Routing Configuration Commands

Table of Contents

Chapter 1 RIP Configuration Commands

1.1 RIP Configuration Commands

RIP Configuration Commands Include:

- auto-summary
- default-information originate
- default-metric
- ip rip authentication
- ip rip message-digest-key
- ip rip passive
- ip rip password
- ip rip receive version
- ip rip send version
- ip rip split-horizon
- neighbor
- network
- offset
- router rip
- timers expire
- timers holddown
- timers update
- validate-update-source
- version
- distance
- filter
- maximum-count
- show ip rip

- show ip rip database
- show ip rip protocol
- debug ip rip database
- debug ip rip protocol

1.1.1 auto-summary

To activate the automatic summarization function, use the auto-summary command. To turn off this function, use the no form of this command.

auto-summary

no auto-summary

parameter

This command has no parameter or keywords.

default

Enabled by default

command mode

router configuration

instruction

Routing summarization reduces the amount of routing information in the routing tables and switching information. Routing Information Protocol(RIP) do not support subnet mask, therefore, if it is forwarded to subnets, routing possibly cause ambiguity. RIP Version 1 always uses routing summarizarion. If using RIP Version 2, you can turn off routing summarization by using the no auto-summary command. When routing summarization is off,. Subnets are advertised..

example

To specify RIP version on Serial 1/0 as RIP Version 2 and turn off routing summarization function router rip
version 2
no auto-summary

related commands

version

1.1.2 default-information originate

To generate a default route, use the default-information originate command. To disable this function , use the no form of this command..

default-information originate

no default-information originate

parameter

none

default

disable this function by default

command mode

router configuration

instruction

After the default-information originate command is activated, the routing information(0.0.0.0/0) is accompanied when send routing updating.

example

When send routing updating information, the default routing(0.0.0.0/0) is accompanied.

router rip
version 2
network 172.68.16.0
default-information originate
ip route default f0/0

1.1.3 default-metric

To set default metric values for import routing, use the default-metric command. To return the default stata, use the no form of this command..

default-metric number

no default-metric

parameter

	parameter	description	
	number	Default metric value. It has a value from 1 to 16.	

default

Built-in, automatic metric translations, as appropriate for each routing protocol

command mode

router configuration

instruction

The default-metric command is used to set default routing metric used in importing routing of other routing protocols into Rip packets. When import routing of other protocols, use the specified default routing by default-metric if no specified routing metric.

example

The following example shows a routing switch in autonomous system 119 using both the RIP and the OSPF routing protocols. The example advertises OSPF-derived routes using the RIP protocol and assigns the OSPF-derived routes a RIP metric of 8.

```
router rip default-
metric 8 redistribute
ospf 119
```

related commands

redistribute

default-information originate

1.1.4 ip rip authentication

To specify the type of authentication used in Routing Information Protocol (RIP) Version 2 packets, use the ip rip authentication mode command in interface configuration mode. To restore plain text authentication, use the no form of this command.

ip rip authentication {**simple** | **message-digest**}

no ip rip authentication

parameter

parameter	description
simple	Plain text authentication.
message-digest	Keyed Message Digest 5 (MD5) authentication.

default

disabled

command mode

interface configuration mode

instruction

RIP Version 1 does not support authentication.

example

The following example configures the interface to use MD5 authentication:

```
ip rip authentication message-digest
```

related commands

ip rip password

ip rip message-digest-key

1.1.5 ip rip message-digest-key

To activate Routing Information Protocol (RIP) Version 2 packets authentication and specify Message Digest 5 (MD5) authentication used on the interface, use the ip rip message-digest-key md5 command. To prevent the authentication, use the no form of this command

ip rip message-digest-key *key-id* **md5 password**

no ip rip message-digest-key [*key-id*]

parameter

parameter	description
key-id	A key identifier
password	The specified password

default

MD5 authentication is invalid.

command mode

interface configuration mode

instruction

No authentications are carried out on interface if no passwords are configured using the ip rip message-digest-key key-id md5 password command.

example

The following example configures interface to receive and send MD5 authentication packets that belong to password ‘mykey’:

ip rip message-digest-key 4 md5 mykey

related commands

ip rip authentication

1.1.6 ip rip passive

To cancel the routing switch to send routing updating on interface, use the ip rip passive command. To reactivate the routing updating, use the no form of this command.

ip rip passive

no ip rip passive

parameter

none

default

send routing updates on the interface

command mode

interface configuration mode

instruction

If you cancel routing updating on a certain interface, a specified subnetwork will keep on announcing to other interfaces, and the routing updating that from other routing switches can be continuedly accepted and dealt with on this interface.

example

The following example sends RIP packets updating to all interfaces that belong to the network 172.16.0.0 (except Ethernet interface 1/0):

interface ethernet 1/0

ip address 172.15.0.1 255.255.0.0

ip rip passive

router rip

network 172.16.0.0

related commands

none

1.1.7 ip rip password

To activate Routing Information Protocol (RIP) Version 2 packets authentication and specify the plain text authentication used on the interface, use the ip rip password command Use the no form of this command to prevent authentication.

ip rip password *password*

no ip rip password *password*

parameter

parameter	description
password	the specified password

default

no authenctication

command mode

interface configuration mode

instruction

No authentications are carried out on interface without using the ip rip password command to configure any password.

example

The following example configures interface to receive and send any plain text authentication packet that belong to password ‘mykey’

ip rip password mykey

related commands

ip rip authentication

1.1.8 ip rip receive version

To specify a Routing Information Protocol (RIP) version to receive on specified interface, use the ip rip receive version command in interface configuration mode. To follow the global version rules, use the no form of this command.

ip rip receive version [**1**] [**2**]

no ip rip receive version

parameter

parameter	description
1	(Optional) Accepts only RIP Version 1 packets on the interface.
2	(Optional) Accepts only RIP Version 2 packets on the interface.

default

Accepts RIP Version 1 and RIP Version 2 packets

command mode

interface configuration mode

instruction

Use this command to override the default behavior of RIP as specified by the version command. This command applies only to the interface being configured. You can configure the interface to receive both RIP versions.

example

The following example configures the interface to receive both RIP Version 1 and Version 2 packets:

ip rip receive version 1 2

The following example configures the interface to receive only RIP Version 1 packets:

ip rip receive version 1

related commands

ip rip send version

version

1.1.9 ip rip send version

To specify a Routing Information Protocol (RIP) version to send on specified interface, use the ip rip send version command in interface configuration mode. To follow the global version rules, use the no form of this command.

ip rip send version [**1** | **2** | **compatibility**]

no ip rip send version

parameter

parameter	description
1	(Optional) Sends only RIP Version 1 packets out the interface.
2	(Optional) Sends only RIP Version 2 packets out the interface.
compatibility	(Optional) Broadcasts only RIP Version 2 packets out the interface.

default

Sends only RIP Version 1 packets

command mode

interface configuration mode

instruction

Use this command to override the default behavior of RIP as specified by the version command. This command applies only to the interface being configured. the interface can be configured to receive both RIP Version 1 and Version 2 packets

example

The following example configures the interface to send only RIP Version 1 packets out the interface:

ip rip send version 1

The following example configures the interface to send only RIP Version 2 packets out the interface:

ip rip send version 2

related commands

ip rip receive version

version

1.1.10 ip rip split-horizon

To enable the split horizon mechanism, use the ip split-horizon command in interface configuration mode. To disable the split horizon mechanism, use the no form of this command.

ip rip split-horizon

no ip rip split-horizon

parameter

none

default

Default behavior varies with media type.

command mode

interface configuration mode

instruction

For all interfaces except those for which either Frame Relay or Switched Multimegabit Data Service (SMDS) encapsulation is enabled, the default condition for this command is ip split-horizon; in other words, the split horizon feature is active. If the interface configuration includes either the encapsulation frame-relay or encapsulation smds command, then the default is for split horizon to be disabled.

Note: For networks that include links over X.25 packet switched networks (PSNs), the neighbor routing switch configuration command can be used to defeat the split horizon feature. You can as an alternative explicitly specify the no ip split-horizon command in

your configuration. However, if you do so you must similarly disable split horizon for all routing switches in any relevant multicast groups on that network.

If split horizon has been disabled on an interface and you want to enable it, use the ip split-horizon command to restore the split horizon mechanism.

Note: In general, changing the state of the default for the ip split-horizon command is not recommended, unless you are certain that your application requires a change in order to properly advertise routes. If split horizon is disabled on a serial interface (and that interface is attached to a PSN), you must disable split horizon for all routing switches and access servers in any relevant multicast groups on that network.

example

The following simple example disables split horizon on a serial link. The serial link is connected to an X.25 network.

```
interface serial 1/0
encapsulation x25 no
ip rip split-horizon
```

related commands

neighbor

1.1.11 neighbor

To define a neighboring routing switch with which to exchange routing information, use the neighbor command in routing switch configuration mode. To remove an entry, use the no form of this command.

neighbor *ip-address*

no neighbor *ip-address*

parameter

parameter	description
ip-address	IP address of a peer routing switch with which routing information will be exchanged.

default

No neighboring routing switches are defined.

command mode

router configuration

instruction

This command permits the point-to-point (nonbroadcast) exchange of routing information in order to meet special requirements of the specified nonbroadcast network.

example

In the following example, the neighbor routing switch configuration command permits the sending of routing updating to specific neighbors.

router rip

neighbor 131.108.20.4

related commands

network

1.1.12 network

To specify a list of networks for the Routing Information Protocol (RIP) routing process, use the network command in routing switch configuration mode. To remove an entry, use the no form of this command.

network *network-numbe* <*network-mask*>

no network *network-number* <*network-mask*>

parameter

parameter	description
Network-number	IP address of the network of directly connected networks.
Network-mask	(optional) IP mask of the network of directly connected networks

default

No networks are specified.

command mode

router configuration

instruction

The network number specified must not contain any subnet information. There is no limit to the number of network commands you can use on the routing switch. RIP routing updates will be sent and received only through interfaces on this network.

RIP sends updates to the interfaces in the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP updates.

example

The following example defines RIP as the routing protocol to be used on all interfaces connected to networks 128.99.0.0 and 192.31.7.0:

router rip
network 128.99.0.0
network 192.31.7.0

related commands

router rip

1.1.13 offset

To add an offset to incoming and outgoing metrics to routes learned via Routing Information Protocol (RIP), use the offset command in routing switch configuration mode. To remove an offset list, use the no form of this command.

offset {*type number* | *****} {**in | out**} *access-list-name* **offset**

no offset {*type number* | *****} {**in | out**}

parameter

parameter	description
In	Applies the access list to incoming metrics.
Out	Applies the access list to outgoing metrics.
access-list-name	Standard access list number to be applied. Access list number 0 indicates all access lists. If offset is 0, no action is taken.
offset	Positive offset to be applied to metrics for networks matching the access list.
type	Interface type to which the offset list is applied.
number	(Optional) Interface number to which the offset list is applied.

default

This command is disabled by default.

command mode

router configuration

instruction

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

example

In the following example, the routing switch applies an offset of 10 to routes learned from Ethernet interface 1/0:

offset ethernet 1/0 in 21 10

1.1.14 router rip

To configure the Routing Information Protocol (RIP) routing process, use the router rip command in global configuration mode. To turn off the RIP routing process, use the no form of this command.

router rip

no router rip

parameter

none

default

No RIP routing process is defined.

command mode

global configuration mode

instruction

User should first enable RIP to enter router configuration mode to configure all global parameters of RIP. However, it is regardless whether RIP is enabled if you configure parameters related to interface,

example

The following example shows how to begin the RIP routing process:

router rip

related commands

network (RIP)

1.1.15 timers expire

To adjust RIP network timers, use the timers expire router configuration command. To restore the default timers, use the no form of this command.

timers expire interval

no timers expire

parameter

parameter	description
expire	Interval of time in seconds after which a route is declared invalid; it should be at least three times the value of update. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters holddown. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. The default is 180 seconds.

default

180 seconds

command mode

router configuration

instruction

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network.

Note: The current and default timer values can be seen by the show ip rip command.

example

In the following example, if a routing switch is not heard from in 30 seconds, the route is declared unusable.

router rip

timers expire 30

1.1.16 timers holddown

To adjust RIP network timers, use the timers holddown routing switch configuration command. To restore the default timers, use the no form of this command.

timers holddown second

no timers holddown

parameter

parameter	description
second	Interval in seconds during which routing information regarding better paths is suppressed. It should be at least three times the value of update. A route enters into a holddown state when an update packet is received that indicates the route is unreachable. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets. When holddown expires, routes advertised by other sources are accepted and the route is no longer inaccessible. The default is 120 seconds.

default

120 seconds

command mode

router configuration

instruction

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network.

Note:

The current and default timer values can be seen by the show ip rip command.

example

In the following example, if a routing switch is not heard from in 30 seconds, the route is declared unusable.

router rip

timers holddown 30

1.1.17 timers update

To adjust RIP network timers, use the timers update routing switch configuration command. To restore the default timers, use the no form of this command.

timers update update

no timers update

parameter

parameter	description
update	Rate in seconds at which updates are sent. This is the fundamental timing parameter of the routing protocol. The default is 30 seconds.

default

30 seconds

command mode

router configuration

instruction

The basic timing parameters for RIP are adjustable. Since RIP is executing a distributed, asynchronous routing algorithm, it is important that these timers be the same for all routing switches and access servers in the network.

Note:

The current and default timer values can be seen by the show ip rip command.

example

In the following example, updates are broadcast every 5 seconds.

router rip timers

update 5

Note that by setting a short update period, you run the risk of congesting slow-speed serial lines; however, this is not a big concern on faster-speed Ethernets and T1-rate serial lines. Also, if you have many routes in your updates, you can cause the routing switches to spend an excessive amount of time processing updates.

1.1.18 validate-update-source

To have the software validate the source IP address of incoming routing updates for RIP routing protocols, use the validate-update-source routing switch configuration command. To disable this function, use the no form of this command.

validate-update-source

no validate-update-source

parameter

This command has no parameters or keywords.

default

Enabled

command mode

router configuration

instruction

This command is only applicable to RIP and IGRP. The software ensures that the source IP address of incoming routing updates is on the same IP network as one of the addresses defined for the receiving interface.

Disabling split horizon on the incoming interface will also cause the system to perform this validation check.

For unnumbered IP interfaces (interfaces configured as ip unnumbered), no checking is performed.

example

In the following example, a routing switch is configured to not perform validation checks on the source IP address of incoming RIP updates:

```
router rip
  network 128.105.0.0
  no validate-update-source
```

1.1.19 version

To specify a RIP version used globally by the routing switch, use the version routing switch configuration command. Use the no form of this command to restore the default value.

version {1 | 2}

no version

parameter

parameter	description
1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

default

The software receives RIP Version 1 and Version 2 packets, but sends only Version 1 packets.

command mode

router configuration

instruction

To specify RIP versions used on an interface basis, use the ip rip receive version and ip rip send version commands; or it will send RIP packets in terms of the global configuration version.

example

The following example enables the software to send and receive RIP Version 2 packets:

version 2

related commands

ip rip receive version

ip rip send version

1.1.20 distance

To define an administrative distance for RIP routes, use the distance command in routing switch configuration mode.

