



# Configuring Accounting for IPv6 Layer 2 Bridged Traffic

---

This document contains information about and instructions for configuring sampling to reduce the CPU overhead of analyzing traffic with Flexible NetFlow.

NetFlow is a Cisco technology that provides statistics on packets flowing through a 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 Monitoring IPv6 Bridged Flows, on page 1](#)
- [Information About Monitoring IPv6 Layer 2 Bridged Traffic, on page 2](#)
- [How to Configure the Monitoring of IPv6 Layer 2 Bridged Traffic, on page 2](#)
- [Configuration Examples for Monitoring IPv6 Layer 2 Bridged Traffic, on page 9](#)
- [Additional References, on page 12](#)
- [Feature Information for Configuring Accounting for IPv6 Layer 2 Bridged Traffic, on page 13](#)

## 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.

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

## Prerequisites for Monitoring IPv6 Bridged Flows

- The networking device must be running a Cisco release release that supports Flexible NetFlow.
- The networking device must be configured for IPv6 routing.

- One of the following must be enabled on your router and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding IPv6 or distributed Cisco Express Forwarding IPv6.
- You have configured a flow record, flow monitor, flow exporter, and flow sampler.

## Information About Monitoring IPv6 Layer 2 Bridged Traffic

This feature expands the **ipv6 flow monitor** command to include a **layer2-bridged** keyword that enables you to configure Flexible Netflow to monitor IPv6 Layer 2 bridged traffic on both Switched Virtual Interfaces (SVIs) and VLANs, with or without flow samplers.

## How to Configure the Monitoring of IPv6 Layer 2 Bridged Traffic

Only the keywords and arguments required for the Flexible NetFlow commands used in these tasks are explained in these tasks. For information about the other keywords and arguments available for these Flexible NetFlow commands, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

## Configuring a Flow Record, Flow Monitor, and Exporter to Monitor IPv6 Layer 2 Bridged Traffic

To configure a flow record, flow monitor, and exporter to monitor IPv6 Layer 2 bridged traffic, perform this task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record *name***
4. **match datalink source-vlan-id**
5. **match flow cts destination group**
6. **match flow cts source group**
7. **match flow direction**
8. **match interface input**
9. **match interface input physical**
10. **match interface output**
11. **match ipv4 destination address**
12. **match ipv4 dscp**
13. **match ipv4 precedence**
14. **match ipv4 protocol**
15. **match ipv4 source address**
16. **match ipv4 tos**
17. **match transport destination-port**
18. **match transport source-port**
19. **collect counter bytes**

20. `collect counter packets`
21. `collect interface output`
22. `collect interface input`
23. `collect ipv4 destination mask`
24. `collect ipv4 destination prefix`
25. `collect ipv4 source mask`
26. `collect ipv4 source prefix`
27. `collect timestamp sys-uptime first`
28. `collect timestamp sys-uptime last`
29. `collect transport tcp flags`
30. `exit`
31. `flow exporter exporter-name`
32. `export-protocol netflow-v9`
33. `destination ip-address`
34. `exit`
35. `flow monitor name`
36. `record record-name`
37. `exporter exporter-name`
38. `end`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>flow record name</b> <b>Example:</b> Device(config)# flow record ipv6-bridged-traffic	Configures a flow record to monitor IPv6 bridged Layer 2 traffic and enters Flexible NetFlow flow record configuration mode.
Step 4	<b>match datalink source-vlan-id</b> <b>Example:</b> Device(config-flow-record)# match datalink source-vlan-id	Configures the source VLAN ID as a key field.
Step 5	<b>match flow cts destination group</b> <b>Example:</b> Device(config-flow-record)# match flow cts destination group	Configures the flow CTS destination group as a key field.

