BGP Commands

Use the commands in this chapter to configure and monitor Border Gateway Protocol (BGP). For BGP configuration information and examples, refer to the “Configuring BGP” chapter of the Network Protocols Configuration Guide, Part 1.
aggregate-address

To create an aggregate entry in a BGP routing table, use the aggregate-address router configuration command. To disable this function, use the no form of this command.

```
aggregate-address address mask [as-set] [summary-only] [suppress-map map-name]
    [advertise-map map-name] [attribute-map map-name]
no aggregate-address address mask [as-set] [summary-only] [suppress-map map-name]
    [advertise-map map-name] [attribute-map map-name]
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Aggregate address.</td>
</tr>
<tr>
<td>mask</td>
<td>Aggregate mask.</td>
</tr>
<tr>
<td>as-set</td>
<td>(Optional) Generates autonomous system set path information.</td>
</tr>
<tr>
<td>summary-only</td>
<td>(Optional) Filters all more specific routes from updates.</td>
</tr>
<tr>
<td>suppress-map map-name</td>
<td>(Optional) Name of route map used to select the routes to be suppressed.</td>
</tr>
<tr>
<td>advertise-map map-name</td>
<td>(Optional) Name of route map used to select the routes to create AS-SET origin communities.</td>
</tr>
<tr>
<td>attribute-map map-name</td>
<td>(Optional) Name of route map used to set the attribute of the aggregate route.</td>
</tr>
</tbody>
</table>

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

You can implement aggregate routing in BGP either by redistributing an aggregate route into BGP or by using this conditional aggregate routing feature.

Using the aggregate-address command with no arguments will create an aggregate entry in the BGP routing table if there are any more-specific BGP routes available that fall in the specified range. The aggregate route will be advertised as coming from your autonomous system and has 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
**aggregate-address** when aggregating many paths, because this route must be continually withdrawn and re-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, 193.*.*.*) but will also suppress advertisements of more-specific routes to all neighbors. If you only want to suppress advertisements to certain neighbors, you may use the **neighbor distribute-list** command, with caution. If a more specific route leaks out, all BGP speakers 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.

**Example**

The following example creates an aggregate address. The path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized.

```plaintext
router bgp 5
aggregate-address 193.0.0.0 255.0.0.0 as-set
```

**Related Commands**

You can use the master indexes or search online to find documentation of related commands.

- **match as-path**
- **match ip address**
- **route-map**
auto-summary

To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the auto-summary router configuration command. To disable this feature and transmit subprefix routing information across classful network boundaries, use the no form of this command.

```
auto-summary
no auto-summary
```

Syntax Description

This command has no arguments or keywords.

Default

Enabled (the software summarizes subprefixes to the classful network boundary when crossing classful network boundaries).

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Route summarization reduces the amount of routing information in the routing tables.

By default, BGP does not accept subnets redistributed from IGP. To advertise and carry subnet routes in BGP, use an explicit network command or the no auto-summary command. If you disable auto-summarization and have not entered a network command, you will not advertise network routes for networks with subnet routes unless they contain a summary route.

Example

In the following example, network numbers are not summarized automatically:

```
router bgp 6
no auto-summary
```
**bgp always-compare-med**

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

```
bgp always-compare-med
no bgp always-compare-med
```

**Syntax Description**

This command has no arguments or keywords.

**Default**

The Cisco IOS software does not compare MEDs for paths from neighbors in different autonomous systems.

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 11.0.

The MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED.

By default, during the best-path selection process, MED comparison is done only among paths from the same autonomous system. This command changes the default behavior by allowing comparison of MEDs among paths regardless of the autonomous system from which the paths are received.

**Example**

The following example configures the BGP speaker in autonomous system 100 to compare MEDs among alternative paths, regardless of the autonomous system from which the paths are received:

```
router bgp 109
bgp always-compare-med
```
**bgp bestpath as-path ignore**

To prevent the router from considering as-path as a factor in the algorithm for choosing a route, use the `bgp bestpath as-path ignore` router configuration command. To allow the router to consider as-path in choosing a route, use the `no` form of this command.

```plaintext
bgp bestpath as-path ignore
no bgp bestpath as-path ignore
```

**Syntax Description**

This command has no arguments or keywords.

**Default**

The router considers as-path in choosing a route.

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 12.0.

**Example**

The following example prevents the BGP router from considering as-path as a factor in choosing a route.

```plaintext
router bgp 210
bgp bestpath as-path ignore
```

**Related Commands**

`show ip bgp neighbor`
bgp bestpath med-confed

To enable MED comparison among paths learned from confederation peers, use the `bgp bestpath med-confed` router configuration command. To prevent the software from considering the MED attribute in comparing paths, use the `no` form of this command.

```
bgp bestpath med-confed
no bgp bestpath med-confed
```

Syntax Description

This command has no arguments or keywords.

Default

The software does not consider the MED attribute when choosing among paths learned from confederation peers.

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0.

The comparison between MEDs is only made if there are no external ASs in the path (an external AS is an AS that is not within the confederation). If there is an external AS in the path, then the external MED is passed transparently through the confederation, and the comparison is not made.

For example, assume that AS 65000, 65001, 65002, and 65004 are part of the confederation; AS1 is not; and we are comparing route A with four paths. If `bgp bestpath med-confed` is enabled, path 1 would be chosen. The fourth path has a lower MED, but it is not involved in the MED comparison because there is an external AS in this path.

```
path= 65000 65004, med=2
path= 65001 65004, med=3
path= 65002 65004, med=4
path= 65003 1, med=1
```

Example

The following command enables the BGP router to compare MED values for paths learned from confederation peers.

```
router bgp 210
  bgp bestpath med-confed
```

Related Commands

```
show ip bgp
show ip bgp neighbors
```
To have Cisco IOS software consider a missing MED attribute in a path as having a value of infinity, making the path without a MED value the least desirable path, use the `bgp bestpath missing-as-worst` router configuration command. To return the router to the default (assign a value of 0 to the missing MED), use the no form of this command.

```
bgp bestpath missing-as-worst
no bgp bestpath missing-as-worst
```

**Syntax Description**
This command has no arguments or keywords.

**Default**
The software assigns a value of 0 to the missing MED, causing the path with the missing MED attribute to be considered the best path.

**Command Mode**
Router configuration

**Usage Guidelines**
This command first appeared in Cisco IOS Release 12.0.

**Example**
The following command specifies that the BGP router to consider a missing MED attribute in a path as having a value of infinity, making this path the least desirable path.

```
router bgp 210
bgp bestpath missing-as-worst
```

**Related Commands**
- `show ip bgp`
- `show ip bgp neighbors`
bgp client-to-client reflection

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

    bgp client-to-client reflection
    no bgp client-to-client reflection

Syntax Description

This command has no arguments or keywords.

Default

When a route reflector is configured, the route reflector reflects routes from a client to other clients.

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

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. Use the no bgp client-to-client reflection command to disable client-to-client reflection.

If client-to-client reflection is enabled, the clients of a route reflector cannot be members of a peer group.

Example

In the following example, the local router is a route reflector. The three neighbors are fully meshed, so client-to-client reflection is disabled.

    router bgp 5
    neighbor 155.24.95.22 route-reflector-client
    neighbor 155.24.95.23 route-reflector-client
    neighbor 155.24.95.24 route-reflector-client
    no bgp client-to-client reflection

Related Commands

You can use the master indexes or search online to find documentation of related commands.

    bgp cluster-id
    neighbor route-reflector-client
    show ip bgp
To configure the cluster ID if the BGP cluster has more than one route reflector, use the `bgp cluster-id` router configuration command. To remove the cluster ID, use the `no` form of this command.

```
bgp cluster-id  cluster-id
no bgp cluster-id  cluster-id
```

**Syntax Description**

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

**Default**

The router ID of the single route reflector in a cluster

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 11.0.

Together, a route reflector and its clients form a cluster.

Usually a cluster of clients will have a single route reflector. In that case, the cluster is identified by the router ID of the route reflector. In order to increase redundancy and avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster.

If the cluster has more than one route reflector, use this command to configure the cluster ID.

**Example**

In the following example, the local router 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**

You can use the master indexes or search online to find documentation of related commands.

- `bgp client-to-client reflection`
- `neighbor route-reflector-client`
- `show ip bgp`
**bgp confederation identifier**

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

```
bgp confederation identifier autonomous-system
no bgp confederation identifier autonomous-system
```

**Syntax Description**

Table:

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autonomous-system</td>
<td>Autonomous system number that internally includes multiple autonomous systems.</td>
</tr>
</tbody>
</table>

**Default**

No confederation identifier is configured.

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.3.

Another way to reduce the IBGP mesh is to divide an autonomous system into multiple autonomous systems and group them into a single confederation. Each autonomous system is fully meshed within itself, and has a few connections to another autonomous system in the same confederation. Even though the peers in different autonomous systems have EBGP sessions, they exchange routing information as if they are IBGP peers. Specifically, the next-hop and local preference information is preserved. This enables you to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems. To the outside world, the confederation looks like a single autonomous system.

**Example**

In the following example, the autonomous system is divided into autonomous systems 4001, 4002, 4003, 4004, 4005, 4006, and 4007 and identified by the confederation identifier 5. Neighbor 1.2.3.4 is someone inside your routing domain confederation. Neighbor 3.4.5.6 is someone outside your routing domain confederation. To the outside world, there appears to be a single autonomous system with the number 5.

```
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**

You can use the master indexes or search online to find documentation of related commands.

```
bgp confederation peers
```
bpg confederation peers

To configure the autonomous systems that belong to the confederation, use the 
bpg confederation peers router configuration command. To remove an autonomous system from
the confederation, use the no form of this command.

bpg confederation peers autonomous-system [autonomous-system]
no bpg confederation peers autonomous-system [autonomous-system]

Syntax Description

autonomous-system Autonomous system number.

Default

No confederation peers are configured.

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

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

Example

The following example specifies that autonomous systems 1090, 1091, 1092, and 1093 belong to a
single confederation:

```
router bgp 1090
  bpg confederation peers 1091 1092 1093
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

bpg confederation identifier
bgp dampening

To enable BGP route dampening or change various BGP route dampening factors, use the `bgp dampening` global configuration command. To disable the function or restore the default values, use the `no` form of this command.

```
bgp dampening [half-life reuse suppress max-suppress-time] [route-map map]
no bgp dampening [half-life reuse suppress max-suppress-time] [route-map map]
```

**Syntax Description**

**half-life**

(Optional) 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 (which is 15 minutes by default). The process of reducing the penalty happens every 5 seconds. The range of the half-life period is 1 to 45 minutes. The default is 15 minutes.

**reuse**

(Optional) If the penalty for a flapping route decreases enough to fall below this value, the route is unsuppressed. The process of unsuppressing routes occurs at 10-second increments. The range of the reuse value is 1 to 20000; the default is 750.

**suppress**

(Optional) A route is suppressed when its penalty exceeds this limit. The range is 1 to 20000; the default is 2000.

**max-suppress-time**

(Optional) Maximum time (in minutes) a route can be suppressed. The range is 1 to 20000; the default is 4 times the `half-life`. If the `half-life` value is allowed to default, the maximum suppress time defaults to 60 minutes.

**route-map map**

(Optional) Name of route map that controls where BGP route dampening is enabled.

**Default**

Disabled by default.

- `half-life` is 15 minutes
- `reuse` is 750
- `suppress` is 2000
- `max-suppress-time` is 4 times `half-life`

**Command Mode**

Global configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 11.0.

If this command is used with no arguments, it enables BGP route dampening. The arguments `half-life`, `reuse`, `suppress`, and `max-suppress-time` are position-dependent. Therefore, if any of them are used, they must all be specified.
Example

The following example sets the half-life to 30 minutes, the reuse value to 1500, the suppress value to 10000; and the maximum suppress time to 120 minutes:

```
bgp dampening 30 1500 10000 120
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- `clear ip bgp dampening`
- `clear ip bgp flap-statistics`
- `show ip bgp dampened-paths`
- `show ip bgp flap-statistics`
**bgp default local-preference**

To change the default local preference value, use the `bgp default local-preference` router configuration command. To return to the default setting, use the `no` form of this command.

```
bgp default local-preference value
no bgp default local-preference value
```

**Syntax Description**

- `value`  
  Local preference value from 0 to 4294967295. Higher is more preferred.

**Default**

Local preference value of 100

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0.

Generally, the default value of 100 allows you to easily define a particular path as less preferable than paths with no local preference attribute. The preference is sent to all routers and access servers in the local autonomous system.

**Example**

The following example raises the default local preference value from the default of 100 to 200:

```
router bgp 200
bgp default local-preference 200
```

**Related Commands**

You can use the master indexes or search online to find documentation of related commands.

`set local-preference`
To have Cisco IOS software compare the MED variable when choosing among routes advertised by the same sub-AS within a confederation, use the `bgp deterministic med` router configuration command. To disallow the comparison, use the `no` form of this command.

```
bgp deterministic med
no bgp deterministic med
```

Syntax Description

This command has no arguments or keywords.

Default

The software does not compare the MED variable for paths advertised by a sub-AS.

Command Mode

Router configuration mode

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0.

If `bgp always-compare-med` is enabled, all paths are fully comparable, including those from other ASes in the confederation, even if `bgp deterministic med` is also enabled.

Example

The following example specifies that the BGP router compare MED variables when choosing among routes advertised by the same sub-AS within a confederation.

```
router 204
  bgp deterministic med
```

Related Commands

```
show ip bgp
show ip bgp neighbors
```
**bgp log-neighbor-changes**

To enable logging of BGP neighbor resets, use the `bgp log-neighbor-changes` router configuration command. To disable the logging of changes in BGP neighbor adjacencies, use the `no` form of this command.

```
bgp log-neighbor-changes
no bgp log-neighbor-changes
```

**Syntax Description**

This command has no arguments or keywords.

