

## Appendix

### IP Video Surveillance QoS Reference Chart

The reference chart in [Figure A-1](#) is useful when implementing IP video surveillance on routers and switches. The formula for converting a ToS byte value to DSCP using decimal values is to divide the ToS byte number by 4. Example ToS decimal value of 160 / 4 = 40. The DSCP value of '40' is CS5.

**Figure A-1** IP Video Surveillance QoS Reference Chart

Hex	ToS Decimal	IP Precedence	Class-map Name	DSCP	Binary
E0	224	7 Network Control		56 CS7	11100000
C0	192	6 Internetwork Control	NETWORK-CONTROL	48 CS6	11000000
B8	184		VOICE	46 EF	10111000
A0	160	5 Critical	BROADCAST-VIDEO	40 CS5	10100000
88	136			34 AF41	10001000
80	128	4 Flash Override		32 CS4	10000000
68	104			26 AF31	01101000
60	96	3 Flash	CALL-SIGNALING	24 CS3	01100000
48	72			18 AF21	01010000
40	64	2 Immediate	OAM	16 CS2	01000000
20	32	1 Priority		8 CS1	00100000
00	0	0 Routine		0 Dflt	00000000

### IP SLA Probe Sample Configurations

These are sample IP SLA UDP Jitter operation probes which can be used as a baseline for determining a range of network performance suitable for transporting video surveillance media feeds. It is assumed that sufficient bandwidth exists between source and sink nodes. These probes are reporting on a range of network latency, jitter and loss which should provide acceptable video quality.



**Tip**

Reported MOS score values of 4 or above should be expected to provide a baseline for serviceable video quality.

## WAN Latency Probe

This probe provides a baseline for a WAN connection suitable for transporting H.264 based video.

```
no ip sla 1090
ip sla 1090
  udp-jitter 10.81.0.26 16090 source-ip 10.81.7.25 codec g729a codec-numpackets 50
  tos 160
  threshold 100
  timeout 500
  owner VideoSurveillance
  tag IPVS_test_probe
ip sla schedule 1090 start-time now life 7200
```

The round trip time (RTT) is approximately 30ms with jitter of approximately 2ms. No loss was detected, however, this probe only generates 50 sample packets.

```
zhallxxx-vpn-881#show ip sla stat 1090
IPSLAs Latest Operation Statistics

IPSLA operation id: 1090
  Latest RTT: 30 milliseconds
Latest operation start time: 17:34:05.074 edt Mon Jul 13 2009
Latest operation return code: OK
RTT Values:
  Number Of RTT: 50                      RTT Min/Avg/Max: 28/30/42 milliseconds
Latency one-way time:
  Number of Latency one-way Samples: 50
  Source to Destination Latency one way Min/Avg/Max: 12/13/22 milliseconds
  Destination to Source Latency one way Min/Avg/Max: 15/17/29 milliseconds
Jitter Time:
  Number of SD Jitter Samples: 49
  Number of DS Jitter Samples: 49
  Source to Destination Jitter Min/Avg/Max: 0/2/9 milliseconds
  Destination to Source Jitter Min/Avg/Max: 0/2/9 milliseconds
Packet Loss Values:
  Loss Source to Destination: 0           Loss Destination to Source: 0
  Out Of Sequence: 0           Tail Drop: 0
  Packet Late Arrival: 0       Packet Skipped: 0
Voice Score Values:
  Calculated Planning Impairment Factor (ICPIF): 11
MOS score: 4.06
Number of successes: 1
Number of failures: 0
Operation time to live: 7187 sec
```

## LAN Latency Probe

This probe is from the test lab environment and has expected LAN latency. In LAN environments, RTT is expected to be less than 4ms, jitter should be reported as zero (0), and loss should approach zero.

```
no ip sla 22
ip sla 22
  udp-jitter 192.0.2.1 16000 codec g729a codec-numpackets 50
  tos 160
  timeout 500
  threshold 100
  owner VideoSurveillance
  tag IPVS_test_probe
```

```

vrf IPVS
ip sla schedule 22 start now life 7200

vpn-jk2-7206-1#show ip sla stat 22

Round Trip Time (RTT) for      Index 22
    Latest RTT: 1 milliseconds
Latest operation start time: 09:56:54.073 edt Tue Jul 14 2009
Latest operation return code: OK
RTT Values:
    Number Of RTT: 50                RTT Min/Avg/Max: 1/1/2 milliseconds
Latency one-way time:
    Number of Latency one-way Samples: 0
    Source to Destination Latency one way Min/Avg/Max: 0/0/0 milliseconds
    Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds
Jitter Time:
    Number of SD Jitter Samples: 49
    Number of DS Jitter Samples: 49
    Source to Destination Jitter Min/Avg/Max: 0/0/0 milliseconds
    Destination to Source Jitter Min/Avg/Max: 0/1/1 milliseconds
Packet Loss Values:
    Loss Source to Destination: 0                Loss Destination to Source: 0
    Out Of Sequence: 0                Tail Drop: 0
    Packet Late Arrival: 0    Packet Skipped: 0
Voice Score Values:
    Calculated Planning Impairment Factor (ICPIF): 11
MOS score: 4.06
Number of successes: 2
Number of failures: 0
Operation time to live: 7130 sec