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 6</b>	<b>match flow cts source group</b> <b>Example:</b> <pre>Device(config-flow-record)# match flow cts source group</pre>	Configures the flow CTS source group as a key field.
<b>Step 7</b>	<b>match flow direction</b> <b>Example:</b> <pre>Device(config-flow-record)# match flow direction</pre>	Configures the flow direction as a key field.
<b>Step 8</b>	<b>match interface input</b> <b>Example:</b> <pre>Device(config-flow-record)# match interface input</pre>	Configures the input interface as a key field.
<b>Step 9</b>	<b>match interface input physical</b> <b>Example:</b> <pre>Device(config-flow-record)# match interface input physical</pre>	Configures the physical input interface as a key field.
<b>Step 10</b>	<b>match interface output</b> <b>Example:</b> <pre>Device(config-flow-record)# match interface input</pre>	Configures the output interface as a key field.
<b>Step 11</b>	<b>match ipv4 destination address</b> <b>Example:</b> <pre>Device(config-flow-record)# match ipv4 destination address</pre>	Configures the IPv4 destination address as a key field.
<b>Step 12</b>	<b>match ipv4 dscp</b> <b>Example:</b> <pre>Device(config-flow-record)# match ipv4 dscp</pre>	Configures the IPv4 DSCP as a key field.
<b>Step 13</b>	<b>match ipv4 precedence</b> <b>Example:</b> <pre>Device(config-flow-record)# match ipv4 precedence</pre>	Configures the IPv4 precedence as a key field.
<b>Step 14</b>	<b>match ipv4 protocol</b> <b>Example:</b> <pre>Device(config-flow-record)# match ipv4 protocol</pre>	Configures the IPv4 protocol as a key field.

	Command or Action	Purpose
<b>Step 15</b>	<b>match ipv4 source address</b> <b>Example:</b> <pre>Device(config-flow-record)# match ipv4 source address</pre>	Configures the IPv4 source address as a key field.
<b>Step 16</b>	<b>match ipv4 tos</b> <b>Example:</b> <pre>Device(config-flow-record)# match ipv4 tos</pre>	Configures the IPv4 TOS as a key field.
<b>Step 17</b>	<b>match transport destination-port</b> <b>Example:</b> <pre>Device(config-flow-record)# match transport destination-port</pre>	Configures the transport destination port as a key field.
<b>Step 18</b>	<b>match transport source-port</b> <b>Example:</b> <pre>Device(config-flow-record)# match transport source-port</pre>	Configures the transport source port as a key field.
<b>Step 19</b>	<b>collect counter bytes</b> <b>Example:</b> <pre>Device(config-flow-record)# collect counter bytes</pre>	Collects the total number of bytes.
<b>Step 20</b>	<b>collect counter packets</b> <b>Example:</b> <pre>Device(config-flow-record)# collect counter packets</pre>	Collects the total number of packets.
<b>Step 21</b>	<b>collect interface output</b> <b>Example:</b> <pre>Device(config-flow-record)# collect interface output</pre>	Collects the output interface.
<b>Step 22</b>	<b>collect interface input</b> <b>Example:</b> <pre>Device(config-flow-record)# collect interface input</pre>	Collects the input interface.
<b>Step 23</b>	<b>collect ipv4 destination mask</b> <b>Example:</b>	Collects the Ipv4 destination mask.

	Command or Action	Purpose
	Device(config-flow-record)# collect ipv4 destination mask	
<b>Step 24</b>	<b>collect ipv4 destination prefix</b> <b>Example:</b> Device(config-flow-record)# collect ipv4 destination prefix	Collects the Ipv4 destination prefix.
<b>Step 25</b>	<b>collect ipv4 source mask</b> <b>Example:</b> Device(config-flow-record)# collect ipv4 source mask	Collects the Ipv4 source mask.
<b>Step 26</b>	<b>collect ipv4 source prefix</b> <b>Example:</b> Device(config-flow-record)# collect ipv4 source prefix	Collects the Ipv4 source prefix.
<b>Step 27</b>	<b>collect timestamp sys-uptime first</b> <b>Example:</b> Device(config-flow-record)# collect timestamp sys-uptime first	Collects the first timestamp of the system uptime.
<b>Step 28</b>	<b>collect timestamp sys-uptime last</b> <b>Example:</b> Device(config-flow-record)# collect timestamp sys-uptime last	Collects the last timestamp of the system uptime.
<b>Step 29</b>	<b>collect transport tcp flags</b> <b>Example:</b> Device(config-flow-record)# collect transport tcp flags	Collects the TCP transport flags.
<b>Step 30</b>	<b>exit</b> <b>Example:</b> Device(config-flow-record)# exit	Exits Flexible NetFlow flow record configuration mode.

