



Implementing Video Monitoring

Configuring Video Monitoring is a four-step procedure, which includes configuring the relevant class-maps and policy maps, and binding the video monitoring policy to an interface.

- [Prerequisites for Implementing Video Monitoring, on page 1](#)
- [Information About Implementing Video Monitoring, on page 1](#)
- [Implementing Video Monitoring, on page 6](#)
- [Configuration Examples for Implementing Video Monitoring , on page 15](#)
- [Additional References, on page 20](#)

Prerequisites for Implementing Video Monitoring

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- You must install and activate packages for advanced video services. For detailed information about optional package installation, see *Cisco IOS XR Getting Started Guide for the Cisco CRS Router*.
- You must install and activate a package for the multicast routing software and enable multicast routing on the system. Video monitoring is supported on interfaces that are multicast-enabled. For detailed information about multicast routing, refer to the chapter Implementing Layer 3 Multicast Routing on Cisco CRS Routers.

Information About Implementing Video Monitoring

Video Monitoring

Poor video experience is a major cause for concern among service providers in terms of service costs and loss of revenue. To avoid the service costs of help desk time, NOC (network operation center) troubleshooting resources, and truck rolls, the capability of monitoring video traffic is essential. On Cisco IOS XR software, problems in video flows can be easily diagnosed by video monitoring.

Introduction to Video Monitoring

Packet loss is one common cause of video quality degradation. Its impact is more significant on compressed video flows. The video traffic transported through the service provider IP network is mostly compressed video – MPEG or similar encoding. Because of the way compression occurs, the traffic is extremely loss-sensitive. The video is encoded with an independent frame (I-frame) every few seconds, with subsequent frames being deltas from the I-frame. If the loss is in an I-frame, a 3 ms loss of traffic (roughly one IP packet) can result in a viewing degradation for up to 1.2 seconds.

Jitter is a key flow characteristic that requires careful buffer provisioning in the end device. The set top box (STB) that displays the media on a screen needs to decode the video in real-time. It buffers the incoming video stream so that it can decode and display the image smoothly. Large network jitter can lead to buffer underrun or overrun on the STB. Depending on how large the jitter is, this will create a visual distortion or a freezing of the video at display.

End-to-end delay in transmission is not significant for a broadcast-only application. However, as the video applications get to be more interactive, the end-to-end latency (delay) becomes a critical Quality of Experience (QoE) component. Data loss is a major contributor for poor QoE.

Three main contributors to poor QoE can be summed up as:

- Packet Loss
- Jitter
- Delay

Video Monitoring plays a very significant role in improving video quality, and thus, in enhancing the QoE. Video monitoring is implemented on the routers and enables network operators to measure and track video transport performance on a per-flow basis. The video packets flow through a router. We can use the packet headers and compute a metric that gives us a measure of the network performance impacting the quality of the video. This information from multiple routers is compared for the same flow to get a clear end-to-end picture of the video issues in the network and the affected flows.

Problems in video flows (and more generally, any streaming flow) can be diagnosed by video monitoring. The purpose of video monitoring is to detect perturbations and anomalies introduced by the network that cause a degraded QoE; that is, it measures the transport performance for streaming (video) traffic. Encoding errors, audio-video-lag, and other errors too cause poor QoE. However, these are introduced by the encoding device and not the network. These latter errors are not monitored.

Key Features Supported on Video Monitoring

Direct Measurements from Data Plane

Video monitoring plays a significant role in improving video quality and therefore enhances the QoE. Video monitoring implemented on Cisco CRS Routers enable the network operator to measure and track video transport performance on a per-flow basis in real time. In contrast to the conventional traffic monitoring solutions, (where sampled flows have to be sent to the control plane or additional hardware, such as dedicated blade on the router), video monitoring on Cisco CRS Router performs the monitoring operation on the data plane itself. This enables video monitoring to analyze forwarded packets in real time, to compute a metric that provides a measure of the network performance impacting the quality of the video.

Local Storage and Remote Access

Video monitoring measures packet loss and jitter at wire-speed, and stores collected information on the router, in order that the network operator can access it through a user interface. Furthermore, the performance metrics measured and stored on multiple routers can be accessed through standard SNMP from a remote operation center. These metrics provide a clear end-to-end picture of the video flow that can be composed and analyzed.