Distance weight <address mask <access-list-name>>

parameter

parameter	description
weight use 10 to 255	Administrative distance. An integer from 1 to 255. It is recommended to (The values 0 to 9 are reserved for internal use.) Routes with a distance value of 255 are not installed in the routing table.)
address	(Optional) Source IP address (in four-part, dotted decimal notation)
mask	(Optional) IP address mask (in four-part, dotted decimal notation) If a certain digit is 0, software will omit the corresponding value in the address.
access-list-name	(Optional) Named access list to be applied to incoming routing updates.

default

120

command mode

EXEC

instruction

Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. When the optional access list name or number is used with this command, it is applied when a network is being inserted into the routing table. This behavior allows filtering of networks according to the IP address of the routing switch that supplies the routing information.

example

The following example sets the administrative distance to 100 for the routing switch with the address 192.1.1.0/24.

router rip

distance 100 192.1.1.0 255.255.255.0

1.1.21 filter

To filter for RIP routes, use the filter command.

filter * in access-list {*access-list-name*}

filter * in gateway {*access-list-name*}

filter * in prefix { *prefix-list-name*}

filter type *number* **in access-list** {*access-list-name*}

filter type *number* **in gateway** {*access-list-name*}

filter type *number* **in prefix** {*prefix-list-name*}

no filter * in

no filter type *number* **in**

filter * out access-list {*access-list-name*}

filter * out gateway {*access-list-name*}

filter * out prefix { *prefix-list-name*}

filter type number out access-list {*access-list-name*}

filter type number out gateway {*access-list-name*}

filter type number out prefix {*prefix-list-name*}

no filter * out

no filter type *number* **out**

parameter

parameter	description
access-list-name	Standard IP access list name. This list defines networks of which are received or suppressed in routing update.
prefix-list-name	Standard IP prefix list name. This list defines networks of which are received or suppressed in routing update.
in/out	Applies access list for in/out routing update.
type	(Optional) Interface type
number	(Optional)Indicates number of interface on which applies the access list for in/out routing update. If no interface is defined, the access list is applicabale to all in/out routing update.

default

disabled

command mode

EXEC

instruction

Filter the route that are to be sent and received.If you use the access-list command to configure access list for dynamic routing protocol, you shoul use the standard access list.

example

The following example filter route 10.0.0.0/8 from interface s2/1:

router rip
filter s2/1 out access-list mylist
ip access-list standard mylist
deny 10.0.0.0 255.0.0.0

1.1.22 maximum-count

To configure the maximum route count in local RIP routing table, use the maximum-count command. Use the no form of this command to restore default setting.

maximum-count *number*

no maximum-count

parameter

parameter	description
number	The maximum route count to be confgirued, in the range from 512 to 4096.

default

1024

command mode

router configuration

instruction

Use this command to configure the maximum route count in local RIP routing table. When routes in local routing table exceed the maximum value, no routes will be added to routing table.

example

The following example configures 2000 as the maximum route count in the local RIP routing table:

router rip maximum-
count 2000

related commands

none

1.1.23 show ip rip

To display RIP main information, use the show ip rip command.

show ip rip

parameter

none

default

none

command mode

EXEC

instruction

User can see the current configuration status about RIP according to the output of this command.

example

The following example displays configuration parameter information about RIP:

router#show ip rip
RIP protocol: Enabled
Decided on the interface version
control AUTO-SUMMARY: Yes
Update: 30, Expire: 180, Holddown: 120
Distance: 120
default-metric: 1

The meaning of the above fields are as follows:

field	description
Enabled	Indicates current state of the active routing protocol process.
Distance	Indicates current administrative distance.

version	Indicates current version of the protocol.
AUTO-SUMMARY	Indicates whether to allow auto-summary or not.
Update	Interval of time at which updates are sent.
Holddown	Interval (in seconds) during which routing information regarding better paths is suppressed.
Expire	Interval of time after which a route is expired.
RIP default-metric	Default metric value during redistribute

1.1.24 show ip rip database

To display summary address entries in the Routing Information Protocol (RIP),use the show ip rip database command

show ip rip database

parameter

none

default

none

command mode

EXEC

instruction

Summary address entries will appear in the database from output of this command.

example

The following output shows a summary address entry:

router#show ip rip database
1.0.0.0/8 auto-summary
1.1.1.0/24 directly connected Loopback1
100.0.0.0/8 via 192.1.1.2 00:00:02
192.1.1.0/24 directly connected Serial2/1
192.1.1.0/24 auto-summary

The meanings of the following fields are as follows:

field	description

Network-number/network-mask	RIP routes
Summary/connected/via gateway	The corresponding RIP route types
interface	RIP directly connected and summary routes interface
time	refreshed time

1.1.25 show ip rip protocol

To display RIP protocol configuration information, use the show ip rip protocol command.

show ip rip protocol

parameter

none

default

none

command mode

EXEC

instruction

User can see the current RIP protocol configuration information from output of this command.

example

The following example displays RIP protocol configuration information:

```
router#show ip rip
protocol RIP is Active
  Sending updates every 30 seconds, next due in 30
  seconds Invalid after 180 seconds, holddown 120
  update filter list for all interfaces is:
  update offset list for all interfaces
  is: Redistributing:
  redistribute connect
  Default version control: send version 1, receive version 1 2
   Interface          Send          Recv
   Async0/0             1             1 2
```

FastEthernet0/0 1 1 2
Serial1/0 1 1 2
Ethernet1/1 1 1 2
Serial2/0 1 1 2
Serial2/1 1 1 2
Loopback1 1 1 2
Automatic network summarization is in effect Routing for Networks:
174.168.0.0/16
Distance: 120 (default is 120)

1.1.26 debug ip rip database

To monitor RIP routed events, use the debug ip rip database command.

debug ip rip database

parameter

none

default

none

command mode

EXEC

instruction

User can see some events of the current RIP routes from output of this command.

example

Thd following example monitors some events of the RIP routes:

router# debug ip rip database
RIP-DB: Adding summary route 192.1.1.0/24 <metric 0> to RIP database

The meanings of the above fields are as follows:

field	description
summary	Indicates the route type that added to the routing table
192.1.1.0/24	Indicates the route that added to the routing table
<metric 0>	Route metric value

1.1.27 debug ip rip protocol

To monitor RIP packets, use the debug ip rip protocol command.

debug ip rip protocol

parameter

none

default

none

command mode

EXEC

instruction

User can see the current content of RIP packets from the output of this command.

example

The following example monitors RIP packets:

router# debug ip rip protocol
RIP: send to 255.255.255.255 via
Loopback1 vers 1, CMD_RESPONSE,
length 24 192.1.1.0/0 via 0.0.0.0 metric 1.

The following output will be displayed when ran on the version 2:

RIP: send to 255.255.255.255 via
Loopback1 vers 2, CMD_RESPONSE,
length 24 192.1.1.0/24 via 0.0.0.0 metric 1

The meaning of the above fields are as follows:

field	description
Send/Recv	Indicates packets that are sent or received packets
to 255.255.255.255	Iindicates the destination address of IP packets
via Loopback1	Indicatesthe interface on which RIP packets that are sent and received.
vers 2	Indicates version of RIP packets that are sent and received.
CMD_RESPONSE/ CMD_REQUEST	Indicates type of the packet
length 24	Indicates length of packet.

192.1.1.0/24	Indicates destination network in routing informaiohti
via 0.0.0.0	Indicates next hop address.
metric	Route metric value

Chapter 2 OSPF Configuration Commands

2.1 OSPF Configuration Commands

OSPF Configuration Commands Include:

- area authenticaion
- area default-cost
- area range
- area stub
- area virtual-link
- debug ip ospf adj
- debug ip ospf events
- debug ip ospf flood
- debug ip ospf lsa-generation
- debug ip ospf packet
- debug ip ospf retransmission
- debug ip ospf spf
- debug ip ospf tree
- default-information originate
- default-metric
- distance ospf
- filter
- ip ospf cost
- ip ospf dead-interval
- ip ospf hello-interval
- ip ospf message-digest-key
- ip ospf network
- ip ospf passive

- ip ospf password
- ip ospf priority
- ip ospf retransmit-interval
- ip ospf transmit-delay
- neighbor
- network area
- redistribute
- router ospf
- show ip ospf
- show ip ospf border-routers
- show ip ospf database
- show ip ospf interface
- show ip ospf neighbor
- show ip ospf virtual-link
- summary-address
- timers delay
- timers hold

2.1.1 area authentication

To enable authentication for an Open Shortest Path First (OSPF) area, use the area authentication command in routing switch configuration mode. To remove an or a authentication specification of an area specified area from the configuration, use the no form of this command.

area *area-id* **authentication** [**simple | message-digest**]

no area *area-id* **authentication**

no area *area-id*

parameter

parameter	description
area-id	Identifier of the area for which authentication is to be enabled.

simple	(Optional)authentication information, Plain text authentication
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the area-id argument.

default

no authentication of interface receiving OSPF packet by default

command mode

router configuration

instruction

The authentication value will be added into OSPF packet.The authentication type of all routing swithces in the same area must be the same.The authentication password for all OSPF routing switches on a network must be the same if they are to communicate with each other via OSPF..

example

The following example mandates authentication simple for areas 0 and 36.0.0.0.

```
interface ethernet 1/0
ip address 131.119.251.201
255.255.255.0 ip ospf password adcdefgh
!
interface ethernet 1/0
ip address 36.56.0.201 255.255.0.0
ip ospf password ijklmnop
!
router ospf 1
network 36.0.0.0 255.0.0.0 area 36.0.0.0
network 131.119.0.0 255.255.0.0 area 0
area 36.0.0.0 authentication simple area 0
authentication simple
```

related commands

ip ospf password

ip ospf message-digest-key

2.1.2 area default-cost

To specify a cost for the default summary route that is sent into a stub area or not-so-stubby area (NSSA), use the area default-cost command in router address

family topology or routing switch configuration mode. To remove the assigned default route cost, use the no form of this command.

area *area-id* **default-cost cost**

no area *area-id* **default-cost**

no area *area-id*

parameter

parameter	description
area-id	Identifier for the stub area.
cost	Cost for the default summary route used for a stub

default

cost.1

command mode

router configuration

instruction

This command is used only on an routing switch attached to a stub area or NSSA.

After configured the area stub default-information-originate command, the routing switch will send LSA(SUM-NER-LSA) including default router information to correspondent field, the cost configured I this command is the correspondent cost used in LSA.

Note:

To remove the specified area from the software configuration, use the no area area-id command (without other keywords). That is, the no area area-id command removes all area options, such as area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

example

The following example assigns a default cost of 20 to stub network 36.0.0.0:

```
interface ethernet 1/0
ip address 36.56.0.201 255.255.0.0
!
```

router ospf 201
network 36.0.0.0 255.0.0.0 area
36.0.0.0 area 36.0.0.0 stub
area 36.0.0.0 default-cost 20

related commands

area nssa

area stub

2.1.3 area range

To consolidate and summarize routes at an area boundary, use the area range command. To disable this function, use the no form of this command.

area *area-id* **range** *address mask*[**not-advertise**]

no area *area-id* **range** *address mask* **not-advertise**

no area *area-id* **range** *address mask*

no area *area-id*

parameter

parameter	description
area-id	Identifier of the area for which routes are to be summarized. It can be specified as either a decimal value or an IPv6 prefix.
address	IP address
mask	IP address mask
advertise	(Optional) Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

default

This command is disabled by default.

command mode

router configuration

instruction

The area range command is used only with Area Border Routing switches. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called route summarization.

Multiple area range routing switch configuration commands can be configured. Thus, OSPF can summarize addresses for many different sets of address ranges.

Note: To remove the specified area from the software configuration, use the no area area-id command (with no other keywords). That is, the no area area-id command removes all area options, such as area default-cost, area nssa, area range, area stub, and area virtual-link.

example

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 36.0.0.0 and for all hosts on network 192.42.110.0:

```
interface ethernet 0
ip address 192.42.110.201 255.255.255.0
!
interface ethernet 1
ip address 36.56.0.201 255.255.0.0
!
router ospf 201
network 36.0.0.0 255.0.0.0 area 36.0.0.0
network 192.42.110.0 255.0.0.0 area 0 area
36.0.0.0 range 36.0.0.0 255.0.0.0 area 0
range 192.42.110.0 255.255.255.0
```

2.1.4 area stub

To define an area as a stub area, use the area stub command. To disable this function, use the no form of this command.

area *area-id* **stub** [**no-summary**]

no area *area-id* **stub**

no area *area-id*

parameter

parameter	description
area-id	Identifier for the stub area; either a decimal value or an IP address.
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.

default

No stub area is defined.

command mode

router configuration

instruction

You must configure the area stub command on all routers and access servers in the stub area. Use the area router configuration command with the default-cost keyword to specify the cost of a default internal route sent into a stub area by an ABR switch.

There are two stub area router configuration commands: the stub and default-cost options of the area routing switch configuration command. In all routing switches attached to the stub area, the area should be configured as a stub area using the stub keyword of the area command. Use the default-cost keyword only on an ABR attached to the stub area. The default-cost keyword provides the metric for the summary default route generated by the ABR into the stub area.

To further reduce the number of link-state advertisements (LSAs) sent into a stub area, you can configure the no-summary keyword on the ABR switch to prevent it from sending summary LSAs (LSA type 3) into the stub area.

Note: To remove the specified area from the software configuration, use the no area area-id command (with no other keywords). That is, the no area area-id command removes all area options, such as area authentication, area default-cost, area nssa, area range, area stub, and area virtual-link.

example

The following example assigns a default cost of 20 to stub network 36.0.0.0:

```
interface ethernet 0
ip address 36.56.0.201 255.255.0.0
!
router ospf 201
```

network 36.0.0.0 255.0.0.0 area
36.0.0.0 area 36.0.0.0 stub
area 36.0.0.0 default-cost 20

related commands

area authentication

area default-cost

2.1.5 area virtual-link

To define a virtual link, use the area virtual-link command

area *area-id* **virtual-link** *neighbor-ID* [**authentication** simple | message-digest] [**dead-interval** *dead-value*][**hello-interval** *hello-value*][*retrans-value*][**transdly** *dly-value*][**password** *pass-string*] [key-id **retransmit-interval** MD5 md5-string] message-digest-key

no area *area-id* **virtual-link** *neighbor-ID*

parameter

parameter	description
area-id	Area ID assigned to the transit area for the virtual link.
neighbor-id	Router ID associated with the virtual link neighbor.
simple	Plain text authentication. The value must be the same for all routing switches and access servers attached to a common network.
message-digest	Enables Message Digest 5 (MD5) on virtual-link. The value must be the same for all routing switches and access servers attached to a common network.
dead-value	Time (in seconds) that hello packets are not seen before a neighbor declares the router down. The value must be the same for all routing switches and access servers attached to a common network.
hello-value	Time (in seconds) between the hello packets that the software sends on an interface. The value must be the same for all routing switches and access servers attached to a common network.
retrans-value	Time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The value must be the same for all routing switches and access servers attached to a common network.
dly-value	Delay value in seconds to inform LSA on virtual-link for a routing switch. The configured value on both sides of the virtual-link should be the same.
pass-string	If virtual-link uses plain text authentication, the the maximum character of the configured password should be 8. The configuied value on both sides of the virtual-link should be the same.

key-id	If virtual-link uses MD5 authentication, the valid range of the used MD5 key should from 1 to 255. The configured value on both sides of the virtual-link should be the same.
MD5-String	Configures MD5 password, which is 16-character at most. The configured value on both sides of the virtual-link should be the same.

default

No virtual-link is configured.

Default value of other parameters are as follows:

Hello-value: 10s, Dead-value : 40s, Retrans-value : 5s, dly-value : 1s, no authentication

command mode

OSPFrouter configuration

instruction

To establish a virtual link, user should configure both sides of the virtual link. The virtual link will fail if this command is only configured on one side.

