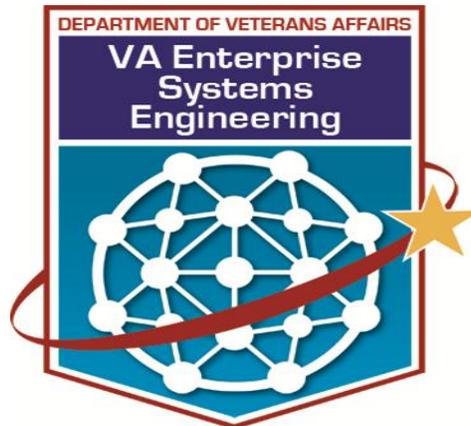




# DEPARTMENT OF VETERANS AFFAIRS (VA)

---



OFFICE OF INFORMATION AND TECHNOLOGY (OIT)  
VA SERVICE DELIVERY ENGINEERING (SDE)  
ENTERPRISE SYSTEMS ENGINEERING (ESE)

---

## **VA Enterprise Standard: VIDEO CODEC/RECORDING**

Version 1.0  
June 22, 2012

## Revision History

Date	Reason for Changes	Version	Author
June 22, 2012	Initial draft	1.0	

# Table of Contents

1

<b>1. Introduction .....</b>	<b>4</b>
1.1. Scope .....	4
1.2. Objective .....	5
<b>2. Core Standards.....</b>	<b>6</b>
2.1. H.323 .....	6
2.2. SIP .....	7
<b>3. Video Codec/Recording Device Standards .....</b>	<b>9</b>
3.1. CODECs .....	10
3.2. Recording Devices .....	13

## 1. Introduction

In order to ensure the successful integration of new Video Conferencing (VC) technology into the infrastructure, organizations implementing Video Conferencing endpoints should understand the established specifications in use within the VC infrastructure.

Video Conferencing is an extension of traditional telephony technologies (i.e., dial up telephone service) with the added feature of being able to see the person or persons with whom one is talking. Classically, the telecommunications network used for video conferencing connectivity has been (and still is today) a traditional circuit switched telephony network such as EVTN provides videoconferencing services to the entire VA. The EVTN is the network for VA video conferencing connectivity. This network is based in TDM technologies and typically provides IP-based connectivity for access to the network. Addressability is handled as with any other telephone instrument, the address is the phone number associated with the line from the circuit switch to the instrument.

VTC systems/CODECs can be interconnected via an IP based network. The protocol that was developed for VTC transmission across an IP based network is H.323. This is in reality a suite of protocols that provides the complete range of VTC capabilities. The session content or media is carried across the network using Real Time Protocol (RTP) or Secure RTP (SRTP).

### 1.1. Scope

The Video Codec/Recording Standards were created through the cooperative efforts of members of the industry and government. The standard is mandatory for the VA enterprise and optional for all other government agencies. Before using this document, VA users should check with EVTN for information technology standards, interoperability to see if a more recent version has been approved.

The purpose of this standard is to provide a standards-based reference document for users as an aid in the acquisition of VA video conferencing equipment.

A standard is a set of rules or requirements that are determined by a consensus opinion of subject matter experts and prescribe criteria for a product, process, test or procedure. The general benefits of a standard are quality, interchangeability of parts or systems, and consistency. VA Information Technology (IT) standards are based on business needs provided through or supported by IT Services. The VA IT Services are designed to support business processes and are constructed from software, hardware and infrastructure components. Establishing and enforcing standards for the selection and configuration of these supporting components improves the maintainability, reliability and availability of VA IT services within projected economic constraints in alignment with business needs.

This standard document lists the acceptable and recommended specifications for VA infrastructure video products. Sections include standard specifications for subject components, decisions supporting the standard specifications, guidelines or recommendations for

implementing the standard specifications, and supplemental factors to consider for when evaluating subject components. Other supplementary documents will provide guidance on procuring components that meet the standard specifications, guidance on integrating them with existing components, and explanation of how the subject components fit into the VA video conferencing Architecture.