Proactive and Reactive Usages

Video monitoring on Cisco CRS Routers serve both reactive and proactive usage for service providers. It can be used to verify the quality of video service, before scaling up the service coverage to new customers. Also, it is a powerful tool for analysis and can be used to troubleshoot customer calls. Network operators can configure video monitoring to raise an alarm for various events such as variation in packet loss, jitter, flow rate, number of flows, and so on. Such an alarm can be configured to get triggered at any possible value or range.

Flow on Video Monitoring

Video monitoring uses four pieces of packet header fields to distinguish a unique flow - source IP address, destination IP address, source UDP port, and destination UDP port (this implies protocol ID is always UDP).

Unicast and Multicast

Video monitoring supports not only the monitoring of flows with IPv4 multicast destination address in the IP header, but also supports the monitoring of flows with unicast destination addresses.

Flow Rate Types and Protocol Layer

Video monitoring monitors CBR (constant bit rate) flows at the IP layer. In other words, video monitoring can monitor CBR-encoded media streams (for example, MPEG-2) encapsulated in UDP datagram, inside an IPv4 packet. Video monitoring allows users to configure expected packet rate at IP layer, or bit rate at media layer (along with the number and size of media packets).

Metrics

Video monitoring supports both packet loss and jitter metrics that follow MDI (media delivery index, RFC 4445) definition at the IP-UDP level. The MDI metrics are MLR (media loss rate) and DF (delay factor). Video monitoring uses MRV (media rate variation) which is an extension of MDI MLR; that is, MLR captures only loss, while MRV captures both loss and excess. Video monitoring DF is the same as MDI definition, where DF represents one nominal packet inter-arrival time in addition to the monitored MDI jitter. Along with the two key metrics, Video monitoring supports packet count, byte count, packet rate, bit rate, packet size, TTL (Time to Live) field in IP header, number of flows, raised alarms, and time stamp for various events.



Note The term MDI jitter, is used to signify the correctness of DF metric measured by Video monitoring. MDI jitter is measured by comparing the actual packet arrival time against the nominal arrival reference, while simple inter-packet jitter is measured by the time difference between two consecutive packet arrivals. The former captures the performance of CBR flow more precisely than the latter.

For Cisco CRS Router, only MRV is applicable.

High Availability Features

Video monitoring on Cisco CRS Router supports high availability at various levels. It supports process OIR (online insertion and removable), line card OIR, RP (route processor) fail over, and router reload. Configuration is persistent for all high availability scenarios. Monitored statistics data are preserved at process OIR and RP FO.

Interface Types and Direction

To activate video monitoring, you must configure video monitoring service policy on an interface. There are four types of interfaces to which you can attach the video monitoring policy; these are main interface, subinterface, ethernet bundle interface, and ethernet bundle subinterface. Video monitoring supports only layer 3 interfaces and not layer 2 interfaces. Video monitoring can be configured only on the input direction of the interface.

Flow Rate

Video monitoring supports standard definition (SD) video traffic (mostly compressed) of up to 100 Mbps flow rate. For uncompressed video streams, flow rate of max 3 Gbps is supported.

User Interface for Input

Video monitoring supports traditional CLI (command line interface) input for configuration that follows MQC (modular QoS configuration) syntax. You can configure video monitoring by configuring access control list (ACL), class map, and policy map; it can be activated by attaching the service policy to an interface. In-place policy modification is supported.



Note

In place policy modification internally behaves like policy removal and attach. So, flows are newly detected on the interface.

User Interface for Output

Video monitoring offers various show and clear commands for retrieving the monitored statistics. Refer the Video Monitoring Commands on Cisco CRS Routers module in the *Multicast Command Reference for Cisco CRS Routers* for a detailed description of the video monitoring commands.

You can configure TCA (threshold crossing alert) as a part of the policy map to enable video monitoring to generate syslog message for various conditions. You can also retrieve standing alarms by using **show** command or through a SNMP pull. XML is supported by video monitoring.

Number of Class Maps and Policy Maps

To use video monitoring, you must configure class map and policy map that acts as a filter to determine which flow to monitor on the data plane. Video monitoring supports a maximum of 512 class maps per policy-map, and a maximum of 1500 class maps per system. It supports a maximum of 1500 policy maps on the system.

