Cisco IOS Metadata Command Reference

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1

Metadata Command Reference 1

debug metadata 2

match application (class-map) 5

metadata application-params 9

metadata flow 12

metadata flow (troubleshooting) 14

metadata flow transmit 16

metadata flow reverse transmit 17

metadata source nbar 19

show metadata 21

show metadata application table 24

show metadata flow 26

Metadata Command Reference

- debug metadata, page 2
- match application (class-map), page 5
- metadata application-params, page 9
- metadata flow, page 12
- metadata flow (troubleshooting), page 14
- metadata flow transmit, page 16
- metadata flow reverse transmit, page 17
- metadata source nbar, page 19
- show metadata, page 21
- show metadata application table, page 24
- show metadata flow, page 26

debug metadata

To enable debugging for metadata flow, use the **debug metadata** command in privileged EXEC mode. To disable debugging for metadata flow, use the **no** form of this command.

Cisco IOS Release 15.1(1)SY and Later Releases

debug metadata{**encode-decode**{**details**| **errors**| **events**}| **flow**{**all**| **core**| **cpl**| **table**}| **ha**| **nbar**}

no debug metadata{**encode-decode**{**details**| **errors**| **events**}| **flow**{**all**| **core**| **cpl**| **table**}| **ha**| **nbar**}

Releases Prior to Cisco IOS Release 15.1(1)SY

debug metadata{**encode-decode**{**details**| **errors**| **events**}| **flow**{**core**| **table**}}

no debug metadata{**encode-decode**{**details**| **errors**| **events**}| **flow**{**core**| **table**}}

Syntax Description

encode-decode	Enables debugging of the metadata encoding and decoding mechanism.
details	Enables debugging of the details related to the metadata encoding and decoding mechanism.
errors	Debugs any errors that occurred during the encode-decode process.
events	Debugs events that occurred during the encode-decode process.
flow	Debugs details related to metadata flow.
all	Debugs metadata flow information.
core	Debugs core metadata events information.
cpl	Debugs metadata flow classification information.
table	Debugs metadata flow table information.
ha	Debugs details related to metadata high availability (HA).
nbar	Debugs details related to metadata network-based application recognition (NBAR).

Command Default

Debugging for metadata flow is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.1(1)SY	This command was modified. The **all**, **cpl**, **ha**, and **nbar** keywords were added.

Examples

The following is sample output from the **debug metadata encode-decode details** command. The debug output shows the process for creating the IP Flow Information Export (IPFIX) template and decoding the metadata information. The last two lines indicate the length, variable length information ID, and the metadata application name.

```
Device# debug metadata encode-decode details
```

```
*Jul 14 03:24:50.395: MED-IPFIX: Hdr: Ver 10 msg len 66
*Jul 14 03:24:50.395: MED-IPFIX: Hdr: Export time = Thu
*Jul 14 08:54:50 2011
*Jul 14 03:24:50.395: MED-IPFIX: Hdr: Seq num = 4
*Jul 14 03:24:50.395: MED-IPFIX: Hdr: Obs dom ID = 0
*Jul 14 03:24:50.395: MED-IPFIX: Creating IP FIX Template, 79CD778
*Jul 14 03:24:50.395: MED-IPFIX: Decoded and saved ID 256 Templates Address 79CD778
*Jul 14 03:24:50.395: MED-IPFIX: Decoding 2 Template fields
*Jul 14 03:24:50.395: MED-IPFIX: len=4 936750775487430656
*Jul 14 03:24:50.395: MED-IPFIX: VLIE len 17 [telepresence-data]
```