This standard provides the VA with interoperability and performance requirements and options. The technical parameters of this standard may be exceeded to satisfy certain specific requirements, provided that the minimum mandatory requirements are met and that interoperability is maintained.

This document is based on the international recommendations from the International Telecommunications Union - Telecommunication Standardization Sector (ITU-T) for video teleconferencing. Specifically the H.320, H.323 and T.120 series of recommendations. It also includes the multipoint features and functionality of H.231.

Wherever possible, this document implements the International Telecommunications Union (ITU) standards as ratified. There are a few exceptions to meet specific VA requirements, such as security that is not currently included or not clear in the ITU standards.

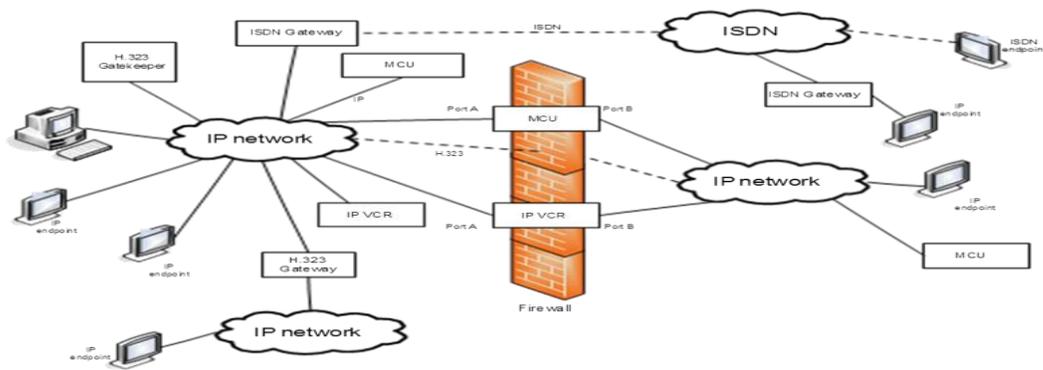


Figure 1: Overview of video conferencing

## 1.2. Objective

(1) **Standardization.** It is necessary for all participants to use standard video equipment when dialing into a videoconference. EVTN policy recommends facilities only acquire videoconferencing equipment that conforms to the ITU standards.

(2) **Interoperability.** Interoperability within the VA depends on the adoption of international interoperability standards. All major videoconferencing vendors are implementing these standards in today's videoconferencing equipment and software applications.

(3) **Network.** VA policy recommends that no video equipment be acquired without first cons•  
Enable successful passing throughout the enterprise

## 2. Core Standards

### 2.1. H.323

H The H.323 standard is an umbrella specification that includes the standards H.225.0, H.245, the H.235-series, the H.450-series documents, and the H.460-series and also allows the use of T.120 for data collaboration and file transfer. H.323 provides a cornerstone foundation for audio, video, and data communications over packet-based networks for EVTN. It specifies the components, protocols, and procedures needed. While it may operate over a variety of transports, H.323 is almost exclusively used only on IP networks.

Figure 2 below, shows the user equipment interfaces, video codec, audio codec, telematic equipment, H.225.0 layer, system control functions and the interface to the packet-based network. All H.323 terminals shall have a system control unit, H.225.0 layer, Network Interface and an audio codec unit. The video codec unit and user data applications are optional.