Video PIE Installation

Video monitoring requires video PIE installation. Depending on the RP type, the video pie name has the following version:

- hfr-video-px.pie

Video Monitoring Terminology

To implement and configure video monitoring service on Cisco CRS Routers, you must first understand video monitoring terminology and concepts.

Interval duration and interval updates

Video monitoring analyzes continuously all packets on the data plane for a time period called interval duration, which is configured by the user. Statistics are exported periodically at the end of each interval duration. These exported statistics are called interval updates. The status of a video monitoring flow and its transition is described solely in reference to these interval updates. Also, all exported video monitoring flow statistics are stored in terms of these interval updates.

The interval duration is a vital video monitoring parameter. Video monitoring configuration anchors upon interval duration for functions such as frequency of export, number of exports to store, time to delete inactive flows, and so on. All video monitoring functionalities, including raising alarm (for stopped flows and flows with performance degradation), are based on the contents of interval updates.

Video monitoring flows

A video monitoring flow is an instance of a packet stream whose header fields match the configured class map (and its associated access control list). A unique flow is local to the interface to which a video monitoring service policy is attached. A video monitoring flow is composed of a series of stored interval updates. A unique flow that is created on video monitoring after a monitoring interval is called a new flow.

Flow stop

If the router stops receiving packets on a monitored flow for one full interval update or longer, the monitored flow is considered as being stopped.

Flow resumption

When a stopped video monitoring flow resumes receiving packets, a normal interval update is exported in the next monitoring interval. A resumed flow has one or more zero intervals, followed by a normal interval update.

Flow switchover

A video monitoring flow on an ethernet bundle interface, or on an ethernet bundle sub-interface, may move from one physical member interface to another; that is, the packet stream stops flowing on one interface and starts flowing on another interface. This is defined as a flow switchover. In such a case, if both interfaces are on the same line card, video monitoring treats the pre-switchover flow and the post-switchover flow as the same flow. Otherwise, it treats them as two different flows.

Flow deletion

If a stopped video monitoring flow continues to export zero intervals for a configured timeout (in terms of the number of monitoring intervals), the flow is considered dead and is marked for deletion. The duration for which the user can control inactive flows is indicated using the timeout parameter. The actual deletion for all the marked flows takes place after some delay by the periodic sweeping function. Once deleted, all exported statistics (series of interval updates including zero intervals) are completely removed from storage.

Implementing Video Monitoring

Configuring Video Monitoring is a four-step procedure, which includes configuring the relevant class-maps and policy maps, and binding the video monitoring policy to an interface.

Creating IPv4 Access Lists

This step is similar to typical IPv4 access list creation and configuration. An example configuration of ACL for video monitoring is presented here for quick reference. For more details, refer to the *Implementing Access lists and Prefix lists* chapter of the *IP Addresses and Services Configuration Guide for Cisco CRS Routers*.

This task configures a standard IPv4 access list.

Standard access lists use source addresses for matching operations.



Note Video Monitoring policy allows **deny** statements in ACL configuration, but **deny** statements are treated as **permit**. Also, log or log-input is not supported in ACL configuration.

SUMMARY STEPS

1. **configure**
2. **ipv4 access-list** *name*
3. [*sequence-number*] **remark** *remark*
4. [*sequence-number*] **permit udp** *source* [*source-port*] **destination** [*destination-port*]
5. Repeat Step 4 as necessary, adding statements by sequence number. Use the **no** *sequence-number* command to delete an entry.
6. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure	
Step 2	ipv4 access-list <i>name</i> Example: RP/0/RP0/CPU0:router# ipv4 access-list acl_1	Enters IPv4 access list configuration mode and configures access list acl_1.
Step 3	[<i>sequence-number</i>] remark <i>remark</i> Example: RP/0/RP0/CPU0:router(config-ipv4-acl)# 10 remark Do not allow user1 to telnet out	(Optional) Allows you to comment on the permit statement that follows in the named access list. <ul style="list-style-type: none"> • The remark can be up to 255 characters; anything longer is truncated. • Remarks can be configured before or after permit statements, but their location details should be consistent.

