BGP Commands: show ip through Z

show ip as-path-access-list

To display the contents of all current autonomous system (AS) path access lists, use the **show ip as-path-access-list** command in user EXEC or privileged EXEC mode.

show ip as-path-access-list [*number*]

Syntax Description

number	(Optional) Specifies the AS path access list number. The range is from 1 to 500.

Command Default

If the *number* argument is not specified, command output is displayed for all AS path access lists.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show ip as-path-access-list** command:

```
Router# show ip as-path-access-list

AS path access list 34
    deny RTR$
AS path access list 100
    permit 100$
```

The table below describes the fields shown in the display.

Table 1: show ip as-path-access-list Field Descriptions

Field	Description
AS path access list	Indicates the AS path access list number.

Field	Description
deny	Indicates the number of packets that are rejected since the regular expression failed to match the representation of the AS path of the route as an ASCII string.
permit	Indicates the number of packets that are forwarded since the regular expression matched the representation of the AS path of the route as an ASCII string.

Related Commands

Command	Description
ip as-path access-list	Configures an autonomous system path filter using a regular expression.

show ip bgp

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

show ip bgp [*ip-address* [*mask* [**longer-prefixes** [**injected**] | **shorter-prefixes** [*length*] | **bestpath** | **multipaths** | **subnets**] | **bestpath** | **multipaths**] | **all** | **oer-paths** | **prefix-list** *name* | **pending-prefixes** | **route-map** *name* | **version** {*version-number* | **recent** *offset-value*}]

Syntax Description

ip-address	(Optional) IP address entered to filter the output to display only a particular host or network in the BGP routing table.
mask	(Optional) Mask to filter or match hosts that are part of the specified network.
longer-prefixes	(Optional) Displays the specified route and all more-specific routes.
injected	(Optional) Displays more-specific prefixes injected into the BGP routing table.
shorter-prefixes	(Optional) Displays the specified route and all less-specific routes.
length	(Optional) The prefix length. The range is a number from 0 to 32.
bestpath	(Optional) Displays the best path for this prefix.
multipaths	(Optional) Displays multipaths for this prefix.
subnets	(Optional) Displays the subnet routes for the specified prefix.
all	(Optional) Displays all address family information in the BGP routing table.
oer-paths	(Optional) Displays Optimized Edge Routing (OER) controlled prefixes in the BGP routing table.
prefix-list *name*	(Optional) Filters the output based on the specified prefix list.
pending-prefixes	(Optional) Displays prefixes that are pending deletion from the BGP routing table.

route-map *name*	(Optional) Filters the output based on the specified route map.
version *version-number*	(Optional) Displays all prefixes with network versions greater than or equal to the specified version number. The range is from 1 to 4294967295.
recent *offset-value*	(Optional) Displays the offset from the current routing table version. The range is from 1 to 4294967295.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0	This command was modified. The display of prefix advertisement statistics was added.
12.0(6)T	This command was modified. The display of a message indicating support for route refresh capability was added.
12.0(14)ST	This command was modified. The **prefix-list**, **route-map**, and **shorter-prefixes** keywords were added.
12.2(2)T	This command was modified. The output was modified to display multipaths and the best path to the specified network.
12.0(21)ST	This command was modified. The output was modified to show the number of Multiprotocol Label Switching (MPLS) labels that arrive at and depart from a prefix.
12.0(22)S	This command was modified. A new status code indicating stale routes was added to support BGP graceful restart.
12.2(14)S	This command was modified. A message indicating support for BGP policy accounting was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(15)T	This command was modified. A new status code indicating stale routes was added to support BGP graceful restart.
12.3(2)T	This command was modified. The **all** keyword was added.

Release	Modification
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.3(8)T	This command was modified. The **oer-paths** keyword was added.
12.4(15)T	This command was modified. The **pending-prefixes**, **bestpath**, **multipaths**, and **subnets** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(22)T	This command was modified. The **version** *version-number* and the **recent** *offset-value* keyword and argument pairs were added.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.
12.2(33)SXI1	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format was changed to asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format was changed to asplain.
12.2(33)SRE	This command was modified. The command output was modified to show the backup path and the best external path information. Support for the best external route and backup path was added. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.2(1)S	This command was modified to display an Resource Public Key Infrastructure (RPKI) validation code per network, if one applies.
Cisco IOS XE Release 3.5S	This command was modified to display an RPKI validation code per network, if one applies.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(4)S	This command was modified. Output about discarded or unknown path attributes was added for the BGP Attribute Filter feature. Output about additional path selection was added for the BGP Additional Paths feature. Output about paths imported from a virtual routing and forwarding (VRF) table to the global table was added for the BGP Support for IP Prefix Export from a VRF table into the global table.
Cisco IOS XE Release 3.7S	This command was modified. Output about discarded or unknown path attributes was added for the BGP Attribute Filter feature. Output about additional path selection was added for the BGP Additional Paths feature. Output about paths imported from a VRF table to the global table was added for the BGP Support for IP Prefix Export from a VRF table into the global table.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

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

When changes are made to the network address, the network version number is incremented. Use the **version** keyword to view a specific network version.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538, for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2, for example—as the only configuration format, regular expression match, and output display, with no asplain support.

oer-paths Keyword

In Cisco IOS Release 12.3(8)T and later releases, BGP prefixes that are monitored and controlled by OER are displayed by entering the **show ip bgp** command with the **oer-paths** keyword.

Examples

The following sample output displays the BGP routing table:

```
Device# show ip bgp

BGP table version is 6, local router ID is 10.0.96.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f
RT-Filter, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

      Network          Next Hop            Metric LocPrf Weight  Path

N*   10.0.0.1          10.0.0.3                 0             0  3 ?

N*>                    10.0.3.5                 0             0  4 ?

Nr   10.0.0.0/8        10.0.0.3                 0             0  3 ?

Nr>                    10.0.3.5                 0             0  4 ?

Nr>  10.0.0.0/24       10.0.0.3                 0             0  3 ?

V*>  10.0.2.0/24       0.0.0.0                  0         32768  i

Vr>  10.0.3.0/24       10.0.3.5                 0             0  4 ?
```

The table below describes the significant fields shown in the display.

Table 2: show ip bgp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
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. • d—The table entry is dampened. • h—The table entry history. • *—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 (iBGP) session. • r—The table entry is a RIB-failure. • S—The table entry is stale. • m—The table entry has multipath to use for that network. • b—The table entry has a backup path to use for that network. • x—The table entry has a best external route to use for the network.
Origin codes	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: • a—Path is selected as an additional path. • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from an Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
RPKI validation codes	If shown, the RPKI validation state for the network prefix, which is downloaded from the RPKI server. The codes are shown only if the **bgp rpki server** or **neighbor announce rpki state** command is configured.

Field	Description
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, the value of the interautonomous system metric.
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.
(stale)	Indicates that the following path for the specified autonomous system is marked as “stale” during a graceful restart process.

The following sample output shows the BGP routing table with 4-byte autonomous system numbers, 65536 and 65550, shown under the Path field. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Device# show ip bgp

BGP table version is 4, local router ID is 172.16.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 65536  i
*> 10.2.2.0/24      192.168.3.2              0             0 65550  i
*> 172.16.1.0/24    0.0.0.0                  0         32768 i
```

The following sample output displays information about the 192.168.1.0 entry in the BGP routing table:

```
Device# show ip bgp 192.168.1.0

BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
  Additional-path
  Advertised to update-groups:
     3
  10 10
    192.168.3.2 from 172.16.1.2 (10.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
  10 10
    192.168.1.2 from 192.168.1.2 (10.3.3.3)
```

```
      Origin IGP, localpref 100, valid, external, best , recursive-via-connected
```

The following sample output displays information about the 10.3.3.3 255.255.255.255 entry in the BGP routing table:

```
Device# show ip bgp 10.3.3.3 255.255.255.255

BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
Multipath: eBGP
Flag: 0x860
  Advertised to update-groups:
     1
  200
    10.71.8.165 from 10.71.8.165 (192.168.0.102)
      Origin incomplete, localpref 100, valid, external, backup/repair
      Only allowed to recurse through connected route
  200
    10.71.11.165 from 10.71.11.165 (192.168.0.102)
      Origin incomplete, localpref 100, weight 100, valid, external, best
      Only allowed to recurse through connected route
  200
    10.71.10.165 from 10.71.10.165 (192.168.0.104)
      Origin incomplete, localpref 100, valid, external,
      Only allowed to recurse through connected route
```

The table below describes the significant fields shown in the display.

Table 3: show ip bgp ip-address Field Descriptions

Field	Description
BGP routing table entry for	IP address or network number of the routing table entry.
version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	The number of available paths, and the number of installed best paths. This line displays "Default-IP-Routing-Table" when the best path is installed in the IP routing table.
Multipath	This field is displayed when multipath load sharing is enabled. This field will indicate if the multipaths are iBGP or eBGP.
Advertised to update-groups	The number of each update group for which advertisements are processed.
Origin	Origin of the entry. The origin can be IGP, EGP, or incomplete. This line displays the configured metric (0 if no metric is configured), the local preference value (100 is default), and the status and type of route (internal, external, multipath, best).

Field	Description
Extended Community	This field is displayed if the route carries an extended community attribute. The attribute code is displayed on this line. Information about the extended community is displayed on a subsequent line.

The following is sample output from the **show ip bgp** command entered with the **all** keyword. Information about all configured address families is displayed.

```
Device# show ip bgp all

For address family: IPv4 Unicast   *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 ?
*> 10.13.13.0/24    0.0.0.0                  0         32768 ?
*> 10.15.15.0/24    0.0.0.0                  0         32768 ?
*>i10.18.18.0/24    172.16.14.105         1388  91351      0 100 e
*>i10.100.0.0/16    172.16.14.107          262    272      0 1 2 3 i
*>i10.100.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.101.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.103.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.104.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.100.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*>i10.101.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*  10.100.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*  10.101.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*> 10.102.0.0/16    172.16.14.108         1388             0 100 e
*> 172.16.14.0/24   0.0.0.0                  0         32768 ?
*> 192.168.5.0      0.0.0.0                  0         32768 ?
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
For address family: VPNv4 Unicast   *****
BGP table version is 21, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vpn1)
*> 10.1.1.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.2.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.3.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.4.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.5.0/24      192.168.4.3           1622             0 100 53285 33299 51178
{27016,57039,16690} e
*>i172.17.1.0/24    10.3.3.3                10     30      0 53285 33299 51178 47751 ?
*>i172.17.2.0/24    10.3.3.3                10     30      0 53285 33299 51178 47751 ?
*>i172.17.3.0/24    10.3.3.3                10     30      0 53285 33299 51178 47751 ?
*>i172.17.4.0/24    10.3.3.3                10     30      0 53285 33299 51178 47751 ?
*>i172.17.5.0/24    10.3.3.3                10     30      0 53285 33299 51178 47751 ?
For address family: IPv4 Multicast   *****
BGP table version is 11, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
```

```
*> 10.40.40.0/26    172.16.14.110        2219             0 21 22 {51178,47751,27016} e
*                   10.1.1.1             1622             0 15 20 1 {2} e
*> 10.40.40.64/26   172.16.14.110        2219             0 21 22 {51178,47751,27016} e
*                   10.1.1.1             1622             0 15 20 1 {2} e
*> 10.40.40.128/26  172.16.14.110        2219             0 21 22 {51178,47751,27016} e
*                   10.1.1.1             2563             0 15 20 1 {2} e
*> 10.40.40.192/26  10.1.1.1             2563             0 15 20 1 {2} e
*> 10.40.41.0/26    10.1.1.1             1209             0 15 20 1 {2} e
*>i10.102.0.0/16    10.1.1.1              300    500       0 5  4 {101,102} e
*>i10.103.0.0/16    10.1.1.1              300    500       0 5  4 {101,102} e
For address family: NSAP Unicast *****
BGP table version is 1, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network                    Next Hop                Metric LocPrf Weight Path
* i45.0000.0002.0001.000c.00     49.0001.0000.0000.0a00                100      0 ?
* i46.0001.0000.0000.0000.0a00   49.0001.0000.0000.0a00                100      0 ?
* i47.0001.0000.0000.000b.00     49.0001.0000.0000.0a00                100      0 ?
* i47.0001.0000.0000.000e.00     49.0001.0000.0000.0a00
```

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

```
Device# show ip bgp 10.92.0.0 255.255.0.0 longer-prefixes

BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*> 10.92.0.0         10.92.72.30         8896         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.1.0         10.92.72.30         8796         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.11.0        10.92.72.30        42482         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.14.0        10.92.72.30         8796         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.15.0        10.92.72.30         8696         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.16.0        10.92.72.30         1400         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.17.0        10.92.72.30         1400         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.18.0        10.92.72.30         8876         32768 ?
*                    10.92.72.30                          0 109 108 ?
*> 10.92.19.0        10.92.72.30         8876         32768 ?
*                    10.92.72.30                          0 109 108 ?
```

The following is sample output from the **show ip bgp shorter-prefixes** command. An 8-bit prefix length is specified.

```
Device# show ip bgp 172.16.0.0/16 shorter-prefixes 8

*> 172.16.0.0         10.0.0.2                               0 ?
*                     10.0.0.2                 0             0 200 ?
```

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

```
Device# show ip bgp prefix-list ROUTE

BGP table version is 39, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                               0 ?
*                   10.0.0.2                 0             0 200 ?
```

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

```
Device# show ip bgp route-map LEARNED_PATH

BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                             0 ?
*                   10.0.0.2                 0           0 200 ?
```

The following output indicates (for each neighbor) whether any of the additional path tags (group-best, all, best 2 or best 3) are applied to the path. A line of output indicates rx pathid (received from neighbor) and tx pathid (announcing to neighbors). Note that the "Path advertised to update-groups:" is now per-path when the BGP Additional Paths feature is enabled.

```
Device# show ip bgp 10.0.0.1 255.255.255.224

BGP routing table entry for 10.0.0.1/28, version 82
Paths: (10 available, best #5, table default)
  Path advertised to update-groups:
     21         25
  Refresh Epoch 1
  20 50, (Received from a RR-client)
    192.0.2.1 from 192.0.2.1 (192.0.2.1)
      Origin IGP, metric 200, localpref 100, valid, internal, all
      Originator: 192.0.2.1, Cluster list: 2.2.2.2
      mpls labels in/out 16/nolabel
      rx pathid: 0, tx pathid: 0x9
  Path advertised to update-groups:
     18         21
  Refresh Epoch 1
  30
    192.0.2.2 from 192.0.2.2 (192.0.2.2)
      Origin IGP, metric 200, localpref 100, valid, internal, group-best, all
      Originator: 192.0.2.2, Cluster list: 4.4.4.4
      mpls labels in/out 16/nolabel
      rx pathid: 0x1, tx pathid: 0x8
  Path advertised to update-groups:
     16         18         19         20         21         22         24
     25         27
  Refresh Epoch 1
  10
    192.0.2.3 from 192.0.2.3 (192.0.2.3)
      Origin IGP, metric 200, localpref 100, valid, external, best2, all
      mpls labels in/out 16/nolabel
      rx pathid: 0, tx pathid: 0x7
  Path advertised to update-groups:
     20         21         22         24         25
  Refresh Epoch 1
  10
    192.0.2.4 from 192.0.2.4 (192.0.2.4)
      Origin IGP, metric 300, localpref 100, valid, external, best3, all
      mpls labels in/out 16/nolabel
      rx pathid: 0, tx pathid: 0x6
  Path advertised to update-groups:
     10         13         17         18         19         20         21
     22         23         24         25         26         27         28
  Refresh Epoch 1
  10
    192.0.2.5 from 192.0.2.5 (192.0.2.5)
      Origin IGP, metric 100, localpref 100, valid, external, best
      mpls labels in/out 16/nolabel
      rx pathid: 0, tx pathid: 0x0
  Path advertised to update-groups:
     21
  Refresh Epoch 1
  30
    192.0.2.6 from 192.0.2.6 (192.0.2.6)
```

```
    Origin IGP, metric 200, localpref 100, valid, internal, all
    Originator: 192.0.2.6, Cluster list: 5.5.5.5
    mpls labels in/out 16/nolabel
    rx pathid: 0x1, tx pathid: 0x5
  Path advertised to update-groups:
     18         23         24         26         28
  Refresh Epoch 1
  60 40, (Received from a RR-client)
    192.0.2.7 from 192.0.2.7 (192.0.2.7)
    Origin IGP, metric 250, localpref 100, valid, internal, group-best
    Originator: 192.0.2.7, Cluster list: 3.3.3.3
    mpls labels in/out 16/nolabel
    rx pathid: 0x2, tx pathid: 0x2
  Path advertised to update-groups:
     25
  Refresh Epoch 1
  30 40, (Received from a RR-client)
    192.0.2.8 from 192.0.2.8 (192.0.2.8)
    Origin IGP, metric 200, localpref 100, valid, internal, all
    Originator: 192.0.2.8, Cluster list: 2.2.2.2
    mpls labels in/out 16/nolabel
    rx pathid: 0x1, tx pathid: 0x3
  Path advertised to update-groups:
     18         21         23         24         25         26         28
  Refresh Epoch 1
  20 40, (Received from a RR-client)
    192.0.2.9 from 192.0.2.9 (192.0.2.9)
    Origin IGP, metric 200, localpref 100, valid, internal, group-best, all
    Originator: 192.0.2.9, Cluster list: 2.2.2.2
    mpls labels in/out 16/nolabel
    rx pathid: 0x1, tx pathid: 0x4
  Path advertised to update-groups:
     21
  Refresh Epoch 1
  30 40
    192.0.2.9 from 192.0.2.9 (192.0.2.9)
    Origin IGP, metric 100, localpref 100, valid, internal, all
    Originator: 192.0.2.9, Cluster list: 4.4.4.4
    mpls labels in/out 16/nolabel
    rx pathid: 0x1, tx pathid: 0x1
```

The following is sample output from the **show ip bgp** command that displays unknown and discarded path attributes:

```
Device# show ip bgp 192.0.2.0/32

BGP routing table entry for 192.0.2.0/32, version 0
Paths: (1 available, no best path)
  Refresh Epoch 1
  Local
    192.168.101.2 from 192.168.101.2 (192.168.101.2)
      Origin IGP, localpref 100, valid, internal
      unknown transitive attribute: flag 0xE0 type 0x81 length 0x20
        value 0000 0000 0000 0000 0000 0000 0000 0000
              0000 0000 0000 0000 0000 0000 0000 0000

      unknown transitive attribute: flag 0xE0 type 0x83 length 0x20
        value 0000 0000 0000 0000 0000 0000 0000 0000
              0000 0000 0000 0000 0000 0000 0000 0000

      discarded unknown attribute: flag 0x40 type 0x63 length 0x64
       value 0000 0000 0000 0000 0000 0000 0000 0000
              0000 0000 0000 0000 0000 0000 0000 0000
```

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

```
Device# show ip bgp version

BGP table version is 5, local router ID is 10.2.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*> 192.168.34.2/24 10.0.0.1 0 0 1 ?
*> 192.168.35.2/24 10.0.0.1 0 0 1 ?
```

The following example shows how to display the network version:

```
Device# show ip bgp 192.168.34.2 | include version

BGP routing table entry for 192.168.34.2/24, version 5
```

The following sample output from the **show ip bgp version recent** command displays the prefix changes in the specified version:

```
Device# show ip bgp version recent 2

BGP table version is 5, local router ID is 10.2.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network              Next Hop      Metric LocPrf  Weight   Path
*> 192.168.134.1/28     10.0.0.1         0             0       1 ?
*> 192.168.134.19/28    10.0.0.1         0             0       1 ?
*> 192.168.134.34/28    10.0.0.1         0             0       1 ?
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
clear ip bgp	Resets BGP connections using hard or soft reconfiguration.
ip bgp community new-format	Configures BGP to display communities in the format AA:NN.
ip prefix-list	Creates a prefix list or adds a prefix-list entry.
route-map	Defines the conditions for redistributing routes from one routing protocol into another routing protocol.
router bgp	Configures the BGP routing process.

show ip bgp bmp

To display information about the BGP Monitoring Protocol (BMP) servers and neighbors, use the **show ip bgp bmp** command in privileged EXEC mode.

show ip bgp bmp {**neighbors** | **server** {*server-number* | **details** | **summary**}}

Syntax Description

neighbors	Displays information about the BGP neighbors configured for BMP.
server	Displays information about the BMP servers.
server-number	Displays information about a particular BMP server. The range of BMP servers you can display is from 1 to 4.
details	Displays detailed information about BMP servers.
summary	Displays a summary of the BMP server status.

Command Default

No information about the BGP BMP servers or the BGP BMP neighbors is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S

Usage Guidelines

Use the **neighbor bmp-activate** and the **bmp** commands to configure the BMP servers, clients, and BGP neighbors. Once configured, use the **show ip bgp bmp** command to display the following information:

- Number of BMP servers configured.
- Number of BGP neighbors configured for BMP.
- Current state of the BMP servers.
- Duration of the initial refresh delay and buffer size for BMP.
- Various queues, such as TransitionQ, MonitoringQ, ConfigQ, and StatsQ, configured for the BGP BMP neighbors and BMP servers.
- The IP address or network address, port number, status, uptime, number of messages sent, and the number of active and configured BMP servers for a BGP BMP neighbor.

Examples

The following is sample output from the **show ip bgp bmp server** command for server number 1. The attributes displayed are configured in the BMP server configuration mode:

```
Device# show ip bgp bmp server 1

Print detailed info for 1 server number 1.

bmp server 1
address: 10.1.1.1    port 8000
description SERVER1
up time 00:06:22
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

The following is sample output from the **show ip bgp bmp server** command for server number 2. The attributes displayed are configured in the BMP server configuration mode:

```
Device# show ip bgp bmp server 2

Print detailed info for 1 server number 2.

bmp server 2
address: 20.1.1.1    port 9000
description SERVER2
up time 00:06:23
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

The following is sample output from the **show ip bgp bmp server summary** command after deactivating the BMP server 1 and 2 connections:

```
Device# show ip bgp bmp server summary

Number of BMP servers configured: 2
Number of BMP neighbors configured: 10
Number of neighbors on TransitionQ: 0, MonitoringQ: 0, ConfigQ: 0
Number of BMP servers on StatsQ: 0
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 3s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB

ID Host/Net          Port  TCB                Status  Uptime    MsgSent   LastStat
1  10.1.1.1          8000  0x0                Down              0
2  20.1.1.1          9000  0x0                Down              0
```

The following is sample output from the **show ip bgp bmp neighbors** command, which shows the status of the BGP BMP neighbors after reactivating the BMP server 1 and 2 connections:

```
Device# show ip bgp bmp server neighbors

Number of BMP neighbors configured: 10
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 3s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB

Neighbor           PriQ      MsgQ      CfgSvr#             ActSvr#             RM Sent
30.1.1.1           0         0         1  2                1  2                16
2001:DB8::2001     0         0         1  2                1  2                15
40.1.1.1           0         0         1  2                1  2                26
2001:DB8::2002     0         0         1  2                1  2                15
```

```
50.1.1.1           0         0         1  2              1  2              16
60.1.1.1           0         0         1  2              1  2              26
2001:DB8::2002     0         0         1                 1                 9
70.1.1.1           0         0         2                 2                 12
Neighbor           PriQ      MsgQ      CfgSvr#           ActSvr#           RM Sent
80.1.1.1           0         0         1                 1                 10
2001:DB8::2002     0         0         1  2              1  2              16
```

Related Commands

Command	Description
bmp	Configures BMP parameters on BGP BMP servers.
neighbor bmp-activate	Activates monitoring of BMP servers.

show ip bgp all dampening

To display BGP dampening information, use the **show ip bgp all dampening**command in user EXEC or privileged EXEC mode.

show ip bgp all dampening {**dampened-paths**| **flap-statistics** [**filter-list** *filter-list*| **quote-regexp** *regexp*| **regexp** *regexp*]| **parameters**}

Syntax Description

dampened-paths	Display routes suppressed due to dampening.
flap-statistics	Displays flap statistics of routes.
filter-list *filter-list*	(Optional) Used with the **flap-statistics** keyword, displays routes that conform to the specified filter list in the range 1-500.
quote-regexp *regexp*	(Optional) Used with the **flap-statistics** keyword, displays routes matching the AS path “regular expression”.
regexp *regexp*	(Optional) Used with the **flap-statistics** keyword, displays routes matching the AS path regular expression.
parameters	Display details of configured dampening parameters.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use this command to display BGP dampening information.

Examples

The following example show how to display the BGP dampening parameters.

```
Router# show ip bgp all dampening parameters

For address family: IPv4 Unicast
% dampening not enabled for base
For address family: VPNv4 Unicast
```

```
% dampening not enabled for base
For vrf: Cust_A
 dampening 15 750 2000 60 (DEFAULT)
  Half-life time      : 15 mins       Decay Time       : 2320 secs
  Max suppress penalty: 12000         Max suppress time: 60 mins
  Suppress penalty    :  2000         Reuse penalty    : 750
For vrf: Cust_B
 dampening 15 750 2000 60 (DEFAULT)
  Half-life time      : 15 mins       Decay Time       : 2320 secs
  Max suppress penalty: 12000         Max suppress time: 60 mins
  Suppress penalty    :  2000         Reuse penalty    : 750
For address family: IPv4 Multicast
% dampening not enabled for base

Router#
```

The table below describes the significant fields shown in the display.

Table 4: show ip bgp all dampening Field Descriptions

Field	Description
Half-life time	Time after which a penalty is decreased, in minutes. Once the interface has been assigned a penalty, the penalty is decreased by half after the half-life period. The process of reducing the penalty happens every 5 seconds. The range of the half-life is 1 to 45 minutes. The default is 1 minute.
Decay Time	Penalty value below which an unstable interface is unsuppressed, in seconds. The process of unsuppressing routers occurs at 10-second increments. The range of the reuse value is 1 to 20000 seconds. The default value is 750 seconds.
Max suppress penalty	Limit at which an interface is suppressed when its penalty exceeds that limit, in seconds. The default value is 2000 seconds.
Max suppress time	Maximum time that an interface can be suppressed, in minutes. This value effectively acts as a ceiling that the penalty value cannot exceed. The default value is four times the half-life period.