- The video codec (H.261, etc.) encodes the video from the video source (i.e., camera) for transmission and decodes the received video code which is output to a video display
- The audio codec (G.711, etc.) encodes the audio signal from the microphone for transmission and decodes the received audio code which is output to the loudspeaker
- The data channel supports telematic applications such as electronic whiteboards, still image transfer, file exchange, database access, audio graphics conferencing, etc
- The standardized data application for real-time audio graphics conferencing is Rec. ITU-T T.120
- Other applications and protocols may also be used via H.245 negotiation
- The System Control Unit (H.245, H.225.0) provides signaling for proper operation of the H.323 terminal and provides for call control, capability exchange, signaling of commands and indications, and messages to open and fully describe the content of logical channels
- H.225.0 Layer (H.225.0) Defines functions of Registration, Admission, and Status (RAS) and formats the transmitted video, audio, data and control streams into messages for

output to the network interface and retrieves the received video, audio, data and control streams from messages which are input from the network interface

- H225.0 performs logical framing; sequence numbering, error detection and error correction as appropriate to each media type

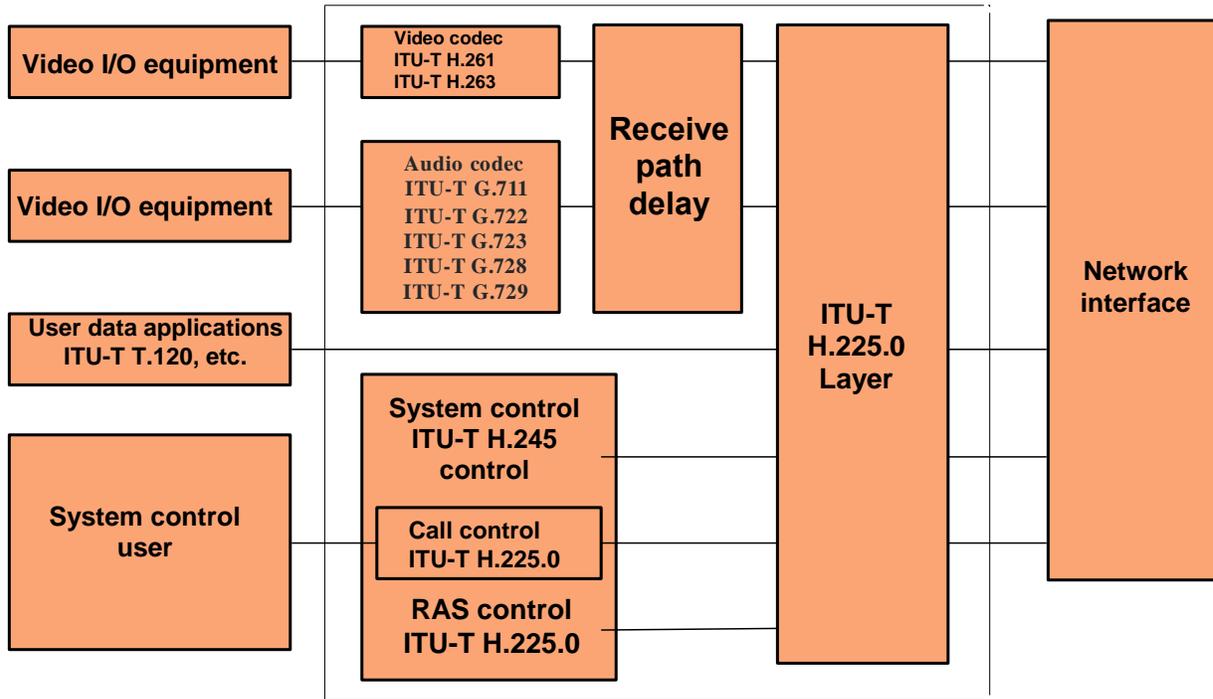


Figure 2: H.323 Diagram

## 2.2. SIP

SIP is a signaling protocol for Internet. By means of SIP mechanisms, end systems and proxy servers can provide services such as call forwarding, called and calling number delivery, terminal capability negotiation, caller and called authentication, blind and supervised call transfer invitations to multicast conferences and personal mobility in addition to the ability to reach a called party under a single, location-independent address even when the user changes terminals, terminal-type negotiation and selection.

