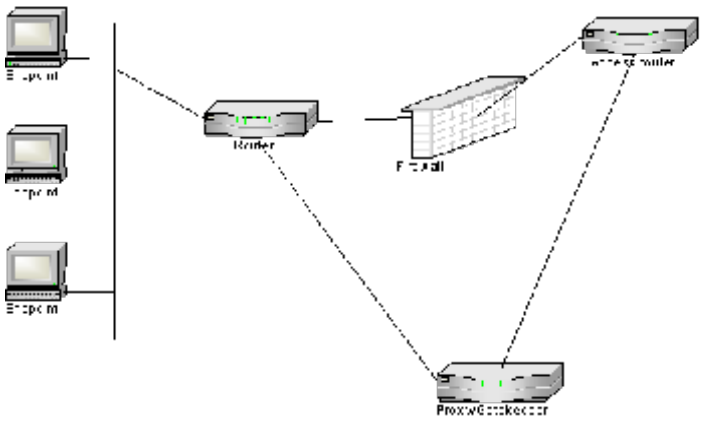
Using the Service

Local Network Set-up

To register for, and use Janet Videoconferencing, organisations need to ensure they have an internet connection with enough bandwidth capable of supporting the IP videoconferencing. Janet Videoconferencing 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 [illegible] avoiding potential local network load issues.



[1]

Figure 1: *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 [2] factsheet provides more basic information on room setup or there is an in-depth report on Videoconferencing Rooms [3] available from the Video Technology Advisory Service (VTAS) [4].

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) [5].

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 [5] 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 Janet Videoconferencing 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) [4].

Also, VTAS [4] offers a number of unbiased Product Evaluation Reports [6] 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 heirarchy 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**.

Global Dialling Scheme (GDS)

In order to ensure standardised H.323 videoconferences can take place both within the UK and world wide, an H.323 GDS [5] has been developed. SURFnet in the Netherlands, HEAnet in Ireland and ViDeNet in the US have also implemented this scheme. The GDS [5] has been developed because a standardised H.323 addressing scheme is yet to be created. The GDS [5] uses standards based E.164 addressing.

The GDS [5] is based on numeric addressing which allows the greatest flexibility in interfacing with other communication devices e.g. ISDN based videoconferencing systems and conventional or mobile phones. The GDS [5] comprises four components:

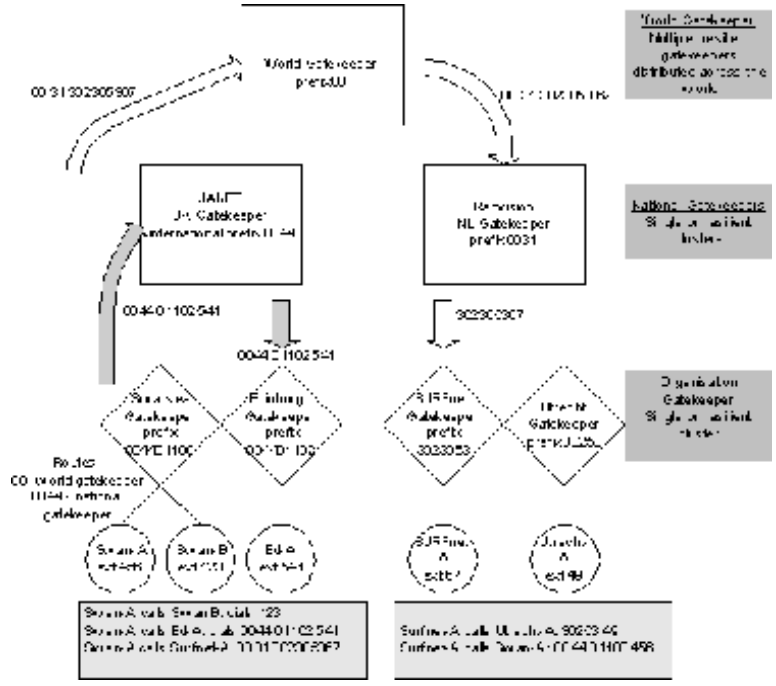
- an international dialling prefix, which is specified as 00;
- the ITU-T country telephone code, that is between one and three digits, in the case of the UK 44;
- a zone prefix, which is five digits starting with a zero e.g. 01100 that is the zone prefix for an organisation;
- a three to five digit extension number.

Here is an example number that might be used to dial a system in a university:

00	44	01100	12345
International prefix	UK dialling code	Zone prefix	Extension number

Zone prefixes are assigned by JANET(UK) in the UK and by other National Education and Research Networks in other countries. Once an organisation has installed a gatekeeper it can apply to the Janet Videoconferencing [7] to register it. After successfully completing the registration a zone prefix will be assigned. The organisation can then assign its own three to five digit extension number. The only restriction to the allocation of extension numbers is that they cannot start with a zero.

The diagram below shows how a UK call would take place between Swansea University and Edinburgh University (grey arrows), and how an international call would take place between Swansea University and SURFnet in the Netherlands.



[8]

Figure 2: *The gatekeeper hierarchy on which the dialling scheme operates*

Monitoring

To ensure that faultfinding and fault diagnosis can be undertaken, the Janet Videoconferencing Management Centre will monitor elements of Janet Videoconferencing. 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.

Links
[1] http://community.ja.net/system/files/images/ipvideo01.gif
[2] http://www.ja.net/documents/publications/factsheets/037-planning-rooms.pdf
[3] http://www.ja.net/documents/services/video/vcrooms.pdf
[4] http://www.ja.net/vtas
[5] http://www.wvn.ac.uk/support/h323address.htm
[6] http://www.ja.net/services/video/vtas/productevaluations/index.html
[7] http://www.ja.net/jvcs
[8] http://community.ja.net/system/files/images/ipvideo02.gif