

VNS Video-Over-IP Guidelines

Overview

The North Carolina Information Highway Video Conferencing Network has been used for years to provide distance-learning classes throughout the State's network of universities, community colleges, high schools and state agencies. Connections are established between sites using a circuit switching technology that physically connects each site together at a specified time for a specified period using a scheduler.

The advantages of moving to an IP based videoconferencing network include typically less expensive video systems that can be IP-only. The ability to connect to a larger global network of users that are not dependent on physical pathway connections of their locally built switched network.

Videoconferencing over IP operates ideally on a network that offers efficiency in the delivery of real-time video data packets. The dedicated T1 circuits of the H.320 standards-based world provided predictable quality over dedicated paths. Since IP packets are routed through a combination of dedicated circuits, non-switched connections, and large metropolitan networks, it is important to maintain data packet integrity of real-time video data through every connection, all the way to the other video endpoint. Real-time video must arrive fast and error free at its destination.

IP standards-based videoconferencing was engineered for videoconferencing that takes place on a data network without any quality-of-service, such as the Internet. Such networks are not intended for delivery of sensitive near real-time applications. The data network is used for multiple purposes: e-mail, web browsing, and other activities are inter-mixed with IP videoconferencing.

The audio/video information within a videoconference is segmented into chunks by the application, encoded and compressed, put into a series of data packets and sent over the network to the remote end at basically constant intervals. The data packets arrive at their destination at varying times, if at all, and often out of order. To keep the "real time" impression of an interactive videoconference, the packets must arrive, on time and in time to be re-ordered for delivery through the videoconferencing terminal.

Today your site is connected to the State owned network using some type of data transmission circuit (connectivity). Typically your site has a dedicated circuit provided by the State of NC. This dedicated circuit provides connectivity from your site to the larger State owned data, video, and voice network. In most cases Internet connectivity is also provided to your site using the same dedicated circuit. If you are using video conferencing for distance learning you currently have the choice of using either an H.320 capable video conferencing system or an H.323 (video over IP) system.



Office of Information Technology Services

ITS Video Network Services has developed these guidelines to ensure the highest possible degree of quality when configuring video over IP systems and LANs. These guidelines cover basic configuration of hardware and network architecture and components that are critical to reliable video communications.

What is H.323 (Video Over IP)?

H.323 is an umbrella recommendation from the International Telecommunications Union (ITU), setting standards for multimedia communications over LANs that do not guarantee quality of service. H.323 is part of a larger series of ITU-T communications standards for voice, data, and videoconferencing.

The first H.323 specification was approved in 1996, and subsequent versions have increased functionality. Using H.323 standards, a network manager can restrict network bandwidth used for applications like videoconferencing.

H.323 defines four major components for a network-based communications system: terminals, gateways, gatekeepers, and multipoint control units (MCU). Voice, video, and data are all supported across this common four-part architecture.

* Terminals or (Endpoints) are the video conferencing systems on a LAN that supports voice, video and data. H.323 terminals must also support H.245, which is used to negotiate channel usage and capabilities. Three other components are required: Q.931 for call signaling and call setup; Registration/Admission/Status, which is used to communicate with a gatekeeper; and support for sequencing audio and video packets.

A device called a codec accomplishes video processing in the video terminal. Codec is short for Coder/Decoder. A typical video conferencing system is comprised of a codec, cameras, audio system, video monitors, and network interface.

* Gateways are optional in an H.323 conference. Gateways provide many services, the most common being translation between H.323 conferencing endpoints and other terminal types. The ITS Video Network Services gateways bridge the NCIH H.320 network to the new H.323 IP network.

* A gatekeeper provides call control services to registered endpoints. In many ways, an H.323 gatekeeper acts as a virtual switch, and it performs address translation and manages bandwidth. The collection of all terminals, gateways, and MCUs managed by a single gatekeeper is known as an H.323 Zone.

* MCUs provide the capability to bring three or more parties on a single voice or video call. The MCU also provides key functions for multicast, including control over resource streaming to avoid bandwidth contention.



Office of Information Technology Services

Problems that may affect a video call

The path along the network between video end points, or from your sites video system to the MCU, has a significant impact on videoconferencing performance. Network packets do not necessarily take the shortest path from one location to another; routers determine which path is taken. A router examines the destination address of the packet and then calculates where to send it. Every pass through a router is called a "hop." Because a calculation is involved, even though it occurs at very high speed, every hop adds a bit of delay to the total time required to transit the entire path. Excessive network hops can degrade video performance. ITS Video Network Services recommends that video signals take no more than six hops to ensure their quality. A trace will determine the number of hops on your connection. If an independent ISP is involved there can be an excessive number of hops on your sites circuit. Usually with independent ISPs there is no way to guarantee that you will be provided the minimum recommended number of hops.

There are five fundamental network problems that affect IP video. They are *bandwidth, packet loss, latency, jitter and policies.*

Bandwidth – There should be enough space in a network path for all of your data, video, and voice packets to get through unimpeded. For a rough idea of scale, a typical ISDN videoconference uses around 128-384Kbps (kilobits per second). IP-based H.323 video systems can use the same amount of bandwidth or more. A typical IP video system can connect at between 128 – 768 K/bps. The bandwidth required for a given videoconferencing speed is higher on IP networks than on ISDN networks, because of the overhead packet requirements of TCP/IP. 20% overhead is required for a video call, so for example a 384Kbps IP video will actually use about 460 K/bps of bandwidth. This overhead space along with the number of video conferencing units located at your site is important when planning your sites bandwidth requirements.

Different clients are sensitive to discrepancies in bandwidth symmetry in different ways depending on if the bandwidth restriction is incoming or outgoing. In most cases, only video frame rate is affected, though some clients may drop the video or even the call all together.

Packet loss is when packets fail to arrive correctly, too late to be useful, or not arriving at all. This can be due to insufficient bandwidth along the path (when congestion occurs, routers will drop packets), or perhaps errors in transmission. Errors occur most commonly on wireless links such as microwave, satellite or local wireless Ethernet. They can however also occur on copper and even fiber links. Packet loss results in effects such as "tiling" within the video window, missing pieces or blank areas within the video window, and/or disruptions in audio.