**Default**

No BGP neighbor changes are logged.

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 11.1 CC and 12.0.

The `bgp log-neighbor-changes` command enables logging of BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

Using the `bgp log-neighbor-changes` command to enable status change message logging does not create a significant performance hit, unlike, for example, enabling per BGP update debugging. If the UNIX syslog facility is enabled, messages are sent to the UNIX host running the syslog daemon so that the messages can be stored and archived. If the UNIX syslog facility is not enabled, the status change messages are retained in the router’s internal buffer, and are not stored to disk. You can set the size of this buffer, which is dependent upon the available RAM, using the `logging buffered` command.

The neighbor status change messages are not tracked if `bgp log-neighbor changes` is not enabled, except for the reset reason, which is always available as output of the `show ip bgp neighbor` command.

The log messages display the following reasons for changes in a neighbor’s status:

- BGP protocol initialization
- No memory for path entry
- No memory for attribute entry
- No memory for prefix entry
- No memory for aggregate entry
- No memory for dampening info
- No memory for BGP updates
- BGP Notification received
- Erroneous BGP Update received
- User reset request
The `bgp log-neighbor-changes` command enables logging of Enhanced IGRP neighbor adjacencies, but messages for BGP neighbors are logged only if they are specifically enabled with the `bgp log-neighbor-changes` command.

Use the `show logging` command to display the log for the BGP neighbor changes.

Example

The following configuration will log neighbor changes for BGP:

```
  bgp router 100
  bgp log-neighbor-changes
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
  logging buffered
  show ip bgp neighbor
  show logging
```
bgp fast-external-fallover

To immediately reset the BGP sessions of any directly adjacent external peers if the link used to reach them goes down, use the `bgp fast-external-fallover` router configuration command. To disable this function, use the `no` form of this command.

```
bgp fast-external-fallover
no bgp fast-external-fallover
```

Syntax Description
This command has no arguments or keywords.

Default
Enabled

Command Mode
Router configuration

Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.

Example
The following example disables the automatic resetting of BGP sessions:

```
router bgp 109
no bgp fast-external-fallover
```
clear ip bgp

To reset a BGP connection using BGP soft reconfiguration, use the clear ip bgp EXEC command at the system prompt.

\[ \text{clear ip bgp \{* | address | peer-group name\} [soft [in | out]]} \]

Syntax Description

- \*: Resets all current BGP sessions.
- address: Resets only the identified BGP neighbor.
- peer-group-name: Resets the specified BGP peer group.
- soft: (Optional) Soft reconfiguration.
- in | out: (Optional) Triggers inbound or outbound soft reconfiguration. If the in or out option is not specified, both inbound and outbound soft reconfiguration are triggered.

Command Mode
EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

If you specify BGP soft reconfiguration, by including the soft keyword, the sessions are not reset and the router sends all routing updates again. To generate new inbound updates without resetting the BGP session, the local BGP speaker should store all received updates without modification regardless of whether it is accepted by the inbound policy, using the neighbor soft-reconfiguration command. This process is memory intensive and should be avoided if possible. Outbound BGP soft configuration does not have any memory overhead. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes in the BGP timer’s specifications
- Changes to the BGP administrative distance
- Changes to BGP-related route maps

Example

The following example resets all current BGP sessions:

\[ \text{clear ip bgp *} \]
Related Commands

You can use the master indexes or search online to find documentation of related commands.

- clear ip bgp
- neighbor soft-reconfiguration
- show ip bgp
- timers bgp
clear ip bgp dampening

To clear BGP route dampening information and unsuppress the suppressed routes, use the `clear ip bgp dampening` EXEC command.

`clear ip bgp dampening [address mask]`

**Syntax Description**

- `address` (Optional) IP address of the network about which to clear dampening information.
- `mask` (Optional) Network mask applied to the `address`.

**Command Mode**

EXEC

**Usage Guidelines**

This command first appeared in Cisco IOS Release 11.0.

**Example**

The following example clears route dampening information about the route to network 150.0.0.0 and unsuppresses its suppressed routes:

```
clear ip bgp dampening 150.0.0.0 255.255.0.0
```

**Related Commands**

You can use the master indexes or search online to find documentation of related commands.

- `bgp dampening`
- `show ip bgp dampened-paths`
clear ip bgp flap-statistics

To clear BGP flap statistics, use the clear ip bgp flap-statistics EXEC command.

    clear ip bgp flap-statistics [{regexp regexp} | {filter-list list} | {address mask}]
    clear ip bgp address flap-statistics

Syntax Description

regexp regexp   (Optional) Clears flap statistics for all the paths that match the regular expression.

filter-list list (Optional) Clears flap statistics for all the paths that pass the access list.

address         (Optional) Clears flap statistics for a single entry at this IP address. If this argument is placed before flap-statistics, the router clears flap statistics for all paths from the neighbor at this address.

mask            (Optional) Network mask applied to the address.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

If no arguments or keywords are specified, the router clears flap statistics for all routes.

The flap statistics for a route are also cleared when a BGP peer is reset. Although the reset withdraws the route, there is no penalty applied in this instance even though route flap dampening is enabled.

Example

The following example clears all of the flap statistics for paths that pass access list 3:

    clear ip bgp flap-statistics filter-list 3

Related Commands

You can use the master indexes or search online to find documentation of related commands.

    bgp dampening
clear ip bgp peer-group

To remove all the members of a BGP peer group, use the `clear ip bgp peer-group` EXEC command.

```
clear ip bgp peer-group tag
```

Syntax Description

```
tag
```
Name of the BGP peer group to clear.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Example

The following example removes all members from the BGP peer group `internal`:

```
clear ip bgp peer-group internal
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

`neighbor peer-group (assigning members)`
default-information originate (BGP)

To allow the redistribution of network 0.0.0.0 into BGP, use the default-information originate router configuration command. To disable this function, use the no form of this command.

```
default-information originate
no default-information originate
```

Syntax Description
This command has no arguments or keywords.

Default
Disabled

Command Mode
Router configuration

Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.
The same functionality will result from the network 0.0.0.0 command, using the network router configuration command.

Example
The following example configures BGP to redistribute network 0.0.0.0 into BGP:

```
router bgp 164
   default-information originate
```

Related Commands
You can use the master indexes or search online to find documentation of related commands.

neighbor ebgp-multihop
**default-metric (BGP, OSPF, and RIP)**

To set default metric values for the BGP, OSPF, and RIP routing protocols, use this form of the `default-metric` router configuration command. To return to the default state, use the `no` form of this command.

```
default-metric number
no default-metric number
```

**Syntax Description**

`number`  
Default metric value appropriate for the specified routing protocol.

**Default**

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

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0.

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.

In BGP, this sets the Multi Exit Discriminator (MED) metric. (The name of this metric for BGP Versions 2 and 3 is INTER_AS.)

**Example**

The following example shows a router in autonomous system 109 using both the RIP and the OSPF routing protocols. The example advertises OSPF-derived routes using the RIP protocol and assigns the IGRP-derived routes a RIP metric of 10.

```
router rip
  default-metric 10
  redistribute ospf 109
```

**Related Commands**

You can use the master indexes or search online to find documentation of related commands.

`redistribute`
distance bgp

To allow the use of external, internal, and local administrative distances that could be a better route to a node, use the distance bgp router configuration command. To return to the default values, use the no form of this command.

```
distance bgp external-distance internal-distance local-distance
no distance bgp
```

Syntax Description

- **external-distance**: Administrative distance for BGP external routes. External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Acceptable values are from 1 to 255. The default is 20. Routes with a distance of 255 are not installed in the routing table.

- **internal-distance**: Administrative distance for BGP internal routes. Internal routes are those routes that are learned from another BGP entity within the same autonomous system. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.

- **local-distance**: Administrative distance for BGP local routes. Local routes are those networks listed with a network router configuration command, often as back doors, for that router or for networks that are being redistributed from another process. Acceptable values are from 1 to 255. The default is 200. Routes with a distance of 255 are not installed in the routing table.

Defaults

```
external-distance: 20
internal-distance: 200
local-distance: 200
```

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

An administrative distance is 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 an integer between 0 and 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, or if some internal routes should really be preferred by BGP.

**Note** Changing the administrative distance of BGP internal routes is considered dangerous and is not recommended. One problem that can arise is the accumulation of routing table inconsistencies, which can break routing.
Example

In the following example, internal routes are known to be preferable to those learned through the
IGP, so the administrative distance values are set accordingly:

    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 bgp 20 20 200
**ip as-path access-list**

To define a BGP-related access list, use the `ip as-path access-list` global configuration command. To disable use of the access list, use the `no` form of this command.

```
ip as-path access-list access-list-number (permit | deny) as-regular-expression
no ip as-path access-list access-list-number (permit | deny) as-regular-expression
```

### Syntax Description

- **access-list-number**: Integer from 1 to 199 that indicates the regular expression access list number.
- **permit**: Permits access for matching conditions.
- **deny**: Denies access to matching conditions.
- **as-regular-expression**: Autonomous system in the access list using a regular expression. See the “Regular Expressions” appendix in the Dial Solutions Command Reference for information about forming regular expressions.

### Default

No access lists are defined.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

You can specify an access list filter on both inbound and outbound BGP routes. In addition, you can assign weights based on a set of filters. Each filter is an access list based on regular expressions. If the regular expression matches the representation of the autonomous system path of the route as an ASCII string, then the `permit` or `deny` condition applies. The autonomous system path does not contain the local autonomous system number. Use the `ip as-path access-list` global configuration command to define an BGP access list, and the `neighbor` router configuration command to apply a specific access list.

### Example

The following example specifies that the BGP neighbor with IP address 128.125.1.1 is not sent advertisements about any path through or from the adjacent autonomous system 123:

```
ip as-path access-list 1 deny _123_
ip as-path access-list 1 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 1 out
```
ip as-path access-list

Related Commands
You can use the master indexes or search online to find documentation of related commands.

   neighbor distribute-list
   neighbor filter-list
ip bgp-community new-format

To display BGP communities in the format AA:NN (AS-community number/2-byte number), use the **ip bgp-community new-format** global configuration command. To re-enable the previous display format for BGP communities (NN:AA), use the **no** form of this command.

```
ip bgp-community new-format
no ip bgp-community new-format
```

Syntax Description
This command has no argument or keywords.

Usage Guidelines
This command first appeared in Cisco IOS Release 12.0.

The BGP communities RFC specifies that a BGP community is made up of two parts 2 bytes long. The first part is the AS number and the second part is a 2 byte number. In the most recent version of the RFC, a community is of the form AA:NN. The Cisco default community format is in the format NNAA. The **ip bgp-community new-format** command changes the community format to AANN to conform to the most recent RFC.

Example

```
router# show ip bgp community 12345:111 local-as
BGP table version is 10, local router ID is 224.0.0.10
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric LocPrf Weight Path
*> 2.2.2.2/32       158.43.222.2           0             0 222 ?
*> 111.0.0.0        158.43.222.2           0             0 222 ?
*> 158.43.0.0       158.43.222.2           0             0 222 ?
*> 158.43.44.44/32  158.43.222.2           0             0 222 ?
```

Related Command
**show ip bgp x.x.x.x**

Related Command
**show ip bgp x.x.x.x**

Related Command
**show ip bgp x.x.x.x**

Related Command
**show ip bgp x.x.x.x**
### ip community-list

To create a community list for BGP and control access to it, use the `ip community-list` global configuration command. To delete the community list, use the `no` form of this command.

```
ip community-list community-list-number {permit | deny} community-number
no ip community-list community-list-number
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>community-list-number</code></td>
<td>Integer from 1 to 99 that identifies one or more permit or deny groups of communities.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Permits access for a matching condition.</td>
</tr>
<tr>
<td><code>deny</code></td>
<td>Denies access for a matching condition.</td>
</tr>
<tr>
<td><code>community-number</code></td>
<td>Community number configured by a <code>set community</code> command. Valid value is one of the following:</td>
</tr>
<tr>
<td></td>
<td>• A number from 1 to 4294967200. You can specify a single number or multiple numbers separated by a space.</td>
</tr>
<tr>
<td></td>
<td>• <code>internet</code>—The Internet community.</td>
</tr>
<tr>
<td></td>
<td>• <code>no-export</code>—Routes with this community are sent to peers in other sub-autonomous systems within a confederation. Do not advertise this route to an EBGP peer. External systems are those outside the confederation. If there is no confederation, an external system is any EBGP peer.</td>
</tr>
<tr>
<td></td>
<td>• <code>local-as</code> Send this route to peers in other sub-autonomous systems within the local confederation. Do not advertise this route to an external system.</td>
</tr>
<tr>
<td></td>
<td>• <code>no-advertise</code> Do not advertise this route to any peer (internal or external).</td>
</tr>
</tbody>
</table>

#### Default

Once you permit a value for the community number, the community list defaults to an implicit deny for everything else that has not been permitted.

#### Command Mode

Global configuration

#### Usage Guidelines

This command first appeared in Cisco IOS Release 10.3. The `local-as` attribute was added in Cisco IOS Release 12.0.
Example

In the following example, Cisco IOS software permits all routes except the routes with the communities 5 and 10 or 10 and 15:

   ip community-list 1 deny 5 10
   ip community-list 1 deny 10 15
   ip community-list 1 permit internet

The following example permits all routes within the local autonomous system:

   ip community-list 1 permit local-as

Related Commands

You can use the master indexes or search online to find documentation of related commands.

set community
show ip bgp community
match as-path

To match a BGP autonomous system path access list, use the **match as-path** route-map configuration command. To remove a path list entry, use the **no** form of this command.

```
match as-path path-list-number
no match as-path path-list-number
```

**Syntax Description**

```
path-list-number           Autonomous system path access list. An integer from 1 to 199.
```

**Default**

No path lists are defined.