The following is sample output from the **debug metadata flow all** command. The first line of the output displays the addition of an event. The output then shows the details of the ingress and egress interfaces. Next, the display shows the various application names and the associated application IDs. The ID is followed by the classification types and the matching of the applications. The last line indicates that an appropriate match was detected and the control plane classification has completed successfully.

```
Device# debug metadata flow all
```

```
*Jul 14 08:07:23.155: FMD SIG: Process RSVP Event RSVP_FMD_EVENT_PAYLOAD_RECEIVED(1)
*Jul 14 08:07:23.155: FMD : fmd_post_events: posting event 0
*Jul 14 08:07:23.167: FMD Process Event - FMD_RSVP_TRANSPORT_ADD
*Jul 14 08:07:23.167: (fmd_add_event_process): For Source IP/Port : 67372036/1000
*Jul 14 08:07:23.167: FMD DB Lookup: Hash 391
*Jul 14 08:07:23.167: FMD Event for Ingress Interface Ethernet0/0 , Egress Interface
Ethernet0/1
*Jul 14 08:07:23.167: FMD Classification Src Type 96, Len 17, Value telepresence-data
*Jul 14 08:07:23.167: FMD Classification Dest Type 95, Len 4, Value
*Jul 14 08:07:23.167: App name telepresence-data id 218104286 in Metadata local app table
*Jul 14 08:07:23.167: FMD Classification Src Type 96, Len 11, Value webex-audio
*Jul 14 08:07:23.167: FMD Classification Dest Type 95, Len 4, Value
*Jul 14 08:07:23.167: App name webex-audio id 12 in Metadata local app table
*Jul 14 08:07:23.167: FMD Classification Src Type 96, Len 11, Value webex-audio
*Jul 14 08:07:23.167: FMD Classification Dest Type 96, Len 17, Value telepresence-data *Jul
 14 08:07:23.167: FMD Classification Src Type 96, Len 11, Value webex-audio
*Jul 14 08:07:23.167: FMD Classification Dest Type 0, Len 0, Value
*Jul 14 08:07:23.167: FMD Classification: Match Passed for type 95 value Router-201
*Jul 14 08:07:23.167: FMD Classification: Found 1 filters matching
*Jul 14 08:07:23.167: FMD Event: Input policy Matched, Add flow to CFT
*Jul 14 08:07:23.167: FMD Event: PPCP Binding Succeeded
*Jul 14 08:07:23.167: FMD fmd_add_update_ingress_cft_fo : fid 4

*Jul 14 08:07:23.167: FMD Event: Local Flow ID 0
```

```
*Jul 14 08:07:23.167: (fmd_add_event_process): Update with Template Addres 79CD778, Md Addr
 947F810
*Jul 14 08:07:23.167: fmd_add_ipv4_flow_node_to_hash: Hash 391
*Jul 14 08:07:23.167: FMD Event: DB Addition Succeded
```

Related Commands

Command	Description
metadata application-params	Enters metadata application entry configuration mode and creates new metadata application parameters.
show metadata application table	Displays a list of metadata applications defined on a device.
show metadata flow	Displays metadata flow information.

match application (class-map)

To use the metadata application as a match criterion for control plane classification, use the **match application** command in QoS class-map configuration mode. To remove a previously configured metadata application from being used as a match criterion for control plane classification, use the **no** form of this command.

match application {**application-group** *application-group-name* | **attribute** {**category** {**business-and-productivity-tools**| **voice-and-video**}| **device-class** *device-class-type* | **media-type** *media-type*| **sub-category** {**remote-access-terminal**| **voice-video-chat-collaboration**}}| *application-name* [**source** {**msp** | **nbar** | **rsvp**}| **vendor** *vendor-name* **version** *version-number*]}

no match application {**application-group** *application-group-name* | **attribute** {**category** {**business-and-productivity-tools**| **voice-and-video**}| **device-class** *device-class-type* | **media-type** *media-type*| **sub-category** {**remote-access-terminal**| **voice-video-chat-collaboration**}}| *application-name* [**source** {**msp** | **nbar** | **rsvp**}| **vendor** *vendor-name* **version** *version-number*]}

Syntax Description

application-group *application-group-name*	Specifies the application group that the control plane classification engine must match. Use one of the following values to specify the relevant application group: **telepresence-group**, **vmware-group**, **webex-group**.
attribute	Specifies the relevant attribute to match.
category	Specifies the category type that the control plane classification engine must match.
business-and-productivity-tools	Specifies the business and productivity tools.
voice-and-video	Specifies the voice and video category.
device-class *device-class-type*	Specifies the device class to match. Use one of the following values to specify the relevant device class: **desktop-conferencing**, **desktop-virtualisation**, **physical-phone**, **room-conferencing**, **software-phone**, **surveillance**.
media-type *media-type*	Specifies the type of media to match. Use one of the following values to specify the relevant media type: **audio**, **audio-video control**, **data**, and**video**.
sub-category	Specifies the subcategory to match.
remote-access-terminal	Specifies the remote access terminal subcategory.
voice-video-chat-collaboration	Specifies the voice, video, and collaboration subcategory.

application-name	Name of the application that the control plane classification engine must match. The following applications are supported: **cisco-phone**, **citrix**, **h323**, **jabber**, **rtp**, **rtsp**, **sip**, **telepresence-control**, **telepresence-data**, **telepresence-media**, **vmware-view**, **webex-data**, **webex-meeting**, **webex-streaming**, **webex-video**, **webex-voice**, **wyze-zero-client**.
source	(Optional) Specifies the source of the application.
msp	Specifies the application source as Media-Proxy Services (MSP).
nbar	Specifies the application source as Network Based Application Recognition (NBAR).
rsvp	Specifies the application source as the Resource Reservation Protocol (RSVP).
vendor *vendor-name*	(Optional) Specifies the name of the vendor. Enter ? after the **vendor** keyword to get a list of supported vendors for the respective application name.
version *version-number*	(Optional) Specifies the version number.