```

**Tip**


---

Historically, the minimum interval between clock interrupts in Cisco IOS has been 4ms. Reporting values between 0 and 4ms may not be precise.

---

## Access-layer Switch Commands

The following **show** commands are from the Cisco Catalyst 3750 Series switch. These commands illustrate how to determine what interface a particular Cisco IP camera is attached and what data rate the camera is streaming to the Media Server.

### Determine Interface

Determine which interface a particular camera is attached by specifying the last four digits of the MAC address of the camera as a filter to the **show cdp neighbors** command. The MAC address is printed on the exterior label of the camera. In this example, the last four digits are '79D3'. The entire MAC address can be specified, but usually the last four digits are unique in the small population of cameras attached to an individual switch.

```

3750-access#show cdp neighbors detail | begin 79D3
Device ID: 001DE5EA79D3
Entry address(es):
  IP address: 192.0.2.52
Platform: CIVS-IPC-2500, Capabilities: Host

```

```
Interface: GigabitEthernet1/0/2, Port ID (outgoing port): eth0
[output truncated]
```

## Determine Data Rate

From the output above, the camera in question is at IP address 192.0.2.52 on interface GigabitEthernet1/0/2. To view the interface statistics, the **show interfaces** command can be issued for the target interface.

```
3750-access#show interfaces gigabitEthernet 1/0/2
GigabitEthernet1/0/2 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 0019.2f98.0102 (bia 0019.2f98.0102)
  Description: Cisco Video Surveillance 2500 Series IP Camera
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 2/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:49, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:08:50
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  1 minute input rate 1082000 bits/sec, 107 packets/sec
  1 minute output rate 0 bits/sec, 0 packets/sec
[output truncated]
```

From the output above, the video feed of the camera is transmitting approximately 1Mbps at 107 packets per second over the time period of the last minute. The **load-interval interface** command has overridden the default value of 5 minutes to 1 minute in this example.

The **show interfaces** command can also be issued with the **summary** keyword and this method provides useful information on transmitted and received data rates as well as queue drops.

```
3750-access#show interfaces g1/0/2 summary
```

```
*: interface is up
IHQ: pkts in input hold queue      IQD: pkts dropped from input queue
OHQ: pkts in output hold queue     OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)           RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)           TXPS: tx rate (pkts/sec)
TRTL: throttle count

  Interface                IHQ   IQD   OHQ   OQD   RXBS  RXPS   TXBS  TXPS  TRTL
  -----
* GigabitEthernet1/0/2      0     0     0     0 1097000 108     0     0     0
```



### Tip

The asymmetrical bandwidth consumption of IP video surveillance is evident in the above display. The sample camera is configured with a resolution of D1 at a constant bit rate (CBR) of 1Mbps using MPEG-4 as the codec. The switch is receiving approximately 1Mbps from the camera, but transmitting zero (0) Mbps to the camera.

## Interface Configuration

The interface configuration for the sample camera is shown below.

```
3750-access#show run int g 1/0/2
Building configuration...

Current configuration : 409 bytes
!
interface GigabitEthernet1/0/2
  description Cisco Video Surveillance 2500 Series IP Camera
  switchport access vlan 208
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 001d.e5ea.79d3
  load-interval 60
  mls qos trust dscp
  macro description CIVS-IPC-2500
  spanning-tree portfast
  spanning-tree bpdupfilter enable
end
```

## Service-module session command

The **service-module session** command is used to Telnet into the NME-VMSS Cisco Video Management and Storage System NME and the EVM-IPVS-16A 16-port Analog Video Gateway for management. When these logical interfaces are configured in a VRF (*ip vrf forwarding IPVS*, for example) the **service-module session** command will fail because the interface IP address in the the VRF and the session is initiated from the global routing table.