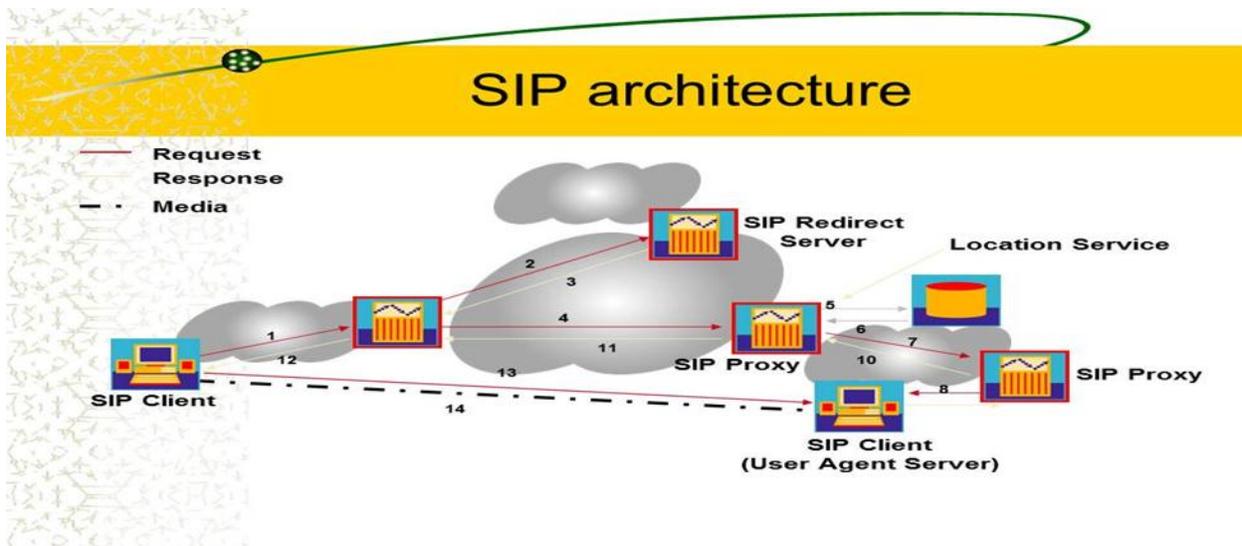


Figure 3: SIP Protocol Architecture

### SIP Components

The SIP protocol defines several entities. Each entity has a specific function and participates in SIP communication as a client (initiates requests), as a server (responds to requests), or as both. One physical device can have the functionality of more than one logical SIP entity.

### User Agent

A User Agent (UA) is an application that interfaces between the user and the SIP network.

### UAC

A UAC is an application that initiates SIP requests to a UAS. A UAC can be a program or a device that interacts with a user.

### UAS

The User Agent Server (UAS) is server applications that accepts the request from a UAC and generates accept, reject, or redirect responses on behalf of the user.

### Proxy Server

SIP Proxy servers are elements that route SIP requests to UAS and SIP responses to UAC. A SIP Proxy server acts as both a UAC and UAS. SIP defines three types of proxy servers: Call Stateful Proxy, Stateful Proxy, and Stateless Proxy.

#### Call Stateful Proxy

Call Stateful Proxy Servers need to be informed of all SIP transactions and therefore are always in the path taken by SIP messages traveling between users. These proxy servers store state information from the moment the session is established until the

moment it ends.

#### Stateful Proxy

A Stateful Proxy Server stores state-related information to a given transaction until the transaction concludes

#### Stateless Proxy

A Stateless Proxy Server forgets all information once a request or response has been processed. A stateless proxy forwards every request it receives downstream and every response it receives upstream.

### **Registrar**

A SIP Registrar contains the location of all UA's within a domain. A registrar acts as the front end to the location service for a domain, reading and writing mappings based on the contents on REGISTER requests

### **Redirect Server**

A redirect server accepts a SIP request, maps the address and returns a list of possible locations to the client that initiated the request.

