Implementing Video Monitoring Service on Cisco ASR 9000 Series Routers

This module describes how to implement the video monitoring service on Cisco ASR 9000 Series Aggregation Services Routers running Cisco IOS XR software. Video monitoring service monitors application traffic quality (mainly video) by measuring per-flow statistics on the router. The feature provides scalable and efficient inline monitoring of flows.

Feature History for Configuring Multicast Routing on the Cisco ASR 9000 Series Routers

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>The Video Monitoring feature was introduced.</td>
</tr>
<tr>
<td>Release 3.9.1</td>
<td>Included a scenario related to high bandwidth flow support for Video Monitoring service and other related changes.</td>
</tr>
<tr>
<td>Release 4.0.1</td>
<td>Support for Video Flow Monitoring Trap and Clone feature was included.</td>
</tr>
</tbody>
</table>

Contents

- Prerequisites for Implementing Video Monitoring, page 1183
- Information About Implementing Video Monitoring, page 1184
- Implementing Video Monitoring, page 1188
- Configuration examples for Implementing Video Monitoring, page 1205
- Additional References, page 1210

Prerequisites for Implementing Video Monitoring

These prerequisites are required to implement 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 ASR 9000 Series Aggregation Services Router Getting Started Guide.
• 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 ASR 9000 Series Routers.

Information About Implementing Video Monitoring

To implement Video Monitoring features described in this document, you must understand these concepts:

• Introduction to Video Monitoring, page 1184
• Key features supported on Video Monitoring, page 1185
• Video Monitoring Terminology, page 1187

Introduction to 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 the Cisco ASR9000 routers, problems in video flows can be easily diagnosed by 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 similarly) encoded, in most cases. 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 artifact or even a "black screen" at the 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 ASR 9000 Series 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 ASR 9000 Series Router performs the monitoring operation on 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 ASR 9000 Series Router serves 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).

**Multicast vs. Unicast**

In the current release, video monitoring monitors the flows with IPv4 multicast destination address in the IP header. It does not monitor the 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 user to configure 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.

Number of Flows

In the current release, video monitoring on Cisco ASR9000 Series routers support a maximum of 1024 flows per NP (network processor). The number of maximum flows for each line card or for each system varies, depending on the number of NPs on the line card and the number of line cards on the system. Per-chassis flow scale depends on the number of NPs on the chassis.

For example, if you have a Cisco ASR 9000 Series router box with 4 line cards, and if each line card has 8 NPs, per-chassis flow scales up to $1K \times 8 \times 4 = 32K$ flows for each chassis.

High Availability Features

Video monitoring on Cisco ASR 9000 Series Router supports high availability at various levels. It supports process OIR (online insertion and removable), line card OIR, RSP (route switch processor) fail over, and router reload. Configuration is persistent for all high availability scenarios. Monitored statistics data are preserved at process OIR and RSP 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 (that is, L2 transport interfaces on an L2VPN bridge domain). Video monitoring can be configured only on the input direction of the interface.

Flow Rate and DF Precision

Video monitoring on Cisco ASR 9000 Series Router offers DF metric performance of 1 ms precision. Furthermore, video monitoring supports standard definition (SD) video traffic (mostly compressed) of up to 100 Mbps flow rate.
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 not supported. Once attached to an interface, the configured service policy can be modified only after detaching it from 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 ASR 9000 Series Routers module in the Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference 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 1024 class maps per policy-map, and a maximum of 1024 class maps per system. It supports a maximum of 256 policy maps on the system.

Video Monitoring Trap and Clone

Trap and clone is an extension to the basic performance monitoring service feature, where the packets from a selected number of flows can be filtered (trapped), duplicated (cloned), and sent to a remote device on the network for a more fine-grained analysis of the video quality. The cloned packets are replicated by the multicast forwarding process to the the interface specified in the performance traffic clone profile. The remote device can perform a deeper analysis of the data at the MPEG layer level. This device can be used both as a debugging and a monitoring tool. Also, this device can act as a service engine blade on the same router.

