



# Configuring Media Flow Analytics

This chapter contains information about media flow analytics for Cisco's IP fabric for media solution.

- [RTP Flow Monitoring, on page 1](#)
- [Guidelines and Limitations for RTP Flow Monitoring, on page 1](#)
- [Configuring RTP Flow Monitoring, on page 2](#)
- [Displaying RTP Flows and Errors, on page 3](#)
- [Clearing RTP Flows, on page 4](#)

## RTP Flow Monitoring

Real-Time Transport Protocol (RTP) is a network protocol for delivering audio and video over IP networks. It is designed for end-to-end, real-time transfer of streaming media. The protocol provides facilities for jitter compensation and detection of packet loss, which are common during UDP transmissions on an IP network.

RTP flow monitoring caches RTP flows on the switch and detects any gaps in the RTP sequence number, which indicates a loss in RTP frames. This information helps to pinpoint where the loss is occurring and enables you to better plan hardware resources.

## Guidelines and Limitations for RTP Flow Monitoring

The following guidelines and limitations apply to RTP flow monitoring:

- Only Cisco Nexus 9300-FX, 9300-FX2, and 9300-FX3 platform switches support RTP flow monitoring.  
In addition, beginning with Cisco NX-OS 9.3(6), Cisco Nexus 9300-GX platform switches support RTP flow monitoring.
- When RTP flow monitoring is configured with an initial ACL, and then changed to a different ACL, the RTP configuration must be removed with the `no flow rtp` form of the command and then configured again with the required ACL.
- Reboot the switch after configuring UDF for RTP flow monitoring.
- You can configure only one RTP flow monitoring UDF.
- The RTP flow monitoring UDF must be the first UDF.
- Traditional NetFlow Monitor and RTP flow monitoring cannot coexist on the switch.

# Configuring RTP Flow Monitoring

You can configure RTP flow monitoring for Cisco Nexus 9300-FX, 9300-FX2, and 9300-FX3 platform switches.

In addition, beginning in Cisco NX-OS 9.3(6), you can configure RTP flow monitoring for Cisco Nexus 9300-GX platform switches.

## Before you begin

Enable UDF for RTP flow monitoring using the **udf netflow\_rtp netflow-rtp** command, copy the running configuration to startup, and reboot the switch. Make sure that the RTP flow monitoring UDF is the first UDF.

## SUMMARY STEPS

1. **configure terminal**
2. **[no] feature netflow**
3. (Optional) **ip access-list *acl***
4. **[no] {ip | ipv6} flow rtp [*acl*]**

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
<b>Step 2</b>	<b>[no] feature netflow</b> <b>Example:</b> <pre>switch(config)# feature netflow</pre>	Enables RTP flow monitoring globally on the switch.
<b>Step 3</b>	(Optional) <b>ip access-list <i>acl</i></b> <b>Example:</b> <pre>ip access-list ipv4-test-acl  10 permit ip any 224.0.1.39/32  20 permit ip any 224.0.1.40/32</pre>	Configures an ACL policy to filter any specific traffic.
<b>Step 4</b>	<b>[no] {ip   ipv6} flow rtp [<i>acl</i>]</b> <b>Example:</b> <pre>switch(config)# ip flow rtp</pre>	Enables RTP flow monitoring for IPv4 or IPv6 flows. <ul style="list-style-type: none"> <li>• This command also creates a system-wide access control list (ACL) to filter the UDP port range of 16384 to 32767. This range is the RFC standard UDP port range for RTP traffic.</li> </ul> <p><b>Note</b> The <b>ignore routable</b> command filters any multicast traffic.</p> <pre>switch(config)# show ip access-list IP access list nfm-rtp-ipv4-acl</pre>

	Command or Action	Purpose
		<pre>ignore routable 10 permit udp any any range 16384 32767</pre> <p><b>Note</b> When an ACL is specified in the command, only traffic that matches the specified ACL is reported as RTP flows.</p> <pre>switch(config)# ip flow rtp ipv4-test-acl</pre>

## Displaying RTP Flows and Errors

To display the RTP flows and errors, perform one of the following tasks.

<b>show flow rtp details</b>	Displays all IPv4 and IPv6 RTP flows.
<b>show flow rtp details {ipv4   ipv6}</b>	Displays either IPv4 or IPv6 RTP flows.
<b>show flow rtp errors active</b>	Displays details of all RTP flows that are currently experiencing losses (if the packet loss is detected in at least one update interval within the last 10 seconds). The loss statistics for the active loss window are also displayed. Because the loss window is still considered active, the loss end time shows as “N/A.”
<b>show flow rtp errors history</b>	Displays details of the last 1000 historical loss windows (in reverse chronological order) and their respective flow details.