### **SIP interoperates with:**

- Secure Device Provisioning (SDP) to describe the payload of message content and characteristics
- Systems Applications and Products (SAP) for advertising multimedia session via multicast
- Resource Reservation Protocol (RSVP) to reserve network resources for providing Quality of Service (QoS)
- RTP for real-time transmission
- Real Time Streaming Protocol (RTSP) for controlling delivery of streaming media.
- Remote Authentication Dial-In User Service (RADIUS) for authentication
- Lightweight Directory Access Protocol (LDAP) for location discovery

### **3. Video Codec/Recording Device Standards**

The H.323 standard specifies four kinds of components which provide the communication services: terminals, gateways, gatekeepers and multipoint control units. This document describes the standards for terminals, specifically Codecs and Recording devices.

The following sections will define what Standards each system will need to support to be introduced into the VA network. Any equipment or system being procured must not require additional infrastructure to support its functionality outside of what is already deployed in the EVTN.

The following sections will define what Standards each system will need to support to be introduced into the VA network. Any equipment or system being procured must not require additional infrastructure to support its functionality outside of what is already deployed in the EVTN.

### 3.1. CODECS

Codecs (also referred to as Terminals in H.323) are the conference rooms on the Local Area Network (LAN) that provide real-time, two-way video and audio communications. These specifications were determined through market and independent research. A Codec is an endpoint in the LAN that participates in real-time, two-way communications with another H.323 terminal, gateway, or MCU. A Codec must support audio communication and can also support audio with video, audio with data, or a combination of all three.

An H.323 terminal can be a Personal Computer (PC) or a stand-alone device with the capability to interwork with other multimedia terminals such as: H.324 terminals on wireless networks, H.310 and H.321 terminals in B-ISDN, H.320 terminals on ISDN and H.322 terminals on guaranteed QoS LANs

ID	Primary attribute	Secondary attribute	Specification
1	Protocol	Video	ITU-T H.323 H.323 Annex H.225 H.235 H.245 H.264 Q.931 RAS T.120 IETF SIP
		Audio	ITU-T G.711 G.729 Polycom Siren 14 Advanced Audio Coding –Low Delay (AAC-LD) Advanced Audio Coding- Low Complexity (AAC-LC)
		Network	Simple Network Management Protocol (SNMP) v2 SNMP v3 HyperText Transfer Protocol (HTTP) Hypertext Transfer Protocol Secure (HTTPS) Secure Socket Shell (SSH) Secure Copy (SCP) Cisco Telepresence Management Suite(TMS)
		Quality of Service (QoS)	DiffServ and TOS/IP

		Management	SNMP v2 SNMP v3 HTTP HTTPS SSH SCP Cisco TMS
2	Support	Technical support	Required: phone support 24/7
3	Security	FIPS 140-2 certification	Required

## Explanation of Standard

### Video:

The following H.323 annexes will be required for the Codecs:

#### H.225

H.225 communication is between H.323 entities on the same packet-based network, using the same transport protocol. This packet-based network may be a single segment or ring, or it logically could be an enterprise data network comprising multiple packet-based networks bridged or routed to create one interconnected network. It should be emphasized that operation of H.323 terminals over the entire Internet, or even several connected packet-based networks may result in poor performance.

#### H.235

H.235 is part of H.323v4 and is the emerging standard for authenticating signaling and encrypting media for H.323 endpoints. H.235 messages expand upon H.323 signaling by defining crypto-tokens, which are data structures containing cryptographic information. H.323 signaling messages may contain one or more crypto-tokens.

#### H.245

H.245 specifies syntax and semantics of terminal information messages as well as procedures to use them for in-band negotiation at the start of or during communication. The messages cover receiving and transmitting capabilities as well as mode preference from the receiving end, logical channel signaling, and control and indication. Acknowledged signaling procedures are specified to ensure reliable audiovisual and data communication.

#### H.264:

Standard for video compression, and is currently one of the most commonly used formats for the recording, compression and is currently the EVTN Standard

H.264 v7 is the latest approved version for use in the VA(Later versions will need to be disabled to apply to the VA standard).

