Videoconferencing sub-standards

The sub-standards most likely to be met with in practice are detailed below:

1. Video Coding Standards

H.261 Video CODEC

For audio visual services; this defines the way in which the picture information is compressed and coded to enable transmission over low bandwidth networks. It is the baseline coding which is mandatory for most videoconferencing systems to ensure interoperability at a basic level.

H.261 Annex D Graphics

The coding format for transmission of still images over H.320 conferencing at a screen resolution up to a maximum of 704 x 576 pixels, i.e. 4 x CIF. (See also 3.6.4.1 below)

H.262 (MPEG2)

Video coding used in broadband, i.e. H.310 ATM, conferencing systems.

H.263 Video CODEC

For audio visual services, a variation of the H.261 CODEC but specifically designed for low bit rate transmission, i.e. H.324 (GSTN) and H.323 (IP) networks at 64128kbit/s.

H.263+ Video CODEC

H.263+ is an enhanced version of H.263 coding giving improved coding efficiency at the expense of increased CODEC complexity.

H.263++ Video CODEC

H.263++ is an even more efficient CODEC, particularly for pictures containing movement.

H.264 Video CODEC

H.264 is also known as MPEG4 Advanced Video Coding (AVC). The latest video CODEC developed jointly between the ITUT and ISO/IEC. It uses more sophisticated compression techniques than H.263 coding and is designed to require less bandwidth for an equivalent quality signal using other compression algorithms.

2 Audio Coding Standards

G.711

To ensure interoperability between systems G.711 is the baseline audio coding algorithm. It is mandatory in most videoconferencing systems. This coding produces an upper frequency limit of 3.4kHz/s (i.e. telephone quality) and occupies up to 64kbit/s of data.

G.722.1

An improved coding for audio signals giving higher quality signals with an upper frequency limit of 7kHz/s but only occupying 4856/ 64kbit/s of data.

G.723.1

Coding for ultra low bandwidth applications and occupying only 5.3/6.3kbit/s.

G.728

Low bit rate coding producing 3.4kHz upper frequency limit but occupying only 16kbit/s of bandwidth.

G.729

Coding for very low bandwidth applications and occupying 8kbit/s.

3 Structure for Communication (i.e. data stream formats)

H.221

Defines the frame structure for 641920kbit/s audio visual channels, i.e. videoconferencing up to 1920kbit/s (in H.320 systems).

H.224

A protocol for real time simplex control, i.e. one-way communication.

H.225.0

Call signalling and packet multiplex protocols for packet based (i.e. H.323) conference systems.

H.230

Frame control and indicating signals for conferencing equipment.

H.231

Multipoint control signals for conferencing channels up to 1920kbit/s (i.e. for communication between three or more sites conferencing up to 1920kbit/s).

H.233]

H.234] Encryption option for H.3xx conferences.

H.235]

H.241

Extended video procedures for H.3xx series terminals.

H.242

System for establishing communication between terminals in H.320 conference systems up to 1920kbit/s.

H.243

Protocol for communication between three or more conferencing units up to 1920kbit/s, i.e. multipoint conferencing.

H.245

Control protocol used in H.310 and H.323 conferencing systems.

H.281

Far end camera control, i.e. control of the remote site's camera from the local site.

H.282/H283

Remote control of devices other than a camera.

H.323 Annex Q

Far end camera control within H.323 systems. This has now been superseded and is included within the latest (07/2003) H.323 recommendations.

H.331

Broadcasting type audio visual multipoint systems and terminal equipment.

4 Still Image Transfer Formats

4.1 H.261 Annex D and T.81

H.320 systems can offer the option for transferring still images at a resolution greater than the basic H.261 video resolution. It is H.261 Annex D coding. This provides a resolution up to a maximum of 4xCIF i.e. 704 x 576 pixels. While these still images are being transmitted then the normal motion videoconference images are suppressed. Alternatively some products offer Joint Photographic Expert Group (JPEG) still image coding (see 3.8.1 below) which is defined by ITUT standard T.81.

5 ITUT

Sub-standards Applied to an H.323 CODEC

Figure 3 shows the components of a typical H.323 videoconferencing CODEC. A simplified diagram, it is intended to illustrate how the various standards apply within a videoconferencing system. The flow lines are bidirectional. The vision transmit path starts at the local camera (video input), the output video signal then being coded and compressed by the video CODer (part of the video CODEC) before being multiplexed with the audio and other data streams. It then feeds to the network (IP in this case).

The inverse path takes an IP data signal arriving (via the network) from the remote site; it is demultiplexed into separate video, audio, data and control signals and then directed to the relevant DECoder e.g. to the video DECoder (part of the video CODEC). The decoded video give an image from the remote site. The own on the diagram.

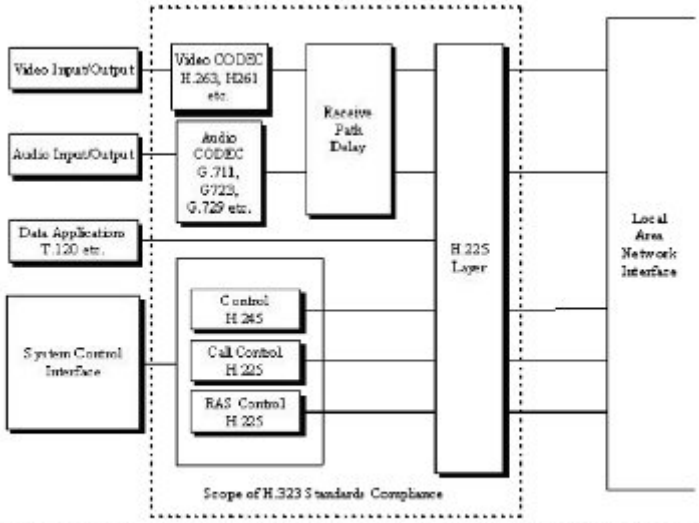

Figure 3: Block Diagram of an H.323 CODEC (*In this diagram, 'RAS control' refers to Registration, Admission and Status control)

[1]

5.1 H.235 Security and Encryption for H.323 Conferences

This ITU standard defines the security and encryption for H.323 and other H series connections that utilise the H.245 control protocol. H.323 networks by their nature do not guarantee either Quality of Service (QoS) or security of the data. The two main concerns are authentication and privacy. Authentication enables an endpoint to verify that a caller is who they say they are. The privacy of data can also a worry during conferences as without precautions an H.323 network is relatively easy to interrogate.

The standard has been developed over several years and has three versions: 1, 2 and 3. Each iteration supersedes its predecessor. In common with other ITU standards there are mandatory, recommended and optional requirements. Within the standard are Annexes defining interoperability at specific levels of security:

Annex D defines the baseline measures that are utilised in managed environments with

symmetric keys/passwords assigned among the entities (terminal gatekeeper, gatekeeper gatekeeper, gateway gatekeeper). This method uses a simple but secure password profile protection. It may also incorporate voice encryption for secure speech transmission.

Annex E is an optional suggested signature security profile deploying digital signatures, certificates and a public key infrastructure. As administration of passwords is not required between entities it enables much more efficient connection to a final endpoint via gatekeepers, gateways and MCUs on the network. It may incorporate annex D voice encryption and/or random number data encryption for messages.

To achieve maximum interoperability the ITU recommends that CODECs should have the ability to negotiate and to be selective concerning the cryptographic techniques utilised, and the manner in which they are used.

Links
[1] http://community.ja.net/system/files/vcstandards03.jpg