**Command Mode**

Route-map configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0.

The values set by the **match** and **set** commands override global values. For example, the weights assigned with the **match as-path** and **set weight** route-map commands override the weights assigned using the **neighbor weight** and **neighbor filter-list** commands.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route-map section with an explicit match specified.

The implemented weight is based on the first matched autonomous system path.

**Example**

The following example sets the autonomous system path to match BGP autonomous system path access list 20:

```
route-map igp2bgp
match as-path 20
```

**Related Commands**

You can use the master indexes or search online to find documentation of related commands.

```
match community-list
match interface
match ip address
match ip next-hop
match ip route-source
match metric
match route-type
match tag
```
route-map
set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
set weight
To match a BGP community, use the `match community-list` route-map configuration command. To remove the community list entry, use the `no` form of this command.

```
match community-list community-list-number [exact]
no match community-list community-list-number [exact]
```

### Syntax Description

- `community-list-number` Community list number in the range 1 to 99.
- `exact` (Optional) Indicates an exact match is required. All of the communities and only those communities in the community list must be present.

### Default

No community list is defined.

### Command Mode

Route-map configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

A route map can have several parts. Any route that does not match at least one `match` clause relating to a `route-map` command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route-map section with an explicit match specified.

Matching based on community list is one of the types of match clauses applicable to BGP.

### Examples

In the following example, the routes that match community list 1 will have the weight set to 100. Any route that has community 109 will have the weight set to 100.

```
ip community-list 1 permit 109
!
routemap set_weight
  match community-list 1
  set weight 100
```

In the following example, the routes that match community list 1 will have the weight set to 200. Any route that has community 109 alone will have the weight set to 200.

```
ip community-list 1 permit 109
!
routemap set_weight
  match community-list 1 exact
  set weight 200
```
Related Commands

You can use the master indexes or search online to find documentation of related commands.

- route-map
- set weight
neighbor advertisement-interval

To set the minimum interval between the sending of BGP routing updates, use the `neighbor advertisement-interval` router configuration command. To remove an entry, use the `no` form of this command.

```
neighbor {ip-address | peer-group-name} advertisement-interval seconds
no neighbor {ip-address | peer-group-name} advertisement-interval seconds
```

Syntax Description

- `ip-address` Neighbor’s IP address.
- `peer-group-name` Name of a BGP peer group.
- `seconds` Time in seconds. Integer from 0 to 600.

Default

30 seconds for external peers and 5 seconds for internal peers.

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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 sets the minimum time between sending BGP routing updates to 10 seconds:

```
router bgp 5
neighbor 4.4.4.4 advertisement-interval 10
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

`neighbor peer-group (creating)`
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** router configuration command. To send no route as a default, use the **no** form of this command.

```
neighbor {ip-address | peer-group-name} default-originate [route-map map-name]
no neighbor {ip-address | peer-group-name} default-originate [route-map map-name]
```

**Syntax Description**

- **ip-address**
  - Neighbor’s IP address.

- **peer-group-name**
  - Name of a BGP peer group.

- **route-map map-name**
  - (Optional) Name of the route map. The route map allows route 0.0.0.0 to be injected conditionally.

**Default**

No default route is sent to the neighbor.

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 11.0. Modifications to permit extended access lists first appeared in Cisco IOS Release 12.0.

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.

**Examples**

In the following example, the local router injects route 0.0.0.0 to the neighbor 160.89.2.3 unconditionally:

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

In the following example, the local router injects route 0.0.0.0 to the neighbor 160.89.2.3 only if there is a route to 198.92.68.0 (that is, if a route with any mask exists, such as 255.255.255.0 or 255.255.0.0):

```
router bgp 109
  network 160.89.0.0
  neighbor 160.89.2.3 remote-as 200
  neighbor 160.89.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
  match ip address 1
!
access-list 1 permit 198.92.68.0
```

In the following example, the last line of the configuration has been changed to show the use of an extended access list. The local router injects route 0.0.0.0 to the neighbor 160.89.2.3 only if there is a route to 198.92.68.0 with a mask of 255.255.0.0:

```
router bgp 109
  network 160.89.0.0
  neighbor 160.89.2.3 remote-as 200
  neighbor 160.89.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
  match ip address 1
!
access-list 100 permit ip host 198.92.68.0 host 255.255.255.0
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

neighbor ebgp-multihop
neighbor description

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

```
neighbor {ip-address | peer-group-name} description text
no neighbor {ip-address | peer-group-name} description [text]
```

Syntax Description

- `ip-address` Neighbor’s IP address.
- `peer-group-name` Name of a BGP peer group.
- `text` Text (up to 80 characters) that describes the neighbor.

Default

There is no description of the neighbor.

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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
```
neighbor distribute-list

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

```
neighbor (ip-address | peer-group-name) distribute-list (access-list-number | name/ prefix-list prefixlistname) {in | out}
no neighbor (ip-address | peer-group-name) distribute-list (access-list-number | name) {in | out}
```

Syntax Description

- `ip-address`  Neighbor’s IP address.
- `peer-group-name`  Name of a BGP peer group.
- `access-list-number | name`  Number or name of a standard or extended access list. It can be an integer from 1 to 199.
- `in`  Access list is applied to incoming advertisements to that neighbor.
- `out`  Access list is applied to outgoing advertisements from that neighbor.

Default

No BGP neighbor is specified.

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The `peer-group-name` argument first appeared in Cisco IOS Release 11.0. The `access-list-name` argument first appeared in Cisco IOS Release 11.2.

Using distribute lists is one of two ways to filter BGP advertisements. The other way is to use AS-path filters, as with the `ip as-path access-list` global configuration command and the `neighbor filter-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.

Example

The following example applies list 39 to incoming advertisements to neighbor 120.23.4.1:

```
router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 distribute-list 39 in
```
Related Commands

You can use the master indexes or search online to find documentation of related commands.

- `ip as-path access-list`
- `neighbor filter-list`
- `neighbor peer-group (creating)`
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` router configuration command. 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
```

Syntax Description

- `ip-address`           IP address of the BGP-speaking neighbor.
- `peer-group-name`      Name of a BGP peer group.
- `ttl`                  (Optional) Time-to-live in the range 1 to 255 hops.

Default

Only directly connected neighbors are allowed.

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The `peer-group-name` argument first appeared in Cisco IOS Release 11.0.

This feature should only be used under the guidance of technical support staff.

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.

To prevent the creation of loops through oscillating routes, the multihop will not be established if the only route to the multihop peer is the default route (0.0.0.0).

Example

The following example allows connections to or from 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

You can use the master indexes or search online to find documentation of related commands.

- `neighbor default-originate`
- `neighbor peer-group (creating)`
- `network (BGP)`
neighbor filter-list

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

```
neighbor {ip-address | peer-group-name} filter-list access-list-number {in | out | weight weight}
no neighbor {ip-address | peer-group-name} filter-list access-list-number {in | out | weight weight}
```

Syntax Description

- **ip-address**: IP address of the neighbor.
- **peer-group-name**: Name of a BGP peer group.
- **access-list-number**: Number of an autonomous system path access list. You define this access list with the `ip as-path access-list` command.
- **in**: Access list to incoming routes.
- **out**: Access list to outgoing routes.
- **weight weight**: Assigns a relative importance to incoming routes matching autonomous system paths. Acceptable values are 0 to 65535.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

This command establishes filters on both inbound and outbound BGP routes. Any number of weight filters are allowed on a per-neighbor basis, but only one in or out filter is allowed. The weight of a route affects BGP’s route-selection rules.

The implemented weight is based on the first matched autonomous system path. Weights indicated when an autonomous system path is matched override the weights assigned by global neighbor commands. In other words, the weights assigned with the `match as-path` and `set weight` route-map commands override the weights assigned using the `neighbor weight` and `neighbor filter-list` commands.

See the “Regular Expressions” appendix in the Dial Solutions Command Reference for information on forming regular expressions.

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

In the following 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 123:

```
ip as-path access-list 1 deny _123_
ip as-path access-list 1 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 1 out
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
ip as-path access-list
neighbor distribute-list
neighbor peer-group (creating)
neighbor weight
```
neighbor maximum-prefix

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

```
neighbor {ip-address | peer-group-name} maximum-prefix maximum [threshold]
[warning-only]
no neighbor {ip-address | peer-group-name} maximum-prefix maximum
```

Syntax 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.
- **threshold** (Optional): Integer specifying at what percentage of `maximum` the router starts to generate a warning message. The range 1 to 100; the default is 75 (percent).
- **warning-only** (Optional): Allows the router to generate log message when the `maximum` is exceeded, instead of terminating the peering.

Default

Disabled; there is no limit on the number of prefixes.

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

This command allows you to configure a maximum number of prefixes 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 keyword `warning-only` 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
```
neighbor maximum-prefix

Related Commands
You can use the master indexes or search online to find documentation of related commands.

  clear ip bgp
neighbor next-hop-self

To disable next-hop processing of BGP updates on the router, use the **neighbor next-hop-self** router configuration command. 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
```

**Syntax Description**

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

**Default**

Disabled

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0. The `peer-group-name` argument first appeared in Cisco IOS Release 11.0.

This command is useful in nonmeshed networks (such as Frame Relay or X.25) where BGP neighbors may not have direct access to all other neighbors on the same IP 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.

For a finer granularity of control, see the **set ip next-hop** command.

**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**

You can use the master indexes or search online to find documentation of related commands.

- **neighbor peer-group (creating)**
- **set ip next-hop**
To enable MD5 authentication on a TCP connection between two BGP peers, use the `neighbor password` router configuration command. To disable this function, use the `no` form of this command.

```
neighbor (ip-address | peer-group-name) password string
no neighbor (ip-address | peer-group-name) password
```

**Syntax Description**

- `ip-address`: IP address of the BGP-speaking neighbor.
- `peer-group-name`: Name of a BGP peer group.
- `string`: Case-sensitive password of up to 80 characters. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces. You cannot specify a password in the format `number-space-anything`. The space after the number causes problems.

**Default**

Disabled

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 11.0.

You can invoke authentication between two BGP peers, causing each segment sent on the TCP connection between them to be verified. This feature must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. The authentication feature uses the MD5 algorithm. Specifying this command causes the generation and checking of the MD5 digest on every segment sent on the TCP connection.

Configuring a password for a neighbor will cause an existing session to be torn down and a new one established.

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.

If a router has a password configured for a neighbor, but the neighbor router does not, a message such as the following will appear on the console while the routers attempt to establish a BGP session between them:

```
%TCP-6-BADAUTH: No MD5 digest from [peer’s IP address]:11003 to [local router’s IP address]:179
```

Similarly, if the two routers have different passwords configured, a message such as the following will appear on the console:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer’s IP address]:11004 to [local router’s IP address]:179
```
Example

The following example enables the authentication feature between this router and the BGP neighbor at 131.102.1.1. The password that must also be configured for the neighbor is $bla4u00=2nkq$.

```
router bgp 109
  neighbor 131.108.1.1 password bla4u00=2nkq
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- `neighbor peer-group (creating)`
**neighbor peer-group (assigning members)**

To configure a BGP neighbor to be a member of a peer group, use the **neighbor peer-group** router configuration command. To remove the neighbor from the peer group, use the **no** form of this command.

```
neighbor ip-address peer-group peer-group-name
no neighbor ip-address peer-group peer-group-name
```

**Syntax Description**

- `ip-address`  
  IP address of the BGP neighbor who belongs to the peer group specified by the `tag`.
- `peer-group-name`  
  Name of the BGP peer group to which this neighbor belongs.

**Default**

There are no BGP neighbors in a peer group.

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 11.0.

The neighbor at the IP address indicated inherits all the configured options of the peer group.

**Example**

The following example assigns three neighbors to the peer group named `internal`:

```
router bgp 100
neighbor internal peer-group
neighbor internal remote-as 100
neighbor internal update-source loopback 0
neighbor internal route-map set-med out
neighbor internal filter-list 1 out
neighbor internal filter-list 2 in
neighbor 171.69.232.53 peer-group internal
neighbor 171.69.232.54 peer-group internal
neighbor 171.69.232.55 peer-group internal
neighbor 171.69.232.55 filter-list 3 in
```

**Related Commands**

You can use the master indexes or search online to find documentation of related commands.

- **neighbor peer-group (creating)**
- **neighbor shutdown**
neighbor peer-group (creating)

To create a BGP peer group, use the **neighbor peer-group** router configuration command. To remove the peer group and all of its members, use the **no** form of this command.

```
neighbor peer-group-name peer-group
no neighbor peer-group-name peer-group
```

**Syntax Description**

```
peer-group-name
```

Name of the BGP peer group.

**Default**

There is no BGP peer group.

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 11.0.

Often in a BGP speaker, there are many neighbors configured with the same update policies (that is, same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and make update calculation more efficient.

Peer group members can spanned multiple logical IP subnets, and can transit, or pass along, routes from one peer group member to another.

Once a peer group is created with the **neighbor peer-group** command, it can be configured with the **neighbor** commands. By default, members of the peer group inherit all the configuration options of the peer group. Members can also be configured to override the options that do not affect outbound updates.

Peer group members will always inherit the following configuration options: remote-as (if configured), version, update-source, out-route-map, out-filter-list, out-dist-list, minimum-advertisement-interval, and next-hop-self. All the peer group members will inherit changes made to the peer group.

