IP Video Conferencing Recommendations by the K-20 Technical Working Group

January 29, 2014
# Table of Contents

1. Background .............................................................. 2
2. Issue ........................................................................... 2
3. Scope .......................................................................... 2
4. IP Video Conferencing Overview .................................. 3
5. Optimizing and Maintaining the Local Network for IP Video .................................................. 4
   5.1. Introduction ................................................................. 4
   5.2. H.323 Video Call Technical Requirements .................. 5
   5.3. Network Design Considerations ................................... 5
   5.4. Optimizing the Local Network Environment ................ 9
6. Multipoint Control Units and Gatekeepers .......................................................... 10
   6.1. Requesting ViDeNet Number Assignments and Registered Endpoints ....... 11
   6.2. Assisting Off-Net Sites with Gatekeeper Registration ....................... 12
7. Assessing Local Endpoint Equipment Needs ....................................................... 13
8. IP Video Equipment Installation and Configuration .................................................. 14
   8.1. Endpoint Configuration and General H.323 Settings ....................... 14
   8.2. H.323 Desktop Video Conferencing ................................... 16
9. Managing IP Video Connection Quality .............................................................. 19
10. Operating and Troubleshooting IP Video Equipment .............................................. 20
11. Network Monitoring, Assessment, and Troubleshooting ........................................ 21
   11.1. Overview ................................................................. 21
   11.2. Why Use Network Monitoring/Assessment? ......................... 22
   11.3. Monitoring Scenarios ............................................... 22
Appendix A - Glossary ........................................................................ 24
Appendix B - Gatekeeper Peering ................................................................. 29
Appendix C - Firewall Configuration ............................................................... 31
Appendix D - Network Assessment Tools ......................................................... 38
Appendix E - IP Video Conferencing Implementation Checklist .............................. 42
Appendix F - List of NTSC Video Working Group Members ............................... 43
1. Background

The K-20 Education Network connects nearly 500 educational institutions throughout the State of Washington, including private universities and colleges, the SBCTC (State Board for Community and Technical Colleges) and associated colleges, a number of libraries, the Office of the Superintendent of Public Instruction (OSPI), the Educational Service Districts (ESDs), and K-12 school districts. The product of a collaborative effort including all of the above institutions as well as state government and private sector entities, K-20 provides infrastructure to support distance education and lifelong learning opportunities for persons of all ages throughout the diverse geography of Washington State. By using the K-20 Network, educational institutions are able to share information and applications, develop partnerships, and deliver essential programs, allowing the state’s educational system to be more creative, effective, and efficient.

Video Conferencing is one of the primary technologies used to collaborate and educate within K-20. This technology has the potential to transcend many of the limitations of geography and time, enabling educators to interact with students and develop collaborative learning environments beyond the confines of a typical classroom. Although video conferencing is often referred to as a single technology, the term actually encompasses a range of technologies and connectivity options that have evolved to meet user needs in a variety of settings.

2. Issue

When the Washington K-20 Education Network was created in 1996, video conferencing networks typically used H.320 standards and ISDN-based connectivity for both end-user systems and the Multipoint Control Unit (MCU) devices that managed calls involving multiple sites. By 1999, newer video conferencing systems from companies such as Polycom and Tandberg became available with limited support for connectivity to IP-based Local Area Networks (LANs) although ISDN remained the primary calling option for most video conferencing users. Today, ISDN connectivity is no longer use at K-20 connected institutions, IP networking is ubiquitous, and the IP capabilities of new video conferencing systems are sophisticated. In some instances, IP-based video conferencing equipment facilitates increased portability and flexibility due to its presence on the Local Area Network IP environment. Because of these developments and trends, there is increasing interest and activity within the K-20 Education Network focused on developing a better understanding of the challenges and requirements facing institutions as they implement and upgrade IP-based video conferencing resources.

3. Scope

This document is intended to provide institutional video conferencing support personnel such as Video Institutional Technical Units (VITUs) and Information Technology staff with information to aid them in the planning, implementation, and support of IP-based video conferencing. The
document will serve as an information resource for these groups, as well as a repository for new and updated information as related technologies continue to develop, mature, and find a place in the K-20 realm. Please contact Michael Evans at 360-292-4192 or michaele@k20wa.org if you have questions, comments, or additional information you would like to contribute to further the development of this documentation.

4. IP Video Conferencing Overview

Implementation of H.323 IP-based video conferencing requires technical support staff to think carefully about the acquisition and implementation of interactive video systems. Historically, IP-based LANs and WANs used technologies that were not designed with the requirements of IP video in mind. In these LAN environments, IP data traffic propagated on a collision sensing network based upon the idea that many network devices would share the communications link, sending out short bursts of data intermittently that sometimes competed for the wire. Many Ethernet environments began to drop packets at utilization levels above 70 percent. (Thankfully, the development of switched LAN environments and full-duplex connectivity at speeds of 100Mbps and faster mitigated or eliminated some of the limitations that once wreaked havoc with video connections on those legacy networking environments.) Also, for many types of data – for example, data carrying the information to display a web page in a browser – the amount of time between packets or the relative size of a packet in relation to those around it may vary considerably, but the variations probably won’t have a major impact on the end user’s experience. With these types of network data exchange, there is no problem with having a “best-effort” quality of delivery and providing for data to be sent over again if it contains errors or part of the information is lost. The requirements of H.323 IP-based video, however, are very different.

IP video conferencing using H.323 requires multiple streams of data to set up and manage the call, send video and audio information, and handle tasks such as far-end camera control. Although the data is sent as IP packets, the data streams are continuous, rather than intermittent, in order to maintain the video and audio connection. The amount of data in the streams also varies depending on the call content. For example, the amount of motion present in the camera view (this includes pan/tilt/zoom movement by the operator) combined with the overhead of managing the H.323 data streams in a typical IP video system creates a variable data throughput utilizing up to 460Kbps for a 384Kbps video call.

Effective management of procedures and technologies can help you address these issues within your local environment. Working with your institution’s IT staff to evaluate existing network infrastructure and plan for additional bandwidth needs are key components in the process of integrating video conferencing into an IP environment. Optimizing connectivity between video conferencing endpoints and the local network is critical as well. Evaluating and planning how to align the configuration of video conferencing endpoints with network border equipment, such as firewalls and bandwidth management devices, is also an important part of the process.
Another important aspect of IP interactive video conferencing is the concept of a gatekeeper. The gatekeeper provides a centralized means of associating the IP address of network endpoints with their system names, as well as providing a method of managing access to the Multipoint Control Units (MCUs) and generating logs of call connections and related activities. By registering with the gatekeeper, IP endpoints reserve a place in the network hierarchy and dialing plan.

You have probably heard people talking about QoS, or Quality of Service, when discussing video over IP. Quality of service methods use hardware and/or software to manage the available network bandwidth based upon predefined rules. Also, many new video conferencing products include features designed to improve the ability of systems to adjust to and absorb timing variations both within and among the data streams, as well as manage packet loss to some degree. Newer video algorithms help to improve call quality using the same or reduced amounts of bandwidth, potentially helping to keep network resource utilization to a minimum. K-20 is currently engaged in enabling QoS throughout the core network and to the edge routers and is optimizing support for this feature.

Determining the needs of end-users, optimizing the local network environment, and understanding the special requirements of H.323 IP video will help you facilitate a smooth and successful IP video implementation. Communication and team cooperation regarding configuration issues, network outages, traffic management, and call quality are all important aspects of this effort. Only through planning, effective implementation, and ongoing maintenance will interactive video and traditional data traffic be able to co-exist on IP networks.

5. Optimizing and Maintaining the Local Network for IP Video

5.1. Introduction

As mentioned earlier, legacy Local Area Networks were not generally optimized for IP video conferencing traffic. Fortunately, there are steps that can be taken to help ensure the local network will be a suitable environment for IP video. First and foremost, it is imperative that each institution’s video conferencing staff work closely with Information Technology staff during the IP video planning and preparation stage. This cooperation is critical to both the initial and ongoing success of IP video conferencing, as well as the continued effectiveness of applications already operating on the local network. The two teams and network end-users will benefit from regular meetings and information sharing regarding upgrades, configuration changes, and troubleshooting efforts relating to both the local network and IP video conferencing devices using the network. Secondly, it is vital that video support staff members communicate with educators, administrators and financial staff to ensure technical plans for video conferencing are in alignment with the curriculum, policy and financial goals of the institution. Finally, K-12 video conferencing support personnel are encouraged to consult with their regional or sector VITUs and/or RITUs regularly to keep those representatives involved in the planning, implementation, and maintenance phases of IP video conferencing initiatives.
5.2. H.323 Video Call Technical Requirements

As mentioned earlier, H.323 IP video conferencing requires separate data streams for call setup, channel control, video, and audio. Also, a suite of protocols, including H.225, H.245, H.26x, G.721, G.722, UDP, RTP, RTCP, and others form the building blocks of an H.323 video call as shown in Figure 1.

