Document Control

Document Title	Video Conferencing Standard
Version	1.0
Owner	NISG Telecoms, NHS National Services Scotland
Author	John Potts, john.potts@nhs.net, 0131 275 6687
Creation date	12th February 2010
Compliance	Recommended
Reviewers and Distribution	National Infrastructure Group, STAG, eHealth IMT Leads

Version Control

Date	Version	Author	Changes
12/02/2010	0.1 – 0.3	John Potts	Various drafts
18/02/2010	0.4	John Potts	Amendments to naming conventions following TAG meeting
09/03/2010	0.5	John Potts	Add Overview
27/04/2010	0.6	Paul McLaren	Transferred to eHealth Standards template
19/10/2010	0.7	Hazel Archer	Review following pilot implementation, addition of summary
11/02/2011	0.8	Paul McLaren	Update of dial plan (NHS Lanarkshire and Lothian naming conventions)
29/07/2011	0.9	Paul McLaren	Updating around referencing of N3 to NHS Wide Area Network. Added Health Scotland to Dial Plan & Changed QIS to HIS.
21/09/2011	1.0	Paul McLaren	Standard approved by eHealth Leads and published.

Consultation Record

Date	Notes
02-03/2010	Consultations with national video conferencing project technical advisory group
07/2011	Final round of consultation with stakeholders

Contents

1 Executive Summary 5
1.1 Quality of Service 5
1.2 IP Addressing 5
1.3 Firewall Recommendations 5
1.4 Gatekeeper Hierarchy 5
1.5 Dial Plan 6
1.6 H323 ID & URL Dialling 7
2 Quality of Service (QoS) on the NHS Wide Area Network. 8
2.1 Why do we need QoS? 8
2.2 QoS on the NHS Wide Area Network 8
2.3 QoS for Video Services 8
3 IP Addressing Policy for Video Conferencing in NHS Scotland 9
4 Firewall Traversal Issues 9
4.1 Deployment of H.323 for Video Conferencing. 9
4.2 Firewall and Port Issues 10
4.3 Network Address Translation Issue 11
5 Firewall Port and NAT Solutions 11
5.1 Option 1 - De-Militarised Zone (DMZ) deployment 12
5.2 Option 2 - H.323-aware firewall 12
5.3 Option 3 - Co-edged proxy/router 12
5.4 Option 4 - Border Negotiation Devices 13
6 Firewall Recommendations 13
7 Gatekeeper Architecture 14
7.1 Gatekeepers 14
7.2 Interconnected Gatekeeper Zones 14
Gatekeeper Hierarchy 16
8 Numbering Plan 16
8.1 About Dial Plans 16
8.2 Hierarchical Dial Plan 17
8.3 Dial Plan Structure 17
8.4 Dial Plan - E.164 Derived 17
8.4.1 Dial Plan 19

9 Naming Convention 21
10 SIP 22
10.1 What Is SIP? 22
10.1.1 H323 ID & URL Dialling 23

1 Executive Summary

1.1 Quality of Service

To achieve Quality of Service for video services, network traffic is marked at the WAN 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.

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

1.2 IP Addressing

The IP subnet reserved for video services is 10.247.64.0/18 (10.247.64.0 to 10.247.127.255)

Applications for video addresses should be made to nisgtelecom.nss@nhs.net

1.3 Firewall Recommendations

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.
It is planned that for VC, the DMZ deployment (5.1) or H.323 aware firewalls (5.2) can be adopted both centrally at the data centre and locally at the Health Boards. When these solutions aren't appropriate, border negotiation devices (5.4) should be considered.

