be redistributed to the other route protocol Domain. Within the autonomous System, it means that OSPF can input the route learned by the RIP. And the routes learned by OSPF can also be redistributed to the RIP. Between autonomous Systems, OSPF can input the routes learned by BGP; and OSPF routes can also be injected to BGP.
- Authentication--The Plaintext and MD5 Authentications are supported between the neighboring routers within a area.
- Router Interface Parameters--The configurable Parameters include: Outgoing Cost, Retransmission Interval, Interface Transmission Delay, router Priority, Judgement on the router Switching-off Interval, the Interval of Hello Message and the Authentication Password.
- Virtue Link--Supporting the Virtue Link
- NSSA area--Refer to RFC 1587
- OSPF---RFC 1793 on the virtual circuit.

5.2 OSPF Configuration Test List

OSPF requires to exchange routing data among all routers, ABR and ASBR in a area. In order to simplify the configuration, you may let them all work under default parameters without authentication, etc... but if you want to alter some parameters, you should guarantee the identity of the parameters on all routers.

In order to configure OSPF complete the following tasks. Besides the necessity of activating OSPF, other configurations are all optional.

- Start OSPF
- Configure the interface parameter of OSPF
- OSPF configuration on different physical networks
- Configure route summary within OSPF domain
- Configure the gathering of a forward router
- Create default route
- Select router ID through LOOPBACK interface
- Configure the management distance of OSPF
- Configure the route calculating timer
- The supervision and maintenance of OSPF

In addition to that, about configuring route redistribution, please refer to the related content about "Route Redistribution" of "Protocol-independent Feather Configurations of IP routing Protocol".

5.3 OSPF Configuration Tast

5.3.1 Starting OSPF

Like other routing protocols, activating OSPF demands creating OSPF routing process, allocation of an IP address range related to the executing process, allocation of an area ID related to IP address range. Under the global configuration mode, use the following commands:

Command	Purpose
router ospf <i>process-id</i>	This command activates OSPF routing protocol, and enters router configuration mode.
network <i>address mask area area-id</i>	This command configures the interface(s) running OSPF and the area ID of the interface

5.3.2 Configuring the Interface Parameter of OSPF

During the implementation of OSPF, it is permitted to change the OSPF parameters related to interface according to the requirement. There is no need to change any parameter, but you should guarantee the identity of certain parameters on all routers on connected network.

Under interface configuration mode, use the following commands to configure interface parameters:

Command	Purpose
ip ospf cost <i>cost</i>	Configure the metric of OSPF interface to forward packets.
ip ospf retransmit-interval <i>seconds</i>	The seconds taken to retransmit LSA between the neighbors belonging to the same OSPF interface.
ip ospf transmit-delay <i>seconds</i>	Configure the estimated time to transmit LSA on an OSPF interface (second as the unit).
ip ospf priority <i>number</i>	Configure the priority of router to become the DR router
ip ospf hello-interval <i>seconds</i>	Configure the time interval to send hello packet on OSPF interface.
ip ospf dead-interval <i>seconds</i>	If the router does not receive "hello" packet from the neighbor within the time interval defined, it considers the neighbor router to be turned off.
ip ospf authentication-key <i>key</i>	It is an authentication password of the adjacent router in an address, which uses simple password authentication of OSPF.
ip ospf message-digest-key <i>keyid</i> md5 <i>key</i>	Demand OSPF to use MD5 authentication.
ip ospf passive	Do not send "hello" message on the interface.

5.3.3 Configuring OSPF Network Type

No matter what the physical media type of the network is, you can configure your network to be broadcasting network or non-broadcasting, multi-access network. Using this feature, you can flexibly configure the network, you can configure the physical broadcasting network to be a non-broadcasting, multi-access network; you can also configure non-broadcasting network (X.25, Frame Relay, and SMDS) to be broadcasting network. This feature also reduces the configuration of the neighbors, for detailed information, please refer to the related content of non-broadcasting network's configuration of OSPF.

Configure non-broadcasting, multi-access network to be broadcasting network or non-broadcasting network, that is, to suppose there exists virtual links from every router to other routers, or suppose they consist of a full-mesh network. Because of the restriction of expenses, it is usually not practical; or a partially full-mesh network. Under this situation, you can configure a point-to-multiple point network. Routers not adjacent to each other can exchange routing information through virtual links.

OSPF point-to-multiple point interface can be defined as several point-to-point network interfaces, which creates multiple host routes. OSPF point-to-multiple point network has the following advantages over non-broadcasting, multi-access network and point-to-point network:

Point-to-multiple point network is easy to configure, it does not demand neighbor configuration command, it only uses one IP and will not produce DR.

Because it does not need to full-mesh network topology, it costs less.

It is more reliable. Even when virtual links fail, it can still maintain the connection.

Under interface configuration mode, configure OSPF network type with the following command:

Command	Purpose
ip ospf network {broadcast non-broadcast {point-to-multipoint [non-broadcast]}}	This command configures the network type of OSPF.

At the end of this chapter, you can see an example of the configuration of OSPF point-to-multiple point network.

5.3.4 Configuring One-to-Multiple Broadcast Network

You do not need to describe the neighbor relations in point-to-multiple point network and broadcasting network. But you can use command “neighbor” to describe the priority of a certain neighbor.

Before using this command, some OSPF point-to-multiple point protocol traffic is multicast traffic. So for point-to-multiple point interface, command “neighbor” is not needed. Packet “hello”, update packet and confirmation packet are all transmitted through broadcasting form, especially, multicast “hello” packet can dynamically discover all neighbors.

In point-to-multiple point network, the router supposes that all neighbors have the same metric. This value can be configured through command “ip ospf cost”. In fact, the bandwidth of every neighbor is different, so the value should be different. This feature only applies to point-to-multiple point interface.

Using the following command to configure the interface to be point-to-multipoint interface and allocate a metric for each neighbor:

Command	Purpose
ip ospf network point-to-multipoint	On broadcasting media, configure the interface to be a point-to-multiple point network
Exit	Return to global configuration mode
router ospf <i>process-id</i>	Configure an OSPF router process and enter into router configuration mode.
neighbor <i>ip-address cost number</i>	Designate a neighbor and allocate a metric for it

For each neighbor wishing to designate its metric, repeat step 4. Otherwise use the value designated by command “ip ospf cost”.

5.3.5 Configuring Non-Broadcasting Network

Because there are many routers in the OSPF network, so there must be one DR elected for the network. If the broadcasting ability is not configured, it is requested to perform parameter configuration for the selection process.

These parameters only carry out configuration on the routers that are eligible to become DR or BDR.

Under router configuration mode, use the following command to configure routers of non-broadcasting network which are mutually related:

Command	Purpose
neighbor <i>ip-address</i> [priority <i>number</i>] [poll-interval <i>seconds</i>]	Configure the router connected to the non-broadcasting network

You can designate the following parameters for a neighbor router:

- The precedence of neighbor router.
- Non-broadcasting poll interval.
- Interface accessible to the neighbor

In point to multiple point, non-broadcasting network, you can use command “neighbor” to designate neighbor relation. Allocate an optional priority.

In the previous software versions, some users configure point to multipoint connections on non-broadcasting media (IP over ATM), so the router cannot dynamically discover its neighbor router. This feature permits the usage of command “neighbor” on point to multipoint interface.

In a point to multipoint network, the router supposes all neighbors have the same metric. This value can be configured through the command “ip ospf cost”. In fact, as the bandwidth of each neighbor is different, the value should also be different. This feature only applies to point to multiple point interfaces.

Under interface configuration mode, use the following command to configure point to multiple point interfaces on media that do not support broadcasting.

Command	Purpose
ip ospf network point-to-multipoint non-broadcast	Configure point to multiple point interface on non-broadcasting media
exit	Enter into global configuration mode.
router ospf <i>process-id</i>	Create a OSPF routing process and enter into router configuration mode
neighbor <i>ip-address</i> [cost <i>number</i>]	Designate an OSPF neighbor and allocate a metric for it

Repeat step 4 for each neighbor.

5.3.6 Configure OSPF domain

Configurable area parameters include: authentication, designating Stub area, designating metric for default summary route. Authentication adopts protection based on passwords.

Stub areas are those that don't distribute external routes in them. Instead, ABR generates a default external route to enter the stub area, enable it to enter the external

network of the autonomous system. In order to utilize the features OSPF Stub support, you should use default route in the Stub area. In order to additionally reduce LSA number sent into the Stub area, you can prohibit gathering ABR to reduce the sending of summary LSA (type3) entered into the Stub area.

Under router configuration mode, use the following command to define the area parameter:

Command	Purpose
area area-id authentication simple	Activates OSPF area authentication
area area-id authentication message-digest	Enables OSPF to use MD5 for authentication
area area-id stub [no-summary]	Defines a Stub area
area area-id default-cost cost	Sets metric for default route in Stub area.

5.3.7 Configuring the NSSA Area of OSPF

The NSSA area is similar to the STUB area. However, the NSSA area allows external routes to be entered. The route summary and packet filtration are also supported during transmission. If ISP requires to use the remote network with different routing protocols, the NSSA can simplify management.

The enterprise-core boundary router cannot run in the STUB area of OSPF if NSSA is not applied. That's because the routes of the remote network cannot be forwarded to the STUB area. The simple routing protocols such as RIP can be advertised, but two kinds of routing protocols need be maintained. NSSA can put the center router and the remote router in the same NSSA area and OSPF thus be applied to the remote network.

When the NSSA area is used, note that the route generated by the ABR router can enter the NSSA area once NSSA is configured. Each router in the same area must admit that they are in the NSSA area, or different routers cannot communicate with each other. The displayed release must be used on ABR to avoid packet transmission confusement of the router.

Run the following command in router configuration mode to set the NSSA area of OSPF:

Command	Purpose
Area area-id nssa [no-redistribution][no-summary][default-information -originate]	Configures the OSPF NSSA area.

5.3.8 Configuring Route Summary Within OSPF Domain

This feature enables ABR to broadcast a summary route to other areas. In OSPF, ABR will broadcast every network to other areas. If the network number can be allocated according to a certain method, and be continuous, you can configure ABR to broadcast a summary route to other areas. A summary route can cover all networks within a certain range.

Under router configuration mode, use the following commands to define the address ranges:

Command	Purpose
area <i>area-id range address mask</i>	Define the address range for route summary.

5.3.9 Configuring the Gathering of a Forwarding Router

When distributing routes from other router areas to OSPF router area, each performs independent broadcasting in the form of external LSA. But you can configure the router to broadcast a route, which covers a certain address range. This method can reduce the size of OSPF link status database.

Under the router configuration mode, use the following command to configure gathering the router:

Command	Purpose
summary-address <i>prefix mask [not advertise]</i>	Describe the address and mask that cover the distribution route, only one gathering route is broadcasted.

5.3.10 Creating Default Route

You can demand ASBR to create a default route to enter into the OSPF route area. Whenever you configure a router distribute route to enter into OSPF domain, this router automatically changes into ASBR. But, ASBR does not create default route entering into OSPF route area by default.

Under router configuration mode, use the following command to force ASBR to create a default route:

Command	Purpose
default-information originate [always] [route-map map-name]	Force ASBR to create a default route entering into OSPF route area.

5.3.11 Selecting Router ID Through Loopback Interface

OSPF uses the biggest IP address configured on the interface as its router ID. If the interface connected to this IP address changes into DOWN state, or this IP address is deleted, OSPF process will restart to calculate new router ID and resend routing information from all interfaces.

If one loopback interface is configured with IP address, then the router uses that IP address as its router ID, since loopback interface will never become Down, and all these make the routing table more stable.

The router preferably uses LOOPBACK interface as the router ID, meanwhile selects the biggest IP address among all loopback interfaces as the router ID. If there is no loopback interface, then uses the biggest IP address of the router. You cannot designate OSPF to use any special interface.