	Command or Action	Purpose
Step 4	<p>[<i>sequence-number</i>] permit udp <i>source</i> [<i>source-port</i>] destination [<i>destination-port</i>]</p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config-ipv4-acl)# 20 permit udp 172.16.0.0/24 eq 5000 host 225.0.0.1 eq 5000</pre>	<p>Allows you to specify the source and destination ports with these conditions.</p> <ul style="list-style-type: none"> • Video monitoring supports only udp. • Use the <i>source</i> keyword to specify the network or host number from which the packet is being sent. • Use the optional <i>source-wildcard</i> argument to specify the wildcard bits to be applied to the source. • Use the <i>destination</i> keyword to specify the network or host number to which the packet is being sent. • Use the optional <i>destination-wildcard</i> argument to specify the wildcard bits to be applied to the destination.
Step 5	Repeat Step 4 as necessary, adding statements by sequence number. Use the no <i>sequence-number</i> command to delete an entry.	Allows you to revise an access list.
Step 6	commit	

Configuring class-map

This task sets up the flow classifier. This may match either an individual flow, or it may be an aggregate filter matching several flows.

SUMMARY STEPS

1. **configure**
2. **class-map type traffic** *class-map-name*
3. **match access-group ipv4** *acl-name*
4. **end-class-map**
5. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure	
Step 2	<p>class-map type traffic <i>class-map-name</i></p> <p>Example:</p> <pre>RP/0/RP0/CPU0:router(config)# class-map type traffic class1</pre>	Enters the class-map mode. The class-map type must always be entered as traffic.

	Command or Action	Purpose
Step 3	match access-group ipv4 <i>acl-name</i> Example: <pre>RP/0/RP0/CPU0:router(config-cmap)# match access-group ipv4 acl1</pre>	Enter the ACL to be matched for this class. Only eight ACL's can be matched per class.
Step 4	end-class-map Example: <pre>RP/0/RP0/CPU0:router(config-cmap)# end-class-map</pre>	Completes the class-map configuration.
Step 5	commit	

Configuring policy-map

The policy map for video monitoring is of the performance-traffic type. Only one level of hierarchy is supported for video monitoring policy-maps. This means that no hierarchical policy map configuration is supported for video monitoring.

The policy map configuration for video monitoring has these three parts:

- Flow parameters configuration: Specifies the different properties of the flow that are monitored such as interval duration, required history intervals, timeout, etc.
- Metric parameters configuration: Specifies the metrics that need to be calculated for the flow that are monitored.
- React parameters configuration: Specifies the parameters, based on which, alerts are generated for the flow.

The configuration hierarchy is from *policy* to *class* to *flow*. This means that all the parameters that are specified above are applied to all flows that match a particular class, in the policy-map. While specifying flow and react parameters for flows matching a given class is optional, its metric parameters is mandatory.

Configuring policy-map with metric parameters

The metric parameters in a policy map can be:

- Layer 3 packet rate or
- Media bit rate (with the number of media packet counts and size in the UDP payload specified).



Note Layer 3 packet rate and Media rate have mutually exclusive configuration commands.

The configuration for each metric parameter is described in this section.

Layer 3 packet-rate

SUMMARY STEPS

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *traffic class-name*
4. **monitor metric ip-cbr**
5. **rate layer3 packet** *packet-rate* pps
6. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure	
Step 2	policy-map type <i>performance-traffic policy-map-name</i> Example: RP/0/RP0/CPU0:router(config)# policy-map type performance-traffic policy1	Enters the policy-map mode. The policy-map type should always be entered as performance traffic.
Step 3	class type <i>traffic class-name</i> Example: RP/0/RP0/CPU0:router(config-pmap)# class type traffic class-name	Enter the class-map to be matched for this policy. Multiple classes can be specified for a single policy.
Step 4	monitor metric ip-cbr Example: RP/0/RP0/CPU0:router(config-pmap-c)# monitor metric ip-cbr	Enters the IP-CBR metric monitor submenu. Note Currently only ip-cbr metric monitoring is supported for video monitoring.
Step 5	rate layer3 packet <i>packet-rate</i> pps Example: RP/0/RP0/CPU0:router(config-pmap-c-ipcbr)# rate layer3 packet packet-rate pps	Specifies the IP layer3 packet rate in packets per second (pps).
Step 6	commit	

Media bit-rate

The metric parameters for media bit-rate consist of the media bit rate, media packet count and packet size. The rate media option enables the user to specify the number of media payload packets (that is MPEG-2 datagrams) that is present in one UDP packet, and the size of each of such media payload. It is mandatory to specify the media bit rate. There are no defaults for packet count and packet size in Cisco IOS XR Software Release 3.9.1. These values must be configured.