A circumvention is to initiate the **service-module session** command, identify the IP address and port number (see *Trying 192.0.2.1, 2066 ...* below), allow the session command to timeout or reset (CTL+SHIFT6+x), and then issue a Telnet command sourcing from the VRF. Examples are shown below for both types of modules.

```
vpn1-2851-1#service-module integrated-Service-Engine 1/0 session
Trying 192.0.2.1, 2066 ...
% Connection reset by user
```

```
vpn1-2851-1#telnet 192.0.2.5 2066 /vrf IPVS
Trying 192.0.2.1, 2066 ... Open
```

```
=
==
=== Site 130    === vpn1-2851-1
==
=
SITE130-VSM>
```

```
vpn1-2851-1#service-module video-Service-Engine 2/0 session
Trying 192.0.2.5, 2130 ...
% Connection reset by user
```

```
vpn1-2851-1#telnet 192.0.2.5 2130 /vrf IPVS
Trying 192.0.2.5, 2130 ... Open
```

```
=  
==  
=== Site 130    === vpn1-2851-1  
==  
=  
SITE130-Analog-Gateway>
```

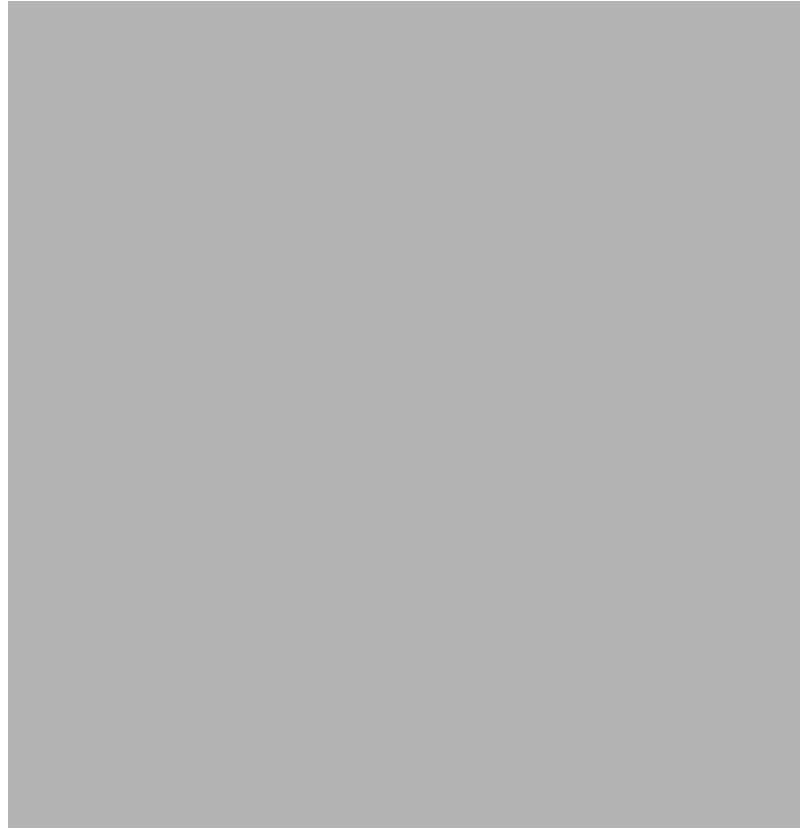
## IP Multicast

In IP multicast transmissions, a host sends one copy of each packet to a special address that can be used by several hosts interested in receiving the packets. Those hosts are members of a designated multicast group and can be located anywhere on the network. Using IP multicast to transmit video traffic reduces the overall network load and minimizes the impact on the source of the video from unnecessary replication of a common data stream.

By using multicast protocols, the hosts that want to receive traffic from a multicast group can join and leave the group dynamically. Hosts can be members of more than one group and must explicitly join a group before receiving content. Since IP multicast traffic relies on UDP, which, unlike TCP, has no built-in reliability mechanism such as flow control or error recovery mechanisms, tools such as QoS can improve the reliability of a multicast transmission.

Some edge devices may communicate with the Media Server using unicast or multicast communications. The use of IP Multicast offers some benefits when a video stream is to be archived by several Media Servers, since only a single stream is required from the IP camera or encoder.

[Figure A-2](#) shows an example where a single multicast stream is generated by an IP camera and archived by two Media Servers. The Media Servers propagate the video streams to the viewers using IP Unicast transmission. Using multicast protocols, Cisco routers and switches replicate the video stream to only the segments and hosts that require it, using approximately 8 Mbps of bandwidth throughout the network.

**Figure A-2** *IP Multicast***Note**

The Media Server only supports IP unicast between the Media Server and the viewers, but it can communicate through IP multicast with edge devices that support IP multicast.