#### H.263 and H.261

Standard that can be used in the VA as backup/secondary protocol. H.263 (v2 or higher) can be used as the primary standard for Content only.

#### Q.931

Call setup and termination

#### RAS

Manages registration, admission, status which allows the gatekeeper to manage the endpoint, allow the endpoint to request admission for a call, and allow the gatekeeper to provide address resolution functionality for the endpoint

#### RTP and RTCP

Protocols used to sequence the audio and video packets. The RTP header contains a time stamp and sequence number, allowing the receiving device to buffer as much as necessary to remove jitter and latency by synchronizing the packets to play back a continuous stream of sound. RTCP controls RTP and gathers reliability information and periodically passes this information onto session participants.

#### SIP

VA currently uses SIP in their desktop video clients and many codecs support and use SIP. SIP is also used in certain other applications. SIP is a text-based protocol for initiating interactive communication sessions between users, including voice, video, and chat in an IP network.

#### Audio:

##### G.711

Pulse Code Modulation (PCM) of voice frequency is a required standard in H.323

##### G.729

Description of an algorithm for the coding of speech signals at 8 kbit/s using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP) and is the preferred EVTN standard for voice to voice call

#### Polycom Siren 14

Due to a significant amount of Polycom systems in the EVTN and the continued used of these codecs this transform-based codec must be supported.

#### AAC-LD

Format designed to combine the advantages of perceptual audio coding with the low delay necessary for two-way communication currently used in EVTN desktop client software.

#### ACC-LC

Used in EVTN legacy equipment

#### Network:

Currently the VA is using IPv4 for network devices but the EVTN expects a change to IPv6 in the future so in planning for this change, all new equipment must support both protocols along with the necessary protocols to work in the environment (DNS, DHCP, and NTP).

#### Quality of Service:

QoS is required to ensure that more important traffic can be configured to receive priority on the network or deliver a level of service necessary to complete and maintain a call. As QoS is implemented throughout the network these protocols will be necessary to properly mark video traffic.

#### Management:

Cisco TMS is the scheduling and management system for EVTN endpoints and systems. In order to support all systems, any new equipment must be able to interface with TMS in order to schedule calls and make necessary changes to the system. TMS uses SNMP (v2 and v3) and HTTP(s).

SSH is needed to interface with the system for various command line configuration changes.

SCP is needed to interface with the system for upgrades and certain file changes on the system.

#### Security:

Due to the sensitive nature of an individual's health information, security of information is necessary. FIPS 140-2 is a standard that describes US Federal Government requirements that Information Technology (IT) products should meet for Sensitive, but Unclassified (SBU) use. The standard was published by the National Institute of Standards and Technology (NIST) and defines the security requirements that must be satisfied by a cryptographic module used in a security system protecting unclassified information within IT systems.

### **3.2. Recording Devices**

Recording and Playback, also known as *video on demand*, is an add-on to streaming solutions. This means the proceedings of a videoconference or other programming can be captured and

stored on a hard disk. This would require a high capacity disk, since video files can be quite large, reaching several hundred megabytes, depending on the length of the program, the compression ratio, scan refresh rate, and window size, among other factors. Software allows non-conference users to access and play stored videoconferences, using the media streaming application; these users need only a browser or media client such as Real Player, or Windows Media Player.

A recording device enables VA to share knowledge and enhance communication by recording their video conferences and multimedia presentations for live and on-demand access. It enables creation and management of multimedia content from any H.323 or Session Initiation Protocol (SIP) video endpoint. Live or recorded content can be distributed to any PC.