Under global mode, use the following command, to configure IP Loopback interface.

Command	Purpose
interface loopback 0	Create a loopback interface and enter into

	interface configuration mode.
ip address <i>ip-address mask</i>	Allocate an IP address for the interface.

5.3.12 Configuring the Management Distance of OSPF

Management distance is defined as the reliability level of routing information source, such as a router or a group of routers. Generally speaking, management distance is an integer between 0-255, the higher the value is, the lower the reliability level it is. If the management distance is 255, then the route information source will not be trusted and should be neglected.

OSPF uses 3 different types of management distances: inter-domain, inner-domain and exterior. The route within an area is inner-domain; the route to other areas is inter-domain; the route distributed from other route protocol domains is exterior. The default value of every kind of route is 110.

Under router configuration mode, use the following command to configure the distance value of OSPF:

Command	Purpose
distance ospf [<i>intra-area dist1</i>] [<i>inter-area dist2</i>] [<i>external dist3</i>]	Change the management distance value of OSPF inner-domain, inter-domain and exterior route.

5.3.13 Configuring the Route Calculation Timer

You can configure the time delay between the time when OSPF receives topologic change information and when it starts to calculate SPF. You can also configure the interval between two consecutive calculations of SPF. Under router configuration mode, use the following command to configure:

Command	Purpose
timers delay <i>delaytime</i>	Set the time delay in the route calculation in a area.
timers hold <i>holdtime</i>	Set the minimum time interval of route calculation in a area.

5.3.14 Configuring the On-Demand Link

OSPF over on-demand circuits is an upgrade of OSPF, which enables the protocol more efficient in case of on-demand dialing network surfing. The OSPF protocol is to regularly exchange the HELLO packets and the link-state broadcast-refresh packets among the connected routers after the connection is first established or the information contained in the packet is changed, which means that the minimum spanning tree will be recalculated and the packet will be transmitted only when the topology is really changed.

If the point-to-point connection is among the routers, the configuration should be conducted on one terminal. Of course, the router on the other terminal must support this trait. If the point-to-multipoint connection is among the routers, the configuration must be conducted on the multipoint terminal.

It is recommended to configure the on-demand dialing in the STUB area. If this attribute is configured on each router in the STUB area, the routers outside the STUB area are allowed not to support the on-demand dialing. If on-demand dialing is configured in a standard area, other standard areas must support this trait, because the second kind of external link-state broadcast packets will be broadcast in all areas.

When the trait is configured on the broadcast-based network, the link-state broadcast packets can be restraint, while the HELLO packets cannot be restraint. That's because the HELLO packets are used to maintain the neighborhood relation and to select DR.

Run the following command in interface mode:

Command	Purpose
ip ospf demand-circuit	Configures OSPF on-demand dialing.

5.3.15 Monitoring and Maintaining OSPF

It can display the statistic information of the network, such as: the statistics about the content of IP routing Table, cache and database and etc... This information can help you to judge the utilization of the network resource, and solve the network problem. You can understand the availability of the network nodes, discover the route the network data packet goes through the network.

Use the following commands to display various routing statistics:

Command	Purpose
show ip ospf [<i>process-id</i>]	Display the general information about OSPF routing process.
show ip ospf <i>process-id</i> [database [<i>router network summary asbr-summary external database-summary</i>]][<i>link-state-id</i>][self-originate]	Display the related information about OSPF database.
show ip ospf border-routers	Display the internal routing table entry of ABR and ASBR.
show ip ospf interface	Display the information about OSPF interface.
show ip ospf neighbor	Display the OSPF neighbor information according to the interface.
debug ip ospf adj	Supervise the adjacency establishment of OSPF.
debug ip ospf events	Supervise the interface and neighbour events of OSPF.
debug ip ospf flood	Supervise the flooding process of OSPF database.
debug ip ospf lsa-generation	Supervise the LSA generation of OSPF.
debug ip ospf packet	Supervise the message of OSPF.
debug ip ospf retransmission	Supervise the message retransmission process of OSPF.
debug ip ospf spf [<i>intra external</i>]	Supervise the SPF calculation route of OSPF.

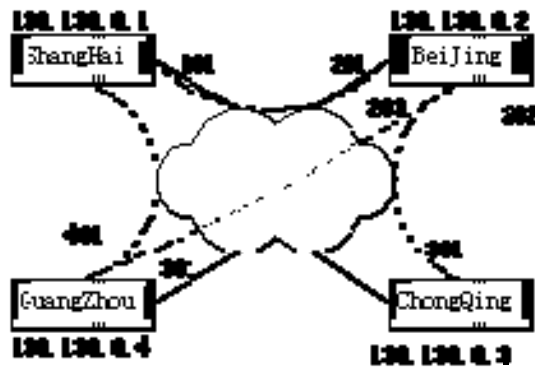
<code>debug ip ospf tree</code>	Supervise the establishment of SPF tree of OSPF
---------------------------------	---

5.4 Examples of OSPF Configuration

Here are the examples of OSPF configuration:

5.4.1 Examples of OSPF one-to-multi Point Configuration

Beijing uses DLCI201 to communicate with Shanghai, DLCI202 to communicate with Jelly, and DLCI203 with Platty. Neon uses DLCI101 to communicate with Mollie and DLCI102 with Platty. Platty can communicate with Neon (via DLCI 401) and Mollie (via DLCI 402). Jelly can communicate with Mollie via DLCI301.



The configuration of BEIJING:

```

Hostname Beijing
!
interface serial 1/0
ip address 130.130.0.2 255.255.0.0
encapsulation frame-relay
frame-relay map 130.130.0.1 pvc 201 broadcast
frame-relay map 130.130.0.3 pvc 202 broadcast
frame-relay map 130.130.0.4 pvc 203 broadcast
ip ospf network point-to-multipoint
!
router ospf 1
network 130.130.0.0 255.255.0.0 area 0

```

The configuration of ShangHai:

```

hostname shanghai
!
interface serial 1/0
ip address 130.130.0.1 255.0.0.0

```

```
encapsulation frame-relay
frame-relay map 130.130.0.2 pvc 101 broadcast
frame-relay map 130.130.0.4 pvc 102 broadcast
ip ospf network point-to-multipoint
!
router ospf 1
network 130.130.0.0 255.255.0.0 area 0
```

The configuration of GuangZhou:

```
hostname guangzhou
!
interface serial 1/0
ip address 130.130.0.4 255.0.0.0
encapsulation frame-relay
physical speed 1000000
frame-relay map 130.130.0.1 pvc 401 broadcast
frame-relay map 130.130.0.2 pvc 402 broadcast
ip ospf network point-to-multipoint
!
router ospf 1
network 130.130.0.0 255.255.0.0 area 0
```

The configuration of ChongQing:

```
hostname chongqing
!
interface serial 1/1
ip address 130.130.0.3 255.0.0.0
encapsulation frame-relay
physical speed 2000000
frame-relay map 130.130.0.2 pvc 301 broadcast
ip ospf network point-to-multipoint
!
router ospf 1
network 130.130.0.0 255.255.0.0 area 0
```

5.4.2 Examples of OSPF point to multipoints, non-broadcasting configuration

```
interface Serial1/0
ip address 10.0.1.1 255.255.255.0
ip ospf network point-to-multipoint non-broadcast
encapsulation frame-relay
frame-relay local-dlci 200
frame-relay map 10.0.1.3 pvc 202
frame-relay map 10.0.1.4 pvc 203
frame-relay map 10.0.1.5 pvc 204
no shut
```

```

!
router ospf 1
network 10.0.1.0 0.0.0.255 area 0
neighbor 10.0.1.3 cost 5
neighbor 10.0.1.4 cost 10
neighbor 10.0.1.5 cost 15

```

Here is the configuration of the router on the other side:

```

interface Serial1/2
ip address 10.0.1.3 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint non-broadcast
no ip mroute-cache
no keepalive
no fair-queue
frame-relay local-dlci 301
frame-relay map 10.0.1.1 pvc 300
no shut
!
router ospf 1
network 10.0.1.0 0.0.0.255 area 0

```

5.4.3 Examples of the configuration of variable length sub-network masks

OSPF, static routing supports variable length sub-network masks (VLSMs). Through VLSMs, it can use different masks to the same network number on different interfaces, this saves IP addresses, and can more efficiently utilize the address space of the network.

In the following example, it only uses 30bit sub-network masks and reserves address space of 2 bit as the host address for the serial ports. For point-to-point serial link, which only requires two host addresses, it is enough.

```

interface ethernet 1/0
ip address 131.107.1.1 255.255.255.0
! 8 bits of host address space reserved for ethernet
interface serial 1/1
ip address 131.107.254.1 255.255.255.252
! 2 bits of address space reserved for serial lines
! Router is configured for OSPF and assigned AS 107
router ospf 107
! Specifies network directly connected to the router
network 131.107.0.0 0.0.255.255 area 0.0.0.0

```

5.4.4 Examples of the configuration of OSPF route and route distribution

OSPF requires exchanging information among many internal routers, ABRs and ASBRs. Under minimum configuration, the routers based on OSPF can work under default parameters and have no requirement of authentication.

Here are three examples of configuration:

The first example practices the basic OSPF command.

The second example configures the configuration of internal router, ABR and ASBR in a single OSPF autonomous system.

The third example illustrates a more complex example of configuration with various OSPF tools.

1. An example of basic OSPF configuration

The following example illustrates a simple OSPF configuration. Activate routing process 90 , then connect the Ethernet interface 0 to area 0.0.0.0. Meanwhile, redistribute RIP to OSPF, OSPF to RIP.

```
interface ethernet 1/0
  ip address 130.130.1.1 255.255.255.0
  ip ospf cost 1
!
interface ethernet 1/0
  ip address 130.130.1.1 255.255.255.0
!
router ospf 90
  network 130.130.0.0 255.255.0.0 area 0
  redistribute rip
!
router rip
  network 130.130.0.0
  redistribute ospf 90
```

2. An example of the basic configuration of inner router, ABR and ASBR

The following example allocates 4 areas ID for 4 IP address range. Firstly, routing process 109 is activated, the 4 areas are: 10.9.5.0, 2, 3, 0. The masks of area 10.9.50.0,2,3 designate the address range, but area 0 includes all the networks.

```
router ospf 109
  network 131.108.20.0 255.255.255.0 area 10.9.50.0
  network 131.108.0.0 255.255.0.0 area 2
  network 131.109.10.0 255.255.255.0 area 3
  network 0.0.0.0 0.0.0.0 area 0
!
! Interface Ethernet1/0 is in area 10.9.50.0:
interface ethernet 1/0
  ip address 131.108.20.5 255.255.255.0
!
```

```
! Interface Ethernet1/1 is in area 2:
interface ethernet 1/1
  ip address 131.108.1.5 255.255.255.0
!
! Interface Ethernet1/2 is in area 2:
interface ethernet 1/2
  ip address 131.108.2.5 255.255.255.0
!
! Interface Ethernet1/3 is in area 3:
interface ethernet 1/3
  ip address 131.109.10.5 255.255.255.0
!
! Interface Ethernet1/4 is in area 0:
interface ethernet 1/4
  ip address 131.109.1.1 255.255.255.0
!
! Interface FastEthernet0/0 is in area 0:
interface FastEthernet0/0
  ip address 10.1.0.1 255.255.0.0
```

The functions of network area configuration command are ordinal, so the order of the commands is important. The router matches the address/mask pair of each interface in order. For detailed information, please refer to the related content in the reference of related network protocol command in "OSPF command".