## Multicast Addressing

IP multicast uses the class D range of IP addresses, from 224.0.0.0 through 239.255.255.255. Within this range, several addresses are reserved by the Internet Assigned Numbers Authority (IANA):

- **224.0.0.0 through 224.0.0.255**—Link-Local addresses that are used by network protocols only in a local segment.
- **224.0.1.0 through 238.255.255.255**—Globally scoped addresses that can be routed across the Internet or any organization. They are unique and globally significant.
- **239.0.0.0 through 239.255.255.255**—Used in private domains and not routed between domains. Similar to the IP address range from RFC1918.

## Forwarding Multicast Traffic

Forwarding multicast packets through a network is different than unicast routing. With unicast traffic, routers consider the destination address and how to find the single destination host. In multicast traffic, the source sends traffic to a multicast group address, which in turn can be reached by multiple hosts or receivers.

Routers rely on distribution trees to reach all multicast receivers. The two types of multicast trees are as follows:

- **Source trees**—The root is located at the multicast source and a tree to all receivers is formed via the shortest path tree (SPT).
- **Shared trees**—The root is not necessarily the multicast source. The tree is shared by all sources relying on a defined common root. This shared root is the Rendezvous Point (RP).

Similar to IP unicast, IP multicast traffic uses its own Layer 2, management, and routing protocols.

Figure A-3 shows the interaction between these different protocols.

**Figure A-3**      *Interaction Between IGMP and PIM*



- PIM is the multicast routing protocol that is responsible for building multicast delivery trees and for enabling multicast packet forwarding.
- IGMP is used by hosts to dynamically register to multicast groups. The communication occurs between the router and the host.
- IGMP snooping is used to prevent multicast flows from flooding all ports on a VLAN by monitoring the Layer 3 IGMP packets.

## Proxy Processes

Proxy processes allow for the replication of individual video feeds at different frame rates for multiple users or system processes. When a video feed is first registered with the Media Server, the server creates a proxy or process to manage connections and video streams from video sources into the Media Server.

The Media Server can support a large number of proxy processes on a single server or an architecture with distributed proxy processes on multiple Media Servers.

There are two types of proxy processes:

- [Direct Proxy](#)
- [Parent-Child Proxies](#)



## Direct Proxy

A direct proxy is the process created on the Media Server to maintain connectivity with the edge device (IP camera or encoder). The proxy is capable of requesting video from the edge device with different video configurations such as frame rate and video resolution. One direct proxy exists for a given video stream.

In the example in [Figure A-4](#), the Media Server maintains connectivity and receives video from four different IP cameras. The Media server is responsible for replicating the video feeds to four different viewers.

**Figure A-4**      *Direct Proxy*



[Table A-1](#) shows the active processes from [Figure A-4](#). The four OM viewers are viewing live video from different cameras; each of the viewers is receiving the video feeds directly from the Media Server. The Media Server is receiving four unique video streams, replicating them a total of 11 times.

**Table A-1**      *Active Processes*

Video Source	Active Viewers	Number of Active Streams from the Media Server to Clients
Camera A	Viewer 1, Viewer 2, Viewer 3, Viewer 4	4
Camera B	Viewer 2, Viewer 2, Viewer 4	3 (two streams to Viewer 2)
Camera C	Viewer 1, Viewer 2, Viewer 4	3
Camera D	Viewer 1	1
Total Streams		11

## Parent-Child Proxies

Video feeds can originate from the direct proxy or from a different Media Server. A proxy video feed can be the parent to another video feed served by a different Media Server. Parent proxies may be from remote or local hosts and may be nested in a hierarchy with inheritance rights.

A direct proxy becomes a parent when a child proxy is created. A child proxy receives its video directly from a parent proxy. A child proxy has the same resolution, quality, and media type of its parent, but in the case of MJPEG video streams, a lower frame rate may be configured for the child feed.

Parent-child proxies allow for more efficient network utilization by distributing video feeds closer to the viewers. This is very important in environments with remote branch offices or with limited bandwidth available for video delivery. By replicating a single video feed to a location with several viewers, the bandwidth requirements throughout the network are reduced.

In order to conserve bandwidth, the child process connects to the parent source only when video streaming is requested by a viewer.

In [Figure A-5](#), Media Server MS1 is acting as the parent for two feeds that are served by Media Server MS2. Video feeds from cameras A and B are replicated to Media Server MS2, which in turn can be served to a large number of users or other child feeds.

The environment in [Figure A-5](#) has generated a total of six proxy processes:

- Media Server MS1 is the direct proxy to four edge devices but also replicates eleven different video streams to other viewers or child feeds.
- Media Server MS2 has created two child proxy feeds, Child A and Child B. These feeds can be propagated to any viewers locally on Site B, reducing the bandwidth requirements across the wide area connections.

**Figure A-5**      *Parent-Child Proxy*



Table A-2 shows the different streams required to distribute the video feeds from Figure A-5.