Note With the media bit rate configured to 1052800 bps, media packet count to 7, and media packet size to 188 bytes, the media packet rate is 100 pps at layer 3. The calculation is: $1052800 / (7 * 188 * 8) = 100$ pps.

SUMMARY STEPS

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *traffic class-name*
4. **monitor metric ip-cbr**
5. **rate media bit -rate** {bps|kbps|mbps|gbps}
6. **media packet count in-layer3** *packet-count*
7. **media packet size** *packet-size*
8. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure	
Step 2	policy-map type <i>performance-traffic policy-map-name</i> Example: RP/0/RP0/CPU0:router(config)# policy-map type performance-traffic policy1	Enters the policy-map mode. The policy-map type should always be entered as performance traffic.
Step 3	class type <i>traffic class-name</i> Example: RP/0/RP0/CPU0:router(config-pmap)# class type traffic class-name	Enters the class-map to be matched for this policy. Multiple classes can be specified for a single policy.
Step 4	monitor metric ip-cbr Example: RP/0/RP0/CPU0:router(config- pmap-c)# monitor metric ip-cbr	Enters the IP-CBR metric monitor submenu. Note Currently only ip-cbr metric monitoring is supported for video monitoring.
Step 5	rate media bit -rate {bps kbps mbps gbps} Example: RP/0/RP0/CPU0:router(config- pmap-c-ipcbr)# rate media 100 mbps	Specifies the media bit rate for the flow in bps, kbps, mbps or gbps. The configuration can be committed here. Optional parameters can also be specified. Note The default unit of media bit-rate is kbps.
Step 6	media packet count in-layer3 <i>packet-count</i> Example: RP/0/RP0/CPU0:router(config- pmap-c-ipbr)# media packet count in-layer3 10	Specifies the number of media packets for each IP payload.

	Command or Action	Purpose
Step 7	media packet size packet-size Example: <pre>RP/0/RP0/CPU0:router(config-pmap-c-ipcbr)# media packet size 188</pre>	Specifies the size in bytes for each media packet in the IP payload.
Step 8	commit	

Configuring policy-map with flow parameters

The flow parameters in a policy map are optional.

For video monitoring, the data plane continuously monitors the flows and the metrics that are exported at the end of every interval. The duration of this interval and the number of such intervals that need to be stored for each flow (history) can also be optionally specified by the user. You can specify these flow parameters for each flow:

- **Interval Duration:** The time interval at whose end, metrics are exported. This is specified in multiples of 5 (any value between 10 and 300 seconds). The default value is 30.
- **History:** The number of intervals containing flow information (flow ID, metrics, etc.) that needs be stored for each flow. This can be any value between 1 and 60. The default value is 10.
- **Timeout:** The timeout in multiples of interval duration after which an inactive flow is marked for deletion. This can be any value between 2 and 60. The default value is 2.
- **Max Flows per class:** The maximum number of flows that need to be monitored for each class in the policy. This can be any value between 1 and 1024. The default value is 4096.

Monitoring this parameter requires maintaining a count per class in hardware and metro hardware does not provide the functionality to read the stats counter. Due to this limitation, this parameter is not supported. If the user has specified this parameter in the policy, the maximum number of flows per class is limited to maximum number of flows per line card.

SUMMARY STEPS

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *traffic class-name*
4. monitor parameters
5. **{interval duration** *duration* | **flows** *number of flows* | **history** *intervals* | **timeout** *duration* }
6. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure	
Step 2	policy-map type <i>performance-traffic policy-map-name</i> Example:	Enters the policy-map mode. The policy-map type should always be entered as performance traffic.

	Command or Action	Purpose
	RP/0/RP0/CPU0:router(config)# policy-map type performance-traffic policy1	
Step 3	class type <i>traffic class-name</i> Example: RP/0/RP0/CPU0:router(config-pmap)# class type traffic class-name	Enter the class-map to be matched for this policy. Multiple classes can be specified for a single policy.
Step 4	monitor parameters Example: RP/0/RP0/CPU0:router(config-pmap-c)# monitor parameters	Enters the flow monitor submodule.
Step 5	{interval duration <i>duration</i> flows <i>number of flows</i> history <i>intervals</i> timeout <i>duration</i> } Example: RP/0/RP0/CPU0:router(config-pmap-c-fparam)# interval duration 10	<ul style="list-style-type: none"> • Select the interval duration option to specify the interval duration per flow; range is 10 to 300 (must be in multiples of 5). The default value is 30. • Select the history option to specify the maximum number of interval data that will be stored per flow. It can be any value between 1 and 60. The default value is 10. • Select the timeout option to specify the timeout in multiples of the interval duration after which an inactive flow will be marked for deletion. Range is between 2 and 60. The default value is 0, indicating a static flow. • Select the flows option to specify the maximum number of flows that can be monitored per class. Range is between 1 and 1024. The default value is 1024.
Step 6	commit	