The parameter-id must be a non-zero character, for the virtual link and the transit areda must be a non-backbone area. The configured area-id of the virtual link must be the same.

The neighbor-ID must be the same as the ospf router-id on the remote side during configuration, or the virtual link will not be established. Even if the configured neighbor-ID is another IP address of the other side.

You must make sure that all parameters on both sides must be the same.

The authentication parameters that configured on virtual-link become effective only when configured authentication types of virtual-link or configured the relevant authentication methods in backbone are (via the command area authentication)Only one kind of authentication parameter can be configured on virtual-link, that is, the MD5 and the plain text authenticationm are mutually exclusive.

Use the command no area area-id veitual-link neighbor-ID to cancel the formerly-configured virtual link.

Use the command show ip ospf virtual-link to check state of the virtual link.

example

The following example configured a virtual link between router A and router B:

The configuration on router A (router-id: 200.200.200.1)

!

router ospf 100
network 192.168.20.0 255.255.255.0 area 1
area 1 virtual-link 200.200.200.2
!

The configuration on router B :

!
router ospf 100
network 192.168.30.0 255.255.255.0 area 1
area 1 virtual-link 200.200.200.1
!

related commands

show ip ospf virtual-link

2.1.6 debug ip ospf adj

To monitor Open Shortest Path First (OSPF)-related estabilishment process , use the debug ospf adj command

debug ip ospf adj

parameter

none

default

none

command mode

EXEC

instruction

User can check the process of OSPF-related estabilishment process from the output of this command.

example

Router# debug ip ospf adj
OSPF: Interface 192.168.40.0 on Serial1/0 going down
OSPF NBR: 192.168.40.2 address 192.168.40.2 on Serial1/0 is dead, state DOWN
OSPF NBR: 192.168.40.3 address 192.168.40.3 on Serial1/0 is dead, state DOWN
Line on Interface Serial1/0, changed state to up

Line protocol on Interface Serial1/0 changed state to up
OSPF: Interface 192.168.40.0 on Serial1/0 going Up
OSPF: 2 Way Communication to 192.168.40.2 on Serial1/0, state 2WAY
OSPF: NBR 192.168.40.2 on Serial1/0 Adjacency OK, state
NEXSTART. OSPF: NBR Negotiation Done. We are the SLAVE
OSPF: NBR 192.168.40.2 on Serial1/0 Negotiation Done. We area the
SLAVE OSPF: Exchange Done with 192.168.40.2 on Serial1/0
OSPF: Loading Done with 192.168.40.2 on Serial1/0, database Synchronized
(FULL) OSPF: 2 Way Communication to 192.168.40.3 on Serial1/0, state 2WAY
OSPF: NBR 192.168.40.3 on Serial1/0 Adjacency OK, state
NEXSTART. OSPF: NBR Negotiation Done. We are the SLAVE
OSPF: NBR 192.168.40.3 on Serial1/0 Negotiation Done. We area the
SLAVE OSPF: Bad Sequence with 192.168.40.3 on Serial1/0, state
NEXSTART OSPF: NBR Negotiation Done. We are the SLAVE
OSPF: NBR 192.168.40.3 on Serial1/0 Negotiation Done. We area the
SLAVE OSPF: Exchange Done with 192.168.40.3 on Serial1/0
OSPF: Loading Done with 192.168.40.3 on Serial1/0, database Synchronized (FULL)
……

2.1.7 debug ip ospf events

To monitor OSPF interface and OSPF-related events, , use the debug ip ospf events command.

debug ip ospf events

parameter

none

default

none

command mode

EXEC

instruction

To display OSPF interface and OSPF-related adjacency events from the ouput of this command.

example

Router# debug ip ospf events
OSPF: Interface Serial1/0 going Up

OSPF: INTF(192.168.40.0) event INTF_UP
OSPF: NBR(192.168.40.2) event HELLO_RX
OSPF: NBR(192.168.40.2) event TWOWAY
OSPF: NBR(192.168.40.2) event ADJ_OK
OSPF: NBR(192.168.40.2) event NEGO_DONE
OSPF: NBR(192.168.40.2) event EXCH_DONE
OSPF: NBR(192.168.40.2) event LOAD_DONE
OSPF: NBR(192.168.40.3) event HELLO_RX
OSPF: NBR(192.168.40.3) event TWOWAY
OSPF: NBR(192.168.40.3) event ADJ_OK
OSPF: NBR(192.168.40.3) event NEGO_DONE
OSPF: NBR(192.168.40.3) event SEQ_MISMATCH
OSPF: NBR(192.168.40.3) event NEGO_DONE
OSPF: NBR(192.168.40.3) event EXCH_DONE
OSPF: NBR(192.168.40.3) event LOAD_DONE
……

2.1.8 debug ip ospf flood

To display OSPF-related database pervasion process, use the debug ip ospf flood command.

debug ip ospf flood

parameter

none

default

none

command mode

EXEC

instruction

To display OSPF-related database pervasion process from the output of this command.

example

Router# debug ip ospf flood
OSPF: recv UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 2 SEQ 0x8000022B

OSPF: Send UPDATE, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ 0x80000234

OSPF: Send ACK, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 2 SEQ 0x8000022B

OSPF: recv ACK, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ 0x80000234

OSPF: recv ACK, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 18 SEQ 0x80000233

OSPF: Send UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 10 SEQ 0x8000022B

OSPF: recv UPDATE, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 5 SEQ 0x8000021C

OSPF: Send UPDATE, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 6 SEQ 0x8000021C

OSPF: Send UPDATE, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ 0x80000235

OSPF: recv ACK, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 4 SEQ 0x8000021C

……

2.1.9 debug ip ospf lsa-generation

To display OSPF-related LSA generation process, use the debug ip ospf lsa generation command.

debug ip ospf lsa-generation

parameter

none

default

none

command mode

EXEC

instruction

To display OSPF interface and adjacency events from the output of this command.

example

router# debug ip ospf lsa-generation

……

OSPF: Send UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 10 SEQ 0x8000022D

OSPF: recv UPDATE, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 5 SEQ 0x8000021E

OSPF: Send UPDATE, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 6 SEQ 0x8000021E

OSPF: Send UPDATE, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ 0x80000239

OSPF: recv ACK, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 4 SEQ 0x8000021E

OSPF: Send ACK, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 5 SEQ 0x8000021E

OSPF: recv UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 1 SEQ 0x8000022E

OSPF: Send UPDATE, type 1 LSID 192.168.40.2 ADV_RTR 192.168.40.2 AGE 2 SEQ 0x8000022E

OSPF: recv ACK, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ 0x80000239

OSPF: recv ACK, type 1 LSID 192.168.40.3 ADV_RTR 192.168.40.3 AGE 6 SEQ 0x8000021E

OSPF: recv ACK, type 1 LSID 192.168.20.240 ADV_RTR 192.168.20.240 AGE 1 SEQ 0x80000239

……

2.1.10 debug ip ospf packet

To display OSPF packets, use the debug ip ospf packet command.

debug ip ospf packet

parameter

none

default

none

command mode

EXEC

instruction

To display OSPF interface and adjacency events from the output of this command.

example

router# debug ip ospf packet

OSPF: Recv HELLO packet from 192.168.40.3 (addr: 192.168.40.3) area 0 from

Serial1/0 OSPF: End of hello processing

OSPF: Send HELLO to 224.0.0.5 on Loopback0

HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 44

OSPF: Send HELLO to 224.0.0.5 on Loopback0
HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 44 OSPF:
Send HELLO to 224.0.0.5 on Loopback0
HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 44
OSPF: Recv HELLO packet from 192.168.40.2 (addr: 192.168.40.2) area 0 from
Serial1/0 OSPF: End of hello processing
OSPF: Send HELLO to 224.0.0.5 on Serial1/0
HelloInt 30 Dead 120 Opt 0x2 Pri 1 len 52
OSPF: Recv HELLO packet from 192.168.40.3 (addr: 192.168.40.3) area 0 from
Serial1/0 OSPF: End of hello processing
OSPF: Send HELLO to 224.0.0.5 on Loopback0
HelloInt 10 Dead 40 Opt 0x2 Pri 1 len 44
……

2.1.11 debug ip ospf retransmission

To display retransmission of OSPF paceket, uset the debug ip ospf retransmission command;

debug ip ospf retransmission

parameter

none

default

none

command mode

EXEC

instruction

To display transmission processo OSPF packets.

example

router# debug ip ospf retransmission
OSPF: retransmit UPDATE to 192.168.40.3 (RID 192.168.40.3), state FULL
……

2.1.12 debug ip ospf spf

To display information of SPF algorithm, use the debug ip ospf spf statistic command

debug ip ospf spf statistic

debug ip ospf spf

debug ip ospf spf intra

debug ip ospf spf inter

debug ip ospf spf external

parameter

none

default

none

command mode

EXEC

instruction

The debug ip ospf spf statistic command displays the OSPF routes calculation process.

example

router# debug ip ospf spf
OSPF: run ospf_spf_run
OSPF: start doing SPF for AREA
0.0.0.0 OSPF: RTAB_REV(ospf) 1390.
OSPF : Initializing to do SPF
OSPF: addroute LSID 192.168.20.240
OSPF: ospf_nh_find: 192.168.40.2
……
OSPF: addroute LSID 192.168.40.3
OSPF: build a OSPF_ROUTE, dest:
192.168.40.3 OSPF: addroute LSID 192.168.40.2
……
OSPF: SPF Area A running Network Summary
OSPF: Processing LS_SUM_NET 192.168.40.24, mask 255.255.255.248, adv 192.168.40.3, age 599
OSPF: addroute LSID 192.168.40.24 OSPF:
ospf_build_route RT 192.168.40.24

OSPF: build route 192.168.40.24(255.255.255.248).
……
OSPF: Processing LS_SUM_NET 1.1.1.1, mask 255.255.255.255, adv 192.168.20.240, age 228 OSPF: addroute LSID 192.168.20.236
OSPF: build a OSPF_ROUTE, dest: 192.168.20.236
OSPF: start Building AS External Routes
OSPF: processing LS_ASE 192.168.42.0, mask 255.255.255.248, adv 192.168.20.236, age 258 OSPF: addroute LSID 192.168.42.0
OSPF: ospf_build_route RT 192.168.42.0
OSPF: build route 192.168.42.0(255.255.255.248).
OSPF: processing LS_ASE 192.168.43.0, mask 255.255.255.0, adv 192.168.20.236, age 258 OSPF: addroute LSID 192.168.43.0
OSPF: ospf_build_route RT 192.168.43.0
OSPF: build route 192.168.43.0(255.255.255.0).
OSPF: processing LS_ASE 192.168.44.0, mask 255.255.255.0, adv 192.168.20.236, age 258 OSPF: addroute LSID 192.168.44.0
OSPF: ospf_build_route RT 192.168.44.0
OSPF: build route 192.168.44.0(255.255.255.0).
……
OSPF: end doing SPF for AREA 0.0.0.0

2. Description of the displaying fields:

Field	Description
LSA(192.168.20.236, LS_SUM_ASB)	ID and type of LSA

2.1.13 debug ip ospf tree

To display establishment of SPF tree of OSPF, use the debug ip ospf tree.

debug ip ospf tree

parameter

none

default

none

command mode

EXEC

instruction

To display establishment of SPF tree of OSPF from the output of this command.

example

router# debug ip ospf
tree B3710_221#
OSPF: add LSA(192.168.40.0, LS_STUB) 1600 under LSA(192.168.20.240, LS_RTR)
OSPF: add LSA(192.168.40.2, LS_RTR) 1600 under LSA(192.168.20.240, LS_RTR)
OSPF: add LSA(192.168.40.3, LS_RTR) 1600 under LSA(192.168.20.240, LS_RTR)
OSPF: add LSA(192.168.40.1, LS_STUB) 0 under LSA(192.168.20.240, LS_RTR) OSPF:
add LSA(192.168.40.3, LS_STUB) 1600 under LSA(192.168.40.3, LS_RTR) OSPF: add
LSA(192.169.1.5, LS_RTR) 3200 under LSA(192.168.40.2, LS_RTR) OSPF: add
LSA(192.168.40.18, LS_STUB) 1600 under LSA(192.168.40.2, LS_RTR) OSPF: add
LSA(192.168.40.2, LS_STUB) 1600 under LSA(192.168.40.2, LS_RTR) OSPF: add
LSA(192.168.40.17, LS_STUB) 3200 under LSA(192.169.1.5, LS_RTR)
OSPF: add LSA(192.168.40.24, LS_SUM_NET) 1601 under LSA(192.168.40.3, LS_RTR)
OSPF: add LSA(192.168.40.32, LS_SUM_NET) 3200 under LSA(192.168.40.2, LS_RTR)
OSPF: add LSA(192.168.40.40, LS_SUM_NET) 14577 under LSA(192.169.1.5, LS_RTR)
OSPF: add LSA(192.168.20.236, LS_SUM_ASB) 3200 under LSA(192.168.40.2, LS_RTR)

Description of the displaying fields:

Field	Description
LSA(192.168.20.236, LS_SUM_ASB)	ID and type of LSA
add	Sub-LSA
under	parent LSA

2.1.14 default-information originate (OSPF)

To generate a default external route into an Open Shortest Path First (OSPF) routing domain, use the default-information originate command

default-information originate [**always**] [**route-map** *map-name*]

no default-information originate [**always**] [**route-map** *map-name*]

parameter

parameter	description
originate	Generate a default external route into an Open Shortest Path First (OSPF) routing domain
Always	(Optional) Always advertises the default route regardless of whether the

	software has a default route.
route-map map-name	(Optional) Routing process will generate the default route if the route map is satisfied.

default

This command is disabled by default. No default external route is generated into the OSPF routing domain.

command mode

router configuration

instruction

Whenever you use the redistribute or the default-information router configuration command to redistribute routes into an OSPF routing domain, the software automatically becomes an Autonomous System Boundary Router Switch. However, an ASBR Switch does not, by default, generate a default route into the OSPF routing domain. The software still must have a default route for itself before it generates one, except when you have specified the always keyword.