![Figure 1](image)

Maintaining these streams requires bandwidth overhead of up to 20% in order to maintain an H.323 video call. In other words, a 384Kbps IP video call requires a total bandwidth of about 460Kbps and a 512Kbps IP video call requires about 620Kbps of total bandwidth in order to avoid the issue of not having enough overhead to support the call. Also, variations in the timing between packets (jitter) both within a single stream (intra-stream) and among concurrent streams (inter-stream) and in the total time required for packets to go from one location to another (latency) can spell trouble for the quality of the connection. Packet loss is associated with network jitter, and a loss of 1% or more is often enough to seriously impact the quality of a video over IP call, although some newer technologies can reduce the impact of marginal packet losses. Generally, end-to-end latency is optimal below 150 milliseconds and becomes increasingly marginal up to 300 milliseconds. Because the video and audio content travel in separate streams containing packets of variable length, synchronization can be lost between the streams due to differences in the handling of the two types of data as they move through the network. Timing differences greater than 30 milliseconds between the video and audio streams will result in observed ‘lip sync’ issues that can distract from an otherwise effective call. Also, because the video stream requires more bandwidth than the audio, it often tends to degrade more noticeably when the network is carrying a lot of traffic and packet loss is occurring more frequently.

5.3. Network Design Considerations

Evaluating your K-20 bandwidth requirements can be a challenging process. First of all, tracking your usage will probably lead you to the conclusion that your institution’s bandwidth needs vary widely over time. The K-20 bandwidth usage statistics available online at [http://stats.wa-k20.net/k20cgp/](http://stats.wa-k20.net/k20cgp/) can provide valuable tools to help you with information gathering and analysis. As mentioned
earlier, you will also need to remember that each added IP video conferencing system placing and maintaining a 384Kbps call results in approximately 460Kbps of bandwidth usage including the overhead required to manage the call. One approach is to work with your network administrator to calculate the total bandwidth requirements for all video conferencing resources used simultaneously added to the highest anticipated peak bandwidth needed for all other applications connecting to K-20, plus an additional 20% to provide reasonable overhead. The resulting number should give you a good idea of your current bandwidth needs plus anticipated IP video conferencing bandwidth requirements. Another important point to keep in mind is that once this number is determined and connectivity is adjusted appropriately, regular monitoring and evaluation of bandwidth usage trends will need to continue in order to keep your bandwidth resources in alignment with the needs of your users.

One approach commonly used for managing and allocating LAN and WAN resources is virtual LAN, or VLAN, technology. Using VLAN architecture, the network resources can be logically grouped through software configuration rather than being limited to their physical connections to other network equipment. This allows network managers to select a group of devices – such as IP ITV equipment – and place those devices on their own virtual network within the larger LAN or WAN environment. In this way, network resources such as bandwidth allocation can be better administrated, and allocated. One point to remember, however, is that the local networking environment may need to be reconfigured or updated in order to support VLAN technology, so you will want to talk to your network administrator if you are interested in exploring this option. Also, if new VLANs are being configured to support video equipment, the associated changes will have to be made to all network equipment in the local network path. There have been cases where an institution’s video conferencing support staff tried to implement new video conferencing systems using information given to them by the network administrators and later learned the equipment couldn’t reach outside networks because the VLAN changes were made on some but not all of the local network devices.

Firewalls pose significant challenges to the effective use of IP video conferencing, because they are designed to regulate traffic between the outside world and the network infrastructure behind the firewall. H.323 IP video conferencing is particularly sensitive to blocking and filtering because it consists of a suite of protocols utilizing a number of ports in order to set up and maintain an H.323 video call on multiple data streams. If a gatekeeper is used, UDP ports 1718 and 1719 are needed to support RAS (Registration, Admission, and Status) functions. The call is initiated using a single fixed TCP port (1720) to start the call using the H.225 protocol. Next, a dynamic TCP port opens using the H.245 protocol for capabilities exchange and channel control. The last step in call setup is the opening of 2 dynamic UDP ports for each type of media that was negotiated for the call, typically video, audio, and far-end camera control. Additional features, such as content sharing, may result in other port requirements as well. Table 1 shows the port allocations required to support a typical 384Kbps IP call on the K-20 network.
Many newer video conferencing systems allow the dynamic ports to be limited to a narrow range, such as 3230-3235 for the TCP ports and 3230-3253 for UDP ports. This greatly reduces the number of ports that must be opened on the firewall to facilitate IP video conferencing, allowing both IP video traffic and network security features to be better managed. Also, bear in mind that firewall issues will need to be addressed on both ends of the connection in order for both sides to successfully place and maintain calls, so working with the personnel at locations you plan on conducting point-to-point IP video conferences with is essential.

There are a number of different makes and models of firewalls in use throughout the K-20 network. Firewall configuration is another aspect of preparing your network for IP video that will require you to work closely with your IT department. Keeping the software on both network devices and video endpoints up-to-date will help to minimize potential issues and ensure you have the most current features available for your systems. You will also need to review the latest documentation from both your firewall and endpoint vendors regarding support for H.323 IP video conferencing.

Refer to Appendix C for additional information about firewalls and firewall traversal considerations.

Bandwidth management is another aspect of network design and operations that can have a large impact on video conferencing activities. Bandwidth management devices are placed on the network border inside the firewall to help network administrators with monitoring, evaluating, and allocating bandwidth usage by various applications. Bandwidth management devices are sometimes initialized by setting them up to monitor existing traffic on a network and once the traffic flows are understood, profiles, policies, and partitioning functions can be set,
giving the network administrator a set of tools to help maintain a balance among the various applications and users of network resources. Packet shapers (products of Bluecoat Systems, Inc.) operate by 'marking' the packets as they travel through the network and can recognize specific components of H.323 IP video conferencing. Bandwidth can be reserved and optimized by application or protocol as well. These devices can generate a variety of reports, graphs and charts depicting many detailed network traffic metrics. For more information about packet shaping devices, visit http://www.bluecoat.com/products/packetshaper.

Another bandwidth management product currently used by K-20 institutions is NetEnforcer (now a subsidiary of Allot Communications). Like Packet Shapers, NetEnforcer devices are placed on the network border, but they use a different model than Packeteer's products. Rather than marking packets, these systems use packet inspection and fair weighted queuing to facilitate the prioritization of various kinds of network traffic. The NetEnforcer can also be used within a server environment to provide bandwidth management for networks of varying size. Like the Packeteer, the NetEnforcer interface can generate many reports, graphs and charts regarding network traffic patterns, and many detailed features are accessible by right-clicking directly on the charts and graphs in the user interface, providing an intuitive environment for drilling down on specific metrics. For more information about NetEnforcer products, go to http://www.allot.com/index.php?option=com_content&task=view&id=45&Itemid=88888966.

Recently, many institutions have been moving away from standalone appliances for bandwidth management partly because of the costs of the related hardware, software, licensing, and maintenance for the devices. Bandwidth management features are included in many modern firewall/security appliances, wireless management, and wired router and switches. Network administrators are leveraging these embedded features to manage the bandwidth available to various applications and protocols within their local networks. Also, many K-20 customers now have significant bandwidth available via Ethernet connections and this has reduced the need for bandwidth management in some situations.

One important point to keep in mind is bandwidth management equipment or software does not magically resolve all network problems or operate at maximum efficiency without ongoing attention. Also, some institutions may not derive much benefit from the presence of bandwidth management on their networks, especially those institutions running few applications and a small number of devices. Network administrators must keep a watchful eye on the various aspects of network performance, tweak the bandwidth management settings as required, and keep the operating systems and plug-ins or other supporting software up-to-date. Experienced users of these devices report that the most common mistake new users make is to begin setting policies to limit and managing network traffic before appropriate monitoring and analysis have been completed. Training and experience are critical to the effective utilization of bandwidth management systems, and the proper use of these types of network tools once again underscores the importance of cooperation and communication between and among network administrators and video conferencing support personnel.

