IP Videoconferencing

The JANET Videoconferencing Service (JVCS) [1] provides videoconferencing services to the Janet community within the UK. It consists of centralised equipment, a Service Desk and Booking Service [2] to facilitate videoconferences using both ISDN and IP technologies. The service supports point-to-point (one-to-one) and multipoint videoconferences and provides a bridges to allow conferencing between IP and ISDN systems. This document is intended to outline how IP videoconferencing can be used, gives recommendations for organisations wishing to use the service and provides an overview of the service. Some familiarity with videoconferencing and IP networking is assumed.

Overview

The JVCS IP infrastructure complies with the International Telecommunications Union Standardisation Sector (ITU-T) H.323 umbrella of protocols for IP videoconferencing. The service consists of three elements:

- Multipoint Control Unit (MCU) and IP-ISDN gateway capacity;
- gatekeepers, that provide call admission control (allowing IP videoconferencing to be managed on user organisation networks) and call routing (allowing users to simply dial other users across the network in a similar way to making phone calls);
- Global Dialling Scheme (GDS), that works in conjunction with the local, national and international gatekeepers to route calls appropriately.

Security of IP videoconferences can be improved through the use of proxy gatekeepers or H.323 aware firewalls. It should be noted that, as part of the IP videoconferencing service endpoints are automatically dialled from the MCU. An IP dial-in facility is also available to those organisations whose network security may not allow the MCU to dial them.

MCU, gateway, and gatekeeper equipment has been deployed at different co-locations on the Janet backbone for resilience.

Service Policies

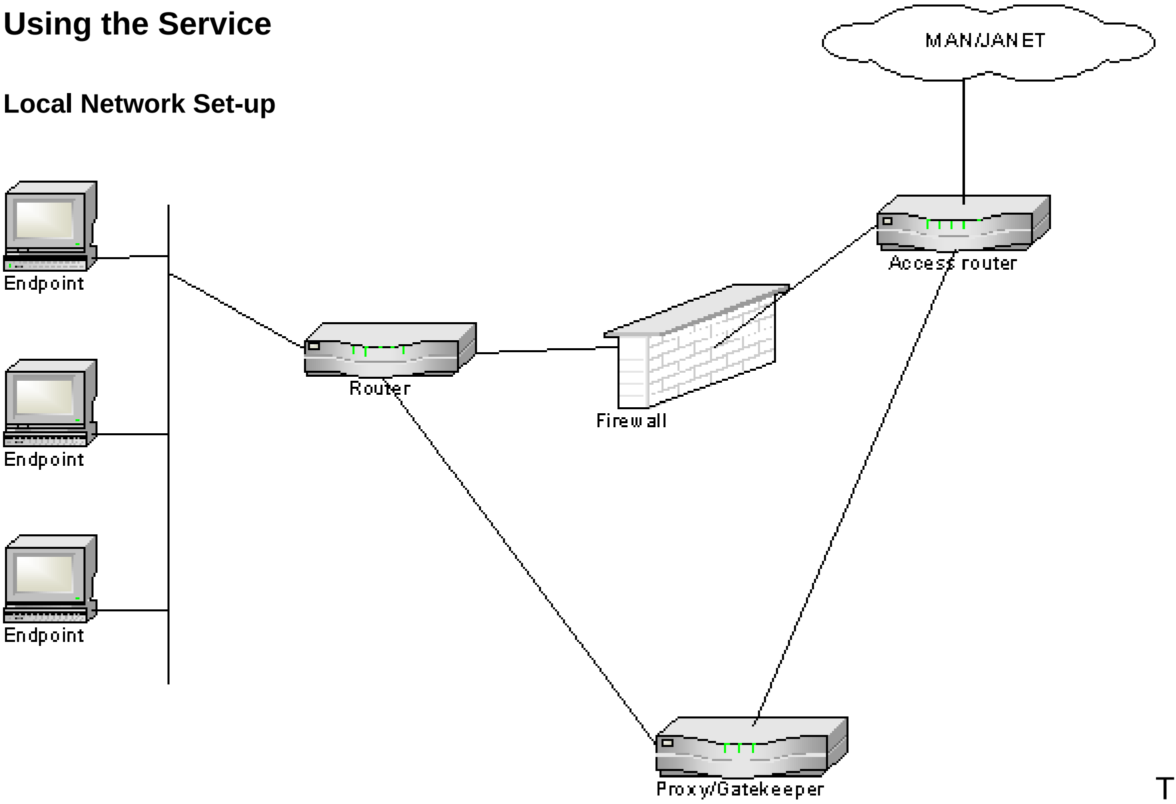
JANET(UK) organisations with a primary connection are able to register to use JVCS-IP. This involves registration of their videoconferencing endpoints (studios, desktop systems and all other endpoints) with the Booking Service [2]. Once registered, each organisation is required to successfully complete a quality assurance test. The test is carried out with the assistance of JVCS, and involves measuring the objective audio/video quality and network connectivity of an organisation’s videoconferencing endpoint. These tests are repeated at six month intervals after initial registration.