The following is sample output for the **show ip bgp all dampening dampened-paths** command. The output includes dampened paths for individual VRFs.

```
Router# show ip bgp all dampening dampened-paths

For address family: IPv4 Unicast
% dampening not enabled for base
For address family: VPNv4 Unicast
% dampening not enabled for base
For vrf: Cust_A
BGP table version is 42, local router ID is 144.124.23.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network          From             Reuse    Path
Route Distinguisher: 1:100 (Cust_A)
*d 10.10.10.10/32   172.16.1.2       00:04:49 65001 ?
*d 20.20.20.20/32   172.16.1.2       00:04:59 65001 ?
For address family: IPv4 Multicast
% dampening not enabled for base
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show dampening interface	Displays a summary of the dampening parameters and status.

show ip bgp cidr-only

To display routes with classless interdomain routing (CIDR), use the **show ip bgp cidr-only** command in user EXEC or privileged EXEC mode.

show ip bgp cidr-only

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip bgp cidr-only** command in privileged EXEC mode:

```
Router# show ip bgp cidr-only

BGP table version is 220, local router ID is 172.16.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*> 192.168.0.0/8    172.16.72.24                         0 1878 ?
*> 172.16.0.0/16    172.16.72.30                         0 108 ?
```

The table below describes the significant fields shown in the display.

Table 5: show ip bgp cidr-only Field Descriptions

Field	Description
BGP table version is 220	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
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 (iBGP) session.
Origin codes	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 an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
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 access server has some non-BGP route to this network.
Metric	If shown, the value of the interautonomous system metric.
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.

Field	Description
Path	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.

show ip bgp cluster-ids

To display the cluster IDs applied to any neighbor and other cluster information, use the **show ip bgp cluster-ids** command in user EXEC or privileged EXEC mode.

show ip bgp cluster-ids

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

Use this command to display cluster IDs, including the number of neighbors using each cluster ID, and those cluster IDs for which intracluster client-to-client route reflection has been disabled.

Examples

The following is sample output for the **show ip bgp cluster-ids** command:

```
Device# show ip bgp cluster-id

Global cluster-id: 1.1.1.10 (configured: 0.0.0.0)
BGP client-to-client reflection:         Configured    Used
   all (inter-cluster and intra-cluster): ENABLED
   intra-cluster:                          ENABLED       ENABLED

List of cluster-ids:
Cluster-id     #-neighbors C2C-rfl-CFG C2C-rfl-USE
0.0.0.1                  1 ENABLED     ENABLED
0.0.0.2                  1 DISABLED    DISABLED
0.0.0.3                  1 DISABLED    DISABLED
0.0.0.4                  0 DISABLED    DISABLED
```

The table below describes the significant fields shown in the display.

Table 6: show ip bgp cluster-ids Field Descriptions

Field	Description
Global cluster-id	Global cluster ID, which is either configured by the **bgp cluster-id** command or, in the absence of such configuration, the router ID of the local route reflector.

Field	Description
configured:	Global cluster ID configured by the **bgp cluster-id** command. The cluster ID 0.0.0.0 means no cluster ID was configured, so the router ID is used as the default cluster ID.
BGP client-to-client reflection:	Configured and Used are column headings for the data below them. Because of the order in which the software processes the commands, what is configured might not be what is used. See the **bgp client-to-client reflection intra-cluster** command for the rules that determine whether reflection is enabled or not.
all (inter-cluster and intra-cluster):	Intracluster and intercluster client-to-client reflection is ENABLED (which is the default) or DISABLED by the **bgp client-to-client reflection** command.
intra-cluster:	Intracluster client-to-client reflection is ENABLED (which is the default) or DISABLED by the **bgp client-to-client reflection intra-cluster** command. Values are displayed for what is Configured and what is Used because they could be different values. See the **bgp client-to-client reflection intra-cluster** command for the rules that determine whether reflection is enabled or not.
List of cluster-ids: Cluster-id	Cluster IDs configured on the device.
#-neighbors	Number of neighbors that are using each cluster ID (regardless of whether the cluster ID is configured directly or by a template).
C2C-rfl-CFG	Client-to-client reflection configured displays ENABLED (the default) or DISABLED, based on what is configured.
C2C-rfl-USE	Client-to-client reflection used displays ENABLED (the default) or DISABLED, based on what command value is used. See the **bgp client-to-client reflection intra-cluster** command for the rules that determine whether reflection is enabled or not.

Related Commands

Command	Description
bgp client-to-client reflection	Enables route reflection from a BGP route reflector to clients.

Command	Description
bgp client-to-client reflection intra-cluster	Enables intracluster client-to-client route reflection to clients for the specified clusters.
bgp cluster-id	Sets the global cluster ID on a route reflector.
neighbor cluster-id	Sets a cluster ID for a neighbor.

show ip bgp community

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

show ip bgp community [*community-number*] **[gshut] [local-as] [no-advertise] [no-export] [exact]**

Syntax Description

community-number	(Optional) Displays routes that have a community number in the range from 1 to 4294967200, or AA:NN (autonomous system-community number/2-byte number).
gshut	(Optional) Displays routes that have the well-known Graceful Shutdown (GSHUT) community.
local-as	(Optional) Displays routes that have the well-known local-AS community, which means do not send outside the local autonomous system.
no-advertise	(Optional) Displays routes that have the well-known no-advertise community, which means do not advertise to any peer.
no-export	(Optional) Displays routes that have the well-known no-export community, which means do not export to the next autonomous system.
exact	(Optional) Displays only routes that have the same communities as the communities specified in this command.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.0	This command was modified. The **local-as** community was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(2)S	This command was modified. The **gshut** keyword was added.
Cisco IOS XE Release 3.6S	This command was modified. The **gshut** keyword was added.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.2(4)S	This command was implemented on the Cisco 7200 series router.

Examples

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

    Network          Next Hop          Metric LocPrf Weight Path
 *> 172.16.2.2/32    10.43.222.2           0             0 222 ?
 *> 10.0.0.0         10.43.222.2           0             0 222 ?
 *> 10.43.0.0        10.43.222.2           0             0 222 ?
 *> 10.43.44.44/32   10.43.222.2           0             0 222 ?
 *  10.43.222.0/24   10.43.222.2           0             0 222 i
 *> 172.17.240.0/21  10.43.222.2           0             0 222 ?
 *> 192.168.212.0    10.43.222.2           0             0 222 i
 *> 172.31.1.0       10.43.222.2           0             0 222 ?
```

The table below describes the significant fields shown in the display.

Table 7: show ip bgp community Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
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 (iBGP) session.
Origin codes	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 an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (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.

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

```
Router# show ip bgp community gshut

BGP table version is 44, local router ID is 87.87.87.87
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
*> 1.1.1.1/32       192.168.10.1                           0 65546 14 i
*> 1.1.1.2/32       192.168.10.1                           0 65546 14 i
*> 1.1.1.3/32       192.168.10.1                           0 65546 14 i
*> 1.1.1.4/32       192.168.10.1                           0 65546 14 i
*> 1.1.1.5/32       192.168.10.1                           0 65546 14 i
*> 1.1.1.6/32       192.168.10.1                           0 65546 14 i
*> 1.1.1.7/32       192.168.10.1                           0 65546 14 i
*> 1.1.1.8/32       192.168.10.1                           0 65546 14 i
*> 1.1.1.9/32       192.168.10.1                           0 65546 14 i
*> 1.1.1.10/32      192.168.10.1                           0 65546 14 i
*> 2.2.2.2/32       192.168.10.1                           0 65546 4260036618 i
*> 2.2.2.3/32       192.168.10.1                           0 65546 4260036618 i
*> 2.2.2.4/32       192.168.10.1                           0 65546 4260036618 i
*> 2.2.2.5/32       192.168.10.1                           0 65546 4260036618 i
```

show ip bgp community-list

To display routes that are permitted by the Border Gateway Protocol (BGP) community list, use the **show ip bgp community-list** command in user EXEC or privileged EXEC mode.

show ip bgp community-list {*community-list-number*| *community-list-name* **[exact-match]**}

Syntax Description

community-list-number	A standard or expanded community list number in the range from 1 to 500.
community-list-name	Community list name. The community list name can be standard or expanded.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.0(10)S	Named community list support was added.
12.0(16)ST	Named community lists support was integrated into Cisco IOS Release 12.0(16)ST.
12.1(9)E	Named community lists support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community lists support was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB to support the Cisco 10000 Series Routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command requires you to specify an argument when used. The **exact-match** keyword is optional.

Examples

The following is sample output of the **show ip bgp community-list** command in privileged EXEC mode:

```
Router# show ip bgp community-list 20

BGP table version is 716977, local router ID is 192.168.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
* i10.3.0.0         10.0.22.1             0    100      0 1800 1239 ?
*>i                 10.0.16.1             0    100      0 1800 1239 ?
* i10.6.0.0         10.0.22.1             0    100      0 1800 690 568 ?
*>i                 10.0.16.1             0    100      0 1800 690 568 ?
* i10.7.0.0         10.0.22.1             0    100      0 1800 701 35 ?
*>i                 10.0.16.1             0    100      0 1800 701 35 ?
*                   10.92.72.24                    0 1878 704 701 35 ?
* i10.8.0.0         10.0.22.1             0    100      0 1800 690 560 ?
*>i                 10.0.16.1             0    100      0 1800 690 560 ?
*                   10.92.72.24                    0 1878 704 701 560 ?
* i10.13.0.0        10.0.22.1             0    100      0 1800 690 200 ?
*>i                 10.0.16.1             0    100      0 1800 690 200 ?
*                   10.92.72.24                    0 1878 704 701 200 ?
* i10.15.0.0        10.0.22.1             0    100      0 1800 174 ?
*>i                 10.0.16.1             0    100      0 1800 174 ?
* i10.16.0.0        10.0.22.1             0    100      0 1800 701 i
*>i                 10.0.16.1             0    100      0 1800 701 i
*                   10.92.72.24                    0 1878 704 701 i
```

The table below describes the significant fields shown in the display.

Table 8: show ip bgp community-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
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 (iBGP) session.

Field	Description
Origin codes	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 an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (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** command in user EXEC or privileged EXEC mode.

show ip bgp dampened-paths

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

On the Cisco 10000 series router, use the **show ip bgp dampening dampened-paths** command to display BGP dampened routes.

Examples

The following is sample output from the **show ip bgp dampened-paths** command in privileged EXEC mode:

```
Router# show ip bgp dampened-paths

BGP table version is 10, local router ID is 172.29.232.182
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         172.16.232.177   00:18:4 100 ?
*d 10.2.0.0         172.16.232.177   00:28:5 100 ?
```

The table below describes the significant fields shown in the display.

Table 9: show ip bgp dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.

Field	Description
local router	IP address of the router where route dampening is enabled.
*d	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp dampening	Clears BGP route dampening information and unsuppresses the suppressed routes.

show ip bgp dampening dampened-paths

To display Border Gateway Protocol (BGP) dampened routes on the Cisco 10000 series router, use the **show ip bgp dampening dampened-paths** command in user EXEC or privileged EXEC mode.

show ip bgp dampening dampened-paths [*community-list-number*| *community-list-name* **[exact-match]**]

Syntax Description

community-list-number	(Optional) Community list number. The range is from 1 to 500.
community-list-name	(Optional) Community list name.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.

Usage Guidelines

For router platforms other than the Cisco 10000 series router, use the **show ip bgp dampened-paths** command to display BGP dampened routes.

Examples

The following example show how to display BGP dampened routes information:

```
Router# show ip bgp dampening dampened-paths

BGP table version is 10, local router ID is 172.29.232.182
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         172.16.232.177   00:18:4 100 ?
*d 10.2.0.0         172.16.232.177   00:28:5 100 ?
```

The table below describes the significant fields shown in the display.

Table 10: show ip bgp dampening dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
*d	Route to the network is dampened.
From	IP address of the peer that advertised this path.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system (AS) path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp dampening	Clears BGP route dampening information and unsuppresses the suppressed routes.
show dampening interface	Displays a summary of the dampening parameters and status.
show ip bgp dampened-paths	Displays IPv6 Border Gateway Protocol (BGP) dampened routes.

show ip bgp dampening flap-statistics

To display Border Gateway Protocol (BGP) flap statistics for all paths on the Cisco 10000 series router, use the **show ip bgp dampening flap-statistics** command in privileged EXEC mode.

show ip bgp dampening flap-statistics [*ip-address* **[mask]**| **cidr-only**| **filter-list** *access-list-number*| **injected-paths**| **labels**| **prefix-list** *prefix-list*| **quote-regexp** *regexp*| **regexp** *regexp*| **route-map** *route-map-name*| **template** {**peer-policy** *template-name*| **peer-session** *template-name*}]

Syntax Description

ip-address	(Optional) IP address for the flap statistics that you want to display.
mask	(Optional) Mask to filter or match hosts that are part of the specified network.
cidr-only	(Optional) Displays flap statistics for routes with classless interdomain routing (CIDR).
filter-list *access-list-number*	(Optional) Displays flap statistics for routes that conform to the specified autonomous system (AS) path access list number.
injected-paths	(Optional) Displays flap statistics for all injected paths.
labels	(Optional) Displays flap statistics for IPv4 Network Layer Reachability Information (NLRI) labels.
prefix-list *prefix-list*	(Optional) Filters output based on the specified prefix list.
quote-regexp *regexp*	(Optional) Filters output based on the specified quoted expression.
regexp *regexp*	(Optional) Filters output based on the specified regular expression.
route-map *route-map-name*	(Optional) Filters output based on the specified route map.
template	(Optional) Displays peer-policy or peer-session template information.
peer-policy *template-name*	(Optional) Used with the **template** keyword, displays peer-policy template information for the specified template name.

peer-session *template-name*	(Optional) Used with the **template** keyword, displays peer-session template information for the specified template name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.

Usage Guidelines

For router platforms other than the Cisco 10000 series router, use the **show ip bgp flap-statistics** command to display BGP flap statistics.

Examples

The following example show how to display the BGP flap statistics for routes with non-natural network masks (CIDR):

```
Router# show ip bgp dampening flap-statistics cidr-only

BGP table version is 56, local router ID is 100.10.7.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i205.0.5.0/30     100.10.5.11              0    100      0 i
*>i205.0.5.4/30     205.0.5.1                0    100      0 105 ?
*>i205.10.5.9/32    205.0.5.1                2    100      0 105 ?
*>i205.10.5.13/32   205.0.5.1                2    100      0 105 ?
*>i206.0.6.0/30     100.10.5.11              0    100      0 i
*>i206.0.6.4/30     206.0.6.1                0    100      0 106 ?
*>i206.10.6.9/32    206.0.6.1                2    100      0 106 ?
*>i206.10.6.13/32   206.0.6.1                2    100      0 106 ?
*> 207.0.7.0/30     0.0.0.0                  0         32768 i
*> 207.0.7.4/30     207.0.7.1                0             0 107 ?
*> 207.10.7.9/32    207.0.7.1                2             0 107 ?
*> 207.10.7.13/32   207.0.7.1                2             0 107 ?
*> 208.0.8.0/30     0.0.0.0                  0         32768 i
*> 208.0.8.4/30     208.0.8.1                0             0 108 ?
*> 208.10.8.9/32    208.0.8.1                2             0 108 ?
*> 208.10.8.13/32   208.0.8.1                2             0 108 ?
```

The table below describes the significant fields shown in the display.

Table 11: show ip bgp dampening flap-statistics cidr-only Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.

Field	Description
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 (iBGP) session.
Network	Internet address of the network that the entry describes.
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 access server has some non-BGP route to this network.
Metric	If shown, the value of the interautonomous system metric.
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. 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.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.

Command	Description
clear ip bgp flap-statistics	Clears BGP flap statistics.
show dampening interface	Displays a summary of the dampening parameters and status.
show ip bgpflap-statistics	Displays BGP flap statistics.

show ip bgp dampening parameters

To display detailed Border Gateway Protocol (BGP) dampening information on the Cisco 10000 series router, use the **show ip bgp dampening parameters** command in privileged EXEC mode.

show ip bgp dampening parameters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2S	This command was introduced.

Examples

The following example shows how to display detailed BGP dampening information:

```
Router# show ip bgp dampening parameters

dampening 15 750 2000 60 (DEFAULT)
  Half-life time      : 15 mins       Decay Time       : 2320 secs
  Max suppress penalty: 12000         Max suppress time: 60 mins
```

The table below describes the significant fields shown in the display.

Table 12: show ip bgp dampening parameters Field Descriptions

Field	Description
Half-life time	Time after which a penalty is decreased, in minutes. Once the interface has been assigned a penalty, the penalty is decreased by half after the half-life period. 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 1 minute.
Decay Time	Penalty value below which an unstable interface is unsuppressed, in seconds. The process of unsupressing routers occurs at 10 second increments. The range of the reuse value is 1 to 20000 seconds. The default value is 750 seconds.
Max suppress penalty	Limit at which an interface is suppressed when its penalty exceeds that limit, in seconds. The default value is 2000 seconds.

Field	Description
Max suppress time	Maximum time that an interface can be suppressed, in minutes. This value effectively acts as a ceiling that the penalty value cannot exceed. The default value is four times the half-life period.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp dampening	Clears BGP dampening information.
show dampening interface	Displays a summary of the dampening parameters and status.

show ip bgp extcommunity-list

To display routes that match the extended community list in the Border Gateway Protocol (BGP) routing table, use the **show ip bgp extcommunity-list** command in user EXEC or privileged EXEC mode.

show ip bgp extcommunity-list [*list-name*]

Syntax Description

list-name	(Optional) Specifies an extended community list name.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(27)SBC	This command was integrated into the Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

You need to configure the extended community lists by using the **ip extcommunity-list** command for the **show ip bgp extcommunity-list** command to display the output.

Examples

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

```
Router# show ip bgp extcommunity-list 1
Standard extended community-list list1
     9 permit RT:1:100 RT:2:100
     19 deny RT:5:100 RT:6:200
     29 permit RT:4:100
     39 permit RT:5:900
     49 permit RT:4:100 RT:6:200
```

The table below describes the significant fields shown in the display.

Table 13: show ip bgp extcommunity-list Field Descriptions

Field	Description
Standard extended community-list	The standard named extended community list.
permit	Permits access for a matching condition. Once a permit value has been configured to match a given set of extended communities, the extended community list defaults to an implicit deny for all other values.
RT	The route target (RT) extended community attribute.
deny	Denies access for a matching condition.

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community list to configure VPN route filtering.
router bgp	Configures the BGP routing process.
show route-map	Displays configured route maps.

show ip bgp filter-list

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

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, or on the Cisco 10000 series router this is a number from 1 to 500.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

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

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

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                           0 109 108 ?
*  172.16.1.0       172.16.72.30                           0 109 108 ?
*  172.16.11.0      172.16.72.30                           0 109 108 ?
*  172.16.14.0      172.16.72.30                           0 109 108 ?
*  172.16.15.0      172.16.72.30                           0 109 108 ?
*  172.16.16.0      172.16.72.30                           0 109 108 ?
*  172.16.17.0      172.16.72.30                           0 109 108 ?
*  172.16.18.0      172.16.72.30                           0 109 108 ?
*  172.16.19.0      172.16.72.30                           0 109 108 ?
*  172.16.24.0      172.16.72.30                           0 109 108 ?
*  172.16.29.0      172.16.72.30                           0 109 108 ?
*  172.16.30.0      172.16.72.30                           0 109 108 ?
*  172.16.33.0      172.16.72.30                           0 109 108 ?
*  172.16.35.0      172.16.72.30                           0 109 108 ?
*  172.16.36.0      172.16.72.30                           0 109 108 ?
*  172.16.37.0      172.16.72.30                           0 109 108 ?
```

```
*  172.16.38.0      172.16.72.30                         0 109 108 ?
*  172.16.39.0      172.16.72.30                         0 109 108 ?
```

The table below describes the significant fields shown in the display.

Table 14: show ip bgp filter-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
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 (iBGP) session.
Origin codes	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 an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
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 route 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.

Field	Description
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. 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.

show ip bgp flap-statistics

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

show ip bgp flap-statistics[**regexp** *regexp*| **filter-list** *access-list*| *ip-address mask*[**longer-prefix**]]

Syntax Description

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

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

Examples

The following is sample output from the **show ip bgp flap-statistics** command in privileged EXEC mode:

```
Router# show ip bgp flap-statistics

BGP table version is 10, local router ID is 172.29.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From            Flaps Duration Reuse    Path
```

```
*d 10.0.0.0         172.29.232.177  4     00:13:31 00:18:10 100
*d 10.2.0.0         172.29.232.177  4     00:02:45 00:28:20 100
```

The table below describes the significant fields shown in the display.

Table 15: show ip bgp flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
Network	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Flaps	Number of times the route has flapped.
Duration	Time (in hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp flap-statistics	Clears BGP flap statistics.

show ip bgp inconsistent-as

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

show ip bgp inconsistent-as

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip bgp inconsistent-as** command in privileged EXEC mode:

```
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
*  10.1.0.0         172.29.232.55          0             0 300 88 90 99 ?
*>                  172.29.232.52       2222             0 400 ?
*  172.29.0.0       172.29.232.55          0             0 300 90 99 88 200 ?
*>                  172.29.232.52       2222             0 400 ?
*  10.200.199.0     172.29.232.55          0             0 300 88 90 99 ?
*>                  172.29.232.52       2222             0 400 ?
```

show ip bgp injected-paths

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

show ip bgp injected-paths

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Examples

The following is sample output from the **show ip bgp injected-paths** command in EXEC mode:

```
Router# show ip bgp injected-paths

BGP table version is 11, local router ID is 10.0.0.1
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
*> 172.16.0.0       10.0.0.2                               0 ?
*> 172.17.0.0/16    10.0.0.2                               0 ?
```

The table below describes the significant fields shown in the display.

Table 16: show ip bgp injected-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
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. d—The table entry is dampened. h—The table entry history. *—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 (iBGP) session.
Origin codes	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 an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (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	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
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 ipv4

To display entries in the IP version 4 (IPv4) Border Gateway Protocol (BGP) routing table, use the **show ip bgp ipv4** command in privileged EXEC mode.

show ip bgp ipv4 {**mdt** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*}| **mvpn** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*}| **unicast** *prefix*| **multicast** *prefix* | **tunnel**}

Syntax Description

mdt	Displays entries for multicast distribution tree (MDT) sessions.
all	Displays all the entries in the routing table.
rd *route-distinguisher*	Displays information about the specified VPN route distinguisher.
vrf *vrf-name*	Displays information about the specified VRF.
mvpn	Displays entries for multicast VPN (MVPN) sessions.
unicast	Displays entries for unicast sessions.
prefix	Displays entries for the specified prefix.
multicast	Displays entries for multicast sessions.
tunnel	Displays entries for tunnel sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(29)S	This command was modified. The **mdt** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
12.4(20)T	This command was modified. The **mdt** keyword was added.
15.2(1)S	This command was modified. An RPKI validation code is displayed per network, if one applies.
Cisco IOS XE 3.5S	This command was modified. An RPKI validation code is displayed per network, if one applies.
Cisco IOS XE 3.7S	This command was modified. Imported paths from a VRF table to the global routing table are displayed, if any.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.
Cisco IOS XE 3.8S	This command was modified. The **mvpn** keyword was added.

Examples

The following is sample output from the **show ip bgp ipv4 unicast** command:

```
Router# show ip bgp ipv4 unicast

 BGP table version is 4, local router ID is 10.0.40.1
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
*> 10.10.10.0/24    172.16.10.1              0             0  300 i
*> 10.10.20.0/24    172.16.10.1              0             0  300 i
*  10.20.10.0/24    172.16.10.1              0             0  300 i
```

The following is sample output from the **show ip bgp ipv4 multicast** command:

```
Router# show ip bgp ipv4 multicast

 BGP table version is 4, local router ID is 10.0.40.1
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
*> 10.10.10.0/24    172.16.10.1              0             0  300 i
*> 10.10.20.0/24    172.16.10.1              0             0  300 i
*  10.20.10.0/24    172.16.10.1              0             0  300 i
```

The table below describes the significant fields shown in the display.

Table 17: show ip bgp ipv4 unicast Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
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. • d—The table entry is damped. • h—The table entry history. • *—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 Border Gateway Protocol (IBGP) session.
Origin codes	Origin of the entry. The origin code is displayed at the end of each line in the table. It can be one of the following values: • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from an Exterior Gateway Protocol (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, the value of the interautonomous system metric.
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.

Field	Description
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show ip bgp ipv4 unicast** *prefix* command. The output indicates the imported path information from a VRF named vpn1.

```
Device# show ip bgp ipv4 unicast 150.1.1.0

BGP routing table entry for 150.1.1.0/24, version 2
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  65002, imported path from 1:1:150.1.1.0/24 (vpn1)
    4.4.4.4 (metric 11) from 4.4.4.4 (4.4.4.4)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      mpls labels in/out nolabel/16
```

Related Commands

Command	Description
clear ip bgp ipv4 mdt	Resets MDT IPv4 BGP address-family sessions.
export map	Exports IP prefixes from a VRF table into the global table.
show ip bgp	Displays entries in the BGP routing table.

show ip bgp ipv4 multicast

To display IP Version 4 multicast database-related information, use the **show ip bgp ipv4 multicast** command in EXEC mode.

show ip bgp ipv4 multicast [*command*]

Syntax Description

command	(Optional) Any multiprotocol BGP command supported by the **show ip bgp ipv4 multicast** *command*.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command in conjunction with the show ip rpf command to determine if IP multicast routing is using multiprotocol BGP routes.

To determine which multiprotocol BGP commands are supported by the **show ip bgp ipv4 multicast** *command*, enter the following command while in EXEC mode:

```
Router# show ip bgp ipv4 multicast ?
```

The **show ip bgp ipv4 multicast** command replaces the **show ip mbgp** command.

Examples

The following is sample output from the **show ip bgp ipv4 multicast** command:

```
Router# show ip bgp ipv4 multicast

MBGP table version is 6, local router ID is 192.168.200.66
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
*> 10.0.20.16/28     0.0.0.0                0      0 32768 i
*> 10.0.35.16/28     0.0.0.0                0      0 32768 i
```

```
*> 10.0.36.0/28      0.0.0.0                  0      0 32768 i
*> 10.0.48.16/28     0.0.0.0                  0      0 32768 i
*> 10.2.0.0/16       0.0.0.0                  0      0 32768 i
*> 10.2.1.0/24       0.0.0.0                  0      0 32768 i
*> 10.2.2.0/24       0.0.0.0                  0      0 32768 i
*> 10.2.3.0/24       0.0.0.0                  0      0 32768 i
*> 10.2.7.0/24       0.0.0.0                  0      0 32768 i
*> 10.2.8.0/24       0.0.0.0                  0      0 32768 i
*> 10.2.10.0/24      0.0.0.0                  0      0 32768 i
*> 10.2.11.0/24      0.0.0.0                  0      0 32768 i
*> 10.2.12.0/24      0.0.0.0                  0      0 32768 i
*> 10.2.13.0/24      0.0.0.0                  0      0 32768 i
```

The table below describes the significant fields shown in the display.

Table 18: show ip bgp ipv4 multicast Field Descriptions

Field	Description
MBGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
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. d—The table entry is dampened. h--The table entry is historical. *—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 (iBGP) session.
Origin codes	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 an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration or address family configuration command. e—Entry originated from an Exterior Gateway Protocol (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.

Field	Description
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, the value of the interautonomous system metric.
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.

Related Commands

Command	Description
show ip rpf	Displays how IP multicast routing does RPF.

show ip bgp ipv4 multicast summary

To display a summary of IP Version 4 multicast database-related information, use the **show ip bgp ipv4 multicast summary** command in EXEC mode.

show ip bgp ipv4 multicast summary

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show ip bgp ipv4 multicast summary** command replaces the **show ip mbgp summary** command.

Examples

The following is sample output from the **show ip bgp ipv4 multicast summary** command:

```
Router# show ip bgp ipv4 multicast summary

BGP router identifier 10.0.33.34, local AS number 34
BGP table version is 5, main routing table version 1
4 network entries and 6 paths using 604 bytes of memory
5 BGP path attribute entries using 260 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
2 BGP community entries using 48 bytes of memory
2 BGP route-map cache entries using 32 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 8/28 prefixes, 12/0 paths, scan interval 15 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.33.35      4    35     624     624        5    0    0 10:13:46        3
```

The table below describes the significant fields shown in the display.

Table 19: show ip bgp ipv4 multicast summary Field Descriptions

Field	Description
Neighbor	IP address of configured neighbor in the multicast routing table.
V	Version of multiprotocol BGP used.
AS	Autonomous system to which the neighbor belongs.
MsgRcvd	Number of messages received from the neighbor.
MsgSent	Number of messages sent to the neighbor.
TblVer	Number of the table version, which is incremented each time the table changes.
InQ	Number of messages received in the input queue.
OutQ	Number of messages ready to go in the output queue.
Up/Down	Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).
State/PfxRcd	State of the neighbor/number of routes received. If no state is indicated, the state is up.

Related Commands

Command	Description
show ip rpf	Displays how IP multicast routing does RPF.

show ip bgp ipv6 multicast

To display multicast entries in the IPv6 BGP routing table, use the **show ip bgp ipv6 multicast** command in user EXEC or privileged EXEC mode.

show ip bgp ipv6 multicast [*prefix*/*length*]

Syntax Description

prefix/*length*	(Optional) IPv6 network number (entered to display a particular network in the IPv6 BGP routing table) and length of the IPv6 prefix. • For the length, a decimal value indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was modified. It displays information about imported paths from a VRF, if any.

Usage Guidelines

The **show ip bgp ipv6 multicast** command provides output similar to the **show ip bgp** command, except that it is IPv6 multicast-specific.

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.

show ip bgp ipv6 unicast

To display entries in the Internet Protocol version 6 (IPv6) Border Gateway Protocol (BGP) routing table, use the **show ip bgp ipv6 unicast** command in user EXEC or privileged EXEC mode.

show ip bgp ipv6 unicast [*prefix*/*length*]

Syntax Description

prefix /*length*	(Optional) IPv6 network number and length of the IPv6 prefix, entered to display a particular network in the IPv6 BGP routing table. • The *length* is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was modified. The command displays the RPKI validation state, if present, as part of the path description.
15.2(1)S	This command was modified. The command displays the RPKI validation state, if present, as part of the path description.
Cisco IOS XE Release 3.7S	This command was modified. It displays information about imported paths from a VRF, if any.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

The **show ip bgp ipv6 unicast** command provides output similar to the **show ip bgp** command, except that it is IPv6 specific.

Examples

The following is sample output from the **show bgp ipv6 unicast** *prefix*/*length* command, showing the RPKI state of the path:

```
Router# show bgp ipv6 unicast 2010::1/128
```

```
BGP routing table entry for 2010::1/128, version 5
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     1          2
  Refresh Epoch 1
  3
    2002::1 (FE80::A8BB:CCFF:FE00:300) from 2002::1 (10.0.0.3)
      Origin IGP, metric 0, localpref 100, valid, external, best
      path 079ECBD0 RPKI State not found
```

The table below describes the significant fields shown in the display.

Table 20: show ip bgp ipv6 Field Descriptions

Field	Description
BGP routing table entry for	IPv6 prefix and prefix length, internal version number of the table. This number is incremented whenever the table changes.
Paths:	Number of routes available to destination.
Advertised to update-groups:	Update group numbers.
3	Autonomous system number.
2002::1 (FE80::A8BB:CCFF:FE00:300) from 2002::1 (10.0.0.3)	Address of the neighbor from which the path was received, link local address of the neighbor, from address of the neighbor, BGP router ID of the neighbor.
Origin	Indicates the origin of the entry.
metric	If shown, the value of the interautonomous system metric.
localpref	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
valid	Path is legitimate.
external	Path is an External Border Gateway Protocol (EBGP) path.
best path	Path is flagged as the best path; number indicates which path in memory.
RPKI State	RPKI state of the network prefix shown at the beginning of the output. The state could be valid, invalid, or not found.

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.

show ip bgp l2vpn

To display Layer 2 Virtual Private Network (L2VPN) address family information from the Border Gateway Protocol (BGP) table, use the **show ip bgp l2vpn** command in user EXEC or privileged EXEC mode.

With BGP show Command Argument

show ip bgp l2vpn vpls {**all** | [**summary** | [**slow**]| **ve-id** *id-value*]| {**block-offset** | [*value*]}| **rd** {*route-distinguisher* | [**ve-id** | {**block-offset** | [*value*]}]}} [*bgp-keyword*]

With IP Prefix and Mask Length Syntax

show ip bgp l2vpn vpls {**all**| **rd** *route-distinguisher*} [*ip-prefix*/*length* [**[bestpath]**] [**longer-prefixes** [**[injected]**]] [**[multipaths]**] [**shorter-prefixes** [[*mask-length*]]] [**[subnets]**]]

With Network Address Syntax

show ip bgp l2vpn vpls {**all**| **rd** *route-distinguisher*} [*network-address* [*mask*| **bestpath**| **multipaths**] **[bestpath]** [**longer-prefixes [injected]**] **[multipaths]** [**shorter-prefixes** [*mask-length*]] **[subnets]**]

Syntax Description

vpls	Displays L2VPN address family database information for the Virtual Private LAN Service (VPLS) subsequent address family identifier (SAFI).
all	Displays the complete L2VPN database.
rd *route-distinguisher*	Displays prefixes that match the specified route distinguisher.
ve-id *id-value*	(Optional) Displays the target VPLS Endpoint (VE) ID and ID value.
summary	(Optional) Displays a summary of BGP neighbor status.
slow	(Optional) Displays a summary of slow-peer status.
block-offset *value*	Displays the target block-offset value.
bgp-keyword	(Optional) Argument representing a **show ip bgp** command keyword that can be added to this command. See the table below.
ip-prefix/*length*	(Optional) The IP prefix address (in dotted decimal format) and the length of the mask (0 to 32). The slash mark must be included.
bestpath	(Optional) Displays the best path for the specified prefix.

longer-prefixes	(Optional) Displays the route and more specific routes.
injected	(Optional) Displays more specific routes that were injected because of the specified prefix.
multipaths	(Optional) Displays the multipaths for the specified prefix.
shorter-prefixes	(Optional) Displays the less specific routes.
mask-length	(Optional) The length of the mask as a number in the range from 0 to 32. Prefixes longer than the specified mask length are displayed.
subnets	(Optional) Displays the subnet routes for the specified prefix.
network-address	(Optional) The IP address of a network in the BGP routing table.
mask	(Optional) The mask of the network address, in dotted decimal format.

Command Default

If no arguments or keywords are specified, this command displays the complete L2VPN database.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE2.6	This command was integrated into Cisco IOS XE Release 2.6.
Cisco IOS XE3.8S	This command was modified. RFC4761 is fully supported in Cisco IOS XE Release 3.8S.

Usage Guidelines

The table below displays optional **show ip bgp** command keywords that can be configured with the **show ip bgp l2vpn** command. Replace the *bgp-keyword* argument with the appropriate keyword from the table. For more details about each command in its **show ip bgp** *bgp-keyword* form, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols,* Release 12.2.

Table 21: Optional show ip bgp Command Keywords and Descriptions

Keyword	Description
community	Displays routes that match a specified community.
community-list	Displays routes that match a specified community list.
dampening	Displays paths suppressed because of dampening (BGP route from peer is up and down).
extcommunity-list	Displays routes that match a specified extcommunity list.
filter-list	Displays routes that conform to the filter list.
inconsistent-as	Displays only routes that have inconsistent autonomous systems of origin.
neighbors	Displays details about TCP and BGP neighbor connections.
oer-paths	Displays all OER-managed path information.
paths [*regexp*]	Displays autonomous system path information. If the optional *regexp* argument is entered, the autonomous system paths that are displayed match the autonomous system path regular expression.
peer-group	Displays information about peer groups.
pending-prefixes	Displays prefixes that are pending deletion.
prefix-list	Displays routes that match a specified prefix list.
quote-regexp	Displays routes that match the quoted autonomous system path regular expression.
regexp	Displays routes that match the autonomous system path regular expression.
replication	Displays the replication status update groups.
route-map	Displays routes that match the specified route map.
rt-filter-list	Displays the specified inbound route target filter list.
summary	Displays a summary of BGP neighbor status.
update-group	Displays information on update groups.

Examples

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **all** keywords are used to display the complete L2VPN database:

```
Device# show ip bgp l2vpn vpls all

BGP table version is 5, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 45000:100
*> 45000:100:172.17.1.1/96
                    0.0.0.0                              32768 ?
*>i45000:100:172.18.2.2/96
                    172.16.1.2               0    100      0 ?
Route Distinguisher: 45000:200
*> 45000:200:172.17.1.1/96
                    0.0.0.0                              32768 ?
*>i45000:200:172.18.2.2/96
                    172.16.1.2               0    100      0 ?
```

The table below describes the significant fields shown in the display.

Table 22: show ip bgp l2vpn vpls all Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
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. • d—The table entry is dampened. • h—The table entry is a historical entry. • *—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 (iBGP) session. • r—The table entry failed to install in the routing information base (RIB) table. • S—The table entry is Stale (old). This entry is useful in BGP graceful restart situations.

Field	Description
Origin codes	Origin of the entry. The origin code is displayed at the end of each line in the table. It can be one of the following values: • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e—Entry originated from an Exterior Gateway Protocol (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, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** command in route-map configuration mode. 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.
Route Distinguisher	Route distinguisher that identifies a set of routing and forwarding tables used in virtual private networks.

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **all** keywords are used to display information about all VPLS BGP signaling prefixes (including local generated and received from remote):

```
Device#show ip bgp l2vpn vpls all

BGP table version is 14743, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
```

```
Network               Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65000:1
*>i 65000:1:VEID-3:Blk-1/136
                      3.3.3.3                  0    100       0 ?
*> 65000:1:VEID-4:Blk-1/136
                      0.0.0.0                             32768 ?
*>i 65000:1:VEID-5:Blk-1/136
                      2.2.2.2                  0    100       0 ?
*>i 65000:1:VEID-6:Blk-1/136
                      4.4.4.4                  0    100       0 ?
Route Distinguisher: 65000:2
*> 65000:2:VEID-20:Blk-20/136
                      0.0.0.0                             32768 ?
*>i 65000:2:VEID-21:Blk-20/136
                      2.2.2.2                  0    100       0 ?
*>i 65000:2:VEID-22:Blk-20/136
                      3.3.3.3                  0    100       0 ?
*>i 65000:2:VEID-23:Blk-20/136
                      4.4.4.4                  0    100       0 ?
```

The following example shows output for the **show ip bgp l2vpn** command when the **vpls**, **all** and **summary** keywords are used to display information about the L2VPN VPLS address family:

```
Device# show ip bgp l2vpn vpls all summary

BGP router identifier 10.1.1.1, local AS number 65000
BGP table version is 14743, main routing table version
14743
6552 network entries using 1677312 bytes of memory
6552 path entries using 838656 bytes of memory
3276/3276 BGP path/bestpath attribute entries using
760032 bytes of memory
1638 BGP extended community entries using 65520 bytes of
memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3341520 total bytes of memory
BGP activity 9828/3276 prefixes, 9828/3276 paths, scan
interval 60 secs
Neighbor        V           AS  MsgRcvd  MsgSent  TblVer  InQ OutQ  Up/Down
State/PfxRcd
10.2.2.2        4        65000   90518   90507    14743   0     0  8w0d     1638
10.3.3.3        4        65000    4901    4895    14743   0     0  2d01h    1638
10.4.4.4        4        65000    4903    4895    14743   0     0  2d01h    1638
```

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **rd** *rd* keywords are used to display information about all VPLS BGP signaling prefixes with the specified rd, i.e. the same VPLS instance:

```
Device# show ip bgp l2vpn vpls rd 65000:3

BGP table version is 14743, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65000:3
*> 65000:3:VEID-30:Blk-30/136
                      0.0.0.0                            32768 ?
*>i 65000:3:VEID-31:Blk-30/136
                      2.2.2.2                  0  100       0 ?
*>i 65000:3:VEID-32:Blk-30/136
                      3.3.3.3                  0  100       0 ?
*>i 65000:3:VEID-33:Blk-30/136
                      4.4.4.4                  0  100       0 ?
```

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **rd** keywords are used to display the L2VPN information that matches the route distinguisher 45000:100. Note that the information displayed is a subset of the information displayed using the **all** keyword.

```
Device# show ip bgp l2vpn vpls rd 45000:100

BGP table version is 5, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 45000:100
*> 45000:100:172.17.1.1/96
                    0.0.0.0                            32768 ?
*>i45000:100:172.18.2.2/96
                    172.16.1.2               0    100      0 ?
```

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **all** keywords are used to display information about an individual prefix:

```
Device# show ip bgp l2vpn vpls all ve-id 31 block 30

BGP routing table entry for 65000:3:VEID-31:Blk-30/136, version 11
Paths: (1 available, best #1, table L2VPN-VPLS-BGP-Table)
   Not advertised to any peer
   Refresh Epoch 2
   Local
     2.2.2.2 (metric 2) from 2.2.2.2 (2.2.2.2)
       Origin incomplete, metric 0, localpref 100, valid, internal, best
       AGI version(0), VE Block Size(10) Label Base(16596)
       Extended Community: RT:65000:3 L2VPN L2:0x0:MTU-1500
       rx pathid: 0, tx pathid: 0x0
                0    100      0 ?
```

Related Commands

Command	Description
address-family l2vpn	Enters address family configuration mode to configure a routing session using L2VPN endpoint provisioning information.
show bgp l2vpn vpls	Displays L2VPN VPLS address family information from the BGP table.

show ip bgp neighbors

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the **show ip bgp neighbors** command in user or privileged EXEC mode.

show ip bgp [**ipv4** {**multicast**| **unicast**}| **vpnv4 all**| **vpnv6 unicast all**] **neighbors** [**slow**| *ip-address*| *ipv6-address* [**advertised-routes**| **dampened-routes**| **flap-statistics**| **paths** [*reg-exp*]| **policy [detail]**| **received prefix-filter**| **received-routes**| **routes**]]

Syntax Description

ipv4	(Optional) Displays peers in the IPv4 address family.
multicast	(Optional) Specifies IPv4 multicast address prefixes.
unicast	(Optional) Specifies IPv4 unicast address prefixes.
vpnv4 all	(Optional) Displays peers in the VPNv4 address family.
vpnv6 unicast all	(Optional) Displays peers in the VPNv6 address family.
slow	(Optional) Displays information about dynamically configured slow peers.
ip-address	(Optional) IP address of the IPv4 neighbor. If this argument is omitted, information about all neighbors is displayed.
ipv6-address	(Optional) IP address of the IPv6 neighbor.
advertised-routes	(Optional) Displays all routes that have been advertised to neighbors.
dampened-routes	(Optional) Displays the dampened routes received from the specified neighbor.
flap-statistics	(Optional) Displays the flap statistics of the routes learned from the specified neighbor (for external BGP peers only).
paths *reg-exp*	(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.
policy	(Optional) Displays the policies applied to this neighbor per address family.

detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs), and autonomous system path filter lists.
received prefix-filter	(Optional) Displays the prefix list (outbound route filter [ORF]) sent from the specified neighbor.
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. The output displayed when this keyword is entered is a subset of the output displayed by the **received-routes** keyword.

Command Default

The output of this command displays information for all neighbors.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Mainline and T Release	Modification
10.0	This command was introduced.
11.2	This command was modified. The **received-routes** keyword was added.
12.2(4)T	This command was modified. The **received** and **prefix-filter** keywords were added.
12.2(15)T	This command was modified. Support for the display of BGP graceful restart capability information was added.
12.3(7)T	This command was modified. The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.4(4)T	This command was modified. Support for the display of Bidirectional Forwarding Detection (BFD) information was added.
12.4(11)T	This command was modified. Support for the **policy** and **detail** keywords was added.
12.4(20)T	This command was modified. The output was modified to support BGP TCP path MTU discovery.

Mainline and T Release	Modification
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.

Command History

S Release	Modification
12.0(18)S	This command was modifed. The output was modified to display the no-prepend configuration option.
12.0(21)ST	This command was modifed. The output was modified to display Multiprotocol Label Switching (MPLS) label information.
12.0(22)S	This command was modified. Support for the display of BGP graceful restart capability information was added. Support for the Cisco 12000 series routers (Engine 0 and Engine 2) was also added.
12.0(25)S	This command was modified. The **policy** and **detail** keywords were added.
12.0(27)S	This command was modified. The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.0(31)S	This command was modified. Support for the display of BFD information was added.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.2(18)SXE	This command was modified. Support for the display of BFD information was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was modified. The output was modified to support BGP TCP path Maximum Transmission Unit (MTU) discovery.
12.2(33)SRB	This command was modified. Support for the **policy** and **detail** keywords was added.

S Release	Modification
12.2(33)SXH	This command was modified. Support for displaying BGP dynamic neighbor information was added.
12.2(33)SRC	This command was modified. Support for displaying BGP graceful restart information was added.
12.2(33)SB	This command was modified. Support for displaying BFD and the BGP graceful restart per peer information was added, and support for the **policy** and **detail** keywords was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI1	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)SRE	This command was modified. Support for displaying BGP best external and BGP additional path features information was added. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was modified. The **slow** keyword was added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)S	This command was modified. The Layer 2 VPN address family is displayed if graceful restart or nonstop forwarding (NSF) is enabled.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
15.2(4)S	This command was modified and implemented on the Cisco 7200 series router. The configured discard and treat-as-withdraw attributes are displayed, along with counts of incoming Updates with a matching discard attribute or treat-as-withdraw attribute, and number of times a malformed Update is treat-as-withdraw. The capabilities of the neighbor to send and receive additional paths that are advertised or received are added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Command History

Cisco IOS XE	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Cisco IOS XE	Modification
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
Cisco IOS XE Release 3.1S	This command was modified. The **slow** keyword was added.
Cisco IOS XE Release 3.6S	This command was modified. Support for displaying BGP BFD multihop and C-bit information was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router and the output modified. The configured discard and treat-as-withdraw attributes are displayed, along with counts of incoming Updates with a matching discard attribute or treat-as-withdraw attribute, and number of times a malformed Update is treat-as-withdraw. The capabilities of the neighbor to send and receive additional paths that are advertised or received are added.
Cisco IOS XE Release 3.8S	This command was modified. In support of the BGP Multi-Cluster ID feature, the cluster ID of a neighbor is displayed if the neighbor is assigned a cluster.

Usage Guidelines

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

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

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538, for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Cisco IOS Releases 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and Later Releases

When BGP neighbors use multiple levels of peer templates, determining which policies are applied to the neighbor can be difficult.

In Cisco IOS Release 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and later releases, the **policy** and **detail** keywords were added to display the inherited policies and the policies configured directly on the specified neighbor. Inherited policies are policies that the neighbor inherits from a peer group or a peer policy template.

Examples

Example output is different for the various keywords available for the **show ip bgp neighbors** command. Examples using the various keywords appear in the following sections.

Examples

The following example shows output for the BGP neighbor at 10.108.50.2. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```
Device# show ip bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:             0          0
    Prefixes Total:               0          0
    Implicit Withdraw:            0          0
    Explicit Withdraw:            0          0
    Used as bestpath:           n/a          0
    Used as multipath:          n/a          0
                                 Outbound    Inbound
  Local Policy Denied Prefixes:  --------    -------
    Total:                              0          0
  Number of NLRIs in the update sent: max 0, min 0
  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
```

```
AckHold            27         18            0x0
SendWnd             0          0            0x0
KeepAlive           0          0            0x0
GiveUp              0          0            0x0
PmtuAger            0          0            0x0
DeadWait            0          0            0x0
iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539
SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6
Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

The table below describes the significant fields shown in the display. Fields that are preceded by the asterisk character (*) are displayed only when the counter has a nonzero value.

Table 23: show ip bgp neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous system number of the neighbor.
local AS 300 no-prepend (not shown in display)	Verifies that the local autonomous system number is not prepended to received external routes. This output supports the hiding of the local autonomous systems when a network administrator is migrating autonomous systems.
internal link	“internal link” is displayed for iBGP neighbors; “external link” is displayed for external BGP (eBGP) neighbors.
BGP version	BGP version being used to communicate with the remote router.
remote router ID	IP address of the neighbor.
BGP state	Finite state machine (FSM) stage of session negotiation.
up for	Time, in hh:mm:ss, that the underlying TCP connection has been in existence.
Last read	Time, in hh:mm:ss, since BGP last received a message from this neighbor.
last write	Time, in hh:mm:ss, since BGP last sent a message to this neighbor.

Field	Description
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving messages.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor. “advertised and received” is displayed when a capability is successfully exchanged between two routers.
Route refresh	Status of the route refresh capability.
MPLS Label capability	Indicates that MPLS labels are both sent and received by the eBGP peer.
Graceful Restart Capability	Status of the graceful restart capability.
Address family IPv4 Unicast	IP Version 4 unicast-specific properties of this neighbor.
Message statistics	Statistics organized by message type.
InQ depth is	Number of messages in the input queue.
OutQ depth is	Number of messages in the output queue.
Sent	Total number of transmitted messages.
Revd	Total number of received messages.
Opens	Number of open messages sent and received.
Notifications	Number of notification (error) messages sent and received.
Updates	Number of update messages sent and received.
Keepalives	Number of keepalive messages sent and received.
Route Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Default minimum time between...	Time, in seconds, between advertisement transmissions.
For address family:	Address family to which the following fields refer.

Field	Description
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
neighbor version	Number used by the software to track prefixes that have been sent and those that need to be sent.
1 update-group member	Number of the update-group member for this address family.
Prefix activity	Prefix statistics for this address family.
Prefixes Current	Number of prefixes accepted for this address family.
Prefixes Total	Total number of received prefixes.
Implicit Withdraw	Number of times that a prefix has been withdrawn and readvertised.
Explicit Withdraw	Number of times that a prefix has been withdrawn because it is no longer feasible.
Used as bestpath	Number of received prefixes installed as best paths.
Used as multipath	Number of received prefixes installed as multipaths.
* Saved (soft-reconfig)	Number of soft resets performed with a neighbor that supports soft reconfiguration. This field is displayed only if the counter has a nonzero value.
* History paths	This field is displayed only if the counter has a nonzero value.
* Invalid paths	Number of invalid paths. This field is displayed only if the counter has a nonzero value.
Local Policy Denied Prefixes	Prefixes denied due to local policy configuration. Counters are updated for inbound and outbound policy denials. The fields under this heading are displayed only if the counter has a nonzero value.
* route-map	Displays inbound and outbound route-map policy denials.
* filter-list	Displays inbound and outbound filter-list policy denials.

Field	Description
* prefix-list	Displays inbound and outbound prefix-list policy denials.
* Ext Community	Displays only outbound extended community policy denials.
* AS_PATH too long	Displays outbound AS_PATH length policy denials.
* AS_PATH loop	Displays outbound AS_PATH loop policy denials.
* AS_PATH confed info	Displays outbound confederation policy denials.
* AS_PATH contains AS 0	Displays outbound denials of autonomous system 0.
* NEXT_HOP Martian	Displays outbound martian denials.
* NEXT_HOP non-local	Displays outbound nonlocal next-hop denials.
* NEXT_HOP is us	Displays outbound next-hop-self denials.
* CLUSTER_LIST loop	Displays outbound cluster-list loop denials.
* ORIGINATOR loop	Displays outbound denials of local originated routes.
* unsuppress-map	Displays inbound denials due to an unsuppress map.
* advertise-map	Displays inbound denials due to an advertise map.
* VPN Imported prefix	Displays inbound denials of VPN prefixes.
* Well-known Community	Displays inbound denials of well-known communities.
* SOO loop	Displays inbound denials due to site-of-origin.
* Bestpath from this peer	Displays inbound denials because the best path came from the local router.
* Suppressed due to dampening	Displays inbound denials because the neighbor or link is in a dampening state.
* Bestpath from iBGP peer	Deploys inbound denials because the best path came from an iBGP neighbor.
* Incorrect RIB for CE	Deploys inbound denials due to RIB errors for a customer edge (CE) router.
* BGP distribute-list	Displays inbound denials due to a distribute list.

Field	Description
Number of NLRIs...	Number of network layer reachability attributes in updates.
Connections established	Number of times a TCP and BGP connection has been successfully established.
dropped	Number of times that a valid session has failed or been taken down.
Last reset	Time, in hh:mm:ss, since this peering session was last reset. The reason for the reset is displayed on this line.
External BGP neighbor may be...	Indicates that the BGP time to live (TTL) security check is enabled. The maximum number of hops that can separate the local and remote peer is displayed on this line.
Connection state	Connection status of the BGP peer.
unread input bytes	Number of bytes of packets still to be processed.
Connection is ECN Disabled	Explicit congestion notification status (enabled or disabled).
Local host: 10.108.50.1, Local port: 179	IP address of the local BGP speaker. BGP port number 179.
Foreign host: 10.108.50.2, Foreign port: 42698	Neighbor address and BGP destination port number.
Enqueued packets for retransmit:	Packets queued for retransmission by TCP.
Event Timers	TCP event timers. Counters are provided for starts and wakeups (expired timers).
Retrans	Number of times a packet has been retransmitted.
TimeWait	Time waiting for the retransmission timers to expire.
AckHold	Acknowledgment hold timer.
SendWnd	Transmission (send) window.
KeepAlive	Number of keepalive packets.
GiveUp	Number of times a packet is dropped due to no acknowledgment.
PmtuAger	Path MTU discovery timer.

Field	Description
DeadWait	Expiration timer for dead segments.
iss:	Initial packet transmission sequence number.
snduna:	Last transmission sequence number that has not been acknowledged.
sndnxt:	Next packet sequence number to be transmitted.
sndwnd:	TCP window size of the remote neighbor.
irs:	Initial packet receive sequence number.
rcvnxt:	Last receive sequence number that has been locally acknowledged.
rcvwnd:	TCP window size of the local host.
delrcvwnd:	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 higher than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT:	Shortest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT:	Longest recorded round-trip timeout.
ACK hold:	Length of time the local host will delay an acknowledgment to carry (piggyback) additional data.
IP Precedence value:	IP precedence of the BGP packets.
Datagrams	Number of update packets received from a neighbor.
Rcvd:	Number of received packets.

Field	Description
out of order:	Number of packets received out of sequence.
with data	Number of update packets sent with data.
total data bytes	Total amount of data received, in bytes.
Sent	Number of update packets sent.
Second Congestion	Number of update packets with data sent.
Datagrams: Rcvd	Number of update packets received from a neighbor.
retransmit	Number of packets retransmitted.
fastretransmit	Number of duplicate acknowledgments retransmitted for an out of order segment before the retransmission timer expires.
partialack	Number of retransmissions for partial acknowledgments (transmissions before or without subsequent acknowledgments).
Second Congestion	Number of second retransmissions sent due to congestion.

Examples

The following partial example shows output for several external BGP neighbors in autonomous systems with 4-byte autonomous system numbers, 65536 and 65550. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router# show ip bgp neighbors

BGP neighbor is 192.168.1.2,  remote AS 65536, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 02:03:38, last write 02:03:38, hold time is 120, keepalive interval is 70
seconds
  Configured hold time is 120, keepalive interval is 70 seconds
  Minimum holdtime from neighbor is 0 seconds
.
.
.
BGP neighbor is 192.168.3.2,  remote AS 65550, external link
 Description: finance
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 02:03:48, last write 02:03:48, hold time is 120, keepalive interval is 70
seconds
  Configured hold time is 120, keepalive interval is 70 seconds
  Minimum holdtime from neighbor is 0 seconds
```

Examples

The following example displays routes advertised for only the 172.16.232.178 neighbor:

```
Device# show ip bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
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
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0               0         32768 i
```

The table below describes the significant fields shown in the display.

Table 24: show ip bgp neighbors advertised-routes Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
local router ID	IP address of the local BGP speaker.
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. • d—The table entry is dampened and will not be advertised to BGP neighbors. • h—The table entry does not contain the best path based on historical information. • *—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 (iBGP) session.

Field	Description
Origin codes	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 Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system used to forward a packet to the destination network. An entry of 0.0.0.0 indicates that there are non-BGP routes in the path to the destination network.
Metric	If shown, this is the value of the interautonomous system metric. This field is not used frequently.
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.