The following example shows sample output for the **show flow rtp details** command:

```
RTP Flow timeout is 1440 minutes
IPV4 Entries
SIP      DIP      BD ID S-Port D-Port Intf/Vlan Name  Packet Count BytesPerSec  FlowStart
50.1.1.2 20.1.1.2 4151 16385 17999 Ethernet1/49/1 269207033    594468000    00:21:16
PST Apr 07 2019
20.1.1.2 50.1.1.2 4100 16385 18999 port-channel500 2844253      199000       00:21:59
PST Apr 07 2019

IPv6 Entries
SIP      DIP      BD ID S-Port D-Port Intf/Vlan Name  Packet Count BytesPerSec  FlowStart
20::2    50::2    4100 30000 31999 port-channel500 2820074      199000       00:22:04
PST Apr 07 2019
50::2    20::2    4151 30000 31999 Ethernet1/49/1 3058232      199000       00:21:16
```

PST Apr 07 2019

The following example shows sample output for the **show flow rtp errors active** command:

RTP Flow timeout is 1440 minutes

IPV4 Entries

SIP	DIP	BD ID	S-Port	D-Port	Intf/Vlan Name	Packet Count
BytesPerSec	FlowStart		Packet Loss	Loss Start	Loss End	
30.30.1.2	20.20.1.2	4197	30000	20392	Ethernet1/98	200993031
10935633	20:23:15 UTC May 30 2019	1558		03:48:32 UTC May 31 2019		N/A
20.20.1.2	30.30.1.2	4196	30000	20392	Ethernet1/97	204288988
11114959	20:23:15 UTC May 30 2019	222		03:48:30 UTC May 31 2019		N/A



**Note** When an RTP flow enters the “active-errored” state, the following syslog message appears:

```
%NFM-1-RTP_FLOW_ERROR_DETECTED: Flow SIP: 30.30.1.2 DIP: 20.20.1.2 Interface: Ethernet1/98
loss detected
```

The following example shows sample output for the **show flow rtp errors history** command:

RTP Flow timeout is 1440 minutes

IPV4 Entries

SIP	DIP	BD ID	S-Port	D-Port	Intf/Vlan Name	Packet Count
BytesPerSec	FlowStart		Packet Loss	Loss Start	Loss End	
20.20.1.2	30.30.1.2	4196	30000	20392	Ethernet1/97	204187441
11122753	20:23:15 UTC May 30 2019	2061		03:47:57 UTC May 31 2019		03:47:57
30.30.1.2	20.20.1.2	4197	30000	20392	Ethernet1/98	199495510
10937237	20:23:15 UTC May 30 2019	1882		03:45:06 UTC May 31 2019		03:45:06
20.20.1.2	30.30.1.2	4196	30000	20392	Ethernet1/97	202753418
11116269	20:23:15 UTC May 30 2019	4976		03:45:05 UTC May 31 2019		03:45:05
20.20.1.2	30.30.1.2	4196	30000	20392	Ethernet1/97	202630465
11123369	20:23:15 UTC May 30 2019	2139		03:44:32 UTC May 31 2019		03:44:32
30.30.1.2	20.20.1.2	4197	30000	20392	Ethernet1/98	197973969
10938370	20:23:15 UTC May 30 2019	1854		03:41:41 UTC May 31 2019		03:41:41



**Note** When an RTP flow is no longer in the “active-errored” state, the following syslog message appears:

```
%NFM-1-RTP_FLOW_ERROR_STOP: Flow SIP: 30.30.1.2 DIP: 20.20.1.2 Interface: Ethernet1/98 loss
no longer detected
```

## Clearing RTP Flows

To clear RTP flows, perform one of the following tasks.

<b>clear flow rtp detail</b>	Clears all RTP flows and loss histories.
------------------------------	--

<b>clear flow rtp detail {ipv4   ipv6}</b>	Clears either IPv4 or IPv6 RTP flows and loss histories.
<b>[no] flow rtp timeout</b> <i>value</i> <b>Example:</b> <pre>switch(config)# flow rtp timeout 100</pre>	<p>Clears non-active RTP flows from the <b>show rtp details</b>, <b>show flow rtp errors active</b>, and <b>show flow rtp errors history</b> tables.</p> <p>The default value is 1440 minutes (24 hours), and the range is from 0 to 1440 minutes. A value of 0 prevents RTP flows from being cleared.</p> <p><b>Note</b> This command does not clear active RTP flows.</p>