When you use this command for the OSPF process, you must satisfy the route-map argument. Use the default-information originate always route-map command when you do not want the dependency on the default network in the routing table.

example

The following example specifies a metric of 100 for the default route redistributed into the OSPF routing domain and an external metric type of Type 1:

```
router ospf 109
redistribute rip
default-information originate
```

related commands

Redistribute

2.1.15 default-metric

To set default metric values for the Open Shortest Path First (OSPF) routing protocol, use the default-metric command. To return to the default state, use the no form of this command.

default-metric *value*

no default-metric

parameter

parameter	description
value	Default metric value appropriate for the specified routing protocol, in the range 1~4294967295.

default

Default metric value is 10.

command mode

router configuration

instruction

The default-metric command is used in conjunction with the redistribute router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metrics. Whenever metrics do not convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

example

The example assigns 10 as the default metric routes.

router_config_ospf_100#default-metric 3

related commands

redistribute

2.1.16 distance ospf

To define Open Shortest Path First (OSPF) route administrative distances based on route type, use the distance ospf command To restore the default value, use the no form of this command.

distance ospf {[**intra-area** *dist1*] [**inter-area** *dist2*] [**external** *dist3*]}

no distance ospf [**intra-area**] [**inter-area**] [**external**]

parameter

parameter	description

intra-area dist1	(Optional) Sets the distance for routes in an area, learned by redistribution. The default value is 110.
inter-area dist2	(Optional) Sets the distance for all routes from one area to another area. The default value is 110.
external dist3	(Optional) Sets the distance for routes from other routing domains, learned by redistribution. The default value is 110.

default

intra-area: 110

inter-area: 110

external: 150

command mode

router configuration

instruction

This command performs the same function as the distance command used withan access list. However, the distance ospf command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list.

example

The following example changes the external distance to 200:

Router A
router ospf 1
redistribute ospf 2 distance
ospf external 200
!
router ospf 2
redistribute ospf 1
distance ospf external
200 Router B
router ospf 1
redistribute ospf 2
distance ospf external 200
!
router ospf 2
redistribute ospf 1
distance ospf external 200

related commands

distance

2.1.17 filter

To configure routing fliter list, use the filter command. Use the no filter command to restore the default.

filter {**interface-type** *interface*-number | *****} {**in | out** } {**access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*}

no filter {**interface-type** *interface*-number | *****} {**in** | out} {**access-list** *access-list-name* | **gateway** *access-list-name* | **prefix-list** *prefix-list-name*}

parameter

parameter	description
***interface*-type**	Interface type
interface-number	Interface number
*****	All interfaces
In	Filters incoming ospf routes
out	Filters outgong routes
access-list-name	Name of access list
access-list-name	Name of access list
prefix-list-name	Name of prefix list

default

none

command mode

router configuration

instruction

none

example

filter * in access-list mylist

2.1.18 ip ospf cost

To specify the cost of OSPF protocol on an interface, use the ip ospf cost command in interface configuration mode. To restore to the default value, use the no form of this command.

ip ospf cost cost

no ip ospf cost

parameter

parameter	description
cost	the cost of OSPF protocol. It can be a value in the range from 1 to 65535.

default

Default value of the OSPF protocol cost depends on rate of the interface.

command mode

interface configuration mode

example

The following example sets the interface cost value to 2:

ip ospf cost 2

specify the the interface cost of OSPF protocol, to restore the default value,use the no ip ospf command

2.1.19 ip ospf dead-interval

To set the dead-interval of specified routing switch in neighbourhood, use the ip ospf dead-interval command in interface configuration mode. To restore the default value, use the no form of this command.

ip ospf dead-interval *seconds*

ip ospf dead-interval

parameter

parameter	description
Seconds	Interval (in seconds) of specified routing switch in neighbourhood. The

	range is 1 to 65535.

default

40 seconds

command mode

interface configuration

instruction

The dead interval is advertised in OSPF hello packets and sent with OSPF hello packets. This value must be the same for all networking devices on a specific network and four times the interval set by the ip ospf hello-interval command.

example

The following example sets the OSPF dead interval to 60 seconds:

router_config_S1/0#ip ospf dead-interval 60

related commands

ip ospf hello-interval

2.1.20 ip ospf hello-interval

To specify the interval between hello packets that the Cisco IOS software sends on the interface, use the ip ospf hello-interval command. To return to the default value, use the no form of this command.

ip ospf hello-interval *seconds*

no ip ospf hello-interval

parameter

parameter	description
Seconds	Specifies the interval (in seconds)of sending hello packets. The range is from 1 to 255.

default

10 seconds

command mode

interface configuration mode

instruction

This value is advertised in the hello packets and sent with the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

example

The following example sets the interval between hello packets to 20 seconds:

router_config_S1/0#ip ospf hello-interval 20

related commands

ip ospf dead-interval

2.1.21 ip ospf message-digest-key

To enable Open Shortest Path First (OSPF) Message Digest 5 (MD5) authentication, use the ip ospf message-digest-key md5 command. To remove an old MD5 key, use the no form of this command.

ip ospf message-digest-key *keyid* **md5 key**

no ip ospf message-digest-key *keyid*

parameter

parameter	description
keyid	An identifier in the range from 1 to 255.
key	Alphanumeric password of up to 16 bytes.

default

OSPF MD5 authentication is disabled.

command mode

interface configuration mode

instruction

Usually, one key per interface is used to generate authentication information when sending packets and to authenticate incoming packets. The same key identifier on the neighbor router must have the same key value.

The process of changing keys is as follows. Suppose the current configuration is as follows:

```
interface ethernet 1
ip ospf message-digest-key 100 md5 OLD
```

You change the configuration to the following:

```
interface ethernet 1
ip ospf message-digest-key 101 md5 NEW
```

The system assumes its neighbors do not have the new key yet, so it begins a rollover process. It sends multiple copies of the same packet, each authenticated by different keys. In this example, the system sends out two copies of the same packet—the first one authenticated by key 100 and the second one authenticated by key 101.

Rollover allows neighboring routers to continue communication while the network administrator is updating them with the new key. Rollover stops once the local system finds that all its neighbors know the new key. The system detects that a neighbor has the new key when it receives packets from the neighbor authenticated by the new key.

After all neighbors have been updated with the new key, the old key should be removed. In this example, you would enter the following:

```
interface ethernet 1
no ip ospf message-digest-key 100
```

Then, only key 101 is used for authentication on Ethernet interface 1.

We recommend that you not keep more than one key per interface. Every time you add a new key, you should remove the old key to prevent the local system from continuing to communicate with a hostile system that knows the old key. Removing the old key also reduces overhead during rollover.

example

The following example sets a new key 19 with the password 8ry4222:

```
interface ethernet 1
ip ospf message-digest-key 10 md5 xvv560qle ip
ospf message-digest-key 19 md5 8ry4222
```

related commands

area authentication

2.1.22 ip ospf network

To configure the Open Shortest Path First (OSPF) network type, use the ip ospf network command. To return to the default value, use the no form of this command.

ip ospf network { **broadcast | nonbroadcast | point_to_multipoint** | **point-to-point**}

no ip ospf network { **broadcast | nonbroadcast | point_to_multipoint | point-to-point**}

parameter

parameter	description
broadcast	Sets the network type to broadcast.
nonbroadcast	Sets the network type to nonbroadcast multiaccess
point-to-point	Sets the network type to point-to-point.
point-to-multipoint	Sets the network type to point-to-multipoint.

command mode

interface configuration mode

instruction

Using this feature, you can configure broadcast networks as NBMA networks. Configuring NBMA networks as point-to-multipoint network if there is no assurance to direct connection between any two routing switches..

example

The following example sets serial1/0 as a nonbroadcast network type:

router_config_S1/0#ip ospf network nonbroadcast

2.1.23 ip ospf passive

To cancel sending a HELLO packets on an interface, use the ip ospf passive command. Use the no form of this command to reactivate the sending of HELLO packet.

ip ospf passive

no ip ospf passive

parameter

This command has no keywords or parameters.

default

disabled

command mode

all configruration mode

instruction

If you cancel sending a HELLO packet on an interface, a specified subnetwork wll keep on declaring to other interfaces, and the routing update from other routing switch to this interface can still be received and dealt with. This is usually applicable to the STUB network, for in this kind of network there is usually no other OSPF routing switches.

example

The following example sends a HELLO packet to all interfaces(except for Ethernet 1/0) overridden by network 172.16.0.0:

interface ethernet 1/0

ip address 172.16.0.1 255.255.0.0

ip ospf passive

router ospf 110

network 172.16.0.0 255.255.0.0 area 1

related commands

none

2.1.24 ip ospf password

To configure password for a neighbor route, use the ip ospf password command. Use the no form of this command to cancel the configuration.

ip ospf password *password*

no ip ospf password

parameter

parameter	description
password	Any consecutive 8-digit character string

default

No password is predefined by default.

command mode

Interface configuration mode

instruction

The password generated by this command directly inserts OSPF information packet. This command can configure one password for each network of each interface. All neighbor routers must have the same password to exchange OSPD routing information.

Note: This command is only valid when configured with the area authentication command.

example

ip ospf password yourpass

related commands

area authentication

2.1.25 ip ospf priority

To set the router priority, use the ip ospf priority command. To return to the default value, use the no form of this command.

ip ospf priority *priority*

no ip ospf priority

parameter

parameter	description
priority	specifies the priority. The range is from 0 to 255.

default

Priority of 1

command mode

interface configuration mode

instruction

When two routing switches attached to a network both attempt to become the designated routing switch, the one with the higher routing switch priority takes precedence. If there is a tie, the routing switch with the higher routing switch ID takes precedence. A routing switch with a routing switch priority set to zero is ineligible to become the designated routing switch or backup designated routing switch. routing switch priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

This priority value is used when you configure Open Shortest Path First (OSPF)for nonbroadcast networks using the neighbor routing switch configuration command for OSPF.

example

The following example sets the routing switch priority value to 8:

router_config_S1/0#ip ospf priority 8

related commands

neighbor

2.1.26 ip ospf retransmit-interval

To specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface, use the ip ospf retransmit-interval command. To return to the default value, use the no form of this command.

ip ospf retransmit *seconds*

no ip ospf retransmit

parameter

parameter	description
seconds	Time (in seconds) between retransmissions. The range is from 1 to 65535 seconds.

default

The default is 5 seconds.

command mode

interface configuration mode

instruction

When a routing switch sends an LSA to its neighbor, it keeps the LSA until it receives back the acknowledgment message. If the routing switch receives no acknowledgment, it will resend the LSA. The setting of the seconds argument should be greater than the expected round-trip delay between any two routing switches on the attached network..

example

The following example sets the retransmit interval value to 8 seconds:
router_config_S1/0#ip ospf retransmit 8

2.1.27 neighbor

To configure Open Shortest Path First (OSPF) routing switch interconnecting to nonbroadcast networks, use the neighbor command. To remove a configuration, use the no form of this command.

neighbor *ip-address* [*priority numbe*r] [**poll-interval** *seconds*] [**cost** *number*]

no neighbor *ip-address* [*priority number*] [**poll-interval** *seconds*] [*cost number*]

parameter

parameter	description
ip-address	Interface IP address of the neighbor.
priority number	(Optional) A number that indicates the router priority value of the nonbroadcast neighbor associated with the IP address specified. The default is 0. This keyword does not apply to point-to-multipoint interfaces.

poll-interval seconds	(Optional) A number value that represents the poll interval time (in seconds). RFC 1247 recommends that this value be much larger than the hello interval. The default is 120 seconds (2 minutes). This keyword does not apply to point-to-multipoint interfaces.
cost number	(Optional) Assigns a cost to the neighbor, in the form of an integer from 1 to 65535. Neighbors with no specific cost configured will assume the cost of the interface, based on the ip ospf cost command. For point-to-multipoint interfaces, the cost keyword and the number argument are the only options that are applicable. This keyword does not apply to nonbroadcast multiaccess (NBMA) networks.

default

no default value

command mode

router configuration

instruction

In X.25 and Frame Relay networks you can configure OSPF to run as a broadcast network. Detailed information is as follow:

In X.25 and frame relay map

One nonbroadcast network neighbor must be configured in the routing switch. The neighbor address must be on the primary address of the interface.

If a neighboring router has become inactive, it may still be necessary to send hello packets to the dead neighbor. These hello packets will be sent at a reduced rate called Poll Interval.

When the routing switch first starts up, it sends only hello packets to those routing switches with nonzero priority, that is, routing switches that are eligible to become designated routeing switch (DRs) and backup designated routing switches (BDRs). After the DRs and BDRsare selected, DRs and BDRs will then start sending hello packets to all neighbors in order to form adjacencies.

example

The following example declares a routing switch at address 131.108.3.4 on a nonbroadcast network, with a priority of 1 and a poll interval of 180 seconds:

```
router ospf
neighbor 131.108.3.4 priority 1 poll-interval 180
```

The following example illustrates a point-to-multipoint network with nonbroadcast:

```
interface Serial0
ip address 10.0.1.1 255.255.255.0
ip ospf network point-to-multipoint non-broadcast
encapsulation frame-relay
no keepalive
frame-relay local-dlci 200
frame-relay map ip 10.0.1.3 202
frame-relay map ip 10.0.1.4 203
frame-relay map ip 10.0.1.5 204
no shut
!
router ospf 1
network 10.0.1.0 255.255.255.0 area 0
neighbor 10.0.1.3 cost 5
neighbor 10.0.1.4 cost 10
neighbor 10.0.1.5 cost 15
```

related commands

ip ospf priority

2.1.28 network area

To define the interfaces on which Open Shortest Path First (OSPF) runs and to define the area ID for those interfaces, use the network area command. To disable the feature, use the no form of this command.

network *network mask* **area** *area_id* [**advertise** | **not-advertise**]

[**no**] **network** *network mask* **area** *area_id* [**advertise** | **not-advertise**]

parameter

parameter	description
network	Network Ip address, in dotted decimal format.
mask	Mask, in dotted decimal format.
area_id	Id of area.
Advertise notadvertise	Specifies whether to advertise the abstract information or not

default

This command is disabled by default. command mode

router configuration

instruction

Any individual interface can only be attached to a single area. If the address ranges specified for different areas overlap, the software will adopt the first area in the network command list and ignore the subsequent overlapping portions. Importing network range and specifying the range can reduce the switch state of routing information among areas

Example

The following example defines network range 10.0.0.0 255.0.0.0 and adds to area 2:

router_config_ospf_10#network 10.0.0.0 255.0.0.0 area 2

2.1.29 redistribute

To configure OSPF to redistribute routes of other routing protocols, use the redistribute command. Use the no form of this command to restore the default.

redistribute protocol [*as-number*] [**route-map map-tag**]

no redistribute protocol [*as-number*] [**route-map map-tag**]

parameter

parameter	Description
protocol	Redistributes former protocols that learned, it should be one of the following: eigrp、bgp、connect、ospf、rip、static
as_number	(Optional) Autonomous system number. There is no parameter for connect, rip and static.
map-tag	(Optional) Name of the route map

default

disabled

command mode

router configuration

instruction

none

example

The following example redistributes OSPF protocol from the autonomous system 0:

Redistribute ospf 0

2.1.30 router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the router ospf command. To terminate an OSPF routing process, use the no form of this command.

router ospf *process-id*

no router ospf *process-id*

parameter

parameter	description
process-id	Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.

default

No OSPF routing process is defined.

command mode

global configuration mode

instruction

You can specify multiple OSPF routing processes in each router.

example

The following example configures an OSPF routing process and assign a process number of 109:

router ospf 109

related commands

network area

2.1.31 show ip ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the show ip ospf command.

show ip ospf [*process-id*]

parameter

parameter	description
process-id	(Optional) Process ID. If

default

none

command mode

EXEC

instruction

Troubleshoot OSPF problems according to the output of this command. To display only the global configuration information of the corresponding OSPF process if configured with the process-id parameter.

example

The following display the configuration information of OSPF process :

router#show ip ospf

OSPF process: 1, Router ID is 192.168.99.81

Distance: intra-area 110 inter-area 130 external

150 Source Distance Access-list

240.240.1.1/24 1 what

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

Number of areas is 3

AREA: 1

Number of interface in this area is 1(UP: 1)

Area authentication type: None

AREA: 36.0.0.1

This is a stub area.