Examples

The following is sample output from the **show ip bgp neighbors** command entered with the **check-control-plane-failure** option configured:

```
Device# show ip bgp neighbors 10.10.10.1

BGP neighbor is 10.10.10.1,  remote AS 10, internal link
 Fall over configured for session
 BFD is configured. BFD peer is Up. Using BFD to detect fast fallover (single-hop) with
c-bit check-control-plane-failure.
 Inherits from template cbit-tps for session parameters
  BGP version 4, remote router ID 10.7.7.7
  BGP state = Established, up for 00:03:55
  Last read 00:00:02, last write 00:00:21, hold time is 180, keepalive interval is 60 seconds

  Neighbor sessions:
    1 active, is not multisession capable (disabled)
```

```
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Enhanced Refresh Capability: advertised and received
    Multisession Capability:
    Stateful switchover support enabled: NO for session 1
```

Examples

The following is sample output from the **show ip bgp neighbors** command entered with the **paths** keyword:

```
Device# show ip bgp neighbors 172.29.232.178 paths 10

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

The table below describes the significant fields shown in the display.

Table 25: show ip bgp neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	Autonomous system path for that route, followed by the origin code for that route.

Examples

The following example shows that a prefix list that filters all routes in the 10.0.0.0 network has been received from the 192.168.20.72 neighbor:

```
Device# show ip bgp neighbors 192.168.20.72 received prefix-filter

Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

The table below describes the significant fields shown in the display.

Table 26: show ip bgp neighbors received prefix-filter Field Descriptions

Field	Description
Address family	Address family mode in which the prefix filter is received.
ip prefix-list	Prefix list sent from the specified neighbor.

Examples

The following sample output shows the policies applied to the neighbor at 192.168.1.2. The output displays both inherited policies and policies configured on the neighbor device. Inherited polices are policies that the neighbor inherits from a peer group or a peer-policy template.

```
Device# show ip bgp neighbors 192.168.1.2 policy

Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

Examples

The following is sample output from the **show ip bgp neighbors** command that verifies that Bidirectional Forwarding Detection (BFD) is being used to detect fast fallover for the BGP neighbor that is a BFD peer:

```
Device# show ip bgp neighbors

BGP neighbor is 172.16.10.2,  remote AS 45000, external link
.
.
.
 Using BFD to detect fast fallover
```

Examples

The following is sample output from the **show ip bgp neighbors** command that verifies that BGP TCP path maximum transmission unit (MTU) discovery is enabled for the BGP neighbor at 172.16.1.2:

```
Device# show ip bgp neighbors 172.16.1.2

BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

Examples

The following is sample output from the **show ip bgp neighbors** command that verifies that the neighbor 192.168.3.2 is a member of the peer group group192 and belongs to the subnet range group 192.168.0.0/16, which shows that this BGP neighbor was dynamically created:

```
Device# show ip bgp neighbors 192.168.3.2
```

```
BGP neighbor is *192.168.3.2,  remote AS 50000, external link
 Member of peer-group group192 for session parameters
 Belongs to the subnet range group: 192.168.0.0/16
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:06:35
  Last read 00:00:33, last write 00:00:25, hold time is 180, keepalive intervals
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent       Rcvd
    Opens:                  1          1
    Notifications:          0          0
    Updates:                0          0
    Keepalives:             7          7
    Route Refresh:          0          0
    Total:                  8          8
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
  Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
  group192 peer-group member
.
.
.
```

Examples

The following is partial output from the **show ip bgp neighbors** command that verifies the status of the BGP graceful restart capability for the external BGP peer at 192.168.3.2. Graceful restart is shown as disabled for this BGP peer.

```
Device# show ip bgp neighbors 192.168.3.2

BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Inherits from template S2 for session parameters
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:01:41
  Last read 00:00:45, last write 00:00:45, hold time is 180, keepalive intervals
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
.
.
.
Address tracking is enabled, the RIB does have a route to 192.168.3.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

Examples

The following is partial output from the **show ip bgp neighbors** command. For this release, the display includes the Layer 2 VFN address family information if graceful restart or NSF is enabled.

```
Device# show ip bgp neighbors

Load for five secs: 2%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:49:17.034 GMT Wed Sep 22 2010
BGP neighbor is 10.1.1.3,  remote AS 2, internal link
```

```
 BGP version 4, remote router ID 10.1.1.3
 BGP state = Established, up for 00:14:32
 Last read 00:00:30, last write 00:00:43, hold time is 180, keepalive interval is 60 seconds

 Neighbor sessions:
   1 active, is not multisession capable (disabled)
 Neighbor capabilities:
   Route refresh: advertised and received(new)
   Four-octets ASN Capability: advertised and received
   Address family IPv4 Unicast: advertised and received
   Address family L2VPN Vpls: advertised and received
   Graceful Restart Capability: advertised and received
     Remote Restart timer is 120 seconds
     Address families advertised by peer:
       IPv4 Unicast (was not preserved), L2VPN Vpls (was not preserved)
   Multisession Capability:
 Message statistics:
   InQ depth is 0
   OutQ depth is 0

                        Sent       Rcvd
   Opens:                  1          1
   Notifications:          0          0
   Updates:                4         16
   Keepalives:            16         16
   Route Refresh:          0          0
   Total:                 21         33
 Default minimum time between advertisement runs is 0 seconds
For address family: IPv4 Unicast
 Session: 10.1.1.3
 BGP table version 34, neighbor version 34/0
 Output queue size : 0
 Index 1, Advertise bit 0
 1 update-group member
 Slow-peer detection is disabled
 Slow-peer split-update-group dynamic is disabled
                             Sent       Rcvd
 Prefix activity:            ----       ----
   Prefixes Current:            2         11 (Consumes 572 bytes)
   Prefixes Total:              4         19
   Implicit Withdraw:           2          6
   Explicit Withdraw:           0          2
   Used as bestpath:          n/a          7
   Used as multipath:         n/a          0
                               Outbound    Inbound
 Local Policy Denied Prefixes:    --------    -------
   NEXT_HOP is us:                     n/a          1
   Bestpath from this peer:             20        n/a
   Bestpath from iBGP peer:              8        n/a
   Invalid Path:                        10        n/a
   Total:                               38          1
 Number of NLRIs in the update sent: max 2, min 0
 Last detected as dynamic slow peer: never
 Dynamic slow peer recovered: never
For address family: L2VPN Vpls
 Session: 10.1.1.3
 BGP table version 8, neighbor version 8/0
 Output queue size : 0
 Index 1, Advertise bit 0
 1 update-group member
 Slow-peer detection is disabled
 Slow-peer split-update-group dynamic is disabled
                             Sent       Rcvd
 Prefix activity:            ----       ----
   Prefixes Current:            1          1 (Consumes 68 bytes)
   Prefixes Total:              2          1
   Implicit Withdraw:           1          0
   Explicit Withdraw:           0          0
   Used as bestpath:          n/a          1
   Used as multipath:         n/a          0
                               Outbound    Inbound
 Local Policy Denied Prefixes:    --------    -------
   Bestpath from this peer:             4        n/a
```

```
    Bestpath from iBGP peer:              1        n/a
    Invalid Path:                         2        n/a
    Total:                                7          0
  Number of NLRIs in the update sent: max 1, min 0
  Last detected as dynamic slow peer: never
  Dynamic slow peer recovered: never
  Address tracking is enabled, the RIB does have a route to 10.1.1.3
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is enabled, restart-time 120 seconds, stalepath-time 360 seconds
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Mininum incoming TTL 0, Outgoing TTL 255
Local host: 10.1.1.1, Local port: 179
Foreign host: 10.1.1.3, Foreign port: 48485
Connection tableid (VRF): 0
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0xE750C):
Timer          Starts    Wakeups            Next
Retrans            18          0             0x0
TimeWait            0          0             0x0
AckHold            22         20             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
Linger              0          0             0x0
iss: 3196633674  snduna: 3196634254  sndnxt: 3196634254     sndwnd:  15805
irs: 1633793063  rcvnxt: 1633794411  rcvwnd:      15037  delrcvwnd:   1347
SRTT: 273 ms, RTTO: 490 ms, RTV: 217 ms, KRTT: 0 ms
minRTT: 2 ms, maxRTT: 300 ms, ACK hold: 200 ms
Status Flags: passive open, gen tcbs
Option Flags: nagle, path mtu capable
Datagrams (max data segment is 1436 bytes):
Rcvd: 42 (out of order: 0), with data: 24, total data bytes: 1347
Sent: 40 (retransmit: 0 fastretransmit: 0),with data: 19, total data bytes: 579
```

Examples

The following is sample output from the **show ip bgp neighbors** command that indicates the discard attribute values and treat-as-withdraw attribute values configured. It also provides a count of received Updates matching a treat-as-withdraw attribute, a count of received Updates matching a discard attribute, and a count of received malformed Updates that are treat-as-withdraw.

```
Device# show ip bgp vpnv4 all neighbors 10.0.103.1

BGP neighbor is 10.0.103.1,  remote AS 100, internal link
 Path-attribute treat-as-withdraw inbound
 Path-attribute treat-as-withdraw value 128
 Path-attribute treat-as-withdraw 128 in: count 2
 Path-attribute discard 128 inbound
 Path-attribute discard 128 in: count 2

      Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    MALFORM treat as withdraw:            0          1
    Total:                                0          1
```

Examples

The following output indicates that the neighbor is capable of advertising additional paths and sending additional paths it receives. It is also capable of receiving additional paths and advertised paths.

```
Device# show ip bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
```

```
 Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is 60 seconds

 Neighbor capabilities:
   Additional paths Send: advertised and received
   Additional paths Receive: advertised and received
   Route refresh: advertised and received(old & new)
   Graceful Restart Capabilty: advertised and received
   Address family IPv4 Unicast: advertised and received
```

Examples

In the following output, the cluster ID of the neighbor is displayed. (The vertical bar and letter “i” for “include” cause the device to display only lines that include the user's input after the “i”, in this case, “cluster-id.”) The cluster ID displayed is the one directly configured through a neighbor or a template.

```
Device# show ip bgp neighbors 192.168.2.2 | i cluster-id

 Configured with the cluster-id 192.168.15.6
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
bgp enhanced-error	Restores the default behavior of treating Update messages that have a malformed attribute as withdrawn, or includes iBGP peers in the Enhanced Attribute Error Handling feature.
neighbor path-attribute discard	Configures the device to discard unwanted Update messages from the specified neighbor that contain a specified path attribute.
neighbor path-attribute treat-as-withdraw	Configures the device to withdraw from the specified neighbor unwanted Update messages that contain a specified attribute.
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
neighbor send-label explicit-null	Enables a BGP router to send MPLS labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router.
router bgp	Configures the BGP routing process.

show ip bgp path-attribute discard

To display all prefixes for which an attribute has been discarded, use the **show ip bgp path-attribute discard** command in user EXEC or privileged EXEC mode.

show ip bgp path-attribute discard

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Examples

The following is sample output from the **show ip bgp path-attribute discard** command:

```
Device# show ip bgp path-attribute discard

Network          Next Hop
2.1.1.1/32       192.168.101.2
```

The table below describes the significant fields shown in the display.

Table 27: show ip bgp path-attribute discard Field Descriptions

Field	Description
Network	Network address and prefix length of the prefix that had a path attribute discarded.
Next Hop	Address of the next hop toward that network.

Related Commands

Command	Description
neighbor path-attribute discard	Configures the device to discard specific path attributes from Update messages from the specified neighbor.

show ip bgp path-attribute unknown

To display all prefixes that have an unknown attribute, use the **show ip bgp path-attribute unknown** command in user EXEC or privileged EXEC mode.

show ip bgp path-attribute unknown

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Examples

The following is sample output from the **show ip bgp path-attribute unknown** command:

```
Device# show ip bgp path-attribute unknown

Network          Next Hop
2.1.1.1/32       192.168.101.2
```

The table below describes the significant fields shown in the display.

Table 28: show ip bgp path-attribute unknown Field Descriptions

Field	Description
Network	Network address and prefix length of the prefix that had an unknown path attribute.
Next Hop	Address of the next hop toward that network.

show ip bgp paths

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

show ip bgp paths

Cisco 10000 Series Router

show ip bgp paths *regexp*

Syntax Description

regexp	Regular expression to match the BGP autonomous system paths.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Examples

The following is sample output from the **show ip bgp paths** command in privileged EXEC mode:

```
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 ?
```

The table below describes the significant fields shown in the display.

Table 29: show ip bgp paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Hash	Hash bucket where path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

show ip bgp peer-group

To display information about BGP peer groups, use the **show ip bgp peer-group** command in user EXEC or privileged EXEC mode.

show ip bgp peer-group [*peer-group-name*] **[summary]**

Syntax Description

peer-group-name	(Optional) Displays information about a specific peer group.
summary	(Optional) Displays a summary of the status of all the members of a peer group.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH, and the output was modified to support BGP dynamic neighbors.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S, with the modified output to support BGP dynamic neighbors.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S, with the modified output to support BGP dynamic neighbors.
15.2.(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Examples

The following is sample output from the **show ip bgp peer-group** command for a peer group named internal in privileged EXEC mode:

```
Router# show ip bgp peer-group internal

BGP peer-group is internal, remote AS 100
  BGP version 4
  Minimum time between advertisement runs is 5 seconds
```

```
 For address family:IPv4 Unicast
  BGP neighbor is internal, peer-group internal, members:
           10.1.1.1         10.1.1.2
  Index 3, Offset 0, Mask 0x8
  Incoming update AS path filter list is 53
  Outgoing update AS path filter list is 54
  Route map for incoming advertisements is MAP193
  Route map for outgoing advertisements is MAP194
  Update messages formatted 0, replicated 0
```

The following output from the **show ip bgp peer-group** command shows information about a configured listen range group, group192. In Cisco IOS Release 12.2(33)SXH, 15.0(1)S, and XE Release 3.1S and later releases, the BGP dynamic neighbor feature introduced the ability to support the dynamic creation of BGP neighbor peers using a subnet range associated with a peer group (listen range group).

```
Router# show ip bgp peer-group group192

BGP peer-group is group192,  remote AS 40000
  BGP peergroup group192 listen range group members:
  192.168.0.0/16
  BGP version 4
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP neighbor is group192, peer-group external, members:
  *192.168.3.2
  Index 0, Offset 0, Mask 0x0
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
```

show ip bgp quote-regexp

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

show ip bgp quote-regexp *regexp*

Syntax Description

regexp	The regular expression to match the Border Gateway Protocol (BGP) autonomous system paths. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command. **Note** The regular expression has to be an exact match.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following is sample output from the **show ip bgp quote-regexp** command in EXEC mode:

```
Router# show ip bgp quote-regexp "^10_" | begin 10.40

*> 10.40.0.0/20     10.10.10.10                          0 10 2548 1239 10643 i
*> 10.40.16.0/20    10.10.10.10                          0 10 2548 6172 i
*> 10.40.32.0/19    10.10.10.10                          0 10 2548 6172 i
*> 10.41.0.0/19     10.10.10.10                          0 10 2548 3356 3703 ?
```

```
*> 10.42.0.0/17     10.10.10.10                          0 10 2548 6172 i
```

Note Although the columns in the above display are not labeled, see the Field Descriptions table below for detailed information.

The table below describes the significant fields shown in the display from left to right.

Table 30: show ip bgp quote-regexp Field Descriptions

Field	Description
Status codes	Status of the table entry; for example, * in the above display. 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. d—The table entry is dampened. h—The table entry history. *—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 (iBGP) session. r—The table entry failed to install in the routing table. S—The table entry is a stale route.
Network	IP address of a network entity; for example, 24.40.0.0/20 in the above display.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network; for example, 10.10.10.10. in the above display. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.; for example, 0 in the above display.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command; for example, 10 in the above display. The default value is 100.
Weight	Weight of the route as set via autonomous system filters; for example, 2548 in the above display.

Field	Description
Path	Autonomous system paths to the destination network; for example, 1239 in the above display. There can be one entry in this field for each autonomous system in the path.
Origin codes	Origin of the entry; for example, ? in the above display. 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 an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.

The following output from the **show ip bgp quote-regexp** command shows routes that match the quoted regular expression for the 4-byte autonomous system number 65550. The 4-byte autonomous system number is displayed in the default asplain format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router# show ip bgp quote-regexp "^65550$"

BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.2.2.0/24     192.168.3.2              0       0 65550 i
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
router bgp	Configures the BGP routing process.
show ip bgp regexp	Displays routes matching the autonomous system path regular expression.

show ip bgp regexp

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

show ip bgp regexp *regexp*

Syntax Description

regexp	Regular expression to match the BGP autonomous system paths. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the **router bgp** command.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

To ensure a smooth transition we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, are upgraded to support 4-byte autonomous system numbers.

Examples

The following is sample output from the **show ip bgp regexp** command in privileged EXEC mode:

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

```
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                           0 109 108 ?
*  172.16.1.0       172.16.72.30                           0 109 108 ?
*  172.16.11.0      172.16.72.30                           0 109 108 ?
*  172.16.14.0      172.16.72.30                           0 109 108 ?
*  172.16.15.0      172.16.72.30                           0 109 108 ?
*  172.16.16.0      172.16.72.30                           0 109 108 ?
*  172.16.17.0      172.16.72.30                           0 109 108 ?
*  172.16.18.0      172.16.72.30                           0 109 108 ?
*  172.16.19.0      172.16.72.30                           0 109 108 ?
*  172.16.24.0      172.16.72.30                           0 109 108 ?
*  172.16.29.0      172.16.72.30                           0 109 108 ?
*  172.16.30.0      172.16.72.30                           0 109 108 ?
*  172.16.33.0      172.16.72.30                           0 109 108 ?
*  172.16.35.0      172.16.72.30                           0 109 108 ?
*  172.16.36.0      172.16.72.30                           0 109 108 ?
*  172.16.37.0      172.16.72.30                           0 109 108 ?
*  172.16.38.0      172.16.72.30                           0 109 108 ?
*  172.16.39.0      172.16.72.30                           0 109 108 ?
```

The following example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release. After the **bgp asnotation dot** command is configured, the regular expression match format for 4-byte autonomous system paths is changed to asdot notation format. Although a 4-byte autonomous system number can be configured in a regular expression using either asplain or asdot format, only 4-byte autonomous system numbers configured using the current default format are matched. In the first example, the **show ip bgp regexp** command is configured with a 4-byte autonomous system number in asplain format. The match fails because the default format is currently asdot format and there is no output. In the second example using asdot format, the match passes and the information about the 4-byte autonomous system path is shown using the asdot notation.

Note The asdot notation uses a period which is a special character in Cisco regular expressions. to remove the special meaning, use a backslash before the period.

```
Router# show ip bgp regexp ^65536$

Router# show ip bgp regexp ^1\.0$

BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

The following is sample output from the **show ip bgp regexp** command after the **bgp asnotation dot** command has been entered to display 4-byte autonomous system numbers in dot notation in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or later release. The dot notation is the only format for 4-byte autonomous system numbers in Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3.

Note The asdot notation uses a period which is a special character in Cisco regular expressions. to remove the special meaning, use a backslash before the period.

```
Router# show ip bgp regexp ^1\.14$
```

```
BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.14   i
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
router bgp	Configures the BGP routing process.
show ip bgp quote-regexp	Displays routes matching the autonomous system path regular expression.

show ip bgp replication

To display update replication statistics for Border Gateway Protocol (BGP) update groups, use the **show ip bgp replication** command in EXEC mode.

show ip bgp replication [*index-group*| *ip-address*]

Syntax Description

index-group	(Optional) Displays update replication statistics for the update group with the corresponding index number. The range of update-group index numbers is from 1 to 4294967295.
ip-address	(Optional) Displays update replication statistics for this neighbor.

Command Modes

EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The output of this command displays BGP update-group replication statistics.

When a change to outbound policy occurs, the router automatically recalculates update-group memberships and applies the changes by triggering an outbound soft reset after a 3-minute timer expires. This behavior is designed to provide the network operator with time to change the configuration if a mistake is made. You can manually enable an outbound soft reset before the timer expires by entering the **clear ip bgp** *ip-address* **soft out** command.

Examples

The following sample output from the **show ip bgp replication** command shows update-group replication information for all neighbors:

```
Router# show ip bgp replication

BGP Total Messages Formatted/Enqueued : 0/0
     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         1 internal        1       10.4.9.21        0        0      0      0
         2 internal        2        10.4.9.5        0        0      0      0
```

The following sample output from the **show ip bgp replication**command shows update-group statistics for the 10.4.9.5 neighbor:

```
Router# show ip bgp replication 10.4.9.5

     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         2 internal        2       10.4.9.5        0        0      0      0
```

The table below describes the significant fields shown in the display.

Table 31: show ip bgp replication Field Descriptions

Field	Description
Index	Index number of the update group.
Type	Type of peer (internal or external).
Members	Number of members in the dynamic update peer group.
Leader	First member of the dynamic update peer group.

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.
clear ip bgp update-group	Clears BGP update-group member sessions.
debug ip bgp groups	Displays information related to the processing of BGP update groups.
show ip bgp peer-group	Displays information about BGP update groups.

show ip bgp rib-failure

To display Border Gateway Protocol (BGP) routes that failed to install in the Routing Information Base (RIB) table, use the **show ip bgp rib-failure** command in privileged EXEC mode.

show ip bgp rib-failure

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3	This command was introduced.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

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

```
Router# show ip bgp rib-failure

Network          Next Hop                    RIB-failure   RIB-NH Matches
10.1.15.0/24     10.1.35.5          Higher admin distance             n/a
10.1.16.0/24     10.1.15.1          Higher admin distance             n/a
```

The table below describes the significant fields shown in the display.

Table 32: show ip bgp rib-failure Field Descriptions

Field	Description
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.

Field	Description
RIB-failure	Cause of RIB failure. Higher admin distance means that a route with a better (lower) administrative distance such as a static route already exists in the IP routing table.
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and **bgp suppress-inactive** is configured for the address family being used. There are three choices: • Yes—Means that the route in the RIB has the same next hop as the BGP route or next hop recurses down to the same adjacency as the BGP nexthop. • No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route. • n/a—Means that **bgp suppress-inactive** is not configured for the address family being used.

Related Commands

Command	Description
bgp suppress-inactive	Configures a router to suppress the advertisement of BGP routes that are not installed in the RIB and FIB tables.
clear ip bgp	Resets a BGP connection or session.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show ip bgp rpki servers

To display the current state of communication with the Resource Public Key Infrastructure (RPKI) cache servers, use the **show ip bgp rpki servers** command in user EXEC or privileged EXEC mode.

show ip bgp rpki servers

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

This command is useful after configuring the **bgp rpki server** command.

Examples

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

```
Router# show ip bgp rpki servers

BGP SOVC neighbor is 10.0.96.254 connected to port 32000
Flags 0, Refresh time is 5, Serial number is 1
InQ has 0 messages, OutQ has 0 messages, formatted msg 9
Session IO flags 0, Session flags 10000008
 Neighbor Statistics:
  Nets Processed 13

Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Minimum incoming TTL 0, Outgoing TTL 255
Local host: 10.0.96.2, Local port: 56238
Foreign host: 10.0.96.254, Foreign port: 32000
Connection tableid (VRF): 0

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0xCD931):
Timer          Starts    Wakeups            Next
Retrans            10          0             0x0
TimeWait            0          0             0x0
AckHold             9          9             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            1          0        0x1554E6
```

```
DeadWait            0          0             0x0
Linger              0          0             0x0

iss: 1144343423  snduna: 1144343528  sndnxt: 1144343528     sndwnd:   5840
irs: 2151800169  rcvnxt: 2151800610  rcvwnd:      15944  delrcvwnd:    440

SRTT: 221 ms, RTTO: 832 ms, RTV: 611 ms, KRTT: 0 ms
minRTT: 3 ms, maxRTT: 300 ms, ACK hold: 200 ms
Status Flags: none
Option Flags: higher precendence, nagle, path mtu capable

Datagrams (max data segment is 1460 bytes):
Rcvd: 11 (out of order: 0), with data: 9, total data bytes: 440
Sent: 20 (retransmit: 0 fastretransmit: 0),with data: 9, total data bytes: 104
```

Related Commands

Command	Description
bgp rpki server	Connects to an RPKI server and enables the validation of BGP prefixes based on the AS from which the prefix originates.
neighbor announce rpki state	Sends and receives the RPKI status and prefix/AS pairs to and from an IBGP neighbor.

show ip bgp rpki table

To display the currently cached list of networks and associated autonomous system (AS) numbers received from the Resource Public Key Infrastructure (RPKI) server, use the **show ip bgp rpki table** command in user EXEC or privileged EXEC mode.

show ip bgp [**ipv6 unicast**] **rpki table**

Syntax Description

ipv6 unicast	(Optional) Displays only the IPv6 prefixes.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

This command is useful after configuring the **bgp rpki server** command to see the list of networks and corresponding AS numbers received from the RPKI server.

Examples

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

```
Router# show ip bgp rpki table

12 BGP sovc network entries using 1056 bytes of memory
13 BGP sovc record entries using 260 bytes of memory

Network              Maxlen  Origin-AS  Source  Neighbor
1.1.0.0/16           24      1          0       10.0.96.254
3.0.0.0/24           24      2          0       10.0.96.254
4.0.0.0/24           24      3          0       10.0.96.254
4.0.0.0/8            8       3          0       10.0.96.254
5.0.0.0/24           24      4          0       10.0.96.254
8.0.0.0/4            6       200        0       10.0.96.254
8.2.0.0/8            24      36394      0       10.0.96.254
9.2.0.0/16           24      34000      0       10.0.96.254
10.0.0.0/6           8       100        0       10.0.96.254
```

The table below describes the significant fields shown in the display.

Table 33: show ip bgp rpki table Field Descriptions

Field	Description
Network	Prefix and mask length received from RPKI server.
Maxlen	Limit on the prefix length of the corresponding network (the value is provided by the server).
Origin-AS	Number of the AS from which the prefix originated.
Source	Value is always 0.
Neighbor	IP address of the RPKI cache server from which the record came.

Related Commands

Command	Description
bgp rpki server	Connects to an RPKI server and enables the validation of BGP prefixes based on the AS from which the prefix originates.
neighbor announce rpki state	Sends and receives the RPKI status and prefix/AS pairs to and from an IBGP neighbor.

show ip bgp rtfilter

To display information about BGP route target (RT) filtering, use the **show ip bgp rtfilter** command in user EXEC or privileged EXEC mode.

show ip bgp rtfilter {**all | default | rt** {*ASN*| *ip-address*} **:***nn*}

Syntax Description

all	Displays RT information for all VPNs.
default	Displays the default RT filter.
rt	Displays a specific RT filter prefix.
*ASN***:***nn*	Autonomous system number, followed by a colon and number.
*ip-address***:***nn*	IP address, followed by a colon and a number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)S	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use this command if you have configured the BGP: RT Constrained Route Distribution feature and you want to display RT filter information.

Note If you enter the **all** keyword, many more optional keywords are available that are not shown here.

Examples

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

```
Router# show ip bgp rtfilter all

BGP table version is 14, local router ID is 192.168.7.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network  Next Hop Metric LocPrf  Weight Path
*>i0:0:0:0 192.168.2.2 0 100 0 i
*>i1:2:1:100 192.168.6.6 0 100 0 i
* i1:2:3:3 192.168.2.2 0 100 0 i
*> 0.0.0.0   32768 i
*>i1:2:150:1 192.168.6.6 0 100 0 i
* i1:2:200:200 192.168.2.2 0 100 0 i
*> 0.0.0.0    32768 i
```

The table below describes the fields shown in the display.

Table 34: show ip bgp rtfilter Field Descriptions

Field	Description
Network	RT filter prefix.
Next Hop	Next hop in the RT filter prefix.
Metric	BGP metric associated with the RT filter prefix.
LocPref	BGP local preference.
Weight	BGP weight.
Path	Path information associated with the RT prefix.