Command Default

Metadata-based control plane classification is disabled.

Command Modes

QoS class-map configuration (config-cmap)

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(1)T	This command was modified. The **source**, **msp**, **nbar**, and **rsvp** keywords were added.

Usage Guidelines

Enabling metadata-based control plane classification on a per-platform, per-line card basis for Quality of Service (QoS) policies involves the following key steps:

- Creating a class map with metadata-based filters.
- Creating a policy map that uses classes.

- Attaching a policy map to the target.

You can use the **match application** command to enable metadata-based filters that can be applied to a class map. Specifying the required application name ensures that the respective policies can be applied only to those flows that match the application name. The classification engine makes its first match.

You can use the **match application** command in conjunction with the any other **match** commands for specifying match criteria for classes. For example, you can use the **match dscp** command along with the **match application** command as the classification criteria for flows.

You can use the **show metadata flow classification table** command to check the metadata-based classification information.

You can use the **debug metadata flow all** command to check if a particular classification has been successfully created.

Note With CSCub24690, the **webex-data**, **webex-streaming**, **webex-video**, and **webex-voice** keywords are not supported in the **match application** *application-name* command.

Examples

The following example shows how to configure a class map c1 and specify metadata application webex-meeting as the matching criterion, thus achieving control plane classification. Only those flows that match the metadata application webex-meeting will be considered for the appropriate action.

```
Device(config)# class-map c1
Device(config-cmap)# match application webex-meeting
```

The following configuration is provided for the completeness of the example.

A policy map p1 that uses the previously configured class c1 is created. The requirement in this example is to provide a guaranteed bandwidth of 1 Mb/s to all the flows that match the criterion defined for class c1:

```
Device(config)# policy-map p1
Device(config-pmap)# class c1
Device(config-pmap-c)# priority 1
```

The following configuration example shows how to attach a policy to a target interface:

```
Device(config)# interface gigabitethernet 0/0
Device(config-if)# service-policy output p1
```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change.
class-map	Creates a class map to be used for matching packets to a specified class.
debug metadata	Enables debugging for metadata flow.
metadata application-params	Enters metadata application entry configuration mode and creates new metadata application parameters.

Command	Description
policy-map	Enters policy-map configuration mode and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
priority	Gives priority to a class of traffic belonging to a policy map.
service-policy	Attaches a policy map to an input interface, a VC, an output interface, or a VC that will be used as the service policy for the interface or VC.
show metadata flow	Displays metadata flow information.

metadata application-params

To enter metadata application entry configuration mode and create new metadata application parameters, use the **metadata application-params** command in global configuration mode. To remove previously configured metadata application parameters, use the **no** form of this command.

metadata application-params *app-param-name*

no metadata application-params *app-param-name*

Syntax Description

app-param-name	Metadata application name that can be used as the match criterion for provisioning control plane classification.

Command Default

The application parameters for metadata-based classification are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

To create new metadata application parameters that can be used as match criteria for provisioning control plane classification, use the **metadata application-params** command. The **metadata application-params** command places the device in metadata application entry configuration mode. Use the following commands in metadata application entry configuration mode to configure the properties of the application. Configuring the name and ID is mandatory.

- **default—**Default properties for the name, description, and ID for the specified application.
- **description** *description-text***—**Description of the application. Supports up to 55 characters.
- **identifier** *id-value***—**Application ID. Internally maps to the application name. The range is from 1 to 16777215.
- **name** *name***—**Name of the application. Supports up to 24 characters.

Use the **show metadata application table** command to display the details of all metadata applications.

Examples

The following example shows how to create a new metadata application with appropriate parameters:

```
Device(config)# metadata application-params app1
Device(config-md-app-entry)# name instant-messaging-audio
Device(config-md-app-entry)# identifier 243
Device(config-md-app-entry)# description instant messaging audio recordings
```

The following output of the **show metadata application table** command shows the name and ID of all the metadata applications configured on a specific endpoint:

```
Device# show metadata application table

ID     Name                  Vendor                Vendor id
--------------------------------------------------------------------------------
113    telepresence-media    -                     -
114    telepresence-contr$   -                     -
478    telepresence-data     -                     -
414    webex-meeting         -                     -
56     citrix                -                     -
81     cisco-phone           -                     -
472    vmware-view           -                     -
473    wyze-zero-client      -                     -
61     rtp                   -                     -
64     h323                  -                     -
5060   sip                   -                     -
554    rtsp                  -                     -
496    jabber                -                     -
5222   xmpp-client           -                     -
```

The table below describes the significant fields shown in the display.