**Table A-2** *Parent-Child Proxies*

Video Source	Active Viewers	Number of Active Streams from the Media Server to Clients
Camera A	Viewer1, Viewer 2, MS2	3
Camera B	Viewer 2, Viewer 2, MS2	3 (two streams to OM Viewer 2)
Camera C	Viewer 1, Viewer 2	2
Camera D	Viewer 1, Viewer 3, Viewer 4	3
Parent A	MS2	1
Parent B	MS2	1
Child A	Viewer 3, Viewer 4	2
Child B	Viewer 4	1
Site B: Local Streams		3
Site B: Remote Streams		4

Since Media Servers do not provide transcoding features, the video quality and resolution remain the same for all child feeds. When using MJPEG streams, the frame rate can be lowered to reduce the bandwidth utilization by child feeds. Figure A-6 shows an example of how frame rates can be lowered between parent and child feeds. The original video feed for all cameras is 30 fps, but is reduced to 15 fps by child feeds A and B in order to conserve bandwidth.

The example in Figure A-6 also shows how video feeds can be replicated indefinitely between Media Servers. In this example, Media Server MS1 is the direct proxy to three IP camera feeds. In turn, two of the feeds are parents for feeds going into Media Server MS2.

**Figure A-6** *MJPEG Frame Rate Reduction for Child Feeds*



**Note**

The frame rate of a MJPEG child feed can only be equal to or lower than the parent feed.

# Glossary

<b>A</b>	
<b>Alarm</b>	The action or event that triggers an alarm for which an event profile is logged. Events can be caused by an encoder with serial contact closures, a motion detected above defined thresholds, or another application using the soft-trigger command API.
<b>Alarm Trigger</b>	The action or event that triggers an alarm for which an event profile is logged. Events can be caused by an encoder with serial contact closures, a motion detected above defined thresholds, another application using the soft-trigger command API, or a window or door opening/closing.
<b>Alert</b>	The action or event that triggers an alarm for which an event profile is logged. Events can be caused by an encoder with serial contact closures, a motion detected above defined thresholds, or another application using the soft-trigger command API.
<b>API</b>	Application Programming Interface
<b>Archive</b>	A place in which records or historical documents are stored and/or preserved. An archive is a collection of video data from any given proxy source. This enables a feed from a camera-encoder to be stored in multiple locations and formats to be viewed at a later time. There are three types of archives: Regular, where the archive recording terminates after a pre-set time duration lapses and is stored for the duration of its Days-to-Live. Loop, where the archive continuously records until the archive is stopped. Loop archives reuse the space (first-in-first-out) allocated after every completion of the specified loop time. Clip, the source of the archive is extracted from one of the previous two types and is stored for the duration of its Days-to-Live.
<b>Archive Clip</b>	The source of the archive that is extracted from one of the other two types and stored for the duration of its Days-to-Live.
<b>Archive Server</b>	Programs which receive incoming video streams or loops, interprets them, and takes the applicable action.
<b>Archiver</b>	An application that manages off-line storage of video/audio onto back-up tapes, floppy disks, optical disks, etc.
<b>C</b>	
<b>Camera Controls</b>	Permits users to change the camera lens direction and field view depth. Panning a camera moves its field of view back and forth along a horizontal axis. Tilting commands move it up and down the vertical axis. Zooming a camera moves objects closer to or further from the field of view. Many of these cameras also include focus and iris control. A camera may have a subset of these features such as zoom, pan, or tilt only.
<b>Camera Drivers</b>	Responsible for converting standardized URL commands supported by the module into binary control protocols read by a specific camera model.