Latency is the time delay between an event occurring and the remote end seeing it. Latency is introduced both by the encoding/decoding process, and hence depends on the equipment used, and also by the time it takes packets to traverse the network. There is



Office of Information Technology Services

little you can usually do to change the network latency, on any large scale, beyond getting directly involved with a carrier or a research network.

Excessive latency increases the chances of people "talking over one another" because they don't realize that the person at the other end has started speaking too. This is less significant in calls with less than 50ms of network latency. It can become very troublesome in calls with more than 150ms. Another problem is that the latency for the audio and video may be different, and hence lip movements don't appear synchronized with the audio. This is a function of both the terminal and the network, and can vary dramatically — some products try to compensate for it. You should experiment to see if it is an issue for your applications.

Jitter is the random variation in latency due to things like competing processes running on the terminal (for example on your desktop PC), other traffic temporarily blocking the path through routers along the way, or even the network path changing during a videoconference. This random variation is one of several things that cause packets to arrive out of order from their transmitted order. Jitter results in uneven and unpredictable quality within a videoconference and the end station client will try to compensate for it by buffering the traffic up to some finite time, before playing it out to you. This increases the latency even further.

Policies are introduced by things like firewalls and network address translation (NAT) devices that are generally used to try to hide or protect network elements from the wider Internet. H.323 uses dynamically allocated ports and is thus not very firewall-friendly.

WAN Connectivity and Bandwidth Planning

Network Bandwidth

Network bandwidth is the data rate that can be supported by your network connections and pipelines. Network bandwidth can refer to the theoretical limit or the actual usage. Most often when people discuss network bandwidth they are talking about the perceived speed of their local area network, but network bandwidth alone does not measure speed. The latency, or delays in processing, associated with the network also affects the speed of the network. Network bandwidth monitoring can identify bottlenecks as well as underutilized pipelines and should be part of the planning process.

Network Bandwidth -- Capacity Planning

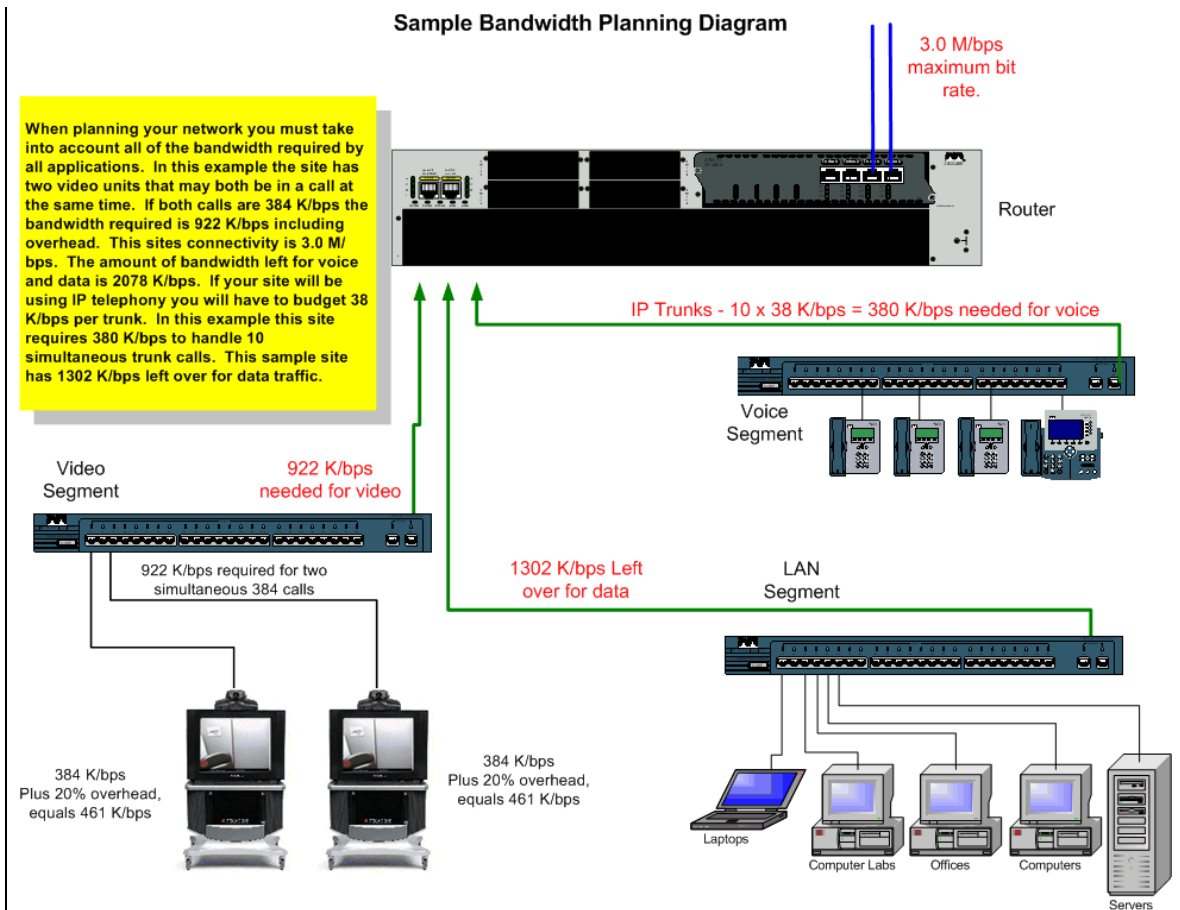
Another reason to monitor network bandwidth usage is for capacity planning. You need to know how network bandwidth usage fluctuates at different times of the day as well as from month to month if you are to make an informed decision about capacity growth or contraction.

Bandwidth planning requires that you evaluate two different metrics: the *total bandwidth* and the *highest bursting bandwidth*.

