H.323 site deployment

The acquisition, set up and deployment of an H.323 videoconferencing studio is outside of the scope of this guide; such information is available from the VTAS web site. However, there are security considerations to be made in the deployment. In the simplest case, the site will be deploying a single, fixed-location studio-based H.323 system, to be used by university or college members who wish to participate in videoconferences with people at other Janet connected sites.

Topology considerations

The main site considerations include:

- **Connectivity of the H.323 terminal.** It is highly desirable that the terminal has good connectivity to the campus or site edge router. This implies either a direct cable or fibre to the router, or an efficient, Ethernet-switched path. There should be no Ethernet hub devices in the path. In addition to ensuring good network performance, this also reduces the chance that any management traffic (from systems support staff workstations to the H.323 terminal) or any live videoconference session data can be ‘snooped’ in transit.

- **Dedicated connectivity.** If a site topology for the H.323 device is such that it is directly connected to the edge router, with a dedicated port on that router, it may (although not necessarily) make it easier for the site to apply a favourable Quality of Service (QoS) policy to that device, or to mark the traffic on that port for favourable treatment by an upstream Premium IP-configured router [JANETQOS]. A Janet QoS position statement was published in December 2002 [JANETQOS-PP]. The dedicated connectivity thus offers the potential for better QoS, while also being more secure (there is less opportunity for data interception or snooping).
- Firewall location and use. It is desirable, but not essential, that the H.323 terminal is protected from unwanted external Internet access by use of an appropriate firewall. It is becoming common for UK Higher Education (HE) sites to deploy firewalls many with ‘default deny’ inbound connection policies. If the H.323 terminal is on a dedicated connection to the campus edge router, and has no other internal site connectivity, a firewall may not be necessary if the device itself can be tested and known to be secure. Firewall usage is discussed in more detail later in this guide.

Potential topologies for a basic H.323 studio terminal deployment are illustrated in Figure 1.

Image not found or type unknown

Figure 1: Options for H.323 terminal connection topology

The terminal could be:

- **Directly connected via fibre or copper Ethernet to the site edge router.** In this case there is no firewall protection, although Access Control Lists (ACLs) on the router may be applied. The source IP address of the H.323 terminal on the dedicated interface can be reasonably trusted for QoS assurances. Snooping of data on campus is most difficult in scenario (a). Where a dedicated fibre path is not available, use of VLAN technology (if the local network hardware supports it) may provide a virtual path for the H.323 traffic.
- **Directly connected to an interface on the site firewall (in effect a mini De-Militarised Zone or DMZ).** In this case the H.323 terminal is better protected, but QoS guarantees may not be so readily available (depending on QoS support in the firewall itself).
- **Connected via the general campus network.** This may be the easiest solution for most sites, but it raises the risk of on-site snooping. Use of Ethernet switching can minimise this, but some Ethernet switch devices can be 'tricked' by frame flooding [CONVERY] into replicating data onto non-intended ports.

Note in many sites the firewall and edge router functions may be combined in a single device that combines the advantages and disadvantages of cases (a) and (b).

There is no 'correct' deployment; each has implications and associated costs. In the studio deployment case where JANET organisations wish to use the JVCS-IP, bookings will usually be made on the basis of use of a site's own H.323 gatekeeper with a JVCS-IP service MCU device.

It is preferable for a site to deploy its own gatekeeper, so that it can manage its own security policy; that gatekeeper can also be used for local site videoconferencing, or videoconferences run outside the JVCS-IP service. However, the site is also able to use the Janet gatekeeper if it wishes.

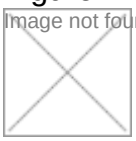
A site may have its own MCU, but the JVCS-IP service does not support cascaded MCU usage, so any MCU the site operates should only be used for the site's own videoconferencing activities.

A site may also wish to deploy an H.323 proxy. Such a proxy acts loosely in a similar way to a Web proxy. It can receive H.323 connections as if targeted at the real H.323 endpoint, and relay them to that endpoint; this is applicable to incoming or outgoing H.323 calls (thus two communicating systems might have two proxies in the path between them).

The proxy/gatekeeper function is often combined in a single unit.

There are two common topologies that may be considered for proxy/gatekeeper deployment, as shown in Figures 2 and 3.

Figure 2: DMZ topology for a site H.323 proxy/gatekeeper deployment



In Figure 2 the topology is such that the proxy/gatekeeper is hosted in a DMZ at the site border. This topology has the advantage that any compromise of the proxy server may be less

damaging as the internal network is not exposed (the attacker will need to breach the firewall to the interior network. However it has the disadvantage that all traffic will pass over the DMZ network twice (in and out); this may cause a degradation in service if the bandwidth utilisation is high.

In the ‘pass through’ topology in Figure 3 the proxy/gatekeeper can be configured to allow the proxy through if it comes in on a dedicated physical port. It has the advantage of not replicating traffic in the way the DMZ deployment does. This is generally secure as the service is locked down to one well-known port, but should a breach occur, the internal network is exposed. There have been no reports of breaches of proxy/gatekeeper devices on the WVN to date; thus the topology of Figure 3 would generally be recommended (but be reviewed based on operational experience).

The WVN configuration has the H.323 proxy as an alternative to the firewall. In fact, all WVN sites operate securely without requiring H.323-aware firewalls. WVN endpoints use the WVN gatekeeper and proxy and so the site access router (which could be a non H.323-aware firewall) only lets through the H.323 traffic from and to the WVN proxy, for the studios that are the other side of the proxy. This is the configuration shown in Figure 3 below. In both cases it is possible that the site edge or access router may be functionally combined into a single unit with the site firewall.

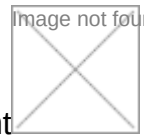


Figure 3: Pass-through topology for a site H.323 proxy/gatekeeper deployment

A proxy can act as a ‘concentrator’ for inbound H.323 connections, such that they are routed through a single device with access on well-known ports. Such a proxy is not absolutely necessary, but it does add a great deal to the security of the 'regular' studio.