Video Monitoring Terminology

To implement and configure video monitoring service on Cisco ASR 9000 Series Routers, you must 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. This 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 one monitoring interval is called a new flow. Thus, a packet stream that lives shorter than one monitoring interval is not exported as a video monitoring flow, and therefore is not stored.

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

If a stopped video monitoring flow starts receiving packets, a normal interval update will be 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 streams stops flowing on one interface and starts flowing on another interface. This is defined as 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. 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 actual deletion for all the marked flows takes place after some delay by the periodic (every 150s) 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, policy maps and binding the video monitoring policy to an interface.

- Creating IPv4 Access Lists, page 1189
- Configuring class-map, page 1190
- Configuring policy-map, page 1192
- Configuring service policy on an interface, page 1201
- Configuring Trap and Clone on an interface, page 1203
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 Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services configuration guide.

This task configures a standard IPv4 access list.

Standard access lists use source addresses for matching operations.

Note

Video Monitoring policy does not allow explicit deny statements in ACL configuration. 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 where you planned. Use the no sequence-number command to delete an entry.
6. end
   
   or
   
   commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 ipv4 access-list name</td>
<td>Enters IPv4 access list configuration mode and configures access list acl_1.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# ipv4 access-list acl_1</td>
<td></td>
</tr>
<tr>
<td>Step 3 [sequence-number] remark remark</td>
<td>(Optional) Allows you to comment on the permit statement that follows in the named access list.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-ipv4-acl)# 10 remark Do not allow user1 to telnet out</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The remark can be up to 255 characters; anything longer is truncated.</td>
</tr>
<tr>
<td></td>
<td>• Remarks can be configured before or after permit statements, but their location should be consistent.</td>
</tr>
</tbody>
</table>
### 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. end or commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> class-map type traffic <strong>class-map-name</strong></td>
<td>Enters the class-map mode. The class-map type must always be entered as traffic.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config)# class-map type traffic class1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> match access-group ipv4 <strong>acl-name</strong></td>
<td>Enter the ACL to be matched for this class. Only one ACL can be matched per class.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-cmap)# match access-group ipv4 acl1</td>
<td></td>
</tr>
</tbody>
</table>
### 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 will be 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 will be monitored.
- **React parameters configuration**: Specifies the parameters, based on which, alerts are generated for the flow.

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong>&lt;br&gt;end-class-map</td>
<td>Completes the class-map configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;RP/0/RSP0/CPU0:router(config-cmap)# end-class-map</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong>&lt;br&gt;end or commit</td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td><strong>Example:</strong>&lt;br&gt;RP/0/RSP0/CPU0:router(config-cmap)# commit</td>
<td></td>
</tr>
</tbody>
</table>

- When you issue the **end** command, the system prompts you to commit changes:
  - Uncommitted changes found, commit them before exiting (yes/no/cancel)?
    - Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
    - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
    - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.
Configuring policy-map with metric parameters

The metric parameters in a policy map can be:

- Layer3 packet rate or
- Media bit rate (with the number of media packet counts and size in the UDP payload specified).

\*\*\* Note \*\*\*

Layer3 packet rate and Media rate have mutually exclusive configuration commands.

The configuration for each case is described in this section.

