Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands

Last Updated: April 1, 2012

This module contains information about and instructions for configuring NetFlow Top Talkers feature. The NetFlow Top Talkers feature can be configured using the Cisco IOS command-line interface (CLI) or with SNMP commands using the NetFlow MIB. The NetFlow Top Talkers feature uses NetFlow functionality to obtain information regarding heaviest traffic patterns and most-used applications in the network. The NetFlow MIB allows you to configure NetFlow and the NetFlow Top Talkers feature using SNMP commands from a network management workstation.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 Configuring NetFlow Top Talkers

Before you enable NetFlow and NetFlow Top Talkers, you must:

- Configure the router for IP routing
- Ensure that one of the following is enabled on your router, and on the interfaces that you want to configure NetFlow on: Cisco Express Forwarding (CEF), distributed CEF, or fast switching
- Understand the resources required on your router because NetFlow consumes additional memory and CPU resources.

Restrictions for Configuring NetFlow Top Talkers

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later the **ip flow ingress** command is used to enable NetFlow on an interface.

Cisco IOS Release 12.2(33)SXH

Some of the keywords and arguments for the commands used to configure the NetFlow MIB and Top Talkers feature are not supported in 12.2(33)SXH. See the syntax descriptions for the commands in the command reference (URL for the 12.2SX NF CR to be added later) for details.

Information About Configuring NetFlow Top Talkers

Overview of the NetFlow MIB and Top Talkers Feature

NetFlow collects traffic flow statistics on routing devices. NetFlow has been used for a variety of applications, including traffic engineering, usage-based billing, and monitoring for denial-of-service (DoS) attacks.

The flows that are generating the heaviest system traffic are known as the "top talkers."

The NetFlow Top Talkers feature allows flows to be sorted so that they can be viewed. The top talkers can be sorted by either of the following criteria:

- By the total number of packets in each top talker
- By the total number of bytes in each top talker

The usual implementation of NetFlow exports NetFlow data to a collector. The NetFlow MIB and Top Talkers feature performs security monitoring and accounting for top talkers and matches and identifies key users of the network. This feature is also useful for a network location where a traditional NetFlow export

operation is not possible. The NetFlow MIB and Top Talkers feature does not require a collector to obtain information regarding flows. Instead, these flows are placed in a special cache where they can be viewed. The NetFlow MIB part of the NetFlow MIB and Top Talkers feature allows you to configure the NetFlow Top Talkers feature using SNMP.

In addition to sorting top talkers, you can further organize your output by specifying criteria that the top talkers must match, such as source or destination IP address or port. The **match** command is used to specify this criterion. For a full list of the matching criteria that you can select, refer to the **match**command in the Cisco IOS command reference documentation.

Benefits of the NetFlow MIB and Top Talkers Feature

Top talkers can be useful for analyzing network traffic in any of the following ways:

- Security--You can view the list of top talkers to see if traffic patterns consistent with DoS attack are present in your network.
- Load balancing--You can identify the most heavily used parts of the system and move network traffic over to less-used parts of the system.
- Traffic analysis--Consulting the data retrieved from the NetFlow MIB and Top Talkers feature can assist you in general traffic study and planning for your network.

An additional benefit of the NetFlow MIB and Top Talkers feature is that it can be configured for a router either by entering CLI commands or by entering SNMP commands on a network management system (NMS) workstation. The SNMP commands are sent to the router and processed by a MIB. You do not have to be connected to the router console to extract the list of top talkers information if an NMS workstation is configured to communicate using SNMP to your network device. For more information on configuring your network device to use MIB functionality for the NetFlow MIB and Top Talkers feature, see Configuring SNMP Support on the Networking Device, page 4.

Cisco IOS Release 12.2(33)SXH on Cisco 6500 Series Switches

The **show ip flow top-talkers** command was modified in Cisco IOS Release 12.2(33)SXH for the Cisco 6500 Series switches to support displaying the top talkers for a specific module. The **show ip flow top-talkers module** *number* command displays the top talkers for that module. The **show ip flow top-talkers** command without the module keyword shows the top talkers in the hardware switched path (a merged list of top lists from all modules) and then software switched top talkers. The NetFlow MIB can be used to request the top talker list and to set and/or get the configuration parameters for the NetFlow MIB Top Talkers feature.

How to Configure NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands

Note   Some of the tasks in this section include examples of the SNMP CLI syntax used to set configuration parameters on the router and to read values from MIB objects on the router. These SNMP CLI syntax examples are taken from a Linux workstation using public-domain SNMP tools. The SNMP CLI syntax for your workstation might be different. Refer to the documentation that was provided with your SNMP tools for the correct syntax for your network management workstation.

Configuring SNMP Support on the Networking Device

If you want to configure the NetFlow Top Talkers feature using the Cisco IOS CLI, you do not have to perform this task.

If you want to configure the NetFlow Top Talkers feature using the NetFlow MIB and SNMP, you must perform this task.