Total bandwidth is the total sum of all bandwidth consumed by all network devices on your LAN including servers, internet workstations, voice over IP applications, and video conferencing applications.

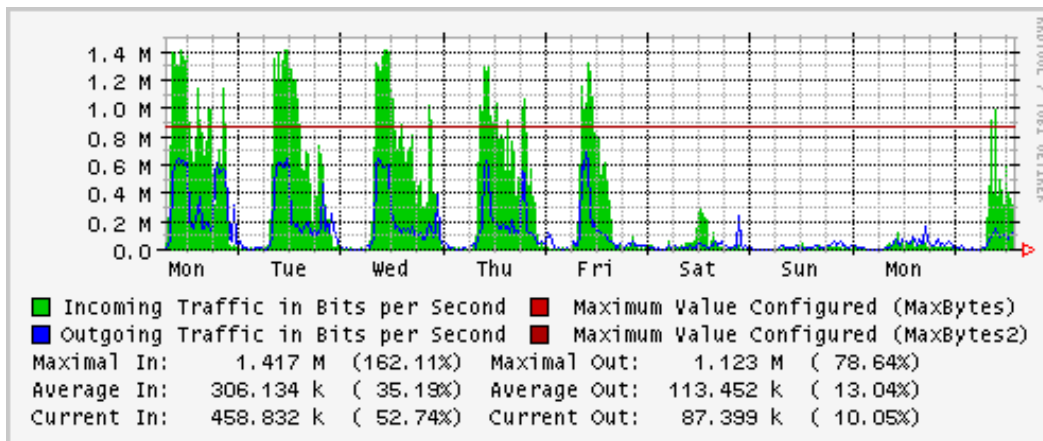
Highest bursting bandwidth is the total amount of predicible bursts that may occur. Bursts usually occur when a large amount of temporary data is transferred in or out of your network. A file transfer will produce an unpredictable burst during the time of transfer from one point to another. A 384 K/bps video call will be a constant, predictable amount of bandwidth consumption. When estimating bandwidth consumption for this application you can say that the bandwidth requirement for a 384 K/bps video connection will be 384 K/bps plus 20% overhead or 460 K/bps of maximum consumption during a call. Internet workstations, for example may consume only a very small amount of bandwidth if not transferring files, or receiving data.

This sample bandwidth-planning diagram shows this site using video, voice, and data. For visual purposes each application is broken down into separate segments using three separate switches. Each segment has its own bandwidth requirements with 3.0 M/bps connectivity to the site.



If your sites data connection is provided by ITS Data Services, a data analysis can be requested to see whether the existing amount of bandwidth will suffice for all applications or whether more bandwidth is needed. If the data connection is not provided by ITS, the client should contact their Internet Service Provider for this information.

The following illustration is an actual data analysis of bandwidth usage at Lenoir Community College during a single week. The Y co ordinate at the left of the graph indicates the amount of bandwidth used. As you can see there are peaks that approach 90% of the maximum 1.544 M/bps. These peaks usually occur during the busiest part of the day.



ITS Data Services offers several options for connectivity to your site. A 1.544 M/bps (T-1), a 3 M/bps, and a 6 M/bps circuit upgrade is available to link your site to the State owned network and the Internet. It is important to plan your network and consider the future needs of your campus or agency before ordering your bandwidth upgrade. We find that many sites are pushing 90-100% utilization of their maximum bandwidth on their current circuits. A typical campus network will have a mixture of data, video, and voice traffic traversing their campus in the near future. Correct planning can ensure that each site has enough bandwidth to handle daily activities at peak traffic hours.

ITS Video Network Services (VNS) has spent many hours engineering circuit configurations that will provide optimum throughput and quality on voice, video, and data applications.

Some advantages of purchasing your connectivity from the State of NC, ITS:

1. The ability to configure your connectivity with “Quality of Service, (QoS)”.



Office of Information Technology Services

2. State circuits are engineered for the fewest number of network hops.
3. 24 x 7 Helpdesk Support
4. Access by State ITS engineers to network equipment for monitoring and troubleshooting.
5. The ability to continually monitor your sites traffic to determine the percent of bandwidth utilization, or errors that may degrade quality.
6. Engineered and tested router hardware that provides the best configuration for video, voice, and data.
7. Our ability to expedite the repair of faulty lines and circuits that are managed by ITS Video Network Services.

Connectivity from Telcos and Internet Service Providers (ISPs)

Connectivity and bandwidth planning must also be accomplished when connectivity is ordered from independent ISPs or telephone companies. For video conferencing to be successful, all LAN configurations and conditions recommended in this document should also apply to circuits ordered through Telcos and ISPs.

It is crucial to provision your circuit with enough bandwidth incoming and outgoing to handle all of your sites video, voice, and data applications, and to allow for a reasonable amount of growth.

It is important to request the least number of network hops as possible. It may be possible to request a guaranteed number of hops or a not to exceed number when consulting with your provider's sales representative.

Typically an independent provider will not offer or guarantee any type of Quality of Service. It is recommended that you inquire if QoS is an option.

Know what you are buying. Independent providers offer many different configurations when selling network connectivity. They offer both symmetrical and non-symmetrical bandwidth, depending on your sites requirements. Usually non-symmetrical connectivity is less expensive. Symmetrical bandwidth is defined as the same amount of bandwidth incoming and outgoing at your site. This is referred to as the uplink and downlink. An example of a symmetrically provisioned circuit is a circuit with 768 K/bps Up and 768 K/bps Down. An example of Non-symmetrical provisioning can be 768 K/bps UP and 1.544 M/bps Down. It is crucial that a data analysis of your requirements both ways be accomplished to avoid costly errors in when ordering connectivity directly from an independent provider.

Quality of Service

Quality of Service (QoS) is a set of capabilities used to create differentiated services for network traffic, thereby providing better service for selected network traffic. For example, with QoS, bandwidth can be increased for critical traffic, and limited for non-critical traffic; consistent network response can be achieved, among other things. This allows the use of network connections more efficiently.