<b>Child Proxy</b>	<p>An agent, process, or function that acts as a substitute or stand-in for another. A proxy is a process that is started on a host acting as a source for a camera and encoder. This enables a single camera-encoder source to be viewed and recorded by hundreds of clients. There are three types of proxies:</p> <p>A “direct” proxy is the initial or direct connection between the edge camera-encoder source. By definition at least one direct proxy exists for a given video source.</p> <p>A “parent” proxy is the source of a nested or child proxy. Parent proxies may be from remote or local hosts. Proxies are nested in a hierarchy with inheritance rights.</p> <p>A “child” proxy is the result of a nested or parent proxy. Child proxies run on the local host. Proxies are nested in a hierarchy with inheritance rights. A child proxy has the same resolution, quality, and media type of its parent, but can have a lower framerate for motion JPEG.</p>
<b>Clip</b>	<p>A place in which records or historical documents are stored and/or preserved. An archive is a collection of video data from any given proxy source. This enables a feed from a camera-encoder to be stored in multiple locations and formats to be viewed at a later time. There are three types of archives:</p> <p>Regular: where the archive recording terminates after a pre-set time duration lapses and is stored for the duration of its Days-to-Live.</p> <p>Loop: where the archive continuously records until the archive is stopped. Loop archives reuse the space (first-in-first-out) allocated after every completion of the specified loop time.</p> <p>Clip: the source of the archive is extracted from one of the previous two types and is stored for the duration of its Days-to-Live.</p>
<b>D</b>	
<b>Direct Proxy</b>	<p>An agent, process, or function that acts as a substitute or stand-in for another. A proxy is a process that is started on a host acting as a source for a camera and encoder. This enables a single camera-encoder source to be viewed and recorded by hundreds of clients. There are three types of proxies: A “direct” proxy is the initial or direct connection between the edge camera-encoder source. By definition at least one direct proxy exists for a given video source. A “parent” proxy is the source of a nested or child proxy. Parent proxies may be from remote or local hosts. Proxies are nested in a hierarchy with inheritance rights. A “child” proxy is the result of a nested or parent proxy. Child proxies run on the local host. Proxies are nested in a hierarchy with inheritance rights. A child proxy has the same resolution, quality, and media type of its parent, but can have a lower frame rate for motion JPEG.</p>
<b>DVR</b>	Digital Video Recorder/Recording: broadcasts on a hard disk drive which can then be played back at a later time
<b>E</b>	
<b>Encoder Driver</b>	Sends the output of a camera driver to the encoder to which the camera is attached (via the network protocol supported by a particular type of encoder).
<b>ES</b>	Cisco Video Surveillance Encoding Server
<b>Event</b>	<p>When an incident or event occurs, it is captured by a device or application and is tagged. An event is a collection of information about an incident, including name, associated video sources, and a timestamp. If the event setup includes triggered clips, an event will have trigger tracking or video data associated directly with it. Users will need to use the event log to refer to times within a referenced archive, typically a master loop. By using the API to seek to a specific UTC timestamp, events can be used to look up occurrences in an archive that were not necessarily associated with the original event.</p>

<b>Event Setup</b>	A collection of processes and configurations designed to track and notify when alarms or alerts are triggered. Types of event profiles includes event trigger tracking only, event triggers with archive clips, and motion detection. When an event profile includes a trigger from an encoder, part of the profile includes scripts copied to the encoder which release an event notification. When an event profile includes event triggered clips, a pre-post buffer archive is started from the proxies associated with the event profile. Once a trigger occurs, a clip is extracted from the pre-post buffer.
<b>F</b>	
<b>Feed</b>	The transmission of a video signal from point to point.
<b>FPS</b>	Frames Per Second
<b>Frame Rate</b>	The rate at which the source is being recorded. For motion JPEG sources, the play rate is the number of frames-per-second or fps. For MPEG sources, the play rate is the number of megabits-per-second or Mbps and kilobits per second or Kbps.
<b>H</b>	
<b>HTTP</b>	Hypertext Transfer Protocol
<b>J</b>	
<b>J2EE</b>	Java 2 Enterprise Edition
<b>JPEG</b>	JPEG (pronounced “jay-peg”) stands for Joint Photographic Experts Group, the original name of the committee that wrote the standard. JPEG is designed for compressing full color or gray-scale images of natural, real-world scenes. JPEG is “lossy,” meaning that the decompressed image is not exactly the same as the original. A useful property of JPEG is that the degree of lossiness can be varied by adjusting compression parameters. This means that the image maker can trade off file size against output image quality. The play rate is the number of frames-per-second or fps.
<b>K</b>	
<b>Kbps</b>	The rate at which the source is being recorded. For motion JPEG sources, the play rate is the number of frames-per-second or fps. For MPEG sources, the play rate is the number of megabits-per-second or Mbps and kilobits per second or Kbps.
<b>L</b>	
<b>Layout</b>	The geometric description of one or more video panes.
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>Loop</b>	A loop is a hardware or software device which feeds the incoming signal or data back to the sender. It is used to aid in debugging physical connection problems.
<b>M</b>	
<b>Mbps</b>	The rate at which the source is being recorded. For motion JPEG sources, the play rate is the number of frames-per-second or fps. For MPEG sources, the play rate is the number of megabits-per-second or Mbps and kilobits per second or Kbps.
<b>Media Server</b>	A device that processes multimedia applications.
<b>MPEG</b>	MPEG (pronounced “em-peg”) stands for Moving Picture Experts Group and is the name of family of standards used for the compression of digital video and audio sequences. MPEG files are smaller for and use very sophisticated compression techniques. The play rate is the number of megabits-per-second or Mbps and kilobits per second or Kbps.
<b>N</b>	
<b>NTSC</b>	National Television System Committee
<b>P</b>	