If a peer group is not configured with a remote-as, the members can be configured with the **neighbor {ip-address | peer-group-name} remote-as** command. This command allows you to create peer groups containing EBGP neighbors.

**Example for an IBGP Peer Group**

In the following example, the peer group named **internal** configures the members of the peer group to be IBGP neighbors. By definition, this is an IBGP peer group because the **router bgp** command and the **neighbor remote-as** command indicate the same autonomous system (in this case, AS 100).
All the peer group members use loopback 0 as the update source and use set-med as the outbound route-map. The neighbor internal filter-list 2 in command shows that, except for 171.69.232.55, all the neighbors have filter-list 2 as the inbound filter list.

```
router bgp 100
neighbor internal peer-group
neighbor internal remote-as 100
neighbor internal update-source loopback 0
neighbor internal route-map set-med out
neighbor internal filter-list 1 out
neighbor internal filter-list 2 in
neighbor 171.69.232.53 peer-group internal
neighbor 171.69.232.54 peer-group internal
neighbor 171.69.232.55 peer-group internal
neighbor 171.69.232.55 filter-list 3 in
```

Example for an EBGP Peer Group

The following example defines the peer group named external-peers without the neighbor remote-as command. This is what makes it an EBGP peer group. Each individual member of the peer group is configured with its respective AS-number separately. Thus the peer group consists of members from autonomous systems 200, 300, and 400. All the peer group members have set-metric route map as an outbound route map and filter-list 99 as an outbound filter list. Except for neighbor 171.69.232.110, all of them have 101 as the inbound filter list.

```
router bgp 100
neighbor external-peers peer-group
neighbor external-peers route-map set-metric out
neighbor external-peers filter-list 99 out
neighbor external-peers filter-list 101 in
neighbor 171.69.232.90 remote-as 200
neighbor 171.69.232.90 peer-group external-peers
neighbor 171.69.232.100 remote-as 300
neighbor 171.69.232.100 peer-group external-peers
neighbor 171.69.232.110 remote-as 400
neighbor 171.69.232.110 peer-group external-peers
neighbor 171.69.232.110 filter-list 400 in
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- `clear ip bgp peer-group`
- `neighbor peer-group (assigning members)`
- `show ip bgp peer-group`
neighbor prefix-list

To distribute BGP neighbor information as specified in a prefix list, use the neighbor access-list router configuration command. To remove an entry, 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}
```

Syntax Description

- **ip-address**: Neighbor’s IP address.
- **peer-group-name**: Name of a BGP peer group.
- **prefix-list**: Applies a prefix list to the route to be matched.
- **prefix-listname**: Name of a prefix list.
- **in**: Access list is applied to incoming advertisements to that neighbor.
- **out**: Access list is applied to outgoing advertisements from that neighbor.

Default

No BGP neighbor is specified.

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 12.0.

Using prefix lists is one of two ways to filter BGP advertisements. The other way is to use AS-path filters, as with the `ip as-path access-list` global configuration command and the `neighbor filter-list` command, and access or prefix lists, as 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.

**Note**  Do not use both `neighbor access-list` and `neighbor prefix-list` commands for a single BGP peer. Do not apply both a `neighbor distribute-list` and a `neighbor prefix-list` command to the same neighbor.

Examples

The following example applies prefix list `abc` to incoming advertisements to neighbor 120.23.4.1:

```bash
router bgp 109
network 131.108.0.0
neighbor 120.23.4.1 prefix-list abc in
```
The following example applies prefix list CustomerA to incoming advertisements to neighbor 120.23.4.1:

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- clear ip prefix-list
- ip as-path access-list
- ip prefix-list
- ip prefix-list description
- ip prefix-list sequence-number
- neighbor filter-list
- neighbor peer-group (creating)
- show ip prefix-list
neighbor remote-as

To add an entry to the BGP neighbor table, use the `neighbor remote-as` router configuration command. 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
```

**Syntax Description**

- `ip-address` Neighbor’s IP address.
- `peer-group-name` Name of a BGP peer group.
- `number` Autonomous system to which the neighbor belongs.

**Default**

There are no BGP neighbor peers.

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0. The `peer-group-name` argument first appeared in Cisco IOS Release 11.0.

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.

**Examples**

The following example specifies that a router at the address 131.108.1.2 is a neighbor in autonomous system number 109:

```
router bgp 110
  network 131.108.0.0
  neighbor 131.108.1.2 remote-as 109
```
neighbor remote-as

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. The first router listed is in the same Class B network address space, but in a different autonomous system; the second neighbor command illustrates specification of an internal neighbor (with the same autonomous system number) at address 131.108.234.2; and the last neighbor command specifies a neighbor on a different network.

```
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

You can use the master indexes or search online to find documentation of related commands.

```
neighbor peer-group (creating)
```
neighbor route-map

To apply a route map to incoming or outgoing routes, use the `neighbor route-map` router configuration command. 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}
```

Syntax Description

- `ip-address` Neighbor’s IP address.
- `peer-group-name` Name of a BGP peer group.
- `map-name` Name of route map.
- `in` Apply to incoming routes.
- `out` Apply to outgoing routes.

Default

No route maps are applied to a peer.

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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.

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 applies a route map named `internal-map` to 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 1
  set local-preference 100
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

`neighbor peer-group (creating)`
neighbor route-reflector-client

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 router configuration command. To indicate that the neighbor is not a client, use the no form of this command. When all the clients are disabled, the local router is no longer a route reflector.

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

Syntax 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

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

By default, all 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.

If you use route reflectors, all IBGP speakers need not be fully meshed. In the route reflector model, an internal 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.

If client-to-client reflection is enabled (by default it is enabled), clients of a route reflector cannot be members of a peer group. The bgp client-to-client reflection command controls client-to-client reflection.

Example

In the following 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

You can use the master indexes or search online to find documentation of related commands.

- bgp client-to-client reflection
- bgp cluster-id
- show ip bgp
To specify that a COMMUNITIES attribute should be sent to a BGP neighbor, use the `neighbor send-community` router configuration command. 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
```

**Syntax Description**

- `ip-address` Neighbor’s IP address.
- `peer-group-name` Name of a BGP peer group.

**Default**

No COMMUNITIES attribute is sent to any neighbor.

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.3. The `peer-group-name` argument first appeared in Cisco IOS Release 11.0.

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 example, the router belongs to autonomous system 109 and is configured to send the COMMUNITIES attribute to its neighbor at IP address 198.92.70.23:

```
router bgp 109
neighbor 198.92.70.23 send-community
```

**Related Commands**

You can use the master indexes or search online to find documentation of related commands.

- `match community-list`
- `neighbor peer-group (creating)`
- `set community`
neighbor shutdown

To disable a neighbor or peer group, use the `neighbor shutdown` router configuration command. To re-enable 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
```

**Syntax Description**

- `ip-address` Neighbor’s IP address.
- `peer-group-name` Name of a BGP peer group.

**Default**

No change is made to the status of any BGP neighbor or peer group.

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 12.0.

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, this could mean a large number of peering sessions are suddenly terminated.

To view 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.

“State/PfxRcd” shows the current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the `neighbor maximum prefix` command) is reached, the string “PfxRcd” appears in the entry, the neighbor is shut down, and the connection is Idle.

**Related Commands**

You can use the master indexes or search online to find documentation of related commands.

- `neighbor maximum prefix`
- `show ip bgp summary`
neighbor soft-reconfiguration

To configure the Cisco IOS software to start storing updates, use the neighbor soft-reconfiguration router configuration command. 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]
```

Syntax Description

- **ip-address**: IP address of the BGP-speaking neighbor.
- **peer-group-name**: Name of a BGP peer group.
- **inbound**: Keyword indicating that the update to be stored is an incoming update.

Inbound is currently required with this command, since a keyword is required and no other keywords are available.

Default

Soft reconfiguration is not enabled

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

This command requires at least one keyword. Currently the only keyword available is **inbound**, so the use of **inbound** is not optional.

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

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 131.108.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy. When inbound soft reconfiguration is done later, the stored information will be used to generate a new set of inbound updates.

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

You can use the master indexes or search online to find documentation of related commands.

- clear ip bgp
- neighbor peer-group (creating)
neighbor timers

To set the timers for a specific BGP peer or peer group, use the `neighbor timers` router configuration command. 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
```

**Syntax Description**

- `ip-address` (Optional) A BGP peer or peer group IP address.
- `peer-group-name` (Optional) Name of the BGP peer group.
- `keepalive` Frequency, in seconds, with which the Cisco IOS software sends `keepalive` messages to its peer. The default is 60 seconds.
- `holdtime` Interval, in seconds, after not receiving a `keepalive` message that the software declares a peer dead. The default is 180 seconds.

**Default**

- `keepalive`: 60 seconds
- `holdtime`: 180 seconds

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 12.0

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

**Example**

The following example changes the keepalive timer to 70 seconds and the holdtime timer to 210 seconds for the BGP peer 192.98.47.0:

```
routerv bgp 109
neighbor 192.98.47.0 timers 70 210
```
neighbor update-source

To have the Cisco IOS software allow internal BGP sessions to use any operational interface for TCP connections, use the `neighbor update-source` router configuration command. 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
```

Syntax Description

- `ip-address` IP address of the BGP-speaking neighbor.
- `peer-group-name` Name of a BGP peer group.
- `interface` Loopback interface.

Default

Best local address

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

This feature works in conjunction with the loopback interface feature described in the “Interface Configuration Overview” chapter of the Cisco IOS Interface Configuration Guide.

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 loopback interface’s IP address rather than the best local address:

```
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

You can use the master indexes or search online to find documentation of related commands.

`neighbor peer-group (creating)`
neighbor version

To configure the Cisco IOS software to accept only a particular BGP version, use the neighbor version router configuration command. To use the default version level of a neighbor, use the no form of this command.

```
neighbor {ip-address | peer-group-name} version value
no neighbor {ip-address | peer-group-name} version value
```

Syntax Description

- **ip-address**: IP address of the BGP-speaking neighbor.
- **peer-group-name**: Name of a BGP peer group.
- **value**: BGP version number. The version can be set to 2 to force the software to only use Version 2 with the specified neighbor. The default is to use Version 4 and dynamically negotiate down to Version 2 if requested.

Default

BGP Version 4

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Entering this command disables dynamic version negotiation.

Our implementation of BGP supports BGP Versions 2, 3, and 4. If the neighbor does not accept default Version 4, dynamic version negotiation is implemented to negotiate down to Version 2.

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 locks down to Version 4 of the BGP protocol:

```
router bgp 109
neighbor 131.104.27.2 version 4
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- **neighbor peer-group (creating)**
neighbor weight

To assign a weight to a neighbor connection, use the `neighbor weight` router configuration command. 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
```

Syntax Description

- `ip-address` Neighbor’s IP address.
- `peer-group-name` Name of a BGP peer group.
- `weight` Weight to assign. Acceptable values are 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

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

All routes learned from this neighbor will have the assigned weight initially. The route with the highest weight will be chosen as the preferred route when multiple routes are available to a particular network.

The weights assigned with the `match as-path` and `set weight` route-map commands override the weights assigned using the `neighbor weight` and `neighbor filter-list` commands.

---

**Note** For weight changes to take effect, it may be necessary to use `clear ip bgp peer-group *`.

---

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 sets the weight of all routes learned via 151.23.12.1 to 50:

```
router bgp 109
neighbor 151.23.12.1 weight 50
```
neighbor weight

Related Commands

You can use the master indexes or search online to find documentation of related commands.

neighbor distribute-list
neighbor filter-list
neighbor peer-group (creating)
**network (BGP)**

To specify the list of networks for the BGP routing process, use this form of the `network` router configuration command. To remove an entry, use the `no` form of this command.

```
network network-number [mask network-mask]
no network network-number [mask network-mask]
```

**Syntax Description**

- `network-number` Network that BGP will advertise.
- `mask` Network or subnetwork mask.
- `network-mask` (Optional) Network mask address.

**Default**

No networks are specified.

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0. The limit of 200 network commands per BGP router was removed in Cisco IOS Release 12.0.

These types of networks can be learned from connected routes, dynamic routing, and from static route sources.

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

**Example**

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

```
  router bgp 120
  network 131.108.0.0
```

**Related Commands**

You can use the master indexes or search online to find documentation of related commands.

- `default-information originate (BGP)`
- `neighbor ebgp-multihop`
- `network backdoor`
- `network mask`
- `network weight`
- `router bgp`
network backdoor

To specify a backdoor route to a BGP border router that will provide better information about the network, use the network backdoor router configuration command. To remove an address from the list, use the no form of this command.

- network address backdoor
- no network address backdoor

Syntax Description

**address**

IP address of the network to which you want a backdoor route.

Default

No network is advertised.

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

A backdoor network is treated as a local network, except that it is not advertised.

Example

The following example configures network 131.108.0.0 as a local network and network 192.31.7.0 as a backdoor network:

```
router bgp 109
network 131.108.0.0
network 192.31.7.0 backdoor
```
**network weight**

To assign an absolute weight to a BGP network, use the `network weight` router configuration command. To delete an entry, use the `no` form of the command.

```
network address mask weight weight [route-map map-name]
no network address mask weight weight [route-map map-name]
```

**Syntax Description**

- `address`  
  IP address of the network.
- `mask`  
  Network mask of the network.
- `weight`  
  Absolute weight, or importance. It can be an integer from 0 to 65535.
- `route-map map-name`  
  (Optional) Name of route-map.

**Default**

Weight is unmodified. Weight is zero if the original default weight has not been modified by other router configuration commands.

**Command Mode**

Router configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0.

The weight specified by this command overrides a weight assigned by the `redistribute` command.

**Example**

In the following example, the BGP network has a weight of 100:

```
router bgp 5
  network 193.0.0.0 255.0.0.0 weight 100
```
**router bgp**

To configure the Border Gateway Protocol (BGP) routing process, use the `router bgp` global configuration command. To remove a routing process, use the `no` form of this command.