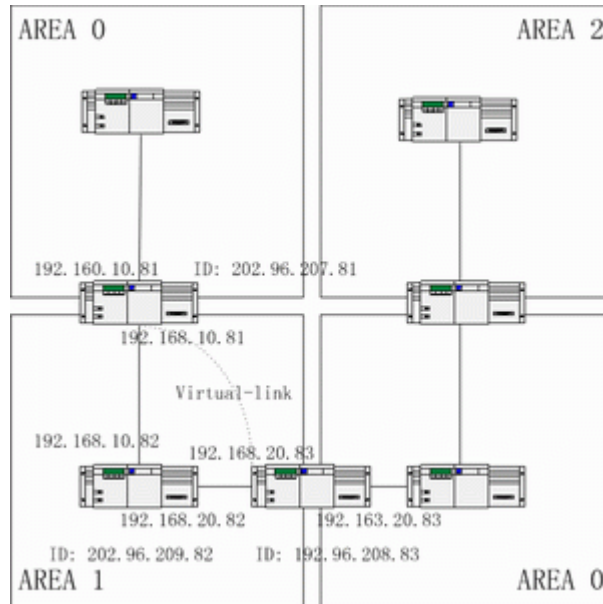
Let's return to the first network area in the above example. The area ID 10.9.50.0 is configured with an interface sub-network mask as 131.108.20.0. So Ethernet interface 0 matches. So Ethernet interface 0 only exists in area 10.9.50.0.

Then come to the second area. Except interface 0, apply the same process on other interfaces, then Ethernet interface 1 matches. So interface 1 connects to area2.

Continue the matching of other network areas. NOTICE that the last network area command is a special case, which means that the rest interfaces are all connected to network area 0.

An example of the complex configuration of interior router, ABR and ASBR.

The following example illustrates the configuration of several routers in a single OSPF autonomous system. Figure 24 is the network topology of the example:



1. Configure the router according to the above Figure:

RouterA:

```
interface loopback 0/0
ip address 202.96.207.81 255.255.255.0
!
interface Ethernet 1/0
ip address 192.168.10.81 255.255.255.0
!
interface ethernet 1/0
ip address 192.160.10.81 255.255.255.0
!
router ospf 192
network 192.168.10.0 255.255.255.0 area 1
network 192.160.10.0 255.255.255.0 area 0
!
```

RouterB:

```
interface loopback 0/0
ip address 202.96.209.82 255.255.255.252
!
interface Ethernet 1/0
ip address 192.168.10.82 255.255.255.0
!
interface ethernet 1/1
ip address 192.160.20.82 255.255.255.0
!
router ospf 192
network 192.168.20.0 255.255.255.0 area 1
```

```

network 192.168.10.0 255.255.255.0 area 1
!
routerC:
interface loopback 0/0
ip address 202.96.208.83 255.255.255.252
!
interface Ethernet 1/0
ip address 192.163.20.83 255.255.255.0
!
interface ethernet 1/1
ip address 192.160.20.83 255.255.255.0
!
router ospf 192
network 192.168.20.0 255.255.255.0 area 1
network 192.163.20.0 255.255.255.0 area 0
!

```

3. Configuration examples for complicated internal router, ABR and ASBR

The following example shows how to configure multiple routers in a single OSPF autonomous system. Figure 4-2 shows the network topology of the configuration example:

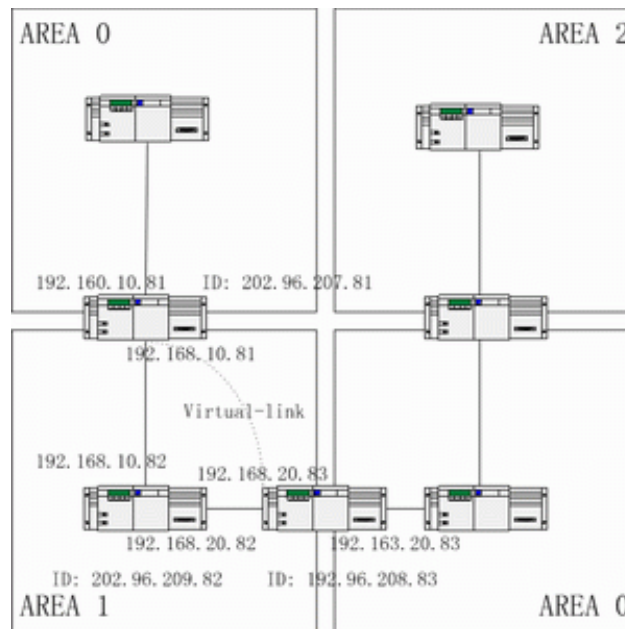


Figure 4-2 Network topology of the configuration example

Configure the router according to Figure 4-2:

Router A:

```
interface loopback 0/0
ip address 202.96.207.81 255.255.255.0
!
interface Ethernet 1/0
ip address 192.168.10.81 255.255.255.0
!
interface ethernet 1/0
ip address 192.160.10.81 255.255.255.0
!
router ospf 192
network 192.168.10.0 255.255.255.0 area 1
network 192.160.10.0 255.255.255.0 area 0
!
```

Router B:

```
interface loopback 0/0
ip address 202.96.209.82 255.255.255.252
!
interface Ethernet 1/0
ip address 192.168.10.82 255.255.255.0
!
interface ethernet 1/1
ip address 192.160.20.82 255.255.255.0
!
router ospf 192
network 192.168.20.0 255.255.255.0 area 1
network 192.168.10.0 255.255.255.0 area 1
!
```

Router C:

```
interface loopback 0/0
ip address 202.96.208.83 255.255.255.252
!
interface Ethernet 1/0
ip address 192.163.20.83 255.255.255.0
!
interface ethernet 1/1
ip address 192.160.20.83 255.255.255.0
!
router ospf 192
network 192.168.20.0 255.255.255.0 area 1
network 192.163.20.0 255.255.255.0 area 0
!
```


4. an example of complex OSPF on ABR router configuration

Here is an example of OSPF configuration:

```
interface ethernet 1/0
ip address 192.168.20.81 255.255.255.0
ip ospf password GHGHGHG
ip ospf cost 10
!
interface ethernet 1/1
ip address 192.168.30.81 255.255.255.0
ip ospf password ijklmnop
ip ospf cost 20
ip ospf retransmit-interval 10
ip ospf transmit-delay 2
ip ospf priority 4
!
interface ethernet 1/2
ip address 192.168.40.81 255.255.255.0
ip ospf password abcdefgh
ip ospf cost 10
!
interface ethernet 1/3
ip address 192.168.0.81 255.255.255.0
ip ospf password ijklmnop
ip ospf cost 20
ip ospf dead-interval 80
!
router ospf 192
network 192.168.0.0 255.255.255.0 area 0
network 192.168.20.0 255.255.255.0 area 192.168.20.0
network 192.168.30.0 255.255.255.0 area 192.168.30.0
network 192.168.40.0 255.255.255.0 area 192.168.40.0
area 0 authentication simple
area 192.168.20.0 stub
area 192.168.20.0 authentication simple
area 192.168.20.0 default-cost 20
area 192.168.20.0 authentication simple
area 192.168.20.0 range 36.0.0.0 255.0.0.0
area 192.168.30.0 range 192.42.110.0 255.255.255.0
area 0 range 130.0.0.0 255.0.0.0
area 0 range 141.0.0.0 255.0.0.0
redistribute rip
RIP on network 192.168.30.0
router rip
network 192.168.30.0
redistribute ospf 192
```

!

Chapter 6 Configure BGP

6.1 Overview

This chapter describes how to configure border gateway protocol (BGP). For complete description about BGP commands in this chapter, please refer to other sections related to “BGP command”. BGP is an Exterior Gateway Protocol (EGP) defined in RFC1163, 1267 and 1771. It permits to establish a route selection mechanism among different autonomous systems, this mechanism can automatically guarantee the loop-free routing information exchange between the autonomous systems.

6.1.1 The BGP implementation of the router

In BGP, each route includes a network number, the autonomous system list this route has traverse (called As-path) and other attribute lists. Our router software supports BGP v4 defined in RFC1771. The basic function of BGP is to exchange network reachability information with other BGP systems, including information about AS-path information. This information can be used to construct the AS connection graph which can eliminate route loop, and it can implement AS level routing policy with AS connection graph. BGP v4 supports classless inter-domain router (CIDR), CIDR can reduce the size of the routing table through creating summary routes and thus creates a super network. CIDR removes the concept of network level in BGP, and supports IP prefix broadcasting. CIDR route can be transferred through OSPF, Enhanced IGRP, ISIS-IP and RIP2.

An important difference between exterior gateway routing and interior gateway router is the former has better controllability. In order to control the route, the implementation of BGP provides several optional methods:

- In order to filter routes, it can be based on access-list based on neighbour, aspath-list, prefix-list and also use the access-list based on interface, prefix-list to filter routes or the Nexthop attribute of the routes.
- In order to change the attribute of the routes, you can use the route-map to mend the attributes of BGP routes including MED, Local preference, route value and etc...
- In order to interact with the interior gateway dynamic routing protocol (OSPF, RIP, etc...), you can redistribute route, so as to automatically generate BGP routing information. You can also generate BGP routes through manual configuration of network, aggregation. While generating BGP routes, you can use route-map to configure the attributes of the routes.
- In order to control the precedence of BGP routes in the system, you can use command “distance” to configure the management distance of BGP routes.

6.1.2 How does BGP select the path

The decision process of BGP is established on the basis of comparing route attribute value. When the same network has several routes, BGP selects the best route to the destination. The following process summarizes how BGP selects the best route:

- If it cannot arrive at the next hop, it will not be considered.
- If the path is internal and the synchronization is activated, and if the route is not in IGP, the route will not be considered.
- Select preferable path with the maximum precedence.
- If each route has the same value, preferably select the route with the maximum local precedence.
- If each route has the same local precedence, select preferably the route generated by local router. For example, route may be generated by local router through the using of command “network, aggregate” or by redistributing IGP route.
- If the local precedences are the same, or if there is no route generated by local router, then select preferably the route with the shortest AS path.
- If the AS path lengths are the same, then select preferably the route with the lowest attribute value of “origin” (IGP<EGP<IMCOMPLETE)
- If the attribute values of “Origin” are the same, then select preferable route with the lowest MED value. Unless “bgp always-compare-med” is activated, this comparable can only be carried out between the routes from the same neighbour AS.
- If each route has the same MED, select preferable external path (EBGP) rather than internal path (IBGP). All paths inside the autonomous system confederation are considered to be internal paths, but select preferably EBGP confederation not IBGP confederation.
- If each route has the same connection attribute, select preferable route with a smaller router-id.

6.2 BGP Configuration Task List

6.2.1 Basic configuration task list of BGP

The configuration tasks of BGP can be divided into basic tasks and advanced tasks. The first two entries of basic tasks are necessary to configure BGP, other entries in basic tasks and all advanced tasks are optional.

The basic configuration tasks of BGP include:

- Activate the route selection of BGP.
- Configure BGP neighbor.

- Configure BGP soft reconfiguration
- Reset BGP connection.
- Configure the synchronization between BGP and IGP
- Configure BGP route value
- Configure BGP route filter based on the neighbour
- Configure BGP route filtration based on the interface
- Disable the next hop treatment of BGP update

6.2.2 Advanced BGP configuration tasks list

Advanced, optional BGP configuration tasks are listed as the following:

- Use route-map to filter and modify route update
- Configure aggregate address
- Configure BGP community attribute
- Configure autonomous system confederation
- Configure route reflector
- Shut down peer entity
- Configure multihop external peer body
- Configure the management distance of BGP routes
- Adjust BGP timer.
- Compare MED of routes from different AS.

For more related information about the configuration of the attributes of several IP route selection protocols, please refer to "The configuration of attributes of IP routing which are independent from the protocol".