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

```
Router# show ip bgp rtfilter all summary

BGP router identifier 192.168.7.7, local AS number 1
BGP table version is 14, main routing table version 14
5 network entries using 820 bytes of memory
7 path entries using 336 bytes of memory
2/2 BGP path/bestpath attribute entries using 256 bytes of memory
1 BGP rrinfo entries using 24 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1484 total bytes of memory
BGP activity 7/0 prefixes, 14/5 paths, scan interval 60 secs
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down  State/PfxRcd
192.168.2.2 4 1 13 12 14 0 0 00:03:21        5
```

Related Commands

Command	Description
address-family rtfilter unicast	Enters address family configuration mode and enables Automated Route Target Filtering with a BGP peer.
neighbor default-originate	Allows a BGP speaker (the local router) to send the default route 0:0:0:0 to a neighbor for use as a default route.
show ip bgp rtfilter all summary	Displays summary information about RT filtering.

show ip bgp summary

To display the status of all Border Gateway Protocol (BGP) connections, use the **show ip bgp summary** command in user EXEC or privileged EXEC mode.

show ip bgp [**ipv4** {**multicast**| **unicast**}| **vpnv4 all**| **vpnv6 unicast all**| **topology** {*| *routing-topology-instance-name*}] **[update-group] summary [slow]**

Syntax Description

ipv4 {**multicast** | **unicast**}	(Optional) Displays peers in the IPv4 address family.
vpnv4 all	(Optional) Displays peers in the VPNv4 address family.
vpnv6 unicast all	(Optional) Displays peers in the VPNv6 address family.
topology	(Optional) Displays routing topology information.
*	(Optional) Displays all routing topology instances.
routing-topology-instance-name	(Optional) Displays routing topology information for that instance.
update-group	(Optional) Includes information about the update group of the peers.
slow	(Optional) Displays only information about dynamically configured slow peers.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0	Support for the **neighbor maximum-prefix** command was added to the output.
12.2	This command was modified. • The number of networks and paths displayed in the output was split out to two separate lines. • A field was added to display multipath entries in the routing table.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was modified. A line was added to the output to display the advertised bitfield cache entries and associated memory usage.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH, and the output was modified to support BGP dynamic neighbors.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was modified. The **slow** keyword was added.
Cisco IOS XE Release 3.1S	This command was modified. The **slow** keyword was added.
15.2(1)S	This command was modified. It will show information about how many paths are in each RPKI state.
Cisco IOS XE Release 3.5S	This command was modified. It will show information about how many paths are in each RPKI state.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

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

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

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

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following is sample output from the **show ip bgp summary** command in privileged EXEC mode:

```
Router# show ip bgp summary

BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 199, main routing table version 199
37 network entries using 2850 bytes of memory
59 path entries using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
2 multipath network entries and 4 multipath paths
10 BGP AS-PATH entries using 240 bytes of memory
7 BGP community entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
90 BGP advertise-bit cache entries using 1784 bytes of memory
36 received paths for inbound soft reconfiguration
BGP using 34249 total bytes of memory
Dampening enabled. 4 history paths, 0 dampened paths
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.100.1.1      4   200      26      22      199    0    0 00:14:23 23
10.200.1.1      4   300      21      51      199    0    0 00:13:40 0
```

The table below describes the significant fields shown in the display. Fields that are preceded by the asterisk character (*) are not shown in the above output.

Table 35: show ip bgp summary Field Descriptions

Field	Description
BGP router identifier	In order of precedence and availability, the router identifier specified by the **bgp router-id** command, a loopback address, or the highest IP address.
BGP table version	Internal version number of BGP database.
main routing table version	Last version of BGP database that was injected into the main routing table.
...network entries	Number of unique prefix entries in the BGP database.
...using ... bytes of memory	Amount of memory, in bytes, that is consumed for the path, prefix, or attribute entry displayed on the same line.
...path entries using	Number of path entries in the BGP database. Only a single path entry will be installed for a given destination. If multipath routes are configured, a path entry will be installed for each multipath route.
...multipath network entries using	Number of multipath entries installed for a given destination.
* ...BGP path/bestpath attribute entries using	Number of unique BGP attribute combinations for which a path is selected as the bestpath.
* ...BGP rrinfo entries using	Number of unique ORIGINATOR and CLUSTER_LIST attribute combinations.
...BGP AS-PATH entries using	Number of unique AS_PATH entries.
...BGP community entries using	Number of unique BGP community attribute combinations.
*...BGP extended community entries using	Number of unique extended community attribute combinations.
BGP route-map cache entries using	Number of BGP route-map match and set clause combinations. A value of 0 indicates that the route cache is empty.
...BGP filter-list cache entries using	Number of filter-list entries that match an AS-path access list permit or deny statements. A value of 0 indicates that the filter-list cache is empty.

Field	Description
BGP advertise-bit cache entries using	(Cisco IOS Release 12.4(11)T and later releases only) Number of advertised bitfield entries and the associated memory usage. A bitfield entry represents a piece of information (one bit) that is generated when a prefix is advertised to a peer. The advertised bit cache is built dynamically when required.
...received paths for inbound soft reconfiguration	Number paths received and stored for inbound soft reconfiguration.
BGP using...	Total amount of memory, in bytes, used by the BGP process.
Dampening enabled...	Indicates that BGP dampening is enabled. The number of paths that carry an accumulated penalty and the number of dampened paths are displayed on this line.
BGP activity...	Displays the number of times that memory has been allocated or released for a path or prefix.
Neighbor	IP address of the neighbor.
V	BGP version number spoken to the neighbor.
AS	Autonomous system number.
MsgRcvd	Number of messages received from the neighbor.
MsgSent	Number of messages sent to the neighbor.
TblVer	Last version of the BGP database that was sent to the neighbor.
InQ	Number of messages queued to be processed from the neighbor.
OutQ	Number of messages queued to be sent to the neighbor.
Up/Down	The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.

Field	Description
State/PfxRcd	Current state of the BGP session, and the number of prefixes that have been 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 set to Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the **neighbor shutdown** command.

The following output from the **show ip bgp summary** command shows that the BGP neighbor 192.168.3.2 was dynamically created and is a member of the listen range group, group192. The output also shows that the IP prefix range of 192.168.0.0/16 is defined for the listen range group named group192. In Cisco IOS Release 12.2(33)SXH and later releases, the BGP dynamic neighbor feature introduced the ability to support the dynamic creation of BGP neighbor peers using a subnet range associated with a peer group (listen range group).

```
Router# show ip bgp summary

BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1
BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

The following output from the **show ip bgp summary** command shows two BGP neighbors, 192.168.1.2 and 192.168.3.2, in different 4-byte autonomous system numbers, 65536 and 65550. The local autonomous system 65538 is also a 4-byte autonomous system number and the numbers are displayed in the default asplain format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4       65536       7       7        1    0    0 00:03:04      0
192.168.3.2     4       65550       4       4        1    0    0 00:00:15      0
```

The following output from the **show ip bgp summary** command shows the same two BGP neighbors, but the 4-byte autonomous system numbers are displayed in asdot notation format. To change the display format the **bgp asnotation dot** command must be configured in router configuration mode. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, or Cisco IOS XE Release 2.3 or later releases.

```
Router# show ip bgp summary

BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4         1.0       9       9        1    0    0 00:04:13      0
192.168.3.2     4        1.14       6       6        1    0    0 00:01:24      0
```

The following example displays sample output of the **show ip bgp summary slow** command:

```
Router# show ip bgp summary slow

BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 37, main routing table version 37
36 network entries using 4608 bytes of memory
36 path entries using 1872 bytes of memory
1/1 BGP path/bestpath attribute entries using 124 bytes of memory
1 BGP rrinfo entries using 24 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6700 total bytes of memory
BGP activity 46/0 prefixes, 48/0 paths, scan interval 60 secs
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
6.6.6.6 4 100 11 10 1 0 0 00:44:20 0
```

The following example displays counts of prefix/AS pairs for each RPKI state. The fourth line of output indicates "Path RPKI states: x valid, x not found, x invalid." Of course the line of output indicating RPKI states can be displayed only if the **bgp rpki server** command or the **neighbor announce rpki state** command is configured.

```
Router> show ip bgp summary

For address family: IPv4 Unicast
BGP router identifier 10.0.96.2, local AS number 2
BGP table version is 8, main routing table version 8
Path RPKI states: 0 valid, 7 not found, 0 invalid
6 network entries using 888 bytes of memory
7 path entries using 448 bytes of memory
3/3 BGP path/bestpath attribute entries using 384 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1768 total bytes of memory
BGP activity 12/0 prefixes, 14/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State
/PfxRcd
10.0.0.3        4            3       6       9        8    0    0 00:01:04
  3
10.0.2.4        4            2       5       8        8    0    0 00:01:15
  0
10.0.3.5        4            4       6       7        8    0    0 00:01:14
  3
10.0.96.254     4            1       0       0        1    0    0 never    Idle

For address family: IPv6 Unicast
BGP router identifier 10.0.96.2, local AS number 2
BGP table version is 9, main routing table version 9
Path RPKI states: 3 valid, 4 not found, 0 invalid
6 network entries using 1032 bytes of memory
7 path entries using 616 bytes of memory
5/5 BGP path/bestpath attribute entries using 640 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2336 total bytes of memory
BGP activity 12/0 prefixes, 14/0 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State
/PfxRcd
2001::2         4            2       6       9        6    0    0 00:01:08
  2
2002::1         4            3       7      11        9    0    0 00:01:07
  2
2003::2         4            4       6       8        9    0    0 00:01:08
```

2

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
bgp router-id	Configures a fixed router ID for the local BGP routing process.
neighbor maximum-prefix	Controls how many prefixes can be received from a BGP neighbor.
neighbor shutdown	Disables a BGP neighbor or peer group.
neighbor slow-peer split-update-group dynamic	Causes a dynamically detected slow peer to be moved to a slow update group.
router bgp	Configures the BGP routing process.

show ip bgp template peer-policy

To display locally configured peer policy templates, use the **show ip bgp template peer-policy** command in user EXEC or privileged EXEC mode.

show ip bgp template peer-policy [*policy-template-name* **[detail]**]

Syntax Description

policy-template-name	(Optional) Name of a locally configured peer policy template.
detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs), and AS-path filter lists.

Command Default

If a peer policy template is not specified using the *policy-template-name* argument, all peer policy templates will be displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.0(25)S	The **detail** keyword was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(11)T	Support for the **detail** keyword was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command and support for the **detail** keyword were integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
12.2(33)SB	Support for the **detail** keyword was integrated into Cisco IOS Release 12.2(33)SB.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

This command is used to display locally configured peer policy templates. The output can be filtered to display a single peer policy template using the *policy-template-name* argument. This command also supports all standard output modifiers.

When BGP neighbors use multiple levels of peer templates it can be difficult to determine which policies are associated with a specific template. In Cisco IOS Release 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and later releases, the **detail** keyword was added to display the detailed configuration of local and inherited policies associated with a specific template. Inherited policies are policies that the template inherits from other peer-policy templates.

Examples

The **show ip bgp template peer-policy** command is used to verify the configuration of local peer policy templates. The following sample output shows the peer policy templates named GLOBAL and NETWORK1. The output also shows that the GLOBAL template was inherited by the NETWORK1 template.

```
Device# show ip bgp template peer-policy

Template:GLOBAL, index:1.
Local policies:0x80840, Inherited polices:0x0
 *Inherited by Template NETWORK1, index:2
Locally configured policies:
  prefix-list NO-MARKETING in
  weight 300
  maximum-prefix 10000
Inherited policies:
Template:NETWORK1, index:2.
Local policies:0x1, Inherited polices:0x80840
This template inherits:
  GLOBAL, index:1, seq_no:10, flags:0x1
Locally configured policies:
  route-map ROUTE in
Inherited policies:
  prefix-list NO-MARKETING in
  weight 300
  maximum-prefix 10000
```

The table below describes the significant fields shown in the display.

Table 36: show ip bgp template peer-policy Field Descriptions

Field	Description
Template	Name of the peer template.
index	The sequence number in which the displayed template is processed.
Local policies	Displays the hexadecimal value of locally configured policies.

Field	Description
Inherited polices	Displays the hexadecimal value of inherited policies. The 0x0 value is displayed when no templates are inherited.
Locally configured policies	Displays a list of commands that are locally configured in a peer policy template.
Inherited policies	Displays a list of commands that are inherited from a peer template.

The following sample output of the **show ip bgp template peer-policy** command with the **detail** keyword displays details of the template named NETWORK1, which includes the inherited template named GLOBAL. The output in this example displays the configuration commands of the locally configured route map and prefix list and the inherited prefix list.

```
Device# show ip bgp template peer-policy NETWORK1 detail

Template:NETWORK1, index:2.
Local policies:0x1, Inherited polices:0x80840
This template inherits:
  GLOBAL, index:1, seq_no:10, flags:0x1
Locally configured policies:
  route-map ROUTE in
Inherited policies:
  prefix-list NO-MARKETING in
  weight 300
  maximum-prefix 10000
Template:NETWORK1 <detail>
Locally configured policies:
  route-map ROUTE in
route-map ROUTE, permit, sequence 10
  Match clauses:
    ip address prefix-lists: DEFAULT
ip prefix-list DEFAULT: 1 entries
   seq 5 permit 10.1.1.0/24
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
Inherited policies:
  prefix-list NO-MARKETING in
ip prefix-list NO-MARKETING: 1 entries
   seq 5 deny 10.2.2.0/24
```

Related Commands

Command	Description
inherit peer-policy	Configures a peer policy template to inherit the configuration from another peer policy template.
template peer-policy	Creates a peer policy template and enters policy-template configuration mode.

show ip bgp template peer-session

To display peer policy template configurations, use the **show ip bgp template peer-session** command in user EXEC or privileged EXEC mode.

show ip bgp template peer-session [*session-template-name*]

Syntax Description

session-template-name	(Optional) Name of a locally configured peer session template.

Command Default

If a peer session template is not specified with the *session-template-name* argument, all peer session templates will be displayed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.8S	This command was modified. The cluster ID for the template is displayed.

Usage Guidelines

This command is used to display locally configured peer session templates. The output can be filtered to display a single peer session template with the *peer-session-name* argument. This command also supports all standard output modifiers.

Examples

The **show ip bgp template peer-session** command is used to verify the configuration of local peer session templates. The following example shows the peer session templates named INTERNAL-BGP and CORE1. The output also shows that INTERNAL-BGP is inherited by CORE1.

```
Device# show ip bgp template peer-session

Template:INTERNAL-BGP, index:1
Local policies:0x21, Inherited policies:0x0
 *Inherited by Template CORE1, index= 2
Locally configured session commands:
 remote-as 202
 timers 30 300
Inherited session commands:
Template:CORE1, index:2
Local policies:0x180, Inherited policies:0x21
This template inherits:
  INTERNAL-BGP index:1 flags:0x0
Locally configured session commands:
 update-source loopback 1
 description CORE-123
Inherited session commands:
 remote-as 202
 timers 30 300
```

The table below describes the significant fields shown in the display.

Table 37: show ip bgp template peer-session Field Descriptions

Field	Description
Template:	Name of the peer template.
index:	The sequence number in which the displayed template is processed.
Local policies:	Displays the hexadecimal value of locally configured policies.
Inherited policies:	Displays the hexadecimal value of inherited policies. The 0x0 value is displayed when no templates are inherited.
Locally configured session commands:	Displays a list of commands that are locally configured in a peer template.
Inherited session commands:	Displays a list of commands that are inherited from a peer session template.

The following sample output displays the cluster ID assigned to the template:

```
Device# show ip bgp template peer-session TS1

Template:TS1, index:1
Local policies:0x10000000, Inherited policies:0x0
Locally configured session commands:
```

```
 cluster-id 192.168.0.115
Inherited session commands:
```

Related Commands

Command	Description
bgp cluster-id	Sets the global cluster ID on a route reflector.
inherit peer-session	Configures a peer session template to inherit the configuration from another peer session template.
neighbor cluster-id	Sets the cluster ID for a neighbor.
template peer-session	Creates a peer session template and enters session-template configuration mode.

show ip bgp unicast route-server

To display on a BGP route server which paths are chosen for a route server context, in particular if the normal bestpath was overridden or suppressed, use the **show ip bgp unicast route-server** command in privileged EXEC mode.

show ip bgp {**ipv4**| **ipv6**} **unicast route-server** {**all**| **context** *context-name*} **[summary]**

Syntax Description

ipv4	Displays only IPv4 prefixes.
ipv6	Displays only IPv6 prefixes.
all	Displays information for all route server contexts.
context *context-name*	Displays information for the specified route server context only.
summary	(Optional) Displays the neighbor state for route server clients.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.3S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Use this command on a BGP route server to see the next hop to network prefixes and additional information about the path.

Examples

The following output displays all the routes chosen by the policy for the context named example-context:

```
Route-Server# show ip bgp ipv4 unicast route-server context example-context

Networks for route server context example-context:
   Network          Next Hop            Metric LocPrf Weight Path
*  1.1.1.1/32       10.10.10.22            123             0 22 ?
*  1.1.2.0/24       10.10.10.22            123             0 22 ?
*  1.3.0.0/16       10.10.10.22            123             0 22 ?
*  8.8.0.0/16       10.10.10.22            123             0 22 ?
   100.100.100.21/32 (suppressed)
*> 100.100.100.22/32 10.10.10.22            123             0 22 ?
*  100.100.100.23/32 10.10.10.23            123             0 23 ?
```

```
*> 100.100.100.24/32 10.10.10.24            123             0 24 ?
*> 100.100.100.25/32 10.10.10.25            123             0 25 ?
*> 100.100.100.26/32 10.10.10.26            123             0 26 ?
```

Three types of routes can be in a context, as shown in the preceding output. They are:

- Those where the policy for the context chooses the same path as the regular BGP best path algorithm (for example, 100.100.100.25/32, denoted by ">").
- Those where the policy for the context excluded the regular best path, but found a suitable alternative path to advertise to the client (for example, 1.1.1.1/32, not denoted with ">", but still valid "*").
- Those where the policy for the context excluded all available paths and therefore those routes will not be sent to the client; for example, 100.100.100.21/32, denoted by "(suppressed)".

In the following example, specifying **all** instead of a specific context reveals that different contexts may have differing routes due to the configured policy:

```
Route-Server# show ip bgp ipv4 unicast route-server all

Networks for route server context all-base:
   Network          Next Hop            Metric LocPrf Weight Path
*> 1.1.1.1/32       10.10.10.21             23             0 21 ?
*> 1.1.2.0/24       10.10.10.21             23             0 21 ?
*> 1.3.0.0/16       10.10.10.21             23             0 21 ?
*> 8.8.0.0/16       10.10.10.21             23             0 21 ?
*> 100.100.100.21/32 10.10.10.21            23             0 21 ?
*> 100.100.100.22/32 10.10.10.22           123             0 22 ?
*> 100.100.100.23/32 10.10.10.21            23             0 21 ?
*  100.100.100.24/32 10.10.10.24           123             0 24 ?
*> 100.100.100.25/32 10.10.10.25           123             0 25 ?
*> 100.100.100.26/32 10.10.10.26           123             0 26 ?
Networks for route server context all-policy-deny:
   Network          Next Hop            Metric LocPrf Weight Path
   1.1.1.1/32       (suppressed)
   1.1.2.0/24       (suppressed)
   1.3.0.0/16       (suppressed)
   8.8.0.0/16       (suppressed)
   100.100.100.21/32 (suppressed)
   100.100.100.22/32 (suppressed)
   100.100.100.23/32 (suppressed)
   100.100.100.24/32 (suppressed)
   100.100.100.25/32 (suppressed)
   100.100.100.26/32 (suppressed)
Networks for route server context all-policy:
   Network          Next Hop            Metric LocPrf Weight Path
*  1.1.1.1/32       10.10.10.27             878             0 27 ?
*  1.1.2.0/24       10.10.10.27             878             0 27 ?
*  1.3.0.0/16       10.10.10.27             878             0 27 ?
*  8.8.0.0/16       10.10.10.27             878             0 27 ?
*  100.100.100.21/32 10.10.10.27            878             0 27 ?
*  100.100.100.22/32 10.10.10.27            878             0 27 ?
*  100.100.100.23/32 10.10.10.27            878             0 27 ?
*  100.100.100.24/32 10.10.10.27            878             0 27 ?
*  100.100.100.25/32 10.10.10.27            878             0 27 ?
*  100.100.100.26/32 10.10.10.27            878             0 27 ?
Networks for route server context example-context:
   Network          Next Hop            Metric LocPrf Weight Path
*  1.1.1.1/32       10.10.10.23             123             0 23 ?
*  1.1.2.0/24       10.10.10.23             123             0 23 ?
*  1.3.0.0/16       10.10.10.23             123             0 23 ?
*  8.8.0.0/16       10.10.10.23             123             0 23 ?
   100.100.100.21/32 (suppressed)
*> 100.100.100.22/32 10.10.10.22           123             0 22 ?
*  100.100.100.23/32 10.10.10.23           123             0 23 ?
*  100.100.100.24/32 10.10.10.24           123             0 24 ?
*> 100.100.100.25/32 10.10.10.25           123             0 25 ?
*> 100.100.100.26/32 10.10.10.26           123             0 26 ?
```

In the following example, the **summary** keyword displays output similar to the **show ip bgp summary** command in that it shows the neighbor state for route server clients in the specified context (or all contexts):

```
Route-Server# show ip bgp ipv4 unicast route-server context example-context summary

Route server clients assigned to context example-context:
Neighbor     V   AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.18  4   18     283     291       13    0    0 04:13:21        0
```

In the following example, the **all**keyword and the **summary** keyword display summary output for all contexts:

```
Route-Server# show ip bgp ipv4 unicast route-server all summary

Route server clients without assigned contexts:
Neighbor     V   AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.12  4   12      12      17       12    0    0 00:08:29        0
Route server clients assigned to context all-base:
Neighbor     V   AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.14  4   14      12      17       12    0    0 00:08:25        0
Route server clients assigned to context all-policy-deny:
Neighbor     V   AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.16  4   16      12      13       12    0    0 00:08:24        0
Route server clients assigned to context all-policy:
Neighbor     V   AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.13  4   13      11      14       12    0    0 00:08:22        0
Route server clients assigned to context example-context:
Neighbor     V   AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.18  4   18      12      17       12    0    0 00:08:30        0
```

Related Commands

Command	Description
neighbor route-server-client	Specifies on a BGP route server that a neighbor is a route server client.

show ip bgp update-group

To display information about the Border Gateway Protocol (BGP) update groups, use the **show ip bgp update-group** command in user EXEC or privileged EXEC mode.

show ip bgp update-group [*index-group*| *ip-address*| *ipv6-address*] **[summary]**

Syntax Description

index-group	(Optional) Update group type with its corresponding index number. The range of update-group index numbers is from 1 to 4294967295.
ip-address	(Optional) IP address of a single neighbor that is a member of an update group.
ipv6-address	(Optional) IPv6 address of a single neighbor that is member of an update group.
summary	(Optional) Displays a summary of update-group member information. The output can be filtered to show information for a single index group or peer with the *index-group*, *ip-address*, or *ipv6-address* argument.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S. The *ipv6-address* argument was added.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.8S	This command was modified. The cluster ID for the update group is displayed.

Usage Guidelines

Use this command to display information about BGP update groups. When a change to BGP outbound policy occurs, the router automatically recalculates update group memberships and applies the changes by triggering an outbound soft reset after a 1-minute timer expires. This behavior is designed to provide the network operator with time to change the configuration if a mistake is made. You can manually enable an outbound soft reset before the timer expires by entering the **clear ip bgp** *ip-address* **soft out** command.

Note In Cisco IOS Release 12.0(25)S, 12.3(2)T, and earlier releases, the update group recalculation delay timer is set to 3 minutes.

Neighbors with different cluster IDs are assigned to different update groups.

Examples

The following sample output from the **show ip bgp update-group** command shows update group information for all neighbors:

```
Device# show ip bgp update-group

BGP version 4 update-group 1, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Route map for outgoing advertisements is COST1
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 1 member:
  10.4.9.21
BGP version 4 update-group 2, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 2 members:
  10.4.9.5 10.4.9.8
```

The table below describes the significant fields shown in the display.

Table 38: show ip bgp update-group Field Descriptions

Field	Description
BGP version	BGP version.
update-group	Update-group number and type (internal or external).
Update messages formatted 0, replicated 0	Number of update messages that have been formatted and replicated.
Number of NLRIs...	NLRI sent in an update.
Minimum time between advertisement runs	Minimum time, in seconds, between update advertisements.
Has 2 members	Number of members listed by IP address in the update group.

The following sample output from the **show ip bgp update-group** command shows a summary of update-group information for the 10.4.9.8 neighbor:

```
Device# show ip bgp update-group 10.4.9.8 summary

Summary for Update-group 2 :
-----------------------------
BGP router identifier 10.4.9.4, local AS number 101
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.4.9.5        4   101      35      35        1    0    0 00:26:22        0
10.4.9.8        4   101      39      39        1    0    0 00:26:21        0
```

The table below describes the significant fields shown in the display.

Table 39: show ip bgp update-group summary Field Descriptions

Field	Description
Summary for Update-group 2	Update-group number.
BGP router identifier 10.4.9.4	IP address and AS number for the specified peer.
BGP table version...	Displays incremental changes in the BGP routing table.
Neighbor...	Specific peer information and statistics, including IP address and AS number.

The following sample output displays the cluster ID assigned to the update group:

```
Device# show ip bgp update-group 1.1.1.1

BGP version 4 update-group 60, internal, Address Family: IPv4 Unicast
  BGP Update version : 391/0, messages 0
  Route-Reflector Client
  Configured with the cluster-id 4.0.0.115
  Topology: global, highest version: 391, tail marker: 391
  Format state: Current working (OK, last not in list)
                Refresh blocked (not in list, last not in list)
  Update messages formatted 0, replicated 0, current 0, refresh 0, limit 1000
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 0 seconds
  Has 1 member:
   1.1.1.1
```

Related Commands

Command	Description
bgp cluster-id	Sets the global cluster ID on a route reflector.
clear ip bgp	Resets a BGP connection or session.
clear ip bgp update-group	Clears BGP update-group member sessions.