```
router bgp autonomous-system
no router bgp autonomous-system
```

**Syntax Description**

- **autonomous-system**: Number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.

**Default**

No BGP routing process is enabled by default.

**Command Mode**

Global configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0.

This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

**Example**

The following example configures a BGP process for autonomous system 120:

```
router bgp 120
```

**Related Commands**

You can use the master indexes or search online to find documentation of related commands.

- `network (BGP)`
- `timers bgp`
**set as-path**

To modify an autonomous system path for BGP routes, use the `set as-path` route map configuration command. To not modify the autonomous system path, use the `no` form of this command.

```
set as-path { tag | prepend as-path-string }
no set as-path { tag | prepend as-path-string }
```

**Syntax Description**

- **tag**
  - Converts the tag of a route into an autonomous system path. Applies only when redistributing routes into BGP.

- **prepend as-path-string**
  - Appends the string following the keyword `prepend` to the as-path of the route that is matched by the route map. Applies to inbound and outbound BGP route maps.

**Default**

Autonomous system path is not modified.

**Command Mode**

Route map configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 11.0.

The only global BGP metric available to influence the best path selection is the AS-PATH length. By varying the length of the AS-PATH, a BGP speaker can influence the best path selection by a peer further away.

By allowing you to convert the tag into an autonomous system path, the `set as-path tag` variation of this command modifies the autonomous system length. The `set as-path prepend` variation allows you to “prepend” an arbitrary autonomous system path string to BGP routes. Usually the local autonomous system number is prepended multiple times. This increases the autonomous system path length.

**Examples**

The following example converts the tag of a redistributed route into an autonomous system path:

```
route-map set-as-path-from-tag
match as-path 2
    set as-path prepend 100 100 100
!
router bgp 100
    redistribute ospf 109 route-map set-as-path-from-tag
```
The following example prepends 100 100 100 to all the routes advertised to 131.108.1.1:

```conf
route-map set-as-path
  match as-path 1
  set as-path prepend 100 100 100
!
router bgp 100
  neighbor 131.108.1.1 route-map set-as-path out
```

**Related Commands**

You can use the master indexes or search online to find documentation of related commands.

- `match as-path`
- `match community-list`
- `match interface`
- `match ip address`
- `match ip next-hop`
- `match ip route-source`
- `match metric`
- `match route-type`
- `match tag`
- `route-map`
- `set automatic-tag`
- `set community`
- `set level`
- `set local-preference`
- `set metric`
- `set metric-type`
- `set next-hop`
- `set origin`
- `set tag`
- `set weight`
**set comm-list delete**

To remove communities from the community attribute of an inbound or outbound update, use the **set comm-list delete** configuration command. To negate a previous **set comm-list delete** command, use the **no** form of this command.

```
set comm-list list-num delete
no set comm-list list-num delete
```

### Syntax Description

- **list-num**
  
  A standard or extended community list number.

### Default

No communities are removed.

### Command Mode

Router configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 12.0.

This route-map set command removes communities from the community attribute of an inbound or outbound update using a route map to filter and determine the communities to be deleted. Depending upon whether the route map is applied to the inbound or outbound update for a neighbor, each community that passes the route map “permit” clause and matches the given community list will be removed from the community attribute being received from or sent to the BGP neighbor.

Each entry of a standard community list should list only one community when used with the **set comm-list delete** command. For example, in order to be able to delete communities 10:10 and 10:20, you must use the following format to create the entries:

```
ip community-list 5 permit 10:10
ip community-list 5 permit 10:20
```

The following format for a community list entry, while acceptable otherwise, does not work with the **set comm-list delete** command:

```
config ip community-list 5 permit 10:10 10:20
```

When both the **set community comm** and **set comm-list list-num delete** commands are configured in the same sequence of a route-map attribute, the deletion operation (**set comm-list list-num delete**) is performed before the set operation (**set community comm**).

### Example

In the following example, the communities 100:10 and 100:20 (if present) will be deleted from updates received from 171.69.233.33. Also, except for 100:50, all communities beginning with 100: will be deleted from updates sent to 171.69.233.33.

```
router bgp 100
neighbor 171.69.233.33 remote-as 120
neighbor 171.69.233.33 route-map ROUTEMAPIN in
```
set comm-list delete

neighbor 171.69.233.33 route-map ROUTEMAPOUT out

ip community-list 1 permit 100:10
ip community-list 1 permit 100:20

ip community-list 120 deny 100:50
ip community-list 120 permit 100:.*

route-map ROUTEMAPIN permit 10
set comm-list 1 delete

route-map ROUTEMAPOUT permit 10
set comm-list 120 delete

Related Commands
You can use the master indexes or search online to find documentation of related commands.

set community \textit{comm}
**set community**

To set the BGP COMMUNITIES attribute, use the `set community` route-map configuration command. To delete the entry, use the `no` form of this command.

```
set community { community-number [additive] } | none
no set community { community-number [additive] } | none
```

**Syntax Description**

- `community-number`: Valid values are 1 to 4294967200, `no-export`, or `no-advertise`.
- `additive`: (Optional) Adds the community to the already existing communities.
- `none`: Removes the COMMUNITY attribute from the prefixes that pass the route-map.

**Default**

No BGP COMMUNITIES attributes exist.

**Command Mode**

Route-map configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.3.

You must have a match clause (even if it points to a “permit everything” list) if you want to set tags.

Use the `route-map` global configuration command, and the `match` and `set` route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each `route-map` command has a list of `match` and `set` commands associated with it. The `match` commands specify the `match criteria`—the conditions under which redistribution is allowed for the current `route-map command`. The `set` commands specify the `set actions`—the particular redistribution actions to perform if the criteria enforced by the `match` commands are met. The `no route-map` command deletes the route map.

The `set` route-map configuration commands specify the redistribution `set actions` to be performed when all of a route map’s match criteria are met. When all match criteria are met, all set actions are performed.
Examples

In the following example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to no-export (these routes will not be advertised to any EBGP peers).

```
route-map set_community 10 permit
match as-path 1
set community 109

route-map set_community 20 permit
match as-path 2
set community no-export
```

In the following similar example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to local-as (the router will not advertise this route to an EBGP peer outside the local autonomous system).

```
route-map set_community 10 permit
match as-path 1
set community 109

route-map set_community 20 permit
match as-path 2
set community local-as
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
ip community-list
match community-list
route-map
set comm-list delete
show ip bgp community
```
set dampening

To set the BGP route dampening factors, use the set dampening route-map configuration command. To disable this function, use the no form of this command.

```
set dampening half-life reuse suppress max-suppress-time
no set dampening
```

Syntax Description

- **half-life**: 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 (which is 15 minutes by default). The process of reducing the penalty happens every 5 seconds. The range of the half-life period is 1 to 45 minutes. The default is 15 minutes.

- **reuse**: If the penalty for a flapping route decreases enough to fall below this value, the route is unsuppressed. The process of unsuppressing routes occurs at 10-second increments. The range of the reuse value is 1 to 20000; the default is 750.

- **suppress**: A route is suppressed when its penalty exceeds this limit. The range is 1 to 20000; the default is 2000.

- **max-suppress-time**: Maximum time (in minutes) a route can be suppressed. The range is 1 to 20000; the default is 4 times the half-life. If the half-life value is allowed to default, the maximum suppress time defaults to 60 minutes.

Default

Disabled

Command Mode

Route-map configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

You must have a match clause (even if it points to a “permit everything” list) if you want to set tags.

Use the route-map global configuration command, and the match and set route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each route-map command has a list of match and set commands associated with it. The match commands specify the match criteria—the conditions under which redistribution is allowed for the current route-map command. The set commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the match commands are met. The no route-map command deletes the route map.

The set route-map configuration commands specify the redistribution set actions to be performed when all of a route map’s match criteria are met. When all match criteria are met, all set actions are performed.
When a BGP peer is reset, the route is withdrawn and the flap statistics cleared. In this instance, the withdrawal does not incur a penalty even though route flap dampening is enabled.

Example

The following example sets the half-life to 30 minutes, the reuse value to 1500, the suppress value to 10000; and the maximum suppress time to 120 minutes:

```conf
route-map tag
    match as-path 10
    set dampening 30 1500 10000 120
!
router bgp 100
    neighbor 171.69.233.52 route-map tag in
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- `match as-path`
- `match community-list`
- `match interface`
- `match ip address`
- `match ip next-hop`
- `match ip route-source`
- `match metric`
- `match route-type`
- `match tag`
- `route-map`
- `set as-path`
- `set automatic-tag`
- `set community`
- `set level`
- `set local-preference`
- `set metric`
- `set metric-type`
- `set next-hop`
- `set origin`
- `set tag`
- `set weight`
- `show route-map`
**set ip next-hop**

To indicate where to output packets that pass a match clause of a route map for policy routing, use the `set ip next-hop` route map configuration command. To delete an entry, use the `no` form of this command.

```
set ip next-hop ip-address [...ip-address] [peer-address]
no set ip next-hop ip-address [...ip-address] [peer-address]
```

**Syntax Description**

- **ip-address**
  - IP address of the next hop to which packets are output. It need not be an adjacent router.

- **peer-address**
  - (Optional) Sets the next hop to be the BGP peering address.

**Default**

Disabled

**Command Mode**

Route map configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 11.0. The keyword `peer-address` first appeared in Cisco IOS Release 12.0.

Use the `ip policy route-map` interface configuration command, the `route-map` global configuration command, and the `match` and `set` route map configuration commands, to define the conditions for policy routing packets. The `ip policy route-map` command identifies a route map by name. Each `route-map` command has a list of `match` and `set` commands associated with it. The `match` commands specify the `match criteria`—the conditions under which policy routing occurs. The `set` commands specify the `set actions`—the particular routing actions to perform if the criteria enforced by the `match` commands are met.

If the first next hop specified with the `set ip next-hop` command is down, the optionally specified IP addresses are tried in turn.

When `set ip next-hop` is used with the `peer-address` keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. This means that the same route map can be applied to multiple BGP peers to override third-party next hops.

When `set ip next-hop` is used with the `peer-address` keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. This command has finer granularity than the per-neighbor `neighbor next-hop-self` command, since you can set the next hop for some routes, but not others. The `neighbor next-hop-self` sets the next hop for all routes sent to that neighbor.
The set clauses can be used in conjunction with one another. They are evaluated in the following order:

```
set ip next-hop
set interface
set ip default next-hop
set default interface
```

Examples

In the following example, packets with a Level 3 length of 3 to 50 bytes are output to the router at IP address 161.14.2.2:

```
interface serial 0
  ip policy route-map thataway
!
route-map thataway
  match length 3 50
  set ip next-hop 161.14.2.2
```

In the following example, three routers are on the same FDDI LAN (with IP addresses 1.1.1.1, 1.1.1.2, and 1.1.1.3). Each is in a different autonomous system. The `set ip next-hop peer-address` command specifies that traffic from the router (1.1.1.3) in remote AS 300 for the router (1.1.1.1) in remote AS 100 that matches the route map is passed through the router bgp 200, rather than sent directly to the router (1.1.1.1) in AS 100 over their mutual connection to the LAN:

```
router bgp 200
neighbor 1.1.1.3 remote-as 100
neighbor 1.1.1.3 route-map set-peer-address out
neighbor 1.1.1.1 remote-as 100
route-map set-peer-address permit 10
set ip next-hop peer-address
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
ip policy route-map
match ip address
match length
neighbor next-hop-self
route-map
set default interface
set interface
set ip default next-hop
```
**set metric-type internal**

To set the MED value on prefixes advertised to EBGP neighbors to match the IGP metric of the next hop, use the `set metric internal` route-map configuration command. To return to the default, use the `no` form of this command.

```
set metric-type internal
no set metric-type internal
```

**Syntax Description**

This command has no arguments or keywords.

**Default**

Disabled

**Command Mode**

Route-map configuration

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.3.

This command will cause BGP to advertise a MED that corresponds to the IGP metric associated with the NEXT HOP of the route. This command applies to generated, iBGP-, and eBGP-derived routes.

If this command is used, multiple BGP speakers in a common AS can advertise different MEDs for a particular prefix. Also, note that if the IGP metric changes, BGP will not readvertise the route.

You must have a match clause (even if it points to a “permit everything” list) if you want to set tags.

Use the `route-map` global configuration command, and the `match` and `set` route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each `route-map` command has a list of `match` and `set` commands associated with it. The `match` commands specify the `match criteria`—the conditions under which redistribution is allowed for the current `route-map command`. The `set` commands specify the `set actions`—the particular redistribution actions to perform if the criteria enforced by the `match` commands are met. The `no` `route-map` command deletes the route map.