Before you can use SNMP commands to configure the Top Talkers feature you must configure SNMP support on your networking device. To enable SNMP support on the networking device perform the steps in this task.

Note   The SNMP community read-only (RO) string for the examples is **public**. The SNMP community read-write (RW) string for the examples is **private**. You should use more complex strings for these values in your configurations.

Note   For more information on configuring SNMP support on your networking device, refer to the "Configuring SNMP Support" chapter of the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide* .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string* **ro**
4. **snmp-server community** *string* **rw**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	(Required) Enters global configuration mode.
Step 3	**snmp-server community** *string* **ro** **Example:** Router(config)# snmp-server community public ro	(Required) Sets up the community access string to permit access to SNMP. • The *string* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string. • The **ro** keyword specifies read-only access. SNMP management stations using this string can retrieve MIB objects.
Step 4	**snmp-server community** *string* **rw** **Example:** Router(config)# snmp-server community private rw	(Required) Sets up the community access string to permit access to SNMP. • The *string* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string. • The **rw** keyword specifies read-write access. SNMP management stations using this string can retrieve and modify MIB objects. **Note** The *string* argument must be different from the read-only *string* argument specified in the preceding step (Step 3).
Step 5	**end** **Example:** Router(config)# end	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring Parameters for the NetFlow Main Cache

This optional task describes the procedure for modifying the parameters for the NetFlow main cache. Perform the steps in this optional task using either the router CLI commands or the SNMP commands to modify the parameters for the NetFlow main cache.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-cache entries** *number*
4. **ip flow-cache timeout active** *minutes*
5. **ip flow-cache timeout inactive** *seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**ip flow-cache entries** *number* **Example:** `Router(config)# ip flow-cache entries 4000`	(Optional) Specifies the maximum number of entries to be captured for the main flow cache. • The range for the *number* argument is from 1024 to 524288 entries.
Step 4	**ip flow-cache timeout active** *minutes* **Example:** `Router(config)# ip flow-cache timeout active 30`	(Optional) Configures operational parameters for the main cache. • The **timeout** keyword dissolves the session in the cache. • The **active** *minutes* keyword-argument pair is the number of minutes that an entry is active. The range is from 1 to 60 minutes. The default is 30 minutes.
Step 5	**ip flow-cache timeout inactive** *seconds* **Example:** `Router(config)# ip flow-cache timeout inactive 100`	(Optional) Configures operational parameters for the main cache. • The **timeout** keyword dissolves the session in the main cache. • The **inactive** *seconds* keyword-argument pair is the number of seconds that an inactive entry will stay in the main cache before it times out. The range is from 10 to 600 seconds. The default is 15 seconds.

	Command or Action	Purpose
Step 6	**end**	(Required) Exits the current configuration mode and returns to privileged EXEC mode.
	Example:	
	`Router(config)# end`	

Configuring Parameters for the NetFlow Main Cache

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCICacheEntries.type unsigned** *number*
2. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCIActiveTimeOut.type unsigned** *number*
3. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] c**cnfCIInactiveTimeOut.type unsigned** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c private -m all -v2c** [*ip-address*	*hostname*] **cnfCICacheEntries.type unsigned** *number*	(Optional) Defines the maximum number of entries to be captured for the main flow cache.
		• The value for the *type* argument in **cnfCICacheEntries**.*type* **unsigned** *number* is 0 for the main cache.
	Example:	• The value for the *number* argument in **cnfCICacheEntries**.*type number* is the maximum number of cache entries.

	`workstation% snmpset -c private -m all -`
	`v2c 10.4.9.62 cnfCICacheEntries.0`
	`unsigned 4000`
		• The range for the *number* argument is from 1024 to 524288 entries.

Step 2	**snmpset -c private -m all -v2c** [*ip-address*	*hostname*] **cnfCIActiveTimeOut.type unsigned** *number*	(Optional) Specifies the number of seconds that an active flow remains in the main cache before it times out.
		• The value for the *type* argument in **cnfCIActiveTimeout**.*type* **unsigned** *number* is 0 for the main cache.
	Example:	• The value for the *number* argument in **cnfCIActiveTimeout**.*type* **unsigned** *number* is the number of seconds that an active flow remains in the cache before it times out.

	`workstation% snmpset -c private -m all -`
	`v2c 10.4.9.62 cnfCIActiveTimeOut.0`
	`unsigned 60`
		• The range for the *number* argument is from 1 to 60 minutes. The default is 30 minutes.

	Command or Action	Purpose
Step 3	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] c**cnfCIInactiveTimeOut.type unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCIInactiveTimeOut.0 unsigned 30`	(Optional) Specifies the number of seconds that an inactive flow remains in the main cache before it times out. • The value for the *type* argument in **cnfCIInactiveTimeout**.*type* **unsigned** *number* is 0 for the main cache. • The value for the *number* argument in **cnfCIInactiveTimeout**.*type* **unsigned** *number* is the number of seconds that an inactive flow remains in the main cache before it times out. • The range for the *number* argument is from 10 to 600 seconds. The default is 15 seconds.

