

# H.323

## Videoconferencing Components

The standard that is used for the majority of IP (Internet Protocol) Videoconferencing is H.323, a recommendation by the Telecommunication Standardisation Sector of the International Telecommunications Union (ITU-T). This is the standard that defines multimedia communications for packet-based networks like the Internet and JANET and groups together many other standards, protocols and recommendations. These include the call set-up and completion protocols, and the audio and video encoding and decoding algorithms that H.323 endpoints must support, as well as some that are optional.

### H.323 terminals

An H.323 videoconferencing terminal provides real-time, bi-directional multimedia communications. A terminal consists of a processor that implements the audio and video encoding and decoding compression algorithms; the necessary audio and video inputs and outputs; a user interface; and an operating system that may be dedicated or third-party. All of these elements are highly integrated and are often known collectively as a CODEC (COder/DECoder).

### Gatekeepers, zones and E.164 addressing

A gatekeeper is an H.323 component that allows the H.323 terminals on a network to interoperate. It provides management functions to terminals that are accessed by the terminal registering with a particular gatekeeper. All such registered terminals are in its 'zone'. Gatekeepers are usually deployed on the network to reflect organisational or geographical network topology.

Gatekeepers co-operate with each other to provide terminals with the following services:

- E.164 address translation and resolution – E.164 is an ITU Recommendation for an International Dialling Plan. Use of this plan simplifies H.323 dialling, and allows interoperability between H.323 and other networks. National Research Networks around the world have agreed on a standard for H.323 addressing that conforms to E.164, and this is described at:  
<http://www.wvn.ac.uk/support/h323address.htm>
- Admission and access control - the gatekeeper can be configured to control terminal registration according to various criteria such as IP address and user authentication.
- Bandwidth management – administrators can implement rules for conserving bandwidth to protect other users or to maintain call quality.
- Call set-up – registered terminals initiate and receive call set-up messages via their gatekeeper (although the actual videoconferencing data is not routed through the gatekeeper).
- Call management and tracking – the gatekeeper tracks current calls, and can log them. This information can be useful for monitoring and accounting.
- Routing functions – calls can be routed or re-routed according to rules configured by the administrator.

Gatekeepers are normally implemented as software, running on a router or PC, or as a standalone network device.

## Multipoint Control Units (MCUs)

An MCU is an essential element for calls involving more than two terminals. It acts as a hub to which all of the terminals involved connect, and distributes audio and video between the terminals. Sometimes MCUs are combined with a terminal, gatekeeper or, most commonly, a gateway (see below).

## Gateways

A gateway is usually only required when one or more H.323 terminals are in a conference with a non-H.323 terminal. The most common application is a gateway to an Integrated Services Digital Network (ISDN). The gateway has an interface to both networks and translates the call signals in both directions, enabling seamless communication.

H.323 is very closely related to the ITU-T H.320 Recommendation for circuit-based networks like ISDN. The same audio and video encoding and decoding algorithms are used within both standards. For this reason many terminals can be used on either network, and gateways can move data between the two networks without re-encoding the audio and video data. Also H.323 and H.320 use the T.120 standard for data sharing.

An H.323 proxy is a specialised type of gateway that sits between two IP networks, with an interface to both. All H.323 signals and media packets pass through the proxy as they flow from one terminal to the other. Using a proxy provides security for both sides, as IP addresses are hidden: each side sees only the IP address of the proxy. H.323 proxies are available as router or PC software and will often reside on the same equipment as a gatekeeper.

## Security for H.323 videoconferencing

As with any equipment that is connected to the Internet, the deployment of H.323 equipment has many security implications. The main issues to be considered are:

- Device security – this includes protection from vandalism or theft, or the user gaining access to system settings and changing them. Device security can be ensured by establishing protocols for access to the room and system.
- Network security – includes hacking, virus attack, 'denial of service' attacks. Network security can be ensured by careful network engineering and the use of firewalls, access lists, the deployment of an H.323 proxy, or a combination of these.

## Further information

An Introduction to H.323 Videoconferencing:

<http://www.video.ja.net/323intro.pdf>

JANET IP Videoconferencing Service - IP (JVCS-IP):

<http://www.jvcs.video.ja.net/docs/jvcsip.shtml>

Introduction to Firewalls:

<http://www.ja.net/services/publications/factsheets/009-firewalls.pdf>

Video Technology Advisory Service (VTAS):

<http://www.video.ja.net/>

Packetizer™ Home Page:

<http://www.packetizer.com/>