Physical Security Interoperability Alliance

IP Video Use Case 002 (PSI-UC-IPV002)

Specification Version 1.0
Revision 0.2

Revision History	Description	Date	By
Version 1.0 Rev 0.1	Initial Draft	August 25,2008	Frank Yeh
Version 1.0 Rev 0.2	Added Protocols Section	November 15, 2008	Frank Yeh

1. Description

IP Video Use Case 001 (PSI-UC-IPV001) applies to any device that provides streaming digital video over an IP network. The use case describes all events necessary to connect to such devices over the network, request streaming content from these devices, and view the requested content.

IP Video Use Case 002 expands on PSI_UC-IPV001 by describing how various protocols are used to automate the addition of new devices to an environment, the management and administration of a large population of devices, and the distribution of streaming content to multiple clients.

This combination of functions is typically delivered as a Video Management Solution (VMS), so this use case will describe how a typical VMS uses protocols to support the registration and configuration of devices as well as the streaming of content to multiple clients.

2. Validation

The IP Video Use Case is validated when a user can successfully add devices to a network, configure the devices, and view video from the devices using a VMS.

3. Assumptions

The following pre-conditions are assumed to exist prior to the sequence of events within this use case.

3.1. Video Management System, Clients and IP Video Devices are installed on the IP Network

3.2. Users and Administrators have proper credentials to access applications and devices

4. Protocols, Statuses and Standards Bodies

The protocols relevant to this use case are identical to those referenced in IP Video Use Case 1. Please refer to Use Case 1 for the list of relevant protocols.

5. Entity Enumeration

The following entities participate in this use case:

5.1. Administrator

A person who is responsible for the deployment, operation, and administration of the video systems and IP video devices.

5.2. User

A person who uses video applications.

5.3. Video Managemet Solution

Video Management Solutions typically include servers that provide a user interface, a data store of devices and their configurations, a device interface. In addition, remote clients are often provided to view video from client workstations (as opposed to on the video management server itself).

5.4. IP Video Device

An IP video device, typically a camera or encoder, captures video images and may use a variety of codecs to encode and or compress a video stream prior to distributing it on the network.

6. Functional Dependencies

This section describes all of the major functions that must be executed in order for the use case to operate. These functions are described in reverse chronological order as this allows the relative dependencies of each function to be illustrated.

6.1. Streaming Video

Encoded video content streamed from the IP Video Device to the client must be requested and controlled (EG Select, Play, Stop functions)

6.2. VMS Requests Streaming Video

VMS Requesting Streaming video from Device on behalf of client must know device addresses and capabilities.

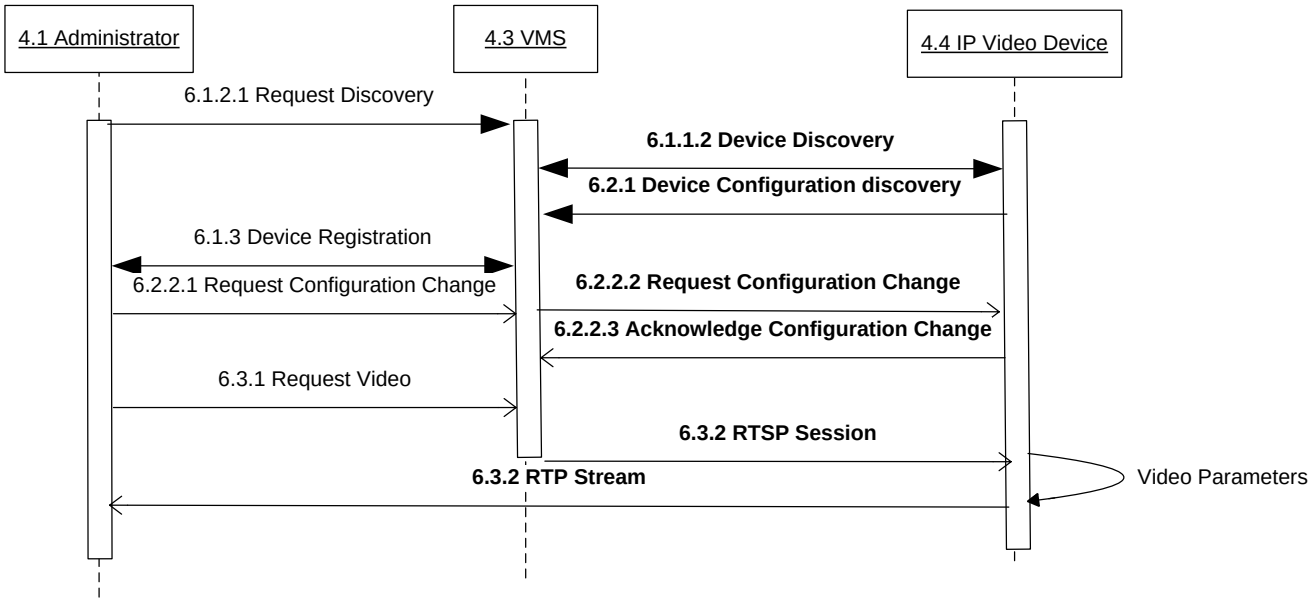
6.3. Device Configuration

Administrator updating configuration of video device using VMS must know which devices exist.

