



Flexible NetFlow - Top N Talkers Support

This document contains information about and instructions for using the Flexible NetFlow - Top N Talkers Support feature. The Flexible NetFlow - Top N Talkers Support feature helps you analyze the large amount of data that Flexible NetFlow captures from the traffic in your network by providing the ability to filter, aggregate, and sort the data in the Flexible NetFlow cache as you display it. When you are sorting and displaying the data in the cache, you can limit the display output to a specific number of entries with the highest values (Top N Talkers) for traffic volume, packet counters, and so on. The Flexible NetFlow - Top N Talkers Support feature facilitates real-time traffic analysis by requiring only the use of **show** commands, which can be entered in many different variations using the available keywords and arguments to meet your traffic data analysis requirements.

NetFlow is a Cisco technology that provides statistics on packets flowing through the router. NetFlow is the standard for acquiring IP operational data from IP networks. NetFlow provides data to support network and security monitoring, network planning, traffic analysis, and IP accounting.

Flexible NetFlow improves on original NetFlow by adding the capability to customize the traffic analysis parameters for your specific requirements. Flexible NetFlow facilitates the creation of more complex configurations for traffic analysis and data export through the use of reusable configuration components.

- [Finding Feature Information, on page 1](#)
- [Prerequisites for Flexible NetFlow - Top N Talkers Support, on page 2](#)
- [Information About Flexible NetFlow - Top N Talkers Support, on page 2](#)
- [How to Analyze Network Traffic Using Flexible NetFlow Top N Talkers, on page 3](#)
- [Configuration Examples for Flexible NetFlow Top N Talkers, on page 7](#)
- [Additional References, on page 7](#)
- [Feature Information for Flexible NetFlow - Top N Talkers, 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.

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 Flexible NetFlow - Top N Talkers Support

- The networking device is running a Cisco release that supports the Flexible NetFlow - Top N Talkers Support feature.

No configuration tasks are associated with the Flexible NetFlow - Top N Talkers Support feature. Therefore, in order for you to use the Flexible NetFlow - Top N Talkers Support feature, traffic analysis with Flexible NetFlow must already be configured on the networking device.

Information About Flexible NetFlow - Top N Talkers Support

Flexible NetFlow Data Flow Filtering

The flow filtering function of the Flexible NetFlow - Top N Talkers Support feature filters the flow data in a flow monitor cache based on the criteria that you specify, and displays the data.

The flow filtering function of the Flexible NetFlow - Top N Talkers Support feature is provided by the **show flow monitor cache filter** command. For more information on the **show flow monitor cache filter** command, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

Flow Sorting and Top N Talkers

The flow sorting function of the Flexible NetFlow - Top N Talkers Support feature sorts flow data from the Flexible NetFlow cache based on the criteria that you specify and displays the data. You can also use the flow sorting function of the Flexible NetFlow - Top N Talkers Support feature to limit the display output to a specific number of entries (top *n* talkers, where *n* is the number of talkers to display) by using the **top** keyword of the **show flow monitor cache sort** command.

The flow sorting and Top N Talkers function of the Flexible NetFlow - Top N Talkers Support feature is provided by the **show flow monitor cache sort** command. For more information on the **show flow monitor cache sort** command, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

Combined Use of Flow Filtering and Flow Sorting with Top N Talkers

where *options* is any permissible combination of arguments and keywords. See the "Configuration Examples for Flexible NetFlow - Top N Talkers Support " section for more information.

Memory and Performance Impact of Top N Talkers

The Flexible NetFlow - Top N Talkers Support feature can use a large number of CPU cycles and possibly also system memory for a short time. However, because the Flexible NetFlow - Top N Talkers Support feature uses only **show** commands, the CPU usage should be run at a low priority because no real-time data processing is involved. The memory usage can be mitigated by using a larger granularity of aggregation or no aggregation at all.

How to Analyze Network Traffic Using Flexible NetFlow Top N Talkers

Filtering Flow Data from the Flexible NetFlow Cache

This task shows you how to use the **show flow monitor cache filter** command with a regular expression to filter the flow monitor cache data and display the results. For more information on regular expressions and the **show flow monitor cache filter** command, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

Perform this task to filter the flow monitor cache data using a regular expression and display the results.