DMZ Port Requirements -

- Firewall at all sites to allow all ports to/from 10.247.64.0/18 on the DMZ interface, or,
- Firewall at all sites to allow the ports shown in table 1 (see section 4.1) to/from 10.247.64.0/18 on the DMZ interface.
- Firewalls to deny access between their DMZ and their local/hosted services

1.4 Gatekeeper Hierarchy

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

1.5 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 health board areas in Scotland. The master gatekeeper will be programmed to add or remove the additional 6 digits that uniquely identifies NHS 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 NHS Scotland	00	44	05		
Ayr & Arran	00	44	05	513	yyyyyy
Borders	00	44	05	514	yyyyyy
Dumfries & Galloway	00	44	05	515	yyyyyy
Fife	00	44	05	516	yyyyyy
Forth Valley	00	44	05	517	yyyyyy
Grampian	00	44	05	511	yyyyyy
Greater Glasgow & Clyde	00	44	05	518	yyyyyy
Highland	00	44	05	510	yyyyyy
Lanarkshire	00	44	05	519	yyyyyy
Lothian	00	44	05	520	yyyyyy
Orkney	00	44	05	521	yyyyyy
Shetland	00	44	05	522	yyyyyy
Tayside	00	44	05	512	yyyyyy
Western Isles	00	44	05	523	yyyyyy
NHS24	00	44	05	524	yyyyyy
NSS	00	44	05	525	yyyyyy
Scottish Ambulance Service	00	44	05	526	yyyyyy
Golden Jubilee Nat Hosp	00	44	05	527	yyyyyy
Health Improvement Scotland	00	44	05	528	yyyyyy
National Education for Scotland	00	44	05	529	yyyyyy
State Hospital	00	44	05	530	yyyyyy
NHS Health Scotland	00	44	05	531	yyyyyy

For example, an endpoint in Highland will have an E164 address programmed into the endpoint of:

510123456

Health boards will be required to educate users that the full external address would be:

004405510123456

1.6 H323 ID & URL Dialling

This field may be left blank or configured for local use as all calls will be routed using E164 addresses. When a call is made using a URL the domain name will be stripped by the VCS and the call routed using the E164 address.

If a user wishes to dial a URL it must be of the form

<9 digit E164 Address>@vc?.scot.nhs.uk where ? is the agreed board identifier (max 3 characters) used in the system name.

e.g. 512123456@vct.scot.nhs.uk for an endpoint in Tayside

For SIP only systems uniquely identified with an individual user (eg PC based systems) the recommended standard remains:

<NHSMail User Name>@vc?.scot.nhs.uk

The VC?.scot.nhs.uk should be routable and should resolve to the appropriate VCS / SIP registrar.

2 Quality of Service (QoS) on the NHS Wide Area Network.

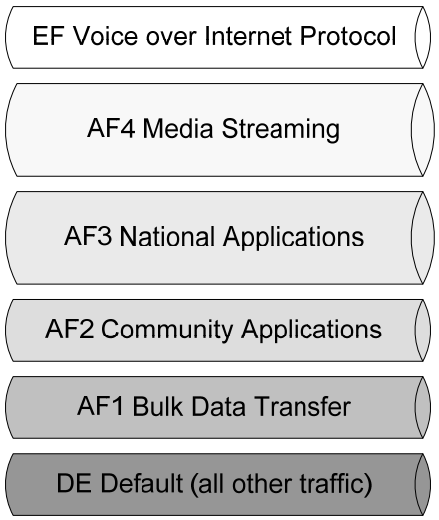
2.1 Why do we need QoS?

The NHS wide area network is a private network connecting more than 3,000 NHS sites in Scotland. The basic network provides connectivity between all of these 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 NHS wide area 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.

2.2 QoS on the NHS Wide Area Network

The NHS wide area network 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.

QoS 6 layer model on the NHS wide area network:



2.3 QoS for Video Services

To achieve Quality of Service for video services, network traffic is marked at the WAN 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 is only effective across the NHS wide area network (i.e between WAN routers) and does not extend to end point devices on the LAN or

non-NHS wide area network routers within COINS. Extension of QOS into the LAN environment can be achieved by setting up VLAN's within the Health Board network to separate video devices from voice and data networks. These VLAN's should adopt QoS wherever possible; this could be by trusting the marked packets, or re-marking locally to local standards.