Configuring policy-map with react parameters

The react parameters in a policy map are optional.

The react parameters are a direct reference for the user to indicate the flow quality. The flow is continuously monitored, and at the end of the interval duration, the statistics are examined to determine whether the threshold specified by the user for the specific parameter has exceeded. If it has, a syslog alarm is generated on the console. Once the alarm is set, no further syslog notifications are issued for the condition.

The following react parameters are used to configure the policy-map:

- **Media Rate variation (MRV):** video monitoring reacts and generates an alarm if the MRV statistic of the flow crosses the user-specified threshold.

- **Media-Stop:** video monitoring reacts and generates an alarm if a flow stops; this is to indicate that no packets were received for the flow during one full monitoring interval.
- **Packet-Rate:** video monitoring reacts and generates an alarm if the packet rate of the flow crosses the user-specified threshold.
- **Flow-Count:** video monitoring reacts and generates an alarm if the flow count for each class crosses the user-specified threshold.

SUMMARY STEPS

1. **configure**
2. **policy-map type** *performance-traffic policy-map-name*
3. **class type** *traffic class-name*
4. **react react-id** {**mrsv** | **delay-factor** | **packet-rate** | **flow-count** | **media-stop**}
5. **threshold type** **immediate**
6. **threshold value** {**ge** | **gt** | **le** | **lt** | **range**} *limit*
7. **action** **syslog**
8. **alarm severity** {**error** | **critical** | **alert** | **emergency**}
9. **alarm type** {**discrete** | **grouped**}
10. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure	
Step 2	policy-map type <i>performance-traffic policy-map-name</i> Example: <pre>RP/0/RP0/CPU0:router(config)# policy-map type performance-traffic policyl</pre>	Enters the policy-map mode. The policy-map type should always be entered as performance traffic.
Step 3	class type <i>traffic class-name</i> Example: <pre>RP/0/RP0/CPU0:router(config-pmap)# class type traffic class-name</pre>	Enter the class-map to be matched for this policy. Multiple classes can be specified for a single policy.
Step 4	react react-id { mrsv delay-factor packet-rate flow-count media-stop } Example: <pre>RP/0/RP0/CPU0:router(config-pmap-c)# react 1 mrsv</pre>	Enters the react parameter configuration submenu. The react ID specified here needs to be unique for each class. Note For the media-stop react parameter, the threshold-type and threshold-value options are not applicable. For the flow-count react parameter, the alarm-type option is not applicable.

	Command or Action	Purpose
Step 5	threshold type immediate Example: <pre>RP/0/RP0/CPU0:router(config- pmap-c-react)# threshold type immediate</pre>	Specifies the trigger type for the threshold. Currently, the available threshold type is immediate.
Step 6	threshold value {ge gt le lt range} limit Example: <pre>RP/0/RP0/CPU0:router(config- pmap-c-react)# threshold value ge 50</pre>	Specifies the trigger value range for the threshold.
Step 7	action syslog Example: <pre>RP/0/RP0/CPU0:router(config- pmap-c-react)# action syslog</pre>	The action keyword specifies the action to be taken if the threshold limit is surpassed. Currently, snmp and syslog actions are the only options available.
Step 8	alarm severity {error critical alert emergency} Example: <pre>RP/0/RP0/CPU0:router(config- pmap-c-react)# alarm severity critical</pre>	Specifies the alarm severity for syslog.
Step 9	alarm type {discrete grouped} Example: <pre>RP/0/RP0/CPU0:router(config- pmap-c-react)# alarm type discrete</pre>	Specifies the alarm type. Discrete alarm is raised for all the flows that exceed the threshold value. Grouped alarm is raised when a certain number or percentage of the flows exceeds the threshold value.
Step 10	commit	

Configuring service policy on an interface

The configured policy-map must be attached to an interface in ingress direction in order to enable the Video Monitoring service.