Layer3 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>configure</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>policy-map type performance-traffic policy-map-name</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Enters the policy-map mode. The policy-map type should always be entered as performance traffic.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>policy-map type performance-traffic policy1</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>class type traffic class-name</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Enter the class-map to be matched for this policy. Multiple classes can be specified for a single policy.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>class type traffic class-name</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>monitor metric ip-cbr</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Enters the IP-CBR metric monitor submode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>monitor metric ip-cbr</code></td>
</tr>
</tbody>
</table>

Note: Currently only ip-cbr metric monitoring is supported for video monitoring.
Implementing Video Monitoring Service on Cisco ASR 9000 Series Routers

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 as 1052800 bps, media packet count as 7, and media packet size as 188 bytes, the media packet rate is 100 pps at layer 3. The calculation is: \( \frac{1052800}{(7 \times 188 \times 8)} = 100 \) 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. end or commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> policy-map type performance-traffic policy-map-name</td>
<td>Enters the policy-map mode. The policy-map type should always be entered as performance traffic.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> class type traffic class-name</td>
<td>Enters the class-map to be matched for this policy. Multiple classes can be specified for a single policy.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> monitor metric ip-cbr</td>
<td>Enters the IP-CBR metric monitor submode.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-pmap-c)# monitor metric ip-cbr</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> Currently only ip-cbr metric monitoring is supported for video monitoring.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> rate media bit-rate {bps</td>
<td>kbps</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# rate media 100 mbps</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> The default unit of media bit-rate is kbps.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> media packet count in-layer3 packet-count</td>
<td>Specifies the number of media packets per IP payload.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-pmap-c-ipcbg)# media packet count in-layer3 10</td>
<td></td>
</tr>
</tbody>
</table>
Implementing Video Monitoring Service on Cisco ASR 9000 Series Routers

 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 the end of which, 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 0. (Note: the timeout value of 0 has a special meaning: the flow will never be timed out and is therefore a static flow).
- **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 1024.

### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong> media packet size packet-size</td>
<td>Specifies the size in bytes for each media packet in the IP payload.</td>
</tr>
</tbody>
</table>

**Example:**

```plaintext
RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# media packet size 188
```

| Step 8 | end or commit | Saves configuration changes. |

**Example:**

```plaintext
RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)
# end
or
RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)
# commit
```

- When you issue the **end** command, the system prompts you to commit changes:
  
  Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:

  - Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
  - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.
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. end or commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router# configure</td>
</tr>
<tr>
<td>Step 2</td>
<td>policy-map type performance-traffic policy-map-name</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1</td>
</tr>
<tr>
<td>Step 3</td>
<td>class type traffic class-name</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name</td>
</tr>
<tr>
<td>Step 4</td>
<td>monitor parameters</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-pmap-c)# monitor parameters</td>
</tr>
</tbody>
</table>
## Implementing Video Monitoring Service on Cisco ASR 9000 Series Routers

### Implementing Video Monitoring

#### Step 5

**Command or Action**

```
(interval duration duration| flows number of flows | history intervals | timeout duration)
```

**Example:**

RP/0/RSP0/CPU0:router(config-pmap-c-fparm)# interval duration 10

**Purpose**

- 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 values are 1024.

#### Step 6

**Command or Action**

```
end
or
commit
```

**Example:**

RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# end

**Purpose**

- **end** saves configuration changes.
- **commit** saves configuration changes.

**Example:**

RP/0/RSP0/CPU0:router(config-pmap-c-ipcbr)# commit

**Note:**

- When you issue the `end` command, the system prompts you to commit changes:

  Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:

  - Entering `yes` saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
  - Entering `no` exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
  - Entering `cancel` leaves the router in the current configuration session without exiting or committing the configuration changes.

- Use the `commit` command to save the configuration changes to the running configuration file and remain within the configuration session.
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 check whether the threshold specified by the user, for the specific parameter, is exceeded. If it is, a syslog alarm is generated on the console. Once the alarm is set, no further syslog notifications are issued for the condition.