ID	Primary attribute	Secondary attribute	Specification
1	Protocol	Video	ITU-T H.323 H.323 Annex H.225 H.235 H.245 H.264 Q.931 RAS T.120 IETF SIP
		Audio	ITU-T G.711 G.729 Polycom Siren 14 Advanced Audio Coding –Low Delay (AAC-LD) Advanced Audio Coding- Low Complexity (AAC-LC)
		Network	Simple Network Management Protocol (SNMP) v2 SNMP v3 HyperText Transfer Protocol (HTTP) Hypertext Transfer Protocol Secure (HTTPS) Secure Socket Shell (SSH) Secure Copy (SCP) Cisco Telepresence Management Suite(TMS)
		Quality of Service (QoS)	DiffServ and TOS/IP
		Management	SNMP v2 SNMP v3 HTTP HTTPS SSH SCP Cisco TMS
2	Support	Technical support	Required: phone support 24/7
3	Security	FIPS 140-2 certification	Required

## Explanation of Standard

### Video:

The following H.323 annexes will be required for Recording Devices:

#### H.225

H.225 communication is between H.323 entities on the same packet-based network, using the same transport protocol. This packet-based network may be a single segment or ring, or it logically could be an enterprise data network comprising multiple packet-based networks bridged or routed to create one interconnected network. It should be emphasized that operation of H.323 terminals over the entire Internet, or even several connected packet-based networks may result in poor performance.

#### H.235

H.235 is part of H.323v4 and is the emerging standard for authenticating signaling and encrypting media for H.323 endpoints. H.235 messages expand upon H.323 signaling by defining crypto-tokens, which are data structures containing cryptographic information. H.323 signaling messages may contain one or more crypto-tokens.

#### H.245

H.245 specifies syntax and semantics of terminal information messages as well as procedures to use them for in-band negotiation at the start of or during communication. The messages cover receiving and transmitting capabilities as well as mode preference from the receiving end, logical channel signaling, and control and indication. Acknowledged signaling procedures are specified to ensure reliable audiovisual and data communication.

#### H.264:

Standard for video compression, and is currently one of the most commonly used formats for the recording, compression and is currently the EVTN Standard H.264 v7 is the latest approved version for use in the VA(Later versions will need to be disabled to apply to the VA standard).

#### H.263 and H.261

Standard that can be used in the VA as backup/secondary protocol. H.263 (v2 or higher) can be used as the primary standard for Content only.

#### Q.931

## Call setup and termination

### RAS

Manages registration, admission, status which allows the gatekeeper to manage the endpoint, allow the endpoint to request admission for a call, and allow the gatekeeper to provide address resolution functionality for the endpoint

### RTP and RTCP

Protocols used to sequence the audio and video packets. The RTP header contains a time stamp and sequence number, allowing the receiving device to buffer as much as necessary to remove jitter and latency by synchronizing the packets to play back a continuous stream of sound. RTCP controls RTP and gathers reliability information and periodically passes this information onto session participants.

### SIP

VA currently uses SIP in their desktop video clients and many codecs support and use SIP. SIP is also used in certain other applications. SIP is a text-based protocol for initiating interactive communication sessions between users, including voice, video, and chat in an IP network.

#### Audio:

##### G.711

Pulse Code Modulation (PCM) of voice frequency is a required standard in H.323

##### G.729

Description of an algorithm for the coding of speech signals at 8 kbit/s using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP) and is the preferred EVTN standard for voice to voice call

##### Polycom Siren 14

Due to a significant amount of Polycom systems in the EVTN and the continued used of these codecs this transform-based codec must be supported.

##### AAC-LD

Format designed to combine the advantages of perceptual audio coding with the low delay necessary for two-way communication currently used in EVTN desktop client software.

##### ACC-LC

Used in EVTN legacy equipment

#### Network:

Currently the VA is using IPv4 for network devices but the EVTN expects a change to IPv6 in the future so in planning for this change, all new equipment must support both protocols along with the necessary protocols to work in the environment (DNS, DHCP, and NTP).

#### Quality of Service:

QoS is required to ensure that more important traffic can be configured to receive priority on the network or deliver a level of service necessary to complete and maintain a call. As QoS is implemented throughout the network these protocols will be necessary to properly mark video traffic.