For ethernet bundle interface, service policy can be attached to only the bundle parent interface and not to the physical member interfaces. For ethernet bundle sub-interfaces, it can be attached to only sub-interfaces. For VLAN sub-interfaces, the service policy cannot be attached to the main interface.

SUMMARY STEPS

1. **configure**
2. **interface type interface-path-id**

3. **service-policy type performance-traffic input** *policy-name*
4. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure	
Step 2	interface <i>type interface-path-id</i> Example: <pre>RP/0/RP0/CPU0:router(config)# interface type interface-path-id</pre>	Configures an interface and enters interface configuration mode. <ul style="list-style-type: none"> • The type argument specifies an interface type. For more information on interface types, use the question mark (?) online help function. • The instance argument specifies either a physical interface instance or a virtual instance. • The naming notation for a physical interface instance is rack/slot/module/port. The slash (/) between values is required as part of the notation. • The number range for a virtual interface instance varies, depending on the interface type.
Step 3	service-policy type performance-traffic input <i>policy-name</i> Example: <pre>RP/0/RP0/CPU0:router(config-if)# service-policy type performance-traffic input policy1</pre>	Attaches the policy to the interface in the ingress direction.
Step 4	commit	

Configuration Examples for Implementing Video Monitoring

Scenario-1

An ethernet bundle interface has three physical members over which multicast video traffic is flowing at 300 pps for each flow.

Use video monitoring to monitor all the flows on this ethernet bundle, and raise a critical-level alarm, if the per-flow traffic load is over 10 % of expected rate. Raise an error-level alarm if the delay factor is greater than 4 ms. Report the collected statistics every 10 seconds. As long as the flow is active, keep the reported statistics for 10 minutes. Remove flow statistics if no packets are received for 30 seconds.

Example

```
ipv4 access-list sample-acl
 10 permit udp any any
!
```

```

class-map type traffic match-any sample-class
match access-group ipv4 sample-acl
end-class-map
!
policy-map type performance-traffic sample-policy
class type traffic sample-class
monitor parameters
  interval duration 10
  history 60
  timeout 3
!
monitor metric ip-cbr
  rate layer3 packet 300 pps
!
react 100 mrv
  threshold type immediate
  threshold value gt 10.00
  action syslog
  alarm severity error
  alarm type discrete
!
react 101 delay-factor
  threshold type immediate
  threshold value gt 4.00
  action syslog
  alarm severity error
  alarm type discrete
!
end-policy-map
!
interface Bundle-Ether10
ipv4 address 172.192.1.1 255.255.255.0
service-policy type performance-traffic input sample-policy
!
interface TenGigE0/6/0/0
bundle id 10 mode on
!
interface TenGigE0/6/0/1
bundle id 10 mode on
!
interface TenGigE0/6/0/2
bundle id 10 mode on
!

```

Scenario-2

A VLAN subinterface is carrying 100 video streams with a common multicast group address of 225.0.0.1 and varying UDP port numbers. The expected packet rate at IP layer is unknown, but the media bit rate is known to be 1052800 bps. The media payload is known to contain MPEG-2 encoded CBR flows and default packetization is used (that is, in one UDP payload, there are seven MPEG packets, where each packet is 188 bytes long).

Do not monitor over 100 flows. Do not timeout and delete any flow even if flow stops, but raise an error-level alarm if the percentage of the stopped flows is over 90 %.

Example

```

ipv4 access-list sample-acl
10 permit udp any host 225.0.0.1

```



```

!
class-map type traffic match-any sample-class
  match access-group ipv4 sample-acl
end-class-map
!
policy-map type performance-traffic sample-policy
  class type traffic sample-class
  monitor parameters
    flows 100
!
  monitor metric ip-cbr
    rate media 1052800 bps
  !
  react 100 media-stop
  action syslog
  alarm severity error
  alarm type grouped percent 90
  !
end-policy-map
!
interface GigabitEthernet0/0/0/0
  no shutdown
!
interface GigabitEthernet0/0/0/0.1
  encapsulation dot1q 500
  ipv4 address 172.192.1.1 255.255.255.0
  service-policy type performance-traffic input sample-policy
!