- Media Rate variation (MRV): video monitoring reacts and generates an alarm if the MRV statistic of the flow crosses the user-specified threshold.
- Delay Factor: video monitoring reacts and generates an alarm if the Delay Factor statistic of the flow crosses the user-specified threshold.
- Media-Stop: video monitoring reacts and generates an alarm if a flow stops; that 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 {mrv | delay-factor | media-stop | packet-rate | flow-count}
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. end or commit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router# configure</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>policy-map type performance-traffic</code> <code>policy-map-name</code></td>
<td>Enters the policy-map mode. The policy-map type should always be entered as performance traffic.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config)# policy-map type performance-traffic policy1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>class type traffic class-name</code></td>
<td>Enter the class-map to be matched for this policy. Multiple classes can be specified for a single policy.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class-name</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>`react react-id {mrv</td>
<td>delay-factor</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-pmap-c)# react 1 mrv</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>threshold type immediate</code></td>
<td>Specifies the trigger type for the threshold. Currently, the available threshold type is immediate.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-pmap-c-react)# threshold type immediate</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>`threshold value {ge</td>
<td>gt</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-pmap-c-react)# threshold value ge 50</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>action syslog</code></td>
<td>The <strong>action</strong> keyword specifies the action to be taken if the threshold limit is surpassed. Currently, syslog action is the only option available.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-pmap-c-react)# action syslog</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>`alarm severity {error</td>
<td>critical</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-pmap-c-react)# alarm severity critical</td>
<td></td>
</tr>
</tbody>
</table>
Implementing Video Monitoring Service on Cisco ASR 9000 Series Routers

Implementing Video Monitoring

With reference to this configuration procedure, note that:

- 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.

### 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-map-name`
4. `end` or `commit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RSP0/CPU0:router# configure</code></td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>interface type interface-path-id</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RSP0/CPU0:router(config)# interface type interface-path-id</code></td>
</tr>
<tr>
<td></td>
<td>Configures an interface and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• The type argument specifies an interface type.</td>
</tr>
<tr>
<td></td>
<td>• The instance argument specifies either a physical interface instance or a virtual instance.</td>
</tr>
<tr>
<td></td>
<td>• The naming notation for a physical interface instance is rack/slot/module/port. The slash (/) between values is required as part of the notation.</td>
</tr>
<tr>
<td></td>
<td>• The number range for a virtual interface instance varies, depending on the interface type.</td>
</tr>
</tbody>
</table>
### Configuring Trap and Clone on an interface

As trap and clone is an extension of the existing video monitoring service, the current control plane infrastructure can be extended to accommodate the configurations for trap and clone.

You can use the flow tuple information (source and destination IP addresses) to install the trap, which eventually leads the matched packets to be further analyzed by a remote device or a local probe.

These steps show how the trap and clone process works in a generic video monitoring scenario:

1. **You must enable video monitoring by installing the appropriate packages (multicast and video PIEs) and configure ACL, class map, policy map, and bind the policy map to an interface.**
2. **You must configure trap and clone by specifying which flows to clone by specifying the source and the destination of the flows.**
3. **The trap gets installed in the data plane by the VidMon control plane and VidMon data plane starts cloning the packets for the specified flows.**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>service-policy type performance-traffic input policy-name</code></td>
<td>Attaches the policy to the interface in the ingress direction.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-if)# <code>service-policy type performance-traffic input policy1</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td><code>commit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-if)# <code>end</code></td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-if)# <code>commit</code></td>
<td></td>
</tr>
</tbody>
</table>

When you issue the `end` command, the system prompts you to commit changes:

Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:

- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.

Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.
The cloned packets are forwarded to the remote monitoring device for further analysis.

**Note**

You can use the `show performance traffic clone profile` command to verify the installed traps. The Video monitoring trap and clone feature is supported only for multicast traffic. This is implemented using static IGMP groups on the clone interface. The clone interface can be on a dedicated port connected to a local probe.

