Video Conferencing Standards for the Scottish Public Sector

Version 1.0

June 2014

Document Control

Document Title	Video Conferencing Standard
Version	1.0
Owner	Technical Design Board
Author	Hazel Archer, hazel.archer@nhs.net
Creation date	3rd January 2014
Compliance	Recommended
Reviewers and Distribution	

Version Control

Date	Version	Author	Changes
3/1/14	0.1	Hazel Archer	Initial drafts combining content from NHS standards and Justice VC Standards
17/2/14	0.2	Hazel Archer	Review following discussion with JaNET
19/2/14	0.3	Hazel Archer	Review following discussion with NHS NSS
26/2/14	0.4	Hazel Archer	Review following comments from John Potts
19/6/14	1.0	Hazel Archer	Ratified by Technical and Design Board

Consultation Record

Date	Notes
17/2/14	Alan Sloan, JVCS
18/2/14	NHS National VC Team
26/2/14	NHS VC Technical Advisory Group
6/3/14	National Technical and Design Board

Contents

1 Summary

1.1 Standards:

- Video conferencing infrastructure should be capable of support H320, H323 and SIP calling. (It is accepted that the use of H320 (ISDN) will decline and that support may be via a bridging service rather than direct dial.)
- Interworking solution should be established to ensure that any protocol translation between H.323 and SIP is transparent to the end user.
- H323 devices should be registered with a gatekeeper arranged in a hierarchy with each gatekeeper only knowing its parent and child gatekeepers.
- H323 based endpoints should be addressed using a 9 digit E164 address based on the agreed dial plan.
- Video conferencing systems using SIP should be compatible with open standards for video encapsulation.
- Endpoints should be named organisation.town.site.room where organisation is defined by the agreed naming convention.
- Firewall traversal should be established to support both H323 and SIP video traffic.

1.2 Recommendations:

- Consideration should be given to establishing a dedicated subnet for video conferencing devices.
- QOS should be implemented on both LAN and WAN links to support video conferencing.
- SIP dialling should be via DNS / SRV record.

2 Introduction

In order to ensure that the benefits of investment in video conferencing technologies are fully realised, it is essential that developments are underpinned by appropriate technical standards to ensure that video calls can be successfully held within, between and outwith public sector partners.

This document deals with the underpinning technology required to support a standards based video conferencing estate. This provides the basis for developing a robust VC infrastructure that is vendor neutral and based on industry standards. By using this approach, previous investment in video technologies is protected, the requirements for new equipment are minimised and services can be shared across the public sector.

The document is based on standards already adopted by NHS Scotland and agreed for adoption by Criminal Justice Partners.

While the document deals with the technical standards needed to support the provision of video conferencing services such as managed bridging services and support services, the specification of these services are outwith it's scope. However it is recognised that a move to a standards based approach will greatly simply their introduction and management

Also excluded from scope is the integration of proprietary systems such as some unified communications systems, Skype and Facetime as these do not conform with the open standards outlined

3 Background

3.1 Development of Standards within NHS Scotland

In 2009, NHS Scotland established a project to enable IP based video conferencing. When planning the initial technology rollout, it became clear that agreement between Health Boards was required in a number of areas. These included:

- Naming conventions
- Dial plan
- Firewall traversal
- IP addressing

A standards based approach was agreed that allowed Boards to build on previous investment and these standards were formally adopted by NHS Scotland and published in September 2011.

In developing the standards, it was accepted that there was a need for local flexibility of infrastructure. This 'standards based approach' has allowed Health Boards to implement the standards on existing infrastructure hence maintaining existing service provision and keeping costs low.

3.2 Collaboration with JANET (Joint Academic Network)

JANET provides video conferencing services to higher and further education, research bodies and schools. As part of the wider global video network, JANET links to the Global Dialling Scheme (GDS). Rather than develop a dial plan restricted to NHS Scotland, it was agreed that the scheme developed should link with JANET and the global network beyond. This provides each video endpoint registered within NHS Scotland a unique numerical ID. Security and policy decisions permitting, this can provide the basis for developing video conferencing links across the public sector in Scotland as well and providing onward links across the world.

3.3 Criminal Justice Video Conferencing Project

The Criminal Justice VC Project was established with a view to optimising the use made of video and similar technologies in making the workings of the judicial system more effective and cost efficient. Since early 2013, technical support for the project has been provided by the Scottish Centre for Telehealth and Telecare as part of their wider agenda.