3 IP Addressing Policy for Video Conferencing in NHS Scotland

The NHS operates an IP Addressing policy on the NHS wide area network, using the private class A addressing scheme (10.0.0.0/8). NHS Scotland has been allocated a portion of this subnet (10.240.0.0/16) which has been proportionally reserved/allocated to Health Boards. An IP subnet has also been reserved for video conferencing in NHS Scotland. This is designed to deliver end to end video across the NHS wide area network in Scotland. The subnet is managed by NISG, and allocated on request when Health Boards are implementing video conferencing to be routed across the NHS wide area network.

As of 2009, all Scottish NHS wide area network routers are now configured to tag any traffic, to or from the video services subnet, into QoS class AF4 described in section 1 above.

The IP subnet reserved for video services is 10.247.64.0/18 (10.247.64.0 to 10.247.127.255)

Please note, that H.323 endpoints without a VC IP Address, cannot register with TMS or route calls using the national infrastructure. Software Video clients (Movi) can register with the national Expressway from any IP Address, providing a valid account has been created within the TMS provisioning directory.

Applications for video addresses should be made to nisgtelecom.nss@nhs.net

4 Firewall Traversal Issues

While H.323 remains the established industry protocol for delivering core video functionality, Session Initiation Protocol (SIP) is gaining in popularity and enables video systems to leverage existing and next generation technologies.

Some of the problems experienced with H.323 video and firewalls are described below.

4.1 Deployment of H.323 for Video Conferencing.

The H.323 protocol works very well where it is used within the same organisational IP, NAT, firewalls and video conferencing network. However, problems are likely to occur when an organisation wishes to make H.323 calls to other organisations which usually mean traversing firewalls and NAT boundaries. The issues that have to be solved in order for H.323 to work across NAT boundaries and/or firewalls can be summarised as, network border traversal issues and can best be explained by considering the complex call set-up procedure for Video.

Whether the call is mediated by a gatekeeper or not, the communication between the endpoints uses ITU Recommendation H.225.0 for call signalling. The call setup procedure can be paraphrased as shown in Table 1 below;-

Table 1: call set up procedure

Endpoint	Protocol	Message	Port
A	H.225.0	Can we set up a call?	1720
B	H.225.0	OK, call proceeding	1720
B	H.225.0	Alerting user (ringing)	1720
A	H.225.0	What port shall we use for the next bit?	1720
B	H.225.0	Let's do H.245 **on these ports**	1720
A	H.245	I can do this and that (these are the speeds/encodings/decoding/etc I am capable of)...	Ports as defined in last step: between 1024 - 65535
B	H.245	I can do this, and that...	As above
A	H.245	Shall we use this encoding, that speed etc? **On these ports?**	As above
B	H.245	Yes, OK	As above
A	H.245	Right, let's go...	As above
A + B	RTP	Media content – two ports (content and control) in each direction, per media	A group of up to six contiguous ports, defined in the last step: between 1024 - 65535

Table 1 shows that up to 64,000 ports would need to be open at the Firewalls to allow H.323 video services across the wide area network.

In addition to the above ports, there are also ports to open to allow endpoint management systems to operate. These ports can be specific to the management system and will be addressed following procurement of the systems.

4.2 Firewall and Port Issues

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.

H.323 protocols port usage as described above, firewalls can be set up to leave certain well known ports open, but in order to cater for every eventuality in an H.323 call it would be necessary to leave 64,000 ports open (1024 - 65,535) – an unacceptably high number for most firewall administrators and one that virtually negates the point of having a firewall in the first place. So, H.323 calls are set up in a way that makes life difficult for firewalls – the call setup starts on well-known ports, but as the call setup is in progress, the two endpoints agree on a subset of the 64,000 ports available in order to exchange further setup information and/or for the transmission of media and media control messages. The precise subset of ports selected is random and unpredictable. Also, media is exchanged inbound on different ports to those used outbound and it is not possible to say from which end the first media packet will arrive.

4.3 Network Address Translation Issue

NAT should be familiar to network managers – it is widely deployed in large private networks. NAT is described fully in RFC1918 “a*ddress allocation for private internets*”. NAT was introduced partly as a means of conserving real or public (also sometimes called 'routable') 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. It does this by defining a set of addresses that should not be used on the NHS wide area network and should only be used within the private network. Thus these addresses are 'unroutable'.