The `set` route-map configuration commands specify the redistribution `set actions` to be performed when all of a route map’s match criteria are met. When all match criteria are met, all set actions are performed.
Example

In the following example, the MED for all the advertised routes to neighbor 160.89.2.3 is set to the corresponding IGP metric of the next hop:

```plaintext
    router bgp 109
    network 160.89.0.0
    neighbor 160.89.2.3 remote-as 200
    neighbor 160.89.2.3 route-map setMED out

    route-map setMED permit 10
    match as-path 1
    set metric-type internal

    ip as-path access-list 1 permit .*
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

`route-map`
set origin

To set the BGP origin code, use the set origin route-map configuration command. To delete an entry, use the no form of this command.

    set origin {igp | egp autonomous-system | incomplete}

Syntax Description

igp               Remote IGP.

egp               Local EGP.

autonomous-system  Remote autonomous system. This is an integer from 0 to 65535.

incomplete        Unknown heritage.

Default

Default origin, based on route in main IP routing table.

Command Mode

Route-map configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

You must have a match clause (even if it points to a “permit everything” list) if you want to set tags.

Use the route-map global configuration command with match and set route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each route-map command has a list of match and set commands associated with it. The match commands specify the match criteria—the conditions under which redistribution is allowed for the current route-map command. The set commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the match commands are met. The no route-map command deletes the route map.

The set route-map configuration commands specify the redistribution set actions to be performed when all of a route map’s match criteria are met. When all match criteria are met, all set actions are performed.

Example

The following example sets the origin of routes that pass the route map to IGP:

    route-map set_origin
    match as-path 10
    set origin igp
**set origin**

**Related Commands**

You can use the master indexes or search online to find documentation of related commands.

- match as-path
- match community-list
- match interface
- match ip address
- match ip next-hop
- match ip route-source
- match metric
- match route-type
- match tag
- route-map
- set as-path
- set automatic tag
- set community
- set level
- set local-preference
- set metric
- set metric-type
- set next-hop
- set tag
- set weight
set weight

To specify the BGP weight for the routing table, use the `set weight` route-map configuration command. To delete an entry, use the `no` form of this command.

```
set weight weight
no set weight weight
```

Syntax Description

`weight` Weight value. It can be an integer from 0 to 65535.

Default

The weight is not changed by the specified route map.

Command Mode

Route-map configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

You must have a match clause (even if it points to a “permit everything” list) if you want to set tags.

The implemented weight is based on the first matched autonomous system path. Weights indicated when an autonomous system path is matched override the weights assigned by global `neighbor` commands. In other words, the weights assigned with the `match as-path` and `set weight` route-map commands override the weights assigned using the `neighbor weight` and `neighbor filter-list` commands.

Example

The following example sets the BGP weight for the routes matching the autonomous system path access list to 200:

```
route-map set-weight
match as-path 10
set weight 200
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

`match as-path`
`match community-list`
`match interface`
`match ip address`
`match ip next-hop`
`match ip route-source`
`match metric`
`match route-type`
`match tag`
`route-map`
set weight

set as-path
set automatic-tag
set community
set level
set local-preference
set metric
set metric-type
set next-hop
set origin
set tag
show ip bgp

To display entries in the BGP routing table, use the **show ip bgp** EXEC command.

```
show ip bgp [network] [network-mask] [longer-prefixes]
```

**Syntax Description**

- **network** (Optional) Network number, entered to display a particular network in the BGP routing table.
- **network-mask** (Optional) Displays all BGP routes matching the address/mask pair.
- **longer-prefixes** (Optional) Displays route and more specific routes.

**Command Mode**

EXEC

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0. The display of prefix advertisement statistics was added in release 12.0.

**Sample Displays**

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

```
Router# show ip bgp

BGP table version is 716977, local router ID is 193.0.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* i3.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>1239</td>
</tr>
<tr>
<td>*&gt;i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>1239</td>
</tr>
<tr>
<td>* i6.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>690 568</td>
</tr>
<tr>
<td>*&gt;i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>690 568</td>
</tr>
<tr>
<td>* i7.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>701 35</td>
</tr>
<tr>
<td>*&gt;i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>701 35</td>
</tr>
<tr>
<td>*</td>
<td>198.92.72.24</td>
<td>0</td>
<td></td>
<td>1878 704 701 35</td>
<td></td>
</tr>
<tr>
<td>* i8.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>690 560</td>
</tr>
<tr>
<td>*&gt;i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>690 560</td>
</tr>
<tr>
<td>*</td>
<td>198.92.72.24</td>
<td>0</td>
<td></td>
<td>1878 704 701 560</td>
<td></td>
</tr>
<tr>
<td>* i13.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>690 200</td>
</tr>
<tr>
<td>*&gt;i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>690 200</td>
</tr>
<tr>
<td>*</td>
<td>198.92.72.24</td>
<td>0</td>
<td></td>
<td>1878 704 701 200</td>
<td></td>
</tr>
<tr>
<td>* i15.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>174</td>
</tr>
<tr>
<td>*&gt;i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>174</td>
</tr>
<tr>
<td>* i16.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>701</td>
</tr>
<tr>
<td>*&gt;i</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0 1800</td>
<td>701</td>
</tr>
<tr>
<td>*</td>
<td>198.92.72.24</td>
<td>0</td>
<td></td>
<td>1878 704 701</td>
<td></td>
</tr>
</tbody>
</table>
```

Table 45 describes significant fields shown in the display.
### Table 45  Show IP BGP Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router.</td>
</tr>
<tr>
<td>Status codes</td>
<td>Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>s—The table entry is suppressed.</td>
</tr>
<tr>
<td></td>
<td>*—The table entry is valid.</td>
</tr>
<tr>
<td></td>
<td>&gt;—The table entry is the best entry to use for that network.</td>
</tr>
<tr>
<td></td>
<td>i—The table entry was learned via an internal BGP session.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>i—Entry originated from IGP and was advertised with a network router configuration command.</td>
</tr>
<tr>
<td></td>
<td>e—Entry originated from EGP.</td>
</tr>
<tr>
<td></td>
<td>?—Origin of the path is not clear Usually, this is a router that is redistributed into BGP from an IGP.</td>
</tr>
<tr>
<td>Network</td>
<td>IP address of a network entity.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, this is the value of the interautonomous system metric. This field is frequently not used.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value as set with the set local-preference route-map configuration command. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show ip bgp` command when you specify `longer-prefixes`:

```
Router# show ip bgp 198.92.0.0 255.255.0.0 longer-prefixes
```

BGP table version is 1738, local router ID is 198.92.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 198.92.0.0</td>
<td>198.92.72.30</td>
<td>8896</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>198.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 198.92.1.0</td>
<td>198.92.72.30</td>
<td>8796</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>198.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 198.92.11.0</td>
<td>198.92.72.30</td>
<td>42482</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>198.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 198.92.14.0</td>
<td>198.92.72.30</td>
<td>8796</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>198.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 198.92.15.0</td>
<td>198.92.72.30</td>
<td>8696</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>198.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 198.92.16.0</td>
<td>198.92.72.30</td>
<td>1400</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>198.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 198.92.17.0</td>
<td>198.92.72.30</td>
<td>1400</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>198.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 198.92.18.0</td>
<td>198.92.72.30</td>
<td>8876</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>198.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 198.92.19.0</td>
<td>198.92.72.30</td>
<td>8876</td>
<td>32768</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>198.92.72.30</td>
<td>0</td>
<td>109</td>
<td>108</td>
<td>?</td>
</tr>
</tbody>
</table>

The following is sample output from the `show ip bgp command`, showing information for prefix 3.0.0.0:

```
show ip bgp 3.0.0.0
```

BGP routing table entry for 3.0.0.0/8, version 628
Paths: (1 available, best #1)
Advertised to peer-groups:
  ebgp
Advertised to non peer-group peers:
  171.69.232.162
  109.65000 297 701 80
  171.69.233.56 from 171.69.233.56 (172.19.185.32)
 -Origin incomplete, localpref 100, valid, external, best, ref 2

**Note** If a prefix has not been advertised to any peer, the display shows “Not advertised to any peer.”
**show ip bgp cidr-only**

To display routes with nonnatural network masks (that is, classless interdomain routing, or CIDR), use the `show ip bgp cidr-only` privileged EXEC command.

```
show ip bgp cidr-only
```

**Syntax Description**

This command has no arguments or keywords.

**Command Mode**

Privileged EXEC

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0.

**Sample Display**

The following is sample output from the `show ip bgp cidr-only` command:

```
Router# show ip bgp cidr-only
BGP table version is 220, local router ID is 198.92.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop          Metric LocPrf Weight Path
*> 192.0.0.0/8      198.92.72.24     0 1878 0
*> 198.92.0.0/16    198.92.72.30     0 108 0
```

Table 46 describes significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version is 220</td>
<td>Internal version number for the table. This number is incremented any time the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>An Internet address of the router.</td>
</tr>
<tr>
<td>Status codes</td>
<td>s—The table entry is suppressed.</td>
</tr>
<tr>
<td></td>
<td>*—The table entry is valid.</td>
</tr>
<tr>
<td></td>
<td>&gt;—The table entry is the best entry to use for that network.</td>
</tr>
<tr>
<td></td>
<td>i—The table entry was learned via an internal BGP session.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>i—Entry originated from IGP and was advertised with a network router configuration command.</td>
</tr>
<tr>
<td></td>
<td>e—Entry originated from EGP.</td>
</tr>
<tr>
<td></td>
<td>?—Origin of the path is not clear Usually, this is a router that is redistributed into BGP from an IGP.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network</td>
<td>Internet address of the network the entry describes.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of the next system to use when forwarding a packet to the</td>
</tr>
<tr>
<td></td>
<td>destination network. An entry of 0.0.0.0 indicates that the access server</td>
</tr>
<tr>
<td></td>
<td>has some non-BGP route to this network.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, this is the value of the interautonomous system metric. This field</td>
</tr>
<tr>
<td></td>
<td>is frequently not used.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value. Default is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Set through the use of autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry</td>
</tr>
<tr>
<td></td>
<td>in this field for each autonomous system in the path. At the end of the</td>
</tr>
<tr>
<td></td>
<td>path is the origin code for the path.</td>
</tr>
<tr>
<td></td>
<td>i—The entry was originated with the IGP and advertised with a</td>
</tr>
<tr>
<td></td>
<td>network router configuration command.</td>
</tr>
<tr>
<td></td>
<td>e—The route originated with EGP.</td>
</tr>
<tr>
<td></td>
<td>?—The origin of the path is not clear. Usually this is a path that is</td>
</tr>
<tr>
<td></td>
<td>redistributed into BGP from an IGP.</td>
</tr>
</tbody>
</table>
show ip bgp community

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

show ip bgp community community-number [exact]

Syntax Description

community-number
Valid value is community number in the range 1 to 4294967200, internet, no-export, local-as, or no-advertise.

You must enter the numerical communities before the well-known communities. For example, the following does not work:

router#show ip bgp community local-as 111:12345

Use the following instead:

router#show ip bgp community 111:12345 local-as

exact
(Optional) Displays only routes that have exactly the same specified communities.

Command Mode
EXEC

Usage Guidelines
This command first appeared in Cisco IOS Release 10.3. The local-as community was added in Cisco IOS Release 12.0.

Sample Display
The following is sample output from the show ip bgp community command:

router#show ip bgp community 111:12345 local-as
BGP table version is 10, local router ID is 224.0.0.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; 2.2.2.2/32</td>
<td>158.43.222.2</td>
<td>0</td>
<td>0</td>
<td>222</td>
<td>?</td>
</tr>
<tr>
<td>&gt; 111.0.0.0</td>
<td>158.43.222.2</td>
<td>0</td>
<td>0</td>
<td>222</td>
<td>?</td>
</tr>
<tr>
<td>&gt; 158.43.0.0</td>
<td>158.43.222.2</td>
<td>0</td>
<td>0</td>
<td>222</td>
<td>?</td>
</tr>
<tr>
<td>&gt; 158.43.44/32</td>
<td>158.43.222.2</td>
<td>0</td>
<td>0</td>
<td>222</td>
<td>?</td>
</tr>
<tr>
<td>&gt; 158.43.222.0/24</td>
<td>158.43.222.2</td>
<td>0</td>
<td>0</td>
<td>222</td>
<td>i</td>
</tr>
<tr>
<td>&gt; 172.17.240.0/21</td>
<td>158.43.222.2</td>
<td>0</td>
<td>0</td>
<td>222</td>
<td>?</td>
</tr>
<tr>
<td>&gt; 192.168.212.0</td>
<td>158.43.222.2</td>
<td>0</td>
<td>0</td>
<td>222</td>
<td>i</td>
</tr>
<tr>
<td>&gt; 203.9.1.0</td>
<td>158.43.222.2</td>
<td>0</td>
<td>0</td>
<td>222</td>
<td>?</td>
</tr>
</tbody>
</table>

Table 47 describes significant fields shown in the display.
## Table 47  Show IP BGP Community Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router.</td>
</tr>
<tr>
<td>Status codes</td>
<td>Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>s—The table entry is suppressed.</td>
</tr>
<tr>
<td></td>
<td>*—The table entry is valid.</td>
</tr>
<tr>
<td></td>
<td>&gt;—The table entry is the best entry to use for that network.</td>
</tr>
<tr>
<td></td>
<td>i—The table entry was learned via an internal BGP session.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>i—Entry originated from IGP and was advertised with a <strong>network</strong> router configuration command.</td>
</tr>
<tr>
<td></td>
<td>e—Entry originated from EGP.</td>
</tr>
<tr>
<td></td>
<td>?—Origin of the path is not clear Usually, this is a router that is redistributed into BGP from an IGP.</td>
</tr>
<tr>
<td>Network</td>
<td>IP address of a network entity.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, this is the value of the interautonomous system metric. This field is frequently not used.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value as set with the <strong>set local-preference</strong> route-map configuration command. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.</td>
</tr>
</tbody>
</table>
show ip bgp community-list

show ip bgp community-list

To display routes that are permitted by the BGP community list, use the show ip bgp community-list EXEC command.

show ip bgp community-list  community-list-number [exact]

Syntax Description

community-list-number Community list number in the range 1 to 99.

exact (Optional) Displays only routes that have an exact match.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

Sample Display

The following is sample output of the show ip bgp community-list command:

Router# show ip bgp community-list 20

BGP table version is 716977, local router ID is 193.0.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* i3.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 1239 ?</td>
</tr>
<tr>
<td>* i13.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 690 200 ?</td>
</tr>
<tr>
<td>* i15.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 174 ?</td>
</tr>
<tr>
<td>* i16.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 701 i</td>
</tr>
<tr>
<td>* i18.0.0.0</td>
<td>193.0.22.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 690 560 ?</td>
</tr>
<tr>
<td>i13.0.0.0</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 690 200 ?</td>
</tr>
<tr>
<td>i15.0.0.0</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 174 ?</td>
</tr>
<tr>
<td>i16.0.0.0</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 701 i</td>
</tr>
<tr>
<td>i18.0.0.0</td>
<td>193.0.16.1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1800 690 560 ?</td>
</tr>
</tbody>
</table>

Table 48 describes significant fields shown in the display.
### Table 48  Show IP BGP Community List Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router.</td>
</tr>
</tbody>
</table>
| Status codes     | Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:  
|                  | s—The table entry is suppressed.                                                                       |
|                  | *—The table entry is valid.                                                                            |
|                  | >—The table entry is the best entry to use for that network.                                           |
|                  | i—The table entry was learned via an internal BGP session.                                             |
| Origin codes     | Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:  
|                  | i—Entry originated from IGP and was advertised with a network router configuration command.            |
|                  | e—Entry originated from EGP.                                                                           |
|                  | ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.|
| Network          | IP address of a network entity.                                                                        |
| Next Hop         | 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. |
| Metric           | If shown, this is the value of the interautonomous system metric. This field is frequently not used.    |
| LocPrf           | Local preference value as set with the set local-preference route-map configuration command. The default value is 100. |
| Weight           | Weight of the route as set via autonomous system filters.                                              |
| Path             | Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. |
**show ip bgp dampened-paths**

To display BGP dampened routes, use the `show ip bgp dampened-paths` EXEC command.

```
show ip bgp dampened-paths
```

**Syntax Description**

This command has no arguments or keywords.