Command	Description
debug ip bgp groups	Displays information related to the processing of BGP update groups.
neighbor cluster-id	Sets the cluster ID for a neighbor.
show ip bgp replication	Displays BGP update-group replication statistics.

show ip bgp vpnv4

To display VPN Version 4 (VPNv4) address information from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4** command in user EXEC or privileged EXEC mode.

show ip bgp vpnv4 {**all**| **rd** *route-distinguisher*| **vrf** *vrf-name*} [[*ip-prefix*/*length* [*mask*| **bestpath**| **multipaths**]| *network-address* [*mask*| **bestpath**| **longer-prefixes**| **multipaths**| **shorter-prefixes**| **subnets**]]| **cidr-only**| **cluster-ids**| **community**| **community-list**| **dampening**| **extcommunity-list** *extcommunity-list-name*| **filter-list**| **inconsistency nexthop-label**| **inconsistent-as**| **labels**| **neighbors** [{*ip-address*| *ipv6-address*} [**advertised-routes**| **dampened-routes**| **flap-statistics**| **paths**| **policy [detail]**| **received**| **received-routes**| **routes**]| **slow**]| **nexthops**| **oer-paths**| **path-attribute** {**discard**| **unknown**}| **paths** [*line*]| **peer-group**| **pending-prefixes**| **prefix-list** *prefix-list-name*| **quote-regexp**| **regexp**| **replication** [*update-group-index*] [*update-group-member-address*]| **rib-failure**| **route-map** *route-map-name*| **summary**| **update-group**| **update-source**| **version** {*version-number*| **recent** *offset-value*}]

Syntax Description

all	Displays the complete VPNv4 database.
rd *route-distinguisher*	Displays Network Layer Reachability Information (NLRI) prefixes that match the named route distinguisher.
vrf *vrf-name*	Displays NLRI prefixes associated with the named VPN routing and forwarding (VRF) instance.
ip-prefix/*length*	(Optional) IP prefix address (in dotted decimal format) and the length of the mask (0 to 32). The slash mark must be included.
longer-prefixes	(Optional) Displays the entry, if any, that exactly matches the specified prefix parameter and all entries that match the prefix in a “longest-match” sense. That is, prefixes for which the specified prefix is an initial substring.
network-address	(Optional) IP address of a network in the BGP routing table.
mask	(Optional) Mask of the network address, in dotted decimal format.
cidr-only	(Optional) Displays only routes that have nonclassful netmasks.
cluster-ids	(Optional) Displays configured cluster IDs.
community	(Optional) Displays routes that match this community.

community-list	(Optional) Displays routes that match this community list.
dampening	(Optional) Displays paths suppressed because of dampening (BGP route from peer is up and down).
extcommunity-list *extended-community-list-name*	(Optional) Displays routes that match the extended community list.
filter-list	(Optional) Displays routes that conform to the filter list.
inconsistency nexthop-label	(Optional) Displays all inconsistent paths.
inconsistent-as	(Optional) Displays only routes that have inconsistent autonomous systems of origin.
labels	(Optional) Displays incoming and outgoing BGP labels for each NLRI prefix.
neighbors	(Optional) Displays details about TCP and BGP neighbor connections.
ip-address	(Optional) Displays information about the neighbor at this IPv4 address.
ipv6-address	(Optional) Displays information about the neighbor at this IPv6 address.
advertised-routes	(Optional) Displays advertised routes from the specified neighbor.
dampened-routes	(Optional) Displays dampened routes from the specified neighbor.
flap-statistics	(Optional) Displays flap statistics about the specified neighbor.
paths	(Optional) Displays path information.
line	(Optional) A regular expression to match the BGP autonomous system paths.
policy [detail]	(Optional) Displays configured policies for the specified neighbor.
slow	(Optional) Displays BGP slow peer information.
nexthops	(Optional) Displays nexthop address table.

oer-paths	(Optional) Displays all OER-controlled paths.
path-attribute	(Optional) Displays path-attribute-specific information.
discard	(Optional) Displays prefixes with discarded path attribute.
unknown	(Optional) Displays prefixes with unknown path attribute.
paths	(Optional) Displays path information.
line	(Optional) A regular expression to match the BGP autonomous system paths.
peer-group	(Optional) Displays information about peer groups.
pending-prefixes	(Optional) Displays prefixes that are pending deletion.
prefix-list *prefix-list*	(Optional) Displays routes that match the prefix list.
quote-regexp	(Optional) Displays routes that match the autonomous system path regular expression.
regexp	(Optional) Displays routes that match the autonomous system path regular expression.
replication	(Optional) Displays replication status of update group(s).
rib-failure	(Optional) Displays BGP routes that failed to install in the VRF table.
route-map	(Optional) Displays routes that match the route map.
summary	(Optional) Displays BGP neighbor status.
update-group	(Optional) Displays information on update groups.
update-source	(Optional) Displays update source interface table.
version	(Optional) Displays prefixes with matching version numbers.
version-number	(Optional) If the **version** keyword is specified, either a *version-number* or the **recent** keyword and an *offset-value* are required.

recent *offset-value*	(Optional) Displays prefixes with matching version numbers.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	This command was modified. The output of the **show ip bgp vpnv4 all** *ip-prefix* command was enhanced to display attributes including multipaths and a best path to the specified network.
12.0(21)ST	This command was modified. The **tags** keyword was replaced by the **labels** keyword to conform to the MPLS guidelines.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(27)S	This command was modified. The output of the **show ip bgp vpnv4 all labels** command was enhanced to display explicit-null label information.
12.3	This command was modified. The **rib-failure** keyword was added for VRFs.
12.2(22)S	This command was modified. The output of the **show ip bgp vpnv4 vrf** *vrf-name* **labels** command was modified so that directly connected VRF networks no longer display as aggregate; no label appears instead.
12.2(25)S	This command was updated to display MPLS VPN nonstop forwarding information.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router. The display output was modified to indicate whether BGP nonstop routing (NSR) with stateful switchover (SSO) is enabled and the reason the last BGP lost SSO capability.
12.2(33)SRA	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID.
12.2(31)SB2	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID.

Release	Modification
12.2(33)SXH	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID. **Note** In Cisco IOS Release 12.2(33)SXH, the command output does not display on the standby Route Processor in NSF/SSO mode.
12.4(20)T	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID.
15.0(1)M	This command was modified. The output was modified to support the BGP Event-Based VPN Import feature.
12.2(33)SRE	This command was modified. The command output was modified to support the BGP Event-Based VPN Import, BGP best external, and BGP additional path features.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was implemented on the Cisco 7200 series router and the output was modified to display unknown attributes and discarded attributes associated with a prefix.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router and the output modified to display unknown attributes and discarded attributes associated with a prefix.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to display VPNv4 information from the BGP database. The **show ip bgp vpnv4 all** command displays all available VPNv4 information. The **show ip bgp vpnv4 all summary** command displays BGP neighbor status. The **show ip bgp vpnv4 all labels** command displays explicit-null label information.

Examples

The following example shows all available VPNv4 information in a BGP routing table:

```
Router# show ip bgp vpnv4 all

BGP table version is 18, local router ID is 10.14.14.14
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
```

```
Route Distinguisher: 1:101 (default for vrf vpn1)
*>i10.6.6.6/32       10.0.0.21              11    100      0 ?
*> 10.7.7.7/32       10.150.0.2             11         32768 ?
*>i10.69.0.0/30      10.0.0.21               0    100      0 ?
*> 10.150.0.0/24     0.0.0.0                 0         32768 ?
```

The table below describes the significant fields shown in the display.

Table 40: show ip bgp vpnv4 all Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows how to display a table of labels for NLRI prefixes that have a route distinguisher value of 100:1.

```
Router# show ip bgp vpnv4 rd 100:1 labels

Network            Next Hop       In label/Out label
Route Distinguisher: 100:1 (vrf1)
   10.0.0.0         10.20.0.60      34/nolabel
   10.0.0.0         10.20.0.60      35/nolabel
   10.0.0.0         10.20.0.60      26/nolabel
                    10.20.0.60      26/nolabel
   10.0.0.0         10.15.0.15      nolabel/26
```

The table below describes the significant fields shown in the display.

Table 41: show ip bgp vpnv4 rd labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Specifies the BGP next hop address.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next-hop router.

The following example shows VPNv4 routing entries for the VRF named vpn1:

```
Router# show ip bgp vpnv4 vrf vpn1

BGP table version is 18, local router ID is 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf test1)
*> 10.1.1.1/32      192.168.1.1              0             0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 10.2.2.2/32      192.168.1.1                           0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 172.16.1.0/24    192.168.1.1              0             0 100 i
* i                 10.4.4.4                 0    100      0 100 i
r> 192.168.1.0      192.168.1.1              0             0 100 i
rbi                 10.4.4.4                 0    100      0 100 i
*> 192.168.3.0      192.168.1.1                           0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
```

The table below describes the significant fields shown in the display.

Table 42: show ip bgp vpnv4 vrf Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows attributes for network 192.168.9.0 that include multipaths, best path, and a recursive-via-host flag:

```
Router# show ip bgp vpnv4 vrf vpn1 192.168.9.0 255.255.255.0

BGP routing table entry for 100:1:192.168.9.0/24, version 44
Paths: (2 available, best #2, table test1)
  Additional-path
  Advertised to update-groups:
     2
  100, imported path from 400:1:192.168.9.0/24
    10.8.8.8 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.8.8.8, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out nolabel/17
  100, imported path from 300:1:192.168.9.0/24
    10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
```

```
mpls labels in/out nolabel/17
```

The table below describes the significant fields shown in the display.

Table 43: show ip bgp vpnv4 all network-address Field Descriptions

Field	Description
BGP routing table entry for ... version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	Number of autonomous system paths to the specified network. If multiple paths exist, one of the multipaths is designated the best path.
Multipath	Indicates the maximum paths configured (iBGP or eBGP).
Advertised to non peer-group peers	IP address of the BGP peers to which the specified route is advertised.
10.22.7.8 (metric 11) from 10.11.3.4 (10.0.0.8)	Indicates the next hop address and the address of the gateway that sent the update.
Origin	Indicates the origin of the entry. It can be one of the following values: • IGP—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • incomplete—Entry originated from other than an IGP or Exterior Gateway Protocol (EGP) and was advertised with the **redistribute** router configuration command. • EGP—Entry originated from an EGP.
metric	If shown, the value of the interautonomous system metric.
localpref	Local preference value as set with the **set local-preference route-map** configuration command. The default value is 100.
valid	Indicates that the route is usable and has a valid set of attributes.
internal/external	The field is internal if the path is learned via iBGP. The field is external if the path is learned via eBGP.
multipath	One of multiple paths to the specified network.

Field	Description
best	If multiple paths exist, one of the multipaths is designated the best path and this path is advertised to neighbors.
Extended Community	Route Target value associated with the specified route.
Originator	The router ID of the router from which the route originated when route reflector is used.
Cluster list	The router ID of all the route reflectors that the specified route has passed through.

The following example shows routes that BGP could not install in the VRF table:

```
Router# show ip bgp vpnv4 vrf xyz rib-failure

Network            Next Hop                      RIB-failure   RIB-NH Matches
Route Distinguisher: 2:2 (default for vrf bar)
10.1.1.2/32        10.100.100.100      Higher admin distance              No
10.111.111.112/32  10.9.9.9            Higher admin distance             Yes
```

The table below describes the significant fields shown in the display.

Table 44: show ip bgp vpnv4 vrf rib-failure Field Descriptions

Field	Description
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.
RIB-failure	Cause of the Routing Information Base (RIB) failure. Higher admin distance means that a route with a better (lower) administrative distance, such as a static route, already exists in the IP routing table.

Field	Description
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and the **bgp suppress-inactive** command is configured for the address family being used. There are three choices: • Yes—Means that the route in the RIB has the same next hop as the BGP route or that the next hop recurses down to the same adjacency as the BGP next hop. • No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route. • n/a—Means that the **bgp suppress-inactive** command is not configured for the address family being used.

The following example shows the information displayed on the active and standby Route Processors when they are configured for NSF/SSO: MPLS VPN.

Note In Cisco IOS Release 12.2(33)SXH, the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature incurred various infrastructure changes. The result of those changes affects the output of this command on the standby Route Processor (RP). In Cisco IOS Release 12.2(33)SXH, the standby RP does not display any output from the **show ip bgp vpnv4** command.

```
Router# show ip bgp vpnv4 all labels

Network          Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0    16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0    17/aggregate(vpn1)
Route Distinguisher: 609:1 (vpn0)
10.13.13.13/32   0.0.0.0    18/aggregate(vpn0)

Router# show ip bgp vpnv4 vrf vpn1 labels

Network          Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0    16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0    17/aggregate(vpn1)


Router# show ip bgp vpnv4 all labels

Network       Masklen   In label
Route Distinguisher: 100:1
10.12.12.12   /32       16
10.0.0.0      /8        17
Route Distinguisher: 609:1
10.13.13.13   /32       18

Router# show ip bgp vpnv4 vrf vpn1 labels
```

```
Network        Masklen   In label
Route Distinguisher: 100:1
10.12.12.12    /32       16
10.0.0.0       /8        17
```

The table below describes the significant fields shown in the display.

Table 45: show ip bgp vpnv4 labels Field Descriptions

Field	Description
Network	The network address from the BGP table.
Next Hop	The BGP next-hop address.
In label	The label (if any) assigned by this router.
Out label	The label assigned by the BGP next-hop router.
Masklen	The mask length of the network address.

The following example displays output, including the explicit-null label, from the **show ip bgp vpnv4 all labels** command on a CSC-PE router:

```
Router# show ip bgp vpnv4 all labels

   Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   10.0.0.0/24       10.0.0.0        19/aggregate(v1)
   10.0.0.1/32       10.0.0.0        20/nolabel
   10.1.1.1/32       10.0.0.0        21/aggregate(v1)
   10.10.10.10/32    10.0.0.1        25/exp-null

   10.168.100.100/32
                     10.0.0.1        23/exp-null
   10.168.101.101/32
                     10.0.0.1        22/exp-null
```

The table below describes the significant fields shown in the display.

Table 46: show ip bgp vpnv4 all labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next-hop router.
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.

The following example displays separate router IDs for each VRF in the output from an image in Cisco IOS Release 12.2(31)SB2, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, Cisco IOS XE Release 2.1, and later releases with the Per-VRF Assignment of BGP Router ID feature configured. The router ID is shown next to the VRF name.

```
Router# show ip bgp vpnv4 all

BGP table version is 5, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vrf_trans) VRF Router ID 10.99.1.2
*> 192.168.4.0      0.0.0.0                  0         32768 ?
Route Distinguisher: 42:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
*> 192.168.5.0      0.0.0.0                  0         32768 ?
```

The table below describes the significant fields shown in the display.

Table 47: show ip bgp vpnv4 all (VRF Router ID) Field Descriptions

Field	Description
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.
vrf	Name of the VRF.
VRF Router ID	Router ID for the VRF.

In the following example, the BGP Event-Based VPN Import feature is configured in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases. When the **import path selection** command is configured, but the **strict** keyword is not included, then a safe import path selection policy is in effect. When a path is imported as the best available path (when the best path or multipaths are not eligible for import), the imported path includes the wording “imported safety path,” as shown in the output.

```
Router# show ip bgp vpnv4 all 172.17.0.0

BGP routing table entry for 45000:1:172.17.0.0/16, version 10
Paths: (1 available, best #1, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2, imported safety path from 50000:2:172.17.0.0/16
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 200, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
```

In the following example, BGP Event-Based VPN Import feature configuration information is shown for Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases. When the **import path selection** command is configured with the **all** keyword, any path that matches an RD of the specified VRF will be imported, even though the path does not match the Route Targets (RT) imported by the specified VRF. In this situation, the imported path is marked as “not-in-vrf” as shown in the output. Note that on the net for vrf-A, this path is not the best path because any paths that are not in the VRFs appear less attractive than paths in the VRF.

```
Router# show ip bgp vpnv4 all 172.17.0.0
```

```
BBGP routing table entry for 45000:1:172.17.0.0/16, version 11
Paths: (2 available, best #2, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2
     10.0.101.2 from 10.0.101.2 (10.0.101.2)
       Origin IGP, metric 100, localpref 100, valid, internal, not-in-vrf
       Extended Community: RT:45000:200
       mpls labels in/out nolabel/16
   2
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 50, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
mpls labels in/out nolabel/16
```

In the following example, the unknown attributes and discarded attributes associated with the prefix are displayed.

```
Device# show ip bgp vpnv4 all 10.0.0.0/8

BGP routing table entry for 100:200:10.0.0.0/8, version 0
Paths: (1 available, no best path)
  Not advertised to any peer
  Refresh Epoch 1
  Local
    10.0.103.1 from 10.0.103.1 (10.0.103.1)
      Origin IGP, localpref 100, valid, internal
      Extended Community: RT:1:100
      Connector Attribute: count=1
       type 1 len 12 value 22:22:10.0.101.22
      mpls labels in/out nolabel/16
      unknown transitive attribute: flag E0 type 129 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      unknown transitive attribute: flag E0 type 140 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      unknown transitive attribute: flag E0 type 120 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      discarded unknown attribute: flag C0 type 128 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
```

The following example is based on the BGP—VPN Distinguisher Attribute feature. The output displays an Extended Community attribute, which is the VPN distinguisher (VD) of 104:1.

```
Device# show ip bgp vpnv4 unicast all 1.4.1.0/24

BGP routing table entry for 104:1:1.4.1.0/24, version 28
Paths: (1 available, best #1, no table)
   Advertised to update-groups:
      1
   Refresh Epoch 1
   1001
     19.0.101.1 from 19.0.101.1 (19.0.101.1)
       Origin IGP, localpref 100, valid, external, best
       Extended Community: VD:104:1
       mpls labels in/out nolabel/16
       rx pathid: 0, tx pathid: 0x0
```

The following example includes “allow-policy” in the output, indicating that the BGP—Support for iBGP Local-AS feature was configured for the specified neighbor by configuring the **neighbor allow-policy** command.

```
Device# show ip bgp vpnv4 all neighbors 192.168.3.3 policy
```

```
Neighbor: 192.168.3.3, Address-Family: VPNv4 Unicast
Locally configured policies:
 route-map pe33 out
 route-reflector-client
 allow-policy
 send-community both
```

Related Commands

Command	Description
import path limit	Specifies the maximum number of BGP paths, per VRF importing net, that can be imported from an exporting net.
import path selection	Specifies the BGP import path selection policy for a specific VRF instance.
neighbor allow-policy	Allows iBGP policies to be configured for the specified neighbor.
set extcommunity vpn-distinguisher	Sets a VPN distinguisher attribute to routes that pass a route map.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show ip bgp vpnv4 all dampening

To display BGP dampening information for the Virtual Private Network Version 4 (VPNv4) address family, use the **show ip bgp vpnv4 all dampening** command in user EXEC or privileged EXEC mode.

show ip bgp vpnv4 all dampening {**dampened-paths** | **flap-statistics** [*network-address* [*mask* | **bestpath** | **multipaths**] | *ip-prefix* / *length*| **cidr-only** | **filter-list** *filter-list*| **oer-paths**| **prefix-list** *prefix-list*| **quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *map-name*| **version** {*number* | **recent** }] | **parameters**}

Syntax Description

dampened-paths	Display routes suppressed due to dampening.
flap-statistics	Displays flap statistics of routes.
network-address	(Optional) Used with the **flap-statistics** keyword, network in the BGP routing table to display.
mask	(Optional) Used with the *network-address* argument, network mask that determines the networks displayed.
bestpath	(Optional) Used with the *network-address* argument, displays the bestpath for this prefix.
multipaths	(Optional) Used with the *network-address* argument, displays the multipaths for this prefix.
ip-prefix/*length*	(Optional) Used with the **flap-statistics** keyword, IP prefix/network length, such as 10.0.0.0/8.
cidr-only	(Optional) Used with the **flap-statistics** keyword, displays only routes with non-natural netmasks.
filter-list *filter-list*	(Optional) Used with the **flap-statistics** keyword, displays routes that conform to the specified filter list in the range 1-500.
oer-paths	(Optional) Used with the **flap-statistics** keyword, displays all OER controlled paths.
prefix-list *prefix-list*	(Optional) Used with the **flap-statistics** keyword, displays routes allowed by the prefix list.
quote-regexp *regexp*	(Optional) Used with the **flap-statistics** keyword, displays routes matching the AS path “regular expression”.
regexp *regexp*	(Optional) Used with the **flap-statistics** keyword, displays routes matching the AS path regular expression.

route-map *map-name*	(Optional) Used with the **flap-statistics** keyword, displays routes allowed by the route map.
version *number*	(Optional) Used with the **flap-statistics** keyword, displays version of BGP table.
recent	(Optional) Used with the **flap-statistics** keyword, displays recent version of BGP table.
parameters	Display details of configured dampening parameters.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use this command to display dampening information for the VPNv4 address family.

Examples

The following example shows dampening flap-statistics for the VPNv4 address family:

```
Router# show ip bgp vpnv4 all dampening flap-statistics

For_address_family: VPNv4 Unicast
% dampening not enabled for base
For vrf: Cust_A
BGP table version is 15, local router ID is 144.124.23.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          From            Flaps Duration Reuse    Path
*>  20.20.20.20/32   172.16.1.2      1     00:01:05          65001
For vrf: Cust_B
*d  11.11.11.11/32   192.168.1.2     3     00:04:22 00:04:49 65001

Router#
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes BGP route dampening parameters.

show ip bgp vpnv4 all sso summary

To display information about Border Gateway Protocol (BGP) peers that support BGP nonstop routing (NSR) with stateful switchover (SSO), use the **show ip bgp vpn4 sso summary** command in privileged EXEC mode.

show ip bgp vpnv4 all sso summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE 3.7S	This command was implemented on the Cisco ASR 903 router.

Usage Guidelines

The **show ip bgp vpnv4 all sso summary** command is used to display the number of BGP neighbors that are in SSO mode.

Examples

The following is sample output from the **show ip bgp vpnv4 all sso summary** command:

```
Router# show ip bgp vpnv4 all sso summary

   Stateful switchover support enabled for 40 neighbors
```

The table below describes the fields shown in the display.

Table 48: show ip bgp vpnv4 all sso summary Field Descriptions

Field	Description
Stateful Switchover support enabled for	Indicates the number of BGP neighbors that are in SSO mode.

Related Commands

Command	Description
neighbor ha-mode sso	Configures a BGP neighbor to support SSO.

show ip bgp vpnv6 unicast all dampening

To display BGP dampening information for the Virtual Private Network Version 6 (VPNv6) address family, use the **show ip bgp vpnv6 unicast all dampening**command in user EXEC or privileged EXEC mode.

show ip bgp vpnv6 unicast all dampening {**dampened-paths**| **flap-statistics**[*network* / *length* | **filter-list** *filter-list*| **injected-paths**| **prefix-list** *prefix-list*| **quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *map-name*] | **parameters**}

Syntax Description

dampened-paths	Display routes suppressed due to dampening.
flap-statistics	Displays flap statistics of routes.
network / *length*	(Optional) Used with the **flap-statistics** keyword, IPv6 prefix network/length in the format *X:X:X:X::X* / *<0-128>*.
filter-list *filter-list*	(Optional) Used with the **flap-statistics** keyword, displays routes that conform to the specified filter list in the range 1-500.
injected-paths	(Optional) Used with the **flap-statistics** keyword, displays all injected paths.
prefix-list *list*	(Optional) Used with the **flap-statistics** keyword, displays routes allowed by the prefix list.
quote-regexp *regexp*	(Optional) Used with the **flap-statistics** keyword, displays routes matching the AS path “regular expression”.
regexp *regexp*	(Optional) Used with the **flap-statistics** keyword, displays routes matching the AS path regular expression.
route-map *map-name*	(Optional) Used with the **flap-statistics** keyword, displays routes allowed by the route map.
parameters	Display details of configured dampening parameters.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

Use this command to display BGP dampening information for the VPNv6 address family.

Examples

The following example shows dampening VPNv6 information:

```
Router# show ip bgp vpnv6 unicast all dampening flap-statistics
For_address_family: VPNv6 Unicast
% dampening not enabled for base
For vrf: RED
For vrf: BLUE
BGP table version is 36, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          From            Flaps Duration Reuse    Path
*d  11::/64          20::2           3     00:03:17 00:05:59 2
*d  22::/64          20::2           3     00:03:17 00:05:59 2
*d  33::/64          20::2           3     00:03:17 00:05:59 2
*d  44::/64          20::2           3     00:03:17 00:05:59 2
*d  55::/64          20::2           3     00:03:17 00:05:59 2
R1#
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes BGP route dampening parameters.

show ip community-list

To display co nfigured community lists, use the **show ip community-list** command in user or privileged EXEC mode.

show ip community-list [*community-list-number*| *community-list-name*] **[exact-match]**

Syntax Description

community-list-number	(Optional) A standard or expanded community list number in the range from 1 to 500.
community-list-name	(Optional) Community list name. The community list name can be standard or expanded.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0(10)S	Named community list support was added.
12.0(16)ST	Named community lists support was integrated into Cisco IOS Release 12.0(16)ST.
12.1(9)E	Named community lists support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community lists support was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command can be used without any arguments or keywords. If no arguments are specified, this command will display all community lists. However, the community list name or number can be specified when entering the **show ip community-list** command. This option can be useful for filtering the output of this command and verifying a single named or numbered community list.

Examples

The following sample output is similar to the output that will be displayed when the **show ip community-list**command is entered in privileged EXEC mode:

```
Router# show ip community-list

Community standard list 1
     permit 3
     deny 5
Community (expanded) access list 101
    deny 4
    permit 6
Named Community standard list COMMUNITY_LIST_NAME
    permit 1
    deny 7
Named Community expanded list COMMUNITY_LIST_NAME_TWO
    deny 2
    permit 8
```

The Field Descriptions table below describes the significant fields shown in the display.

Table 49: show ip community-list Field Descriptions

Field	Description
Community standard list	If shown, this value will display a standard community list number (1 to 99). The standard community list number will immediately follow this value.
Community (expanded) access list	If shown, this value will display an expanded community list number (100 to 500). The expanded community list number will immediately follow this value.
Named community standard list	If shown, this value will display a standard community list name. The standard community list name will immediately follow this value.
Named community expanded list	If shown, this value will display an expanded community list name. The expanded community list name will immediately follow this value.

show ip extcommunity-list

To display routes that are permitted by an extended community list, use the **show ip extcommunity-list** command in user EXEC or privileged EXEC mode.

show ip extcommunity-list [*list-number*| *list-name*]

Syntax Description

list-number	(Optional) Specifies an extended community list number from 1 to 500. A standard extended community list number is from 1 to 99. An expanded extended list is from 100 to 500.
list-name	(Optional) Specifies an extended community list name. If a specific extended community list number is not specified, all locally configured extended community lists will be displayed by default.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.1	This command was introduced.
12.2(25)S	Support for named extended community lists was added. Minor formatting changes were made to the output.
12.3(11)T	Support for named extended community lists was added. Minor formatting changes were made to the output.
12.2(27)SBC	This command was integrated into the Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SXI1	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

If the route target--RT in the output--contains a 4-byte autonomous system number as part of the extended community list, it will be displayed in the appropriate format.

Examples

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

```
Router# show ip extcommunity-list
Standard extended community-list 1
     10 permit RT:64512:10
     20 permit SoO:65400:20
```

```
     30 deny RT:65424:30 SoO:64524:40
Standard extended community-list 99
     10 permit RT:65504:40 SoO:65505:50
     20 deny RT:65406:60 SoO:65307:70
Expanded extended community-list LIST_NAME
     10 permit 0-9* A-Z* a-z*
```

The table below describes the significant fields shown in the display.

Table 50: show ip extcommunity-list Field Descriptions

Field	Description
... extended community-list....	The type of extended community-list (standard or expanded), and the name or number of the extended community list.
10	The sequence number of the extended community list entry. 10 is the lowest default sequence number. Extended community lists increment by 10 when default values are configured.
permit/deny	Indicates a permit or deny sequence entry.
RT/SoO	Indicates the route target or the site of origin used in a standard extended community list.
0-9* A-Z* a-z*	Regular expression used in an expanded extended community list.

The following output is from the **show ip extcommunity-list**command after a 4-byte autonomous system number has been configured as part of the route target. The 4-byte autonomous system number, 65537, is displayed in the default asplain format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router# show ip extcommunity-list 1
Extended community standard list 1
     permit RT:65537:100
```

The following output displays a 4-byte autonomous system number that has been configured as part of the route target. The 4-byte autonomous system number--1.1--is displayed in asdot notation. The dot notation is the only format for 4-byte autonomous system numbers in Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3. This output can also be seen in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or later releases. after the **bgp asnotation dot** command has been entered to display 4-byte autonomous system numbers in dot notation.

```
Router# show ip extcommunity-list 1
Extended community standard list 1
     permit RT:1.1:100
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
router bgp	Configures the BGP routing process.
show route-map	Displays configured route maps.

show ip policy-list

To display information about a configured policy list and policy list entries, use the **show ip policy-list** command in EXEC mode.

show ip policy-list [*policy-list-name*]

Syntax Description

policy-list-name	(Optional) Displays information about the specified policy list with this argument.

