BGP Policy Accounting Output Interface Accounting

Border Gateway Protocol (BGP) policy accounting (PA) measures and classifies IP traffic that is sent to, or received from, different peers. Policy accounting was previously available on an input interface only. The BGP Policy Accounting Output Interface Accounting feature introduces several extensions to enable BGP PA on an output interface and to include accounting based on a source address for both input and output traffic on an interface. 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, page 1
- Prerequisites for BGP PA Output Interface Accounting, page 2
- Information About BGP PA Output Interface Accounting, page 2
- How to Configure BGP PA Output Interface Accounting, page 3
- Configuration Examples for BGP PA Output Interface Accounting, page 10
- Additional References, page 10
- Feature Information for BGP Policy Accounting Output Interface Accounting, page 12

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 for BGP PA Output Interface Accounting

Before using the BGP Policy Accounting Output Interface Accounting feature, you must enable BGP and Cisco Express Forwarding or distributed CEF on the router.
Information About BGP PA Output Interface Accounting

BGP PA Output Interface Accounting

Policy accounting using BGP measures and classifies IP traffic that is sent to, or received from, different peers. Originally, BGP PA was available on an input interface only. BGP PA output interface accounting introduces several extensions to enable BGP PA on an output interface and to include accounting based on a source address for both input and output traffic on an interface. 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 or output interface. A Cisco policy-based classifier maps the traffic into one of eight possible buckets that represent different traffic classes.

Using BGP PA, you can account for traffic according to its origin or the route it traverses. Service providers (SPs) can identify and account for all traffic by customer and can bill accordingly. In the figure below, BGP PA 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 PA Output Interface Accounting

Accounting 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. Policy accounting can also be based on the source address. Service providers can account for traffic and apply billing according to the origin of the traffic or the route that 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 PA Output Interface Accounting

Specifying the Match Criteria for BGP PA
The first task in configuring BGP PA 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. Perform this task to specify the BGP attribute to use for BGP PA and to create the match criteria in a route map.

SUMMARY STEPS
1. enable
2. configure terminal
3. ip community-list {standard-list-number | expanded-list-number [regular-expression] | {standard | expanded} community-list-name} {permit | deny} {community-number | regular-expression}
4. route-map map-name [permit | deny] [sequence-number]
5. match community-list community-list-number [exact]
6. set traffic-index bucket-number
7. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Example: Device# configure terminal</td>
</tr>
<tr>
<td>3</td>
<td>ip community-list {standard-list-number</td>
</tr>
<tr>
<td></td>
<td>expanded-list-number[regular-expression]}</td>
</tr>
<tr>
<td></td>
<td>{standard</td>
</tr>
<tr>
<td></td>
<td>expanded}; community-list-name {permit</td>
</tr>
<tr>
<td></td>
<td>deny}</td>
</tr>
<tr>
<td></td>
<td>{community-number</td>
</tr>
<tr>
<td></td>
<td>regular-expression}</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# ip community-list 30 permit 100:190</td>
</tr>
<tr>
<td>4</td>
<td>route-map map-name {permit</td>
</tr>
<tr>
<td></td>
<td>deny}</td>
</tr>
<tr>
<td></td>
<td>[sequence-number]</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# route-map set_bucket permit 10</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>match community-list community-list-number [exact]</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config-route-map)# match community-list 30</td>
</tr>
<tr>
<td>6</td>
<td>set traffic-index bucket-number</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-route-map)# set traffic-index 2</td>
</tr>
<tr>
<td>7</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-route-map)# exit</td>
</tr>
</tbody>
</table>
Classifying the IP Traffic and Enabling BGP PA

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 that it adds to the routing table according to the match criteria. When the `bgp-policy accounting` command is configured on an interface, BGP policy accounting is enabled.

Perform this task to classify the IP traffic and enable BGP policy accounting.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `router bgp as-number`
4. `table-map route-map-name`
5. `network network-number [mask network-mask]`
6. `neighbor ip-address remote-as as-number`
7. `exit`
8. `interface type number`
9. `ip address ip-address mask`
10. `bgp-policy accounting [input | output] [source]`
11. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1. **Step 1** | enable | Enables privileged EXEC mode.  
Example:  
Device> enable |
| 2. **Step 2** | configure terminal | Enters global configuration mode.  
Example:  
Device# configure terminal |
| 3. **Step 3** | router bgp as-number | Configures a BGP routing process and enters router configuration mode for the specified routing process.  
Example:  
Device(config)# router bgp 65000 |

- Enter your password if prompted.
- The `as-number` argument identifies a BGP autonomous system number.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><code>table-map route-map-name</code></td>
<td>Classifies BGP prefixes entered in the routing table.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-router)# table-map set_bucket</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>network network-number [mask network-mask]</code></td>
<td>Specifies a network to be advertised by the BGP routing process.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-router)# network 10.15.1.0 mask 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>neighbor ip-address remote-as as-number</code></td>
<td>Specifies a BGP peer by adding an entry to the BGP routing table.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-router)# neighbor 10.14.1.1 remote-as 65100</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>exit</code></td>
<td>Exits router configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> Device(config-router)# exit</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>interface type number</code></td>
<td>Specifies the interface type and number and enters interface configuration mode.</td>
</tr>
</tbody>
</table>
|       | **Example:** Device(config)# interface POS 7/0 | - The `type` argument identifies the type of interface.  
- The `number` argument identifies the slot and port numbers of the interface. The space between the interface type and number is optional. |
| 9     | `ip address ip-address mask` | Configures the interface with an IP address. |
|       | **Example:** Device(config-if)# ip-address 10.15.1.2 255.255.255.0 | |
| 10    | `bgp-policy accounting [input | output] [source]` | Enables BGP policy accounting for the interface. |
|       | **Example:** Device(config-if)# bgp-policy accounting input source | - Use the optional `input` or `output` keyword to account for traffic either entering or leaving the router. By default, BGP policy accounting is based on traffic entering the router.  
- Use the optional `source` keyword to account for traffic based on source address. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exits interface configuration mode and returns to global configuration mode.</td>
</tr>
</tbody>
</table>