Once an organisation is registered and using the Booking Service [2], they will be able to manage videoconferencing resources within their organisation and ensure no conflicts occur between room bookings.

Endpoints not registered with the Booking Service [2] may take part in videoconferences with registered organisations by being brought into the conference as a ‘guest endpoint ’ by that organisation. Guest venues undertake a connectivity test rather than a quality assurance test, to ensure that the endpoint is able to connect to the videoconference.

Using the Service

Local Network Set-up



To register for, and use JVCS-IP, organisations need to ensure they have an internet connection with enough bandwidth capable of supporting the IP videoconferencing. JVCS supports call speeds of 128 kbit/s to a maximum of 2 Mbit/s. During an IP videoconference bandwidth can peak at double the call speed being used, for example during a 768 kbit/s videoconference the actual bandwidth required can reach approximately 1.5 Mbit/s. Organisations should also factor in regular network traffic when considering videoconferencing call speeds.

Depending on network quality, higher bandwidth videoconferences can provide higher quality audio and video.

It is recommended that careful consideration be given to the physical network path between CODECs (endpoints) and site access routers, and the amount of traffic traversing the link. Links should ideally be 10/100 Mbit/s full duplex, thus avoiding potential local network load issues.

Typical local network set-up for IP videoconferencing

Room/Venue Set-up

Room/Venue set-up and layout should be considered carefully. Factors to consider include:

- wall coverings
- curtains
- table layout
- microphone positioning
- camera positioning

A Planning Rooms factsheet provides more basic information on room setup or there is an in-depth report on Videoconferencing Rooms available from the Video Technology Advisory Service (VTAS) [3].

Local Gatekeepers

The gatekeeper is a call set-up and management device that allows organisations to control the level of IP videoconferencing traffic on their networks. Within the H.323 standard is the concept of ‘zones’. A gatekeeper manages a zone that has a number of venues registered within it by using admission control, address translation, address resolution and bandwidth control. A single physical gatekeeper can, in some implementations, support multiple logical zones.

The distribution of gatekeepers/zones allows for devolved management, increased security, and a scaleable service. It should also reflect the management and organisational structures of the service and the topology of the network over which the service will operate. The logical distribution of gatekeepers and their associated zones is on an organisational basis. Thus, in the majority of cases, each organisation should have a single gatekeeper that will communicate with other organisations’ gatekeepers via the national or international gatekeeper, to set-up and manage calls. For more information on why gatekeepers are used see the Global Dialling Scheme (GDS) [4].

It is possible, however, that some organisations may not want to run their own gatekeeper. In this case gatekeeper facilities are provided from the centrally located and managed JANET gatekeeper. Another case may be a research group, for example, spread over multiple organisations who may prefer to be part of the same zone for addressing reasons. In this case gatekeeper facilities should be provided from a local or remote organisation, or alternatively from the centrally located and managed Janet gatekeeper.

Organisations that have IP videoconferencing systems and wish to use the Janet service have the option of deploying their own organisational gatekeeper or using a Janet central gatekeeper. The Janet central gatekeeper is provided to allow sites to participate in IP videoconferencing if they have not yet deployed their own gatekeeper.

Each organisation's gatekeeper must be registered with a Janet national gatekeeper in order to be able to send and receive calls using the GDS [4] and to take part in multipoint conferences. Upon registering for the service, a zone prefix will be allocated for that zone and information on how to configure the organisation’s gatekeeper to access the service will be provided. In order to use the service, all venues within an organisation must use the registered gatekeeper.

CODECs

CODEC (endpoint) choice is an extremely important area to consider. Ideally, CODECs should be capable of supporting videoconferences at 2Mbit/s although JVCS-IP is able to support speeds of between 128 kbit/s and 4Mbit/s.

Organisations wishing to use IP must ensure that all CODECs are compliant with the ITU-T H.323 series of recommendations. More information on Videoconferencing Standards is available from the Video Technology Advisory Service (VTAS) [3].

Also, VTAS [3] offers a number of unbiased Product Evaluation Reports which include a number of CODEC evaluations.

CODECs can take a wide range of hardware and software formats. Some of the most popular CODECs are:

- rack based CODECs with ancillary camera(s), monitors and microphone equipment;
- room based CODECs with ancillary camera(s), monitors and microphone equipment;
- desktop hardware CODECs with built-in camera and microphone equipment and ancillary monitor - these are usually standalone devices;
- desktop hardware CODECs with ‘bubble camera’ and ancillary microphone - these are usually PCI based CODEC cards utilising standard PCs;
- desktop software based CODECs with a webcam and a combined microphone and headset.