6.3 Configure basic BGP features

6.3.1 Configuring Basic BGP Features

1. Activate the route selection of BGP

In order to activate BGP route selection, use the following commands under global configuration mode to activate BGP route selection:

Command	Purpose
---------	---------

router bgp autonomous-system	Under router configuration mode, activate BGP route selection process.
network <i>network-number/masklen</i> [route-map <i>route-map-name</i>]	Tag the network as local autonomous system and add it to the BGP list.

Notes:

For exterior gateway routing protocol, the using of configuration command “network ” to configure an IP network canand to only control which networks will be informed. This is opposite to interior gateway protocol (IGP), such as RIP, it is using command “network” to decide where to send the update.

Command “network” is used to import IGP routes to BGP routing table. Router resource, such as configured RAM, decides the upper limit of the usable command “network”. As a choice, you can use command “redistribute” to achieve the same effect.

2. Configure BGP neighbour

To configure BGP neighbour is to establish the peer to exchange routing information. BGP neighbour ought to be configured in order to exchange routing information with the outer world.

BGP supports two kinds of neighbours: internal neighbour (IBGP) and external neighbour (EBGP). Internal neighbours are in the same AS; external neighbours are in different ASs. Normally, external neighbours are adjacent to each other and share the same sub-network. But internal neighbours can be at any place in the same AS.

Use configuration command “Neighbor” to configure BGP neighbour:

Command	Purpose
neighbor <i>{ip-address peer-group-name}</i> remote-as <i>number</i>	Designate a BGP neighbour.

For example about the configuration of the BGP neighbor, please refer to the section in the bottom of this chapter “an example of the configuration of the BGP neighbor”.

3. Configure BGP soft reconfiguration

Generally speaking, BGP neighbors only exchange all routes when the connections are established, after that, they only exchange update routes. So if the configured routing policy gently changes, in order to apply it on the received routes, it is necessary to clear BGP session. The clearing of BGP session will cause the invalidation of cache and will exert great influence on the operation of the network. Soft reconfiguration function enables the configuration and activation of policy without clearing BGP session. So, we recommend you to use soft reconfiguration, currently, we enable the soft reconfiguration based on each neighbour. When the soft reconfiguration is used on the incoming update produced by the neighbor, it is called incoming soft reconfiguration; When the soft reconfiguration is used on the outgoing update to the neighbor, it is called outgoing soft reconfiguration. Applying incoming soft reconfiguration can make the new input policy effective, Applying outgoing soft reconfiguration makes new local output policy effective without the reset of BGP session.

In order to generate new incoming update without resetting of BGP session, local BGP speaker should save the received incoming update without any modification, regardless whether it would be accepted or denied under current incoming policy. This

will be very memory consuming and should be avoided. On the other hand, outgoing reconfiguration does not have any extra memory consumption, so it is always effective. You can trigger outgoing soft reconfiguration on the other side of BGP session to make the new local incoming policy effective.

In order to permit incoming soft reconfiguration, you should configure the BGP to save all accepted routing update. Outgoing reconfiguration need not be pre-configured.

Use the following router configuration command to configure BGP soft reconfiguration:

Command	Purpose
Neighbor <i>{ip-address peer-group-name}</i> soft-reconfiguration [inbound]	Configure BGP soft reconfiguration

If you use parameter “**peer-community-name**” to designate BGP peer community, all peer community members in it will inherit the feature of this command.

4. Reset BGP connection

Once two routers are defined as BGP neighbours, they create a BGP connection, and exchange routing information. If the BGP routing policy has been changed, or other configurations have been changed, then you should reset the BGP connection in order to make the change of configuration effective. Use one of the following two management mode commands to reset BGP connection:

Command	Purpose
clear ip bgp <i>{* address}</i>	Reset all BGP connections. Recreate a special BGP connection.

5. Configure the synchronization between BGP and IGP

If you permit another AS to transfer data to the third AS through your AS, then the synchronization between your AS internal routing state and the routing information it broadcasted to another ASs is very important. For example, if your BGP wants to broadcast routes before all routers in your AS get to know the routes through IGP, then your AS may receive some information that some routers cannot route. In order to prevent these situations, BGP should wait until all IGP routers inside AS get to know that routing information, this is the synchronization between BGP and IGP, and the synchronization is activated by default.

Under certain situations, it is not necessary to synchronize. If you do not permit other ASs to transfer data through your AS, or if all routers in your AS will run BGP, you can cancel the Synchronization function. Cancelling that feature will enable you to put fewer routes in your IGP, and enable quicker convergence of BGP. Use the following router configuration command to cancel synchronization:

Command	Purpose
no synchronization	Cancel the synchronization between BGP and IGP.

While canceling synchronization, you should use command “clear ip bgp” to clear BGP dialogue.

For an example about BGP synchronization, please refer to the section in the bottom of this chapter “an example of BGP path filtration by the neighbors”.

Normally, you do not expect to redistribute all routes to your IGP. A common design is to redistribute one or two routes, and make them the external routes in IGRP, or force the BGP session to generate an AS default route. When BGP redistribute routes to IGP, only the routes acquired through EBGP will be redistributed. Under most situations, you do not want to allocate your IGP to BGP, just use configuration command "network " to list the network in AS, then your network will be broadcasted. The networks listed in this form are called local network, and enables BGP to have attribute "Origin" of IGP. They must appear in the main IP routing table, and are effective; for example, they are direct-connected routes, static routes or routes known through IGP. BGP routing process periodically scans the main IP routing table to check the existence of a local network, and accordingly updates BGP routing table if you really want BGP to execute redistribution, you must be very careful, because these may be the routes in IGP that are injected by other routers through BGP, this may bring force a kind of situation that BGP potentially injects the information into IGP, and then send back the information to BGP. Vice versa.

6. Configure BGP route value

BGP route value is a number set to BGP route in order to control the route selection process, value is local for the router. The value ranges from 0 to 65535. BGP route generated locally has a default value of 32768, the route got from the neighbour values 0. The administrator can implement routing policy through the change of route value.

Use the following router configuration command to configure BGP route weight:

Command	Purpose
neighbor {ip-address peer-group-name} weight weight	Designate a value to each route from one neighbour.

Besides, you can change the route weight through route-map.

7. Configure BGP route filter based on the neighbour

There are 4 methods in BGP implementation of router software to filter BGP routes of the designated neighbours:

Use Aspath list filter together with global configuration command "**ip aspath-list**" and command "**neighbour filter-list**".

Command	Purpose
ip aspath-list aspaths-list-name { permit deny } as-regular-expression	Define an accessing list relative to BGP.
router bgp autonomous-system	Enter into router configuration mode.
neighbor {ip-address peer-group-name} filter-list aspath-list-name { in out }	Establish a BGP filter.

Use access list together with global configuration command "ip access-list" and command "neighbour distribute-list".

Command	Purpose
ip access-list standard access-list-name	Define an access list.
router bgp autonomous-system	Enter into router configuration mode.
neighbor {ip-address peer-group-name} distribute-list access-list-name { in out }	Establish a BGP filter.

Use prefix list together with global configuration command “ip prefix-list” and command “neighbour prefix-list”.

Command	Purpose
ip prefix-list <i>prefix-list-name</i> { permit deny } A.B.C.D/n ge x le y	Define a prefix list.
router bgp <i>autonomous-system</i>	Enter into router configuration mode.
neighbor { <i>ip-address</i> <i>peer-group-name</i> } prefix-list <i>prefix-list-name</i> { in out }	Establish a BGP filter.

Use route-map together with global configuration command “route-map” and command “neighbour route-map”.

Using route-map can not only filter routes, but also changes routes attribute, the usage will be described in the following chapters.

For example based on neighbour filter route, please refer to “example of BGP route filtration based on the neighbor”.

8. Configure BGP route filtration based on the interface

Configuring BGP route filtration based on the interface can be achieved through using access list and prefix list. Network number and the gateway address of the routes can be filtered. It can designate “access-list” option to use access list for filtration of network number of the routes, designate “prefix-list” option to use prefix list for filtration of network number of the routes, designate “gateway” option to use access list for filtration of “nexthop” attribute of the routes. It can even filter the network number and “nexthop” attribute of routes at the same time, but “access-list” option cannot be used together with “prefix-list” option. Designate “*” can filter the routes on all interfaces.

To order to configure the filtration of BGP routes based on the interface, you should carry out the following configurations under BGP configuration mode:

Command	Purpose
filter interface { in out } { access-list <i>access-list-name</i> } { prefix-list <i>prefix-list-name</i> } { gateway <i>access-list-name</i> }	Filter BGP routes based on the interface.

For examples of route filtration based on the interface, please refer to “examples of BGP route filtration based on the interface”.

9. Disable the nexthop treatment of BGP update

You can configure to disable the nexthop treatment of neighbour BGP update. This may be useful in non-broadcasting network (such as FR or X.25), in FR or X.25 network, BGP neighbour may not directly access all other neighbors in the same IP sub-network. There are two methods to cancel nexthop treatment:

1. Use the local IP address of this BGP connection to replace the nexthop address of the outgoing route;
2. Use route-map to designate the nexthop address of incoming or outgoing routes. (Please refer to other chapters)

3. Use the following router configuration command to disable nexthop treatment and use the local IP address of this BGP connection to replace the nexthop address of the outgoing routes.

Command	Purpose
neighbor { <i>ip-address</i> <i>peer-group-name</i> } next-hop-self	Disable the nexthop treatment while carrying out BGP neighbour update.

Using this command to configure will enable the current router to inform itself to be the nexthop of the route. So, other BGP neighbours will forward packets to this network to the current router. This is very useful in non-broadcasting network environment, because there exists a path from the current router to the designated neighbor. But it is not the case in broadcasting network environment, because this will induce unnecessary extra hops.

6.3.2 Configure advanced BGP features

1. Use route-map to filter and modify route update

You can use route-map to filter route update and modify parameter attribute based on each neighbour. Route-map can be applied both on incoming update and outgoing update. Only the routes passing route-map can be processed while sending or accepting route update.

Route-map supports incoming and outgoing update to match with AS path, community and network number. AS matching demands the using of command "aspath-list"; the matching based on community demands the using of command "community-list", the matching based on the network demands the use of command "ip access-list".

Use the following BGP configuration command to configure route-map for filtration and modification of route update:

Command	Purpose
neighbor { <i>ip-address</i> <i>peer-group-name</i> } route-map <i>route-map-name</i> { in out }	Apply route-map on incoming or outgoing routes.

For examples of using route-map to filter and modify the route update, please refer to "Examples of BGP route-map".

2. Configure aggregate address

Classless inter-domain routing can create aggregate routing (and super network) to minimize the routing table. You can configure aggregate routing in BGP through redistributing aggregate routes to BGP or through using conditional aggregate attributes described in the following task list. If there is at least one more detailed record in BGP routing table, add the aggregate address to the BGP routing table.

Use one or more router configuration commands in the following to create an aggregate address in the routing table:

Command	Purpose
aggregate <i>network/len</i>	Create aggregate address in BGP routing table.
aggregate <i>network/len</i> summary-only	Broadcast summary address only.

aggregate <i>network/len</i> route-map <i>map-name</i>	Generate aggregate address according to conditions designated by route-map.
--	---

For examples regarding the using of BGP route aggregation, please refer to the section in the bottom of this chapter “examples of BGP route aggregation”.

3. Configure BGP community attribute

The routing policy that BGP supports is mainly based on one of the 3 values in BGP routing information:

- Network number of routes:
- *as_path* attribute value of routes:
- The “community” attribute value of routes

Dividing the routes into communities through “community” attribute, and applying the routing policy based on the community, thereby simplifies the configuration of control of routing information.

Community is a group of routes with the common attributes; each route may belong to several communities. AS administrators can define a certain route belongs to a certain community.