<b>Pan-Tilt-Zoom Controls</b>	Permits users to change the camera lens direction and field view depth. Panning a camera moves its field of view back and forth along a horizontal axis. Tilting commands move it up and down the vertical axis. Zooming a camera moves objects closer to or further from the field of view. Many of these cameras also include focus and iris control. A camera may have a subset of these features such as zoom, pan, or tilt only.
<b>Parent proxy</b>	An agent, process, or function that acts as a substitute or stand-in for another. A proxy is a process that is started on a host acting as a source for a camera and encoder. This enables a single camera-encoder source to be viewed and recorded by hundreds of clients. There are three types of proxies: A “direct” proxy is the initial or direct connection between the edge camera-encoder source. By definition at least one direct proxy exists for a given video source. A “parent” proxy is the source of a nested or child proxy. Parent proxies may be from remote or local hosts. Proxies are nested in a hierarchy with inheritance rights. A “child” proxy is the result of a nested or parent proxy. Child proxies run on the local host. Proxies are nested in a hierarchy with inheritance rights. A child proxy has the same resolution, quality, and media type of its parent, but can have a lower frame rate for motion JPEG.
<b>Proxy</b>	An agent, process, or function that acts as a substitute or stand-in for another. A proxy is a process that is started on a host acting as a source for a camera and encoder. This enables a single camera-encoder source to be viewed and recorded by hundreds of clients. There are three types of proxies: A “direct” proxy is the initial or direct connection between the edge camera-encoder source. By definition at least one direct proxy exists for a given video source. A “parent” proxy is the source of a nested or child proxy. Parent proxies may be from remote or local hosts. Proxies are nested in a hierarchy with inheritance rights. A “child” proxy is the result of a nested or parent proxy. Child proxies run on the local host. Proxies are nested in a hierarchy with inheritance rights. A child proxy has the same resolution, quality, and media type of its parent, but can have a lower frame rate for motion JPEG.
<b>Proxy Command</b>	A URL-based API that is neither application-platform nor programming language specific. Commands are sent to dynamically loaded modules (e.g. info.bwt, command.bwt, event.bwt, &c.) using arguments in the form of name-value pairs.
<b>Proxy Server</b>	An agent, process, or function that acts as a substitute or stand-in for another. A proxy is a process that is started on a host acting as a source for a camera and encoder. This enables a single camera-encoder source to be viewed and recorded by hundreds of clients. There are three types of proxies: A “direct” proxy is the initial or direct connection between the edge camera-encoder source. By definition at least one direct proxy exists for a given video source. A “parent” proxy is the source of a nested or child proxy. Parent proxies may be from remote or local hosts. Proxies are nested in a hierarchy with inheritance rights. A “child” proxy is the result of a nested or parent proxy. Child proxies run on the local host. Proxies are nested in a hierarchy with inheritance rights. A child proxy has the same resolution, quality, and media type of its parent, but can have a lower frame rate for motion JPEG.
<b>Proxy Source</b>	An agent, process, or function that acts as a substitute or stand-in for another. A proxy is a process that is started on a host acting as a source for a camera and encoder. This enables a single camera-encoder source to be viewed and recorded by hundreds of clients. There are three types of proxies: A “direct” proxy is the initial or direct connection between the edge camera-encoder source. By definition at least one direct proxy exists for a given video source. A “parent” proxy is the source of a nested or child proxy. Parent proxies may be from remote or local hosts. Proxies are nested in a hierarchy with inheritance rights. A “child” proxy is the result of a nested or parent proxy. Child proxies run on the local host. Proxies are nested in a hierarchy with inheritance rights. A child proxy has the same resolution, quality, and media type of its parent, but can have a lower frame rate for motion JPEG.



