

VNS Video-Over-IP Guidelines Summary

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 to 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 must 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*.

ITS Offerings

ITS Data Services offers several options for connectivity to your site. A 1.544 Mbps (T-1), a 3 Mbps, and a 6 Mbps circuit upgrade is available to link your site to the State owned network and the Internet. Additional, higher bandwidth links are also available.

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 must also apply to circuits ordered through Telcos and ISPs.



Office of Information Technology Services

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

Quality of Service

ITS Data Services offers 1.544 Mbps (T-1), a 3 Mbps, and a 6 Mbps 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.

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 100 Mbps Ethernet connection to all video conferencing end-points. Switched Ethernet provides a more reliable connection for your data traffic than data hubs.

IP video service rates are defined with 384 Kbps as a default speed for all videoconferences. The VNS Web Scheduler and MCU can also support different speed rates such as 128 Kbps and 256 Kbps. 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 Kbps videoconference you will need roughly 460 Kbps of bandwidth, full duplex through your network. All videoconferencing must be done over full duplex 100 Mbps 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 match the end-point Ethernet card setting. When possible, both the end point port and the switch port must 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.

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. Segmentation can be accomplished either physically or virtually by creating a VLAN for video.

Firewall Configuration

NAT or Private IP Addresses for Video Conferencing.

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.
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.
3. Establish the end point behind firewalls 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, allows 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.
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



Office of Information Technology Services

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.

Gatekeeper Registration

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.

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.

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.

ITS Video Network Services will support several major manufacturers equipment. The list of ITS tested equipment can be found at www.ncih.net.



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 must be disabled and only allowed when requested by ITS Video Network Services personnel. Consult the operating manual of your specific video endpoint for instructions on disabling these interfaces. As an alternative these ports can also be blocked in the firewall. Access lists can be created allowing access to web, telnet, and FTP by essential personnel only.