Number of interface in this area is 0(UP: 0)

Area authentication type: None

AREA: 192.168.20.0

Number of interface in this area is 0(UP: 0)

Area authentication type: None
Net Range list:
10.0.0.0/255.0.0.0 Not-Advertise
140.140.0.0/255.255.0.0 Advertise
filter list on receiving UPDATE is Gateway:
weewe filter list on sending UPDATE is Prefix:
trtwd Summary-address list:
150.150.0.0/16
advertise router#

description of the displaying fields

field	description
OSPF process: 1	OSPF process ID
Router ID is 192.168.99.81	Routing switch ID
Distance: intra-area 110 inter-area 130 external 150	The default administrative distance that the current routing switch adopts
Source Distance Access-lis	Administrative distance based on concrete routing configuration
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs	Value of two timer related to OSPF
Number of areas is 3	The number of the field that currently configured and the parameter configured in each field
filter list on receiving	The configured filter list on receiving routes
filter list on sending	The configured filter list on sending routes
Summary-address list	The configured routing summary address

2.1.32 show ip ospf border-routers

To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the show ip ospf border-routers command.

show ip ospf border-routers

parameter

none

default

none

command mode

EXEC

example

router#
router#sh ip os bor
OSPF process: 1
Codes: i - Intra-area route, I - Inter-area route
Destination Adv-Rtr Cost Type Area
i 192.168.20.77 192.168.20.77 11 ABR
0 router#

field description:

field	description
Destination	Routing switch ID of the destination.
Adv-Rtr	Next hop toward the destination.
Cost	Cost of using this route.
Type	The routing switch type of the destination; it is either an ABR or ASBR or both.
Area	The area ID of the area from which this route is learned.

2.1.33 show ip ospf database

To display lists of information related to the Open Shortest Path First (OSPF) database, use the show ip ospf database command.

show ip ospf database

parameter

none

default

none

command mode

EXEC

instruction

Display lists of information related to the Open Shortest Path First (OSPF) database in accordance with debugging information of the command, and it is helpful for users in troubleshooting

example

router#
router#show ip ospf
database OSPF process: 1
(Router ID 192.168.99.81)
AREA: 0
Router Link States
Link ID ADV Router Age Seq # Checksum Link count
192.168.20.77 192.168.20.77 77 0x8000008a 0x90ed 1
192.168.99.81 192.168.99.81 66 0x80000003 0xd978 1
Net Link States
Link ID ADV Router Age Seq # Checksum
192.168.20.77 192.168.20.77 80 0x80000001
0x9625 Summary Net Link States
Link ID ADV Router Age Seq # Checksum
192.168.99.0 192.168.99.81 87 0x80000003 0xd78c
AREA: 1
Router Link States
Link ID ADV Router Age Seq # Checksum Link count
192.168.99.81 192.168.99.81 70 0x80000002 0x0817 1
Summary Net Link States
Link ID ADV Router Age Seq # Checksum
192.168.20.0 192.168.99.81 66 0x80000006 0xd1c1
router#

field description:

field	Description
AREA: 1	OSPF area.
Router Link States/Net Link States/Summary Net Link States	LSA type
Link ID	LSA ID.
ADV Router	Advertising routing switch's ID.

Age	Link state age.
Seq #	Link state sequence number
Checksum	Fletcher checksum of the complete contents of the link state advertisement.

2.1.34 show ip ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the show ip ospf interface command.

show ip ospf interface

parameter

none

default

none

command mode

EXEC

instruction

To display configuration and operation situation of OSPF on an interface according to the debugging information of this command. Users can confirm whether the configuration is right or not and it is helpful in troubeshooting

example

router#sh ip os int
Ethernet 1/0 is up, line protocol is up
Internet Address: 192.168.20.81/24, Nettype:
BROADCAST OSPF process is 1, AREA 0, Router ID
202.96.135.201 Cost 10, Transmit Delay is 1 sec, Priority 1
Hello interval 10, Dead timer 40, Retransmit
5 OSPF INTF State is DrOther
Designated Router id 131.119.254.10, Interface address 131.119.254.10
Backup Designated router id 131.119.254.28, Interface addr
131.119.254.28 Neighbor Count is 8, Adjacent neighbor count is 2
Adjacent with neighbor 131.119.254.28 (Backup Designated
Router) Adjacent with neighbor 131.119.254.10 (Designated
Router) router#

displaying field description:

field	description
Internet Address:	Interface IP address
Nettype	Net type of OSPF interface
OSPF process is	OSPF process number
AREA	OSPF area.
Router ID	Routing switch ID
Cost	Cost of routing switch OSPF interface
Transmit Delay is	Transmit delay
Priority	Priority of routing switch interface
Hello interval	Number of seconds until next hello packet is sent out this interface.
Dead timer	Dead timer
Retransmit	Retransmit interval
OSPF INTF State is	OSPF nterface state
Designated Router id	Designated router id and interface ip address
Backup Designated router id	Backup Designated routing switch id and interface ip address
Neighbor Count is	Number of the neighbor routing switch
Adjacent neighbor count is	Number of the adjacent neighbor that has established
Adjacent with neighbor	List of the adjacent neighbor

2.1.35 show ip ospf neighbor

To display Open Shortest Path First (OSPF)-neighbor information, use the show ip ospf neighbor command.

show ip ospf neighbor

parameter

none

default

none

command mode

EXEC

instruction

To display neighbor situation of OSPF from the output of this command to help user troubleshoot OSPF.

example

router#show ip ospf
neighbor OSPF process: 1
AREA 1
Neighbor Pri State DeadTime Address Interface
21.0.0.32 1 FULL /DR 31 192.168.99.32
Ethernet1/0 AREA 36.0.0.1
Neighbor Pri State DeadTime Address Interface
199.199.199.137 1 EXSTART/DR 31 202.19.19.137
Ethernet2/1 AREA 192.168.20.0
Neighbor Pri State DeadTime Address Interface
140.140.0.46 1 FULL /DR 108 140.140.0.46 Serial 1/0
133.133.2.11 1 FULL /DR 110 133.133.2.11 Serial1/0
192.31.48.200 1 FULL / DROTHER 31 192.31.48.200 Ethernet1/0

Displaying field description:

field	description
OSPF process	OSPF process number
AREA	OSPF area
Neighbor	Neighbor routing switch ID.
Pri	Routing switch priority of the neighbor, neighbor state.
State	OSPF state.
DeadTime	Expected time before software will declare the neighbor dead.
Address	Neighbor ip address
Interface	Interface to which connects the neighbor

2.1.36 show ip ospf virtual-link

To display information of Open Shortest Path First (OSPF) virtual links, use the show ip ospf virtual-links command.

show ip ospf virtual-link

parameter

none

default

none

command mode

EXEC

instruction

The information displayed by the show ip ospf virtual-links command is useful in debugging OSPF routing operations. To display the detailed information of adjacency relation of the OSPF neighbor, use the show ip ospf neighbor command

example

router#show ip ospf vir

Virtual Link Neighbor ID 200.200.200.2

(UP) Run as Demand-Circuit

TransArea: 1, Cost is 185

Hello interval is 10, Dead timer is 40 Retransmit is 5

INTF Adjacency state is IPOINT_TO_POINT

Description of the displaying fields:

field	description
neibhbor ID	The configured neighbor ID of the remote side
neighbor state	Adjacency relation of the OSPF neighbor
Demand-Circuit	Indicates working under DC mode
TransArea	The transit area through which the virtual link is formed.
cost	The cost of reaching the OSPF neighbor through the virtual link.
Hello Interval	The current Hello interval
DeadTime	Expected time before software will declare the neighbor dead.
Retrans	Retransmit interval
INTF Adjacency State	The state of virtual link.

related commands

area vritual-link

show ip ospf neighbor

2.1.37 summary-address

To create aggregate addresses for Open Shortest Path First (OSPF), use the summary-address command. To restore the default, use the no form of this command.

summary-address *address mask* [**not-advertise**]

no summary-address *address mask*

parameter

parameter	description
address	Summary address designated for a range of addresses.
Mask	IP subnet mask used for the summary route.
not-advertise	(Optional) Suppress match routes that creat LSA

default

none

command mode

router configuration

instruction

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

Using this command for OSPF causes an OSPF Autonomous System Boundary Routing switch (ASBRs) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. For OSPF, this command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the area range command for route summarization.

example

In the following example, the summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement.

```
summary-address 10.1.0.0 255.255.0.0
```

related commands

area range

ip ospf password

ip ospf message-digest-key

2.1.38 timers delay

To specify the delay interval between OSPF receiving a topology structure variety and initializing a minimum route priority computation, use the timer delay command. Use the no form of this command to resotre default value.

timers delay *spf-delay*

no timers delay

parameter

parameter	description
spf-delay	Delay between topology variety and computation commencement in seconds, from 0 to 65535. Default value is 5 seconds. If the value is o, that indicates there is no delay, namely, once there is a variety, the commencement of computation immediately starts.

default

spf-delay: 5 seconds

command mode

router configuration

instruction

The less the configured time is, the quicker the response to network variety. But this will take up more processing time.

example

timers spf 10

2.1.39 timers hold

To configure the interval between two continuous SPF computation, use the timers hold command. Use the no form of this command to restore the default value.

timers hold *spf-holdtime*

no timers hold

parameter

parameter	description
spf-holdtime	The minimum value between two continuous computation, in the range from 0 to 65535.

default

spf-holdtime: 10 seconds

command mode

router configuration

instruction

The less the configured time is, the quicker the response to network variety. But this will take up more processing time.

example

3. timers spf 20

Chapter 3 BGP Configuration Commands

BGP Configuration Commands include:

- aggregate-address
- bgp always-compare-med
- bgp bestpath med
- bgp client-to-client reflection
- bgp cluster-id
- bgp confederation identifier
- bgp confederation peers
- bgp dampening
- bgp default
- bgp deterministic-med
- bgp redistribute-internal
- clear ip bgp
- debug chat
- debug dialer
- debug ip bgp
- distance
- filter
- neighbor default-originate
- neighbor description
- neighbor distribute-list
- neighbor ebgp-multihop
- neighbor filter-list
- neighbor maximum-prefix
- neighbor next-hop-self

- neighbor password

- neighbor prefix-list
- neighbor remote-as
- neighbor route-map
- neighbor route-reflector-client
- neighbor route-refresh
- neighbor send-community
- neighbor shutdown
- neighbor soft-reconfiguration
- neighbor timers
- neighbor update-source
- neighbor weight
- network (BGP)
- redistribute(BGP)
- router bgp
- show ip bgp
- show ip bgp community
- show ip bgp neighbors
- show ip bgp paths
- show ip bgp prefix-list
- show ip bgp regexp
- show ip bgp summary
- synchronization
- table-map
- timers

3.1.1 aggregate-address

To create an aggregate entry in a Border Gateway Protocol (BGP) database, use the aggregate-address command in address family or routing switch configuration mode. To disable this function, use the no form of this command.

aggregate-address A.B.C.D/n [**summary-only**] [**route-map** *map-name*]

no aggregate-address A.B.C.D/n [**summary-only**] [**route-map** *map-name*]

parameter

parameter	description
A.B.C.D/n	Aggregate network
summary-only	Filters all more-specific routes from updates.
route-map	Name of the route map used to set the attribute of the aggregate route.
map-name	Name of the route map

default

none

command mode

BGP configuration mode

instruction

You can implement aggregate routing in BGP in three methods:first,dynamic implement routing by forwarding redistribute; second, static implement routing by network command; third, static implement routing by aggregate. The routing created in this way are local routing, which can be announced to other equivalent, but not implement local IP address table.

Using the aggregate-address command with no keywords will create an aggregate entry in the BGP or mBGP routing table if any more-specific BGP or mBGP routes are available that fall within the specified range. (A longer prefix which matches the aggregate must exist in the RIB.) The aggregate route will be advertised as coming from your autonomous system and will have the atomic aggregate attribute set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the as-set keyword.)

Using the as-set keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the aggregate-address command when aggregating many paths, because this route must be continually withdrawn and updated as autonomous system path reachability information for the summarized routes changes.

Using the summary-only keyword not only creates the aggregate route (for example, 19.*.*.*) but also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the neighbor distribute-list command, with caution. If a more-specific route leaks out, all BGP or mBGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

Using the suppress-map keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the match clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

Using the advertise-map keyword selects specific routes that will be used to build different components of the aggregate route, such as AS_SET or community. This form of the aggregate-address command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with AS_SET, and advertise it back to some of the same autonomous systems. You must remember to omit the specific autonomous system numbers from the AS_SET to prevent the aggregate from being dropped by the BGP loop detection mechanism at the receiving router. IP access lists and autonomous system path access lists match clauses are supported.

Using the attribute-map keyword allows attributes of the aggregate route to be changed. This form of the aggregate-address command is useful when one of the routes forming the AS_SET is configured with an attribute such as the community no-export attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

example

In the following example, an aggregate BGP address is created :

```
router bgp 5 aggregate-
address 193.0.0.0/8
```

related commands

route-map

3.1.2 bgp always-compare-med

To enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems, use the bgp always-compare-med command. To disallow the comparison, use the no form of this command.

bgp always-compare-med

no bgp always-compare-med

parameter

none

default

Default does not compare the MED for paths from neighbors in different autonomous systems if this command is not enabled or if the no form of this command is entered..

command mode

BGP configuration mode

instruction

Default does not compare the MED for paths from neighbors in different autonomous systems if this command is not enabled or if the no form of this command is entered. The MED is compared only if the autonomous system path for the compared routes is identical.

example

The following example enables the function

router bgp 5

bgp always-compare-med

related commands

bgp bestpath med

bgp deterministic-med

3.1.3 bgp bestpath med

To modify the process way of Border Gateway Protocol (BGP) on Multi Exit Discriminator (MED) attribute, use the bgp bestpath med command. To disable the feature, use the no form of this command.

parameter

parameter	description
confed	Autonous system confederation MED comparison attrubute
missing-as-worst	(Optional) Assigns the value of infinity to received routes that do not carry the MED attribute, making these routes the least desirable.

default

none

command mode

BGP configuration mode

instruction

If the MED attribute of BGP route is not configured, the value of MED is always considered to be 0, that is the least value, which has the most priority. When configured with the missing-as-worst option, if the MED attribute of BGP route is not configured, the value of MED is always considered to be the most maximum value, which has the least priority.

example

By default, the MED comparison between(100)and (200) doesn't occur for they are not the routes from the same sub-autonomous system. But the MED comparison occurs when configured with the bgp bestpath med confed command, for they come from the sub-autonomous system 100 and 200 respecitively in the autonomous system alliance.

related commands

bgp always-compare-med

bgp deterministic-med

3.1.4 bgp client-to-client reflection

To enable or restore route reflection from a BGP route reflector to clients, use the bgp client-to-client reflection command. To disable client-to-client route reflection, use the no form of this command.

bgp client-to-client reflection

no bgp client-to-client reflection

parameter

none

default

Client-to-client route reflection is enabled by default; when a route reflector is configured, the route reflector reflects routes from a client to other clients.

command mode

BGP configuration mode

instruction

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, route reflection is not required. In this case, use the no bgp client-to-client reflection command to disable client-to-client reflection.

example

In the following example, the local routing switch is a route reflector, and the three neighbors are fully meshed, turn off client-to-client reflection

```
router bgp 5
neighbor 192..168.20.190 router-reflector-client
neighbor 192..168.20.191 router-reflector-client
neighbor 192..168.20.192 router-reflector-client
no bgp client-to-client reflection
```

related commands

neighbor route-reflector-client

bgp cluster-id

3.1.5 bgp cluster-id

To set the cluster ID on a route reflector in a route reflector cluster, use the bgp cluster-id command in router configuration mode. To remove the cluster ID, use the no form of this command.

bgp cluster-id *cluster-id*

no bgp cluster-id *cluster-id*

parameter

parameter	description
cluster-id	Cluster ID of this router acting as a route reflector; maximum of 4 bytes.

default

The local routing switch ID of the route reflector is used as the cluster ID when no ID is specified or when the no form of this command is entered.

command mode

BGP configuration mode

instruction

Together, a route reflector and its clients form a cluster. When a single route reflector is deployed in a cluster, the cluster is identified by the routing switch ID of the route reflector. The bgp cluster-id command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables.

example

In the following example, the local routing switch is one of the route reflectors serving the cluster. It is configured with the cluster ID to identify the cluster.

```
router bgp 5
neighbor 198.92.70.24 route-reflector-client
bgp cluster-id 50000
```

related commands

neighbor route-reflector-client

show ip bgp summary

3.1.6 bgp confederation identifier

To specify a BGP confederation identifier, use the bgp confederation identifier command. To remove the confederation identifier, use the no form of this command.

bgp confederation identifier autonomous-system

no bgp confederation identifier autonomous-system

parameter

parameter	description
autonomous-system	Autonomous system number to be configured to internally include multiple autonomous systems.

default

none

command mode

BGP configuration mode

instruction

The bgp confederation identifier command is used to configure a single autonomous system number to identify a group of smaller autonomous systems as a single confederation.