	Command or Action	Purpose
<b>Step 31</b>	<b>flow exporter</b> <i>exporter-name</i> <b>Example:</b> <pre>Device(config)# flow exporter my-flow-exporter</pre>	Creates an FNF flow exporter and enters Flexible NetFlow flow exporter configuration mode.
<b>Step 32</b>	<b>export-protocol</b> <b>netflow-v9</b> <b>Example:</b> <pre>Device(config-flow-exporter)# export-protocol netflow-v9</pre>	Configures NetFlow Version 9 export as the export protocol.
<b>Step 33</b>	<b>destination</b> <i>ip-address</i> <b>Example:</b> <pre>Device(config-flow-exporter)# destination 209.165.201.1</pre>	Configures the IP address of the workstation to which you want to send the NetFlow information.
<b>Step 34</b>	<b>exit</b> <b>Example:</b> <pre>Device(config-flow-exporter)# exit</pre>	Exits Flexible NetFlow flow exporter configuration mode.
<b>Step 35</b>	<b>flow monitor</b> <i>name</i> <b>Example:</b> <pre>Device(config)# flow monitor ipv6-bridged-traffic</pre>	Configures a flow monitor for IPv6 bridged traffic and enters Flexible NetFlow flow monitor configuration mode.
<b>Step 36</b>	<b>record</b> <i>record-name</i> <b>Example:</b> <pre>Device(config-flow-monitor)# record ipv6-bridged-traffic</pre>	Specifies the name of a user-defined flow record that was previously configured.
<b>Step 37</b>	<b>exporter</b> <i>exporter-name</i> <b>Example:</b> <pre>Device(config-flow-monitor)# exporter my-flow-exporter</pre>	Specifies the name of a flow exporter that was previously configured.
<b>Step 38</b>	<b>end</b> <b>Example:</b> <pre>Device(config-flow-monitor)# end</pre>	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.

## Applying a Flow Monitor to a Switched Virtual Interface to Monitor IPv6 Layer 2 Bridged Traffic

To configure Flexible Netflow to monitor IPv6 Layer 2 Bridged Traffic on a SVI, perform this task:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *vlan number*
4. **ipv6 flow monitor** *monitor-name* [**sampler** *monitor-name* ] **layer2-bridged input**
5. **end**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>vlan number</i> <b>Example:</b> Device(config)# interface vlan 100	Configures an interface type and enters interface configuration mode.
<b>Step 4</b>	<b>ipv6 flow monitor</b> <i>monitor-name</i> [ <b>sampler</b> <i>monitor-name</i> ] <b>layer2-bridged input</b> <b>Example:</b> Device(config-if)# ipv6 flow monitor ipv6-bridged-traffic sampler S1 layer2-bridged input	Applies the monitor to the interface.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

## Applying a Flow Monitor to a VLAN to Monitor IPv6 Layer 2 Bridged Traffic

To configure Flexible Netflow to monitor IPv6 Layer 2 Bridged Traffic on a VLAN, perform this task:



**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface** *vlan number*
4. **ipv6 flow monitor** *monitor-name* [**sampler** *monitor-name* ] **layer2-bridged input**
5. **end**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>vlan number</i>  <b>Example:</b> Device(config)# vlan configuration 100	Configures a VLAN and enters VLAN configuration mode.
<b>Step 4</b>	<b>ipv6 flow monitor</b> <i>monitor-name</i> [ <b>sampler</b> <i>monitor-name</i> ] <b>layer2-bridged input</b>  <b>Example:</b> Device(config-vlan)# ipv6 flow monitor ipv6-bridged-traffic sampler S1 layer2-bridged input	Applies the monitor to the VLAN.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> Device(config-vlan)# end	Exits VLAN configuration mode and returns to privileged EXEC mode.

## Configuration Examples for Monitoring IPv6 Layer 2 Bridged Traffic

You can configure Flexible Netflow to monitor IPv6 Layer 2 bridged traffic on both Switched Virtual Interfaces (SVIs) and VLANs, with or without flow samplers.

## Example Configuration for SVI-based Monitoring IPv6 Layer 2 Bridged Traffic

The following example is designed to monitor IPv6 Layer 2 bridged traffic on an SVI. An exporter is not configured because this example is intended to be used to capture additional data for analysis on the router using the **show flow monitor** command.

This sample starts in global configuration mode:

```

!
!
flow record bridged-flow-record
description bridged flow record
match ipv6 destination address
match ipv6 source address
match interface input
collect counter bytes long
collect counter packets long
exit
!
flow monitor bridged-flow-monitor
description bridged flow monitor
record bridged-flow-record
exit
!
interface vlan 100
ipv6 flow monitor bridged-flow-monitor layer2-bridged input
exit
!