Table 1: show metadata application table Field Descriptions

Field	Description
ID	Application ID. Internally maps to the application name.
Name	Name of the application.

Related Commands

Command	Description
debug metadata	Enables debugging for metadata flow.
default	Displays default properties for the name, description, and ID for the specified application.
description	Displays the description of the application.
identifier	Displays the Application ID.
name	Displays the name of the application.

Command	Description
show metadata application table	Displays a list of metadata applications defined on a device.
show metadata flow	Displays metadata flow information.
name	Displays the name of the application.

metadata flow

To enable metadata on all interfaces or on a specific interface, use the **metadata flow** command in global configuration mode or interface configuration mode. To disable metadata, use the **no** form of this command.

metadata flow

no metadata flow

Syntax Description

This command has no arguments or keywords.

Command Default

Metadata is disabled on an interface.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

If you use the **metadata flow** command in global configuration mode, metadata is enabled at the device level. That is, metadata is enabled on all the interfaces configured on the device. If you use the **metadata flow** command in interface configuration mode, metadata is enabled on the specified interface only. You can use the **no metadata flow** command in interface configuration mode to disable metadata on any one interface. However, metadata flows that enter from other interfaces will not be able to pass through an interface on which metadata has been disabled. In such instances, the flow table will not be populated and classification will not complete successfully. When you explicitly enable or disable metadata on an interface, configuration details are retrieved using the nonvolatile generation (NVGEN) method and are displayed in the configuration.

Examples

The following example shows how to enable metadata at the device level:

```
Device(config)# metadata flow
```

The following example shows how to enable metadata at the per-interface level:

```
Device(config)# interface gigabitethernet 0/0
Device(config-if)# metadata flow
```

Related Commands

Command	Description
metadata flow (troubleshooting)	Creates flow entries for testing and troubleshooting the metadata flow.

metadata flow (troubleshooting)

To simulate the creation of flows for testing and troubleshooting metadata, use the **metadata flow** command in global configuration mode. To remove the flows created for testing and troubleshooting, use the **no** form of this command.

Cisco IOS Release 15.1(1)SY and Later Releases

metadata flow

no metadata flow

Releases Prior to Cisco IOS Release 15.1(1)SY

metadata flow [**entry** *entry-name*| **flow-specifier** *flow-specifier-name* | **session-params** *session-name*]

no metadata flow [**entry** *entry-name*| **flow-specifier** *flow-specifier-name* | **session-params** *session-name*]

Syntax Description

entry *entry-name*	Creates a flow entry with the specified name.
flow-specifier *flow-specifier-name*	Configures source and destination information.
session-params *session-name*	Configures session parameters for the flow.

Command Default

Static metadata flow entries are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.1(1)SY	The command was modified. The **entry** *entry-name*, **flow-specifier** *flow-specifier-name*, and **session-params** *session-name* keyword-argument pairs were removed.

Usage Guidelines

You can use the **metadata flow** command along with the associated keywords when you need to simulate an environment consisting of virtual endpoints for testing or troubleshooting purposes.

Use the **metadata flow entry** *entry-name* command to create a flow. To create a successful flow, specify the flow specifier and session parameters.

Using the **flow-specifier** *flow-specifier-name* keyword and argument pair creates a flow specifier and places the device in metadata configuration flow specifier mode. Use the following commands in metadata configuration flow specifier mode to configure the flow tuple for the flow:

- **dest-ip** *ip-address* **dest-port** *port-number***—**Specifies the destination IPv4 address and destination port number for the endpoint.
- **source-ip** *ip-address* **source-port** *port-number***—**Specifies the source IPv4 address and source port number for the endpoint.

Using the **session-params** *session-name* keyword and argument pair places the command in metadata session parameters configuration mode. Use the following related command in metadata session parameters configuration mode to configure the session parameters for the flow:

- **application name** *application-name***—**Associates the specified application name to the session.

Using the **entry** *entry-name* keyword and argument pair places the command in metadata entry configuration mode. In metadata entry configuration mode, use the **flow-specifier** keyword with the previously defined flow specifier and the **session-params** keyword with the previously defined session parameter name to associate with the specified flow entry.

Examples

The following examples show how to create a flow entry, a flow specifier, and session parameters, and how to associate the flow specifier and session parameters with the flow entry.