Draft standards (an updated version of the NHS Standards), were developed and formally agreed at the Justice IT Advisory Group in August 2013. Since then, work has progressed with the Justice Partners (Scottish Prison Service, Police Scotland, Scottish Courts Service, Crown Office and Procurator Fiscals Office, Tribunals Service and the Scottish Legal Aid Board) to progress their development and to identify appropriate technical solutions.

4 Communication Protocols

Standards based video conferencing systems generally support the following 3 protocols:

H.320: This is the standard associate with ISDN video calls and is supported if an additional ISDN option has been purchased.

H.323: H.323 is a protocol standard for multimedia communications. H.323 was designed to support real-time transfer of audio and video data over packet networks like IP. The standard involves several different protocols covering

specific aspects of Internet telephony. The International Telecommunication Union (ITU-T) maintains H.323 and these related standards.

SIP: SIP is an open signaling protocol for establishing any real-time communication session developed in the Internet Engineering Task Force (IETF) The communication session can involve a combination of voice, video, and instant messaging and take place on any device that people use for communicating: laptop computer, Smartphone, mobile phone, IM client, IP phone etc.

While a comparison of H.323 and SIP is outwith the scope of this paper it is relevant to note that both protocols are widely used and appropriate provision should be made to ensure calls between SIP and H.323 devices can be made seamlessly.

STANDARD: Video conferencing infrastructure should be capable of support H320, H323 and SIP calling. (It is accepted that the use of H320 (ISDN) will decline and that support may be via a bridging service rather than direct dial.)

Interworking solution should be established to ensure that any protocol translation between H.323 and SIP is transparent to the end user.

5 H.323

The H.323 standard specifies four kinds of components, which, when networked together, provide the point-to-point and point-to-multipoint multimedia-communication services:

- **Terminals:** An H.323 terminal can either be a stand-alone device such as a video conferencing endpoint or a personal computing device running the appropriate H.323 compliant software.
- **Gateways:** A gateway connects two dissimilar networks. For example a gateway can provide connectivity between an H.323 network running over IP and an ISDN network.
- **Gatekeepers:** A gatekeeper is the focal point for all calls within the H323 network. Gatekeepers provide important services such as: addressing, authorization and authentication of terminals and gateways; bandwidth management; accounting; billing; and charging. Gatekeepers may also provide call-routing services.
- **Multipoint Control Units:** MCUs (also known as a 'bridge') provide support for conferences of three or more H.323 terminals. All terminals participating in the conference establish a connection with the MCU. The MCU manages conference resources, negotiates between terminals for the purpose of determining the audio or video CODEC to use, and may handle the media stream.

5.1 Gatekeeper Hierarchy

Gatekeepers should be arranged in a hierarchy with each gatekeeper only knowing its parent and child gatekeepers as well as any directly registered endpoints. The master Scotland gatekeeper will be linked to the JANET network to provide onward routing.

STANDARD: H323 devices should be registered with a gatekeeper arranged in a hierarchy with each gatekeeper only knowing its parent and child gatekeepers.

5.2 E164 Dial Plan

End points should be programmed with a minimum of the last 9 digits of the E164 address. This will ensure that E164 numbers displayed will operate across all the Scottish public sector. The master gatekeeper will be programmed to add or remove the additional 6 digits that uniquely identifies Scotland (004405) to external calls.

The Dial Plan is detailed below.

	UKERNA Assigned			**Regional or National Gatekeepers** To be programmed into end points	
	International Prefix	Country Code	Zone Prefix	Gatekeeper Prefix	Extension
GDS Number for Scotland	00	44	05		
Shared National Services				600 - 609	yyyyyy
NHS Scotland	00	44	05	500 - 550	yyyyyy
3rd Sector Organisations	00	44	05	580 - 589	yyyyyy
Scottish Government	00	44	05	610 - 619	yyyyyy
Scottish Prison Service	00	44	05	620	yyyyyy
Police Scotland	00	44	05	621	yyyyyy
Scottish Courts	00	44	05	622	yyyyyy
Scottish Legal Aid Board	00	44	05	623	yyyyyy
Crown Office and Procurator Fiscals	00	44	05	624	yyyyyy
Scottish Fire and Rescue Service	00	44	05	625	yyyyyy
Local Authorities	00	44	05	6300 - 6349	yyyyy
Aberdeen City Council				6301	
Aberdeenshire Council				6302	
Angus Council				6303	
Argyll & Bute Council				6304	
Clackmannanshire Council				6305	
Dumfries & Galloway Council				6306	
Dundee City Council				6307	
East Ayrshire Council				6308	
East Dunbartonshire Council				6309	
East Lothian Council				6310	
East Renfrewshire Council				6311	
Edinburgh City Council				6312	
Comhairle nan Eilean Siar (Western Isles Council)				6313 6314	
Falkirk Council					
Fife Council				6315	
Glasgow City Council				6316	
Highland Council				6317	