To implement QoS, QoS properties and policies are defined on devices or device interfaces. The policies can differentiate traffic based on its source, destination, or type. For example, you can recognize traffic based on the network host, port, protocol, or even IP precedence values in the packets.

QoS primarily comes into play when the amount of traffic through an interface is greater than the interface's bandwidth. When the traffic through an interface exceeds the bandwidth, packets form one or more *queues* from which the device selects the next packet to send. By setting the queuing property on a device or interface, you can control how the queues are serviced, thus determining the priority of the traffic.

ITS Data Services offers 1.544 M/bps (T-1), a 3 M/bps, and a 6 M/bps connectivity upgrades with the ability to enable Quality of Service. Video and voice traffic will have the highest priority assigned since these packets are expected to arrive at their destination near real-time. The bursty nature of data traffic, and non-real-time packet arrival requirements allow a lower priority to be assigned.

Circuit upgrade options will consist of new site routers that can be configured for QoS and have an optional built-in firewall. ITS Video Network Services recommends that QoS be enabled on all links carrying Video traffic. Extensive testing has been performed at ITS and each new data service offering has been designed to provide optimum quality and reliability of video traffic.

If your site purchases Internet connectivity from a private ISP there is no way to offer quality of service, or reduced number of hops through the ISP's network.



Office of Information Technology Services

LAN Configuration

On local area networks (your campus or building network), Category-5 (or better) horizontal network wiring or fiber optic vertical wiring is necessary. If wiring does not meet the minimum specification, it will be necessary to upgrade it.

ITS Video Network Services recommends a switched 100mb Ethernet connection to all video conferencing end-points. Switched Ethernet provides a more reliable connection for your data traffic than data hubs.

ITS Video Network Services does not recommend the use of hubs for IP video applications. The most common connection from a campus desktop to the network in the past has been through a device called a hub, which provides a shared Ethernet connection. Unfortunately, shared Ethernet is a "party line" communications system in which every packet sent to or received from any computer plugged in to the hub is echoed to every connected device. When one computer is sending or receiving data, it is given sole access to the network and the other devices are blocked temporarily. This system works well enough if there are only a small number of devices sharing the hub, and if the data being transferred varies in size and is not time sensitive. Since videoconferencing involves a continuing, bi-directional stream of traffic that is time-sensitive, use of a hub tends to degrade performance.

IP video service rates are defined with 384kb as a default speed for all video conferences. The VNS Web Scheduler and MCU can also support different speed rates such as 128kb and 256kb. If there is a mixture of sites with different speed capabilities, the MCU uses transcoding to bridge the different rates together.

The IP connection must provide enough bandwidth to support IP video applications. For a 384 K/bps videoconference you will need roughly 460 K/bps of bandwidth, full duplex through your network. All videoconferencing should be done over full duplex 100 M/bps LAN connections when possible.

Duplex mismatch is the number one cause of packet loss and video freezing. The switch port that an end-point is connected to should match the end-point Ethernet card setting. When possible, both the end point port and the switch port should be hard-coded to match duplex and speed capabilities. ITS Video Network Services will assist the client to make certain that duplex settings match switch settings. ITS Video Network Services recommends locking down switch ports either to 100 full duplex or to 10 half duplex.

This illustration is a guideline for configuring your video endpoint on your local area network. In most cases, higher quality switches have ports that can be hard-coded. Lower cost consumer grade switches have auto detect ports in most cases. Consumer grade switches should be avoided if possible.



Configure Port to
100/Full Duplex

Cable
connection
should be 100
meters or less

Auto should be avoided, however if you have no choice, or don't know if your switch can be set to 100/full, then ensure that both are hard coded to auto.

Configure System NIC
to 100/Full Duplex

Switch ports must be hard-coded to match the video systems configuration. The switch should be a make and model that allows hard-coding the switch ports to 100/full. If the switch is a 10/half switch you must make sure that the video system is hard coded to 10/half also.