A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single autonomous system into multiple subautonomous systems and then grouping them into a single confederation. The subautonomous systems within the confederation exchange routing information like iBGP peers. External peers interact with the confederation as if it is a single autonomous system.

Each subautonomous system is fully meshed within itself and has a few connections to other autonomous systems within the confederation. Next hop, Multi Exit Discriminator (MED), and local preference information is preserved throughout the confederation, allowing you enables to you to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems.

example

In the following example, the routing domain is divided into autonomous systems AS4001, 4002, 4003, 4004, 4005, 4006 and 4007 and identified by the confederation identifier 50000. Neighbor 1.2.3.4 is a peer inside of the routing domain confederation. Neighbor 3.4.5.6 is a peer outside of the routing domain confederation.

```
router bgp 4001
bgp confederation identifier 5
bgp confederation peers 4002 4003 4004 4005 4006
4007 neighbor 1.2.3.4 remote-as 4002
neighbor 3.4.5.6 remote-as 510
```

related commands

bgp confederation peers

show ip bgp summary 30

3.1.7 bgp confederation peers

To configure subautonomous systems to belong to a single confederation, use the bgp confederation peers command in router configuration mode. To remove an autonomous system from the confederation, use the no form of this command.

bgp confederation peers autonomous-system [**autonomous-system**]

no bgp confederation peers autonomous-system [**autonomous-system**]

parameter

parameter	description
autonomous-system	Autonomous system numbers for BGP peers that will belong to the confederation.

default

none

command mode

BGP configuration mode

instruction

The bgp confederation peers command is used to configure multiple autonomous systems as a single confederation. The ellipsis (...) in the command syntax indicates that your command input can include multiple values for the as-number argument.

The autonomous systems specified in this command are visible internally to the confederation. Each autonomous system is fully meshed within itself. The bgp confederation identifier command specifies the confederation to which the autonomous systems belong.

example

In the following example, autonomous systems 1091, 1092 and 1093 are configured to belong to a single confederation under the identifier 1090:

router bgp 1090

bgp confederation identifier 23
bgp confederation peers 1091 1092 1093

related commands

bgp confederation identifier

show ip bgp summary

3.1.8 bgp dampening

To enable BGP route dampening or change BGP route dampening parameters, use the bgp dampening command in address family or router configuration mode. To disable BGP dampening, use the no form of this command.

bgp dampening [**route-map** *name*] | [*half-time resuse-value suppress-value hold-time*]

no bgp dampening [**route-map** *name*] | [*half-time resuse-value suppress-value hold-time*]

parameter

parameter	description
route-map	Name of route map that controls where BGP route dampening is enabled.
name	Name of route map that controls parameters
half-time	Time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period
reuse-value	Reuse values based on accumulated penalties.
suppress-value	A route is suppressed when its penalty exceeds this limit.
hold-time	Maximum time (in minutes) a route can be suppressed.

default

half-time: 15 minutes

reuse-value: 750

suppress-value: 2000

hold-time: 60 minutes

command mode

BGP configuration mode

instruction

The bgp dampening command is used to enable BGP route dampening. This command can be entered without any arguments or keywords. The half-life, reuse, suppress, and hold-time arguments are position-dependent; meaning that if any of these arguments are entered, then all optional arguments must be entered.

When BGP dampening is configured and a prefix is withdrawn, BGP considers the withdrawn prefix as a flap and increases the penalty by a 1000. If BGP receives an attribute change, BGP increases the penalty by 500. If then the prefix has been withdrawn, BGP keeps the prefix in the BGP table as a history entry. If the prefix has not been withdrawn by the neighbor and BGP is not using this prefix, the prefix is marked as dampened. Dampened prefixes are not used in the BGP decision process and not installed to the routing table.

example

In the following example, the bgp dampening command can be used to enable BGP route dampening function and use default parameter configuration. Use the following commands to configure different dampening parameters for different rouing configurations:

```
Router bgp 100
bgp dampening route-map DMAP
!
route-map DMAP 10 permit
match as-path ASLIST-1
set dampening 15 750 2000 60
!
route-map DMAP 20
  permit match as-path
  ASLIST-2
  set dampening 2 750 2000 8
!
ip as-path access-list ASLIST-1 permit ^3_
ip as-path access-list ASLIST-2 permit ^5_
```

related commands

set dampening

3.1.9 bgp default

To configure default parameter of BGP process, use the bgp default command. Use the no form of this command to restore the default value.

bgp default local-preference *<0-4294967295>*

no bgp default local-preference *<0-4294967295>*

parameter

parameter	description
local-preference	Configures default parameter of the local preference.
<0-4294967295>	Default value of the local preference

default

100

command mode

BGP configuration mode

instruction

The route received from IBGP will be set as the local preference by BGP. The default value is 100, which can be modified via this command.

example

The following example configures 200 as the local preference for the route from IBGP neighbor:

router bgp 100

bgp default local-preference 200

related commands

none

3.1.10 bgp deterministic-med

To enforce the deterministic comparison of the Multi Exit Discriminator (MED) value between all paths received from within the same autonomous system, use the bgp deterministic-med command in router configuration mode. To disable the required MED comparison, use the no form of this command.

bgp deterministic-med

no bgp deterministic-med

parameter

none

default

none

command mode

BGP configuration mode

instruction

The bgp always-compare-med command is used to enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. After the bgp always-compare-med command is configured, all paths for the same prefix that are received from different neighbors, which are in the same autonomous system, will be grouped together and sorted by the ascending MED value (received-only paths are ignored and not grouped or sorted). The best path selection algorithm will then pick the best paths using the existing rules; the comparison is made on a per neighbor autonomous system basis and then global basis. The grouping and sorting of paths occurs immediately after this command is entered. For correct results, all routers in the local autonomous system must have this command enabled (or disabled).

example

none

related commands

bgp bestpath med

bgp always-compare-med

3.1.11 bgp redistribute-internal

To configure IBGP redistribution into an interior gateway protocol (IGP), such as RIP or OSPF, use the bgp redistribute-internal command in address family or router configuration mode. To return the router to default behavior and stop iBGP redistribution into IGPs, use the no form of this command.

bgp redistribute-internal

no bgp redistribute-internal

parameter

none

default

IBGP routes are not redistributed into IGP.

command mode

BGP configuration mode

instruction

The bgp redistribute-internal command is used to configure iBGP redistribution into an IGP. The clear ip bgp command must be entered to reset BGP connections after this command is configured. When redistributing BGP into any IGP, be sure to use IP prefix-list and route-map statements to limit the number of prefixes that are redistributed.

example

In the following example, BGP to OSPF3 route redistribution is enabled:

```
router ospf 3
 redistribute bgp 2
!
router bgp 2
 bgp redistribute-internal
!
```

related commands

none

3.1.12 clear ip bgp

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration, use the clear ip bgp command in privileged EXEC mode.

clear ip bgp {***** | *ip-address* | *as-number* | **peer-group** *name* | **aggregates** | **networks** | **redistribute}** [**soft** [**in** | **out]**]

parameter

parameter	description

*	Specifies that all current BGP sessions will be reset.
ip-address	Specifies that only the identified BGP neighbor will be reset.
AS	Specifies that sessions with BGP peers in the specified autonomous system will be reset.
peer-group-name	Specifies that the identified BGP peer group will be reset.
aggregates	Specifies that all aggregate routes will be reset
networks	Specifies that all static network routes will be reset
redistribute	Specifies that all redistributed routes will be reset
soft	Initiates a soft reset
in | out	Initiates inbound or outbound reconfiguration.

command mode

EXEC

instruction

The clear ip bgp command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the neighbor soft-reconfiguration inbound command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

If all BGP routers support the route refresh capability, use the clear ip bgp command with the in keyword. You need not use the soft keyword, because soft reset is automatically assumed when the route refresh capability is supported.

example

The following example clear all the current BGP sessions:

clear ip bgp *

related commands

neighbor soft-reconfiguration

show ip bgp

3.1.13 debug chat

To display script events, like to startup a script, to stop a script, to display the enforcement process of a script, use the debug chat command. Use the no form of this command to stop displaying information.

debug chat

no debug chat

parameter

This command has no parameters or keywords.

command mode

EXEC

example

```
Router#debug chat
Router#SCRIPT: start script default_dialer_script...
SCRIPT:Sending string: ATZ
SCRIPT:Expecting string:
OK SCRIPT: Receive string:
41 54 0D 0D 0A 4F 4B 0D 0A AT...OK..
SCRIPT:Completed match for
expect:OK SCRIPT:Sending string:
ATDT 2 SCRIPT:Expecting string:
CONNECT SCRIPT: Receive string:
43 4F 4E 4E 45 43 54 CONNECT
SCRIPT: Completed match for
expect:CONNECT SCRIPT:Chat script finished
```

The first message indicates the script named default_dialer_script is started up.

The second message indicates the ATZ character string is sent.

The third message indicates the character string OK is expected to be received.

The fourth message indiates the character string OK s received.

The fifth message indicates ATDT 2 character string is send, that is asking for modem dial-up.

The sixth message indicates the character string CONNECT is expected to be received.

The seventh message indicates the expected character string CONNECT is received.

The eighth message indicates the success of script enforcement.

related commands

chat-script

3.1.14 debug dialer

To display debugging information about the packets received on a dialer interface, use the debug dialer events command in privileged EXEC mode. To disable debugging output, use the no form of this command.

debug dialer

no debug dialer

parameter

This command has no parameters or keywords.

command mode

EXEC

example

```
Router#debug dialer
DIALER Serial 1/0: Dialing cause ip(PERMIT).
DIALER Serial 1/0: Dialing using Modem script: default_dialer_script & System script: none
DIALER Serial 1/0: Attempting to dial 2
DIALER Serial 1/0: process started
DIALER Serial 1/0: Chat script default_dialer_script (dialer) started.....
DIALER Serial 1/0: Connection established
DIALER Serial 1/0: Modem script finished successfully
```

The first message indicates that dialer checks whether the packet is permitted to cause dialing, and the result is the ip packet allows cause dialing.

The second message indicates that dialing uses default dialer script as the modem script rather than the system script.

The third message indicates that the dialer number is 2.

The fourth message indicates that the dialer process is started.

The fifth message indicates thath the dialer script is started.

The sixth and seventh message indicate that the connection is established successfully.

3.1.15 debug ip bgp

To display information related to processing of the Border Gateway Protocol (BGP), use the debug ip bgp command in privileged EXEC mode. To disable debugging output, use the no form of this command.

debug ip bgp {**all | fsm | keepalive | open | update**}

no debug ip bgp {**all | fsm | keepalive | open | update**}

parameter

parameter	description
all	Displays all BGP debugging functions.
dampening	Displays BGP dampening.
event	Displays BGP events.
fsm	Displays BGP fsms
keepalive	Displays BGP keepalives.
notify	Displays BGP notifies
open	Displays BGP opens
update	Displays BGP updates.

default

No default behavior or values

command mode

EXEC

instruction

It is valid globally when configured with the debug ip bgp command to display debugging information and other VTY. If configured with the terminal monitor command, the debugging information will also be displayed. Use the no terminal monitor to close this function to disable displaying any debugging information on the VTY.

The command debug ip bgp all can enable all BGP debugging function, including dampening, fsm,keepalives,open and update. Use the no debug ip bgp all command to disable all BGP debugging functions.

example

The following example is the process to establish a BGP. The debugging information shows that a router establishes a connection with BGP neighbor 10.1.1.3.

BGP: 10.1.1.3 start connecting to peer
BGP: 10.1.1.3 went from Idle to Connect
BGP: 10.1.1.3 went from Connect to OpenSent
BGP: 10.1.1.3 send OPEN, length 41
BGP: 10.1.1.3 recv OPEN, length 41
BGP: 10.1.1.3 went from OpenSent to OpenConfirm
BGP: 10.1.1.3 send KEEPALIVE, length 19
BGP: 10.1.1.3 recv KEEPALIVE, length 19
BGP: 10.1.1.3 went from OpenConfirm to Established
BGP: 10.1.1.3 send KEEPALIVE, length 19
BGP: 10.1.1.3 send UPDATE, length 43
BGP: 10.1.1.3 send UPDATE, length 43
BGP: 10.1.1.3 recv KEEPALIVE, length 19
BGP: 10.1.1.3 recv KEEPALIVE, length 19

3.1.16 distance

To configure the administrative distance for BGP routes, use the distance command in router configuration mode. To return to the administrative distance to the default value, use the no form of this command.

distance bgp *external-distance internal-distance local-distance*

no distance bgp

parameter

parameter	description
external-distance	Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The default value is 20.
internal-distance	Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The default value is 200.
local-distance	Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The default value is 200.

default

external-distance: 20

internal-distance: 200

local-distance: 200

command mode

BGP configuration

instruction

The distance bgp command is used to configure a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP (eBGP), or if some internal routes should be preferred by BGP.

example

In the following example, the administrative distance for BGP routes is set:

router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 remote-as 123
neighbor 128.125.1.1 remote-as 47
distance 20 20 200

related commands

set metric

set tag

3.1.17 filter

To filter routes based on an interface in order to realize the administrative strategy. Use the no form of this command to delete the configuration.

filter interface <**in | out**> **access-list** *access-list-name* **gateway** *access-list-name* **prefix-list** *prefix-list-name*

no filter interface <**in | out**> **access-list** *access-list-name* **gateway** *access-list-name* **prefix-list** *prefix-list-name*

parameter

parameter	description

interface	Interface name. Asterisk signifies all interfaces.
in | out	Filter the incoming of outgoing routes
access-list	Specifies the access-list to filter routes
access-list-name	Name of the access list
gateway	Specifies the access list to filter gateway
access-list-name	Name of the access list
prefix-list	Specifies the prefix list to filter routes
prefix-list-name	Name of the prefix list

default

none

command mode

BGP configuration mode

instruction

The access-list option specifies the access list to filter network prefix of routes; the gateway option specifies the access list to filter nexthop attribute of routes; the prefix list option specifies the prefix list filter network prefix of routes.

The access list and the prefix list options are mutually exclusive simultaneously. But then can be used with the gateway option together.

The asterisk signifies all interfaces.