Identifying the Interface Number to Use for Enabling NetFlow with SNMP

If you want to configure the NetFlow Top Talkers feature using the Cisco IOS CLI, you do not have to perform this task.

If you want to configure the NetFlow Top Talkers feature using the NetFlow MIB and SNMP, you must perform this task.

Before you can use SNMP to enable NetFlow on an interface, you must identify the SNMP interface number on the router. To identify the interface number for the interface on which you want to enable NetFlow, perform the steps in this required task.

SUMMARY STEPS

1. **enable**
2. **show snmp mib ifmib ifindex** *type number*
3. Repeat Step 2 to identify the SNMP interface number for any other interfaces on which you plan to enable NetFlow.

DETAILED STEPS

Step 1   **enable**
Enters privileged EXEC mode. Enter the password if prompted.

Example:

`Router> ` **`enable`**

Step 2   **show snmp mib ifmib ifindex** *type number*
Displays the SNMP interface number for the interface specified.

Example:

```
Router# show snmp mib ifmib ifindex GigabitEthernet6/2
Ethernet0/0: Ifindex = 60
```

Step 3   Repeat Step 2 to identify the SNMP interface number for any other interfaces on which you plan to enable NetFlow.

Configuring NetFlow on a Cisco 6500 Series Switch

To enable NetFlow on the switch, perform the steps in this required task using either the CLI commands or the SNMP commands.

Note   This task provides the minimum information required to configure NetFlow on your Cisco 6500 series switch. See the Catalyst 6500 Series Cisco IOS Software Configuration Guide, for more information of configuring NetFlow on your switch.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mls flow** {**ip** | **ipv6**} {**destination** | **destination-source** | **full** | **interface-destination-source** | **interface-full** | **source**}
4. **interface** *type number*
5. **ip flow** {**ingress** | **egress**}
6. **exit**
7. Repeat Steps 4 through 6 to enable NetFlow on other interfaces.
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.

Command or Action	Purpose
Step 3 **mls flow** {**ip** | **ipv6**} {**destination** | **destination-source** | **full** | **interface-destination-source** | **interface-full** | **source**} **Example:** Router(config)# mls flow ip interface-full	Specifies the NetFlow flow mask for IPv4 traffic.
Step 4 **interface** *type number* **Example:** Router(config)# interface GigabitEthernet6/2	(Required) Specifies the interface on which you want to enable NetFlow and enters interface configuration mode.
Step 5 **ip flow** {**ingress** | **egress**} **Example:** Router(config-if)# ip flow ingress **Example:** **Example:** and/or **Example:** Router(config-if)# ip flow egress	(Required) Enables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface • **egress** --Captures traffic that is being transmitted by the interface.
Step 6 **exit** **Example:** Router(config-if)# exit	(Optional) Exits interface configuration mode and returns to global configuration mode. • Use this command only if you want to enable NetFlow on another interface.
Step 7 Repeat Steps 4 through 6 to enable NetFlow on other interfaces.	(Optional) --
Step 8 **end** **Example:** Router(config-if)# end	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring NetFlow on a Cisco 6500 Series Switch

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cseFlowIPFlowMask integer** [**1** | **2** | **3** | **4** | **5** | **6**]

2. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCINetflowEnable**.*interface-number* **integer** [**0** | **1** | **2** | **3**]

3. Repeat Step 2 to enable NetFlow on other interfaces

DETAILED STEPS

	Command or Action	Purpose

Step 1	**snmpset -c private -m all -v2c** [*ip-address*	*hostname*] **cseFlowIPFlowMask integer** [**1**	**2**	**3**	**4**	**5**	**6**]
							
							Example:
							
							`workstation% snmpset -c private -m all -v2c 10.4.9.62`
							`cnfCINetflowEnable.60 integer 1`
								Specifies the NetFlow flow mask for IPv4 traffic.
								
								• 1--destination-only
								• 2--source-destination
								• 3--full-flow
								• 4--source-only
								• 5--interface-source-destination
								• 6--interface-full

Step 2	**snmpset -c private -m all -v2c** [*ip-address*	*hostname*] **cnfCINetflowEnable**.*interface-number* **integer** [**0**	**1**	**2**	**3**]
					
					Example:
					
					`workstation% snmpset -c private -m all -v2c 10.4.9.62`
					`cnfCINetflowEnable.60 integer 1`
						(Required) Configures NetFlow for an interface.
						