Inverclyde Council Midlothian Council Moray Council North Ayrshire Council North Lanarkshire Council Orkney Islands Council Perth & Kinross Council Renfrewshire Council Scottish Borders Council Shetland Islands Council South Ayrshire Council South Lanarkshire Council Stirling Council West Dunbartonshire Council West Lothian Council				6318 6319 6320 6321 6322 6323 6324 6325 6326 6327 6328 6329 6330 6331 6332	
Executive NDPBs x34	Allocated as required by SWAN within the range 650-699				
Advisory NDPBs x 6	Allocated as required by SWAN within the range 650-699				
Tribunals x6	Allocated as required by SWAN within the range 650-699				
Public Corporations x5	Allocated as required by SWAN within the range 650-699				
Executive Agencies x8	Allocated as required by SWAN within the range 650-699				
Non- Ministerial Departments x5	Allocated as required by SWAN within the range 650-699				
Commissions and Ombudsmen x6	Allocated as required by SWAN within the range 650-699				
Other Significant National Bodies x19	Allocated as required by SWAN within the range 650-699				

STANDARD: H323 based endpoints should be addressed using a 9 digit E164 address based on the agreed dial plan.

6 SIP Dialling

SIP actually comprises two protocols -- SIP for initiating and terminating a session between endpoints, and the Session Description Protocol (SDP) for defining the type of session (e.g., voice or video) and session parameters such as codecs or encryption. Since SDP allows application developers to leverage any pre-existing encapsulation protocol, most SIP implementations use the same protocols as H.323 , whether they are voice codecs such as G.711, G.722 or G.729; video codecs, such as H.264; or other supported media encapsulation types.

However standardizing on SIP is not enough to ensure compatibility between devices. Video conferencing sessions make use of an extensive suite of protocols for encapsulation of voice and video, as well as supporting features such as encryption and management. For example, a Microsoft video conferencing client using SIP for signalling but a proprietary video codec for video encapsulation cannot connect to an endpoint using SIP for signalling but an open standard like H.264 for video encapsulation.

STANDARD: Video conferencing systems using SIP should be compatible with open standards for video encapsulation.

RECOMMENDATION: SIP dialling should be via DNS / SRV record.

7 Naming Convention

The name used to identify endpoints appears in various places such as the web interface, the management system, and in the display of the video endpoint unit. The system name is also used in directories. The systems name should be created so that the unit can be easily and uniquely identified.

The naming convention for videoconferencing endpoints is as follows.

Organisation.town.site.room

For example, a videoconferencing endpoint situated in the Conference Room at the Scottish Legal Aid Board HQ in Edinburgh would be displayed in the following format;

SLAB.Edinbugh.HQ.Conference_Room

To avoid names of excessive length, organisations may use recognised abbreviations in the town.site.room section.

STANDARD: Endpoints should be named organisation.town.site.room where organisation is defined by the agreed naming convention.

Organisation Name	Organisation	Town	Site	Room
NHS	NHSxxx	town	site	room
Eg. NHS Ayr & Arran	NHSAA	town	site	room
Scottish Government	SG	town	site	room
Eg Scottish Government Health Departments	SGHD	town	site	room
Scottish Legal Aid Board	SLAB	town	site	room
Scottish Prison Service	SPS	town	site	room
Other, to be agreed by the SWAN Authority	Other	town	site	room

8 IP Communications

8.1 Impact of SWAN

The Scottish Wide Area Network (SWAN) Programme is designed to deliver a single public services network available for the use of any, and potentially all, public service organisations within Scotland; with aggregated demand delivering both cost and performance advantages.

The process is being led by NHS National Services Scotland and a number of other authorities who have formed a 'Vanguard' of organisations who have agreed to enter into a Framework Agreement with the supplier immediately following the successful conclusion of the procurement.