6.4. Discovery and Address Resolution

VMS discovers Device and IP Address

7. Sequence of Events



7.1. Address Resolution/Device Registration

Registration of device IP Addresses to support application access.

Proof Point is to test IP connectivity with the device. VMS application should provide test of connectivity.

7.1.1. Manual IP Address Entry

Device IP Addresses can be entered manually into VMS applications. The Administrator enters a device IP Address into the VMS application. The VMS can use PING or a proprietary protocol to check connectivity with the device. Once the device has been contacted, the Administrator can save it in the VMS database. While it is typical for a VMS to retrieve the device's current configuration at this time, this retrieval will be described in the Device Configuration section below

7.1.2. Automated Device Discovery

7.1.2.1. **Administrator Discovery Request**

The Administrator requests a device discovery via the VMS application.

7.1.2.2. **Automated Device Discovery**

The VMS can use several public or proprietary protocols to discover devices. In some cases devices can advertise themselves on the network once deployed, initiating a self-registration process with the VMS server.

In either case, the entities involved employ a service-oriented architecture in which servers and devices listen on certain IP port numbers for requests to initiate the discovery process and/or send requests to initiate the process. Within this process, some capabilities and configuration of a device are typically included.

7.1.3. Device Registration

Discovered devices are usually presented to the Administrator who can then modify their configuration and save them in the VMS database. Self-registered devices are often registered automatically.

Universal Plug and Play (UPnP) http://www.upnp.org/resources/documents.asp	UPnP provides for several automated device deployment functions. Among these is the discovery of devices by a server and self-registration by devices.

ZeroConf http://www.zeroconf.org	Zeroconf (AKA Apple Bonjour) provides for several automated device deployment functions. Among these is the use of DNS-Based Service Discovery to support device self-registration and device discovery.

IP Media Device API http://www.psia.org	The IP Media Device API is a pre-standard protocol that has been approved by the PSIA's IP Video Working Group. It provides for several automated device deployment functions including automated device discovery.

7.2. *Device Configuration*

Allow Administrators to configure IP devices using VMS applications.

Proof Point is when an Administrator can update configuration of Video Devices via a VMS with the configuration of devices reflected in the VMS databse.

7.2.1. VMS Discovery of Current Device Configuration

As part of the device discovery process, the VMS discovers the configuration of the device. In some cases, the VMS already knows the capabilities of the device. Most VMS solutions today support a limited variety of devices from certain manufacturers. These known devices have their capabilities loaded into the VMS database so that when discovered, only their make and model needs to be communicated. This style of communication is typically performed using vendor-specific protocols defined by the device manufacturer. In other cases, open protocols can be used to allow a device to specify its capabilities during the discovery process. The open protocols used during this process and during the device configuration process are already listed in the device discovery section. In any case, the VMS uses the protocols to discover the devices' current configurations and reflect these in its database.

7.2.2. VMS Device Configuration

7.2.2.1. Administrator Submits Changes to VMS

Once a device's current configuration is known, the VMS presents it to the Administrator via its administrative interface. The Administrator can then request changes to the configuration of a device and submit the configuration change to the VMS.

7.2.2.2. VMS Submits Change Request to Device

The VMS initiates a change request to the device with the requested new configuration.

7.2.2.3. Device Acknowledges Change Request

The Device responds to the change request to let the VMS know it has completed. In some cases, such as a change in the device's IP Address, the device will go offline while the change is completed. Once the device comes back online, the automated discovery process allows the VMS to confirm completion.

7.3. *User Views Video/Audio Stream*

Client requests a Video/Audio Stream from VMS client application. In some cases, the VMS will provide a native 'fat' client that runs on the client workstations and communicates with the VMS server and/or IP Video Devices. In other cases, the VMS provides a web-based object that runs in a web browser for this purpose.

Proof Point is when user requests a video stream and application acknowledges same.

7.3.1. User initiates video request at Client

The user uses the VMS Client interface to login to the VMS Server, select a video feed the available devices, and request video. The VMS server issues an RTSP

Request to the device on behalf of the client. Using RTSP. The VMS negotiates an IP Address and port on which the client will receive an RTP stream from the device. The client uses this information to establish an RTP connection with the device. In an alternate scenario where the VMS is recording video from the device, the VMS server maintains an active content stream from the device and can simply proxy this stream on to the client if video from the device is requested. In either case, the client receives sufficient information from the VMS server to establish an RTP connection and does not have to distinguish where the stream actually comes from.

Real-time Streaming Negotiation Protocol (RTSP) http://tools.ietf.org/html/rfc2326	Within the context of establishing the RTSP connection, the Client negotiates certain parameters (EG port number) with the IP Device. Typically, these parameters will be used to determine how the content will be transported back to the client.

6.3.2 Video is Streamed to Client by Device (or VMS)

The Video Device establishes an RTP stream back to the client

Real-Time Transport Protocol (RTP) http://tools.ietf.org/html/rfc3550	Using RTP, the content is transported back to the client using parameters negotiated in the previous step (using the RTSP protocol)

7.4. Content Streaming and Multicast

No Description of streaming video in a complex environment would be complete without covering how video is streamed to multiple clients from a single source, or multicast.

In this case, the nature of IP Multicast allows multiple clients to view streaming content from a device using of a single multicast IP address. Each client will simply establish an RTP connection using this address and the network will route the traffic accordingly.