NAT is usually overcome by deploying a NAT server at the network boundary, which maintains mappings between private (NAT) addresses and public IP addresses. These mappings may be static (i.e. permanent) or dynamic (i.e. ad hoc and temporary). The problem that NAT presents to a deployment of H.323 is due to the fact that both H.225 messages and H.245 call setup messages bury their network (IP) address deep in the data payload of the IP packet. This payload is examined by the equipment at the other end and the source address within is used as the return address. If the return address is one that is behind a NAT boundary then the packet will never reach its destination, as NAT addresses are unroutable in the NHS wide area network and the call will eventually time-out and fail. A 'naïve' NAT server will only change the addresses in the UDP or IP datagram header and footer, and not alter anything deeper in the protocol stack or in the data payload itself. This explains why H.323 works perfectly well when the two endpoints are within the same network, even when that network is using private (NAT) addresses. As long as the two endpoints have a route to each other then the call will succeed, as the packets exchanged never go beyond their particular NAT domain and so no translation is effected on the IP addresses used.

5 Firewall Port and NAT Solutions

The firewall and NAT problems described above have inhibited the uptake of H.323 videoconferencing and this has hampered the market growth of the associated industry. 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 now 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.

5.1 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, for example. 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.

It is also possible to deploy a variation of this topology where H.323 devices and endpoints are located physically together in the communications or server room, and audio-visual cables are used to carry sound and video to studios and back.

5.2 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.

5.3 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.

5.4 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.

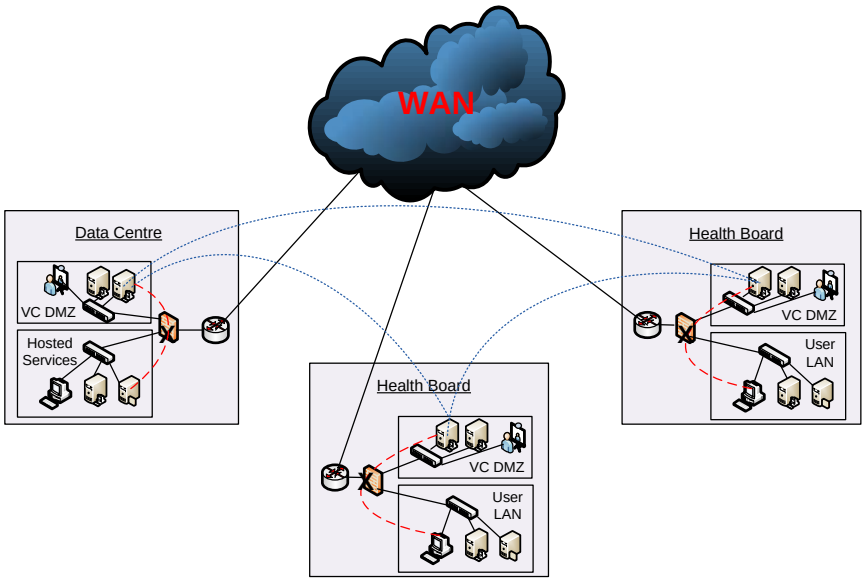
6 Firewall Recommendations

The industry has addressed these firewall traversal problems, and there is a now a range of methods and products 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.
It is planned that for the VC pilot, the DMZ deployment (5.1) or H.323 aware firewalls (5.2) can be adopted both centrally at the data centre and locally at the Health Boards. When these solutions aren't appropriate, border negotiation devices (5.4) should be considered.

DMZ Port Requirements -

- **Firewall at all sites to allow all ports to/from 10.247.64.0/18 on the DMZ interface, or,**
- **Firewall at all sites to allow the ports shown in table 1 (see section 4.1) to/from 10.247.64.0/18 on the DMZ interface.**
- **Firewalls to deny access between their DMZ and their local/hosted services**

DMZ Deployment on the NHS Wide Area Network



7 Gatekeeper Architecture

7.1 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.