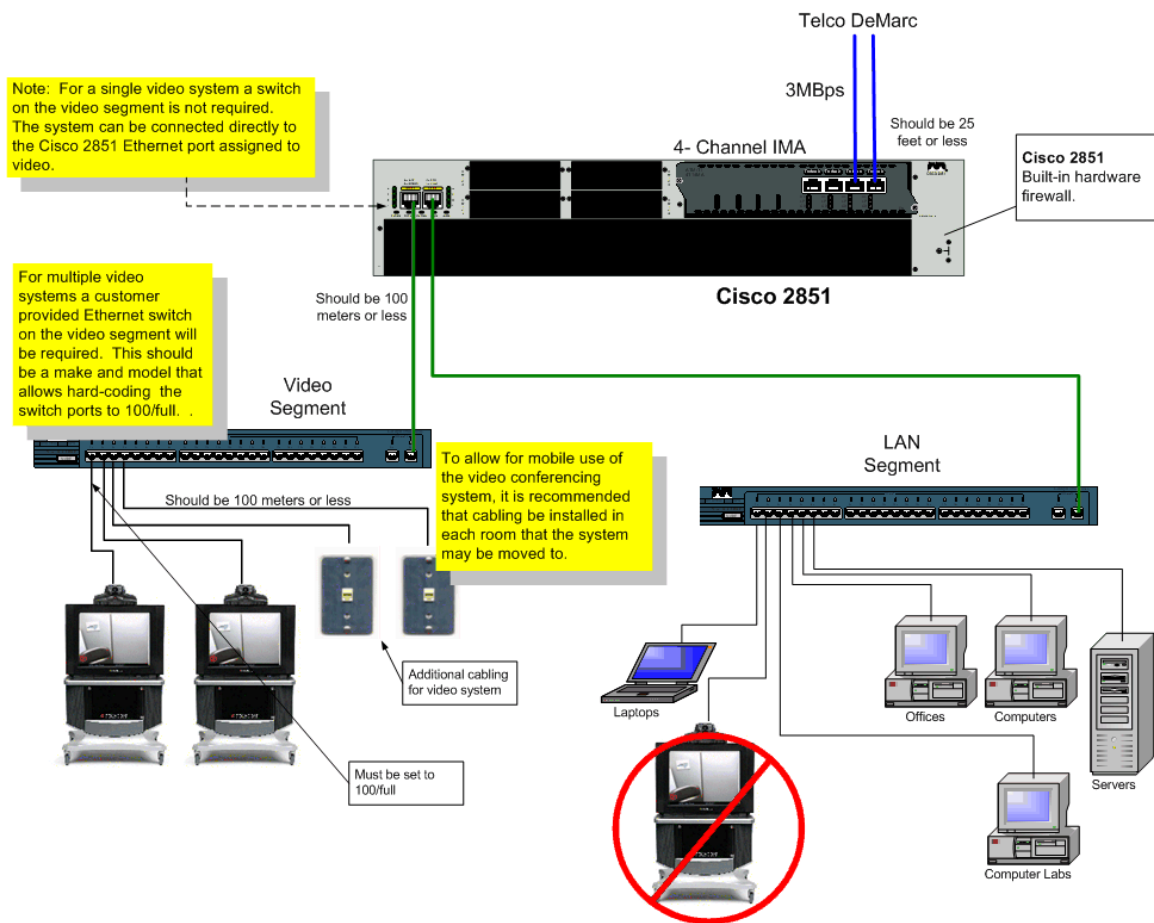


Switch	Video System	
100/Full Duplex	10/Full Duplex	⊘
100/Full Duplex	100/Half Duplex	⊘
100/Full Duplex	Auto	⊘
100/Full Duplex	100/Full Duplex	✓
10/Full Duplex	10/Full Duplex	✓
100/Full Duplex	100/Half Duplex	⊘
Auto	100/Full Duplex	⊘
Auto	100/Half Duplex	⊘
Auto	Auto	✓
Auto	10/Full Duplex	⊘
Auto	10/Half Duplex	⊘

LAN Network Segmentation

ITS Video Network Services may recommend segmenting the LAN, changing out hubs for switches, or possibly buying more WAN connectivity. A detailed assessment of your current network configuration will allow you to determine your network needs.

ITS Video Network Services recommends that the local area network be segmented to separate video from data traffic. This segmented configuration below also allows for multiple video systems on the video segment. This configuration essentially provides a separate network for video.



Firewall Configuration

Firewalls are a common cause of videoconferencing problems because of the number of ports that need to be opened to allow video signals to flow freely through them.

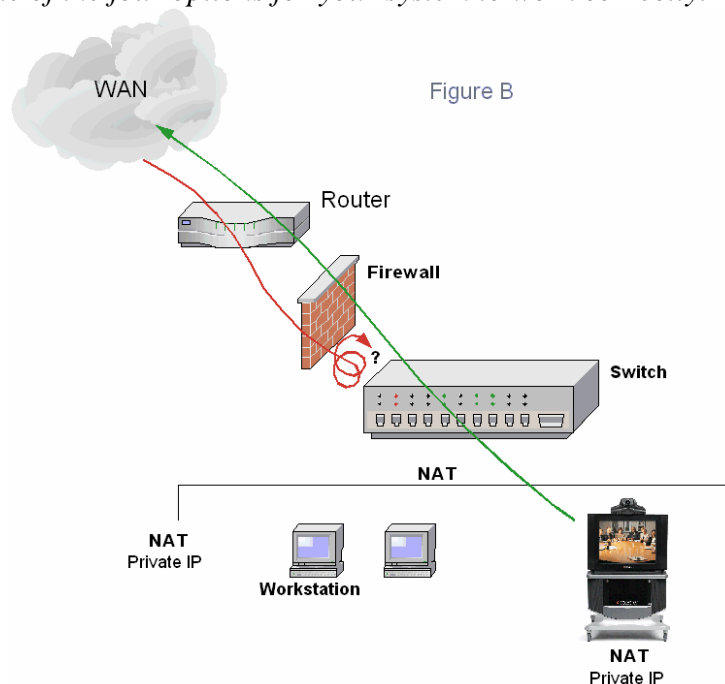
NAT or Private IP Addresses for Video Conferencing.

Since most outgoing firewall ports are open and incoming ports are restricted for security it is easy to make an outgoing call from inside your firewall. An issue exists when incoming video calls have to travel through your firewall and find your endpoint's IP address, especially if the IP address is a private NAT address. Incoming calls to your video unit will not arrive at your video system unless your firewall is configured to forward the IP video ports to the private static IP address of your video unit. See figure B.

Figure B illustrates that when using network address translation there is no real IP address that is visible to the public network, so an incoming call is unable to find its destination.

An outgoing call from the video system has no trouble calling a public IP through the firewall because typically the outgoing ports of the local firewall are open.

If your system is able to make calls but not receive calls, it is likely that you will have to configure one of the four options for your system to work correctly.





Office of Information Technology Services

Your configuration

ITS Video Network Services will assist local technical personnel with video firewall solutions. ITS Video Network Services cannot guarantee a solution for every firewall unless the Ridgeway Solution is elected.

Clients have four ways to address firewall issues, listed in order of preference:

1. If the video conferencing system is an appliance (Not PC Based) establish the end point outside the firewall or in a public DMZ with a public IP address. Refer to the section covering System Security and Password Protection to secure and protect your endpoint from intrusion.