						• The value for the *interface-number* argument is found by entering the router CLI command **show snmp mib ifmib ifindex** on the router in privileged EXEC mode.
						• The values for the *direction* argument are:
						   ◦ 0--Disable NetFlow
						   ◦ 1--Enable Ingress NetFlow
						   ◦ 2--Enable Egress NetFlow
						   ◦ 3--Enable Ingress and Egress NetFlow

Step 3	Repeat Step 2 to enable NetFlow on other interfaces	(Optional) --

Configuring NetFlow on Cisco Routers

To enable NetFlow on the router, perform the steps in this required task using either the CLI commands or the SNMP commands .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip flow** {**ingress** | **egress**}
5. **exit**
6. Repeat Steps 3 through 5 to enable NetFlow on other interfaces.
7. **end**

DETAILED STEPS

Command or Action	Purpose
Step 1 **enable** **Example:** Router> enable	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2 **configure terminal** **Example:** Router# configure terminal	(Required) Enters global configuration mode.
Step 3 **interface** *type number* **Example:** Router(config)# interface GigabitEthernet6/2	(Required) Specifies the interface on which you want to enable NetFlow and enters interface configuration mode.

Command or Action	Purpose

Step 4 **ip flow** {**ingress**	**egress**}
	
	Example:
	
	Router(config-if)# ip flow ingress
	
	Example:
	
	Example:
	
	and/or
	
	Example:
	
	Router(config-if)# ip flow egress
		(Required) Enables NetFlow on the interface.
		
		  • **ingress** --Captures traffic that is being received by the interface
		  • **egress** --Captures traffic that is being transmitted by the interface.

Step 5 **exit** **Example:** Router(config-if)# exit	(Optional) Exits interface configuration mode and returns to global configuration mode. • Use this command only if you want to enable NetFlow on another interface.
Step 6 Repeat Steps 3 through 5 to enable NetFlow on other interfaces.	(Optional) --
Step 7 **end** **Example:** Router(config-if)# end	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring NetFlow on Cisco Routers

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] cnfCINetflowEnable.*interface-number* **integer** [**0** | **1** | **2** | **3**]
2. Repeat Step 1 to enable NetFlow on other interfaces

DETAILED STEPS

	Command or Action	Purpose

Step 1	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] cnfCINetflowEnable.*interface-number* **integer** [**0** | **1** | **2** | **3**]
	
	Example:
	
	`workstation% snmpset -c private -m all -v2c`
	`10.4.9.62 cnfCINetflowEnable.60 integer 1`
		(Required) Configures NetFlow for an interface.
		
		• The value for the *interface-number* argument is found by entering the router CLI command **show snmp mib ifmib ifindex** on the router in privileged EXEC mode.
		• The values for the *direction* argument are:
		
		◦ 0--Disable NetFlow
		◦ 1--Enable Ingress NetFlow
		◦ 2--Enable Egress NetFlow
		◦ 3--Enable Ingress and Egress NetFlow

Step 2	Repeat Step 1 to enable NetFlow on other interfaces	(Optional) --

Configuring NetFlow Top Talkers

This task describes the procedure for configuring the NetFlow Top Talkers feature. Perform the steps in this required task using either the router CLI commands or the SNMP commands to configure the NetFlow Top Talkers feature on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-top-talkers**
4. **top** *number*
5. **sort-by** [**bytes** \| **packets**
6. **cache-timeout** *milliseconds*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**ip flow-top-talkers** **Example:** `Router(config)# ip flow-top-talkers`	(Required) Enters NetFlow Top Talkers configuration mode.
Step 4	**top** *number* **Example:** `Router(config-flow-top-talkers)# top 50`	(Required) Specifies the maximum number of top talkers that will be retrieved by a NetFlow top talkers query. • The range for the *number* argument is from 1 to 200 entries.
Step 5	**sort-by** [**bytes** | **packets** **Example:** `Router(config-flow-top-talkers)# sort-by packets`	(Required) Specifies the sort criterion for the top talkers. • The top talkers can be sorted either by the total number of packets of each top talker or the total number of bytes of each top talker.
Step 6	**cache-timeout** *milliseconds* **Example:** `Router(config-flow-top-talkers)# cache-timeout 30000`	(Optional) Specifies the amount of time that the list of top talkers is retained. • Reentering the **top**, **sort-by**, or **cache-timeout** command resets the timeout period, and the list of top talkers is recalculated the next time they are requested. • The list of top talkers is lost when the timeout period expires. You should configure a timeout period for at least as long as it takes the network management system (NMS) to retrieve all the required NetFlow top talkers. • If this timeout value is too large, the list of top talkers might not be updated quickly enough to display the latest top talkers. If a request to display the top talkers is made more than once during the timeout period, the same results will be displayed for each request. To ensure that the latest information is displayed while conserving CPU time, configure a large value for the timeout period and change the parameters of the **cache-timeout**, **top**, or **sort-by** command when a new list of top talkers is required. • The range for the *number* argument is from 1 to 3,600,000 milliseconds. The default is 5000 (5 seconds).