NAT is a feature that helps to hide the local network infrastructure from the outside world, yet it also poses additional challenges for H.323 IP-based video conferencing. NAT uses a system of local and external addresses to hide an
intranet user from other networks, and is generally an integrated feature of firewall products. A NAT server translates the addresses of local intranet users to an external address, which is then used to identify the local user to remote users. Therefore, remote callers use this external address to reach the local video conferencing system, without knowing the system’s true local address. This process only works if the device running NAT is H.323 aware and both the network equipment and the video conferencing devices are properly configured. You will need to work with the local network administrator to determine whether or not your network uses NAT, and if NAT is in use, whether or not the NAT is H.323 compatible. You can also refer to the documentation for your specific endpoint(s) for additional information. Most recent releases of the major vendors’ endpoint software offer some support for NAT and allow you to specify the external IP address to be used by each video conferencing system.

Newer video conferencing endpoint equipment will require one of four NAT configuration settings as follows:

If the video conferencing system is not behind a NAT, select **Off** for the NAT setting.

**Auto** mode is chosen if the video conferencing system is behind a NAT that allows HTTP traffic.

Manual mode is chosen if the system is behind a NAT that does not allow HTTP traffic. This mode requires a configuration entry for the NAT Public Address you obtain from your local network administrator.

**UPnP**, which stands for Universal Plug and Play. Choose this mode if the system is behind a firewalled NAT router that is certified as being UPnP compatible. Routers used in home and small office environments often meet these criteria.

5.4. Optimizing The Local Network Environment

Optimizing the IP video path may include optimization of configuration settings on equipment, removing unnecessary components, and ensuring the use of high quality equipment and materials. The following are examples of items to evaluate and resolve as necessary:

- Use high quality manufactured CAT5e (or better) cabling and connectors
- Whenever possible, keep network cabling away from fluorescent lighting and AC wiring/outlets
- Don’t exceed 300 feet on UTP Ethernet segments and consider using another medium, such as multimode fiber with media converters, if you must exceed this distance
- Verify that cabling is installed in accordance with ANSI/TIA/EIA wiring standards. For more information, go to [www.siemon.com/us/standards/](http://www.siemon.com/us/standards/)
- Use devices with switched Ethernet interfaces between the ITV equipment and the K-20 border router (remove hubs from path)
- Remember that each switch in the path between the ITV equipment and the K-20 router will add to the total latency of the circuit
- At least 100MBps full-duplex Ethernet connectivity is recommended on all interfaces
- Set routers and switches to 100Mbps (or better) full duplex rather than to auto-negotiate mode
- Local area networks operating with switched connections in full-duplex mode at fast Ethernet or higher speeds using network devices with ample CPU and memory resources will deliver the best performance
- Ensure adequate bandwidth exists across institutional and K-20 WAN connections

For more information about applications, tools, and utilities to assist you with monitoring and evaluating your network performance, contact your local network administrator, regional data or video ITU, and/or refer to section 11 of this document, entitled Network Monitoring, Assessment, and Troubleshooting.

6. Multipoint Control Units and Gatekeepers

The K-20 Multipoint Control Units (MCUs) have considerable resources and features to support IP video conferencing activity. There are approximately 200 ports of IP capacity on the Seattle and Spokane K-20 MGC100 MCUs and an additional 96 ports of IP capacity on the K-20 MGC+100 MCU located at Washington State University. In 2010, K-20 purchased the new Tandberg/Cisco MSE 8000 MCUs which automatically transcode all video connections, support HD video conferencing, allow each participant to choose a custom continuous presence view, and have limited support for new technologies including video streaming. Port count is a moving number on the MSE 8000s due to a wide range of features with varying resource usage, but the Seattle MSE 8000 can support a maximum of 400 standard definition IP ports and the Spokane MSE can support up to 240 IP ports. Additionally, all Seattle and Spokane MCUs are able to provide limited support for gateway calls including both audio-only POTS connections and legacy ISDN endpoints.

The K-20 Gatekeeper performs several important functions. First of all, the gatekeeper manages access to the Seattle and Spokane MCU resources. Secondly, the gatekeeper stores information about an endpoint’s name, E.164 number, and IP address and the relationship of these data points to each other. The K-20 gatekeeper also follows a dialing plan and hierarchy that is based on the ViDeNet initiative, providing a structure to the way endpoint numbers are assigned and other gatekeepers are peered to the primary K-20 gatekeeper.

In order to fully participate in the K-20 IP video conferencing environment, you will need to register your endpoint(s) with the K-20 gatekeeper or peer your institutional gatekeeper with the K-20 gatekeeper. The K-20 gatekeeper and other gatekeepers peered to it comprise a ViDeNet zone. The K-20 zone administrator responds to requests for endpoint number assignments and gatekeeper peering information from institutional representatives and makes the necessary configuration changes to the K-20 gatekeeper. If you need to peer your institutional gatekeeper with the K-20 gatekeeper, please refer to Appendix A. If you do not have an institutional gatekeeper and only need to request number assignments for your endpoint or endpoints, please continue on to section 8.1.
6.1. Requesting ViDeNet Number Assignments and Registering Endpoints

The first step you need to complete is to request an endpoint number assignment or assignments from the K-20 Zone Administrator. To do this you will need to follow the instructions at http://www.wa-k20.net/h323.php?page=4b2&rn0=on&sn3=on. After you have submitted the appropriate information in your request and an endpoint number has been assigned, you will receive an email containing your new 14-digit ViDeNet endpoint number or numbers. You will notice the endpoint numbers are very long – 14 digits – and what follows is an explanation for the components of the number:

An example of a complete ViDeNet endpoint number is 00114790801025

The first part, 0011479, is comprised of the world code, the country code, and the prefix for the K-20 zone

The next section, 080, can be customized to allow K-20 institutions to peer their local gatekeepers with the K-20 gatekeeper

The last four digits, 1025, represent the extension number for an individual endpoint

The last step in the process of registering your video conferencing endpoints with the K-20 gatekeeper is to enter the gatekeeper registration information into the configuration settings on each video conferencing system. As shown in Figure 3, there are three main pieces of information you will need, including the gatekeeper address, the endpoint’s H.323 Name and the H.323 Extension.

Figure 2

The K-20 Gatekeeper IP Address field can be completed as gk.wa-k20.net (preferred) or, if your system configuration does not support DNS, the IP address of 68.179.206.20 can be used.

For the H.323 Name, we suggest using the format Institution Name-Building Name-Room Name. For systems that are moved between or among rooms or for rack-mounted video equipment, we suggest using the
format Institution Name-Building Name-System Number. An example of a name in this format is CVSD-Library-1.

For the H.323 Extension, enter the 14-digit ViDeNet endpoint number assigned to you by the K-20 Zone Administrator.

After you enter the information, you may need to re-boot the system manually before the gatekeeper registration completes. Some systems will re-boot automatically as soon as you change the settings. Most systems will display a message or some other sort of indication that the relationship with the gatekeeper has been established. It is important to note that once an endpoint is registered with the gatekeeper there is constant communication between the endpoint and gatekeeper even when the endpoint is not in a call. You can test whether or not the registration has been successful by attempting to place an IP video call to one of the K-20 loop back (0332222 or 0342222) numbers. After completing a successful loop back test, you will be ready to schedule additional testing with other IP endpoints and/or MCU calls involving other endpoints.

6.2. Assisting Off-Net Sites with Gatekeeper Registration

Sometimes you may need to provide some support to IP video conferencing sites that are outside the K-20 network to enable them to join K-20 multipoint video conferences. In these instances, the following procedures may be helpful in supporting the efforts of these “off-net” sites interested in registering with the K-20 gatekeeper and joining K-20 multipoint video conferencing events.

The K-20 Gatekeeper IP address and H.323 Name information needs to be entered on the video endpoint equipment in the same manner as for K-20 locations, but there is one major difference regarding the H.323 Extension. For the H.323 Extension, the off-net site needs to use their phone contact number or the number of a phone collocated with the video endpoint, in the format 2065551212. This number should not have hyphens, dashes or any other punctuation in it. The gatekeeper needs to have a unique H.323 Extension identified for each endpoint registered to it, and by using a specific phone number at the off-net site you can be certain the site’s endpoint is registered uniquely.

After the site personnel have entered the gatekeeper registration information, they may need to re-boot the video equipment in order to complete registration. If the endpoint is behind a firewall, the off-net site will need to ensure both the video equipment and the firewall are optioned correctly. If NAT, or network address translation, is being used locally, the appropriate settings will also have to be applied to both the firewall and the IP ITV system.

