BGP Policy Accounting

Border Gateway Protocol (BGP) policy accounting measures and classifies IP traffic that is sent to, or received from, different peers. Policy accounting is enabled on an input interface, and counters based on parameters such as community list, autonomous system number, or autonomous system path are assigned to identify the IP traffic.

- Finding Feature Information, on page 1
- Prerequisites, on page 1
- Information About BGP Policy Accounting, on page 2
- How to Configure BGP Policy Accounting, on page 3
- Configuration Examples for BGP Policy Accounting, on page 6
- Additional References, on page 7
- Feature Information for BGP Policy Accounting, on page 8

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites

Before using the BGP Policy Accounting feature, you must enable BGP and CEF or dCEF on the router.

Information About BGP Policy Accounting

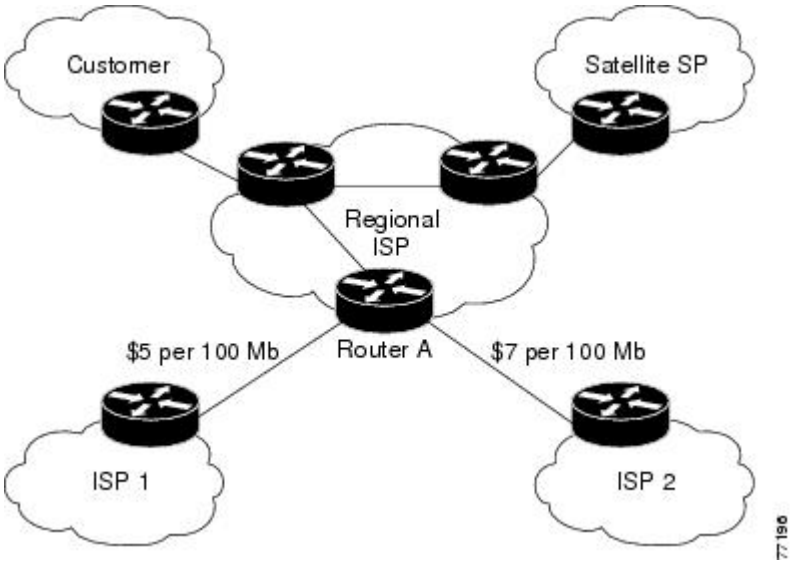
BGP Policy Accounting Overview

Border Gateway Protocol (BGP) policy accounting measures and classifies IP traffic that is sent to, or received from, different peers. Policy accounting is enabled on an input interface, and counters based on parameters such as community list, autonomous system number, or autonomous system path are assigned to identify the IP traffic.

Using the BGP **table-map** command, prefixes added to the routing table are classified by BGP attribute, autonomous system number, or autonomous system path. Packet and byte counters are incremented per input interface. A Cisco IOS policy-based classifier maps the traffic into one of eight possible buckets, representing different traffic classes.

Using BGP policy accounting, you can account for traffic according to the route it traverses. Service providers (SPs) can identify and account for all traffic by customer and bill accordingly. In the figure below, BGP policy accounting can be implemented in Router A to measure packet and byte volumes in autonomous system buckets. Customers are billed appropriately for traffic that is routed from a domestic, international, or satellite source.

Figure 1: Sample Topology for BGP Policy Accounting



BGP policy accounting using autonomous system numbers can be used to improve the design of network circuit peering and transit agreements between Internet service providers (ISPs).

Benefits of BGP Policy Accounting

Account for IP Traffic Differentially

BGP policy accounting classifies IP traffic by autonomous system number, autonomous system path, or community list string, and increments packet and byte counters. Service providers can account for traffic and apply billing, according to the route specific traffic traverses.

Efficient Network Circuit Peering and Transit Agreement Design

Implementing BGP policy accounting on an edge router can highlight potential design improvements for peering and transit agreements.

How to Configure BGP Policy Accounting

Specifying the Match Criteria for BGP Policy Accounting

The first task in configuring BGP policy accounting is to specify the criteria that must be matched. Community lists, autonomous system paths, or autonomous system numbers are examples of BGP attributes that can be specified and subsequently matched using a route map.