7.2 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

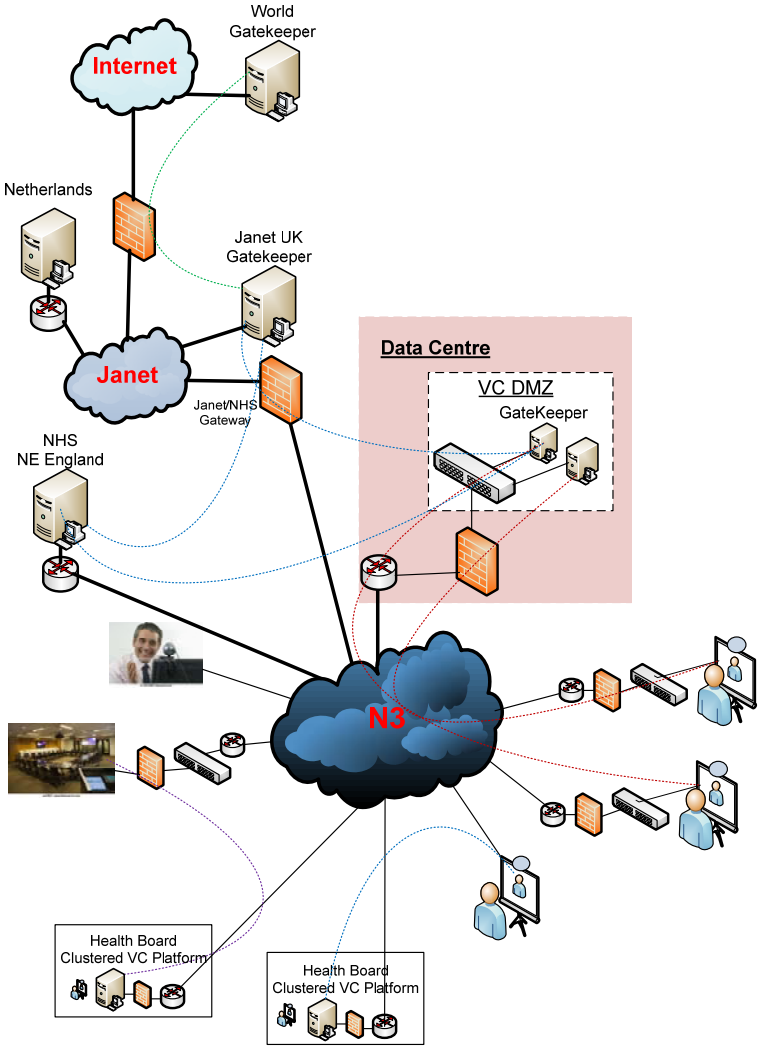
an endpoint in a different zone, we prefix that endpoints H.323 user number with its zone number and dial this extended number.

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 NHS 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.

Gatekeeper Hierarchy



8 Numbering Plan

8.1 About Dial Plans

As you start deploying more than one gatekeeper, it is useful to neighbour the systems together so that they can query each other about their registered endpoints. Before you start, you should consider how you will structure your dial plan. This will determine the aliases assigned to the endpoints, and the way in which the gatekeepers are neighboured together.

The solution chosen for the pilot, is the hierarchical dial plan using the global dialling scheme (GDS), which is sometimes known as the "E.164 addressing scheme". The adoption of clustering is also recommended to provide resilience.

8.2 Hierarchical Dial Plan

In this type of structure one gatekeeper is nominated as the directory for the deployment, and all other gatekeepers are neighboured with it alone. Each gatekeeper is configured with the directory gatekeeper as a neighbour zone with a match mode of Always, and the Directory Gatekeeper is configured with each Gatekeeper as a neighbour zone with a match mode of Pattern and its prefix as the pattern string. There is no need to neighbour the gatekeepers with each other. Adding a new gatekeeper now only requires changing configuration on that system and the directory gatekeeper. However, failure of the directory gatekeeper in this situation could cause significant disruption to communications. Clustering will be considered for increased resilience following the pilot phase.

8.3 Dial Plan Structure

The dial plan is simply a method of allocating a unique number to an H.323 endpoint. The structure is determined by the organisation's size, network structure and just how we are to be seen globally.