SUMMARY STEPS

1. **enable**
2. **show flow monitor** [name] *monitor-name* **cache filter**]] [format {csv | record | table}]

DETAILED STEPS

Step 1 **enable**

Enters privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show flow monitor** [name] *monitor-name* **cache filter**]] [format {csv | record | table}]

Filters the flow monitor cache data on the IPv4 type of service (ToS) value.

Example:

Sorting Flow Data from the Flexible NetFlow Cache

This task shows you how to use the **show flow monitor cache sort** command to sort the flow monitor cache data, and display the results. For more information on the **show flow monitor cache sort** command, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

Perform this task to sort the flow monitor cache data and display the results.

SUMMARY STEPS

1. **enable**
2. **show flow monitor** [name] *monitor-name* **cache sort options** [top [number]] [format {csv | record | table}]

DETAILED STEPS

Step 1 enable

Enters privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 show flow monitor [name] monitor-name cache sort options [top [number]] [format {csv | record | table}]

Displays the cache data sorted on the number of packets from highest to lowest.

Note When the **top** keyword is not used, the default number of sorted flows shown is 20.

Example:

```
Device# show flow monitor FLOW-MONITOR-1 cache sort highest counter packets
```

```
Processed 26 flows
Aggregated to 26 flows
Showing the top 20 flows
IPV4 SOURCE ADDRESS:    10.1.1.3
IPV4 DESTINATION ADDRESS: 172.16.10.11
TRNS SOURCE PORT:      443
TRNS DESTINATION PORT: 443
INTERFACE INPUT:      Et0/0.1
FLOW SAMPLER ID:      0
IP TOS:                0x00
IP PROTOCOL:          6
ip source as:         0
ip destination as:    0
ipv4 next hop address: 172.16.7.2
ipv4 source mask:     /0
ipv4 destination mask: /24
tcp flags:            0x00
interface output:     Et1/0.1
counter bytes:        22760
counter packets:      1569
timestamp first:      19:42:32.924
timestamp last:       19:57:28.656
IPV4 SOURCE ADDRESS:    10.10.11.2
IPV4 DESTINATION ADDRESS: 172.16.10.6
TRNS SOURCE PORT:      65
TRNS DESTINATION PORT: 65
INTERFACE INPUT:      Et0/0.1
FLOW SAMPLER ID:      0
IP TOS:                0x00
IP PROTOCOL:          6
ip source as:         0
ip destination as:    0
ipv4 next hop address: 172.16.7.2
ipv4 source mask:     /0
ipv4 destination mask: /24
tcp flags:            0x00
interface output:     Et1/0.1
counter bytes:        22720
counter packets:      568
timestamp first:      19:42:34.264
timestamp last:       19:57:28.428
```

```

.
.
.
IPV4 SOURCE ADDRESS:      192.168.67.6
IPV4 DESTINATION ADDRESS: 172.16.10.200
TRNS SOURCE PORT:        0
TRNS DESTINATION PORT:   3073
INTERFACE INPUT:         Et0/0.1
FLOW SAMPLER ID:         0
IP TOS:                   0x00
IP PROTOCOL:              1
ip source as:             0
ip destination as:       0
ipv4 next hop address:    172.16.7.2
ipv4 source mask:         /0
ipv4 destination mask:   /24
tcp flags:                0x00
interface output:        Et1/0.1
counter bytes:            15848
counter packets:         344
timestamp first:         19:42:36.852
timestamp last:          19:57:27.836
IPV4 SOURCE ADDRESS:      10.234.53.1
IPV4 DESTINATION ADDRESS: 172.16.10.2
TRNS SOURCE PORT:        0
TRNS DESTINATION PORT:   2048
INTERFACE INPUT:         Et0/0.1
FLOW SAMPLER ID:         0
IP TOS:                   0x00
IP PROTOCOL:              1
ip source as:             0
ip destination as:       0
ipv4 next hop address:    172.16.7.2
ipv4 source mask:         /0
ipv4 destination mask:   /24
tcp flags:                0x00
interface output:        Et1/0.1
counter bytes:            15848
counter packets:         213
timestamp first:         19:42:36.904
timestamp last:          19:57:27.888

```

Displaying the Top N Talkers with Sorted Flow Data

This task shows you how to use the **show flow monitor cache sort** command to sort the flow monitor cache data, and to limit the display results to a specific number of high volume flows. For more information on the **show flow monitor cache sort** command, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

Perform this task to sort the flow monitor cache data and limit the display output using to a specific number of high volume flows.