Although detailed designs have not yet been finalised, the requirements for video conferencing (including Quality of Service) have been included in the tender specification.

Until such time as the SWAN network is in place across all organisations, there will be a requirement for video traffic to passed across either a shared interconnecting link or across the Internet.

NHS National Service Scotland have been designated the SWAN Authority. As such they will be manage the SWAN contract and will be responsible for IP address allocation for shared services. It is therefore recommended that address allocation and agreement of naming conventions should be administered by NHS National Service Scotland on behalf of the Scottish Public Sector.

8.2 IP Addressing

IP addressing for video conferencing is dependent on a number of factors, in particular the ability to establish a video conferencing VLAN to support Quality of Service (QOS).

Within the NHS, the use of a dedicated video subnet routed to a local VLAN has enabled the implementation of QOS on both LAN and WAN links. It is anticipated that the use of such subnets will continue to be supported on the SWAN network. (QOS for PC type devices is not currently supported on the NHS N3 network.)

RECOMMENDATION: Consideration should be given to establishing a dedicated subnet for video conferencing devices.

8.3 Firewall Traversal & NAT

A simple firewall uses rules based on virtual 'ports' and IP addresses to filter traffic. Most Internet applications and services have well known ports on which machines 'listen' for communications. Firewalls will generally be configured to block anything by default but then allow traffic to flow through certain ports, either to and from any IP address or to a subset of IP addresses. The H.323 protocol uses well known ports to set up videoconference calls but, H.323 dynamically (i.e. on a per call basis) selects ports from a large number of possible port numbers. Whereas initial communication may take place on a well known port, much of the conversation that ensues takes place on dynamically selected ports chosen by the endpoints involved as they complete their call setup dialogue and media exchange. Calls may also be started from within or from outside the network, and so a typical firewall is going to block any attempts by anyone on a remote network to call inbound.

NAT (Network Address Translation) is widely deployed in large private networks. NAT is described fully in RFC1918 "a*ddress allocation for private internets*" and was introduced partly as a means of conserving real or public IP addresses. The deployment of NAT allows large organisations to give every computer a unique Internet address without diminishing the available pool of public IP addresses.

The NAT server at the network boundary maintains mappings between private and public IP addresses. However, this can cause problems with H.323 as a 'naïve' NAT server will only translate the address in the datagram header and not deeper in the stack or in the data payload itself. This can lead to the data being un-routable and the call failing

A range of methods and products are available that allow traversal of NAT and firewall boundaries in a secure and timely manner. The preferred solution to overcome these problems will depend upon the local site's security policy, IP addressing policy and choice of firewall products.

A number of solutions for firewall traversal and NAT are detailed in Appendix 3

STANDARD: Firewall traversal should be established to support both H323 and SIP video traffic.

8.4 Quality of Service

A basic network provides connectivity between sites for access to services and exchange of information. Without QoS, each packet is given equal access to resources. If the network cannot tell a voice or video packet from a data packet, it cannot give voice or video priority. In order for the network to efficiently utilise its network resources, it must identify which network traffic is critical traffic and allocate appropriate resources to support those traffic streams. If voice or video is present in the network, it must get priority over all data streams; otherwise, the result could be intermittent voice & video quality.

RECOMMENDATION: QOS should be implemented on both LAN and WAN links to support video conferencing.

9 Appendix 1 H323 and Gatekeeper Architecture

9.1 H323

H323 is an International Telecommunications Union (ITU) standard that provides specification for computers, equipment, and services for multimedia communication over packet based networks that defines how real-time audio, video and data information is transmitted. H.323 is commonly used in VoIP,Internet Telephony, and IP-based videoconferencing.

9.2 Gatekeepers

Although the H.323 standard describes the gatekeeper, as an optional component, it is in practice an essential tool for defining and controlling how voice and video communications are managed over the IP network. Gatekeepers are responsible for providing address translation between an endpoints current IP address and its various H.323 aliases, call control and routing services to H.323 endpoints, system management and security policies.

Gatekeepers provide the intelligence for delivering new IP services and applications. They allow network administrators to configure, monitor and manage the activities of registered endpoints, set policies and control network resources such as bandwidth usage within their H.323 zone. Registered endpoints can be H.323 terminals, gateways or MCU's, (multipoint control units).