When adding the site to an event in the KORRS system, you will need to add the off-net site as an ‘OFF NET IP (Non-K-20) Non-Specified’ site. To check your work, test with the off-net site(s) by calling them via IP once all locations are registered with the gatekeeper and/or by setting up a multipoint test on the K-20 bridge and having the off-net site call the bridge using an assigned IP call-in number.
7. Assessing Local Endpoint Equipment Needs

The K-20 Network consists of an extremely diverse environment with various resources, users, and needs. The best method of determining your equipment needs is to identify how the requirements and goals of your end-users fit with the resources you currently have available and, if necessary, acquire new equipment to help you meet those requirements and goals. Some Polycom and Tandberg systems from the late 1990’s support IP video conferencing but do not support newer technologies, such as the H.264 video protocol and H.239. Some of these early IP-capable devices no longer have active software upgrade paths and may experience more reliability and compatibility issues than newer IP-capable devices.

Newer video conferencing endpoints generally can be grouped into one of four categories as outlined in Table 2.

Table 2: Categories of Video Conferencing Systems

<table>
<thead>
<tr>
<th>Category of System</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop</td>
<td>Software-based video conferencing systems using a personal computer as the hardware platform and a webcam for local video. An example of this type of video conferencing solution is Polycom PVX software and more information about PVX can be found at the Polycom website. These applications are IP-only and generally single-user solutions.</td>
</tr>
<tr>
<td>Office</td>
<td>Hardware-based systems including the codec, camera, and possibly an audio system in a single, compact unit. Some office devices – such as the Polycom VSX3000 – also include an integrated LCD monitor. These systems are usually designed for one or two users.</td>
</tr>
<tr>
<td>Conference Room</td>
<td>Systems for conference rooms typically house the codec, main camera, and sometimes the speakers in one or two components and use one or more external monitors to display the video from the far site or sites. These systems usually have limited ability to support one or more auxiliary cameras and other sources such as DVD players or VCRs. These systems are designed for small to medium-sized groups.</td>
</tr>
<tr>
<td>Large Conference Room</td>
<td>Large conference room systems often are designed as rack-mount codecs with extensive support for multiple monitors, cameras, and DVD players or VCRs, as well as high resolution monitors and room integration systems such as AMX or Crestron controllers. These systems usually are used for larger groups of people than the other devices.</td>
</tr>
</tbody>
</table>

Recently, there has been considerable interest within K-20 regarding the use of desktop software-based video conferencing codecs. While such applications may be appropriate for a single IP video user in some situations, those considering the acquisition and implementation of such
systems are encouraged to contemplate the dependency of such systems on the resources available on the host PC and connected peripherals. Also, cameras, microphones, and audio/visual capabilities of PC/software-based video conferencing solutions tend to be less sophisticated than those associated with stand-alone video appliances. Additionally, some users are interested in software-based systems to enable them to join events from home and, while this is possible, users may need to do considerable technical configuration and be willing to pay for upgraded service in order to achieve the necessary connectivity and IP bandwidth to support a symmetrical 384Kbps IP video call from a broadband Internet home connection.

One point to remember about new video conferencing systems is that the IP support in these units is generally very good. Also, features such as H.264 video and H.239 content sharing are available options in nearly all new video conferencing systems and applications from the major vendors. However, it is important to realize there may be variations in how standards such as H.264 and H.239 are implemented by various vendors. You may want to check with other institutions in your sector or with educational partners of your institution to learn about their challenges and successes, as well as what their plans are for acquiring new video conferencing equipment. This will help you to align your planning and implementation efforts with the broader K-20 community. You might also ask the vendor(s) to allow you to demo the video equipment to test the features and interoperability of specific units to see if they fit well with the needs of your end-users.

8. IP Video Equipment Installation and Configuration

8.1 Endpoint Configuration and General H.323 Settings

Once you have prepared the local network for the presence of IP video and have verified your existing equipment has IP capability or selected new equipment that will meet your IP video conferencing needs, you can proceed with the process of implementing your IP video conferencing systems. Connecting an IP video system to the network is similar to connecting other devices - such as personal computers - to a network. You can save time and avoid some difficulties by reviewing the installation and configuration documentation received with your IP video equipment, as well as ensuring the software version in use is up to date and the current release notes have been read.

Some video conferencing systems have the ability to act as web servers and will assign IP addresses to other devices on the local network when activated in that mode. Before connecting your endpoint to the network, you will need to ensure that this feature is disabled so that connecting the system will not interfere with the normal activity on the network. You may need to obtain some information from your network administrator and the specifics you will need to successfully configure a video conferencing device on the local area network will include some or all of the following:
• Enable the ‘Connect to my LAN’ option on the video conferencing system
• Enable H.323 calling in the video system Call Preference settings
• Enter a static IP address or configure the device to obtain an IP address automatically via Dynamic Host Configuration Protocol (DHCP)
• Enter a Host Name and Domain Name
• Enter DNS server addresses
• Enter default gateway address
• Enter the subnet mask
• Set the LAN connection speed and choose full-duplex mode (Typically 100/Full or Auto)
• Enter your firewall port and NAT configuration settings on the video system

Connect the network port on your video conferencing system to a port on your Local Area Network using a straight-through network cable with RJ45 connectors on each end. (Note: Some video conferencing systems have more than one network port. For example, on some systems the main network port is orange-bordered and the blue or brown bordered port is used to extend the LAN connection to a PC or other local network device. Proper configuration requires the main port to be the one connected to the network.) With the video conferencing system powered up, one steady and one flashing LED next to the LAN port are indications of a normally active link. Figure 2 shows an example of a typical video conferencing endpoint’s network ports.

Figure 3

At this point, you should be able to place an H.323 IP video call to another video conferencing system on your local network by entering the IP address, ensuring your video conferencing system is in H.323 calling mode, and initiating a call. Upon successful completion of a call within your network or in the event you don’t have any other local systems to test with, the next step is to try to call the IP address of a system outside your local network to determine whether or not there are additional
firewall and/or Network Address Translation issues to be worked out before you can place such a call successfully.

Once you have determined that you can call out successfully, you will want to conduct additional testing to ensure that others can call in to your system from the outside. Another important point about call settings is to select your call speed manually rather than using the Auto setting for call speed. The reason is your endpoint may connect at a speed your network is unable to support or may encounter other issues in Auto mode. If you select your calling speed manually you control the call rate and know what the rate is going to be before you connect.

The final step is to follow the directions in Section 6 Multipoint Control Units and Gatekeepers in order to register your video conferencing system or systems with the K-20 gatekeeper. Successful gatekeeper registration will allow you to use the seven digit numbers assigned by the K-20 MCU Scheduling and Support team to connect to the MCUs for multipoint video conferencing events. You will also be able to call other K-20 locations registered with the K-20 gatekeeper using their 14-digit ViDeNet endpoint numbers or H.323 Name. One additional point to keep in mind is that once registered with the gatekeeper, many video conferencing systems are unable to call other endpoints using a simple IP address. You may have to temporarily disable your gatekeeper registration in order to place calls using only the remote location’s IP address.

8.2 H.323 Desktop Video Conferencing
Software Available

The most widely used desktop video conferencing solution within K-20 is the Polycom PVX software. The Desktop Video Conferencing page on the K-20 website at http://www.wa-k20.net/dtv.php?page=4b4&rn0=on&sn3=on focuses primarily on the use of PVX. One important point is PVX works only in Windows environments, although some users have had success using PVX on a Mac running Windows. Another desktop application that has emerged within the past few years is Mirial HD. Mirial is available for both the Mac and PC and supports HD quality up to 1080p and includes an interesting feature that allows the user to treat two remote users either as callers on separate lines or as participants in a three-way video call. One point to keep in mind is that Mirial requires a true HD camera, a fast CPU with good memory resources, and at least 1Mbps of bandwidth to support HD connections. Because Mirial is still a relatively new application within K-20, users are encouraged to test its video and content capabilities with a range of partners in both point-to-point and MCU calls to verify its capabilities in your call environments. Also, obtaining release notes and information about Mirial support can be a bit difficult at times – the company is based in Milan, Italy. For more information about Mirial, visit http://www.mirial.com/products/Mirial_Softphone_HD.html.
Accessories

The most important accessory for desktop video conferencing is a camera to support outgoing video. Many modern laptops have built-in cameras, and a wide range of external cameras are available for use primarily via USB 2.0 interfaces. Most modern webcams supporting USB 2.0 will work with modern desktop video conferencing software, although you are advised to check the manufacturer’s release notes for information about hardware support for specific versions of software. For example, Polycom includes information about compatible cameras, driver versions, and their system resource loads in the release notes for PVX. Another important accessory is a headset with microphone. While some laptops with integrated microphones and noise-cancellation technology will support video conferencing without creating echo artifacts at remote sites, headsets are an inexpensive and effective way to ensure optimal audio quality in both directions within the desktop video conferencing environment. An example headset with stereo output and a single microphone input on standard laptop 1/8” stereo plugs is shown below.