Community attribute is an optional and transferable global attribute ranging from 1 to 4,294,967,200. The famous communities pre-defined in the Internet communities include:

- No-export--- Do not advertise this route to EBGp peer (Including the EBGp peers inside the autonomous system confederation).
- No-advertise---Do not advertise this route to any peer .
- local-as---Do not advertise this route to the exterior of autonomous system (ca send this route to the other sub-AS peers in the autonomous system confederation.)

When generating, accepting or sending routes, BGP speakers can configure, add or modify the route community attribute. when aggregating routes, the generated aggregation includes the “community” attributes from complete communities of all original routes.

By default, “Community” attributes are not sent to the neighbor. Use the following BGP configuration command to designate sending “community” attribute to the neighbour:

Command	Purpose
neighbor <i>{ip-address peer-group-name}</i> send-community	Designate to send attribute “community” to the neighbor.

You need to do the following jobs to configure community attribute for the router:

Command	Purpose
route-map <i>map-name sequence-number</i> {deny}	Configure route-map.

permit}	
set community <i>community-value</i>	Configure rule of setting.
router bgp <i>autonomous-system</i>	Enter into router configuration mode.
neighbor { <i>ip-address</i> <i>peer-group-name</i> } route-map <i>access-list-name</i> { in out }	Apply route-map.

To filter routing information based on community attributes, you need to do the following jobs:

Command	Purpose
ip community-list <i>community-list-name</i> { permit deny } community-expression	Define community list.
route-map <i>map-name</i> <i>sequence-number</i> { deny permit }	Configure route-map.
match <i>community-list-name</i>	Configure rules of matching.
router bgp autonomous-system	Enter into router configuration mode
neighbor { <i>ip-address</i> <i>peer-group-name</i> } route-map <i>route-map-name</i> { in out }	Apply route-map.

For examples of using community attributes, please refer to “Examples of route-map using BGP community attribute”.

4. Configure autonomous system confederation

The way to reduce the number of IBGP connections is to divide an AS into several sub-AS, then form them into an autonomous system confederation. From the external perspective, the confederation looks like an AS. In the confederation, each sub-AS is full-mesh inside, and has connections with other sub-ASs in the same confederation. Even if there are EBGP sessions between peers of different sub-ASs, they may still exchange routing selection information like IBGP peers. Concretely speaking, it is saving the nexthop, MED and local precedence information.

To configure a BGP autonomous system confederation, you should designate the confederation identifier. The confederation identifier is an AS number, from an external perspective, the confederation is just like a single AS with AS number being the confederation identifier.

Use the following BGP configuration command to configure confederation identifier of the autonomous system:

Command	Purpose
bgp confederation0 identifier <i>autonomous-system</i>	Configure the confederation identifier of the autonomous system.

In order to designate the autonomous system number belonging to autonomous system confederation, use the following BGP configuration command:

Command	Purpose
bgp confederation peers autonomous-system [autonomous-system ...]	Designate the AS belongs to the confederation of autonomous system.

For examples of autonomous system confederation, please refer to “examples of BGP autonomous system confederation”.

5. Configure route reflector

Another method to reduce the number of IBGP connections instead of configuring autonomous system confederation is to configure route reflector.

The internal peers of the route reflector are divided into two groups: client peers and all other routers (non-client peers). The route reflector reflects the routes between the two groups; the route reflector and its client peers form a cluster. Non-client peers must be full-mesh connected, but client peers need not. The clients in the cluster do not communicate with IBGP speakers outside the cluster.

When route reflector receives routing information, it completes the following tasks:

- Broadcast the routes from external BGP speaker to all clients and non-client peers.
- Broadcast the routes from non-client to all clients.
- Broadcast the routes from the clients to all clients and non-client peers. So, the client peers need not be full-mesh-connected.

Use the following router configuration command to configure the local router as the reflector and designate neighbors as the router reflector client:

Command	Purpose
neighbor <i>ip-address</i> route-reflector-client	Configure the local router as route reflector and designate neighbors as the client.

An AS may have several route reflectors, the way route reflector to process other route reflectors is the same as the processing of IBGP speakers. Normally, a cluster of clients have only one route reflector, and then the cluster is identified by the route reflector's router ID. In order to increase the redundancy and avoid the failure of single node, a cluster may have more than one route reflectors. In this case, all the route reflectors in the cluster should be configured with 4-bit cluster ID, so that the route reflector can identify the update information of the route reflector in the same cluster. All the route reflectors belonging to the same cluster should be full-mesh-connected, and they should have the same client and non-client peer set.

If there is more than one route reflector in the cluster, you can use the following BGP configuration command to configure cluster ID:

Command	Purpose
bgp <i>cluster-id</i> <i>cluster-id</i>	Configure cluster-ID.

For examples of the configuration of route reflector, please refer to "examples of the configuration of BGP route reflector".

6. Shut down peer entity

Use the following BGP configuration command to shut down BGP neighbour:

Command	Purpose
neighbor { <i>ip-address</i> <i>peer-group-name</i> } shutdown	Shut down BGP neighbour.

Use the following BGP configuration command to activate the neighbour shut down previously:

Command	Purpose
no neighbor shutdown { <i>ip-address</i> <i>peer-group-name</i> }	Activate BGP neighbour.

7. Configure multihop external peer body

By default, external peers should be on a directly connected network, in order to configure multihop external peer, you need to carry out the following task:

Command	Purpose
neighbor ebgp-multihop { <i>ip-address</i> <i>peer-group-name</i> } <i>t</i>	Configure BGP neighbor as multihop external peer.

8. Configure the management distance of BGP routes

Management distance is a kind of measurement of the preference of different routing protocol. BGP uses 3 different management distances: external distance, internal distance and local distance. The routes obtained from external BGP will be assigned with the external distance; the routes obtained from internal BGP will have a distance as internal distance, local routes will be given the local distance. Use the following BGP configuration command to configure BGP route management distance:

Command	Purpose
distance bgp { <i>external-distance</i> <i>internal-distance</i> <i>local-distance</i> }	Configure BGP route management distances.

The change of management distances of BGP route is dangerous, and normally it is not recommended. The external distance should be shorter than the distance of any other dynamic routing protocol and the internal distance should be longer than the distance of any other dynamic routing protocol.

9. Adjust BGP timer

Use the following BGP configuration command to adjust the BGP “keepalive” and “holdtime” timers of detailed neighbour:

Command	Purpose
neighbor timers [<i>ip-address</i> <i>peer group-name</i>] <i>keepalive holdtime</i>	Set “keepalive” and “holdtime” timer interval (count with unit ‘second’) for designated peer or peer community

Use command “no neighbour timers” to reset the timer interval of BGP neighbor or peer community to the default value.

10. Compare MED of routes from different AS

MED is a parameter to be considered when selecting the best route from several paths. The path with lower MED value will be preferably considered than the route with higher MED value.

Under default situation, during the process of selecting the best route, MED’s comparison only takes place in the routes from the same AS. You can permit the MEDs’ comparison to take place in routing selection, regardless of which AS the routes come from.

Use the following BGP configuration command to realize the above objective:

Command	Purpose
bgp always-compare-med	Permit to make MEDs comparison among routes from different AS.

11. Configure the MD5 authentication for BGP neighbor

To make sure of the secure routing information forwarding between ASs, perform the password authentication on the BGP connection through the MD5 option provided by TCP.

Run the following command to achieve the previous purpose:

Command	Purpose
Neighbor A.B.C.D password LINE	Enables the MD5 authentication of the BGP neighbor and set the password.

You can run **no neighbor A.B.C.D password** to cancel the MD5 authentication for the BGP neighbor.

6.4 Monitoring and Maintaining BGP

The administrator can display or delete the BGP routing table or the content of other databases. Of course the detailed statistics information can also be displayed. The following are relative tasks:

- Deleting the BGP routing table and the database
- Displaying the routing table and the system statistics information
- Tracking the BGP information

6.4.1 Deleting the BGP Routing Table and the BGP Database.

The following table lists the tasks relative with high-speed cache deletion, table deletion or BGP database deletion. The commands listed in the following table are all run in EXEC mode.

Command	Purpose
clear ip bgp *	Resets all BGP connections.
clear ip bgp as-number	Resets the BGP connections of the designated autonomous system.
clear ip bgp address	Resets the BGP connections of the designated neighbor.
clear ip bgp address soft {in out}	Deletes the incoming database or the outgoing database of the designated neighbor.
clear ip bgp aggregates	Deletes the routes generated in route aggregation.
clear ip bgp networks	Deletes the routes generated during forwarding process.

clear ip bgp <i>redistribute</i>	Deleting the routes generated by the network command.
---	--

6.4.2 Displaying the Routing Table and the System Statistics Information

The detailed statistics information about the BGP routing table or the database will be displayed. The provided information can decide resource utilization and help resolving network problems. The information about the node reachability can also be displayed.

You can run the following commands to display all kinds of routing statistics information:

Command	Purpose
show ip bgp	Displays the BGP routing table in the system.
show ip bgp prefix	Displays the routes which match the designated prefix list.
show ip bgp community	Displays the statistics information about the group attribute.
show ip bgp regexp <i>regular-expression</i>	Displays the routes which match the designated regular expression.
show ip bgp network	Displays the designated BGP route.
show ip bgp neighbors <i>address</i>	Displays the information about the TCP and the BGP connections of the designated neighbor.
show ip bgp neighbors [<i>address</i>] [received-routes routes advertised-routes]	Displays the routes learned from the special BGP neighbor.
show ip bgp paths	Displays the information about all BGP paths in the database.
show ip bgp summary	Displays the states of all BGP connections.

6.4.3 Tracking the BGP Information

You can observe BGP connection establishment and route transmission/reception by tracking the BGP information, which helps to locate the troubles and resolve the problems. The commands to track the BGP information are shown in the following table:

Command	Purpose
debug ip bgp *	Tracks the general BGP information.
debug ip bgp all	Tracks all BGP information.
debug ip bgp fsm	Tracks the BGP state machine.
debug ip bgp keepalive	Tracks the KeepAlive packets of BGP.
debug ip bgp open	Tracks the OPEN packets of BGP.
debug ip bgp update	Tracks the UPDATE packets of BGP.