Command or Action	Purpose
Step 7 **end** **Example:** `Router(config-flow-top-talkers)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring NetFlow Top Talkers

SUMMARY STEPS

1. **snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsTopN.0 unsigned** *number*
2. **snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsSortBy.0 integer** [**1** | **2** | **3**]
3. **snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsCacheTimeout.0 unsigned** *milliseconds*

DETAILED STEPS

Command or Action	Purpose
Step 1 **snmpset -c** *private* **-m all -v2c** [*ip-address*	*hostname*] **cnfTopFlowsTopN.0 unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsTopN.0 unsigned 50`	(Required) Specifies the maximum number of top talkers that will be retrieved by a NetFlow top talkers query. • The value for the *number* argument in **cnfTopFlowsTopN.0** *number* is the maximum number of top talkers that will be retrieved by a NetFlow top talkers query. • The range for the *number* argument is from 1 to 200 entries.

Step 2 **snmpset -c** *private* **-m all -v2c** [*ip-address*	*hostname*] **cnfTopFlowsSortBy.0 integer** [**1**	**2**	**3**]
			
			Example:
			
			`workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsSortBy.0 integer 2`
				(Required) Specifies the sort criteria for the top talkers.
				
				• Values for *sort-option* in **cnfTopFlowsSortBy.0** [**1**
					2	**3**] are
						
						   ○ 1--No sorting will be performed and that the NetFlow MIB and Top Talkers feature will be disabled.
						   ○ 2--Sorting will be performed by the total number of packets of each top talker.
						   ○ 3--Sorting will be performed by the total number of bytes of each top talker.

Command or Action	Purpose
Step 3 **snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsCacheTimeout.0 unsigned** *milliseconds* **Example:** ```workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsCacheTimeout.0 unsigned 30000```	(Optional) Specifies the amount of time that the list of top talkers is retained. • Reentering the **top**, **sort-by**, or **cache-timeout** command resets the timeout period, and the list of top talkers is recalculated the next time they are requested. • The list of top talkers will be lost when the timeout period expires. You should configure a timeout period for at least as long as it takes the network management system (NMS) to retrieve all the required NetFlow top talkers. • If this timeout value is too large, the list of top talkers might not be updated quickly enough to display the latest top talkers. If a request to display the top talkers is made more than once during the timeout period, the same results will be displayed for each request. To ensure that the latest information is displayed while conserving CPU time, configure a large value for the timeout period and change the parameters of the **cache-timeout**, **top**, or **sort-by** command when a new list of top talkers is required. • The range for the *number* argument is from 1 to 3,600,000 milliseconds. The default is 5000 (5 seconds).

Configuring NetFlow Top Talkers Match Criteria

You can limit the traffic that is displayed by the NetFlow Top Talkers feature by configuring match criteria. The match criteria are applied to data in the main cache. The data in the main cache that meets the match criteria is displayed when you enter the **show ip flow top-talkers** command. To limit the traffic that is displayed by the NetFlow MIB and Top Talkers feature, perform the steps in this optional task.

Before configuring NetFlow MIB and Top Talkers match criteria, you should understand the following:

NetFlow Top Talkers Match Criteria Specified by CLI Commands

You can use the **match** CLI command to specify match criteria to restrict the display of top talkers for the NetFlow MIB and Top Talkers feature. If you do not provide matching criteria, all top talkers are displayed.

Note   When configuring a matching source, destination or nexthop address, both the address and a mask must be configured. The configuration will remain unchanged until both have been specified.

Note   **cnfTopFlowsMatchSampler** matches flows from a named flow sampler. **cnfTopFlowsMatchClass** matches flows from a named class map.

Note   When you are configuring the Top Talkers feature to match bytes and packets, the values that are matched are the total number of bytes and packets in the flow so far. For example, it is possible to match flows containing a specific number of packets, or flows with more or less than a set number of bytes.

For more information on using the match command, see the Cisco IOS NetFlow Command Reference.

NetFlow Top Talkers Match Criteria Specified by SNMP Commands

If you are using SNMP commands to configure NetFlow Top Talkers, see the table below for router CLI commands and equivalent SNMP commands.

Note   Some of the SNMP match criteria options, such as the **cnfTopFlowsMatchSrcAddress** option, require that you enter more than one SNMP commands on the same line. For example, **snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsMatchSrcAddressType.0 integer 1 cnfTopFlowsMatchSrcAddress.0 decimal 172.16.10.0 cnfTopFlowsMatchSrcAddressMask.0 unsigned 24**.

Table 1   ***Router CLI Commands and Equivalent SNMP Commands***

Router CLI Command	SNMP Command
match source address [*ip-address*] [*mask* | */nn*]	**cnfTopFlowsMatchSrcAddress decimal** *ip-address*
	cnfTopFlowsMatchSrcAddressType integer *type* [1]
	cnfTopFlowsMatchSrcAddressMask unsigned *mask*
match destination address [*ip-address*][*mask* | */nn*]	**cnfTopFlowsMatchDstAddress decimal** *ip-address*
	cnfTopFlowsMatchDstAddressType integer *type1*
	cnfTopFlowsMatchDstAddressMask unsigned *mask*

---

[1] The only IP version type that is currently supported is IPv4 (type 1).