Proprietary Desktop Video Conferencing Solutions

Proprietary video and audio conferencing solutions are becoming more widely used because customers find these tools make sense for some conferencing situations, particularly when cost must be kept to a minimum or a site that lacks H.323 video conferencing equipment needs to be included in an event. Keep in mind these solutions generally use proprietary designs that are not compatible with standards-based H.323 conferencing equipment, are limited by the available resources and input/output capabilities of host computers, and may be blocked by application-filtering network equipment. LifeSize video conferencing recently announced a video endpoint that includes integrated Skype support, further blurring the line between standards-based and proprietary video conferencing solutions. Because of recent developments in the broader spectrum of video conferencing and collaboration tools, brief descriptions of a few of these solutions are presented here.
Note: K-20 is resourced and budgeted to maintain only H.323 video conferencing as a centrally managed and supported video conferencing technology. The following information is for informational purposes only for customers who choose to locally use and support the following tools:

Skype

Skype audio and video conferencing have been around for several years and offer a free method of doing basic video and audio conferencing. Skype also supports file transfer, screen sharing, and instant messaging features. Skype charges fees when you go outside the Skype IP network and call cell or landline phones. Some users have reported issues with Skype serving as a supernode and using excess bandwidth over ports 80 and 443 even when not being in a call locally. These ports can be disabled within Skype by un-checking the box at Tools > Options > Connections called “Use port 80 and 443 as alternatives for incoming connections.” Also, some tools can monitor Skype to help you determine if excessive activity is occurring on your connection. One of these tools is called Netlimiter and can be downloaded at [http://www.netlimiter.com/](http://www.netlimiter.com/). You can gain additional information and download Skype at [http://www.skype.com/intl/en-us/features/allfeatures/video-call/](http://www.skype.com/intl/en-us/features/allfeatures/video-call/). For those users with dual core (or greater) processor computers and HD video cameras, Skype now offers a high definition version as well.

Google

Google voice and video chat enables you to use audio, video and text chat and is integrated with Gmail as well as a free service. Google’s solution integrates technologies from both Global IP Solutions and Vidyo. For more information and to download a copy of Google’s voice and video chat client, go to [http://www.google.com/chat/video](http://www.google.com/chat/video).

Yahoo

Yahoo Messenger offers both voice and video chat capabilities similar to the free offerings described above. One thing to keep in mind when installing these “free” applications is toolbars and other features may be part of the installation process and you will want to ensure you understand and accept these additional “features” before installing. You can learn more about Yahoo Messenger at [http://messenger.yahoo.com/](http://messenger.yahoo.com/).

Links to educational resources about using proprietary conferencing solutions in the classroom:

[Information about the use of Skype in a classroom environment](http://www.skype.com/intl/en-us/features/allfeatures/video-call/)
9. Managing IP Video Connection Quality

There are four major components involved in managing IP video connection quality at the local institution level. The first and second components, preparing the local network for IP video traffic and ensuring that enough bandwidth is available between the institution and K-20, have already been covered. Quality of Service, or QoS may be a helpful tool for the K-20 network and is an emerging technology within K-20. Lastly, new technologies integrated into video conferencing equipment enable conferences to use less bandwidth to achieve good quality video or absorb higher error rates without noticeable impact on perceived conference quality. Such technologies can help video conferencing and network support personnel to better utilize available resources.

Quality of Service (QoS) features are evolving technologies within K-20, and currently these features are being tested on some sections of the K-20 network backbone. QoS generally involves tagging specific IP packets to indicate they have a higher priority than others on the network or invoking mechanisms to reserve bandwidth for specific types of IP traffic. Modern video conferencing systems have the ability to configure several QoS settings, as follows:

- IP Precedence represents the priority of IP packets being sent across the network by the video system. The value can be set on a scale of 0 to 5, with a higher number indicating a higher priority within the network.
- DiffServe represents a priority level as well, with the value being set on a scale from 0 to 63, and a higher number indicating a higher level of service.
- RSVP stands for Resource Reservation Setup Protocol and enabling it allows the system to use RSVP to request that routers reserve bandwidth for the IP video call along an IP connection path. The near site, network equipment, and far site must all support RSVP in order for reservation requests to be made to routers along the connection path.

Quality of Service mechanisms will probably be most beneficial to institutions having intermittent spikes in bandwidth requirements or whose K-20 connection bandwidth is in the ‘gray area’ between not enough bandwidth and excess bandwidth due to frequent transient spikes in usage. Quality of Service is an issue that is best addressed by communicating with your network administrator and VITU or RITU to determine the optimal solution for your institution and to ensure compatibility with developments throughout the K-20 network.

Another consideration regarding IP video connection quality is the integration of new features and technologies in the video conferencing endpoint equipment that either make better use of the available bandwidth or increase the ability of the equipment to tolerate errors and packet loss on the circuit without noticeable degradation of the end-user’s video and audio. One example is the increasing usage of H.264 video to obtain improved video quality at a given rate or comparable video quality while reducing the data rate. For example, H.264 video is generally considered to provide about the same perceived video quality at 256Kbps
as the H.263 video protocol did at 384Kbps. This enables the end-user to experience about the same call quality as they did in the past with a 33% reduction in the bandwidth used. The tradeoff is that both the endpoint systems and the MCU must use more processing resources in order to support a protocol such as H.264. Also, some older IP-capable endpoint devices don’t have the processing power to support this standard at all, so H.264 software upgrades aren’t available for these systems.

An example of technology with the potential to maintain call quality under adverse or transient network conditions is the Polycom Video Error Concealment (PVEC) feature available on many video conferencing systems. Normally, packet loss of 1% is enough to seriously impact or even terminate an IP video conference, but PVEC is reported to allow endpoints to communicate with packet losses in the 2% to 3% range with minimal degradation of the call quality. Polycom has begun including an error correction feature called DBC-2 in the most recent product lines. DBC-2 is interesting because it is described as being compatible with the entire range of H.261, H.263, and H.264 protocols. An additional point to consider, however, is that support for some features, including H.264, PVEC, and DBC-2 is limited or not yet implemented on the current software builds for the K-20 MCUs, and support for these types of features on the MCU platform tends to lag behind the features available within the endpoint equipment for use in point-to-point calls.

Many Tandberg/Cisco systems support a feature called Intelligent Packet Loss Recovery (IPLR) that attempts to analyze the received information to determine what has been lost and minimize the impact to the image quality perceived by the viewer. Tandberg claims this technology can reduce the impact of packet loss in both directions of the call, even if the distant endpoint is not a Tandberg product. Tandberg has also implemented downspeeding features in their endpoints which can reduce the transmission rate when high amounts of packet loss are detected to try to find a speed at which no packet loss occurs. The feature is said to be designed so that if reduced speed does not decrease the packet loss, the call rate is returned to the original speed. Most recently, Tandberg/Cisco has introduced an updated technology called ClearPath. ClearPath includes an intelligent downspeeding feature, along with a means of updating the screen using less data than I-frames and a forward error correction approach similar to that used by Polycom DBC-2.

10. Operating and Troubleshooting IP Video Equipment

You will notice immediately upon placing an IP video call that the connection is either completed or rejected almost instantly. Also, if you happen to be monitoring the connection using a network protocol analyzer or bandwidth management device, you will notice the bandwidth usage varies widely on an IP video call depending on the amount of movement ‘seen’ by the camera and the use of specialized features, such as far-end camera control.

If you attempt to place an IP video call and the connection fails, a good first step is to try to connect to one of the MCU IP loop back numbers set aside for testing purposes. The IP loop back numbers are posted at
http://www.k20.ctc.edu/ISDN-support.asp#6 on the KORRS website. If the loop back test works, the connectivity from your endpoint to the K-20 gatekeeper/MCU and back is likely to be working correctly. This result indicates that something on the other side of the K-20 MCU is preventing the far site from connecting. If the loop back test fails, your next step might be to call another video endpoint inside your local network to determine whether or not that connection can be made successfully. By following this systematic process of isolating the section of the system that is causing the problem, you will be able to identify the source and reach a resolution more quickly and efficiently.

Sometimes, loop back testing can help you assist distant endpoints who are having trouble connecting to an MCU event. This is particularly true in situations involving a combination of equipment from more than one vendor. If a distant site is having trouble connecting to the K-20 MCU, ask the support people to call one of the loop back numbers and view their diagnostic screens to see what video and audio protocols are in use. This test will reveal the optimum connection the endpoint is able to negotiate with the MCU, and as an example, if the best the endpoint can negotiate is the H.263 video algorithm and the other endpoints are all connecting fine at H.264, that may explain why that individual site is having trouble, depending on the mode the K-20 MCU is in. The solution might be as simple as disconnecting all other endpoints and having the H.263 site connect first, or the MCU scheduling/support team may be able to adjust the conference to accommodate the site that is experiencing problems.