6.5 Examples of BGP configuration

The following sections provide the examples of BGP configuration:

6.5.1 An example of BGP route-map

The following example illustrates how to use route-map to change the incoming route attribute from the neighbor. Set the metric of all routes that come from neighbour 140.222.1.1 and meet the requirement of ASPATH accessing list "aaa" to 200, local precedence value to 250, and they are accepted, all other routes will be denied.

```
router bgp 100
!
neighbor 140.222.1.1 route-map fix-weight in
neighbor 140.222.1.1 remote-as 1
!
route-map fix-weight permit 10
match as-path aaa
set local-preference 250
set weight 200
!
ip aspath-list aaa permit ^690$
ip aspath-list aaa permit ^1800
```

In the following example, the first entry of route-map "freddy" will set the MED attributes of all routes originating from autonomous system 690 to 127. The second entry allows the routes that don't meet the above conditions to be transferred to neighbor 1.1.1.1.

```
router bgp 100
neighbor 1.1.1.1 route-map freddy out
!
ip aspath-list abc permit ^690_
ip aspath-list xyz permit .*
!
route-map freddy permit 10
match as-path abc
set metric 127
!
route-map freddy permit 20
match as-path xyz
```

The following example illustrates how to use route-map to change the routes from route redistribution:

```
router bgp 100
redistribute rip route-map rip2bgp
!
route-map rip2bgp
match ip address rip
set local-preference 25
```

```

set metric 127
set weight 30000
set next-hop 192.92.68.24
set origin igp
!
ip access-list standard rip
permit 131.108.0.0 255.255.0.0
permit 160.89.0.0 255.255.0.0
permit 198.112.0.0 255.255.128.0

```

6.5.2 An example of neighbour configuration

In the following example, BGP router belongs to AS109, and creates two networks. This router has 3 neighbors: the first neighbor is an external one (in different AS); the second is internal one (with the same AS number). The third is also an external one.

```

router bgp 109
network 131.108.0.0
network 192.31.7.0
neighbor 131.108.200.1 remote-as 167
neighbor 131.108.234.2 remote-as 109
neighbor 150.136.64.19 remote-as 99

```

6.5.3 An example of BGP route filtration based on the neighbor

Here is an example of BGP path filtration based on the neighbor. The routes passing through as-path access list "test1" will receive a metric value as 100. Only routes passing through as-path access list "test2" will be sent to 193.1.12.10, similarly, only those routes passing access list "test3" will be accepted by 193.1.12.10:

```

router bgp 200
neighbor 193.1.12.10 remote-as 100
neighbor 193.1.12.10 filter-list test1 weight 100
neighbor 193.1.12.10 filter-list test2 out
neighbor 193.1.12.10 filter-list test3 in
ip aspath-list test1 permit _109_
ip aspath-list test2 permit _200$
ip aspath-list test2 permit ^100$
ip aspath-list test3 deny _690$
ip aspath-list test3 permit .*

```

6.5.4 Examples of BGP route filtration based on the interface

The following is the example of the configuration of route filtration based on the interface. It filters the routes from interface e1/0 through access list "ac1":

```

router bgp 122
filter e1/0 in access-list ac1

```

The following example uses access list “filter-network” to filter the network numbers of the routes, and meanwhile, uses access list “filter-gateway” to filter gateway address of the routes from interface s1/0.

```
router bgp 100
filter s1/0 in access-list filter-network gateway filter-gateway
```

The following example: uses prefix list “filter-prefix” to filter the network numbers of the routes, and meanwhile, use accessing list “filter-gateway” to filter gateway address of routes from all interfaces.

```
router bgp 100
filter * in prefix-list filter-prefix gateway filter-gateway
```

6.5.5 Examples of using prefix list to configure route filtration

In the following example default route 0.0.0.0/0 is denied.

```
ip prefix-list abc deny 0.0.0.0/0
```

The following example: permits routes matching prefix 35.0.0.0/8:

```
ip prefix-list abc permit 35.0.0.0/8
```

In the following example, BGP process only accepts prefix with length ranges from /8 to /24:

```
router bgp
network 101.20.20.0
filter * in prefix max24
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
!
```

In the following configuration, the router filters routes from all interfaces, it only accepts routes with prefix from 8 to 24:

```
router bgp 12
filter * in prefix-list max24
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
```

Here are some other examples of configuration of prefix lists

The following example: permits routes with prefix length no more than 24 in network 192/8:

```
ip prefix-list abc permit 192.0.0.0/8 le 24
```

The following example: denies routes with prefix length of more than 25 in network 192/8:

```
ip prefix-list abc deny 192.0.0.0/8 ge 25
```

The following example: permits routes with prefix length of more than 8 yet less than 24 in all address space:

```
ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

The following example: denies all routes with prefix length of more than 25 in all address space:

```
ip prefix-list abc deny 0.0.0.0/0 ge 25
```

This example: denies routes from network 10/8, because if the mask on class A network 10.0.0.0/8 is smaller or equal to 32 bit, all routes from that network will be denied:

```
ip prefix-list abc deny 10.0.0.0/8 le 32
```

The following example: denies routes with mask length of more than 25 in network 204.70.1.24:

```
ip prefix-list abc deny 204.70.1.0/24 ge 25
```

The following example: permits all routes:

```
ip prefix-list abc permit any
```

6.5.6 Example of BGP route aggregation

The following example illustrates how to create aggregation routes in BGP. It may be created by route redistribution or the using of conditional route aggregation function.

In the following example, command "redistribute static" is used to redistribute aggregation route 193.*.*:

```
ip route 193.0.0.0 255.0.0.0 null 0
```

```
!
```

```
router bgp 100
```

```
redistribute static
```

When there is at least one route in the routing table within the designated range, the following configuration will create an aggregation route in BGP routing table. The aggregation route will be considered to be from your AS, and has the "atomic" attribution, to indicate the possibilities of the loss of information.

```
router bgp 100
```

```
aggregate 193.0.0.0/8
```

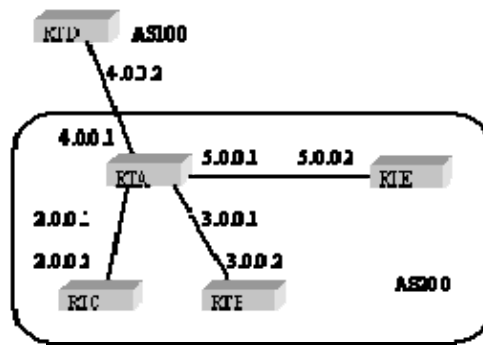
The following example not only creates an aggregation route 193.*.*, but also prohibit it to broadcast the more concrete routes to all the neighbours:

```
router bgp 100
```

```
aggregate 193.0.0.0/8 summary-only
```

6.5.7 Example of BGP route reflector

The following is an example of route reflector configuration. RTA, RTB, RTC, RTE all belong to the same autonomous system AS200, RTA serves as route reflector, RTB and RTC are route reflector clients, and RTE is normal IBGP neighbor. RTD belongs to AS100, and creates EBGP connection with RTA, the configuration is illustrated as the following:



RTA configuration:

```

interface s1/0
ip address 2.0.0.1 255.0.0.0
!
interface s1/1
ip address 3.0.0.1 255.0.0.0
!
interface s1/2
ip address 4.0.0.1 255.0.0.0
!
interface s1/3
ip address 5.0.0.1 255.0.0.0
!
router bgp 200
neighbor 2.0.0.1 remote-as 200 /*RTC IBGP*/
neighbor 2.0.0.1 route-reflector-client
neighbor 3.0.0.1 remote-as 200 /*RTB IBGP*/
neighbor 3.0.0.1 route-reflector-client
neighbor 5.0.0.1 remote-as 200 /*RTE IBGP*/
neighbor 4.0.0.2 remote-as 100 /*RTD EBGP*/
network 11.0.0/8
!
ip route 11.0.0.0 255.0.0.0 2.0.0.12

```

RTB configuration:

```

interface s1/0
ip address 3.0.0.2 255.0.0.0
!
router bgp 200
neighbor 3.0.0.1 remote-as 200 /*RTA IBGP*/
network 13.0.0/8
!
ip route 13.0.0.0 255.0.0.0 3.0.0.12

```

RTC configuration:

```

interface s1/0
ip address 2.0.0.2 255.0.0.0
!
router bgp 200
neighbor 2.0.0.1 remote-as 200 /*RTA IBGP*/
network 12.0.0.0/8
!
ip route 12.0.0.0 255.0.0.0 2.0.0.12

```

RTD configuration:

```

interface s1/0
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200 /*RTA EBGP*/
network 14.0.0.0/8
!
ip route 14.0.0.0 255.0.0.0 4.0.0.12

```

RTE configuration:

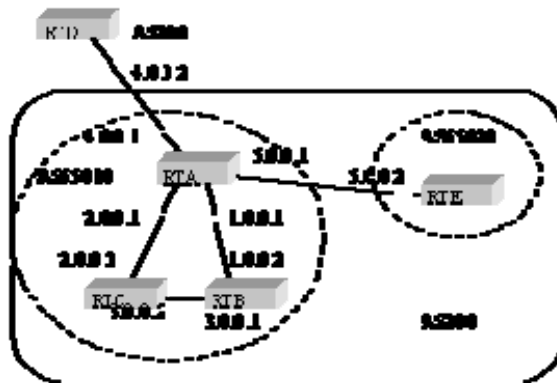
```

interface s1/0
ip address 5.0.0.2 255.0.0.0
!
router bgp 200
neighbor 5.0.0.1 remote-as 200 /*RTA IBGP*/
network 15.0.0.0/8
!
ip route 15.0.0.0 255.0.0.0 5.0.0.12

```

6.5.8 Example of BGP confederation

The following is the configuration of confederation. RTA, RTB, RTC create IBGP connections, and it belongs to a private autonomous system 65010; RTE belongs to another private autonomous system 65020; RTE and RTA establish internal EBGP connection of confederation; AS65010 AS65020 comprise the confederation, whose identifier is AS200; RTD belongs to autonomous system AS100, RTD establishes EBGP connection with autonomous system 200 through RTA.



RTA configuration:

```

interface s1/0
ip address 1.0.0.1 255.0.0.0
!
interface s1/1
ip address 2.0.0.1 255.0.0.0
!
interface s1/2
ip address 4.0.0.1 255.0.0.0
!
interface s1/3
ip address 5.0.0.1 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 1.0.0.2 remote-as 65010 /*RTB IBGP*/
neighbor 2.0.0.2 remote-as 65010 /*RTC IBGP*/
neighbor 5.0.0.2 remote-as 65020 /*RTE EBGP*/
neighbor 4.0.0.2 remote-as 100 /*RTD EBGP*/

```

RTB configuration:

```

interface s1/0
ip address 1.0.0.2 255.0.0.0
!
interface s1/1
ip address 3.0.0.1 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020

```

```
neighbor 1.0.0.1 remote-as 65010 /*RTA IBGP*/
neighbor 3.0.0.2 remote-as 65010 /*RTC IBGP*/
```

RTC configuration:

```
interface s1/0
ip address 2.0.0.2 255.0.0.0
!
interface s1/1
ip address 3.0.0.2 255.0.0.0
!
router bgp 65010
bgp confederation identifier 200
bgp confederation peers 65020
neighbor 2.0.0.1 remote-as 65010 /*RTA IBGP*/
neighbor 3.0.0.1 remote-as 65010 /*RTB IBGP*/
```

RTD configuration:

```
interface s1/0
ip address 4.0.0.2 255.0.0.0
!
router bgp 100
neighbor 4.0.0.1 remote-as 200 /*RTA EBGP*/
```

RTE configuration:

```
interface s1/0
ip address 5.0.0.2 255.0.0.0
!
router bgp 65020
bgp confederation identifier 200
bgp confederation peers 65010
neighbor 5.0.0.1 remote-as 65010 /*RTA EBGP*/
```

6.5.9 Example of route map with BGP group attribute

This section includes three examples of using route map with BGP community attribute.

In the first example, "route map set-community" is applied on the outgoing update of neighbor 171.69.232.50. Set the special community attribute with value "no-export" for the routes passing access list aaa, while other routes are broadcasted normally. This special community attribute will automatically prevent BGP speakers in AS200 from advertising the route outside of the autonomous system.

```
router bgp 100
neighbor 171.69.232.50 remote-as 200
neighbor 171.69.232.50 send-community
neighbor 171.69.232.50 route-map set-community out
```



```
!
route-map set-community 10 permit
match ip address aaa
set community no-export
```

```
!
route-map set-community 20 permit
```

In the second example, “route map set-community” is used for the outgoing update of neighbour 171.69.232.90. All routes originating from AS70 will insert value 200 into the community attribute 200, all other routes will just be advertised normally.

```
route-map bgp 200
neighbor 171.69.232.90 remote-as 100
neighbor 171.69.232.90 send-community
neighbor 171.69.232.90 route-map set-community out
```

```
!
route-map set-community 10 permit
match as-path test1
set community-additive 200 200
```

```
!
route-map set-community 20 permit
match as-path test2
```

```
!
ip aspath-list test1 permit 70$
ip aspath-list test2 permit .*
```

In the third example, selectively set the MED and local preference value of routes from neighbor 171.69.232.55 according to the community attribute value of the routes. All routes matching with community list com1 will be set with MED as 8000, this may include routes with community value “100 200 300” or “900 901”. These routes may have other attribute values.

All routes transmitting community list com2 will be set with the local preference value as 500.

All other routes will be set with the local priority value as 50. So, all the rest of the routes of neighbor 171.69.232.55 have the preference of 50.