Router CLI Command	SNMP Command
match nexthop address [*ip-address*][*mask* | */nn*]	**cnfTopFlowsMatchNhAddress decimal** *ip-address*
	cnfTopFlowsMatchNhAddressType integer *type1*
	cnfTopFlowsMatchNhAddressMask unsigned *mask*
match source port min *port*	**cnfTopFlowsMatchSrcPortLo integer** *port*
match source port max *port*	**cnfTopFlowsMatchSrcPortHi integer** *port*
match destination port min *port*	**cnfTopFlowsMatchDstPortLo integer** *port*
match destination port max *port*	**cnfTopFlowsMatchDstPortHi integer** *port*
match source as *as-number*	**cnfTopFlowsMatchSrcAS integer** *as-number*
match destination as *as-number*	**cnfTopFlowsMatchDstAS integer** *as-number*
match input-interface *interface*	**cnfTopFlowsMatchInputIf integer** *interface*
match output-interface *interface*	**cnfTopFlowsMatchOutputIf integer** *interface*
match tos [*tos-value* | **dscp** *dscp-value* | **precedence** *precedence-value*]	**cnfTopFlowsMatchTOSByte integer** *tos-value* [2]
match protocol [*protocol-number* | **tcp** | **udp**]	**cnfTopFlowsMatchProtocol integer** *protocol-number*
match flow-sampler *flow-sampler-name*	**cnfTopFlowsMatchSampler string** *flow-sampler-name*
match class-map *class*	**cnfTopFlowsMatchClass string** *class*
match packet-range min *minimum-range*	**cnfTopFlowsMatchMinPackets unsigned** *minimum-range*
match packet-range max *maximum-range*	**cnfTopFlowsMatchMaxPackets unsigned** *maximum-range*
match byte-range min *minimum-range*	**cnfTopFlowsMatchMinBytes unsigned** *minimum-range*
match byte-range max *maximum-range*	**cnfTopFlowsMatchMaxPackets unsigned** *maximum-range*

Configuring Source IP Address Top Talkers Match Criteria

Perform the steps in this optional task using either the router CLI commands or the SNMP commands to add source IP address match criteria to the Top Talkers configuration.

---

2 tos-value is 6 bits for DSCP, 3 bits for precedence, and 8 bits (one byte) for ToS.

For information on configuring other Top Talkers match criteria see the following resources:

- Cisco IOS NetFlow Command Reference.
- CISCO-NETFLOW-MIB at the following URL: http://www.cisco.com/go/mibs/ . Select SNMP Object Locator. Then select View & Download MIBs.

You must configure NetFlow Top Talkers before you perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-top-talkers**
4. **match source address** {*ip-address/nn* | *ip-address mask*}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	(Required) Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	(Required) Enters global configuration mode.
Step 3	**ip flow-top-talkers** **Example:** Router(config)# ip flow-top-talkers	(Required) Enters NetFlow Top Talkers configuration mode.

	Command or Action	Purpose

Step 4	**match source address** {*ip-address/nn* | *ip-address mask*}
	
	Example:
	
	`Router(config-flow-top-talkers)#`
	`match source address`
	`172.16.10.0`
	`/24`
		(Required) Specifies a match criterion.
		
		• The **source address** keyword specifies that the match criterion is based on the source IP address.
		• The *ip-address* argument is the IP address of the source, destination, or next-hop address to be matched.
		• The *mask* argument is the address mask, in dotted decimal format.
		• The */nn* argument is the address mask as entered in CIDR format. The **match source address** *172.16.10.0/24* is equivalent to the **match source address** *172.16.10.0 255.255.255.0* command.
		
		Note You must configure at least one of the possible match criteria before matching can be used to limit the traffic that is displayed by the NetFlow Top Talkers feature. Additional match criteria are optional.
		
		Note For a full list of the matching criteria that you can select, refer to NetFlow Top Talkers Match Criteria Specified by CLI Commands, page 17.

Step 5	**end** **Example:** `Router(config-flow-top-talkers)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring Source IP Address Top Talkers Match Criteria