For more information about troubleshooting your specific endpoint equipment, refer to the support section of your vendor’s website, or refer to the troubleshooting section of the documentation you received with your equipment. For additional information about tools and utilities that may help you to evaluate and troubleshoot your local IP network, refer to Appendix D entitled Network Assessment Tools.

11. Network Monitoring, Assessment, and Troubleshooting

11.1 Overview

We often hear people remark that you can’t manage what you can’t measure. There is probably no undertaking where this statement is more relevant than network management, especially from the network monitoring and assessment perspectives. Without an understanding of the level of activity, bottlenecks, and limitations of the local network the administrator is unable to identify and resolve issues impacting IP video conferencing. Perhaps more importantly, proactively monitoring the local network and analyzing results will enable network managers to prevent many problems from reaching the point where they create visible negative impacts on users and will facilitate sound decision-making about network enhancement and scaling.
11.2 Why Use Networking Monitoring/Assessment?

11.2.1 Small Institutions

At first glance, one might assume small institutions don’t need to be concerned about network monitoring or assessment from a video conferencing perspective. Nothing could be further from the truth. Proactive monitoring of a small institution’s network is important partly because limited human resources in the IT department make leveraging technology to assist in network management very important. One advantage for a small institution is that fewer monitoring points may exist than in a larger, more complex network. Also, easily accessed tools can provide assistance for monitoring and assessment of a small institution’s network. For example, the K-20 traffic graphs at http://stats.wa-k20.net/k20cgp/ serve as a good resource to evaluate short and long term data traffic activity into and out of the local network through the K-20 edge router. Also, many free tools are available that may help to support network monitoring/assessment at little or no cost. A list of some of these tools is available at http://www.techrepublic.com/blog/five-apps/five-free-network-monitoring-tools/. The emergence of low-cost PC-based packet management tools such as NetLimiter or Antamedia Bandwidth Manager also facilitate the use of bandwidth management at institutions unable to afford expensive hardware devices. Lastly, network managers are encouraged to leverage embedded features in existing network switches, routers, and security appliances to meet monitoring and analysis needs.

11.2.2 Large Institutions

Large institutions face many of the same challenges as small institutions and may use many of the same resources and approaches as small institutions in meeting those challenges, but these institutions also face greater complexities. Their networks are often comprised of collections of smaller networks under the umbrella of the larger local network environment. Another common challenge is a wide range of priorities, expectations, and needs for various network segments or user groups. Because of these factors, large institutions may require more sophisticated solutions with higher acquisition, licensing, and maintenance costs. Large institutions may have many video endpoints with a variety of configurations and user skill levels and monitoring these devices and their interaction with other network devices on a continuing basis is an important part of ensuring optimum network performance and security.

11.3 Monitoring Scenarios

Network monitoring can be carried out in a number of ways. The approaches listed below may not include all possible network monitoring scenarios for your network, but are intended to give you ideas and stimulate further consideration of possible monitoring activities.
Scenario A: Monitoring the network from a laptop running a desktop video application (such as Polycom PVX) using a personal computer-based network monitoring and analysis tool (such as Wireshark).

This method makes sense when one or more endpoints on a network segment are unable to video conference or use specific H.323 features in calls with endpoints outside the local network. By using a combination of PVX testing and Wireshark tracing and moving the equipment closer to the network core or to external networks, the location of a network issue can be found.

Scenario B: Monitoring the network using a bandwidth management device.

This approach gives network administrators the flexibility to identify specific active applications and/or protocols and manage the resources allocated to each of them. This can be a useful means of ensuring H.323 users have enough bandwidth reserved to ensure good quality conferences while also ensuring other critical applications on the network have enough resources as well.

Scenario C: Monitoring the network using a protocol such as SNMP.

SNMP can be used to monitor many network and client-side devices in networks. The use of the protocol is limited based on the capabilities of the central monitoring device, the type and design of the device being monitored, and the MIBs (Management Information Bases) available for a specific device to be monitored. The MIBs define what variables are available to be monitored on a network device.

The above scenarios are only presented as examples and many other scenarios and techniques are available which may be appropriate in your specific situations.
Appendix A - Glossary

Bandwidth Management – The process of monitoring, prioritizing and reserving network bandwidth based upon the applications in use, the resources available, and the priority of those applications for the institution or institutions operating the network.

CODEC – COmpressor/DECompressor. Hardware and/or software that enables high-bandwidth video and audio signals to be converted into a concentrated digital format that is more easily transmitted and received across limited bandwidth data communications paths.

Default Gateway – A node on a network that serves as an access point to an outside network.

DHCP – Dynamic Host Configuration Protocol is a protocol for automatically assigning IP addresses to hosts joining a network.

DNS – Domain Name System. The Domain Name System (DNS) is a distributed internet directory service. DNS is used mostly to translate between domain names and IP addresses, and to control email delivery. Most internet services rely on DNS to work. If DNS fails or is too slow, web sites cannot be located and email delivery stalls. A DNS Server is a server used to provide this translation function.

Domain Name – The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general.

Endpoint – This term identifies an individual video conferencing system connected to a device on the K-20 network or a network outside of K-20.

E.164 Number - E.164 is an international numbering plan for public telephone systems in which each assigned number contains a country code (CC), a national destination code (NDC), and a subscriber number (SN). There can be up to 15 digits in an E.164 number. The E.164 plan was originally developed by the International Telecommunication Union (ITU).

FTP – File Transfer Protocol. A commonly used method of moving files from one Internet location to another.

Gatekeeper – In H.323 IP telephony, a Gatekeeper is a server that is responsible for network-based services including registration, admission, and status, for which it uses a special protocol called RAS. Gatekeeper functions include address translation, call authorization and bandwidth management.

Gateway – A hardware and/or software implementation that translates between two dissimilar protocols, such as a video conferencing gateway connecting legacy H.320 ISDN endpoints to H.323 IP endpoints. You may encounter the term IP gateway, which refers to an interface between/among IP networks using various protocols such as SIP, H.323, and VoIP or a variety of media types.
G.711 – A protocol supporting 3.4 kHz bandwidth audio transmitted at 48, 56 or 64Kbps. This is narrow-band audio, and sounds like a telephone speakerphone.

G.722 – A protocol supporting 7kHz bandwidth audio transmitted at 48,56 or 64Kbps. This wide-band audio is an ISDN telephony standard with more bandwidth allowing for better quality.

G.722.1 Annex C – This is a new industry standard audio protocol that evolved from Polycom’s Siren14 audio, providing 14Khz high-fidelity wideband audio.

G.728 - 3kHz bandwidth audio transmitted at 16Kbps. This is a relatively new technology with reasonable quality and requires a lower bit rate leaving more bandwidth for video.

H.225 – A call signaling protocol used to set up connections between H.323 endpoints (terminals and gateways), over which the real-time data can be transported. Call signaling involves the exchange of H.225 protocol messages over a reliable call-signaling channel. For example, H.225 protocol messages are carried over TCP in an IP-based H.323 network.

H.320 - A widely used standard for video and audio transmission primarily over ISDN lines.

H.323 - A video compression/ communication standard, H.323 is actually comprised of a suite of protocols with the goal of ensuring the interoperability of IP-based video conferencing endpoints made by a variety of manufacturers.

H.239 – A recommendation published by the ITU-T in July 2003 that is derived from the proprietary Polycom People+Content feature used to send video and content simultaneously during a video conference. Previously, the Polycom version and the similar Tandberg DuoVideo feature were both proprietary and incompatible, but with H.239 as a standard, compatibility between/among systems regarding these features is expected to increase.

H.245 - The ITU-T standard used for the Control Protocol for Multimedia Communication. H.245 is included in the H.225.0 Recommendation. H.245 provides signaling for the proper operation of the H.323 terminal, including capabilities exchange, opening and closing of logical channels together with a full description of these channels, mode preference requests, flow control messages, and general commands and indications.

H.261 – A legacy video coding standard specified by the ITU. It was designed for data rates which are multiples of 64Kbit/s, and is sometimes called p x 64Kbit/s (p is in the range 1-30). These data rates suit ISDN lines, for which this video codec was originally designed.