```

## Example Configuration for VLAN-Based Monitoring of IPv6 Layer3 Bridged Traffic

The following example is designed to monitor IPv6 Layer 2 bridged traffic on a VLAN. An exporter is not configured because this example is intended to be used to capture additional data for analysis on the router using the **show flow monitor** command.

This sample starts in global configuration mode:

```

!
!
flow record bridged-flow-record
description bridged flow record
match ipv6 destination address
match ipv6 source address
match interface input
collect counter bytes long
collect counter packets long
exit
!
flow monitor bridged-flow-monitor
description bridged flow monitor
record bridged-flow-record
exit
!
vlan configuration 100
ipv6 flow monitor bridged-flow-monitor layer2-bridged input
exit
!

```

## Example Configuration for SVI-based Monitoring IPv6 Layer 2 Bridged Traffic Using a Flow Sampler

The following example is designed to monitor IPv6 Layer 2 bridged traffic on an SVI using a sampler. An exporter is not configured because this example is intended to be used to capture additional data for analysis on the router using the **show flow monitor** command.

This sample starts in global configuration mode:

```
!  
!  
flow record bridged-flow-record  
  description bridged flow record  
  match ipv6 destination address  
  match ipv6 source address  
  match interface input  
  collect counter bytes long  
  collect counter packets long  
  exit  
!  
flow monitor bridged-flow-monitor  
  description bridged flow monitor  
  record bridged-flow-record  
  exit  
!  
sampler S1  
  mode deterministic 1 out-of 2  
  exit  
!  
interface vlan 100  
  ipv6 flow monitor bridged-flow-monitor sampler S1 layer2-bridged input  
  exit  
!
```

## Example Configuration for VLAN-Based Monitoring of IPv6 Layer 3 Bridged Traffic Using a Flow Sampler

The following example is designed to monitor IPv6 Layer 2 bridged traffic on a VLAN using a flow sampler. An exporter is not configured because this example is intended to be used to capture additional data for analysis on the router using the **show flow monitor** command.

This sample starts in global configuration mode:

```
!  
!  
flow record bridged-flow-record  
  description bridged flow record  
  match ipv6 destination address  
  match ipv6 source address  
  match interface input  
  collect counter bytes long  
  collect counter packets long  
  exit  
!  
flow monitor bridged-flow-monitor  
  description bridged flow monitor  
  record bridged-flow-record
```

```

exit
!
sampler S1
mode deterministic 1 out-of 2
exit
!
vlan configuration 100
ipv6 flow monitor bridged-flow-monitor sampler S1 layer2-bridged input
exit
!

```

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
Overview of Flexible NetFlow	"Cisco IOS Flexible NetFlow Overview"
Flexible NetFlow Feature Roadmap	"Cisco IOS Flexible NetFlow Features Roadmap"
Emulating original NetFlow with Flexible NetFlow	"Getting Started with Configuring Cisco IOS Flexible NetFlow"
Configuring flow exporters to export Flexible NetFlow data.	"Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters"
Configuring flow sampling to reduce the overhead of monitoring traffic with Flexible NetFlow	"Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic"
Configuring Flexible NetFlow using predefined records	"Configuring Cisco IOS Flexible NetFlow with Predefined Records"
Using Flexible NetFlow Top N Talkers to analyze network traffic	"Using Cisco IOS Flexible NetFlow Top N Talkers to Analyze Network Traffic"
Configuring IPv4 multicast statistics support for Flexible NetFlow	"Configuring IPv4 Multicast Statistics Support for Cisco IOS Flexible NetFlow"
Configuration commands for Flexible NetFlow	<i>Cisco IOS Flexible NetFlow Command Reference</i>

### Standards

Standard	Title
None	--

**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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**RFCs**

RFC	Title
RFC 3954	<i>Cisco Systems NetFlow Services Export Version 9</i>

**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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for Configuring Accounting for IPv6 Layer 2 Bridged Traffic

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1: Feature Information for Flexible Netflow IPv6 Bridged Flows Feature**

Feature Name	Releases	Feature Information
Flexible Netflow - IPv6 bridged flows	15.1(1)SY	Flexible Netflow has been enhanced to enable the accounting of Layer 2 switched or bridged IPv6 traffic, for both SVIs and pure VLANs.