Security

There are a number of security issues related to IP videoconferencing, particularly concerning H.323 in relation to firewalls and conference interception.

The H.323 protocol suite includes a range of individual protocols. For all of these to function correctly an H.323 CODEC requires a number of reachable Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports. The port numbers used for some of these protocols, including the Real Time Protocol (RTP) audio and video streams, are negotiated at connection time, making it impossible to know in advance which port numbers an H.323 session will use.

Unless a firewall is H.323 aware (where the ports used can be determined in real time by monitoring the call control and set-up channel) organisations need to open all ports above 1023 to enable the H.323 data to flow properly. H.323 aware firewalls are suitable for deployment but that still may not remove the need to open firewall ports further up the networking hierarchy e.g. a school whose network sits under a Local Authority's (LA) network may need to have ports opened on the LA's firewall.

An alternative method for allowing H.323 traffic into a site is to deploy an H.323 proxy. The proxy resides on the organisation’s border network, and communicates with the H.323

CODECs within the organisation. H.323 sessions into or out of the network operate via the proxy. Inbound H.323 connections are received by the proxy, which then initiates the final leg of the connection to the internal CODEC. If a firewall is used, the proxy can be chosen to be the only source trusted for inbound H.323 sessions, as all such sessions will effectively be routed through it, see Diagram 1.

Monitoring

To ensure that faultfinding and fault diagnosis can be undertaken, the JVCS Management Centre will monitor elements of JVCS-IP. On registering, organisations will be requested to give permission to the Management Centre to monitor their videoconferencing equipment. Any network faults should be reported using local fault reporting mechanisms. Sites that do not wish to have their videoconferencing equipment monitored should be aware that the Management Centre will be unable to provide fault finding and diagnostic services, and non-centralised issues will have to be resolved at a local level.

Centralised Equipment

Multipoint Control Units (MCUs)

Centralised MCUs are capable of providing Standard Definition (SD) and High Definition (HD) IP based videoconferences. Janet currently operates 2 Polycom MGC-100TM MCUs and 3 Codian MSE 8000 chassis with SD and HD MCU blades. The equipment is used for both point-to-point and multipoint videoconferences to facilitate IP to IP, IP to ISDN and ISDN to ISDN conferences.

Gatewaying and Rate Matching

Many videoconferences taking place within the Janet community use different networking protocols and call speeds. To ensure that the majority of videoconferences are supported, IP to ISDN gateways and rate matching capabilities are built-in to the core centralised videoconferencing equipment.

Gateways

The introduction of IP videoconferencing has been a catalyst for growth in service usage within the Janet community. ISDN videoconferencing is still being used but its growth has not kept up with that of IP.

Rate Matching (Transcoding)

The ability to support videoconferences with CODECs operating at different call speeds is a key factor to the success of the JANET Videoconferencing Service-JVCS . Over the last two years the capabilities of IP based H.323 CODECs have increased significantly and the maximum bandwidth capabilities have risen from 768kbit/s to 6Mbit/s. This growth has resulted in organisations deploying CODECs capable of operating at a variety of different call speeds. The maximum speed of IP is currently 4Mbit/s, the maximum currently supported by the Codian equipment.

Another reason for offering rate matching as part of the overall service concerns network connectivity. While some organisations may have CODECs capable of operating at 6Mbit/s, their network connections may not allow it. Organisations with lower bandwidth connections to Janet may therefore stipulate that their videoconferences be limited to suit their network connections.

Registering to Use JVCS

To register for JVCS please go to the Booking Service [2]

Sites already registered to use JVCS have the option to add another CODEC to their existing videoconferencing information.

Follow the CODEC Operations link after logging in. Enter the details of the CODEC you are adding and your chosen gatekeeper option.

New institutions that are not registered to use JVCS must create an account by selecting add new institution.

Newly registered organisations are required to create a login account and provide general information on CODECs and gatekeeper options. The online prompts are designed to guide you through this process.

If at any time during the registration process you have any questions or need further assistance, please contact the support centre:

Tel: 0131 650 4933

E-mail: vidconf@jvideo.ja.net [5]

Source URL: https://community-stg.jisc.ac.uk/library/videoconferencing-booking-service/ip-videoconferencing

Links
[1] http://www.ja.net/jvcs
[2] http://www.jvcs.ja.net/cgi-bin/vcng/welcome.cgi
[3] http://www.ja.net/vtas
[4] http://www.wvn.ac.uk/support/h323address.htm
[5] mailto:vidconf@jvcs.ja.net