H.263 - A video coding standard specified by the International Telecommunications Union (ITU) that supports video compression (coding) for video-conferencing and video-telephony applications. H.263 was developed to stream video at bandwidths as low as 20K to 24K bit/sec and was based on the H.261 codec. As a general rule, H.263 requires half the bandwidth to achieve the same video quality as H.261.
H.264 - The ITU-T standard for compression that allows higher quality calls to pass over a lower bandwidth for advanced video coding in generic audiovisual services. H.264 enables videoconferences to connect at half the bandwidth of H.263 and still retain the same quality or it will deliver twice the quality at the same bandwidth as H.263, up to a rate of about 512Kbps. H.264 was specified by the Joint Video Team (JVT), a committee made up of Moving Picture Experts Group (MPEG) and International Standards Organization/International Telecommunications Union (ISO/ITU) members. H.264 is also known as MPEG 4 part 10.


IP Address - The unique address of a computer attached to a TCP/IP network. In IPv4, IP addresses are 32 bits long. Each octet is represented in decimal and is separated by dots.

ISDN – Integrated Services Digital Network. Comprised of a set of standards that provide a common architecture for the development and deployment of digitally integrated communications services. Also, a set of standardized customer interfaces and signaling protocols for delivering digital circuit-switched voice/data/video and packet-switched data services.

ITU – Institutional Technical Unit. Human and technical resources supporting the institutions within the K-20 education network. Some ITUs provide video conferencing support, while others are focused on data support. In some cases, an ITU may provide support for both data and video. There are ITUs for the four-year and two-year colleges and universities, as well as the K-12 institutions.

Jitter – The result of a change in latency or the tendency towards lack of synchronization caused by mechanical or electrical changes within the network. Technically, jitter is the phase shift of digital pulses over a transmission medium.

LAN – Local Area Network. A network of computers in a confined area, such as a room, building, or campus. Typically LANs operate at what is considered to be a high bandwidth speed, often in the 100Mbps to 1Gbps range. (See WAN)

Latency - A measure of accumulated delay, representing the length of time required for information to pass through a network end-to-end.

MCU – Multipoint Control Unit. A network device that negotiates and manages video conferencing events involving more than one video conferencing endpoint. MCUs also often provide additional services, including gateway features to allow IP and ISDN endpoints to connect to one another, the ability to connect endpoints that are operating at various calling speeds, as well as support for other features, such as content sharing.

NAT – Network Address Translation. NAT masks the internal IP addresses being used in a LAN from the external network. A NAT server running on a gateway maintains a translation table that maps all internal IP addresses
in outbound requests to its own address and converts all inbound requests to the correct internal host.

Packet Loss – The discarding of data packets in a network due to degraded circuit quality and/or an overloaded device that cannot accept any incoming data at a given moment.

Quality of Service – The ability to define a level of performance in a data communications system. For example, some networks specify modes of service that ensure optimum performance for traffic such as real-time voice and video.

RAS – A protocol for Registration, Admission and Status. In an H.323 audio or video system, the RAS is a control channel over which H.225.0 signaling messages are sent.

RTCP – Real-Time Control Protocol is the control Protocol that works in conjunction with RTP. RTCP control packets are periodically transmitted by each participant in an RTP session to all other participants. Feedback of information to the application can be used to control performance and for diagnostic purposes.

RTP – Real-Time Protocol provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (See RTCP) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers.

Router – An OSI model Layer 3 device that finds the best route between any two networks, even if there are several networks to traverse. Like bridges, remote sites can be connected using routers over dedicated or switched lines to create WANs.

RITU – Regional Institutional Technical Unit. Human and technical resources located at the Educational Service Districts, providing K-20 data and video conferencing support to K-12 institutions in each ESD’s region.

TCP/IP – Transport Control Protocol/Internet Protocol. A protocol suite that can be used to transfer data on the Internet and other packet based networks.

Telnet - A terminal emulation protocol commonly used on the Internet and TCP/IP-based networks. It allows a user at a terminal or PC to log onto a remote computer and run one or more programs. Telnet was originally developed for ARPAnet and is an inherent part of the TCP/IP communications protocol.

UDP – User Datagram protocol. One of the protocols for data transfer that is part of the TCP/IP suite of protocols. UDP is a "stateless" protocol in that UDP makes no provision for acknowledgement of packets received.

UTP – Unshielded Twisted Pair. This is a commonly used type of cable that is composed of two unshielded wires twisted around each other. Due to its
low cost, UTP cabling is used extensively for local area network and telephone applications.

ViDeNet – ViDeNet is a project of ViDe, the Video Development Initiative, exploring issues associated with globally scalable video and voice over IP. ViDeNet is a test bed, where dialing plans, directory services, authentication, network management, measurement and related issues can be explored. ViDeNet is also a community of people, the zone administrators themselves, who share experiences, conduct tests, and ask questions about multimedia conferencing issues. K-20 subscribes to the ViDeNet gatekeeper hierarchy and dialing plan for IP-based video calls, and K-20 IP endpoints, MCUs, and gatekeepers can operate within the K-20 ViDeNet zone.

VITU – Video Institutional Technical Unit. Human and technical resources located at the Educational Service Districts, providing K-20 video conferencing support to K-12 institutions in each ESD’s region. This support includes helpdesk, problem isolation, and resolution of video endpoint problems, as well as technical and operational training for regional K-12 districts.

WAN – Wide Area Network. A geographically dispersed network that connects two or more local area networks (See LAN).

WINS – Windows Internet Naming Service. A system that determines the IP address associated with a particular network computer. This is called name resolution. WINS supports network client and server computers running Windows and can provide name resolution for other computers with special arrangements. WINS uses a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one.
Appendix B – Gatekeeper Peering

Peering is the process of creating a logical connection between your gatekeeper and the K-20 Gatekeeper that allows the two H.323 networks to talk to each other. You would only peer if you are the full administrator of your H.323 zone, which includes your gatekeeper and any endpoints that are registered to it. This logical connection allows endpoints in your zone to connect with endpoints in the K-20 zone, as well as any other zone the K20 Gatekeeper is peered with.

If you are the administrator of a gatekeeper within the WA-K20 zone, you can peer your equipment to the K20 Gatekeeper. This will allow you to register your endpoints directly to your gatekeeper, but still have access to K20 resources such as the MCU. You will also be connected to VideNet allowing you to call out to any VideNet endpoint using their GDS Extension.

To begin the process of peering your gatekeeper, you must send an email to video-eng@wa-k20.net with the following information:

- Contact Information (Name, Email, Phone Number)
- Name of your Organization
- Gatekeeper IP Address and Port
- Gatekeeper Manufacturer and Model

You will then receive an email reply with the following information:

- K20 Gatekeeper IP Address and Port
- Your Gatekeeper’s New 3-Digit Prefix

With this information you will be able to configure your gatekeeper to peer or “neighbor” with the K20 Gatekeeper. Once this peering process is complete, you will be able to dial other K20 endpoints using their H.323 extension or any VideNet endpoint using their GDS Extension.

If you do not know how to configure your gatekeeper using the information you received in the email, you will need to contact your equipment’s manufacturer for technical assistance. If you are using a GNU GK gatekeeper, K-20 engineering can assist by providing an example configuration file for you to view.

After registering your institutional gatekeeper with the K20 Gatekeeper, other sites in both VideNet and in the K20 network will be able to dial your endpoints via H.323. VideNet sites will call you by dialing:

0011479 + Your 3-Digit Prefix + Your Endpoint’s extension

Alternatively, K20 sites will be able to call you using:

Your 3-Digit Prefix + Your Endpoint’s extension

When passing a call through to your system, the K20 Gatekeeper will pass the entire H.323 extension that was dialed by the calling endpoint. Therefore, your equipment will need to be able to handle both of the numbering plans listed
above. Endpoint setup procedures will be like those outlined in section 8.1, except that the last seven digits of your endpoint numbers will be assigned to your endpoints by you, the administrator for your respective zone.
Appendix C – Firewall Configuration

General Information
The information in this section is intended to assist technical support personnel with successfully configuring institutional firewalls to facilitate the traversal of IP video traffic. This appendix focuses primarily on the Cisco PIX/ASA firewalls and Polycom endpoints as examples. You are encouraged to use this information along with the support of your network administrator and regional video/data ITUs to configure your local environment to meet your specific needs.

Recommended Ports for Access to Video Conferencing Endpoints
Modern stateful firewalls are designed to block all incoming connections, while allowing outbound connections (that begin on the inside, protected network) and related return traffic. This means, in most cases, you will only need to open the ports listed below to inbound traffic. The exception would be if you've blocked all or most outbound ports too, then you would need to open these ports to both inbound and outbound traffic (bi-directionally). Please note that we are referring to destination ports, typically source ports are left as "any". A comprehensive list of ports is available at the end of this appendix.