SUMMARY STEPS

1. **enable**
2. **show flow monitor** [name] *monitor-name* **cache sort options** [top [number]] [format {csv | record | table}]

DETAILED STEPS

Step 1 enable

Enters privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 show flow monitor [name] monitor-name cache sort options [top [number]] [format {csv | record | table}]

Displays the cache data sorted on the number of packets from highest to lowest and limits the output to the three highest volume flows.

Example:

```
Device# show flow monitor FLOW-MONITOR-1 cache sort highest counter packets top 3
```

```
Processed 25 flows
Aggregated to 25 flows
Showing the top 3 flows
IPV4 SOURCE ADDRESS:      10.1.1.3
IPV4 DESTINATION ADDRESS: 172.16.10.11
TRNS SOURCE PORT:         443
TRNS DESTINATION PORT:    443
INTERFACE INPUT:          Et0/0.1
FLOW SAMPLER ID:          0
IP TOS:                    0x00
IP PROTOCOL:               6
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /0
ipv4 destination mask:    /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             32360
counter packets:           1897
timestamp first:           19:42:32.924
timestamp last:            20:03:47.100
IPV4 SOURCE ADDRESS:      10.10.11.2
IPV4 DESTINATION ADDRESS: 172.16.10.6
TRNS SOURCE PORT:         65
TRNS DESTINATION PORT:    65
INTERFACE INPUT:          Et0/0.1
FLOW SAMPLER ID:          0
IP TOS:                    0x00
IP PROTOCOL:               6
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /0
ipv4 destination mask:    /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             32360
counter packets:           809
timestamp first:           19:42:34.264
timestamp last:            20:03:48.460
IPV4 SOURCE ADDRESS:      172.16.1.84
```

```

IPV4 DESTINATION ADDRESS: 172.16.10.19
TRNS SOURCE PORT:      80
TRNS DESTINATION PORT: 80
INTERFACE INPUT:       Et0/0.1
FLOW SAMPLER ID:       0
IP TOS:                 0x00
IP PROTOCOL:           6
ip source as:          0
ip destination as:     0
ipv4 next hop address: 172.16.7.2
ipv4 source mask:      /24
ipv4 destination mask: /24
tcp flags:             0x00
interface output:      Et1/0.1
counter bytes:         32320
counter packets:       345
timestamp first:       19:42:34.512
timestamp last:        20:03:47.140

```

Configuration Examples for Flexible NetFlow Top N Talkers

Example: Displaying the Top Talkers with Filtered and Sorted Flow Data

Example: Filtering Using Multiple Filtering Criteria

The following example filters the cache data on the IPv4 destination address and the destination port:

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Flexible NetFlow conceptual information and configuration tasks	<i>Flexible NetFlow Configuration Guide</i>
Flexible NetFlow commands	<i>Cisco IOS Flexible NetFlow Command Reference</i>

Standards/RFCs

Standard	Title
No new or modified standards/RFCs are supported by this feature.	—

MIBs

MIB	MIBs Link
None	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 Flexible NetFlow - Top N Talkers

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 Flexible NetFlow - Top N Talkers

Feature Name	Releases	Feature Information
Flexible NetFlow - Top N Talkers Support		<p>This feature helps you analyze the large amount of data Flexible NetFlow captures from the traffic in your network by providing the ability to filter, aggregate, and sort the data in the Flexible NetFlow cache as you display it.</p> <p>Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE.</p> <p>The following commands were introduced or modified: show flow monitor cache aggregate, show flow monitor cache filter, show flow monitor cache.</p>