```
router bgp 200
neighbor 171.69.232.55 remote-as 100
neighbor 171.69.232.55 route-map filter-on-community in
```

```
!
route-map filter-on-community 10 permit
match community com1
set metric 8000
```

```
!
route-map filter-on-community 20 permit
match community com2
set local-preference 500
```

```
!
route-map filter-on-community 30 permit
set local-preference 50
```

```
!  
ip community-list com1 permit 100 200 300  
ip community-list com1 permit 900 901  
!  
ip community-list com2 permit 88  
ip community-list com2 permit 90  
!
```

Chapter 7 Configure RSVP

7.1 Overview

This chapter explains how to configure RSVP. For details about RSVP Command, see “RSVP Command” in the “Network Protocol Command Reference”. For other document about Command, use index or type in Command in online help.

Try to understand RSVP before configuring it, which would be helpful for users. RSVP protocol can be used by a host to request a certain quality of business to an application data process. Routers can use RSVP protocol to transfer quality of service request and carry out reservation. RSVP request is going to be reserved on each node of data channels.

RSVP resource request is for single task data process. Logically, RSVP separates data sender and receiver, despite sender and receiver are in the same application process. RSVP is above IP protocol. Although RSVP does not transfer data, it belongs to Internet protocol (just like ICMP, IGMP or routing protocol). RSVP implementation is like routing protocol and managing protocol.

RSVP is not a routing protocol; however RSVP is able to assist a current and future routing protocol. A routing protocol decides how to transfer a data package, while RSVP deals with the Quality of Service (QoS) of the transferred data packages.

RSVP and WFQ (weighted fair queuing) or RED (random early detection) coordinate and function together. This kind of coordination contains two major concepts: use the RSVP flow between two ends, and use WFQ dialog between two routers.

7.2 RSVP Configuration Task List

- Enable a RSVP on a Router
- Start RSVP in a IP Phone Module Configuration
- Use RSVP to configure Command
- Configure TOS and Precedence for RSVP flow
- Use access—list in RSVP module

7.3 RSVP Configuration Task

7.3.1 Enable a RSVP on a Router

To enable RSVP on a router, users must configure the interface for starting RSVP, which can be realized by configure Command with interface on the RSVP. When the above configuration is done, RSVP protocol is able to work on these interfaces.

Configure Network interface with RSVP and use the following Commands in interface configurations:

Command	Function
ip rsvp bandwidth [<i>interface-kbps</i>] [<i>single-flow-kbps</i>]	Configure Network interface with RSVP

Notes:

When using ip rsvp bandwidth Command, under default configuration (interface-kbps and single-flow-kbp), the max resource reservation for the whole port and resource reservation for single data process will be limited to just 75% of the port total resource.

7.3.2 Start RSVP in a IP Phone Module Configuration

Before configuring our IP Phone and IP Phone module of the router to use Voice over IP, users have to enable RSVP to use RSVP to reserve resource.

RSVP Command has to be configured on ports that requires RSVP. That is because RSVP is disable by default. (See the last chapter)

IP phone disables QoS (default), therefore, users must configure dial-peer voip Command with enabling QoS Command.

To enable RSVP on interface f0/0, use the following commands in dial – peer Configuration mode of none IVR type:

Command	Function
req-qos { best-effort controlled-load guaranteed-delay }	Used Qos policy in dialpeer.

7.3.3 Use RSVP to configure Command

In this RSVP, users may use Command provided by the module to adjust RSVP. Adjustments including establishing RSVP conversation, RSVP path, path tear, resv, resv tear message transmission. This is going to be useful for users to test RSVP.

Users may use the following Commands in global configuration mode:

Command	Function
ip rsvp local session session-ip-address session-dport {tcp udp}	By setting this Command, users may configure a new RSVP dialog, which can be used by other Commands.
ip rsvp local sender session-id sender-ip-address sender-sport [bandwidth] [burst-size]	Users may send path message with this Command, whose no form may send path tear message.
ip rsvp local reservation session-id sender-ip-address sender-sport [guarantee load] [bandwidth] [burst-size]	Users may send resv message with this Command, whose no form may send resv tear message.

7.3.4 Configure TOS and Precedence for RSVP flow

To obtain better reservation results, users may use Commands offered by RSVP module to configure TOS and Precedence for RSVP. When RSVP flow is over the reserved range, the Command configures a higher TOS. When RSVP flow is within the reserved range, the command configures a lower TOS. So does Precedence.

Users may use the following Command in interface configuration mode:

Command	Function
ip rsvp tos {conform exceed} <i>tos-value</i>	This Command can be used to configure the reserved TOS options.
ip rsvp precedence {conform exceed} <i>precedence-value</i>	This Command can be used to configure the reserved precedence options.

7.3.5 Use access-list in RSVP module

When users are configuring RSVP on a router, they are able to use access-list to accept or reject communication with certain hosts or routers.

Command	Function
ip rsvp neighbor <i>access-list-name</i>	With this function, users may configure the following Commands under interface configuration mode.

Chapter 8 Congiuring PBR

8.1 Overview

This section describe how to configure PBR. PBR is the abbreccation of Policy Based Routing. PBR make the user have the ability to route ip packet according some policy other than dynamic routing protocol. We currently support the following policy: based on the length of ip packet, source ip address. You can set gateway or outgoing interface for packets matching the policy. PBR can support load balance.

The rule for PBR selecting nexthop is following :

- If set ip next-hop is configured, and the gateway is reachble, the gateway will be used. If multiple gateway is configured, use the first reachable gateway, if load-balance key word is used, the load balance is used between these gateways.
- If set interface is configured, and the outgoing interface is routabale(interface protocol up, and ip address is confured), use the outgoing interface. If multiple outgoing interfaces are configured, first routable interface will be used. If load-balance key word is used, the load balance is used between these interface. If both set ip next-hop and set interface configured, , use set ip next-hop first.
- 3.set ip default next-hop or set default interface won't be used untill routing lookup failed.

8.2 PBR Configuration Task List

If you want to use PBR, the following configuration is needed:

- Create standard access-list(optional)
- Creat route-map
- Apply route-map on interface

8.3 PBR Configuration Task

8.3.1 Create standard access-list

To create access-list, following the step bellow:

Command	Function
ip access-list stand <i>net1</i>	Enter access-list configurtion mode.

8.3.2 Create route-map

To create route-map, following the step bellow:

Command	Function
route-map pbr	Enter route-map configuration.
match ip address <i>access-list</i>	Configure matching policy.
match length <i>min_length max_length</i>	Configure matching policy.
set ip [default] next-hop <i>A.B.C.D</i>	Set gateway.
set [default] interface <i>interface_name</i>	Set outgoing interface.

8.3.3 Apply route-map on interface

To enable PBR on interface, following the step bellow:

Command	Function
interface <i>interface_name</i>	Enter interface configuration mode.
ip policy route-map <i>route-map_name</i>	Apply PBR on interface.

8.3.4 Debug PBR

To debug PBR, following the step bellow:

Command	Function
debug ip policy	To debug PBR.

8.4 PBR configuration example

router configure

```

!
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
no ip directed-broadcast
ip policy route-map pbr
!
interface FastEthernet0/0.13
ip address 13.1.1.3 255.255.255.0
no ip directed-broadcast
encapsulation dot1Q 13
bandwidth 100000
delay 1
!
interface FastEthernet0/0.14
ip address 14.1.1.3 255.255.255.0

```

```
no ip directed-broadcast
encapsulation dot1Q 14
!
interface Serial0/0
ip address 11.1.1.1
no ip directed-broadcast
!
ip access-list standard net1
permit 10.1.1.2 255.255.255.255
!
ip access-list standard net2
permit 10.1.1.4 255.255.255.255
!
ip access-list standard net3
permit 10.1.1.21 255.255.255.255
!
route-map pbr 10 permit
match ip address net1
set ip next-hop 13.1.1.99
!
route-map pbr 20 permit
match ip address net2
set ip next-hop 14.1.1.99
!
route-map pbr 30 permit
match ip address net3
set ip next-hop 13.1.1.99 14.1.1.99 load-balance
!
route-map pbr 40 permit
set ip default next-hop 13.1.1.99
```

configure explanation

Policy routing is enabled on interface f0/0. For packets originated from 10.1.1.2, the gateway is 13.1.1.99 if 13.1.1.99 is reachable, if 13.1.1.99 isn't reachable, destination base routing is used. For packets from 10.1.1.21, route-map pbr 30 is used, for load-balance key word is used, both 13.1.1.99 and 14.1.1.99 will be used as the gateway.

Chapter 9 Configuring DNS

9.1 Overview

DNS is Domain Name System for short, DNS is a distributing database using in TCP/IP application.. It can provide the translation of host name and IP address, some information about email and hosts.

The name DNS is used in the TCP/IP network, such as Internet and it orientates hosts and service according to friendly name. When the DNS name is input, the system can translate it into relative information such as IP address.

In DNS system, DNS Resolver equals to a client of DNS Server. The application can get relative information by accessing DNS Server. The base of this information is: getting the IP address according to a host name or getting the host name according to a IP address.

Dynamic DNS Resolver is used in the condition of dynamic IP addresses. Dynamic DNS Resolver can register the information about Host/address to DNS Server autotly, when the IP address changes, it can send updating message to DNS Server and the DNS Server will update its database.

9.1.1 DNS Application

DNS has abroad application:

- Provide translating host name to IP address for ping、telnet and traceroute.
- Provide translating IP address to host name for telnet. When traceroute gets each IP address, it can get the name of the address.
- When IP address of client changes, it can update the address in primary server.

9.1.2 DNS Term

- DNS Resource Record(RR):

Information, which may be empty. The set of resource information associated with a particular name is composed of separate resource records (RRs). The order of RRs in a set is not significant, and need not be preserved by name servers, resolvers, or other parts of the DNS.

- Starting Organism of Authorization (SOA)

A record is used to designated the starting point of the area. The record contains the domain name, e-mail address of the domain administrator and the settings about how to enable the DNS server to update the domain data files.

- Common types of resource records:

Parameter	Description
A	A host address.
CNAME	Identifies the canonical name of an alias.
HINFO	Identifies the CPU and OS used by a host.
MX	Identifies a mail exchange for the domain. See [RFC-974 for details.
NS	The authoritative name server for the domain.
PTR	A pointer to another part of the domain name space.
SOA	Identifies the start of a zone of authority.

- DNS Zone:

In general, the DNS database can be divided into different resource records and each record is called a zone. A zone can include the resource record of all the zones or parts of a zone. A zone is divided into several child zones to simplify the management. After using this distributing frame, the administrator can manage every child zone effectively when the domain name extends.

- Authoritative name server:

The DNS Server which manages the RR is named authoritative name server. Every server can be an authoritative name server or many.

- Primary server and slave server:

In order to ensure the high trustiness, DNS requests use many name servers to support every zone. The RR of every zone updates to a primary server manually or automatically. The primary server can be an authoritative name server having one or more zones. The other servers (named master DNS server) are standby servers servicing for the same zone, and this can avoid some instances when the primary server is abnormal. Master servers make their databases up-to-date by communicating to the primary server. Copying the zone files to many name servers is named zone exchange.

9.2 DNS Configuration Task List

This module realizes the DNS Resolver only and the DNS Server is not the range of this module.

- Enables DNS-based host name-to-address translation
- Specify the IP address of a domain name server
- Set a default domain name
- Defines a list of domains
- Defines static host name-to-address mapping
- Specify times to retry a DNS query

- Specify timeout waiting for response to a DNS query
- Delete the mapping of a host name to IP address in cache
- Specify the IP address of a primary server
- Enable update function of dynamic DNS
- Set the period of DNS update
- Bind the domain name to a IP address or IP address of interface
- The function of information showing or debug showing

9.3 DNS Configuration Task

9.3.1 Enables DNS-based host name-to-address translation

That is,make it query the hosts by name or address. This modual enable DNS lookup by default.

In congure use the following command:

Command	Function
ip domain lookup	Eable DNS lookup.
no ip domain lookup	Disable DNS lookup.

9.3.2 Specify the IP address of a domain name server

It may assign serveral name servers,but can only appoint six at most.The name server assigned before will be queried earlier. When we use the no format without any parameter,it express for delete all the name servers.

In congure use the following command:

Command	Function
ip domain name-server <i>ip-address</i>	Set a domain name server
no ip domain name-server <i>ip-address</i>	Delete domain name server

Note:

- no ip domain name-server *ip-address* Express delete a domain name server which IP address is *ip-address*.
- no ip domain name-server Express delete all the domain name servers.

9.3.3 Set a default domain name

We can complete the host name by a default domain name. But the default domain name is useful only when there is no domain list.

In configure use the following command:

Command	Function
ip domain name <i>name</i>	Specify a default domain name.
no ip domain <i>name</i>	Delete the default domain name.

9.3.4 Defines a list of domains

The DNS Resolver completes a host name by the domain list, it can try the domain list in turn until it find the host or all the domain lists are tried. The domain name will not be used if a domain list exists. We can set six domain lists at most.

In configure use the following command:

Command	Function
ip domain list <i>name</i>	Define a domain list.
no ip domain list <i>name</i>	Delete a domain list.

Notes:

- `no ip domain list name` Express delete a domain name named name.
- `no ip domain list` Express delete all the domain names.

9.3.5 Defines static host name-to-address mapping

Any IP address can correspond to a name, and the same name can correspond to many IP addresses. By doing this, the command such as **telnet**, **ping** can use the names directly.

In configure use the following command:

Command	Function
ip host <i>name address1</i> [<i>address2, ...</i>]	Map a name to some IP address.
no ip host <i>name</i> [<i>address1, ...</i>]	Delete a map.

Example: the following express mapping a name to several IP addresses