The following configuration shows how to create a flow entry:

```
Device(config)# metadata flow entry e1
```

The following example shows how to create a flow specifier with the source IP address, destination IP address, and source and destination port numbers:

```
Device(config)# metadata flow flow-specifier flow1
Device(config-md-flowspec)# source 209.165.201.3 source-port 1000
Device(config-md-flowspec)# destination 209.165.201.20 dest-port 1000
```

The following example shows how to create a session parameter and the associated parameters:

```
Device(config)# metadata flow session-params session1
Device(config-md-session-params)# application name webex-meeting
```

The following example shows how to associate the flow specifier and session parameters with the flow entry:

```
Device(config)# metadata flow entry e1
Device(config-md-entry)# flow-specifier flow1
Device(config-md-entry)# session-params session1
```

Related Commands

Command	Description
debug metadata	Enables debugging for metadata flow.
show metadata application table	Displays a list of metadata applications defined on a device.
show metadata flow	Displays metadata flow information.

metadata flow transmit

To enable Resource Reservation Protocol (RSVP) transmission of flow information learned through network-based application recognition (NBAR) to downstream devices, use the **metadata flow transmit** command in global configuration mode. To disable the downstream flow information transmission, use the **no** form of this command.

metadata flow transmit

no metadata flow transmit

Syntax Description

This command has no arguments or keywords.

Command Default

Flow information is not transmitted downstream.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)M	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The flow information from NBAR is generated only on the node on which NBAR is configured and is not available to downstream devices. Use the **metadata flow transmit** command to enable flow information to be transmitted to downstream devices. When the **metadata flow transmit** command is enabled, the flow information is transmitted to downstream devices using RSVP.

Examples

The following example shows how to enable flow information to be transmitted downstream:

```
Device> enable
Device# configure terminal
Device(config)# metadata flow
Device(config)# metadata flow transmit
Device(config)# exit
```

Related Commands

Command	Description
metadata flow	Enables metadata on a device.

metadata flow reverse transmit

To start Resource Reservation Protocol (RSVP) reverse transmission session for metadata flow information learned through network-based application recognition (NBAR), use the **metadata flow reverse transmit** command in global configuration or interface configuration mode. To disable the reverse transmission of metadata flow information, use the **no** form of this command.

metadata flow reverse transmit

no metadata flow reverse transmit

Syntax Description

This command has no arguments or keywords.

Command Default

No reverse session exists. That is, no reverse session has been created by MSP, MSI or NBAR.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

The flow information from NBAR is generated only on the node on which NBAR is configured and is not available to downstream devices. Use the **metadata flow transmit** command to enable flow information to be transmitted to downstream devices. When an end-device cannot signal metadata, a reverse metadata flow session is created using the **metadata flow reverse transmit** command for the end-device to act as a proxy and signals metadata and support QoS for the reverse session. The reverse sessions are created using the attributes of the forward sessions.

Examples

The following example shows how to enable reverse flow of metadata information in Global configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# metadata flow
Device(config)# metadata flow reverse transmit
Device(config)# exit
```

Examples

The following example shows how to enable reverse flow of metadata information in Interface configuration mode:

```
Device> enable
```

```
Device# configure terminal
Device(config)# metadata flow
Device(config)# interface Ethernet 0/1
Device(config-if)# metadata flow reverse transmit
Device(config)# exit
```

Related Commands

Command	Description
metadata flow	Enables metadata on a device.
metadata flow transmit	Enables RSVP transmission of flow information to downstream devices.
match application	Uses metadata application as a match criterion for control plane classification.
debug metadata	Enables debugging for metadata flow information.
show metadata flow	Displays the metadata flow information.

metadata source nbar

To enable network-based application recognition (NBAR) as a source for metadata, use the **metadata source nbar** command in global configuration mode. To disable NBAR as a source for metadata, use the **no** form of this command.

metadata source nbar

no metadata source nbar

Syntax Description

This command has no arguments or keywords.

Command Default

NBAR is enabled as a source for metadata by default when you create a class map with metadata-based filters, create a policy map that uses the class, and attach the policy map to a target.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)M	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following example shows how to enable NBAR as a source for metadata:

```
Device> enable
Device# configure terminal
Device(config)# metadata flow
Device(config)# metadata flow transmit
Device(config)# metadata source nbar
Device(config)# class-map c1
Device (config-cmap)# match application webex-meeting
Device(config-cmap)# exit
Device(config)# policy-map p1
Device(config-pmap)# class c1
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# interface gigabitethernet 0/0
Device(config-if)# service-policy output p1
Device(config-if)# exit
```

The following example shows how to disable NBAR as a source for metadata:

```
Device> enable
Device# configure terminal
Device(config)# no metadata source nbar
Device(config)# exit
```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change.
class-map	Creates a class map to be used for matching packets to a specified class.
debug metadata	Enables debugging for metadata flow information.
match application	Uses the metadata application as a match criterion for control plane classification.
metadata flow	Enables metadata on a device.
metadata flow transmit	Enables RSVP transmission of flow information to downstream devices.
policy-map	Enters policy-map configuration mode and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface, a VC, an output interface, or a VC that will be used as the service policy for the interface or VC.

show metadata

To display a list of metadata information on a device, use the **show metadata** command in privileged EXEC mode.

show metadata {**application** {[**version** | **version**] **table**}| **filter table**| **flow**}

Syntax Description

application	Displays metadata applications defined on a device.
table	Displays information for the specified application.
version table	Displays the version for a metadata application.
vendor table	Displays the vendor of the specific metadata application.
filter table	Displays metadata information based on the filter criteria.
flow	Displays metadata flow information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)SY	This command was introduced.

Examples

The following is sample output from the **show metadata application table** command:

```
Device# show metadata application table

ID     Name                  Vendor               Vendor id
--------------------------------------------------------------------------------
113    telepresence-media    -                    -
114    telepresence-contr$   -                    -
478    telepresence-data     -                    -
414    webex-meeting         -                    -
56     citrix                -                    -
81     cisco-phone           -                    -
472    vmware-view           -                    -
473    wyze-zero-client      -                    -
61     rtp                   -                    -
64     h323                  -                    -
5060   sip                   -                    -
554    rtsp                  -                    -
496    jabber                -                    -
5222   xmpp-client           -                    -
```

The table below describes the significant fields shown in the display.

Table 2: show metadata application table Field Descriptions

Field	Description
ID	Application ID. Internally maps to the application name.
Name	Name of the application.

The following is sample output from the **show metadata application version table** command:

```
Device#  show metadata application version table

    ID            |    Version
------------------+------------------------------
00000000E0000002  | 1.2
```

The table below describes the significant fields shown in the display.

Table 3: show metadata application version table Field Descriptions

Field	Description
ID	Application ID. Internally maps to the version name.
Version	Version of the application.

The following is sample output from the **show metadata application vendor table** command:

```
Device#  show metadata application vendor table

ID       Name
----------------------------------------------------------
122      Sony
368      Axis Communications AB
5318     Robert Bosch GmbH
5771     Cisco Systems, Inc.
13885    Polycom, Inc.
```

The table below describes the significant fields shown in the display.

Table 4: show metadata application vendor table Field Descriptions

Field	Description
ID	Vendor ID. Internally maps to the vendor name.
Name	Name of the vendor.

Related Commands

Command	Description
metadata application-params	Enters metadata application entry configuration mode and creates new metadata application parameters.

show metadata application table

To display a list of metadata applications defined on a device, use the **show metadata application table** command in privileged EXEC mode.

show metadata application table

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following is sample output from the **show metadata application table** command:

```
Device# show metadata application table

ID     Name                  Vendor                Vendor id
--------------------------------------------------------------------------------
113    telepresence-media    -                     -
114    telepresence-contr$   -                     -
478    telepresence-data     -                     -
414    webex-meeting         -                     -
56     citrix                -                     -
81     cisco-phone           -                     -
472    vmware-view           -                     -
473    wyze-zero-client      -                     -
61     rtp                   -                     -
64     h323                  -                     -
5060    sip                  -                     -
554    rtsp                  -                     -
496    jabber                -                     -
5222   xmpp-client           -                     -
```

The table below describes the significant fields shown in the display.

Table 5: show metadata application table Field Descriptions

Field	Description
ID	Application ID. Internally maps to the application name.
Name	Name of the application.

Related Commands

Command	Description
metadata application-params	Enters metadata application entry configuration mode and creates new metadata application parameters.

show metadata flow

To display metadata flow information, use the **show metadata flow** command in privileged EXEC mode.

show metadata flow {**classification table** | **local-flow-id** *flow-id* [**source** {**msp** | **nbar** | **rsvp**}] | **statistics** | **table** [[**application name** *app-name* [**ip** | **ipv6**]] | **filter** [**destination** {*ip-address* | *ipv6-address*}] [**source** {*ip-address* | *ipv6-address*}] | **ip** | **ipv6**]}

Syntax Description

classification table	Displays metadata control plane classification information.
local-flow-id *flow-id*	Displays information for the specified local flow ID, which is a unique ID for a given five-tuple metadata flow entry created locally. • The local flow ID is automatically generated when the flow entry is created.
source	(Optional) Displays metadata flow information for the specified source.
msp	Displays metadata flow information for Media-Proxy Services.
nbar	Displays metadata flow information for Network-Based Application Recognition (NBAR).
rsvp	Displays metadata flow information for the Resource Reservation Protocol (RSVP).
statistics	Displays metadata flow statistics.
table	Displays metadata flow information for all flow entries.
application	(Optional) Displays metadata flow information for the specified application.
name *app-name*	(Optional) Specifies all the flows for the specified application.
ip	Displays metadata flow information for the specified IP4 address.
ipv6	Displays metadata flow information for the specified IPv6 address.

filter	(Optional) Displays metadata flow information based on the filter criteria.
destination {*ip-address* | *ipv6-address*}	(Optional) Displays metadata flow information for the specified destination address.
source {*ip-address* | *ipv6-address*}	(Optional) Displays metadata flow information for the specified source address.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(1)T	This command was modified. The **source**, **msp**, **nbar**, and **rsvp** keywords were added. IPv6 address information was added to the command output.

Examples

The following is sample output from the **show metadata flow classification table** command:

```
Device# show metadata flow classification table

Policy Type Codes:
QOS     : QOS                            PM      : Performance Monitor
PMD     : Performance Monitor Dynamic    MACE    : MACE
--------------------------------------------------------------------------------
Target          Flow ID    Dir   Policy     Filter(s)
                                 Type
---------------+----------+-----+----------+------------------------------------

Se2/0           1          OUT
Se2/0           2          OUT
Se2/0           3          OUT
Se2/0           4          OUT   QOS        application telepresence-media
Se2/0           5          OUT   QOS        application telepresence-media
Se2/0           6          OUT
Se2/0           7          OUT
Se2/0           8          OUT   QOS        application telepresence-media
Se2/0           9          OUT
```

The table below describes the significant fields shown in the display.

Table 6: show metadata classification table Field Descriptions

Field	Description
Target	Interface name for which the policy map is attached.

Field	Description
Flow ID	Flow entry identifier.
Dir	Direction of the flow entry. IN indicates that the flow is entering the network element. OUT indicates that the flow is exiting the network element. CL indicates that the flow has been classified successfully.

The following is sample output from the **show metadata flow local-flow-id** command:

```
Device# show metadata flow local-flow-id 22

To                                      From

Protocol SPort   DPort   Ingress I/F              Egress I/F
2012:33:1:2::2                          2012:33:1:2::1
UDP      49002   49003   n/a                      Serial2/0

Metadata Attributes :

Global Session Id           :   74657374-2D54-502D-3100-000000000000-00000000-00000000
Clock Frequency             :   123456
End Point Model             :   Test-TP-Model
Application Signaling Type  :   sip
Application Transport Type  :   rtp
Application Traffic Type    :   realtime
Application Device Class    :   room-conferencing
Application Category        :   voice-and-video
Application Group           :   telepresence-group
Application Media Type      :   video
Application Tag             :   218103921 (telepresence-media)
Application Name            :   telepresence-media

Matched filters :

 Direction: IN:
 Direction: OUT:
```

The table below describes the significant fields shown in the display.

Table 7: show metadata flow local-flow-id Field Descriptions

Field	Description
To	Destination address of the flow entry.
From	Source address from where the flow entry is sent.
Protocol	Transport protocol, TCP or UDP, used for the flow.
SPort	Source port of the flow entry. Valid range is from 1 to 65535.
DPort	Destination port of the flow entry. Valid range is from 1 to 65535.
Ingress I/F	Ingress interface. Incoming interface for a given network element.

Field	Description
Egress I/F	Egress interface. Outgoing interface for a given network element.
Global Session ID	Global session ID of the application.
Clock Frequency	Frequency of the application clock.
End Point Model	Model of the application.
Application Signaling Type	Name of the application vendor.
Application Transport Type	Transport type of the metadata application.
Application Traffic Type	Traffic type of the metadata application.
Application Device Class	Classification of the metadata application.
Application Category	Category of the metadata application.
Application Group	Group of the metadata application.
Application Media Type	Type of media for the metadata application.
Application Tag	Application identifier. • Every metadata application name is mapped to a unique application tag.
Application Name	Name of the metadata application.
Direction	Direction for the application.

The following is sample output from the **show metadata flow statistics** command:

```
Device# show metadata flow statistics

Interface specific report :

Serial2/0: Classified flows : Ingress 0, Egress 0

Chunk statistics :

Type                Allocated       Returned        Failed

IP Flow              9                0                0
Flow Key             29               20               0
Source List          4                0                0
Flow Info            29               29               0
Attribute Data       29               29               0
Feature Object       2                0                0

Event Statistics:

Add Flow                 : 9         Delete Flow              : 0
```

```
Received                 : 30       Rejected                 : 0
Transient                : 0        Posted                   : 29
Ingress Change           : 0        Egress Change            : 11
Unknown                   : 0        Source Limit Exceeded    : 0
```

The table below describes the significant fields shown in the displays.

Table 8: show metadata flow statistics Field Descriptions

Field	Description
Interface specific report	Report specifying the number of egress or ingress flows per interface.
Ingress flows	Number of flows that entered the interface.
Egress flows	Number of flows that exited the interface.
Chunk Statistics	Information specific to the chunk memory.
Type	Refers to the type of information or data structure usage for which memory consumption is recorded.
Allocated	Memory allocated for the specified type of information.
Returned	Memory returned to the system for the specified type of information.
Failed	Record of the memory allocation failures.
Event Statistics	Information specific to every flow event that has occurred on the device.
Add Flow	Number of flows added into the network element.
Delete Flow	Number of flows deleted from the network element.
Received	Number of flows received by the network element.
Rejected	Number of flows rejected by the network element.
Transient	Number of flows that are in transient state.
Posted	Number of change notifications received by the Resource Reservation Protocol (RSVP).
Ingress Change	Number of times the ingress interface changed.
Egress Change	Number of times the egress interface changed.
Unknown	Number of times an unknown event was received.

Field	Description
Source Limit Exceeded	Number of times the flow limit defined for the device was exceeded.

The following is sample output from the **show metadata flow table** command:

```
Device# show metadata flow table

Total number of IPV4 metadata flows 6

Flow  To              From            Proto DPort SPort Ingress      Egress

4     10.0.0.1        10.0.0.2        UDP   49008 49007              Se2/0
6     10.0.0.3        10.0.0.4        UDP   49004 49003              Se2/0
5     10.2.0.3        10.2.0.6        UDP   49010 49009              Se2/0
2     10.2.1.6        10.2.2.6        UDP   49004 49003              Se2/0
1     10.2.2.6        10.2.3.6        UDP   49002 49001              Se2/0
3     10.2.3.6        10.2.3.7        UDP   49006 49005              Se2/0


Total number of IPV6 metadata flows 3

To                                      From
Flow  Proto DPort SPort Ingress      Egress

2001:DB8:1::1                          2001:DB8:1::2
9     UDP   49001 49000              Se2/0
2001:DB8:1::3                          2001:DB8:1::4
7     UDP   49001 49000              Se2/0
2001:DB8:1::12                        2001:DB8:1::13
8     UDP   49003 49002              Se2/0
```

Note The output for the IPv6 metadata flow table appears in two lines as the IPv6 addresses can be long.

The following is sample output from the **show metadata flow table ipv6** command:

```
Device# show metadata flow table ipv6

To                                      From
Flow  Proto DPort SPort Ingress      Egress

2001:DB8:1::1                          2001:DB8:1::2
9     UDP   49001 49000              Se2/0
2001:DB8:1::3                          2001:DB8:1::4
7     UDP   49001 49000              Se2/0
2001:DB8:1::12                        2001:DB8:1::13
8     UDP   49003 49002              Se2/0
```

The following is sample output from the **show metadata flow table application name sip ip** command:

```
Device#  show metadata flow table application name sip ip

Flow  To              From           Protocol  DPort  SPort  Ingress   Egress  SSRC

2     209.165.201.14  209.165.201.18  UDP      70    80       Eth1/1   Eth1/2  3000
```

The following is sample output from the **show metadata flow table application name sip ipv6** command:

```
Device# show metadata flow table application name sip ipv6

To                                      From
Flow  Proto DPort SPort Ingress      Egress

2001:DB8:1::3                          2001:DB8:1::4
```

```
9     UDP   49001 49000              Se2/0
2001:DB8:1::5                          2001:DB8:1::6
7     UDP   49001 49000              Se2/0
2001:DB8:1::12                        2001:DB8:1::14
8     UDP   49003 49002              Se2/0
```

The following is sample output from the **show metadata flow table filter destination** command. You can specify the source or destination IPv4 address as the filter criterion.

```
Device# show metadata flow table filter destination 209.165.201.1

Entries To: 209.165.201.1

Flow ID    From             Protocol DPort   SPort   Ingress I/F    Egress I/F
1          209.165.201.3    UDP      1000    1000    Et0/0          Et0/1
2          209.165.201.3    UDP      1001    1001    Et0/0          Et0/1
Total Flows: 2
```

Related Commands

Command	Description
debug metadata	Enables debugging for metadata flow.
metadata application-params	Enters metadata application entry configuration mode and creates new metadata application parameters.
show metadata application table	Displays a list of metadata applications defined on a device.
metadata flow	Enables metadata on a device.