Only one gatekeeper can manage an H.323 zone, but this zone could include several gateways and MCU's.

9.3 Interconnected Gatekeeper Zones

As stated earlier, the gatekeeper defines the zone and manages the registered endpoints within. To call an endpoint within the same zone, we simply dial that endpoints H.323 User Number. But what happens when we want to call an endpoint that is located in another zone? Well, we then also need to know the zone where that endpoint is registered. Each gatekeeper on the same network is identified by a unique number, its zone number. To call an endpoint in a different zone, we prefix that endpoints H.323 user number with its zone number and dial this extended number.

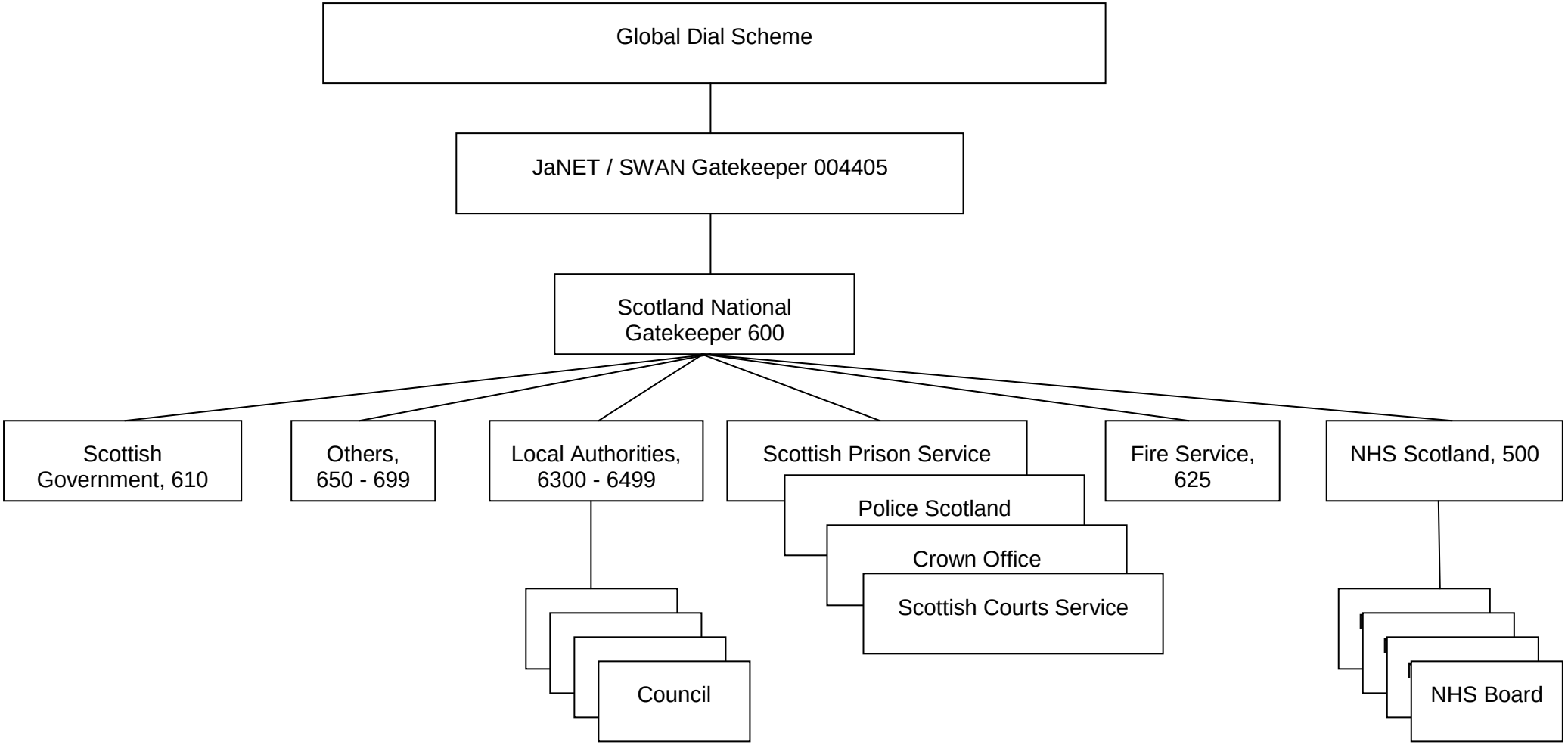
The telephone analogy to the gatekeeper zone number is the STD code for the local exchange. If we want to telephone a person locally, we just dial their local number, but if we want to telephone somebody further afield, we need to prefix their local number with their STD code.