8.4 Dial Plan - E.164 Derived

Companies and institutions who operate globally need to develop a dial plan that addresses every potential endpoint, no matter where it may be. An example of such a dial plan that adheres to the E.164 scheme has been implemented in the UK by the JANET network and other NRENs (National Research and Educational Networks) around the world to support international H.323 conferencing. Implementation of this dial plan is mandatory for participation over these networks

Global Dialling Scheme (GDS)

00	44	XXXXX	YYYYYY

00 = International Dialling Prefix.
44 = Country Code
XXXXX = Zone Prefix
YYYYYY = Endpoint extension number

Zone Prefix	User Group
01XXX	HEIs, FEC's and other organisations with Janet primary connections.
02XXX	Regional Broadcast Consortia and Local Authrities
03XXX	Commercial organisations
04XXX	
05XXX	NHS UK

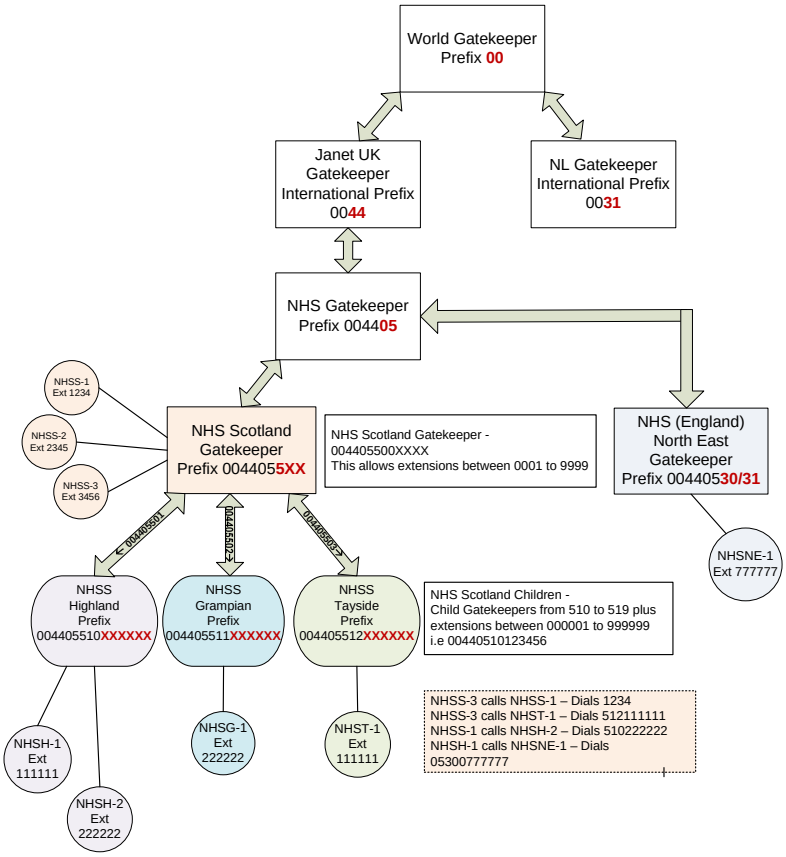
05	XXX

XXX - 30X = North East England
5XX = NHS Scotland

YYYYYY	6 Digit Extension number

This arrangement has recently been expanded to include NHS, and now extended to NHS Scotland.