**Command Mode**

EXEC

**Usage Guidelines**

This command first appeared in Cisco IOS Release 11.0.

**Sample Display**

The following is sample output from the `show ip bgp dampened-paths` command:

```
Router# show ip bgp dampened-paths
BGP table version is 10, local router ID is 171.69.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          From             Reuse   Path
*d 10.0.0.0         171.69.232.177   00:18:4 100 ?
d 12.0.0.0         171.69.232.177   00:28:5 100 ?
```

Table 49 describes the fields in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number for the table. This number is incremented any time the table changes.</td>
</tr>
<tr>
<td>local router</td>
<td>IP address of the router where route dampening is enabled.</td>
</tr>
<tr>
<td>*d Network</td>
<td>Route to the network indicated is dampened.</td>
</tr>
<tr>
<td>From</td>
<td>IP address of the peer that advertised this path.</td>
</tr>
<tr>
<td>Reuse</td>
<td>Time (in hours:minutes:seconds) after which the path will be made available.</td>
</tr>
<tr>
<td>Path</td>
<td>AS-path of the route that is being dampened.</td>
</tr>
</tbody>
</table>

**Related Commands**

You can use the master indexes or search online to find documentation of related commands.

- `bgp dampening`
- `clear ip bgp dampening`
**show ip bgp filter-list**

To display routes that conform to a specified filter list, use the *show ip bgp filter-list* privileged EXEC command.

```
show ip bgp filter-list access-list-number
```

**Syntax Description**

access-list-number  Number of an autonomous system path access list. It can be a number from 1 to 199.

**Command Mode**

Privileged EXEC

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0.

**Sample Display**

The following is sample output from the *show ip bgp filter-list* command:

```
Router# show ip bgp filter-list 2

BGP table version is 1738, local router ID is 198.92.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 198.92.0.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.1.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.11.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.14.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.15.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.16.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.17.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.18.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.19.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.24.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.29.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.30.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.33.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.35.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.36.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.37.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.38.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.39.0</td>
<td>198.92.72.30</td>
<td>0 109 108 ?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
Table 50 describes significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number for the table. This number is incremented any time the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>An Internet address of the access server.</td>
</tr>
<tr>
<td>Status codes</td>
<td>s—The table entry is suppressed. *—The table entry is valid. &gt;—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from IGP and was advertised with a network router configuration command. e—Entry originated from EGP. ?—Origin of the path is not clear Usually, this is a router that is redistributed into BGP from an IGP.</td>
</tr>
<tr>
<td>Network</td>
<td>Internet address of the network the entry describes.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of the next system to use when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, this is the value of the interautonomous system metric. This field is frequently not used.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value. Default is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Set through the use of autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path. i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.</td>
</tr>
</tbody>
</table>
show ip bgp flap-statistics

To display BGP flap statistics, use the show ip bgp flap-statistics EXEC command.

```
show ip bgp flap-statistics [{regexp regexp} | {filter-list list} | {address mask [longer-prefix]}]
```

Syntax Description

- **regexp** regexp (Optional) Clears flap statistics for all the paths that match the regular expression.
- **filter-list** list (Optional) Clears flap statistics for all the paths that pass the access list.
- **address** (Optional) Clears flap statistics for a single entry at this IP address.
- **mask** (Optional) Network mask applied to the **address**.
- **longer-prefix** (Optional) Displays flap statistics for more specific entries.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

If no arguments or keywords are specified, the router displays flap statistics for all routes.

Sample Display

The following is sample output from the `show ip bgp flap-statistics` command:

```
Router# show ip bgp flap-statistics
BGP table version is 10, local router ID is 171.69.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>From</th>
<th>Flaps</th>
<th>Duration</th>
<th>Reuse</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*d 10.0.0.0</td>
<td>171.69.232.177</td>
<td>4</td>
<td>00:13:31</td>
<td>00:18:10</td>
<td>100</td>
</tr>
<tr>
<td>*d 12.0.0.0</td>
<td>171.69.232.177</td>
<td>4</td>
<td>00:02:45</td>
<td>00:28:20</td>
<td>100</td>
</tr>
</tbody>
</table>
```

Table 51 describes the significant fields in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number for the table. This number is incremented any time the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router where route dampening is enabled.</td>
</tr>
<tr>
<td>Network</td>
<td>Route to the network indicated is dampened.</td>
</tr>
<tr>
<td>From</td>
<td>IP address of the peer that advertised this path.</td>
</tr>
<tr>
<td>Flaps</td>
<td>Number of times the route has flapped.</td>
</tr>
</tbody>
</table>
Table 51  Show IP BGP Flap-Statistics Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>Time (in hours:minutes:seconds) since the router noticed the first flap.</td>
</tr>
<tr>
<td>Reuse</td>
<td>Time (in hours:minutes:seconds) after which the path will be made available.</td>
</tr>
<tr>
<td>Path</td>
<td>AS-path of the route that is being dampened.</td>
</tr>
</tbody>
</table>

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- bgp dampening
- clear ip bgp flap-statistics
show ip bgp inconsistent-as

To display routes with inconsistent originating autonomous systems, use the show ip bgp inconsistent-as privileged EXEC command.

show ip bgp inconsistent-as

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Sample Display

The following is sample output from the show ip bgp inconsistent-as command:

```
Router# show ip bgp inconsistent-as
BGP table version is 87, local router ID is 172.19.82.53
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop          Metric LocPrf Weight Path
*  11.0.0.0         171.69.232.55          0             0 300 88 90 99 ?
*>                  171.69.232.52       2222             0 400 ?
*  171.69.0.0       171.69.232.55          0             0 300 90 99 88 200 ?
*>                  171.69.232.52       2222             0 400 ?
*  200.200.199.0    171.69.232.55          0             0 300 88 90 99 ?
*>                  171.69.232.52       2222             0 400 ?
```

show ip bgp neighbors

To display information about the TCP and BGP connections to neighbors, use the show ip bgp neighbors EXEC command.

show ip bgp neighbors [address] [received-routes | routes | advertised-routes | {paths regular-expression} | dampened-routes]
show ip bgp neighbors

Syntax Description

- **address** (Optional) Address of the neighbor whose routes you have learned from. If you omit this argument, all neighbors are displayed.
- **received-routes** (Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
- **routes** (Optional) Displays all routes that are received and accepted. This is a subset of the output from the `received-routes` keyword.
- **advertised-routes** (Optional) Displays all the routes the router has advertised to the neighbor.
- **paths regular-expression** (Optional) Regular expression that is used to match the paths received.
- **dampened-routes** (Optional) Displays the dampened routes to the neighbor at the IP address specified.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The `received-routes` keyword first appeared in Cisco IOS Release 11.2.
Sample Displays

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

```
Router# show ip bgp neighbors 171.69.232.178

BGP neighbor is 171.69.232.178, remote AS 10, external link
Index 1, Offset 0, Mask 0x2
  Inbound soft reconfiguration allowed
  BGP version 4, remote router ID 171.69.232.178
  BGP state = Established, table version = 27, up for 00:06:12
  Last read 00:00:12, hold time is 180, keepalive interval is 60 seconds
  Minimum time between advertisement runs is 30 seconds
  Received 19 messages, 0 notifications, 0 in queue
  Sent 17 messages, 0 notifications, 0 in queue
  Inbound path policy configured
  Route map for incoming advertisements is testing
  Connections established 2; dropped 1
  Connection state is ESTAB, I/O status: 1, unread input bytes: 0
  Local host: 171.69.232.181, Local port: 11002
  Foreign host: 171.69.232.178, Foreign port: 179

Enqueued packets for retransmit: 0, input: 0, saved: 0

Event Timers (current time is 0x530C294):
  Timer          Starts    Wakeups            Next
  Retrans            12          0             0x0
  TimeWait            0          0             0x0
  AckHold            12         10             0x0
  SendWnd            0          0             0x0
  KeepAlive         0          0             0x0
  GiveUp            0          0             0x0
  PmtuAger          0          0             0x0

  iss:  133981889  snduna:  133982166  sndnxt:  133982166     sndwnd:  16108
  irs: 3317025518  rcvnxt: 3317025810  rcvwnd:     16093  delrcvwnd:    291

  SRTT: 441 ms, RTTO: 2784 ms, RTV: 951 ms, KRTT: 0 ms
  minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 300 ms
  Flags: higher precedence, nagle

Datagrams (max data segment is 1460 bytes):
  Rcvd: 15 (out of order: 0), with data: 12, total data bytes: 291
  Sent: 23 (retransmit: 0), with data: 11, total data bytes: 276
```

Table 52 describes the fields shown in the display.

**Table 52** Show IP BGP Neighbors Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP neighbor</td>
<td>IP address of the BGP neighbor and its autonomous system number. If the neighbor is in the same autonomous system as the router, then the link between them is internal; otherwise, it is considered external.</td>
</tr>
<tr>
<td>BGP version</td>
<td>BGP version being used to communicate with the remote router; the neighbor’s router ID (an IP address) is also specified.</td>
</tr>
<tr>
<td>BGP state</td>
<td>Internal state of this BGP connection.</td>
</tr>
<tr>
<td>table version</td>
<td>Indicates that the neighbor has been updated with this version of the primary BGP routing table.</td>
</tr>
<tr>
<td>up for</td>
<td>Amount of time that the underlying TCP connection has been in existence.</td>
</tr>
<tr>
<td>Last read</td>
<td>Time that BGP last read a message from this neighbor.</td>
</tr>
<tr>
<td>hold time</td>
<td>Maximum amount of time that can elapse between messages from the peer.</td>
</tr>
</tbody>
</table>
**Table 52  Show IP BGP Neighbors Field Descriptions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keepalive interval</td>
<td>Time period between sending keepalive packets, which help ensure that the TCP connection is up.</td>
</tr>
<tr>
<td>Received</td>
<td>Number of total BGP messages received from this peer, including keepalives.</td>
</tr>
<tr>
<td>notifications</td>
<td>Number of error messages received from the peer.</td>
</tr>
<tr>
<td>Sent</td>
<td>Total number of BGP messages that have been sent to this peer, including keepalives.</td>
</tr>
<tr>
<td>notifications</td>
<td>Number of error messages the router has sent to this peer.</td>
</tr>
<tr>
<td>Connections established</td>
<td>Number of times the router has established a TCP connection and the two peers have agreed speak BGP with each other.</td>
</tr>
<tr>
<td>dropped</td>
<td>Number of times that a good connection has failed or been taken down.</td>
</tr>
<tr>
<td>Connection state</td>
<td>State of BGP peer.</td>
</tr>
<tr>
<td>unread input bytes</td>
<td>Number of bytes of packets still to be processed.</td>
</tr>
<tr>
<td>Local host, Local port</td>
<td>Peering address of local router, plus port.</td>
</tr>
<tr>
<td>Foreign host, Foreign port</td>
<td>Neighbor’s peering address.</td>
</tr>
<tr>
<td>Event Timers</td>
<td>Table displays the number of starts and wakeups for each timer.</td>
</tr>
<tr>
<td>iss</td>
<td>Initial send sequence number.</td>
</tr>
<tr>
<td>snduna</td>
<td>Last send sequence number the local host sent but has not received an acknowledgment for.</td>
</tr>
<tr>
<td>sndnxt</td>
<td>Sequence number the local host will send next.</td>
</tr>
<tr>
<td>sndwnd</td>
<td>TCP window size of the remote host.</td>
</tr>
<tr>
<td>irs</td>
<td>Initial receive sequence number.</td>
</tr>
<tr>
<td>rcvnxt</td>
<td>Last receive sequence number the local host has acknowledged.</td>
</tr>
<tr>
<td>rcvwnd</td>
<td>Local host’s TCP window size.</td>
</tr>
<tr>
<td>delrecvwnd</td>
<td>Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.</td>
</tr>
<tr>
<td>SRTT</td>
<td>A calculated smoothed round-trip timeout.</td>
</tr>
<tr>
<td>RTTO</td>
<td>Round-trip timeout.</td>
</tr>
<tr>
<td>RTV</td>
<td>Variance of the round-trip time.</td>
</tr>
<tr>
<td>KRTT</td>
<td>New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been retransmitted.</td>
</tr>
<tr>
<td>minRTT</td>
<td>Smallest recorded round-trip timeout (hard wire value used for calculation).</td>
</tr>
<tr>
<td>maxRTT</td>
<td>Largest recorded round-trip timeout.</td>
</tr>
<tr>
<td>ACK hold</td>
<td>Time the local host will delay an acknowledgment in order to piggyback data on it.</td>
</tr>
<tr>
<td>Flags</td>
<td>IP precedence of the BGP packets.</td>
</tr>
<tr>
<td>Datagrams: Rcvd</td>
<td>Number of update packets received from neighbor.</td>
</tr>
<tr>
<td>with data</td>
<td>Number of update packets received with data.</td>
</tr>
<tr>
<td>total data bytes</td>
<td>Total bytes of data.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show ip bgp neighbors` command with advertised-routes:

```
Router# show ip bgp neighbors 171.69.232.178 advertised-routes

BGP table version is 27, local router ID is 171.69.232.181
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
*> 110.0.0.0        171.69.232.179         0    100      0 ?
*> 200.2.2.0        0.0.0.0                0         32768 i
```

The following is sample output from the `show ip bgp neighbors` command with routes:

```
Router# show ip bgp neighbors 171.69.232.178 routes

BGP table version is 27, local router ID is 171.69.232.181
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
*> 10.0.0.0         171.69.232.178        40             0 10 ?
*> 20.0.0.0         171.69.232.178        40             0 10 ?
```

Table 52 shows the fields shown in the display.

### Table 52  Show IP BGP Neighbors Field Descriptions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sent</td>
<td>Number of update packets sent.</td>
</tr>
<tr>
<td>with data</td>
<td>Number of update packets with data sent.</td>
</tr>
<tr>
<td>total data bytes</td>
<td>Total number of data bytes.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show ip bgp neighbors` command with advertised-routes:

```
Router# show ip bgp neighbors 171.69.232.178 advertised-routes

BGP table version is 27, local router ID is 171.69.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 110.0.0.0</td>
<td>171.69.232.179</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 200.2.2.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>i</td>
<td></td>
</tr>
</tbody>
</table>
```

The following is sample output from the `show ip bgp neighbors` command with routes:

```
Router# show ip bgp neighbors 171.69.232.178 routes

BGP table version is 27, local router ID is 171.69.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 10.0.0.0</td>
<td>171.69.232.178</td>
<td>40</td>
<td>0</td>
<td>10</td>
<td>?</td>
</tr>
<tr>
<td>*&gt; 20.0.0.0</td>
<td>171.69.232.178</td>
<td>40</td>
<td>0</td>
<td>10</td>
<td>?</td>
</tr>
</tbody>
</table>
```

Table 53 describes the fields shown in the display.

### Table 53  Show IP BGP Neighbors Advertised-Routes and Routes Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router.</td>
</tr>
<tr>
<td>Status codes</td>
<td>s—The table entry is suppressed. *—The table entry is valid. &gt;—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP session.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from IGP and was advertised with a network router configuration command. e—Entry originated from EGP. ?—Origin of the path is not clear Usually, this is a router that is redistributed into BGP from an IGP.</td>
</tr>
<tr>
<td>Network</td>
<td>IP address of a network entity.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show ip bgp neighbors` command with `paths`:

```
Router# show ip bgp neighbors 171.69.232.178 paths *10

Address    Refcount Metric Path
0x60E577B0      2     40 10 ?
```

**Table 53**  
**Show IP BGP Neighbors Advertised-Routes and Routes Field Descriptions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Hop</td>
<td>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.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, this is the value of the interautonomous system metric. This field is frequently not used.</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value as set with the <code>set local-preference</code> route-map configuration command. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.</td>
</tr>
</tbody>
</table>
**show ip bgp paths**

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

```
show ip bgp paths
```

**Syntax Description**

This command has no arguments or keywords.

**Command Mode**

EXEC

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0.

**Sample Display**

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

```
Router# show ip bgp paths
Address    Hash Refcount Metric Path
0x60E5742C    0        1      0 i
0x60E3D7AC    2        1      0 ?
0x60E5C6C0   11        3      0 10 ?
0x60E577B0   35        2     40 10 ?
```

Table 54 describes significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Internal address where the path is stored.</td>
</tr>
<tr>
<td>Hash</td>
<td>Hash bucket where path is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Number of routes using that path.</td>
</tr>
<tr>
<td>Metric</td>
<td>The multiple exit discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)</td>
</tr>
<tr>
<td>Path</td>
<td>The AS_PATH for that route, followed by the origin code for that route.</td>
</tr>
</tbody>
</table>
show ip bgp peer-group

show ip bgp peer-group
To display information about BGP peer groups, use the show ip bgp peer-group EXEC command.

\[show ip bgp peer-group \[tag\] \[summary\]\]

Syntax Description

tag (Optional) Displays information about that specific peer group.

summary (Optional) Displays a summary of the status of all the members of a peer group.

Command Mode
EXEC

Usage Guidelines
This command first appeared in Cisco IOS Release 11.0.

Sample Display
The following is sample output from the show ip bgp peer-group command:

Router# show ip bgp peer-group0 internal
BGP neighbor is internal, peer-group leader
  BGP version 4
  Minimum time between advertisement runs is 5 seconds
  Incoming update AS path filter list is 2
  Outgoing update AS path filter list is 1
  Route map for outgoing advertisements is set-med
**show ip bgp regexp**

To display routes matching the regular expression, use the `show ip bgp regexp` privileged EXEC command.

```
show ip bgp regexp regular-expression
```

**Syntax Description**

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

**Command Mode**

Privileged EXEC

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0.

**Sample Display**

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

```
Router# show ip bgp regexp 108$
```

BGP table version is 1738, local router ID is 198.92.72.24  
Status codes: s suppressed, v valid, b best, i - internal  
Origin codes: i - IGP, e - EGP, - incomplete  

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 198.92.0.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.1.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.11.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.14.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.15.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.16.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.17.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.18.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.19.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.24.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.29.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.30.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.33.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.35.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.36.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.37.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.38.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>* 198.92.39.0</td>
<td>198.92.72.30</td>
<td>0 109 108</td>
<td>?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Show ip bgp summary**

To display the status of all BGP connections, use the `show ip bgp summary` EXEC command.

**Syntax Description**

This command has no arguments or keywords.

**Command Mode**

EXEC

**Usage Guidelines**

This command first appeared in Cisco IOS Release 10.0. The PfxRcd and Admin entries first appeared in Cisco IOS Release 12.0.

**Sample Display**

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

```
Router# show ip bgp summary

BGP table version is 717029, main routing table version 717029
19073 network entries (37544 paths) using 3542756 bytes of memory
691 BGP path attribute entries using 57200 bytes of memory

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>V</th>
<th>AS</th>
<th>MsgRcvd</th>
<th>MsgSent</th>
<th>TblVer</th>
<th>InQ</th>
<th>OutQ</th>
<th>Up/Down</th>
<th>State/PfxRcd</th>
</tr>
</thead>
<tbody>
<tr>
<td>193.0.16.1</td>
<td>4</td>
<td>1755</td>
<td>32642</td>
<td>2973</td>
<td>717029</td>
<td>0</td>
<td>0</td>
<td>1:27:11</td>
<td></td>
</tr>
<tr>
<td>193.0.17.1</td>
<td>4</td>
<td>1755</td>
<td>4790</td>
<td>2973</td>
<td>717029</td>
<td>0</td>
<td>0</td>
<td>1:27:51</td>
<td></td>
</tr>
<tr>
<td>193.0.18.1</td>
<td>4</td>
<td>1755</td>
<td>7722</td>
<td>3024</td>
<td>717029</td>
<td>0</td>
<td>0</td>
<td>1:28:13</td>
<td></td>
</tr>
<tr>
<td>193.0.19.1</td>
<td>4</td>
<td>1755</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2d02</td>
<td>Active</td>
</tr>
<tr>
<td>193.0.20.1</td>
<td>4</td>
<td>1755</td>
<td>3673</td>
<td>3049</td>
<td>717029</td>
<td>0</td>
<td>0</td>
<td>2:50:10</td>
<td>Idle (PfxRcd)</td>
</tr>
<tr>
<td>193.0.21.1</td>
<td>4</td>
<td>1755</td>
<td>3741</td>
<td>3048</td>
<td>717029</td>
<td>0</td>
<td>0</td>
<td>12:24:43</td>
<td></td>
</tr>
<tr>
<td>193.0.22.1</td>
<td>4</td>
<td>1755</td>
<td>33129</td>
<td>3051</td>
<td>717029</td>
<td>0</td>
<td>0</td>
<td>12:24:48</td>
<td></td>
</tr>
<tr>
<td>193.0.23.1</td>
<td>4</td>
<td>1755</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2d02</td>
<td>Active</td>
</tr>
<tr>
<td>193.0.24.1</td>
<td>4</td>
<td>1755</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2d02</td>
<td>Active</td>
</tr>
<tr>
<td>193.0.25.1</td>
<td>4</td>
<td>1755</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2d02</td>
<td>Active</td>
</tr>
<tr>
<td>193.0.26.1</td>
<td>4</td>
<td>1755</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2d02</td>
<td>Active</td>
</tr>
<tr>
<td>193.0.27.1</td>
<td>4</td>
<td>1755</td>
<td>4269</td>
<td>3049</td>
<td>717029</td>
<td>0</td>
<td>0</td>
<td>12:39:33</td>
<td></td>
</tr>
<tr>
<td>193.0.28.1</td>
<td>4</td>
<td>1755</td>
<td>3037</td>
<td>3050</td>
<td>717028</td>
<td>0</td>
<td>0</td>
<td>2:08:15</td>
<td></td>
</tr>
<tr>
<td>198.92.72.24</td>
<td>4</td>
<td>1878</td>
<td>11635</td>
<td>13300</td>
<td>717028</td>
<td>0</td>
<td>0</td>
<td>0:50:39</td>
<td></td>
</tr>
<tr>
<td>198.92.72.36</td>
<td>4</td>
<td>1001</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>never</td>
<td>Idle (Admin)</td>
</tr>
</tbody>
</table>
```
Table 55 describes significant fields shown in the display.

### Table 55  Show IP BGP Summary Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of BGP database.</td>
</tr>
<tr>
<td>main routing table version</td>
<td>Last version of BGP database that was injected into main routing table.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>IP address of a neighbor.</td>
</tr>
<tr>
<td>V</td>
<td>BGP version number spoken to that neighbor.</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous system.</td>
</tr>
<tr>
<td>MsgRcvd</td>
<td>BGP messages received from that neighbor.</td>
</tr>
<tr>
<td>MsgSent</td>
<td>BGP messages sent to that neighbor.</td>
</tr>
<tr>
<td>TblVer</td>
<td>Last version of the BGP database that was sent to that neighbor.</td>
</tr>
<tr>
<td>InQ</td>
<td>Number of messages from that neighbor waiting to be processed.</td>
</tr>
<tr>
<td>OutQ</td>
<td>Number of messages waiting to be sent to that neighbor.</td>
</tr>
<tr>
<td>Up/Down</td>
<td>The length of time that the BGP session has been in state Established, or the current state if it is not Established.</td>
</tr>
<tr>
<td>State/PfxRcd</td>
<td>Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum prefix command) is reached, the string “PfxRcd” appears in the entry, the neighbor is shut down, and the connection is Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.</td>
</tr>
</tbody>
</table>

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- `neighbor maximum-prefix`
- `neighbor shutdown`
- `show ip bgp summary`
synchronization

To enable the synchronization between BGP and your IGP, use the `synchronization` router configuration command. To enable the Cisco IOS software to advertise a network route without waiting for the IGP, use the `no` form of this command.

```
synchronization
no synchronization
```

Syntax Description
This command has no arguments or keywords.

Default
Enabled

Command Mode
Router configuration

Usage Guidelines
This command first appeared in Cisco IOS Release 10.0.

Usually, a BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. The `no synchronization` command allows the Cisco IOS software to advertise a network route without waiting for 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.

Use `synchronization` if there are routers in the autonomous system that do not speak BGP.

Example
The following example enables a router to advertise a network route without waiting for the IGP:

```
router bgp 120
no synchronization
```
table-map

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

```
table-map route-map-name
no table-map route-map-name
```

Syntax Description

- `route-map-name` Route-map name, from the `route-map` command.

Default

Disabled

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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.

You can use `match` clauses of route maps in the `table-map` command. IP access list, autonomous system paths, and next-hop match clauses are supported.

Example

In the following example, the Cisco IOS software is configured to automatically compute the tag value for the BGP learned routes and to update the IP routing table.

```
route-map tag
match as path 10
  set automatic-tag
!
router bgp 100
  table-map tag
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- `match as-path`
- `match ip address`
- `match ip next-hop`
- `route-map`
timers bgp

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

    timers bgp keepalive holdtime
    no timers bgp

Syntax Description

- **keepalive**: Frequency, in seconds, with which the Cisco IOS software sends keepalive messages to its peer. The default is 60 seconds.

- **holdtime**: Interval, in seconds, after not receiving a keepalive message that the software declares a peer dead. The default is 180 seconds.

Defaults

- **keepalive**: 60 seconds
- **holdtime**: 180 seconds

Command Mode

Router configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Example

The following example changes the keepalive timer to 70 seconds and the holdtime timer to 210 seconds:

    timers bgp 70 210

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- clear ip bgp peer-group
- router bgp
- show ip bgp