Behind the scenes, all the gatekeepers on the network must know how they are related to each other When the gatekeepers are arranged in a multi-tier manner with a hierarchical structure, they are termed as being directory gatekeepers (DGK). This structure is recommended for Scotland, but also links into the wider JANET and Internet world for wider communications with university hospitals and other partners and stakeholders.

A directory gatekeeper only knows its parent and child gatekeepers as well as any directly registered endpoints. If the gatekeeper does not know the zone of the dialled number, it routes the call to its parent DGK, which then searches its database to see if the zone is known. If not known, this parent routes the call to its parent and so on until it eventually

reaches a parent DGK that has a child DGK that matches the zone. The call is then routed down through each child DGK tier until it reaches the specific endpoint.

Figure 1 Gatekeeper Hierarchy



10 Appendix 2 SIP Addressing

Session Initiation Protocol is an open signalling protocol standard developed by the Internet Engineering Task Force (IETF) in cooperation with many industry leaders. SIP is used for establishing, managing, and terminating real-time communications over large IP-based networks. via voice, video, or text (instant messaging), may take place using any combination of SIP-enabled devices, such as a video conferencing client on a laptop, softphone on a laptop computer, a wireless handheld device or PDA, a mobile phone, an instant messaging client on a desktop PC, or an IP phone with videoconferencing capabilities. SIP is an application layer peer-to-peer communication protocol

A key feature of SIP is its ability to use an end-user's *address of record (AOR)* as a single unifying public address for all communications. With SIP-enhanced communications, a user's AOR becomes their single address that links the user to all of the communication devices or services that they use. eg another user's AOR might be - sip:anotheruser@nhssvc.scot.nhs.uk. Using this AOR, you can reach another user on any of their multiple communication devices without having to know each of their unique device addresses or phone numbers.

To compliment AORs, SIP supports *Uniform Resource Identifiers (URIs)* that establish a common addressing scheme for all of an individual's user agents. A URI address follows the same basic format as a web or e-mail address: contact-address@domain. Using this format, SIP can map the unique addresses of a user's multiple devices and services to a communication domain, and then link all the user agents to a user's single AOR for that domain.

10.1 Gatekeeper/SIP

Many gatekeepers will provide interworking between SIP and H.323, translating between the two protocols to enable endpoints that only support one of these protocols to call each other.

In order for a SIP endpoint to be contactable via its registered alias, it must register its location with a SIP registrar. Many gatekeeper can act as a SIP registrars. When SIP mode has been enabled the gatekeeper may act as a SIP proxy server. The role of a proxy server is to forward requests (such as register and invite) from endpoints or other proxy servers. These requests are forwarded on to other proxy servers or to the destination endpoint.

11 Appendix 3 Firewall Port and NAT Solutions

The firewall and NAT problems described have inhibited the uptake of H.323. It is not surprising, then, to find that the industry has addressed the problems posed by NAT boundary traversal and firewall traversal in a number of ways and there are a number of proprietary and standards-based solutions to these problems available. These are described below, and have been loosely grouped as 'network solutions' (those involving a centralised approach with some kind of intervention at the network border) and 'endpoint solutions' (those that involve intervention from the endpoint itself). Some solutions involve interaction between these two elements and may be called hybrid solutions.

11.1 Option 1 - De-Militarised Zone (DMZ) deployment

The DMZ is a concept well-known to the network administrator. It is a subnet between the internal and external networks, usually with public addresses, where hosts on the internal network can initiate contact with servers or other machines within the DMZ but not vice-versa. Machines on the external network can contact those in an organisation's DMZ but, from there, can find no route to the internal, protected network. This is often the location of (outwardly accessible) web or e-mail servers. Placing H.323 equipment within the DMZ will not protect the H.323 endpoints themselves but will protect the rest of the local network from the security issues raised by H.323 deployment.