#### Management:

Cisco TMS is the scheduling and management system for EVTN endpoints and systems. In order to support all systems, any new equipment must be able to interface with TMS in order to schedule calls and make necessary changes to the system. TMS uses SNMP (v2 and v3) and HTTP(s).

SSH is needed to interface with the system for various command line configuration changes.

SCP is needed to interface with the system for upgrades and certain file changes on the system.

#### Security:

Due to the sensitive nature of an individual's health information, security of information is necessary. FIPS 140-2 is a standard that describes US Federal Government requirements that Information Technology (IT) products should meet for Sensitive, but Unclassified (SBU) use. The standard was published by the National Institute of Standards and Technology (NIST) and defines the security requirements that must be satisfied by a cryptographic module used in a security system protecting unclassified information within IT systems.

## 4. Glossary

**CLI:** Command-Line Interface. CODEC—CODER—Decoder. Transforms analog signals into a digital bit stream, and digital signals back into analog signals. In VoIP applications, it specifies the voice coder rate of speech for a dial peer.

**Gateway:** A gateway allows SIP terminals to communicate with terminals configured to other protocols, by converting protocols. A gateway is the point at which a circuit-switched call is encoded and repackaged into IP packets.

**Invite:** A method that initiates a session. It indicates that a user is invited to participate, provides a session description, indicates the type of media, and provides insight regarding the capabilities of the called and calling parties.

**Payload type:** A field within the fixed header portion of the RTP packet that defines the content, format, and encoding scheme of the RTP payload. When a SIP call is set up, the payload type values that are used in this field are listed in the m= line of the session description. These values can be either statically assigned to encoding names, or dynamically assigned within the session description. If a payload type is dynamically assigned, the session description will also include an rtpmap attribute that maps the payload type number to an encoding name. The encoding name identifies the format of the RTP packets (for example, a codec or telephone event).

**RTP:** Real-Time Transport Protocol.

**SDP:** Session Description Protocol.

**SIP:** Session Initiation Protocol. An application-layer protocol originally developed by the Multiparty Multimedia Session Control (MMUSIC) working group of the Internet Engineering Task Force (IETF). Their goal was to equip platforms to signal the setup of voice and multimedia calls over IP networks. SIP features are compliant with IETF RFC 2543, published in March 1999.

**VoIP:** Voice over IP. The ability to carry normal telephone-style voice over an IP-based network.

## 5 References

Quality of Service (QoS) for voice over IP- Cisco documentation.

The effect of dynamic voice codec selection for active calls on voice quality— Thesis by Jered Daniel Ast.

Packet Scan User's Guide — GL Communication Inc.

VoIP —Lecture notes by David Wang.

Measurement Challenges for VoIP infrastructures—Prasad Calyam, Internet2 VoIP Workshop.

VoIP as a collaborative tool on client PC— Intel White paper.

Polycom Administrator's Guide for the VSX Series Version 8.5.3-February 2007

Polycom Getting Started Guide for the VSX Series Version 8.5.3-February 2007

Polycom Release Notes - V Series and VSX Systems, Version 8.7-July 2007

Polycom V2IU 6400-S Converged Network Appliance Users Guide V7.2.2—May 2007

Polycom Firewall Traversal and Security Whitepaper, Frost and Sullivan

Polycom RSS 2000 Product Data

TANDBERG 1500 MXP User Manual, Software version F4, 2005

TANDBERG 3000 MXP and 6000 MXP Reference User Guide For System Integrators, MAY 2007

TANDBERG – API (Dataport User Guide), Software version E4/B9

TANDBERG and H.323 Whitepaper; D50305, Rev 4.0.

TANDBERG Endpoints and IP Whitepaper; D12434, Rev 3.3

TANDBERG Management Suite and Security Whitepaper; D13325, rev. 03

TANDBERG on Streaming - an Application Note; D12408, rev. 05

TANDBERG Expressway and Firewalls; D14001.rev 01