To specify the BGP attribute to use for BGP policy accounting and create the match criteria in a route map, use the following commands in global configuration mode:

SUMMARY STEPS

1. Device(config)# **ip community-list** *community-list-number* {**permit** | **deny**} *community-number*
2. Device(config)# **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
3. Device(config-route-map)# **match community-list** *community-list-number* [**exact**]
4. Device(config-route-map)# **set traffic-index** *bucket-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device(config)# **ip community-list** *community-list-number* {**permit** | **deny**} *community-number*	Creates a community list for BGP and controls access to it. This step must be repeated for each community to be specified.
Step 2	Device(config)# **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]	Enters route-map configuration mode and defines the conditions for policy routing. The *map-name* argument identifies a route map. The optional **permit** and **deny** keywords work with the match and set criteria to control how the packets are accounted for.

	Command or Action	Purpose
		The optional *sequence-number* argument indicates the position a new route map is to have in the list of route maps already configured with the same name.
Step 3	Device(config-route-map)# **match community-list** *community-list-number* [**exact**]	Matches a BGP community.
Step 4	Device(config-route-map)# **set traffic-index** *bucket-number*	Indicates where to output packets that pass a match clause of a route map for BGP policy accounting.

Classifying the IP Traffic and Enabling BGP Policy Accounting

After a route map has been defined to specify match criteria, you must configure a way to classify the IP traffic before enabling BGP policy accounting.

Using the **table-map** command, BGP classifies each prefix it adds to the routing table based on the match criteria. When the **bgp-policy accounting** command is configured on an interface, BGP policy accounting is enabled.

To classify the IP traffic and enable BGP policy accounting, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Device(config)# **router bgp** *as-number*
2. Device(config-router)# **table-map** *route-map-name*
3. Device(config-router)# **network** *network-number* [**mask** *network-mask*]
4. Device(config-router)# **neighbor** *ip-address* **remote-as** *as-number*
5. Device(config-router)# **exit**
6. Device(config)# **interface** *interface-type interface-number*
7. Device(config-if)# **no ip directed-broadcast**
8. Device(config-if)# **ip address** *ip-address mask*
9. Device(config-if)# **bgp-policy accounting**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device(config)# **router bgp** *as-number*	Configures a BGP routing process and enters router configuration mode for the specified routing process.
Step 2	Device(config-router)# **table-map** *route-map-name*	Classifies BGP prefixes entered in the routing table.
Step 3	Device(config-router)# **network** *network-number* [**mask** *network-mask*]	Specifies a network to be advertised by the BGP routing process.
Step 4	Device(config-router)# **neighbor** *ip-address* **remote-as** *as-number*	Specifies a BGP peer by adding an entry to the BGP routing table.
Step 5	Device(config-router)# **exit**	Exits to global configuration mode.

	Command or Action	Purpose
Step 6	Device(config)# **interface** *interface-type interface-number*	Specifies the interface type and number and enters interface configuration mode.
Step 7	Device(config-if)# **no ip directed-broadcast**	Configures the interface to drop directed broadcasts destined for the subnet to which that interface is attached, rather than being broadcast. This is a security issue.
Step 8	Device(config-if)# **ip address** *ip-address mask*	Configures the interface with an IP address.
Step 9	Device(config-if)# **bgp-policy accounting**	Enables BGP policy accounting for the interface.

Verifying BGP Policy Accounting

To verify that BGP policy accounting is operating, perform the following steps:

SUMMARY STEPS

1. Enter the **show ip cef** EXEC command with the **detail** keyword to learn which accounting bucket is assigned to a specified prefix.
2. Enter the **show ip bgp** EXEC command for the same prefix used in Step 1--192.168.5.0-- to learn which community is assigned to this prefix.
3. Enter the **show cef interface policy-statistics** EXEC command to display the per-interface traffic statistics.

DETAILED STEPS

Step 1 Enter the **show ip cef** EXEC command with the **detail** keyword to learn which accounting bucket is assigned to a specified prefix.

In this example, the output is displayed for the prefix 192.168.5.0. It shows that the accounting bucket number 4 (traffic_index 4) is assigned to this prefix.

Example:

```
Device# show ip cef 192.168.5.0 detail

192.168.5.0/24, version 21, cached adjacency to POS7/2
0 packets, 0 bytes, traffic_index 4
  via 10.14.1.1, 0 dependencies, recursive
   next hop 10.14.1.1, POS7/2 via 10.14.1.0/30
   valid cached adjacency
```

Step 2 Enter the **show ip bgp** EXEC command for the same prefix used in Step 1--192.168.5.0-- to learn which community is assigned to this prefix.