11.2 Option 2 - H.323-aware firewall

It is possible to give a firewall (that is often also performing NAT) an awareness of the H.323 protocol, so that it can manage a table of calls and either track the setup exchanges so that it 'learns' the ports to be used by the endpoints concerned. Then it can open them accordingly; and/or it singles out H.323 exchanges and over-writes unroutable IP addresses in outbound packets with a static NAT routable address as the source and re-addresses inbound packets so they reach their destination. Firewalls that perform these kind of functions are said to be 'H.323 aware' – in short, they have some extra functionality that makes them able to allow H.323 calls to be set up and completed without adding any undue latency to the call. These are often referred to as 'H.323 fix-ups 'or 'VoIP fix-ups'. For H.323, network latency is a crucial element of the overall QoS, and is an issue here because the protocol inspection required by H.323 aware firewalls can be computing intensive and thus has the potential to add to the round-trip time for the media being exchanged between the two endpoints. Firewall manufacturers have had varying degrees of success with producing H.323 aware firewalls, and the H.323 elements are sometimes sold as an additional add-on to the basic product, so this approach has failed to solve the problem to the satisfaction of many network managers.

11.3 Option 3 - Co-edged proxy/router

This method is also referred to as an IP/IP gateway as it provides an alternate gateway between the Local Area Network (LAN) and the adjacent network Point of Presence (PoP). This solution involves locating a gateway device at the edge of the network. In fact this device will straddle the two networks in the same way as the firewall. Using routing rules within the network, H.323 packets are routed to a device that is located alongside, but independent of, the firewall. The device has two or more network addresses, and routes to both the outer and the inner network. It monitors H.323 setup conversations between endpoints and replaces all internal network addresses with its own address. It then maintains a table of current calls and routes incoming packets accordingly. By deploying such a device, the firewall is circumvented completely and there is no need to make any changes to

firewall configuration. The H.323 proxy also handles the problem of NAT as the concept works in exactly the same way, whether the internal network uses public or private addresses – either way, they are hidden from the external network, as only the Proxy address is ever forwarded.

11.4 Option 4 - Border Negotiation Devices

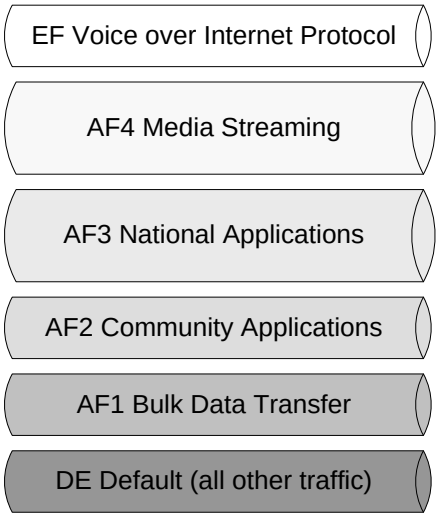
Also known as traversal servers, these devices are situated in the external network and provide a means for endpoints to traverse the firewall and/or NAT boundary without the need for unacceptable alterations to the firewall. Where the endpoint also supports H.460.18, there is no need for a server element within the network, but, as the recommendations were not published until September 2005, many endpoints do not support these recommendations. Where it is necessary to support such legacy endpoints, the external border device works with an internal proxy-server device, which can incorporate an H.323 gatekeeper in the same physical unit. While the traversal server is placed outside the protected network, the proxy-server/gatekeeper is placed within the network and a tunnel through the firewall is built between the two elements. The internal devices are placed in serial with the firewall so that all packets that are passed through them also pass through the firewall, thence to the traversal server and then on into the external network.

12 Appendix 4 Quality of Service (QOS)

12.1 QoS on the SWAN Network

The SWAN network will provides Quality of Service based using the IETF standards-based '*diffserv'* model to optimise use of bandwidth. This model does not reserve bandwidth for specific applications on demand between points on the network, but instead it acts by aggregating traffic of similar character. i.e. a specific group of applications can be guaranteed a minimum throughput, even in the event of network congestion.

Example of QoS 6 layer model:



12.2 QoS for Video Services

To achieve Quality of Service for video services, network traffic is marked at the router, based on source or destination IP address. Video conferencing can be identified and tagged as Assured Forwarding number 4 (AF4) of the six layer model (see diagram above).

However, it must be highlighted here that QoS will only be effective across the SWAN network (i.e between routers) and does not extend to end point devices on the LAN or non-SWAN routers within local networks. Extension of QOS into the LAN environment can be achieved by setting up VLAN's within the local network to separate video devices from voice and data networks. These VLAN's should adopt QoS wherever possible; this could be by trusting the SWAN marked packets, or re-marking locally to local standards.