SUMMARY STEPS

1. **snmpset -c** *private* **-m all -v2c** [*ip-address* \| *hostname*] **cnfTopFlowsMatchSrcAddressType.0 integer 1 cnfTopFlowsMatchSrcAddress.0 decimal** *ip-address* **cnfTopFlowsMatchSrcAddressMask.0 unsigned** *mask*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c** *private* **-m all -v2c** [*ip-address | hostname*] **cnfTopFlowsMatchSrcAddressType. 0 integer 1 cnfTopFlowsMatchSrcAddress.0 decimal** *ip-address* **cnfTopFlowsMatchSrcAddressMask.0 unsigned** *mask* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsMatchSrcAddressType.0 integer 1 cnfTopFlowsMatchSrcAddress.0 decimal 172.16.10.0 cnfTopFlowsMatchSrcAddressMask.0 unsigned 24`	(Required) Specifies a match criterion. • The IP address type of 1 in the **cnfTopFlowsMatchSrcAddressType.0 integer 1** command specifies an IP version 4 (IPv4) address for the IP address type. IPv4 is currently the only IP version that is supported. • The *ip-address* argument in **cnfTopFlowsMatchSrcAddress.0 decimal** *ip-address* is the IPv4 source IP address to match in the traffic that is being analyzed. • The *mask* argument in **cnfTopFlowsMatchSrcAddressMask.0 unsigned** *mask* is the number of bits in the mask for the IPv4 source IP address to match in the traffic that is being analyzed. **Note** You must configure at least one of the possible match criteria before matching can be used to limit the traffic that is displayed by the Top talkers feature. Additional match criteria are optional. **Note** To remove the **cnfTopFlowsMatchSrcAddress** match criterion from the configuration, specify an IP address type of 0 (unknown) with the cnfTopFlowsMatchSrcAddressType.0 integer 0 command. **Note** For a list of router CLI commands and their corresponding SNMP commands, see Configuring Source IP Address Top Talkers Match Criteria, page 21.

Verifying the NetFlow Top Talkers Configuration

To verify the NetFlow Top Talkers configuration, perform the steps in this optional task using either the router CLI command or the SNMP commands.

SUMMARY STEPS

1. **show ip flow top-talkers**

DETAILED STEPS

show ip flow top-talkers
Use this command to verify that the NetFlow MIB and Top Talkers feature is operational. For example:

Example:

```
Router# show ip flow top-talkers
SrcIf          SrcIPaddress   DstIf       DstIPaddress    Pr SrcP DstP Bytes
Et3/0          10.1.1.3       Local       10.1.1.2        01 0000 0000  4800
Et3/0          10.1.1.4       Local       10.1.1.2        01 0000 0000  4800
```

```
Et3/0         10.1.1.5        Local        10.1.1.2        01 0000 0000  800
3 of 10 top talkers shown. 3 flows processed.
```

Verifying the NetFlow Top Talkers Configuration

In this example, even though a maximum of ten top talkers is configured by the **top** command, only three top talkers were transmitting data in the network. Therefore, three top talkers are shown, and the "3 flows processed" message is displayed in the output. If you expect more top talkers to be displayed than are being shown, this condition may possibly be the result of matching criteria, specified by the **match** command, that are overly restrictive.

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsGenerate.0 integer 1**
2. **snmpget -c public -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsReportAvailable**
3. **snmpwalk -c public -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsTable**

DETAILED STEPS

Step 1   **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsGenerate.0 integer 1**
Use this command to initiate a generation of the top talkers statistics:

Example:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsGenerate.0 integer 1
CISCO-NETFLOW-MIB::cnfTopFlowsGenerate.0 = INTEGER: true(1)
```

Step 2   **snmpget -c public -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsReportAvailable**
Use this command to verify that the top talkers statistics are available:

Example:

```
workstation% snmpwalk -c public -m all -v2c 10.4.9.62 cnfTopFlowsReportAvailable
CISCO-NETFLOW-MIB::cnfTopFlowsReportAvailable.0 = INTEGER: true(1)
```

Step 3   **snmpwalk -c public -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsTable**
Use this command to display the NetFlow top talkers:

Example:

```
workstation% snmpwalk -c public -m all -v2c 10.4.9.62 cnfTopFlowsTable
CISCO-NETFLOW-MIB::cnfTopFlowsSrcAddressType.1 = INTEGER: ipv4(1)
CISCO-NETFLOW-MIB::cnfTopFlowsSrcAddress.1 = Hex-STRING: 0A 04 09 08
CISCO-NETFLOW-MIB::cnfTopFlowsSrcAddressMask.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsDstAddressType.1 = INTEGER: ipv4(1)
CISCO-NETFLOW-MIB::cnfTopFlowsDstAddress.1 = Hex-STRING: 0A 04 09 A7
CISCO-NETFLOW-MIB::cnfTopFlowsDstAddressMask.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsNhAddressType.1 = INTEGER: ipv4(1)
CISCO-NETFLOW-MIB::cnfTopFlowsNhAddress.1 = Hex-STRING: 00 00 00 00
CISCO-NETFLOW-MIB::cnfTopFlowsSrcPort.1 = Gauge32: 32773
```