If a none-existant prefix list or access list is configured on an interface, then all routes will pass.

example

The following example configures prefix and gateway to filter routes received on all interface:

```
router bgp 109
filter * in prefix-list prefix-guize gateway gateway-guize
```

related commands

neighbor distribute-list

neighbor filter-list

neighbor route-map

3.1.18 neighbor default-originate

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the neighbor default-originate command in address family or router configuration mode. To send no route as a default, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **default-originate**

no neighbor {*ip-address* | *peer-group-name*} **default-originate**

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.

default

No default route is sent to the neighbor.

command mode

BGP configuration mode

instruction

This command does not require the presence of 0.0.0.0 in the local router. When used with a route map, the default route 0.0.0.0 is injected if the route map contains a match ip address clause and there is a route that matches the IP access list exactly. The route map can contain other match clauses also. You can use standard or extended access lists with the neighbor default-originate command.

example

In the following example, the local router injects route 0.0.0.0 to the neighbor 160.89.2.3 rather than to 160.89.2.1:

```
router bgp 109
network 160.89.0.0
neighbor 160.89.2.1 remote-as 100
neighbor 160.89.2.3 remote-as 200
neighbor 160.89.2.3 default-originate
```

related commands

neighbor ebgp-multihop

3.1.19 neighbor description

To associate a description with a neighbor, use the neighbor description command in router configuration mode. To remove the description, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **description LINE**

no neighbor {*ip-address* | *peer-group-name*} **description LINE**

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
line	Text that describes the neighbor.

default

There is no description of the neighbor.

command mode

BGP configuration mode

instruction

It is easier for user to understand the configuration to associate a description with a neighbor.

example

In the following example, the description of the neighbor is "peer with abc.com":

router bgp 109
network 160.89.0.0
neighbor 160.89.2.3 description peer with abc.com

3.1.20 neighbor distribute-list

To distribute BGP neighbor information as specified in an access list, use the neighbor distribute-list command in address family or router configuration mode. To remove an entry, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **distribute-list** {*access-list name* } {**in | out**}

no neighbor {*ip-address* | *peer-group-name*} **distribute-list** {*access-list name* } {**in | out**}

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
access-list name	Name of a standard or extended access list.
In	Access list is applied to incoming advertisements to that neighbor.
Out	Access list is applied to outgoing advertisements to that neighbor.

default

none

command mode

BGP configuration mode

instruction

Use access-list filters network prefix of BGP routes; use aspath-list filters AS_PATH attribute of BGP routes; use prefix list to filter network prefix of BGP routes.

The access-list option specifies the access list to filter network prefix of routes; the gateway option specifies the access list to filter nexthop attribute of routes; the prefix list option specifies the prefix list filter network prefix of routes.

If you specify a non-existant access list, all routes will be allowed to pass as a result.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

example

The following router configuration mode example applies list beijing to incoming advertisements from neighbor120.23.4.1.

router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 distribute-list beijing in

related commands

ip aspath-list

neighbor filter-list

ip prefix-list 1

neighbor prefix-list

3.1.21 neighbor ebgp-multihop

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the neighbor ebgp-multihop command in router configuration mode. To return to the default, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]

no neighbor {*ip-address* | *peer-group-name*} **ebgp-multihop**

parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
ttl	Time-to-live in the range from 1 to 255 hops.

default

For EBGP-speaking neighbor, only directly connected neighbors are allowed, ttl default value is 1; for IBGP-speaking neighbor, ttl default is 255.

command mode

BGP configuration mode

instruction

Under default, BGP connection can not be established unless EBGP neighbors are directly connected ones. The allowable maximum number of hops for EBGP neighbors can be set with the neighbor ebgp-multihop command. Ttl is configured to 255 if not specified. If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

The following example allows connections to neighbor 131.108.1.1, which resides on a network that is not directly connected:

router bgp 109:

neighbor 131.108.1.1 ebgp-multihop

related commands

neighbor default-originate

3.1.22 neighbor filter-list

To set up a BGP filter, use the neighbor filter-list command in address family or router configuration mode. To disable this function, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **filter-list** *as-path-list name* {**in | out** }

no neighbor {*ip-address* | *peer-group-name*} **filter-list** *as-path-list name* {**in | out** }

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
as-path-list name	AS-PATH list name. The ip as-path-list command can be used to define this list.
In	Access list applied to incoming routes.
Out	Access list applied to outgoing routes.

default

none

command mode

BGP configuration mode

instruction

Use access-list filters network prefix of BGP routes; use aspath-list filters AS_PATH attribute of BGP routes; use prefix list to filter network prefix of BGP routes.

If you specify a non-existant access list, all routes will be allowed to pass as a result.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

example

In the following router configuration mode example, the BGP neighbor with IP address 128.125.1.1 is not sent advertisements about any path through or from the adjacent autonomous system AS123:

```
ip as-path-list shanghai deny _123_
ip as-path-list shanghai deny ^123$

router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 remote-as 123
neighbor 128.125.1.1 remote-as 47
neighbor 128.125.1.1 filter-list shanghai out
```

related commands

ip aspath-list

neighbor distribute-list

ip prefix-list 1

neighbor prefix-list

3.1.23 neighbor maximum-prefix

To control how many prefixes can be received from a neighbor, use the neighbor maximum-prefix command in router configuration mode. To disable this function, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum*

no neighbor {*ip-address* | *peer-group-name*} **maximum-prefix**

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
Maximum	Maximum number of prefixes allowed from this neighbor.

default

This command is disabled by default. There is no limit on the number of prefixes.

command mode

BGP configuration mode

instruction

This command allows you to configure a maximum number of prefixes that a BGP router is allowed to receive from a peer. It adds another mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer. When the number of received prefixes exceeds the maximum number configured, the router terminates the peering (by default). However, if the warning-only keyword is configured, the router instead only sends a log message, but continues peering with the sender. If the peer is terminated, the peer stays down until the clear ip bgp command is issued.

example

The following example sets the maximum number of prefixes allowed from the neighbor at 129.140.6.6 to 1000:

router bgp 109
network 131.108.0.0
neighbor 129.140.6.6 maximum-prefix 1000

related commands

clear ip bgp

3.1.24 neighbor next-hop-self

To configure the router as the next hop for a BGP-speaking neighbor or peer group, use the neighbor next-hop-self command in router configuration mode. To disable this feature, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **next-hop-self no**

neighbor {*ip-address* | *peer-group-name*} **next-hop-self**

parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.

default

This command is disabled by default.

command mode

BGP configuration mode

instruction

The disposal of nexthop attribute in BGP is more complicated than IGP . It usually follows three rules:

4. For EBGP session, configure the local ip address of BGP connection as the nexthop attribute when sending routes;

5. For IBGP session, configure the local ip address of BGP connection as the nexthop attribute if the routes are locally generated; if the routes are learned from EBGP, the nexthop attribute is to be filled in intactly the packet when sending routes;

6. If the nexthop parameter of the ip address of the routes belong to the network of BGP session, then the nexthop attribute always adopts the former nexthop;

This command is useful in unmeshed networks (such as Frame Relay or X.25) where BGP neighbors may not have direct access to all other neighbors on the sameIP subnet. If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

example

The following example forces all updates destined for 131.108.1.1 to advertise this router as the next hop:

router bgp 109

neighbor 131.108.1.1 next-hop-self

related commands

set ip next-hop 18

3.1.25 neighbor password

To enable Message Digest 5 (MD5) authentication on a TCP connection between two BGP peers, use the neighbor password command in router configuration mode. To disable this function, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **password** *LINE*

no neighbor {*ip-address* | *peer-group-name*} **password**

parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
password	Enables MD5 authentication
LINE	Plainr text password

default

none

command mode

BGP configuration mode

instruction

Use the neighbor remote-as command to specify the neighbor before using this command.

You can configure MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. The length of password should between 1 and 20 characters.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

The following example configures ‘abcd’ as the authentication password of neighbor 120.23.4.1:

router bgp 109

neighbor 120.23.4.1 remote-as 108

neighbor 120.23.4.1 password abcd

related commands

neighbor remote-as

3.1.26 neighbor prefix-list

To prevent distribution of Border Gateway Protocol (BGP) neighbor information as specified in a prefix list, a Connectionless Network Service (CLNS) filter expression, or a CLNS filter set, use the neighbor prefix-list command in address family or router configuration mode. To remove a filter list, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **prefix-list** *prefix-listname* {**in | out**}

no neighbor {*ip-address* | *peer-group-name*} **prefix-list** *prefix-listname* {**in | out**}

parameter

parameter	description
ip-address	IP address of neighbor.
peer-group-name	Name of a BGP peer group.
prefix-list	Prefix list is applied to advertisements of that neighbor
prefix-listname	Prefix list 名 Name of a prefix list.
In	Filter list is applied to incoming advertisements from that neighbor.
Out	Filter list is applied to outgoing advertisements to that neighbor.

default

none

command mode

BGP configuration mode

instruction

Using prefix lists is one of three ways to filter BGP advertisements. You can also use AS-path filters, defined with the ip as-path access-list global configuration command

and used in the neighbor filter-list command to filter BGP advertisements. The third way to filter BGP advertisements uses access or prefix lists with the neighbor distribute-list command. If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group. Use the neighbor prefix-list command in address family configuration mode to filter NSAP BGP advertisements.

example

The following router configuration mode example applies the prefix list named abc to incoming advertisements from neighbor 120.23.4.1:

```
router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 prefix-list abc in
```

The following router configuration mode example applies the prefix list named CustomerA to incoming advertisements from neighbor 120.23.4.1:

```
router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 prefix-list CustomerA in
```

related commands

ip prefix-list

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

neighbor filter-list

3.1.27 neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the neighbor remote-as command in router configuration mode. To remove an entry from the table, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **remote-as** *number*

no neighbor {*ip-address* | *peer-group-name*} **remote-as** *number*

parameter

parameter	description

ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
Number	Nmuber of autonomous system to which the neighbor belongs.

default

none

command mode

BGP configuration mode

instruction

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the router bgp global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external. If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

The following example assigns a BGP router to autonomous system 109, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 131.108.0.0 and 192.31.7.0 with the neighbor routers.

```
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
```

related commands

neighbor peer-group (creating)

3.1.28 neighbor route-map

To apply a route map to incoming or outgoing routes, use the neighbor route-map command in address family or router configuration mode. To remove a route map, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **route-map** *map-name* {*in* | *out*} **no**

neighbor {*ip-address* | *peer-group-name*} **route-map** *map-name* {*in* | *out*}

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP or multiprotocol BGP peer group.
map-name	Name of a route map.
in	Applies route map to incoming routes.
Out	Applies route map to outgoing routes.

default

none

command mode

BGP configuration mode

instruction

It is only based on neighbor to filter routes using distribute-list, prefix-list and as-path-list, while it is not only based on neighbor to filter routes but also based on neighbor to modify the attribute of routes to realize a more flexible routing strategy.

Different routes have different attributes. The route-map can modify attributes of different kinds of routes. If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map. The rules which is valid to BGP route are as follows: match aspath-list、match community-list、match ip address 、match ip nexthop 、match ip prefix-list 、 match metric 、match tag 、set aggregator、set as-path、set atomic-aggregate、set community、set community-additive、 set ip nexthop、set local-preference、set metric、set origin、set tag、set weight.

If configured with a non-existent route-map, then all routes is allowed to receive as a result without any modification.

If you specify a BGP or multiprotocol BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

example

The following router configuration mode example applies a route map named internal-map to a BGP incoming route from 198.92.70.24:

```
router bgp 5
neighbor 198.92.70.24 route-map internal-map in
route-map internal-map
match as-path abc
set local-preference 100
```

related commands

neighbor peer-group (creating)

route-map 1

3.1.29 neighbor route-reflector-client

To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the neighbor route-reflector-client command in address family or router configuration mode. To indicate that the neighbor is not a client, use the no form of this command.

neighbor *ip-address* **route-reflector-client**

no neighbor *ip-address* **route-reflector-client**

parameter

parameter	description
ip-address	IP address of the BGP neighbor being identified as a client.

default

There is no route reflector in the autonomous system.

command mode

BGP configuration mode

instruction

By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.

If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Interior BGP peer is configured to be a route reflector responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.

Use the neighbor route-reflector-client command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.

The bgp client-to-client reflection command controls client-to-client reflection.

example

In the following router configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 198.92.70.24.

```
router bgp 5
neighbor 198.92.70.24 route-reflector-client
```

related commands

bgp cluster-id

show ip bgp

3.1.30 neighbor route-refresh

To allow neighbor to use route refresh function, use the neighbor route-refresh command. Use the no form of this command to disable route refresh function.

neighbor *ip-address* **route-refresh**

no neighbor *ip-address* **route-refresh**

parameter

parameter	description
ip-address	BGP neighbor and ip address

default

disabled

command mode

BGP configuration mode

instruction

By default, BGP route exchange for only once when the connection is established, then only exchanging changed routes afterwards. If the routing strategy configuration is modified, it will not become effective immediately. Generally, there are two methods:

- Reset BGP connection
- Use soft-reconfiguration function

The first method is relatively slow, and the routes vary greatly. The second method needs too much storage space and occupies more CPU time. These two methods are not good method, and therefore a new method arises, that is, the route refresh.

The route refresh is a negotiation option based on BGP connection, aiming to send the route refresh request packet to ask neighbor to re-send all update packets to oneself, which do not need to reset BGP connection and also do not need to store a great amount of routes. This a a more ideal solution at the moment.

example

The following example allows neighbor at address 198.92.70.24 to use route refresh function:

```
router bgp 5
neighbor 198.92.70.24 route-refresh
```

related commands

show ip bgp neighbors

3.1.31 neighbor send-community

To specify that a communities attribute should be sent to a BGP neighbor, use the neighbor send-community command in address family or router configuration mode. To remove the entry, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **send-community**

no neighbor {*ip-address* | *peer-group-name*} **send-community**

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.

default

The communities attribute can be sent to the neighbor.

command mode

BGP configuration mode

instruction

The route's group attribute of routes can be configured via the set community command of route-map or via neighbor's routing inform.

Use the show ip bgp neighbors command to see whether allows to send group attribute to neigh or not.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

In the following router configuration mode example, the router belongs to autonomous system 109 and is not permitted to send the communities attribute to its neighbor at IP address 198.92.70.23:

```
router bgp 109
no neighbor 198.92.70.23 send-community
```

related commands

match community-list **4**

neighbor peer-group (creating)

set community 15

set community-additive 17

3.1.32 neighbor shutdown

To disable a neighbor or peer group, use the neighbor shutdown command in router configuration mode. To reenable the neighbor or peer group, use the no form of this command.

neighbor {*ip-address* | *peer-group-name}* **shutdown**

no neighbor {*ip-address* | *peer-group-name}* **shutdown**

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.

default

none

command mode

BGP configuration mode

instruction

The neighbor shutdown command terminates any active session for the specified neighbor or peer group and removes all associated routing information. In the case of a peer group, a large number of peering sessions could be terminated suddenly. To display a summary of BGP neighbors and peer group connections, use the show ip bgp summary command. Those neighbors with an Idle status and the Admin entry have been disabled by the neighbor shutdown command.

related commands

show ip bgp summary

show ip bgp neighbors

3.1.33 neighbor soft-reconfiguration

To configure the software to start storing updates, use the neighbor soft-reconfiguration command in router configuration mode. To not store received updates, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**] **no**

neighbor {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]

parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
inbound	Indicates that the update to be stored is an incoming update.

default

The incoming update is not stored and the outgoing update is stored.

command mode

BGP configuration mode

instruction

Entering this command starts the storage of updates, which is required to do inbound soft reconfiguration. Outbound BGP soft reconfiguration does not require inbound soft reconfiguration to be enabled.