Command Modes

EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into 12.2(15)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip policy-list** command. The output of this command will display the policy-list name and configured match clauses. The following sample output is similar to the output that will be displayed:

```
Router> show ip policy-list

policy-list POLICY-LIST-NAME-1 permit
  Match clauses:
    metric 20
policy-list POLICY-LIST-NAME-2 permit
  Match clauses:
    as-path (as-path filter): 1
```

Related Commands

Command	Description
show route-map	Displays configured route maps and information about referenced policy maps.

show ip prefix-list

To display information about a prefix list or prefix list entries, use the **show ip prefix-list** command in user EXEC or privileged EXEC mode.

show ip prefix-list[**detail**| **summary**]{*prefix-list-name* [**seq** *sequence-number*| *network*/*length* [**longer**| **first-match**]]}

Syntax Description

detail | **summary**	(Optional) Displays detailed or summarized information about all prefix lists.
prefix-list-name	(Optional) Displays the entries in a specific prefix list.
seq *sequence-number*	(Optional) Displays only the prefix list entry with the specified sequence number in the specified prefix-list.
network / *length*	(Optional) Displays all entries in the specified prefix list that use this network address and netmask length (in bits).
longer	(Optional) Displays all entries of the specified prefix list that match or are more specific than the given *network/length.*
first-match	(Optional)Displays the first entry of the specified prefix list that matches the given *network* / *length*.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows the output of the **show ip prefix-list** command with details about the prefix list named test:

```
Router# show ip prefix-list detail test
ip prefix-list test:
Description: test-list
 count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
 seq 10 permit 10.0.0.0/8 (hit count: 0, refcount: 1)
```

Related Commands

Command	Description
clear ip prefix-list	Resets the hit count of the prefix list entries.
distribute-list in (BGP)	Filters networks received in updates.
distribute-list out (BGP)	Suppresses networks from being advertised in updates.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list description	Adds a text description of a prefix list.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.

show ip route

To display contents of the routing table, use the **show ip route** command in user EXEC or privileged EXEC mode.

show ip route [*ip-address* [**repair-paths**| **next-hop-override [dhcp]**| *mask* **[longer-prefixes]**]| *protocol* [*process-id*]| **list** [*access-list-number* | *access-list-name*]| **static download**| **update-queue**]

Syntax Description

ip-address	(Optional) IP address for which routing information should be displayed.
repair-paths	(Optional) Displays the repair paths.
next-hop-override	(Optional) Displays the Next Hop Resolution Protocol (NHRP) next-hop overrides that are associated with a particular route and the corresponding default next hops.
dhcp	(Optional) Displays routes added by the Dynamic Host Configuration Protocol (DHCP) server.
mask	(Optional) Subnet mask.
longer-prefixes	(Optional) Displays output for longer prefix entries.
protocol	(Optional) The name of a routing protocol or the keyword **connected**, **mobile**, **static**, or **summary**. If you specify a routing protocol, use one of the following keywords: **bgp**, **eigrp**, **hello**, **isis**, **odr**, **ospf**, **nhrp**, or **rip**.
process-id	(Optional) Number used to identify a process of the specified protocol.
list	(Optional) Filters output by an access list name or number.
access-list-number	(Optional) Access list number.
access-list-name	(Optional) Access list name.
static	(Optional) Displays static routes.
download	(Optional) Displays routes installed using the authentication, authorization, and accounting (AAA) route download function. This keyword is used only when AAA is configured.

update-queue	(Optional) Displays Routing Information Base (RIB) queue updates.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.2	This command was introduced.
10.0	This command was modified. The "D—EIGRP, EX—EIGRP, N1—SPF NSSA external type 1 route" and "N2—OSPF NSSA external type 2 route" codes were included in the command output.
10.3	This command was modified. The *process-id* argument was added.
11.0	This command was modified. The **longer-prefixes** keyword was added.
11.1	This command was modified. The "U—per-user static route" code was included in the command output.
11.2	This command was modified. The "o—on-demand routing" code was included in the command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA, and the **update-queue** keyword was added.
11.3	This command was modified. The command output was enhanced to display the origin of an IP route in Intermediate System-to-Intermediate System (IS-IS) networks.
12.0(1)T	This command was modified. The "M—mobile" code was included in the command output.
12.0(3)T	This command was modified. The "P—periodic downloaded static route" code was included in the command output.
12.0(4)T	This command was modified. The "ia—IS-IS" code was included in the command output.
12.2(2)T	This command was modified. The command output was enhanced to display information on multipaths to the specified network.

Release	Modification
12.2(13)T	This command was modified. The *egp* and *igrp* arguments were removed because the Exterior Gateway Protocol (EGP) and the Interior Gateway Routing Protocol (IGRP) were no longer available in Cisco software.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.3(2)T	This command was modified. The command output was enhanced to display route tag information.
12.3(8)T	This command was modified. The command output was enhanced to display static routes using DHCP.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRE	This command was modified. The **dhcp** and **repair-paths** keywords were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5. The **next-hop-override** and **nhrp** keywords were added.
15.2(2)S	This command was modified. The command output was enhanced to display route tag values in dotted decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The command output was enhanced to display route tag values in dotted decimal format.
15.2(4)S	This command was implemented on the Cisco 7200 series router.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

Examples

The following is sample output from the **show ip route** command when an IP address is not specified:

```
Device# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
```

```
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
Gateway of last resort is 10.119.254.240 to network 10.140.0.0
O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E    10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E    10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
```

The following sample output from the **show ip route** command includes routes learned from IS-IS Level 2:

```
Device# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
Gateway of last resort is not set
     10.89.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
C       10.89.64.0 255.255.255.0 is possibly down,
          routing via 10.0.0.0, Ethernet0
i L2    10.89.67.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
i L2    10.89.66.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
```

The following is sample output from the **show ip route** *ip-address mask* **longer-prefixes** command. When this keyword is included, the address-mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed. The logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared with 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Device# show ip route 10.0.0.0 10.0.0.0 longer-prefixes

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
```

```
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
     10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C       10.19.64.0 is directly connected, Ethernet0
     10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C       10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S       10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following sample outputs from the **show ip route** command display all downloaded static routes. A “p” indicates that these routes were installed using the AAA route download function.

```
Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

Gateway of last resort is 172.16.17.1 to network 10.0.0.0

        172.31.0.0/32 is subnetted, 1 subnets
P       172.31.229.41 is directly connected, Dialer1 10.0.0.0/8 is subnetted, 3 subnets
P       10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.2.0 [200/0] via 172.31.229.41, Dialer1

Device# show ip route static

     172.16.4.0/8 is variably subnetted, 2 subnets, 2 masks
P       172.16.1.1/32 is directly connected, BRI0
P       172.16.4.0/8 [1/0] via 10.1.1.1, BRI0
S    172.31.0.0/16 [1/0] via 172.16.114.65, Ethernet0
S    10.0.0.0/8 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.114.201/32 is directly connected, BRI0
S       172.16.114.205/32 is directly connected, BRI0
S       172.16.114.174/32 is directly connected, BRI0
S       172.16.114.12/32 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
P    10.1.0.0/16 is directly connected, BRI0
P    10.2.2.0/24 is directly connected, BRI0
S*   0.0.0.0/0 [1/0] via 172.16.114.65, Ethernet0
S    172.16.0.0/16 [1/0] via 172.16.114.65, Ethernet0
```

The following sample output from the **show ip route static download** command displays all active and inactive routes installed using the AAA route download function:

```
Device# show ip route static download

Connectivity: A - Active, I - Inactive

A     10.10.0.0 255.0.0.0 BRI0
A     10.11.0.0 255.0.0.0 BRI0
A     10.12.0.0 255.0.0.0 BRI0
A     10.13.0.0 255.0.0.0 BRI0
I     10.20.0.0 255.0.0.0 172.21.1.1
I     10.22.0.0 255.0.0.0 Serial0
I     10.30.0.0 255.0.0.0 Serial0
I     10.31.0.0 255.0.0.0 Serial1
I     10.32.0.0 255.0.0.0 Serial1
A     10.34.0.0 255.0.0.0 192.168.1.1
A     10.36.1.1 255.255.255.255 BRI0 200 name remote1
I     10.38.1.9 255.255.255.0 192.168.69.1
```

The following sample outputs from the **show ip route nhrp** command display shortcut switching on the tunnel interface:

```
Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
Gateway of last resort is not set
10.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Tunnel0
C       172.16.22.0 is directly connected, Ethernet1/0
H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
     10.11.0.0/24 is subnetted, 1 subnets
C       10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route nhrp

H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
```

The following are sample outputs from the **show ip route** command when the **next-hop-override** keyword is used. When this keyword is included, the NHRP next-hop overrides that are associated with a particular route and the corresponding default next hops are displayed.

```
================================================================
1) Initial configuration
================================================================

Device# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
```

```
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback1
10.10.10.0/24        attached             Tunnel0  <<<<<<<<
10.11.11.0/24        attached             Ethernet0/0
172.16.0.0/12          drop
.
.
.
============================================================
2) Add a next-hop override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.1.1.1
   interface = Tunnel0
============================================================

Device# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets

S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets

S        10.10.10.0 is directly connected, Tunnel0
                  [NHO][1/0] via 10.1.1.1, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback110.10.10.0/24
```

```
10.10.10.0/24       10.1.1.1              Tunnel0

10.11.11.0/24       attached            Ethernet0/0
10.12.0.0/16 drop
.
.
.
================================================================
3) Delete a next-hop override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.11.1.1
   interface = Tunnel0
================================================================

Device# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix              Next Hop            Interface
.
.
.
10.2.1.255/32         receive             Loopback110.10.10.0/24

10.10.10.0/24       attached            Tunnel0
10.11.11.0/24       attached            Ethernet0/0
10.120.0.0/16 drop
.
.
.
```

The table below describes the significant fields shown in the displays:

Table 51: show ip route Field Descriptions

Field	Description
Codes (Protocol)	Indicates the protocol that derived the route. It can be one of the following values: • B—BGP derived • C—Connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H—NHRP • i—IS-IS derived • ia—IS-IS • L—Local • M—Mobile • o—On-demand routing • O—Open Shortest Path First (OSPF) derived • P—Periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—Static • U—Per-user static route • +—Replicated route
Codes (Type)	Type of route. It can be one of the following values: • *—Indicates the last path used when a packet was forwarded. This information is specific to nonfast-switched packets. • E1—OSPF external type 1 route • E2—OSPF external type 2 route • IA—OSPF interarea route • L1—IS-IS Level 1 route • L2—IS-IS Level 2 route • N1—OSPF not-so-stubby area (NSSA) external type 1 route • N2—OSPF NSSA external type 2 route

Field	Description
10.110.0.0	Indicates the address of the remote network.
[160/5]	The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next device to the remote network.
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

Examples

The following is sample output from the **show ip route** command when an IP address is specified:

```
Device# show ip route 10.0.0.1

Routing entry for 10.0.0.1/32
    Known via "isis", distance 115, metric 20, type level-1
    Redistributing via isis
    Last update from 10.191.255.251 on Fddi1/0, 00:00:13 ago
    Routing Descriptor Blocks:
    * 10.22.22.2, from 10.191.255.247, via Serial2/3
       Route metric is 20, traffic share count is 1
       10.191.255.251, from 10.191.255.247, via Fddi1/0
       Route metric is 20, traffic share count is 1
```

When an IS-IS router advertises its link-state information, the router includes one of its IP addresses to be used as the originator IP address. When other routers calculate IP routes, they store the originator IP address with each route in the routing table.

The preceding example shows the output from the **show ip route** command for an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next-hop address. The second is the originator IP address from the advertising IS-IS router. This address helps you determine the origin of a particular IP route in your network. In the preceding example, the route to 10.0.0.1/32 was originated by a device with IP address 10.191.255.247.

The table below describes the significant fields shown in the display.

Table 52: show ip route with IP Address Field Descriptions

Field	Description
Routing entry for 10.0.0.1/32	Network number and mask.
Known via...	Indicates how the route was derived.
Redistributing via...	Indicates the redistribution protocol.

Field	Description
Last update from 10.191.255.251	Indicates the IP address of the router that is the next hop to the remote network and the interface on which the last update arrived.
Routing Descriptor Blocks	Displays the next-hop IP address followed by the information source.
Route metric	This value is the best metric for this Routing Descriptor Block.
traffic share count	Indicates the number of packets transmitted over various routes.

The following sample output from the **show ip route** command displays the tag applied to the route 10.22.0.0/16. You must specify an IP prefix to see the tag value. The fields in the display are self-explanatory.

```
Device# show ip route 10.22.0.0

Routing entry for 10.22.0.0/16
  Known via "isis", distance 115, metric 12
  Tag 120, type level-1
  Redistributing via isis
  Last update from 172.19.170.12 on Ethernet2, 01:29:13 ago
  Routing Descriptor Blocks:
    * 172.19.170.12, from 10.3.3.3, via Ethernet2
        Route metric is 12, traffic share count is 1
        Route tag 120
```

Examples

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.16.2.2 [1/0] are static, and route 10.0.0.0/0 is a default route candidate. The fields in the display are self-explanatory.

```
Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.0.19.14 to network 0.0.0.0
10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.16.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0
S* 10.0.0.0/0 [1/0] via 10.0.19.14
```

The following sample output from the **show ip route repair-paths** command shows repair paths marked with the tag [RPR]. The fields in the display are self-explanatory:

```
Device# show ip route repair-paths

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 3 subnets
C        10.1.1.1 is directly connected, Loopback0
B        10.2.2.2 [200/0] via 172.16.1.2, 00:31:07
                  [RPR][200/0] via 192.168.1.2, 00:31:07
B        10.9.9.9 [20/0] via 192.168.1.2, 00:29:45
                  [RPR][20/0] via 192.168.3.2, 00:29:45
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Serial2/0
L        192.168.1.1/32 is directly connected, Serial2/0
B     192.168.3.0/24 [200/0] via 172.16.1.2, 00:31:07
                     [RPR][200/0] via 192.168.1.2, 00:31:07
B     192.168.9.0/24 [20/0] via 192.168.1.2, 00:29:45
                     [RPR][20/0] via 192.168.3.2, 00:29:45
B     192.168.13.0/24 [20/0] via 192.168.1.2, 00:29:45
                      [RPR][20/0] via 192.168.3.2, 00:29:45

Device# show ip route repair-paths 10.9.9.9

>Routing entry for 10.9.9.9/32
>  Known via "bgp 100", distance 20, metric 0
>  Tag 10, type external
>  Last update from 192.168.1.2 00:44:52 ago
>  Routing Descriptor Blocks:
>  * 192.168.1.2, from 192.168.1.2, 00:44:52 ago, recursive-via-conn
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
>    [RPR]192.168.3.2, from 172.16.1.2, 00:44:52 ago
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
```

Related Commands

Command	Description
show interfaces tunnel	Displays tunnel interface information.
show ip route summary	Displays the current state of the routing table in summary format.

show ip route vrf

To display the IP routing table associated with a specific VPN routing and forwarding (VRF) instance, use the **show ip route vrf** command in user EXEC or privileged EXEC mode.

show ip route vrf *vrf-name* [**connected**| *protocol* [*as-number*]| **list** [*list-number*]| **profile**| **static**| **summary**| [*ip-prefix*| *ip-address*] [*mask*| **longer-prefixes**]| **repair-paths**| **dhcp**| **supernets-only**| **tag** {*tag-value*| *tag-value-dotted-decimal* [*mask*]}]

Syntax Description

vrf-name	Name of the VRF.
connected	(Optional) Displays all connected routes in a VRF.
protocol	(Optional) Routing protocol. To specify a routing protocol, use one of the following keywords: **bgp**, **egp**, **eigrp**, **hello**, **igrp**, **isis**, **ospf**, or **rip**.
as-number	(Optional) Autonomous system number.
list *number*	(Optional) Specifies the IP access list to be displayed.
profile	(Optional) Displays the IP routing table profile.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of routes.
ip-prefix	(Optional) Network for which routing information is displayed.
ip-address	(Optional) Address for which routing information is displayed.
mask	(Optional) Network mask.
longer-prefixes	(Optional) Displays longer prefix entries.
repair-paths	(Optional) Displays repair paths.
dhcp	(Optional) Displays routes added by the DHCP server.
supernets-only	(Optional) Displays only supernet entries.
tag	(Optional) Displays information about route tags in the VRF table.
tag-value	(Optional) Route tag values as a plain decimals.

tag-value-dotted-decimal	(Optional) Route tag values as a dotted decimals.
mask	(Optional) Route tag wildcard mask.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	This command was modified. The *ip-prefix* argument was added. The command output was enhanced to display information on multipaths to the specified network.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was modified. Support for Enhanced Interior Gateway Routing Protocol (EIGRP) VRFs was added.
12.2(15)T	This command was modified. Support for EIGRP VRFs was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. The output was enhanced to display remote label information and corresponding Multiprotocol Label Switching (MPLS) flags for prefixes that have remote labels stored in the Routing Information Base (RIB).
12.2(33)SRE	This command was modified. The **repair-paths**, **dhcp**, and **supernets-only** keywords were added. Support for the Border Gateway Protocol (BGP) Best External and BGP Additional Path features was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.2(2)S	This command was modified. The **tag** keyword and *tag-value*, *tag-value-dotted-decimal*, and *mask* arguments were added to enable the display of route tags as plain or dotted decimals in the command output.
Cisco IOS XE Release 3.6S	This command was modified. The **tag** keyword and *tag-value*, *tag-value-dotted-decimal*, and *mask* arguments were added to enable the display of route tags as plain or dotted decimals in the command output.
15.2(4)S	This command was implemented on the Cisco 7200 series router.

Release	Modification
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following sample output displays the IP routing table associated with the VRF named vrf1:

```
Device# show ip route vrf vrf1

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C    10.0.0.0/8 is directly connected, Ethernet1/3
B    10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20
```

This following sample output shows BGP entries in the IP routing table associated with the VRF named vrf1:

```
Device# show ip route vrf vrf1 bgp

B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:44:14
B  10.0.0.0/8 [20/0] via 10.0.0.1, 03:44:12
B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:43:14
```

The following sample output displays the IP routing table associated with a VRF named PATH:

```
Device# show ip route vrf PATH 10.22.22.0

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 22, type internal
  Last update from 10.22.5.10 00:01:07 ago
  Routing Descriptor Blocks:
  * 10.22.7.8 (Default-IP-Routing-Table), from 10.11.3.4, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.1.9 (Default-IP-Routing-Table), from 10.11.1.2, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.6.10 (Default-IP-Routing-Table), from 10.11.6.7, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.4.10 (Default-IP-Routing-Table), from 10.11.4.5, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
    10.22.5.10 (Default-IP-Routing-Table), from 10.11.5.6, 00:01:07 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
```

The following sample output from the **show ip route vrf** *vrf-name* **tag** command displays route tag information for routes associated with vrf1. The route tags in the sample output are displayed in dotted decimal format.

```
Device# show ip route vrf vrf1 tag 5

Routing Table: vrf1
Routing entry for 10.0.0.1/24
  Known via "static", distance 1, metric 0 (connected)
  Tag 0.0.0.5
  Routing Descriptor Blocks:
```

```
  * directly connected, via Null0
      Route metric is 0, traffic share count is 1
      Route tag 0.0.0.5
```

The following sample outputs from the **show ip route vrf** command include recursive-via-host and recursive-via-connected flags:

```
Device# show ip route vrf v2 10.2.2.2

Routing Table: v2
Routing entry for 10.2.2.2/32
  Known via "bgp 10", distance 20, metric 0
  Tag 100, type external
  Last update from 192.168.1.1 00:15:54 ago
  Routing Descriptor Blocks:
  * 192.168.1.1, from 192.168.1.1, 00:15:54 ago, recursive-via-conn
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: none

Device# show ip route vrf v2 10.2.2.2

Routing Table: v2
Routing entry for 10.2.2.2/32
  Known via "bgp 10", distance 200, metric 0
  Tag 100, type internal
  Last update from 10.3.3.3 00:18:11 ago
  Routing Descriptor Blocks:
  * 10.3.3.3 (default), from 10.5.5.5, 00:18:11 ago, recursive-via-host
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: 16
      MPLS Flags: MPLS Required
```

The table below describes the significant fields shown in the displays.

Table 53: show ip route vrf Field Descriptions

Field	Description
Routing entry for 10.22.22.0/24	Network number.
Known via ...	Indicates how the route was derived.
distance	Administrative distance of the information source.
metric	Metric used to reach the destination network.
Tag	Integer used to tag the route.
type	Indicates whether the route is an L1 type or L2 type of route.
Last update from 10.22.5.10	Indicates the IP address of the device that is the next hop to the remote network and identifies the interface on which the last update arrived.
00:01:07 ago	Specifies the last time the route was updated (in hours:minutes:seconds).

Field	Description
Routing Descriptor Blocks	Displays the next-hop IP address followed by the information source.
10.22.6.10, from 10.11.6.7, 00:01:07 ago	Indicates the next-hop address, the address of the gateway that sent the update, and the time that has elapsed since this update was received (in hours:minutes:seconds).
Route metric	This value is the best metric for this routing descriptor block.
Traffic share count	Indicates the number of packets transmitted over various routes.
AS Hops	Number of hops to the destination or to the device where the route first enters internal BGP (iBGP).

The following is sample output from the **show ip route vrf** command on devices using the Cisco IOS Software Modularity for Layer 3 VPNs feature. The output includes remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the RIB if BGP is the label distribution protocol.

```
Device# show ip route vrf v2 10.2.2.2

Routing entry for 10.2.2.2/32
  Known via "bgp 1", distance 200, metric 0, type internal
  Redistributing via ospf 2
  Advertised by ospf 2 subnets
  Last update from 10.0.0.4 00:22:59 ago
  Routing Descriptor Blocks:
  * 10.0.0.4 (Default-IP-Routing-Table), from 10.0.0.31, 00:22:59 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: 1300
      MPLS Flags: MPLS Required
```

The table below describes the significant fields shown in the display.

Table 54: show ip route vrf Field Descriptions

Field	Description
MPLS label	Displays the BGP prefix from the BGP peer. The output shows one of the following values: • A label value (16–1048575). • A reserved label value, such as explicit-null or implicit-null. • The word "none" if no label is received from the peer. The MPLS label field is not displayed if any of the following conditions is true: • BGP is not the Label Distribution Protocol (LDP). However, Open Shortest Path First (OSPF) prefixes learned via sham links display an MPLS label. • MPLS is not supported. • The prefix is imported from another VRF, where the prefix was an Interior Gateway Protocol (IGP) prefix and LDP provided the remote label for it.
MPLS Flags	Name of the MPLS flag. One of the following MPLS flags is displayed: • MPLS Required—Indicates that packets are forwarded to this prefix because of the presence of the MPLS label stack. If MPLS is disabled on the outgoing interface, the packets are dropped. • No Global—Indicates that MPLS packets for this prefix are forwarded from the VRF interface and not from the interface in the global table. VRF interfaces prevent loops in scenarios that use iBGP multipaths. • NSF—Indicates that the prefix is from a nonstop forwarding (NSF)-aware neighbor. If the routing information temporarily disappears due to a disruption in the control plane, packets for this prefix are preserved.

The following sample output from the **show ip route vrf** command shows repair paths in the routing table. The fields in the display are self-explanatory.

```
Device> show ip route vrf test1 repair-paths 192.168.3.0

Routing Table: test1
Routing entry for 192.168.3.0/24
  Known via "bgp 10", distance 20, metric 0
  Tag 100, type external
  Last update from 192.168.1.1 00:49:39 ago
  Routing Descriptor Blocks:
  * 192.168.1.1, from 192.168.1.1, 00:49:39 ago, recursive-via-conn
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: none
    [RPR]10.4.4.4 (default), from 10.5.5.5, 00:49:39 ago, recursive-via-host
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: 29
MPLS Flags: MPLS Required, No Global
```

Related Commands

Command	Description
show ip cache	Displays the Cisco Express Forwarding table associated with a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show tcp ha connections

To display connection-ID-to-TCP mapping data, use the **show tcp ha connections** command in privileged EXEC mode.

show tcp ha connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(28)SB	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **show tcp ha connections** command is used to display connection-ID-to-TCP mapping data.

Examples

The following is sample output from the **show tcp ha connections** command:

```
Router# show tcp ha connections
SSO enabled for 40 connections
TCB       Local Address           Foreign Address        (state)    Conn Id
71EACE60  10.0.56.1.179           10.0.56.3.58671         ESTAB      37
71EA9320  10.0.53.1.179           10.0.53.3.58659         ESTAB      34
71EA35F8  10.0.41.1.179           10.0.41.3.58650         ESTAB      22
71A21FE0  10.0.39.1.179           10.0.39.3.58641         ESTAB      20
71EAA6E0  10.0.54.1.179           10.0.54.3.58663         ESTAB      35
71EA2238  10.0.40.1.179           10.0.40.3.58646         ESTAB      21
71EABAA0  10.0.55.1.179           10.0.55.3.58667         ESTAB      36
71EAE710  10.0.28.1.179           10.0.28.3.58676         ESTAB      9
71EA2728  10.0.50.1.179           10.0.50.3.58647         ESTAB      31
720541D8  10.0.49.1.179           10.0.49.3.58642         ESTAB      30
71EAA1F0  10.0.44.1.179           10.0.44.3.58662         ESTAB      25
2180B3A8  10.0.33.1.179           10.0.33.3.58657         ESTAB      14
71EAB5B0  10.0.45.1.179           10.0.45.3.58666         ESTAB      26
21809FE8  10.0.32.1.179           10.0.32.3.58653         ESTAB      13
71EA8E30  10.0.43.1.179           10.0.43.3.58658         ESTAB      24
71EAD350  10.0.27.1.179           10.0.27.3.58672         ESTAB      8
2180A9C8  10.0.52.1.179           10.0.52.3.58655         ESTAB      33
2180A4D8  10.0.42.1.179           10.0.42.3.58654         ESTAB      23
71EABF90  10.0.26.1.179           10.0.26.3.58668         ESTAB      7
71EA3AE8  10.0.51.1.179           10.0.51.3.58651         ESTAB      32
720546C8  10.0.59.1.179           10.0.59.3.58643         ESTAB      40
```

The table below describes the significant fields shown in the display.

Table 55: show tcp ha connections Field Descriptions

Field	Description
SSO enabled for	Displays the number of TCP connections that support BGP Nonstop Routing (NSR) with SSO.
TCB	An internal identifier for the endpoint.
Local Address	The local IP address and port.
Foreign Address	The foreign IP address and port (at the opposite end of the connection).
(state)	TCP connection state. A connection progresses through a series of states during its lifetime. The states that follow are shown in the order in which a connection progresses through them. • LISTEN--Waiting for a connection request from any remote TCP and port. • SYNSENT--Waiting for a matching connection request after having sent a connection request. • SYNRCVD--Waiting for a confirming connection request acknowledgment after having both received and sent a connection request. • ESTAB--Indicates an open connection; data received can be delivered to the user. This is the normal state for the data transfer phase of the connection. • FINWAIT1--Waiting for a connection termination request from the remote TCP or an acknowledgment of the connection termination request previously sent.
Conn id	Identifying number of the TCP connection.

slow-peer detection

To use a policy template to specify a threshold time that dynamically determines a BGP slow peer, use the **slow-peer detection** command in policy template configuration mode. To restore the default value, use the **no** form of this command.

slow-peer detection [**threshold** *seconds*]

no slow-peer detection

Syntax Description

threshold *seconds*	(Optional) Specifies the threshold time in seconds that the timestamp of the oldest message in a peers queue can be lagging behind the current time before the BGP peer is determined to be a slow peer. The range is from 120 to 3600; the default is 300.

Command Default

300 seconds

Command Modes

Policy template configuration (config-router-ptmp)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

Update messages are timestamped when they are formatted. The timestamp of the oldest update message in a peers queue is compared to the current time to determine if the peer is lagging more than the configured number of seconds. When a peer is dynamically detected to be a slow peer, the system will send a syslog message. The peer will be marked as recovered and another syslog message will be generated only after the peer's update group converges.