<b>PTZ: Pan Tilt Zoom</b>	Permits users to change the camera lens direction and field view depth. Panning a camera moves its field of view back and forth along a horizontal axis. Tilting commands move it up and down the vertical axis. Zooming a camera moves objects closer to or further from the field of view. Many of these cameras also include focus and iris control. A camera may have a subset of these features such as zoom, pan, or tilt only.
<b>R</b>	
<b>Rate</b>	The rate at which the source is being recorded. For motion JPEG sources, the play rate is the number of frames-per-second or fps. For MPEG sources, the play rate is the number of megabits-per-second or Mbps and kilobits per second or Kbps.
<b>Record Rate</b>	The rate at which the source is being recorded. For motion JPEG sources, the play rate is the number of frames-per-second or fps. For MPEG sources, the play rate is the number of megabits-per-second or Mbps and kilobits per second or Kbps.
<b>Recording</b>	A place in which records or historical documents are stored and/or preserved. An archive is a collection of video data from any given proxy source. This enables a feed from a camera-encoder to be stored in multiple locations and formats to be viewed at a later time. There are three types of archives: Regular, where the archive recording terminates after a pre-set time duration lapses and is stored for the duration of its Days-to-Live. Loop, where the archive continuously records until the archive is stopped. Loop archives reuse the space (first-in-first-out) allocated after every completion of the specified loop time. Clip, the source of the archive is extracted from one of the previous two types and is stored for the duration of its Days-to-Live.
<b>Recording Archive</b>	An archive whose state is running/recording. A running regular archive gathers additional data and increases in size. A running loop archive gathers more data and reuses its allocated space. Regular archives that have not reached their duration and loops that are still recording are running. Running archives have a Days-to-Live value of $\infty$ which does not update until they have stopped.
<b>Repository</b>	A central place where data is stored and maintained. A repository can be a place where multiple databases or files are located for distribution over a network, or a repository can be a location that is directly accessible to the user without having to travel across a network.
<b>S</b>	
<b>Stopped Archive</b>	An archive whose state is stopped. A shelved archive does not gather additional data or increase in size. Regular archives, clips, recordings, and loops that have reached their duration are considered shelved. Shelved archives are stored for the duration of their Days-to-Live.
<b>Stored Archive</b>	An archive whose state is stopped. A shelved archive does not gather additional data or increase in size. Regular archives, clips, recordings, and loops that have reached their duration are considered shelved. Shelved archives are stored for the duration of their Days-to-Live.
<b>Stream</b>	Any data transmission that occurs in a continuous flow.
<b>T</b>	
<b>Tagged Event</b>	When an incident or event occurs, it is captured by a device or application and is tagged. An event is a collection of information about an incident, including name, associated video sources, and a timestamp. If the event setup includes triggered clips, an event will have trigger tracking or video data associated directly with it. Users will need to use the event log to refer to times within a referenced archive, typically a master loop. By using the API to seek to a specific timestamp, events can be used to look up occurrences in an archive that were not necessarily associated with the original event.
<b>Time stamp</b>	An international and universal time system. Representation of time used by computers and many programming languages are most often accurate down to the millisecond. UTC values are used to track archive date/time values and records when events are triggered.

<b>Trap</b>	Used to report alerts or other asynchronous events pertaining to a managed subsystem.
<b>Trigger</b>	The action or event that triggers an alarm for which an event profile is logged. Events can be caused by an encoder with serial contact closures, a motion detected above defined thresholds, or another application using the soft-trigger command API.
<b>U</b>	
<b>UI</b>	User Interface
<b>Update Proxy</b>	Changes the registered information for a proxy source so that the proxy process will serve multiple videos as required. Once a proxy has been updated, all requests for that proxy will be served via the new feed. All clients requesting the feeds will be switched. Proxies are not trans-coded meaning some attributes may not be changed once registered.
<b>V</b>	
<b>Video Feed</b>	The transmission of a video signal from point to point. View: A layout, dwell time, and media sources. VM: Cisco Video Surveillance Virtual Matrix Client VMR: Video Mixing Renderer
<b>W</b>	
<b>Window</b>	All or a portion of the camera view. The display can contain multiple windows either by stacking (only the top one is entirely visible) or tiling (all are visible) or a combination of both.
<b>WMV</b>	Windows Media Video

## References

- Physical Security Products:  
[http://www.cisco.com/en/US/products/ps6918/Products\\_Sub\\_Category\\_Home.html](http://www.cisco.com/en/US/products/ps6918/Products_Sub_Category_Home.html)
- Design Guides:
  - Cisco Validated Designs  
<http://www.cisco.com/go/cvd>
  - Cisco Design Zone  
<http://www.cisco.com/go/designzone>
  - Designing a Campus Network for High Availability  
[http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA\\_campus\\_DG/hacampusdg.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html)
  - HA Campus Recovery Analysis  
[http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA\\_recovery\\_DG/campusRecovery.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_recovery_DG/campusRecovery.html)
- At-a Glance
  - *Cisco Enterprise Campus and Branch Network Architecture for IP Video Surveillance - At-a-Glance*
  - *Cisco IP Video Surveillance Solution Offering - At-a-Glance Document*
- Primers
  - *Cisco IP Video Surveillance Solution Components - A technical Primer*
- White Papers

- *QoS and Admission Control in Cisco IP Video Surveillance - whitepaper*
- *Network Optimization for implementing Cisco IP Video Surveillance solution - whitepaper*
- *Secure Delivery of IP Video Surveillance - whitepaper*
- *Network Management in IP Video Surveillance networks whitepaper*