To use soft reconfiguration, or soft reset, without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the open message sent when the peers establish a TCP session. Clearing the BGP session using the neighbor soft-reconfiguration command has a negative effect on network operations and should only be used as a last resort. Routers can use the clear ip bgp {* | address | peer-group name} in command to clear the BGP session.

To determine whether a BGP router supports this capability, use the show ip bgp neighbors command. If a router supports the route refresh capability, the following message is displayed:

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

The following example enables inbound soft reconfiguration for the neighbor this 131.108.1.1. All the updates received from neighbor will be stored unmodified, regardless of the inbound policy.

```
router bgp 100
neighbor 131.108.1.1 remote-as 200
neighbor 131.108.1.1 soft-reconfiguration inbound
```

related commands

clear ip bgp

neighbor peer-group (creating)

3.1.34 neighbor timers

To set the timers for a specific BGP peer or peer group, use the neighbor timers command in router configuration mode. To clear the timers for a specific BGP peer or peer group, use the no form of this command.

neighbor {*ip-address* | *peer-group-name}* **timers keepalive** *holdtime*

no neighbor {*ip-address* | *peer-group-name*} **timers keepalive** *holdtime*

parameter

parameter	description
ip-address	A BGP peer or peer group IP address.
peer-group-name	Name of the BGP peer group.
Keepalive	Frequency (in seconds) with which the software sends keepalive messages to its peer.
Holdtime	Interval (in seconds) after not receiving a keepalive message that the software declares a peer dead.

default

keepalive: 60 s

holdtime: 180 s

command mode

BGP configuration mode

instruction

Generally, the value of holdtime is three times larger than keepalive. If you configure 0 as the value of keealive and holdtime, then the sending of keepalive packets is disabled, which needs tcp connection manager to inform BGP module for state change.

The timers configured for a specific neighbor or peer group override the timers configured for all BGP neighbors using the timers bgp command.

example

The following example changes the keepalive timer to 70 seconds and the hold-time timer to 210 seconds for the BGP peer 192.98.47.10:

router bgp 109

neighbor 192.98.47.10 timers 70 210

3.1.35 neighbor update-source

To have the software allow Border Gateway Protocol (BGP) sessions to use any operational interface for TCP connections, use the neighbor update-source command

in router configuration mode. To restore the interface assignment to the closest interface, which is called the best local address, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **update-source interface**

no neighbor {*ip-address* | *peer-group-name*} **update-source interface**

parameter

parameter	description
ip-address	IP address of the BGP-speaking neighbor.
peer-group-name	Name of a BGP peer group.
Interface	Interface name

default

Best local address

command mode

BGP configuration mode

instruction

By default, the ip module decides the local ip address of TCP connection when BGP establishes the connection. IP module decides interface depending on routes, and then binds the main ip address of this interface as the local address of TCP. Use the update-source command can bind the main ip address of the local specified interface during the establishment of TCP connection.

It is generally specified to use loopback interface, for the loopback interface ‘s protocol state is always up. And so this keeps the stability of BGP session and avoids route fluctuation.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface:

router bgp 110
network 160.89.0.0
neighbor 160.89.2.3 remote-as 110
neighbor 160.89.2.3 update-source Loopback0

related commands

neighbor peer-group (creating)

3.1.36 neighbor weight

To assign a weight to a neighbor connection, use the neighbor weight command in address family or router configuration mode. To remove a weight assignment, use the no form of this command.

neighbor {*ip-address* | *peer-group-name*} **weight** *weight*

no neighbor {*ip-address* | *peer-group-name*} **weight** *weight*

parameter

parameter	description
ip-address	IP address of the neighbor.
peer-group-name	Name of a BGP peer group.
Weight	Weight to assign. Acceptable values are from 0 to 65535.

default

Routes learned through another BGP peer have a default weight of 0 and routes sourced by the local router have a default weight of 32768.

command mode

BGP configuration mode

instruction

BGP routing metric is the important standard to choose routes. The default metric of all routes that learned from neighbors is 0. Use this command to set metric for routes that learned from neighbor.

If you specify a BGP peer group by using the peer-group-name argument, all the members of the peer group will inherit the characteristic configured with this command.

example

The following router configuration mode example sets the weight of all routes learned via 151.23.12.1 to 50:

router bgp 109 neighbor 151.23.12.1 weight 50

related commands

neighbor peer-group (creating)

set weight 23

3.1.37 network (BGP)

To specify the networks to be advertised by the Border Gateway Protocol (BGP), use the network command. To remove an entry from the routing table, use the no form of this command.

network A.B.C.D/n route-map *map-name* **backdoor**

no network A.B.C.D/n route-map *map-name* **backdoor**

parameter

parameter	description
A.B.C.D/n	Network prefix that BGP will advertise
route-map	The specified route map
map-name	Name of the route map
backdoor	Backdoor network

default

No networks are specified.

command mode

BGP configuration mode

instruction

There are three ways to specify the networks to be included by the BGP:

- Via the redistribute command to include routes dynamically
- Via the network command to include routes statically
- Via the aggregate command to include routes

All routes generated by these three methods are regarded as the local routes which can be informed to other peers but not to be included by local IP routing table.

A totally same route in the main routing table of IP is the basis for the network configured with the network command to become effective.

A more precise or totally same route in the local BTP routing table is the basis for the network to become effective that configured with the aggretgate-address command.

The length of mask code is generated in term of standard network type if not specified

Use the route-map to configure route's attribute.

The backdoor network is used to modify route distance rather than to generate routes. It changes route's default distance that learned from the neighbor to the local route's distance. The default value is 200.

The maximum number of network commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM.

BGP and multiprotocol BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

example

The following example sets up network 131.108.0.0/8 to be included in the BGP updates:

router bgp 120 network

131.108.0.0/8

related commands

redistribute (BGP)

aggregate-address

3.1.38 redistribute(BGP)

To redistribute a route process to Border Gateway Protocol (BGP), use the redistribute command. To remove the redistribute command from the configuration file, use the no form of this command.

redistribute protocol [*process-id*] [route-map *map-name*]

no redistribute protocol [*process-id*] [route-map *map-name*]

parameter

parameter	description
protocol	Type of routing protocol
process-id	Process id of routing protocol, such as process if of ospf

route-map	Applies route map to configure route attribute
map-name	Name of route map

default

disabled

command mode

BGP configuration mode

instruction

There are three ways to specify the networks to be included by the BGP:

- Via the redistribute command to include routes dynamically
- Via the network command to include routes statically
- Via the aggregate command to include routes

All routes generated by these three methods are regarded as the local routes which can be informed to other peers but not to be included by local IP routing table.

Use redistribute command to include routes dynamically to BGP. The change of route source will be reflected to BGP automatically. The automatically-included routes will be informed to other neighbors. The configuration of the redistribute command will re-check the specified type of routes in the routing table. The outer routes in OSPF will not be included to BGP.

Use the route-map to configure route's attribute.

example

The following example configures routes from OSPF process 23 to be redistributed into BGP:

```
router bgp 109
redistribute ospf 23
```

related commands

route-map 1

3.1.39 router bgp

To configure the BGP routing process, use the router bgp command in global configuration mode. To remove a routing process, use the no form of this command.

router bgp *as-number*

no router bgp *as-number*

parameter

parameter	description
as-number	Number of autonomous system

default

No BGP routing process is enabled by default.

command mode

global configuration mode

instruction

The system allows to configure one BGP process at most. The BGP task is established in the process of system initialization, and it is activated when the BGP process is started up. The BGP task only receives information from command module without configuring the BGP process. It is not related to routing module or any other module and will not response other information. The related show and clear command are all invalid.

Use no router bgp command to delete BGP process, and at the same time other configuration related to BGP will also be deleted, such as neighbors and so on. The BGP route in routing table is also be deleted.

To configure BGP process using the show running and show ip bgp summary command to check.

example

The following example configures a BGP process for autonomous system 200:

router bgp 200

related commands

neighbor remote-as

3.1.40 show ip bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use the show ip bgp command in user EXEC or privileged EXEC mode.

show ip bgp [**network**]

parameter

	parameter	description	
	network	Displays the specified routing information	

command mode

EXEC

instruction

The show ip bgp command is used to display the contents of the BGP routing table. The output can be filtered to display entries for a specific prefix, prefix length, and prefixes injected through a prefix list, route map, or conditional advertisement.

example

The following is a group of BGP displaying information. The former two lines display some marked information.

Status code indicates the status of the table entry. The status is displayed at the beginning of each line in the table. S indicates the table entry is suppressed, which is the invalid route and will not be chosen. D indicates the table entry is dampened, which is the invalid route. H indicates the table entry history, which is not a ture route and is the invalid route. “* “indicates the table entry is valid, which can be chosen as the best route.” > “indiates the table entry is the best entry to use for that network. “I” indicates the table entry was learned via an internal BGP (iBGP) session.

Origin codes indicates the origin of the entry. I is the entry originated from an Interior Gateway Protocol (IGP). E is the entry originated from an Exterior Gateway Protocol (EGP). ? is the origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.

IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network. Local preference value as set with the set local-preference route-map configuration command. The default value is 100. Weight of the route as set via autonomous system filters. Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The last line displays number of routes, including all valid and invalid routes.

```
B3710_118#show ip bgp
Status codes: s suppressed, d damped, h history, * valid, > best, i internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  192.168.10.0/24  192.168.69.5                         0 10 400 i
```

```
*>i192.168.10.0/24      192.168.69.14                100      0 (65030) 400 i
*>i192.168.11.0/24      192.168.69.14                100      0 (65030) 400 i
*    192.168.65.0/30    192.168.69.1                 100      0 (65020) 10 ?
*> 192.168.65.0/30      192.168.69.5                          0 10 ?
*    192.168.65.4/30    192.168.69.1                 100      0 (65020) 10 ?
*> 192.168.65.4/30      192.168.69.5                          0 10 ?
*    192.168.65.8/30    192.168.69.1                 100      0 (65020) 10 ?
*> 192.168.65.8/30      192.168.69.5                          0 10 ?
*    192.168.66.0/30    192.168.66.2                 100      0 (65020) ?
*> 192.168.66.0/30      0.0.0.0                               32768 ?
* i192.168.66.4/30      192.168.66.6                 100      0 ?
*> 192.168.66.4/30      0.0.0.0                               32768 ?
*>i192.168.66.8/30      192.168.66.6                 100      0 ?
*>i192.168.67.0/30      192.168.69.18          200   100      0 500 ?

Number of displayed routes: 15
```

related commands

show ip bgp community

show ip bgp neighbors

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

3.1.41 show ip bgp community

To display routes that belong to specified BGP communities, use the show ip bgp community command in EXEC mode.

show ip bgp community

parameter

none

command mode

exec

instruction

This command is used to display statistics information of BGP communities attribute structure in the system.

related commands

show ip bgp

show ip bgp neighbors

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

3.1.42 show ip bgp neighbors

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the show ip bgp neighbors command.

show ip bgp neighbors [*ip-address*] [**received-routes | routes** | **advertised-routes**]

parameter

parameter	description
ip-ddress	IP address of a neighbor. If this parameter is omitted, information about all neighbors is displayed.
received-routes	Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the received-routes keyword.
advertised-routes	Displays all routes that have been advertised to neighbors.

command mode

EXEC

instruction

Use the show ip bgp neighbors command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based on the function or attribute that is displayed in the output.

related commands

show ip bgp

show ip bgp community

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

3.1.43 show ip bgp paths

To display all the BGP paths in the database, use the show ip bgp paths command in EXEC mode.

show ip bgp paths

parameter

none

command mode

EXEC

instruction

This command is used to display statistics information of BGP paths structure.

related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

3.1.44 show ip bgp prefix-list

To display information about a prefix list or prefix list entries, use the show ip prefix-list command.

show ip bgp prefix-list {*prefix-list name*}

parameter

parameter	description
prefix-list name	Name of prefix-list

command mode

EXEC

instruction

This command specifies prefix-list to filter display of the show ip bgp command. Only the routes matching the prefix-list will be displayed.

related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

ip prefix-list

ip prefix-list description

ip prefix-list sequence-number

show ip prefix-list

clear ip prefix-list

3.1.45 show ip bgp regexp

To display routes matching the autonomous system path regular expression, use the show ip bgp regexp command in EXEC mode.

show ip bgp regexp regular-expression

parameter

parameter	description
regular-expression	Regular expression to match the BGP autonomous system paths.

command mode

EXEC

instruction

This command specifies the regular expression to filter the display of the show ip bgp command. Only the routes matching the regular expression will be displayed.

related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

3.1.46 show ip bgp summary

To display the status of all Border Gateway Protocol (BGP) connections, use the show ip bgp summary command.

show ip bgp summary

parameter

This command has no parameters or keywords.

command mode

EXEC

instruction

The show ip bgp summary command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.

A prefix is an IP address and network mask. It can represent an entire network, a subset of a network, or a single host route. A path is a route to a given destination. By default, BGP will install only a single path for each destination. If multipath routes are configured, BGP will install a path entry for each multipath route, and only one multipath route will be marked as the bestpath.

BGP attribute and cache entries are displayed individually and in combinations that affect the bestpath selection process. The fields for this output are displayed when the related BGP feature is configured or attribute is received. Memory usage is displayed in bytes.

example

The following is sample output from the show ip bgp summary command:

router bgp 4 BGP
local AS is 4
Router ID is 192.168.20.72 IGP
synchronization is enabled
Distance: external 20 internal 200

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/Pref
192.168.20.12	4	5	0	0	0	0	0	never	Connect

related commands

show ip bgp

show ip bgp community

show ip bgp neighbors

show ip bgp paths

show ip bgp prefix-list

show ip bgp regexp

show ip bgp summary

3.1.47 synchronization

To enable the synchronization between BGP and your Interior Gateway Protocol (IGP) system, use the synchronization command in address family or router configuration mode. Use the no form of this command to disable this function.

synchronization

no synchronization

parameter

none

default

enabled

command mode

BGP configuration mode

instruction

Usually, a BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. By default, synchronization between BGP and the IGP is turned off to allow the software to advertise a network route without waiting for route validation from the IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems.

IGP function is enabled by default.

To enable to advertise a network route without waiting for the IGP, use the no form of this command.

example

The following example enables router to advertise the route without waiting for IGP synchronization.

```
router bgp 120
no synchronization
```

related commands

router bgp

3.1.48 table-map

To modify metric and tag values when the IP routing table is updated with BGP learned routes, use the table-map command in address family or router configuration mode. To disable this function, use the no form of the command.

table-map <*name*>

no table-map <*name*>

parameter

parameter	description
name	Route map name from the route-map command.

default

none

command mode

BGP configuration mode

instruction

This command adds the route map name defined by the route-map command to the IP routing table. This command is used to set the tag name and the route metric to implement redistribution.

example

none

related commands

none

3.1.49 timers

To adjust BGP network timers, use the timers bgp command. To reset the BGP timing defaults, use the no form of this command.

timers bgp <*keepalive*> <*holdtime*>

no timers bgp <*keepalive*> <*holdtime*>

parameter

parameter	description
keepalive	Frequency (in seconds) with which the software sends keepalive messages to its peer.
holdtime	Interval (in seconds) after not receiving a keepalive message that the software declares a peer dead.

default

Keepalive: 60 seconds

Holdtime: 180 seconds

command mode

BGP configuration mode

instruction

Configure BGP neighbor clock in global configuration mode to modify default clock configuration. The configuration towards neighbor is prior to global configuration.

example

The following example changes the keepalive timer to 10 seconds and the hold-time timer to 40 seconds:

```
router bgp 100
timers bgp 10 40
```

related commands

neighbor timers