Note The **neighbor slow-peer detection** command performs the same function as the **bgp slow-peer detection** command (at the address-family level), except that the **neighbor slow-peer detection** command overrides the address-family level command. When the **neighbor slow-peer detection** command is unconfigured, the system will function according to the address-family level configuration. The **slow-peer detection** command performs the same function through a peer policy template.

Examples

The following example specifies that if the timestamp on a peer's update message is more than 360 seconds before the current time, the peer that sent the update message is considered to be slow. The commands configured under the peer-policy template will be applied to the neighbor once it inherits the peer-policy.

```
Router(config)# router bgp 13
Router(config-router)# template peer-policy ipv4_ucast_pp1
Router(config-router-ptmp)# slow-peer detection threshold 360
Router(config-router-ptmp)# slow-peer split-update-group dynamic
```

Related Commands

Command	Description
bgp slow-peer detection	Specifies a threshold time that dynamically determines a slow peer.
bgp slow-peer split-update-group dynamic	Moves a dynamically detected slow peer to a slow update group.
clear ip bgp slow	Moves dynamically configured slow peers back to their original update groups.
neighbor slow-peer split-update-group dynamic	Moves a dynamically detected slow peer to a slow update group.
slow-peer split-update-group dynamic	Moves a dynamically detected slow peer to a slow update group.

slow-peer split-update-group dynamic

To use a policy template to move a dynamically detected slow peer to a slow update group, use the **slow-peer split-update-group dynamic** command in policy template configuration mode. To disable dynamically detected slow peers from being moved to a slow update group, use the **no** form of this command.

slow-peer split-update-group dynamic [permanent]

no slow-peer split-update-group dynamic

Syntax Description

permanent	(Optional) Specifies that after the slow peer becomes a regular peer (converges), it is not moved back to its original update group automatically. It remains in the slow update group until the network administrator uses one of the **clear slow**commands to move the peer to its original update group.

Command Default

No dynamically detected slow peer is moved to a slow peer update group.

Command Modes

Policy template (config-router-ptmp)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

When a peer is dynamically detected to be a slow peer, the slow peer is moved to a slow update group. If a *static* slow peer update group exists, the dynamic slow peer is moved to the static slow peer update group; otherwise, a new slow peer update group is created and the peer is moved to that group.

- We recommend you configure the **permanent** keyword. If the **permanent** keyword is configured, the peer is not automatically moved to its original update group. After you resolve the root cause of the slow peer, you can use the **clear bgp slow**command to move the peer back to its original update group.
- If the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).

Note The **neighbor slow-peer split-update-group dynamic**command performs the same function as the **bgp slow-peer split-update-group dynamic** command (at the address-family level), except that the **neighbor slow-peer split-update-group dynamic** command overrides the address-family level command. When the **neighbor slow-peer split-update-group dynamic** command is unconfigured, the system will function according to the address-family level configuration. The **slow-peer split-update-group dynamic** command performs the same function through a policy template.

If **slow-peer split-update-group dynamic**is configured, but no slow peer detection is configured, the detection will be done at the default threshold of 300 seconds. That is, detection is enabled automatically with its default threshold.

Examples

In the following example, the timestamp of the oldest message in a peers queue is compared to the current time to determine if the peer is lagging more than 360 seconds. If it is, the neighbor that sent the message is determined to be a slow peer, and is put in the slow peer update group. Because the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).

```
Router(config)# router bgp 13
Router(config-router)# template peer-policy ipv4_ucast_pp1
Router(config-router-ptmp)# slow-peer detection threshold 360
Router(config-router-ptmp)# slow-peer split-update-group dynamic
```

Related Commands

Command	Description
slow-peer detection	Specifies a threshold time that dynamically determines a slow peer.
show ip bgp template peer-policy	Displays locally configured peer policy templates.

slow-peer split-update-group static

To mark a BGP neighbor as a slow peer and move it to a slow update group, use the **slow-peer split-update-group static** command by using a peer policy template. To unmark the slow peer and return it to its original update group, use the **no** form of this command.

slow-peer split-update-group static

no slow-peer split-update-group static

Syntax Description

This command has no arguments or keywords.

Command Default

No peer is marked as slow and moved to a slow peer update group in a static manner using a peer policy template.

Command Modes

Peer policy template (config-router-ptmp)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

Configure a static slow peer when the peer is known to be slow (perhaps due to a slow link or low processing power).

The **neighbor slow-peer split-update-group static**command performs the same function in address-family mode.

Examples

In the following example, the neighbor is marked as a slow peer and is moved to a slow update group.

```
Router(config)# router bgp 13
Router(config-router)# template peer-policy ipv4_ucast_pp1
Router(config-router-ptmp)# slow-peer split-update-group static
```

Related Commands

Command	Description
neighbor slow-peer split-update-group static	Marks a BGP neighbor as a slow peer and moves it to a slow update group.

soo

To set the site-of-origin (SoO) value for a Border Gateway Protocol (BGP) peer policy template, use the **soo** command in policy-template configuration mode. To remove the SoO value, use the **no** form of this command.

soo *extended-community-value*

no soo

Syntax Description

extended-community-value	Specifies the VPN extended community value. The value takes one of the following formats: • A 16-bit autonomous system number, a colon, and a 32-bit number, for example: 45000:3 • A 32-bit IP address, a colon, and a 16-bit number, for example: 192.168.10.2:51 In Cisco IOS Release 12.4(24)T, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. In Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. For more details about autonomous system number formats, see the **router bgp** command.

Command Default

No SoO value is set for a BGP peer policy template.

Command Modes

Policy-template configuration (config-router-ptmp)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(24)T	Support for 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

Use this command to set the SoO value for a BGP peer policy template that a BGP neighbor can inherit. The SoO value is set for a peer policy template, and a BGP neighbor is identified under address family IPv4 VRF configuration mode to inherit the peer policy that contains the SoO value.

The SoO extended community is a BGP extended community attribute that is used to identify routes that have originated from a site so that the readvertisement of that prefix back to the source site can be prevented. The SoO extended community uniquely identifies the site from which a router has learned a route. BGP can use the SoO value associated with a route to prevent routing loops.

In releases prior to Cisco IOS Release 12.4(11)T, 12.2(33)SRB, and 12.2(33)SB, the SoO extended community attribute is configured using an inbound route map that sets the SoO value during the update process. The introduction of the **neighbor soo** and **soo** commands simplifies the SoO value configuration.

In Cisco IOS Release 12.4(24)T, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

In Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

Note If a BGP peer inherits from several peer policy templates that specify different SoO values, the SoO value in the last template applied takes precedence and is applied to the peer. However, direct configuration of the SoO value on the BGP neighbor overrides any inherited template configurations of the SoO value.

Examples

The following example shows how to create a peer policy template and configure an SoO value as part of the peer policy. Under address family IPv4 VRF, a neighbor is identified and configured to inherit the peer policy that contains the SoO value.

```
router bgp 45000
 template peer-policy SOO_POLICY
  soo 45000:3
  exit-peer-policy
 address-family ipv4 vrf SOO_VRF
  neighbor 192.168.3.2 remote-as 50000
  neighbor 192.168.3.2 activate
  neighbor 192.168.3.2 inherit peer-policy SOO_POLICY
  end
```

The following example shows how to create a peer policy template and configure an SoO value using a 4-byte autonomous system number, 1.2 in asdot format, as part of the peer policy. Under address family IPv4 VRF, a neighbor is identified and configured to inherit the peer policy that contains the SoO value. This example requires Cisco IOS Release 12.4(24)T, Cisco IOS XE Release 2.4, or a later release.

```
router bgp 1.2
 template peer-policy SOO_POLICY
  soo 1.2:3
  exit-peer-policy
 address-family ipv4 vrf SOO_VRF
  neighbor 192.168.3.2 remote-as 1.14
  neighbor 192.168.3.2 activate
  neighbor 192.168.3.2 inherit peer-policy SOO_POLICY
  end
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters address family configuration mode to configure a routing session using standard IP Version 4 address prefixes.
neighbor soo	Sets the SoO value for a BGP neighbor or peer group.
router bgp	Configures the BGP routing process.
template peer-policy	Creates a peer policy template and enters policy-template configuration mode.

stats-reporting-period (bmp)

To configure the time interval in which the BGP Monitoring Protocol (BMP) server receives the statistics report from the BGP BMP neighbors, use the **stats-reporting-period** command in BMP server configuration mode. To disable the reporting period for statistics, use the **no** form of the command.

stats-reporting-period *report-period*

no stats-reporting-period

Syntax Description

report-period	Specifies the interval, in seconds, in which a specific BMP server receives the statistics report from its connected BGP BMP neighbors. The value of the reporting period that you can configure, ranges from 1 to 3600 seconds.

Command Default

The BMP server does not receive statistics reporting from the BGP BMP neighbors at periodic intervals.

Command Modes

BMP server configuration (config-router-bmpsrvr)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show ip bgp bmp** command to verify the statistics reporting period that is configured for BMP server.

Examples

The following example show how to enter BMP server configuration mode and configure the statistics reporting period for BMP server 1 and 2:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
Device(config-router-bmpsrvr)# stats-reporting-period 30
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
```

```
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
Device(config-router-bmpsrvr)# stats-reporting-period 30
Device(config-router-bmpsrvr)# end
```

The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The statistics reporting interval on BMP server 1 and 2 has been set to 30 seconds, therefore each server receives statistics messages from its connected BGP BMP neighbor in each cycle of 30 seconds:

```
Device# show ip bgp bmp server summary

Number of BMP servers configured: 2
Number of BMP neighbors configured: 10
Number of neighbors on TransitionQ: 0, MonitoringQ: 0, ConfigQ: 0
Number of BMP servers on StatsQ: 0
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 30s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB

ID Host/Net          Port  TCB                Status  Uptime    MsgSent   LastStat
1  10.1.1.1          8000  0x2A98B07138       Up      00:38:49  162       00:00:09
2  20.1.1.1          9000  0x2A98E17C88       Up      00:38:49  46        00:00:04


Device# show ip bgp bmp server summary

Number of BMP servers configured: 2
Number of BMP neighbors configured: 10
Number of neighbors on TransitionQ: 0, MonitoringQ: 0, ConfigQ: 0
Number of BMP servers on StatsQ: 0
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 30s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB

ID Host/Net          Port  TCB                Status  Uptime    MsgSent   LastStat
1  10.1.1.1          8000  0x2A98B07138       Up      00:40:19  189       00:00:07
2  20.1.1.1          9000  0x2A98E17C88       Up      00:40:19  55        00:00:02
```

Note If we configure several BGP BMP neighbors to be monitored by the BMP servers, for example 10, then 10 statistics messages are received by both servers in each periodic cycle that is configured.

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show ip bgp bmp	Displays information about BMP servers and neighbors.

synchronization

To enable the synchronization between BGP and your Interior Gateway Protocol (IGP) system, use the **synchronization** command in address family or router configuration mode. 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.

Command Default

The behavior of this command is disabled by default.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(8)T	Command default behavior changed to disabled.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

Use the **synchronization** command if routers in the autonomous system do not speak BGP.

Examples

The following example shows how to enable synchronization in router configuration mode. The router validates the network route in its IGP before advertising the route externally.

```
router bgp 65120
 synchronization
```

The following example shows how to enable synchronization in address family configuration mode. The router validates the network route in its IGP before advertising the route externally.

```
router bgp 65120
address-family ipv4 unicast
 synchronization
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.

table-map

To specify a route map that modifies a metric, tag, or traffic index value (of routes that pass the route map) when the IP routing table is updated with BGP learned routes, or to selectively download BGP routes to the RIB, use the **table-map** command in address family or router configuration mode. To disable either function, use the **no** form of the command.

table-map *route-map-name* **[filter]**

no table-map *route-map-name* **[filter]**

Syntax Description

route-map-name	Name of the route map that controls what gets put into the BGP routing table (RIB).
filter	(Optional) Specifies that the route map controls not only the metrics on a BGP route, but also whether the route is downloaded into the RIB. • A BGP route is not downloaded to the RIB if it is denied by the route map.

Command Default

This command is disabled by default.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	This command was modified. Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	This command was modified. The **filter** keyword was added.

Release	Modification
Cisco IOS XE Release 3.9S	This command was modified. Support for the IPv6 address family was added.

Usage Guidelines

A table map references a route map that sets metrics, a tag value, or a traffic index for routes that are updated in the BGP routing table, or controls whether routes are downloaded to the RIB.

When the **table-map** command:

- Does not include the **filter** keyword, the route map referenced is used to set certain properties of a route before the route is installed (downloaded) into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map.
- Includes the **filter** keyword, the route map referenced also controls whether the BGP route is downloaded to the RIB. A BGP route is not downloaded to the RIB if it is denied by the route map.

You can use **match** clauses in the route map that the table map references. The route map can support existing policies similar to the ones available for inbound and outbound route maps of a neighbor, including **match as-path**, **match community**, **match extcommunity**, **match ip address prefix-list**, and **match ip next-hop**.

Unlike a route map, a table map is not followed by **match** or **set** commands.

Note After changing the **table-map** configuration or the route map that it references, you must issue the **clear ip bgp table-map** command in order for the changes to take effect. The **clear ip bgp table-map** command causes a re-download of routes from BGP to the RIB.

Examples

In the following example, a prefix list called NEWNAME permits certain routes. Those routes are subject to the route map named TRAFFIC_BUCKET, which sets the traffic index of those routes to 5. That route map is referenced by the table map, which means that those routes are downloaded and installed in the RIB with their traffic index set to 5. The table map controls which routes had their traffic index set. Because the **filter** keyword is omitted, the table map does not filter routes from being downloaded and installed in the RIB.

```
ip prefix-list NEWNAME
 permit 192.168.35.0/24
 permit 192.168.36.0/24
!
route-map TRAFFIC_BUCKET
 match ip address prefix-list NEWNAME
 set traffic-index 5
!
router bgp 100
 address-family ipv4 unicast
 table-map TRAFFIC_BUCKET
!
clear ip bgp ipv4 unicast table-map
```

In the following example, the Selective Route Download feature is configured by specifying the **filter** keyword. Only routes that pass the route map named FEW_ROUTES are downloaded to the RIB:

```
ip prefix-list NAME3
 permit 192.168.1.1/24
 permit 192.168.5.1/24
```

```
route-map FEW_ROUTES permit 10
 match ip address prefix-list NAME3
!
router bgp 100
 neighbor 192.168.1.1 remote-as
 neighbor 192.168.5.1 remote-as
 address-family ipv4 unicast
  table-map FEW_ROUTES filter
!
clear ip bgp ipv4 unicast table-map
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Places the router in IPv6 address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
clear ip bgp table-map	Initiates a re-download of BGP routes to the RIB.
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a community list number or name.
match extcommunity	Matches an extended community list name.
match ip address prefix-list	Matches routes that pass a prefix list.
match ip next-hop	Matches routes that have a next hop address passed by one of the access lists specified.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

template peer-policy

To create a peer policy template and enter policy-template configuration mode, use the **template peer-policy** command in router configuration mode. To remove a peer policy template, use the **no** form of this command.

template peer-policy *policy-template-name*

no template peer-policy *policy-template-name*

Syntax Description

policy-template-name	Name or tag for the peer policy template.

Command Default

Removing a peer policy template by using the no form of this command removes all policy configurations inside of the template.

Command Modes

Router configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Peer policy templates are used to group and apply the configuration of commands that are applied within specific address-families and NLRI configuration mode. Peer policy templates are created and configured in peer policy configuration mode. BGP policy commands that are configured for specific address-families or NLRI configuration modes are configured in a peer policy template. The following BGP policy commands are supported by peer policy templates:

- **advertisement-interval**
- **allowas-in**
- **as-override**
- **capability**

- **default-originate**
- **distribute-list**
- **dmzlink-bw**
- **exit-peer-policy**
- **filter-list**
- **inherit peer-policy**
- **maximum-prefix**
- **next-hop-self**
- **next-hop-unchanged**
- **prefix-list**
- **remove-private-as**
- **route-map**
- **route-reflector-client**
- **send-community**
- **send-label**
- **soft-reconfiguration**
- **unsuppress-map**
- **weight**

Peer policy templates are used to configure BGP policy commands that are configured for neighbors that belong to specific address-families and NLRI configuration modes. Like peer session templates, peer policy templates are configured once and then applied to many neighbors through the direct application of a peer policy template or through inheritance from peer policy templates. The configuration of peer policy templates simplifies the configuration of BGP policy commands that are applied to all neighbors within an autonomous system.

Peer policy templates support direct and indirect inheritance from up to eight peer policy templates. Inherited peer policy templates are configured with sequence numbers like route-maps. An inherited peer policy template, like a route-map, is evaluated starting with the inherit statement with the lowest sequence number and ending with the highest sequence number. However, there is a difference; a peer policy template will not fall through like a route-map. Every sequence is evaluated, and if a BGP policy command is reapplied with different value, it will overwrite any previous value from a lower sequence number.

Peer policy templates support only general policy commands. BGP policy configuration commands that are configured only for specific address families or NLRI configuration modes are configured with peer policy templates.

Note A BGP neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies from only peer templates.

Examples

The following example creates a peer policy template named CUSTOMER-A. This peer policy template is configured to inherit the configuration from the peer policy templates named PRIMARY-IN and GLOBAL.

```
Router(config-router)# template peer-policy CUSTOMER-A
Router(config-router-ptmp)# route-map SET-COMMUNITY in
Router(config-router-ptmp)# filter-list 20 in

Router(config-router-ptmp)# inherit peer-policy PRIMARY-IN 20
Router(config-router-ptmp)# inherit peer-policy GLOBAL 10
Router(config-router-ptmp)# exit-peer-policy
Router(config-router)#
```

Related Commands

Command	Description
advertisement-interval	Sets the minimum interval between the sending of BGP routing updates.
allowas-in	Configures PE routers to allow readvertisement of all prefixes containing duplicate autonomous system numbers.
as-override	Configures a PE router to override the ASN of a site with the ASN of a provider.
capability orf prefix-list	Configures outbound route filtering and advertises the capability to send and receive ORF updates to the neighbor routers.
default-originate	Originates a default route to the local router.
distribute-list	Distributes BGP neighbor information as specified in an access list.
dmzlink-bw	Advertises the bandwidth of links that are used to exit an autonomous system.
exit peer-policy	Exits policy-template configuration mode and enters router configuration mode.
filter-list	Sets up a BGP filter.
inherit peer-policy	Configures a peer policy template to inherit the configuration from another peer policy template.
maximum-prefix	Controls how many prefixes can be received from a neighbor.
neighbor inherit peer-policy	Configures a router to send a peer policy template to a neighbor so that the neighbor can inherit the configuration.

Command	Description
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
next-hop-self	Disables next-hop processing of BGP updates on the router.
next-hop-unchanged	Propagates the next- hop unchanged for iBGP paths to this router.
prefix-list	Specifies a prefix list, a CLNS filter set, or a CLNS filter expression to be used to filter BGP advertisements.
remove-private-as	Removes the private autonomous system number from outbound routing updates.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
send-community	Specifies that the BGP community attribute should be sent to the specified neighbor.
show ip bgp template peer-policy	Displays locally configured peer policy templates.
show ip bgp template peer-session	Displays locally configured peer session templates.
soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
template peer-session	Creates a peer session template and enters session-template configuration mode.
unsuppress-map	Selectively unsuppresses surpressed routes.
weight	Assigns a weight to a neighbor connection.

template peer-session

To create a peer session template and enter session-template configuration mode, use the **template peer-session** command in router configuration mode. To remove a peer session template, use the **no** form of this command.

template peer-session *session-template-name*

no template peer-session *session-template-name*

Syntax Description

session-template-name	Name or tag for the peer session template.

Command Default

Removing a peer session template by using the **no** form of this command removes all session command configurations inside of the template.

Command Modes

Address family configuration

Router configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Peer session templates are used to group and apply the configuration of general session commands to groups of neighbors that share common session configuration elements. General session commands that are common for neighbors that are configured in different address families can be configured within the same peer session template. Peer session templates are created and configured in peer session configuration mode. Only general session commands can be configured in a peer session template. The following general session commands are supported by peer session templates:

- **description**
- **disable-connected-check**
- **ebgp-multihop**

- **exit peer-session**
- **inherit peer-session**
- **local-as**
- **password**
- **remote-as**
- **shutdown**
- **timers**
- **translate-update**
- **update-source**
- **version**

General session commands can be configured once in a peer session template and then applied to many neighbors through the direct application of a peer session template or through indirect inheritance from a peer session template. The configuration of peer session templates simplify the configuration of general session commands that are commonly applied to all neighbors within an autonomous system.

Peer session templates support direct and indirect inheritance. A peer can be configured with only one peer session template at a time, and that peer session template can contain only one indirectly inherited peer session template. However, each inherited session template can also contain one indirectly inherited peer session template. So, only one directly applied peer session template and up to seven additional indirectly inherited peer session templates can be applied, allowing you to apply up to a maximum of eight peer session configurations to a neighbor: the configuration from the directly inherited peer session template and the configurations from up to seven indirectly inherited peer session templates. Inherited peer session templates are evaluated first, and the directly applied template will be evaluated and applied last. So, if a general session command is reapplied with a different value, the subsequent value will have priority and overwrite the previous value that was configured in the indirectly inherited template.

Peer session templates support only general session commands. BGP policy configuration commands that are configured only for specific address families or NLRI configuration modes are configured with peer policy templates.

Note A BGP neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured only to belong to a peer group or to inherit policies from peer templates.

Examples

The following example creates a peer session template named CORE1. This example inherits the configuration of the peer session template named INTERNAL-BGP.

```
Router(config-router)# template peer-session CORE1
Router(config-router-stmp)# description CORE-123
Router(config-router-stmp)# update-source loopback 1
Router(config-router-stmp)# inherit peer-session INTERNAL-BGP
Router(config-router-stmp)# exit-peer-session
Router(config-router)#
```

Related Commands

Command	Description
description	Configures a description to be displayed by the local or a peer router.
disable-connected-check	Disables connection verification for eBGP peers no more than one hop away when the eBGP peer is configured with a loopback interface.
ebgp-multihop	Accepts or initiates BGP connections to external peers residing on networks that are not directly connected.
exit peer-session	Exits session-template configuration mode and enters router configuration mode.
inherit peer-session	Configures a peer session template to inherit the configuration from another peer session template.
local-as	Allows the customization of the autonomous system number for eBGP peer groupings.
neighbor inherit peer-session	Configures a router to send a peer session template to a neighbor so that the neighbor can inherit the configuration.
neighbor translate-update	Upgrades a router running BGP in the NLRI format to support multiprotocol BGP.
password	Enables MD5 authentication on a TCP connection between two BGP peers.
remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
show ip bgp template peer-policy	Displays locally configured peer policy templates.
show ip bgp template peer-session	Displays locally configured peer session templates.
shutdown	Disables a neighbor or peer group.
timers bgp	Adjusts BGP network timers.
update-source	Specifies that the Cisco IOS software allow internal BGP sessions to use any operational interface for TCP connections.
version	Configures the Cisco IOS software to accept only a particular BGP version.

timers bgp

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

timers bgp *keepalive holdtime* [*min-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. The range is from 0 to 65535.
holdtime	Interval (in seconds) after not receiving a *keepalive* message that the software declares a peer dead. The default is 180 seconds. The range is from 0 to 65535.
min-holdtime	(Optional) Interval (in seconds) specifying the minimum acceptable hold-time from a BGP neighbor. The minimum acceptable hold-time must be less than, or equal to, the interval specified in the *holdtime*argument. The range is from 0 to 65535.

Command Default

keepalive : 60 seconds*holdtime*: 180 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(26)S	The *min-holdtime* argument was added.
12.3(7)T	The *min-holdtime* argument was added.
12.2(22)S	The *min-holdtime* argument was added.
12.2(27)SBC	The *min-holdtime* argument was added and this command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	The *min-holdtime* argument was added and this command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	The *min-holdtime* argument was added and this command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

When configuring the *holdtime* argument for a value of less than twenty seconds, the following warning is displayed:

```
% Warning: A hold time of less than 20 seconds increases the chances of peer flapping
```

If the minimum acceptable hold-time interval is greater than the specified hold-time, a notification is displayed:

```
% Minimum acceptable hold time should be less than or equal to the configured hold time
```

Note When the minimum acceptable hold-time is configured on a BGP router, a remote BGP peer session is established only if the remote peer is advertising a hold-time that is equal to, or greater than, the minimum acceptable hold-time interval. If the minimum acceptable hold-time interval is greater than the configured hold-time, the next time the remote session tries to establish, it will fail and the local router will send a notification stating "unacceptable hold time."

Examples

The following example changes the keepalive timer to 70 seconds, the hold-time timer to 130 seconds, and the minimum acceptable hold-time interval to 100 seconds:

```
router bgp 45000
 timers bgp 70 130 100
```

Related Commands

Command	Description
clear ip bgp peer-group	Removes all the members of a BGP peer group.
router bgp	Configures the BGP routing process.
show ip bgp	Displays entries in the BGP routing table.

update-source (bmp)

To configure the interface source for routing updates on the BGP Monitoring Protocol (BMP) server, use the **update-source** command in BMP server configuration mode. To disable configuration of the interface source, use the **no** form of the command.

update-source *interface-type interface-number*

Syntax Description

interface-type interface-number	Specifies the interface type and number as the source for the BMP server routing updates.

Command Default

No interface source is configured on the BMP servers.

Command Modes

BMP server configuration (config-router-bmpsrvr)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show running-config** command to verify the interface that has been configured.

Examples

The following example show how to enter BMP server configuration mode and configure an interface source for routing updates:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
Device(config-router-bmpsrvr)# update-source ethernet 0/0
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
Device(config-router-bmpsrvr)# update-source ethernet 2/0
Device(config-router-bmpsrvr)# end
```

The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The “update-source” field in the output displays the interface source configured for BMP servers 1 and 2 for routing updates:

```
Device# show running-config | section bmp

bmp server 1
address 10.1.1.1 port-number 8000
description SERVER1
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
update-source Ethernet0/0
activate
exit-bmp-server-mode
bmp server 2
address 20.1.1.1 port-number 9000
description SERVER2
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
update-source Ethernet2/0
activate
exit-bmp-server-mode
neighbor 30.1.1.1 bmp-activate all
neighbor 40.1.1.1 bmp-activate all
neighbor 50.1.1.1 bmp-activate all
```

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show running-config	Displays the running configuration on a device.

ve

To specify the Virtual Private LAN Service (VPLS) endpoint (VE) ID value or ID range value for a VPLS configuration, use the **ve** command in L2VPN VFI autodiscovery configuration mode. To remove the entry, use the **no** form of this command.

ve {**id** *id-value* | **range** *range-value*}

no ve {**id** | **range**}

Syntax Description

id *id-value*	ID value of the VE device. The range is from 1 to 16384.
range *range-value*	ID range value of the VE device. The range is from 11 to 512.

Command Default

No VE ID value or ID range value is specified.

Command Modes

L2VPN VFI autodiscovery configuration (config-vfi-autodiscovery)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

The **ve id** *id-value* command specifies the local VE identifier for the VFI for a VPLS configuration.

The VE ID identifies a VFI within a VPLS service. This means that VFIs in the same VPLS service cannot share the same VE ID. The scope of the VE ID is only within a bridge domain. Therefore, VFIs in different bridge domains within a PE can still use the same VE ID.

The **ve range** *range-value* command overrides the minimum size of the VE block. The default minimum size is 10. Any configured VE range must be higher than 10.

Examples

The following example specifies the VE with the ID value of 1001:

```
Device(config-vfi-autodiscovery)# ve id 1001
```

The following example specifies an ID range of 12:

```
Device(config-vfi-autodiscovery)# ve range 12
```

Related Commands

Command	Description
autodiscovery (MPLS)	Designates a Layer 2 VFI as having BGP autodiscovered pseudowire members.