```
CISCO-NETFLOW-MIB::cnfTopFlowsDstPort.1 = Gauge32: 161
CISCO-NETFLOW-MIB::cnfTopFlowsSrcAS.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsDstAS.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsInputIfIndex.1 = INTEGER: 1
CISCO-NETFLOW-MIB::cnfTopFlowsOutputIfIndex.1 = INTEGER: 0
CISCO-NETFLOW-MIB::cnfTopFlowsFirstSwitched.1 = Timeticks: (12073160) 1 day, 9:32:11.60
CISCO-NETFLOW-MIB::cnfTopFlowsLastSwitched.1 = Timeticks: (12073160) 1 day, 9:32:11.60
CISCO-NETFLOW-MIB::cnfTopFlowsTOS.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsProtocol.1 = Gauge32: 17
CISCO-NETFLOW-MIB::cnfTopFlowsTCPFlags.1 = Gauge32: 16
CISCO-NETFLOW-MIB::cnfTopFlowsSamplerID.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsClassID.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsFlags.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsBytes.1 = Gauge32: 75
CISCO-NETFLOW-MIB::cnfTopFlowsPackets.1 = Gauge32: 1
```

Tip You must convert the source and destination IP addresses from hexadecimal to dotted decimal format used in the display output before you can correlate them to source and destination hosts on your network. For example, in the display output above: 0A 04 09 02 = 10.4.9.2 and 0A 04 09 AF = 10.4.9.175.

Configuration Examples for NetFlow Top Talkers

Configuring NetFlow Top Talkers Using SNMP Commands Example

The following output from the network management workstation shows the command and the response for enabling NetFlow on interface GigabitEthernet6/2 (ifindex number 60):

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCINetflowEnable.60 integer 1
CISCO-NETFLOW-MIB::cnfCINetflowEnable.60 = INTEGER: interfaceDirIngress(1)
```

The following output from the network management workstation shows the command and the response for specifying 5 as the maximum number of top talkers that will be retrieved by a NetFlow top talkers query:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsTopN.0 unsigned 5
CISCO-NETFLOW-MIB::cnfTopFlowsTopN.0 = Gauge32: 5
```

The following output from the network management workstation shows the command and the response for specifying the sort criteria for the top talkers:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsSortBy.0 integer 2
CISCO-NETFLOW-MIB::cnfTopFlowsSortBy.0 = INTEGER: byPackets(2)
```

The following output from the network management workstation shows the command and the response for specifying the amount of time that the list of top talkers is retained:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsCacheTimeout.0 unsigned
2000
CISCO-NETFLOW-MIB::cnfTopFlowsCacheTimeout.0 = Gauge32: 2000 milliseconds
```

Configuring NetFlow Top Talkers Match Criteria Using SNMP Commands Example

The following output from the network management workstation shows the **snmpset** command and the response for specifying the following NetFlow Top Talkers match criteria:

- Source IP address-172.16.23.0
- Source IP address mask-255.255.255.0 (/24)
- IP address type-IPv4

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsMatchSrcAddress.0
decimal 172.16.23.0 cnfTopFlowsMatchSrcAddressMask.0 unsigned 24
cnfTopFlowsMatchSrcAddressType.0 integer 1
CISCO-NETFLOW-MIB::cnfTopFlowsMatchSrcAddress.0 = Hex-STRING: AC 10 17 00
CISCO-NETFLOW-MIB::cnfTopFlowsMatchSrcAddressMask.0 = Gauge32: 24
CISCO-NETFLOW-MIB::cnfTopFlowsMatchSrcAddressType.0 = INTEGER: ipv4(1)
```

The following output from the network management workstation shows the **snmpset** command and the response for specifying the class-map *my-class-map* as aNetFlow Top Talkers match criterion:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsMatchClass.0 s my-class-
map
CISCO-NETFLOW-MIB::cnfTopFlowsMatchClass.0 = STRING: my-class-map.
```

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	Getting Started with Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring Random Sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches

Related Topic	Document Title
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for configuring NetFlow multicast support	Configuring NetFlow Multicast Accounting
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
CISCO-NETFLOW-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL (requires CCO login account): http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Configuring NetFlow Top Talkers using the Cisco IOS CLI or SNMP Commands

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 2   *Feature Information for Configuring NetFlow Top Talkers using the Cisco IOS CLI or SNMP Commands*

Feature Name	Releases	Feature Configuration Information
NetFlow MIB	12.3(7)T, 12.2(25)S 12.2(27)SBC	The NetFlow MIB feature provides MIB objects to allow users to monitor NetFlow cache information, the current NetFlow configuration, and statistics. The following command was introduced by this feature: **ip flow-cache timeout**.

Feature Name	Releases	Feature Configuration Information
NetFlow MIB and Top Talkers	12.3(11)T, 12.2(25)S 12.2(27)SBC 12.2(33)SXH	The NetFlow MIB feature that was originally released in Cisco IOS Release12.3(7)T was modified in Cisco IOS Release 12.3(11)T to support the new NetFlow Top Talkers feature. The modifications to the NetFlow MIB and the new Top Talkers feature were released under the feature name NetFlow MIB and Top Talkers. The NetFlow MIB and Top Talkers feature uses NetFlow functionality to obtain information regarding heaviest traffic patterns and most-used applications (top talkers) in the network. The NetFlow MIB component of the NetFlow MIB and Top Talkers feature enables you to configure top talkers and view the top talker statistics using SNMP. The following commands were introduced by this feature: **cache-timeout**, **ip flow-top-talkers**, **match**, **show ip flow top-talkers**, **sort-by**, and **top**.