```
router_config# ip host djh 172.16.20.209
router_config# ip host djh 172.16.20.210
```

or:

```
router_config# ip host djh 172.16.20.209 172.16.20.210
```

If you want to delete, you can delete a IP address or delete many addresses or delete the host.

```

router_config# no ip host djh 172.16.20.209          /*delete a IP address mapping to a host
name djh*/
router_config# no ip host djh 172.16.20.209 172.16.20.210
/*delete 2 IP address mapping to a host name djh*/
router_config# no ip host djh                    /*delete the host named djh*/

```

9.3.6 Specify times to retry a DNS query

When sending failing or not receiving the correspond, it can send again. By default , the retry times is 3 (times). You can modify the retry times when needing.

In congure use the following command:

Command	Function
ip domain retry <i>count</i>	Set retry times
no ip domain retry	Restore to the default

9.3.7 Specify timeout waiting for response to a DNS query

When sending failing or not receiving the correspond, it can send again. This time is the interval time between two sending.By default , the timeout value is 2 (seconds). You can modify the retry times when needing.

In congure use the following command:

Command	Function
ip domain timeout <i>seconds</i>	Set timout value.
no ip domain timeout	Restore to the default.

9.3.8 Delete the mapping of a host name to IP address in cache

The host having been queried will be set in cache. We can delete one or all of the hosts in cache. The command can't delete the static mapping of host and IP address.

In manager use the following command:

Command	Function
clear ip host <i>name</i>	Delete a host in cache.
clear ip host *	Delte all the hosts in cache.

9.3.9 Specify the IP address of a primary server

You can only specify one primary server, if you specify another,it will replace the one earlier.

In congure use the following command:

Command	Function
ip domain primary-server <i>address</i>	Set a primary server.

no ip domain primary-server	Delete the primary server.
------------------------------------	----------------------------

9.3.10 Enable update function of dynamic DNS

The router having static IP address doesn't need the function, so you can use the no format to disable domain dynamic. By default, the function is disable.

In congure use the following command:

Command	Function
ip domain dynamic enable	Enable domain dynamic.
no ip domain dynamic enable	Disable domain dynamic.

9.3.11 Set the period of DNS update

In congure use the following command:

Command	Function
ip domain dynamic period <i>seconds</i>	Set time of updating period.
no ip domain dynamic period	Restore to the default.

9.3.12 Bind the domain name to a IP address or IP address of interface

This command doesn't support binding the second IP address to a domain name.

After the command is using, the changing of the IP address of interface will update the mapping in the primary server, that is, dynamic domain updating.

In general, it needs to update in the following cases:

- When the router reboots, it should register to the primay server at once.
- By clock
- If the binding command is used, it will add or delete a mapping in primary server.
- When the IP address of a interface changes
- When the interface having been binded is shut up or is deleted

In congure use the following command:

Command	Function
ip domain bind <i>name interface number</i>	Bind the domain name to the primary IP address of interface (Note:an interface can only correspond to one domain name, when you use another,the later will replace for the earlier.)
ip domain bind <i>name interface number singly</i>	Bind the domain name to the primary IP address of interface, and delete all the hosts named <i>name</i>

	in primary server
no ip domain bind <i>name interface number</i>	Delete the mapping of the domain name to the primary IP address of interface
ip domain bind <i>name ip_addr</i>	Bind the domain name to a IP address. (Note: the same domain name can correspond to several IP addresses.)
ip domain bind <i>name ip_addr singly</i>	Bind the domain name to a IP address, and delete all the hosts named <i>name</i> in primary server
no ip domain bind <i>name ip_addr</i>	Delete the mapping of the domain name to the IP address
no ip domain bind <i>name</i>	Delete all the hosts named <i>name</i> in the primary server

Notes:

If the command **ip domain dynamic enable** or **ip domain primary-server** is not been configurated , then command **ip domain bind** and **no ip domain bind** will not be successful, and will not be in flash memory or be deleted from flash memory.

To the command of domain dynamic,the router will register to the primary server autoly,but if the interface shut down, the communication to primary server will fail,that is,it can't register successly. In order that the register goes along after the interface shut up, the modual set a much bigger timeout and retry,so the configuring of retry and timeout go into effect after 30 seconds when the router reboots.

On the side, If we bind a domain name with an interface,when the ip address of the interface changed and makes the communication to the primary server fail,but after a while,it can restore, at this instance, we can enhance the times of retry and the seconds of timeout so that it can update successfully.

9.3.13 The function of information showing or debug showing

The system can show some information such as the default domain name,domain list,the host in the cache and so on.What's more, it can show information when running. This information can help us to resolve some problems.

In manager use the following command

Command	Function
show ip hosts	Show the default domain name,domain list,the host in the cache and so on.
show ip hosts detail	It show some information of the applications using the DNS Resolver unblocking such as the queue ID(or address of a callback) an time before ttl.
debug ip domain	Show the debug information of this modual.

9.4 Examples of BGP configuration

The following configure can query and update.

Chapter 10 PeanutHull Configuration

10.1 DHRP Overview

The Dynamic Host Register Protocol (DHRP) is a way to bind the domain name and the dynamic IP address. The protocol works in this way: the client is allowed to submit its IP address to the server and selects the domain name record, while the server checks whether the client has the domain permission, modifies corresponding DNS records, maintains dynamically-registered domain names when the client is online and automatically deletes these domain names when the client is offline.

The protocol consists of the management protocol and the update protocol, the former providing services such as account application/modification/login and domain name registration/application/modification, and the latter providing services such as dynamic registration update and online state monitoring.

10.2 PeanutHull Commands

The DHRP client program can run on the modules of our router. As to the DHRP server program it has no connection with the modules of our router.

10.2.1 Entering DHRP Configuration State

To add the configuration group of a designated name and enter the DHRP configuration state, run the following commands in global mode:

Command	Purpose
ip peanuthull <i>name</i>	Adds the configuration group of a designated name and enters the DHRP configuration state.
no ip peanuthull <i>name</i>	Deletes the configuration group of a designated name.

10.2.2 Activating DHRP-Based DNS

To activate DHRP-based Domain Name Solution (DNS) to enable automatic server lookup and registration, run the following commands in DHRP configuration mode:

Command	Purpose
enable	Activates DHRP-based DNS.
no enable	Disables DHRP-based DNS.

10.2.3 Designating the Address of the Server

You can designate up to six domain name servers. The first-designated server will be first queried. If it cannot be found, the next server is then queried.

Run the following commands in DHRP configuration mode:

Command	Purpose
server <i>name</i>	Designates the name of a server.
no server	Deletes the name of a server.

10.2.4 Designating a Default Domain Name

To designate a default domain name, run the following commands in DHRP configuration mode:

Command	Purpose
domain <i>name</i>	Designates a default domain name.
no domain	Deletes a default domain name.

10.2.5 Configuring a Connection Port for DHRP Query

If the servers are different, their corresponding port numbers are also different when you set an ID for a connection port.

Run the following corresponding command to designate or delete a port ID in DHRP configuration mode:

Command	Purpose
port <i>num</i>	Designates the port ID.
no port	Deletes the port ID.

10.2.6 Setting a Username for Registration

To set the username, run **username name**. The username which requires during registration need be maintained at the PeanutHull-designated website.

Run the following relative command to set or delete a username:

Command	Purpose
username <i>name</i>	Sets a username.
no username	Deletes a username.

10.2.7 Setting a Password for Registration

To set the password, run **password name**. The password which requires during registration need be maintained at the PeanutHull-designated website.

Run the following relative command to set or delete a password:

Command	Purpose
password <i>password</i>	Sets a password.
no password	Deletes a password.

10.2.8 Binding IP Address and Domain Name

To bind the local IP address or the port to the registered domain name, run the following relative command in DHRP configuration mode:

Command	Purpose
bind interface <i>number</i>	Binds the interface.
bind ip_addr	Binds the IP address.

Note:

Multiple IP addresses may exist on a port, so the system need select the primary IP address. If the port has no IP address, the PeanutHull client cannot be started; if the IP address is allocated to the port or the IP address of the port changes, the PeanutHull client will be re-registered.

10.2.9 Software Module Display and Debug Display

The system can display data which is in specific state, such as the default domain name and some traits about domain name. These information helps to know the system's resource and to resolve the network problem.

Command	Purpose
show ip peanuthull	Displays the default domain name, domain server, host name and the running state of the client.
debug ip domain	Displays the debug information.

10.2.10 PeanutHull Configuration Example

The following example shows how to configure PeanutHull to enable domain name query and dynamic update on the DNS server.

Minimum configuration:

```
!  
ip peanuthull aaa  
server hph016.oray.net  
  username bdtest  
  password bdtest  
  port 5050  
  bind interface f0/2  
enable!
```

Minimum configuration:

```
!  
ip domain name-server 192.168.1.3  
ip domain dynamic enable  
ip domain primary-server 172.16.20.212  
ip domain bind www.bind1.edu.cn interface e1/1  
!
```

Normal configuration:

```
!  
ip domain name aaa.com.cn  
ip domain list com.cn  
ip domain list edu.cn  
ip host djh 172.16.20.209 10.0.0.90  
ip domain name-server 192.168.1.3  
ip domain name-server 172.16.20.212  
ip domain timeout 3  
ip domain retry 2  
ip domain dynamic enable  
ip domain primary-server 172.16.20.212  
ip domain dynamic period 7200  
ip domain bind www.test.edu.cn 202.10.10.56  
ip domain bind www.bind1.edu.cn interface e1/1  
ip domain bind djh.edu.cn 202.10.10.45 singly  
ip domain bind right.edu.cn interface loopback100 singly  
!
```