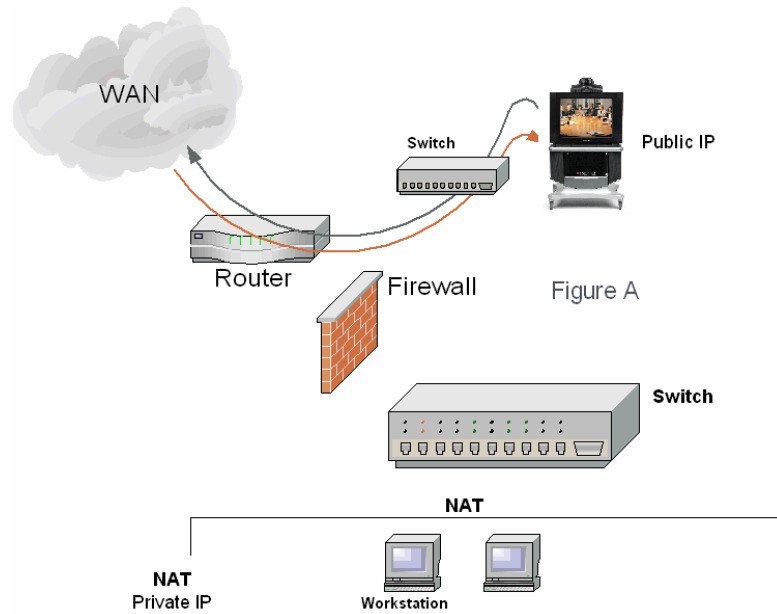
Video Conferencing Appliances



Figure A illustrates a public IP being used by the video system. For proper operation of the video network it is not uncommon to see public IP addresses assigned to video systems.

Since most group video systems tend to be appliance-based systems, there is no operating system such as Windows or Linux with typical vulnerabilities.

As long as the systems web interface, FTP interface, SNMP, and Telnet interface are either password protected or turned off the system is secure.



2. Establish the end point inside the firewall with a private NAT address and forward all H.323 related ports to the IP address of your video endpoint. Make a rule that will allow any IP address to and from the IP address of your endpoint for all ports listed in the table below.

Port forwarding of IP video traffic is one option that can be used to enable two-way communications with your video system. A more reliable and secure option is to use an H.323 proxy or a firewall traversal solution (proxy). Refer to the section covering System Security and Password Protection to secure and protect your endpoint from intrusion.

H.323 Port Requirements

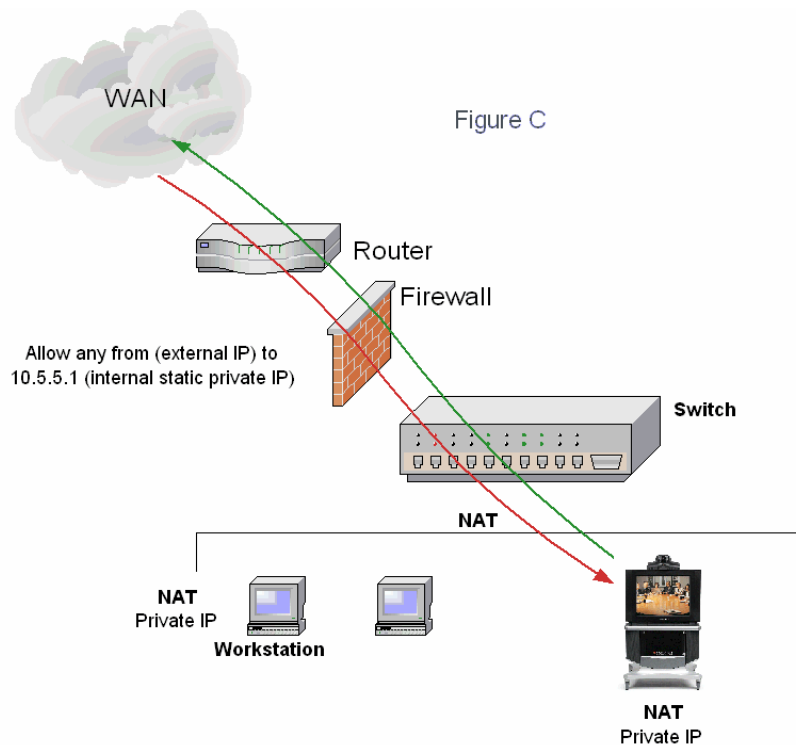
Port	Required/Opt	Port Type	Usage	Direction
80	Optional/Required for outside remote Maintenance	Static TCP	HTTP Interface	
21	Optional/Required for outside remote Maintenance	TCP	Software Updates	(Must Be Bidirectional)
23	Optional/Required for outside remote Maintenance	TCP	Telnet (Diagnostics & API Control)	(Must Be Bidirectional)
389	Optional/Required if network uses ILS	Static TCP	ILS Registration (LDAP)	(Must Be Bidirectional)
1503	Optional/Required if using T.120	Static TCP	T.120	(Must Be Bidirectional)
1718	Required	Static UDP	Gatekeeper Discovery	(Must Be Bidirectional)
1719	Required	Static UDP	Gatekeeper RAS	(Must Be Bidirectional)
1720	Required	Static TCP	H.323 Call Setup	(Must Be Bidirectional)
1731	Required	Static TCP	Audio Call Control	(Must Be Bidirectional)
1024 - 65535	Required	Dynamic TCP Port Allocation	H.245	(Must Be Bidirectional)
1024 - 65535	Required	Dynamic UDP Port Allocation	RTP	(Video Data) (Must Be Bidirectional)
1024 - 65535	Required	Dynamic UDP Port Allocation	RTP	(Video Data) (Must Be Bidirectional)
1024 - 65535	Required	Dynamic UDP Port Allocation	RTCP	(Video Data) (Must Be Bidirectional)

Note: Other ports may be required depending on application and manufacturer of equipment.

Figure C illustrates that allowing or forwarding IP video ports to the private static IP address of your video unit will enable incoming calls to find their destination.

Ports can be limited to only the H.323 ports. It is important to note that IP video systems dynamically select ports above 1024 for video, audio, and control. Fixed ports can only be selected on certain brands of equipment.

This option will require assistance from your firewall administrator and is part of the pre-configuration that should be accomplished prior to certification.



3. Establish the end point behind the firewall and use the endpoint software to limit the number of ports that need to be opened. A firewall technician will then need to make exceptions to and from this IP address with the specified ports. Some equipment manufacturers, Polycom for instance, allow you to keep the large port range 1024-65535 closed and open only 6 ports 3230-3235 for audio, video and control. This is known as using fixed ports.