Example of the hierarchy of Gatekeepers / Dial Plan



8.4.1 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 health board areas in Scotland. The master gatekeeper will be programmed to add or remove the additional 6 digits that uniquely identifies NHS 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 NHS Scotland	00	44	05		
Ayr & Arran	00	44	05	513	yyyyyy
Borders	00	44	05	514	yyyyyy
Dumfries & Galloway	00	44	05	515	yyyyyy
Fife	00	44	05	516	yyyyyy
Forth Valley	00	44	05	517	yyyyyy
Grampian	00	44	05	511	yyyyyy
Greater Glasgow & Clyde	00	44	05	518	yyyyyy
Highland	00	44	05	510	yyyyyy
Lanarkshire	00	44	05	519	yyyyyy
Lothian	00	44	05	520	yyyyyy
Orkney	00	44	05	521	yyyyyy
Shetland	00	44	05	522	yyyyyy
Tayside	00	44	05	512	yyyyyy
Western Isles	00	44	05	523	yyyyyy
NHS24	00	44	05	524	yyyyyy
NSS	00	44	05	525	yyyyyy
Scottish Ambulance Service	00	44	05	526	yyyyyy
Golden Jubilee Nat Hosp	00	44	05	527	yyyyyy
Quality Improvement Service	00	44	05	528	yyyyyy
National Education for Scotland	00	44	05	529	yyyyyy
State Hospital	00	44	05	530	yyyyyy

For example, an endpoint in Highland will have an E164 address programmed into the endpoint of:

510123456

Health boards will be required to educate users that the full external address would be:

004405510123456

9 Naming Convention

The name is used to identify endpoints appears in various places in the web interface of management system, and in the display of the video endpoint unit (so that you can identify it when it is in a rack with other systems). The system name is also used by management systems. We recommend that the systems are named in a way that allows you to easily and uniquely identify it.

Endpoint:

The naming convention for videoconferencing endpoints is as follows.

Healthboard.town.site.room

For example, a videoconferencing endpoint situated in the Conference Room at Aberdeen Royal Infirmary would be displayed in the following format;

NHSG.Aberdeen.ARI.Conference_Room

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

Health Board	Board	Town	Site	Room
Ayr & Arran	NHSAA	town	site	room
Borders	NHSBOR	town	site	room
Dumfries & Galloway	NHSDG	town	site	room
Fife	NHSFIF	town	site	room
Forth Valley	NHSFV	town	site	room
Grampian	NHSG	town	site	room
Greater Glasgow & Clyde	NHSGGC	town	site	room
Highland	NHSH	town	site	room
Lanarkshire	NHSLAN	town	site	room
Lothian	NHSL	town	site	room
Orkney	NHSORK	town	site	room
Shetland	NHSSHE	town	site	room
Tayside	NHST	town	site	room
Western Isles	NHSWI	town	site	room
NHS24	NHS24	town	site	room
NSS	NHSNSS	town	site	room
Scottish Ambulance Service	NHSSAS	town	site	room
Golden Jubilee Nat Hosp	NHSGJ	town	site	room
Quality Improvement Service	NHSQIS	town	site	room
National Education for Scotland	NHSNES	town	site	room

State Hospital	NHSSH	town	site	room

Board identifier – Max 6 characters must be unique and agreed by NSS
4 character names – may be allocated based on board cipher unless prior agreement between boards

e.g. NHSG.Aberdeen.ARI.Committee_Room_1

Person specific devices

SIP address for devices that are uniquely identifiable with an individual person should be allocated an address of the form

jo.bloggs@vc?.scot.nhs.uk

(using NHSMail unique name before "@")

10 SIP

As mentioned earlier in the document, H.323 is the established industry protocol for delivering video functionality, but SIP is gaining popularity and enables video systems to leverage existing and next generation technologies i.e unified communications, instant messaging, VoIP, softphone, presence, etc.

10.1 What Is SIP?

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.

Gatekeeper/SIP

The gatekeeper 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. The gatekeeper can act as a SIP registrar. 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.

10.1.1 H323 ID & URL Dialling

This field may be left blank or configured for local use as all calls to E164 enabled endpoints will be routed using E164 addresses. When a call is made using a URL the domain name will be stripped by the VCS and the call routed using the E164 address.

If a user wishes to dial a URL it must be of the form

<9 digit E164 Address>@vc?.scot.nhs.uk where ? is the agreed board identifier (max 3 characters) used in the system name.

e.g. 512123456@vct.scot.nhs.uk for an endpoint in Tayside

For SIP only systems uniquely identified with an individual user (eg PC based systems) the recommended standard remains:

<NHSMail User Name>@vc?.scot.nhs.uk

The VC?.scot.nhs.uk should be routable and should resolve to the appropriate VCS / SIP registrar.