In this example, the output is displayed for the prefix 192.168.5.0. It shows that the community of 100:197 is assigned to this prefix.

Example:

```
Device# show ip bgp 192.168.5.0

BGP routing table entry for 192.168.5.0/24, version 2
```

```
Paths: (1 available, best #1)
  Not advertised to any peer
  100
    10.14.1.1 from 10.14.1.1 (32.32.32.32)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Community: 100:197
```

Step 3 Enter the **show cef interface policy-statistics** EXEC command to display the per-interface traffic statistics.

In this example, the output shows the number of packets and bytes that have been assigned to each accounting bucket:

Example:

```
Device# show cef interface policy-statistics

POS7/0 is up (if_number 8)
Bucket    Packets               Bytes
1          0                     0
2          0                     0
3          50                    5000
4          100                   10000
5          100                   10000
6          10                    1000
7          0                     0
8          0                     0
```

Monitoring and Maintaining BGP Policy Accounting

Command	Purpose
`Device# show cef interface [type number] policy-statistics`	(Optional) Displays detailed CEF policy statistical information for all interfaces.
`Device# show ip bgp [network] [network mask] [longer-prefixes]`	(Optional) Displays entries in the BGP routing table.
`Device# show ip cef [network [mask]] [detail]`	(Optional) Displays entries in the Forwarding Information Base (FIB) or FIB summary information.

Configuration Examples for BGP Policy Accounting

Example: Specifying the Match Criteria for BGP Policy Accounting

In the following example, BGP communities are specified in community lists, and a route map named set_bucket is configured to match each of the community lists to a specific accounting bucket using the **set traffic-index** command:

```
ip community-list 30 permit 100:190
```

```
ip community-list 40 permit 100:198
ip community-list 50 permit 100:197
ip community-list 60 permit 100:296
!
route-map set_bucket permit 10
match community 30
set traffic-index 2
!
route-map set_bucket permit 20
match community 40
set traffic-index 3
!
route-map set_bucket permit 30
match community 50
set traffic-index 4
!
route-map set_bucket permit 40
match community 60
set traffic-index 5
```

Example: Classifying the IP Traffic and Enabling BGP Policy Accounting

In the following example, BGP policy accounting is enabled on POS interface 7/0 and the **table-map** command is used to modify the bucket number when the IP routing table is updated with routes learned from BGP:

```
router bgp 65000
 table-map set_bucket
 network 10.15.1.0 mask 255.255.255.0
 neighbor 10.14.1.1 remote-as 65100
!
ip classless
ip bgp-community new-format
!
interface POS7/0
 ip address 10.15.1.2 255.255.255.0
 no ip directed-broadcast
 bgp-policy accounting
 no keepalive
 crc 32
 clock source internal
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
BGP commands	Cisco IOS IP Routing: BGP Command Reference
Cisco Express Forwarding (CEF) and distributed CEF (dCEF) commands	Cisco IOS IP Switching Command Reference
Cisco Express Forwarding (CEF) and distributed CEF (dCEF) configuration information	"CEF Overview" module of the *Cisco IOS Switching Services Configuration Guide*

MIBs

MIB	MIBs Link
• CISCO-BGP-POLICY-ACCOUNTING-MIB **Note** CISCO-BGP-POLICY-ACCOUNTING-MIB is only available in the Cisco IOS Release 12.0(9)S, 12.0(17)ST, and later releases. This MIB is not available on any mainline and T-train release.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for BGP Policy Accounting

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for BGP Policy Accounting

Feature Name	Releases	Feature Information
BGP Policy Accounting	12.0(9)S 12.0(17)ST 12.2(13)T 15.0(1)S 12.2(50)SY Cisco IOS XE Release 3.8S	Border Gateway Protocol (BGP) policy accounting measures and classifies IP traffic that is sent to, or received from, different peers. Policy accounting is enabled on an input interface, and counters based on parameters such as community list, autonomous system number, or autonomous system path are assigned to identify the IP traffic. The following commands were introduced or modified: • **bgp-policy** • **set traffic-index** • **show cef interface policy-statistics** • **show ip bgp** • **show ip cef**