Example of port requirements for Polycom video endpoint appliances.

Port	Required/Opt	Port Type	Usage	Direction
389	Optional/Required if network uses ILS	Static TCP	ILS Registration (LDAP)	(Must Be Bidirectional)
1718	Required	Static UDP	Gatekeeper Discovery	(Must Be Bidirectional)
1719	Required	Static UDP	Gatekeeper RAS	(Must Be Bidirectional)
1720	Required	Static TCP	H.323 Call Setup	(Must Be Bidirectional)
1731	Required	Static TCP	Audio Call Control	(Must Be Bidirectional)
3230 3235	Required	TCP/UDP	Signaling and control for audio, call, video, and data/FECC	(Must Be Bidirectional)
3603	Optional	Static TCP	Web Interface	(Must Be Bidirectional)

Other video endpoint manufactures may use different methods of handling firewalls. It is important to determine how your endpoint manufacturer handles firewall traversal.

For additional security refer to the section covering System Security and Password Protection to secure and protect your endpoint from intrusion.

4. Establish the end point behind the firewall and use the Ridgeway Solution. Video Network Services can provide a firewall proxy (Ridgeway) and assist with setup and configuration. The service uses only two well-known ports to pass video traffic through your agency's firewall. 2776 UDP/TCP and 2777 UDP are the only ports that need to be allowed through the firewall for video traffic. With the proxy service the video system's static NAT IP is assigned an alias. The proxy takes care of routing the incoming call to your NAT video system by sending the call to the system's alias. This service allows both outgoing and incoming calls to your unit with no special firewall configuration. The solution is the preferred method of handling NAT and firewalls because it allows your video system to use both its dial-in and dial-out features. IP Video bridging and scheduling services have the ability to dial into your system if they can be reached. Without configuring your firewall with port forwarding or using the Ridgeway service, your video system will be restricted to dial-out only.

The Ridgeway Group (Site) Client should be installed on a stand alone PC connected to the same network segment as your video units. This machine should have Internet access with an Internet browser installed. There should be no firewall restrictions on the internal network from the Group client to each video appliance since they will both be on the same internal secured network. The stand alone PC should remain on at all times and therefore should have a UPS system installed to maintain power. If the Ridgeway group client is turned off or loses power then video endpoints will lose connectivity. Figure D explains the configuration.

The Group client should adhere to the following specifications:

Intel Pentium III, 600Mhz

128 Meg RAM

4.0Gb Hard Drive

100Mb NIC Card

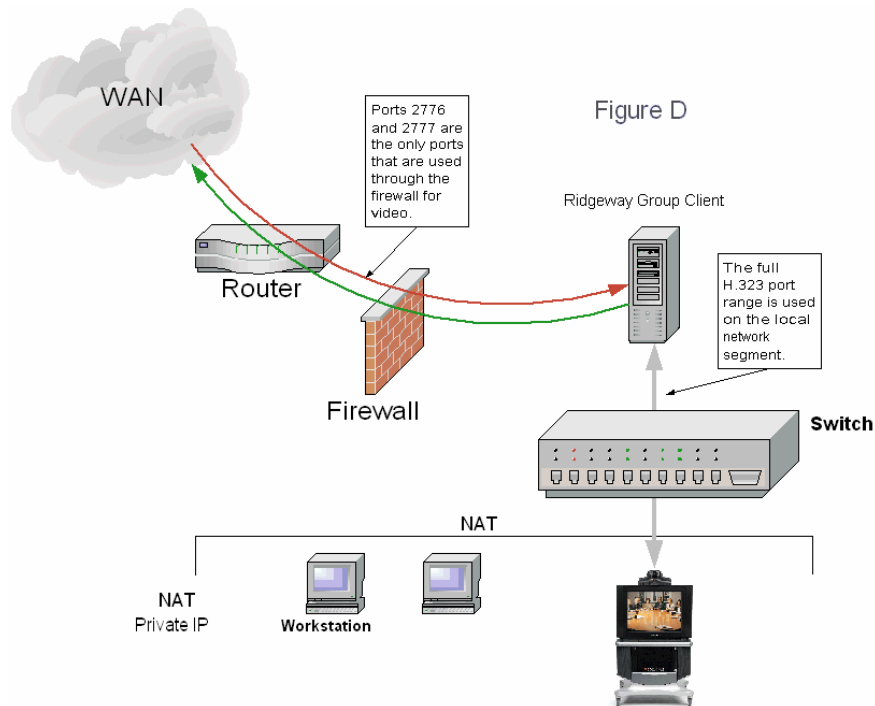
Operating System: Windows 2000 server, Windows 2000 Professional, or XP.

If the Ridgeway Solution is used for firewall traversal, VNS will assist the client in configuring the end point to work with either the Ridgeway Personal or Group Clients. VNS will supply the Ridgeway software and accounts.

Figure D illustrates the Ridgeway group client configuration that provides a video proxy through your firewall.

Ports through the firewall can be limited to only 2776 and 2777 for video. Additional video systems may use the same proxy to traverse the firewall. ITS Video Network Services will provide the Ridgeway application software. Your agency would provide the workstation hardware.

This solution provides a reliable method of handling security through the firewall. This relatively simple installation also allows two way dialing.



Gatekeeper Registration

Gatekeepers provide network services to H.323 terminals, MCUs, and gateways. H.323 devices register with gatekeepers to send and receive H.323 calls. Gatekeepers give permission to make or accept a call based on a variety of factors.

Gatekeepers can provide network services such as:

1. Controlling the number and type of connections allowed across the network.
2. Helping to route a call to the correct destination.
3. Determining and maintaining the network address for incoming calls.

When a client subscribes to one of the ITS Video Network Services Video Services their video endpoint is configured to register to the VNS gatekeeper. Each endpoint is assigned a unique number that follows the ViDeNet dialing scheme. The (Global) Dialing Scheme (GDS) is a numbering plan for the global video and voice over IP network test bed, developed by ViDeNet. It is sometimes referred to as an E.164 number. It resembles the international telephone system, numbering plan, with some exceptions. With the GDS, you can number each participating videoconferencing endpoint, MCU conference and gateway. GDS provides, uniform dialing throughout the world.