### SUMMARY STEPS

1. `configure`
2. `performance traffic clone profile`
3. `performance traffic clone profile profile_name description`
4. `interface type interface-path-id`
5. `clone flow ipv4 source <source-ip> destination <destination-ip>`
6. `end` or `commit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td>Enters global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RSP0/CPU0:router# configure</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>performance traffic clone profile</code></td>
</tr>
<tr>
<td>Enters the performance traffic clone profile mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RSP0/CPU0:router(config)# performance traffic clone profile</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>performance traffic clone profile profile_name description</code></td>
</tr>
<tr>
<td>Configures a description to the clone profile.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RSP0/CPU0:router(config-perf-traf-clo ne-profile)# performance traffic clone profile profile1 description</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>interface type interface-path-id</code></td>
</tr>
<tr>
<td>Configures the egress interface to a clone profile.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RSP0/CPU0:router(config-perf-traf-clo ne-profile)# interface GigabitEthernet 0/0/0/1</code></td>
</tr>
</tbody>
</table>
Configuration examples for Implementing Video Monitoring

This section provides configuration examples for different scenarios.

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, and 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.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5 clone flow ipv4 source &lt;source-ip&gt; destination &lt;destination-ip&gt;</td>
<td>Configures the traffic flows that needs to be cloned, to the clone profile.</td>
</tr>
<tr>
<td><strong>Note</strong> Multiple flows can be associated with a single clone profile. Similarly, a single flow can be associated with the multiple clone profiles.</td>
<td></td>
</tr>
<tr>
<td>Step 6 end or commit</td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# end or RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# commit</td>
<td></td>
</tr>
</tbody>
</table>

**Command or Action**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clone flow ipv4 source &lt;source-ip&gt; destination &lt;destination-ip&gt;</td>
<td>Configures the traffic flows that needs to be cloned, to the clone profile.</td>
</tr>
<tr>
<td><strong>Note</strong> Multiple flows can be associated with a single clone profile. Similarly, a single flow can be associated with the multiple clone profiles.</td>
<td></td>
</tr>
<tr>
<td>end or commit</td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# end or RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# commit</td>
<td></td>
</tr>
</tbody>
</table>

**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, and 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.

**Command or Action**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clone flow ipv4 source &lt;source-ip&gt; destination &lt;destination-ip&gt;</td>
<td>Configures the traffic flows that needs to be cloned, to the clone profile.</td>
</tr>
<tr>
<td><strong>Note</strong> Multiple flows can be associated with a single clone profile. Similarly, a single flow can be associated with the multiple clone profiles.</td>
<td></td>
</tr>
<tr>
<td>end or commit</td>
<td>Saves configuration changes.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# end or RP/0/RSP0/CPU0:router(config-perf-traf-clone-profile)# commit</td>
<td></td>
</tr>
</tbody>
</table>

**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, and 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
```
Configuration examples for Implementing Video Monitoring

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
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

```plaintext
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
!```
Scenario-5

An ethernet interface is configured on a Cisco ASR 9000 Series Router over which multicast video traffic is flowing. Use video monitoring to monitor the performance of all video flows on this ethernet interface. Use the video monitoring trap and clone feature to trap these flow packets and clone (or duplicate) them to a specified egress interface.

Configure a trap and clone profile containing flows that are to be cloned to the specified egress interface. Add a description to the profile.

Example

```
Performance traffic clone profile profile1
   Description video flows monitored by vidmon
   Interface GigE 0/1/1/1
   flow ipv4 source 23.1.1.1 destination 231.2.2.2
```

Additional References

These sections provide references related to implementing multicast routing on Cisco IOS XR software.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast command reference document</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference</td>
</tr>
<tr>
<td>Getting started material</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide</td>
</tr>
<tr>
<td>Modular quality of service command reference document</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC4445</td>
<td>Proposed Media Delivery Index (MDI)</td>
</tr>
</tbody>
</table>
## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>searchable technical content, including links to products, technologies,</td>
<td></td>
</tr>
<tr>
<td>solutions, technical tips, and tools. Registered Cisco.com users can log</td>
<td></td>
</tr>
<tr>
<td>in from this page to access even more content.</td>
<td></td>
</tr>
</tbody>
</table>