**Verifying BGP Policy Accounting**

Perform this task to verify that BGP policy accounting is operating.

**SUMMARY STEPS**

1. `show ip cef [network [mask]] [detail]`
2. `show ip bgp [network] [network-mask] [longer-prefixes]`
3. `show cef interface [type number] policy-statistics [input | output]`
4. `show cef interface [type number] [statistics] [detail]`

**DETAILED STEPS**

**Step 1**

`show ip cef [network [mask]] [detail]`

Enter the `show ip cef` 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 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**

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

Enter the `show ip bgp` 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
```
Step 3  **show cef interface**  [type number]  **policy-statistics**  [input | output]

Displays 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 input
FastEthernet1/0/0 is up (if_number 6)
Corresponding hwidb fast_if_number 6
Corresponding hwidb firstsaw->if_number 6
BGP based Policy accounting on input is enabled
Index Packets Bytes
1  9999 999900
2  0 0
3  0 0
4  0 0
5  0 0
6  0 0
7  0 0
8  0 0
9  0 0
10  0 0
11  0 0
12  0 0
13  0 0
14  0 0
15  0 0
16  0 0
17  0 0
18  0 0
19  0 0
20  0 0
21  0 0
22  0 0
23  0 0
24  0 0
25  0 0
26  0 0
27  0 0
28  0 0
29  0 0
30  0 0
31  0 0
32  0 0
33  0 0
34  1234 123400
35  0 0
36  0 0
37  0 0
38  0 0
39  0 0
40  0 0
41  0 0
42  0 0
43  0 0
44  0 0
45  1000 100000
46  0 0
```
Step 4  `show cef interface [type number] [statistics] [detail]`
Displays the state of BGP policy accounting on a specified interface.

In this example, the output shows that BGP policy accounting has been configured to be based on input traffic at Fast Ethernet interface 1/0/0:

Example:

```
Device# show cef interface Fast Ethernet 1/0/0

FastEthernet1/0/0 is up (if_number 6)
Corresponding hwidb fast_if_number 6
Corresponding hwidb firstsw->if_number 6
Internet address is 10.1.1.1/24
ICMP redirects are always sent
Per packet load-sharing is disabled
IP unicast RPF check is disabled
Inbound access list is not set
Outbound access list is not set
IP policy routing is disabled
BGP based policy accounting on input is enabled
BGP based policy accounting on output is disabled
Hardware idb is FastEthernet1/0/0 (6)
Software idb is FastEthernet1/0/0 (6)
Fast switching type 1, interface type 18
IP Distributed CEF switching enabled
IP Feature Fast switching turbo vector
IP Feature CEF switching turbo vector
Input fast flags 0x100, Output fast flags 0x0, Flags 0x0
ifindex 7(7)
Slot 1 Slot unit 0 VC -1
Transmit limit accumulator 0xE8001A82 (0xE8001A82)
IP MTU 1500
```
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:

```plaintext
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:

```plaintext
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

The following sections provide references related to BGP policy accounting.
Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP commands: complete command syntax, command mode, defaults, usage guidelines, and examples</td>
<td>Cisco IOS IP Routing: BGP Command Reference</td>
</tr>
<tr>
<td>Switching commands: complete command syntax, command mode, defaults, usage guidelines, and examples</td>
<td>Cisco IOS IP Switching Command Reference</td>
</tr>
<tr>
<td>CEF and dCEF configuration information</td>
<td>IP Switching Cisco Express Forwarding Configuration Guide</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-BGP-POLICY-ACCOUNTING-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Link</td>
</tr>
</tbody>
</table>

Feature Information for BGP Policy Accounting Output Interface 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.
BGP Policy Accounting Output Interface Accounting

Table 1: Feature Information for BGP Policy Accounting Output Interface Accounting

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Policy Accounting Output Interface Accounting</td>
<td>12.0(9)S</td>
<td>BGP policy accounting (PA) measures and classifies IP traffic that is sent to, or received from, different peers. Policy accounting was previously available on an input interface only. The BGP Policy Accounting Output Interface Accounting feature introduces several extensions to enable BGP PA on an output interface and to include accounting based on a source address for both input and output traffic on an interface. Counters based on parameters such as community list, autonomous system number, or autonomous system path are assigned to identify the IP traffic.</td>
</tr>
<tr>
<td></td>
<td>12.0(17)ST</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.3(4)T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 2.1</td>
<td></td>
</tr>
</tbody>
</table>

The following commands were introduced or modified:

- `bgp-policy`
- `set traffic-index`
- `show cef interface`
- `show cef interface policy statistics`