Each basic number consists of four parts: < IAC><CC><OP><EN>

1. The International Access Code (IAC)

Also called the world gatekeeper prefix. This is defined as 00

2. A Country Code (CC)

This follows the ITU international access code system. For instance, the country code for the Netherlands is 31. The country code for the United States is 1.

3. An Organizational Prefix (OP)

Many national research organizations follow the telephone number system in their country and use their area code and organizational telephone exchange prefix. For instance, The ITS Video Network Services gatekeeper is assigned 1129. Other gatekeepers in the ViDeNet community locate the ITS Video Network Services gatekeeper by using this unique routing number. The service providers OP MUST be unique within a country.

4. An Endpoint Number (EN)

Your EN will be a number assigned to you by ITS Video Network Services. Each endpoint number MUST be unique within the VNS network. Normally the number assigned by VNS will begin with 555 then 4 digits, which are unique to your video endpoint.

The whole numeric number therefore looks like:

< IAC><CC><OP><EN>

Examples:

The ITS Video Network Services Help Desk number is **00(IAC) 1(CC) 1129(OP) 5551000(EN)**

Typed into your videoconferencing endpoint, the number would simply look like:
00111295551000

Registering to the ITS Video Network Services gatekeeper allows other locations to dial your site using both the IP address AND the GDS number. In cases where your unit is behind a firewall or using NAT, the GDS number may be the only way for someone to dial into your site.

Site Certification

Each site that subscribes to the video services provided by ITS Video Network Services will be certified for operation on the VNS video network. The certification is to ensure that all network, video, and firewall hardware is configured for optimal performance. Connections to video endpoints, MCUs, the gatekeeper, and gateways, are thoroughly tested prior to the first live connection on the network. Dial-in and dial-out testing is also performed to identify any limitations or problems that may affect your video conferencing sessions. All information including serial numbers and passwords collected during certification of your endpoint are stored at ITS Video Network Services for future reference.

It is recommended that prior to scheduling a certification, your video endpoint is at a location that will not be changed. Certification to use the network is not only given to the video endpoint but the entire network connection including network switches, routers, firewalls, cabling, and circuits.

If firewall configuration or network topology changes after an end point has been certified, recertification will be necessary. Recertification will test the recent changes and ensure that future conferences are launched at an acceptable quality level.



Office of Information Technology Services

End Point Hardware and Configuration

Certified Endpoint (Codecs) Products

ITS Video Network Services has spent many hours testing and integrating endpoints and the core H.323 service. In order to provide the most reliable experience, clients are encouraged to utilize a product from the list below. All products tested have past the following criteria.

1. H.323 standards compliant
2. Tested in our lab
3. Tested with our Ridgeway Server
4. Tested with our VNS web based scheduler
5. Tested with the MCU and the GW
6. Tested with the ITS Video Network Services Gatekeeper

ITS Video Network Services will support the following products to work with its H.323 infrastructure:

- Polycom
 - –ViewStation EX, FX, and VS4000,
 - –VSX 7000 (IP only) V.35 will not work on the NCIH
 - –ViaVideo
- Tandberg
 - –770, 880, 990
 - –2500
 - –6000

All of these products are H.323 standards-compliant and have been tested in the ITS laboratory setting with the VNS MCU and Gateway, the Gatekeeper, the Web Scheduler, and the Ridgeway server. They can all use Click & View, a session management application that allows a certified end point to change the appearance of a multipoint videoconference at their own site or for the entire conference. Session management capability is often referred to as Chair Control.

Certified Integrators

All clients are encouraged to utilize a certified vendor in order to have the most reliable service. If ITS Video Network Services has certified a vendor, they have successfully gone through the formal certification process defined below:

- Participated in an ITS Video Network Services service offering presentation. This presentation details ITS Video Network Services H.323 service offerings and their capabilities.



Office of Information Technology Services

- Submitted hourly travel and labor costs
- Agreed to offer an option to maintain a site's existing equipment and new sales.
- Are capable of remote diagnostics
- Are Polycom and Tandberg certified
- Are capable of selling a box or custom room

Using H.264

H.264 is an improved video compression algorithm. The H.264 encoding technique significantly improves the quality of video to allow for lower bandwidth usage. Typically we have seen that using the H.264 standard at 128 K/bps provides a video quality that approaches the quality of an H.263 call at 384 K/bps.

The ITS Video bridge is capable of providing H.264 service with release 7.0. To reduce bandwidth usage a client may choose to purchase a video system capable of H.264 and launch a conference that consumes less bandwidth. This will reduce the overall traffic on your network allowing more bandwidth to data traffic. H.264 may be used at 384 K/bps to improve the overall video quality.

Most major manufacturers of video conferencing systems have employed H.264 in some form. ITS Video Network Services has tested both Polycom and Tandberg endpoints using H.264.

System Security and Password Protection

Most video conferencing systems have a built in web interface, telnet, and FTP server. Video endpoints are also built to respond to SNMP. The web interface allows configuration, control, and monitoring of the system via a web browser. The Telnet and FTP interface is primarily used for software updates, diagnostics, and API control. Calls can be launched and dropped using most systems web interfaces. Your unit also allows configuration changes and software upgrades for remote administration through telnet and FTP. To reduce the risk of unauthorized access to your unit ITS Video Network Services recommends that the highest possible protection be put in place.

For video systems that are assigned a public IP, ITS Video Network Services recommends that the systems built in web interface be password protected. Telnet, SNMP, and FTP access to the video system should be disabled and only allowed when requested by ITS Video Network Services personnel. As an alternative these ports can also be blocked in the firewall. Access lists can be created allowing access to web, telnet,



Office of Information Technology Services

and FTP by essential personnel only. Consult the operating manual of your specific video endpoint for instructions on disabling these interfaces.