```

Under **monitor metric ip-cbr**, these two lines need not be configured as they are defaults:

- media packet count in-layer3 7
- media packet size 188

However, if these parameters are different from default values, they need to be configured.

Scenario-3

A main interface has three groups of multicast streams where the first group has UDP destination port of 1000, the second group has 2000, and the third group has 3000 and 4000. These three groups of streams flow at 100 pps, 200 pps, and 300 pps respectively.

Limit the maximum number of flows in each group to 300 flows and raise the error-level alarm, when they reach 90 % of the provisioned flow capacity.

Example

```

ipv4 access-list sample-acl-1
  10 permit udp any any eq 1000
!
ipv4 access-list sample-acl-2
  10 permit udp any any eq 2000
!
ipv4 access-list sample-acl-3
  10 permit udp any any eq 3000
  20 permit udp any any eq 4000
!
class-map type traffic match-any sample-class-1
  match access-group ipv4 sample-acl-1

```

```

    end-class-map
    !
    class-map type traffic match-any sample-class-2
    match access-group ipv4 sample-acl-2
    end-class-map
    !
    class-map type traffic match-any sample-class-3
    match access-group ipv4 sample-acl-3
    end-class-map
    !
    policy-map type performance-traffic sample-policy
    class type traffic sample-class-1
    monitor parameters
    interval duration 10
    history 60
    timeout 3
    flows 300
    !
    monitor metric ip-cbr
    rate layer3 packet 100 pps
    !
    react 100 flow-count
    threshold type immediate
    threshold value gt 270
    action syslog
    alarm severity error
    !
    class type traffic sample-class-2
    monitor parameters
    interval duration 10
    history 60
    timeout 3
    flows 300
    !
    monitor metric ip-cbr
    rate layer3 packet 200 pps
    !
    react 100 flow-count
    threshold type immediate
    threshold value gt 270
    action syslog
    alarm severity error
    !
    class type traffic sample-class-1
    monitor parameters
    interval duration 10
    history 60
    timeout 3
    flows 300
    !
    monitor metric ip-cbr
    rate layer3 packet 300 pps
    !
    react 100 flow-count
    threshold type immediate
    threshold value gt 270
    action syslog
    alarm severity error
    !
    !
    end-policy-map
    !
    interface GigabitEthernet0/0/0/0
    ipv4 address 172.192.1.1 255.255.255.0

```

```

service-policy type performance-traffic input sample-policy
!

```

Scenario-4

A 10GE main interface receives six high definition (HD) video streams from the digital contents manager (DCM), directly connected to six HD cameras in a sports stadium. Each HD video stream is uncompressed and its bandwidth is as high as 1.611 Gbps at layer 2, which is equivalent to 140625 pps. These six streams are received with multicast groups of 225.0.0.1 through 225.0.0.6, and the UDP port number is 5000.

Raise a critical-level alarm when the delay factor of any flow is above 2 ms, or media loss ratio is above 5 %. Use 10s interval and keep maximum history. Do not monitor more than 6 flows on this interface. Do not time out inactive flows.

Example

```

ipv4 access-list sample-acl
 10 permit udp any eq 5000 225.0.0.0/24 eq 5000
!
class-map type traffic match-any sample-class
 match access-group ipv4 sample-acl
end-class-map
!
policy-map type performance-traffic sample-policy
 class type traffic sample-class
  monitor parameters
   interval duration 10
   history 60
   flows 6
  !
  monitor metric ip-cbr
   rate layer3 packet 140625 pps
  !
  react 100 mrv
   threshold type immediate
   threshold value gt 5.00
   action syslog
   alarm severity critical
   alarm type discrete
  !
  react 200 delay-factor
   threshold type immediate
   threshold value gt 2.00
   action syslog
   alarm severity critical
   alarm type discrete
  !
end-policy-map
!
interface TenGigE0/2/0/0
 ipv4 address 172.192.1.1 255.255.255.0
 service-policy type performance-traffic input sample-policy
!

```

Additional References

Related Documents

Related Topic	Document Title
Multicast command reference document	<i>Multicast Command Reference for Cisco CRS Routers</i>
Getting started material	<i>Cisco IOS XR Getting Started Guide for the Cisco CRS Router</i>
Modular quality of service command reference document	<i>Modular QoS Command Reference for Cisco CRS Routers</i>

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	Title
RFC4445	Proposed Media Delivery Index (MDI)

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