TCP - Destination Ports
1503 Whiteboard, File Sharing
1720 Call setup
1731 Audio call control
3230-3235 RTCP - H.245 call control

UDP - Destination Ports
1718 & 1719 RAS - Gatekeeper
3230-3253 RTP - Audio & Video Streams

Optional Ports
3603 TCP Polycom ViaVideo web interface only
389 TCP Global Directory (LDAP – for Polycom GMS)
80 TCP HTTP - If managed outside of firewall
20/21 TCP FTP - If managed outside of firewall
23 TCP Telnet - If managed outside of firewall

Note: Be sure your endpoints are correctly configured to use these ports.
**Cisco PIX:**

The recommended software version for these firewalls is 6.3(5) or higher. These software versions appear to work well with both newer and older H.323 IP-capable endpoints and their "H.323 fixup" commands handle the newer H.323 versions. If you choose not to upgrade and continue using software version 6.3(3) or earlier, you will need to disable the older "H.323 fixup" commands before using newer VSX series Polycom endpoints, as packet inspection will fail when control messages are spread across multiple packets in accordance with H.323 version 4. On earlier software versions, the "H.323 fixup" commands do not support H.323 Version 3 or Version 4 which is used by newer IP endpoints. Another important note is that the small PIX 501 is unable to support software versions higher than 6.3(5).

**Cisco ASA:**

Software version 8.0 for these devices had a number of issues and some of them could have a negative impact on H.323 activity. One such issue is that H.323 inspection fails when multiple TPKT messages existing within a single packet, which can cause the packet to be rejected by the firewall. Feedback from the K-20 user community suggests upgrading to OS version 8.21 or higher will alleviate this and possibly other H.323-related issues as well.

**CISCO ASA and Codian Issue:**

Recently, some institutions have been unable to connect to the Codian MCUs when they attempt it for the first time. While there are multiple possible causes for this symptom, many institutions with ASA security devices have resolved this issue by removing the H.323 inspect lines from their ASA configurations. The lines that need to be removed are as follows:

```
inspect h323 h225
inspect h323 ras
```

Please contact your local network administrator or regional ITU for assistance with checking and updating your firewall configuration.

**Cisco PIX and ASA:**

If your institution has multiple video conference units and/or locations on different subnets (for portable systems) using a "network group" will allow you to apply rules to all your units or locations into one group. Similarly, using TCP and UDP "service groups" allows you to combine the destination ports into two groups. This allows you to set access to all your endpoints in just two access statements or rules, making additions and changes much simpler. See the Reference Links below for further information.

On the Internet there is some discussion about the need to increase the length of timeouts for H.323 connections on the PIX/ASA firewalls. There is some confusion that these timeouts affect how long a connection can last with some recommending setting the timeout for all day or 10 hours. In fact, all timeouts on the PIX/ASA are IDLE timeouts and close the connection only after there has been no traffic for the time period entered.
The Two Hour Polycom Endpoint Timeout Issue:

Per H.323, TCP 1720 is used for initial call setup and call clearing (H.225) with no further exchange necessary during the call (with the rare exception for call forwarding etc.). TCP 1720 is used again at the completion of a call, when sending H.225 "Release Complete". The issue we find during lengthy H.323 calls is that firewalls interpret the idle TCP 1720 connection as inactive and will close the connection. It is typical firewall protocol to "clean up and close down" inactive ports in order to help maintain a higher level of security. A closed TCP 1720 port can have an adverse affect on an H.323 call and will typically result in a premature disconnection.

In order to avoid TCP 1720 from closing, the Polycom endpoints all send a keep-alive packet at approximately 2 hours by default. The keep-alive is a TCP ACK message with a decremented sequence number to TCP 1720 and is initiated by the calling endpoint. A closed TCP 1720 port on a firewall will cause an ICMP port unreachable response to the TCP ACK message. If a response to the keep-alive is not received, the calling endpoint will assume the far-end is in trouble and terminate the call prematurely. This TCP keep-alive method is per RFC 1122 Sec.4.2.3.6.

A simultaneous packet trace (WireShark/Ethereal) taken on both sides of the firewall should show the reason for premature disconnect. If it is determined that the firewall has closed TCP 1720 prematurely, configure the firewall timeout for a value greater than 2 hours to allow the TCP keep-alive method (RFC 1122 Sec. 4.2.3.6) to function appropriately. If a longer timeout value is not acceptable as a global setting, explore the possibility of applying a longer timeout value to H.323 application inspection (if available) or specifically to TCP port 1720 or if the HDX has a H.225 timeout setting change that to a number that is very small so that it will keep the TCP connection alive or to something very large so that the message never gets sent.

Tandberg’s Approach to the Endpoint Timeout Issue:

Tandberg uses a different approach. Every 30 seconds of a call, their endpoints send a Round Trip Delay over the H.245 channel. This serves multiple purposes, among them are keeping the port open through a firewall and verifying that the far end connection is still alive.

Other Possible Options:

Extend the ‘Time To Live’ setting on the firewall for the related ports/protocols.

Review firewall and endpoint software versions and associated release notes for other possible solutions or workarounds.

The latest versions of Polycom endpoint software have adjustable keep alive settings: VSX v9.0.6.1 and HDX v3.0 are the software platforms that will support this adjustable keep alive interval. Basically, what we’ve done is add the ability to adjust the TCP keep-alive timing from the default of 2 hours. The setting is implemented via a telnet session to the VSX and HDX after the supported build has been installed. The values allowed for adjustment are between 900s (15 minutes) and 9000s (2.5 hours) using the following API command:

-telnet into your device-
Example:
telnet 192.168.1.23
telnet (ip address of codec)
-then change the keep alive interval-
tcp kaInterval (value)
Example:
tcp kaInterval 1800
A keep-alive packet will be sent per 1800 seconds (30 minutes).
The default value is 7200 seconds (2 hours) on VSX. We are changing the
default value on HDX in v3.0 to 1800 seconds (30 minutes).

**Other Suggestions for Cisco Firewalls:**

Sample configurations and PDM screen shots will be available on the new K-20
web site in the future.

**Note: Always make a backup copy of the firewall configuration before
attempting any changes**

Verify you are not running NAT on a device other than the firewall. All NAT must
be configured on the PIX/ASA.

Confirm that your video endpoint is set to use the ports at the beginning of this
appendix.

Note: Over time, Polycom has moved their RAS registration from TCP ports 1718
and 1719 to UDP 1718 and 1719 – you may have to adjust your port
assignments depending on the device and software version you are configuring
for.

**Reference Links:**

Cisco PIX documentation

Cisco ASA documentation

**SonicWALL:**

Some K-20 users have reported major issues with configuring SonicWALL
firewalls for H.323 IP video conferencing and have chosen to bypass the
SonicWALL for video conferencing applications. SonicWALL reports that their new
software releases may mitigate this issue, but there is not enough information
from K-20 users at this point to verify. Please consult your network administrator
or Regional data/video ITUs regarding video traversal across these firewalls.
Placing Video Systems Outside the Firewall:

In some cases, network limitations or specific user needs may require an institution to place their IP video conferencing system or systems on a network segment outside the local firewall, thereby bypassing the firewall security features. In these instances, there are several steps that can be taken to limit the vulnerability of IP video conferencing equipment to hacking or other malicious activity. First of all, placing an administrative password on the system that includes upper and lowercase letters, numbers, and at least one special character will help to prevent unauthorized access to the system configuration. Secondly, disabling FTP, SNMP, and Telnet in the remote access configuration settings will help prevent malicious intrusion as well. Finally, regular monitoring of such systems either over the web or at the system location will help you to spot unusual symptoms such as unscheduled calling that may be indicative of malicious activity from an external source.

Vendor Firewall Traversal Solutions:

Firewall traversal solutions by various vendors have become available in recent years. These solutions generally use a device called a session border controller or other appliance to facilitate the passage of H.323 traffic across local network border devices. One of the limitations of these products is that they tend to work best with a specific vendor's own product line and less well or not at all with other endpoints. Implementation of these solutions may also considerably increase network infrastructure costs. A new protocol called H.460 has emerged recently, and the adoption and implementation of this standard may result in true cross-vendor compatibility for firewall traversal solutions in the future. H.460 utilizes both a session border controller and software at the endpoints to facilitate firewall traversal, and the major vendors have either already upgraded software for their newer endpoints to make them H.460-compliant or have plans to implement the needed software upgrades in the near future. For IP endpoints that are not H.460-compliant, the vendors plan to provide solutions that allow a local gatekeeper inside the institutional firewall to coordinate with the session border controller on the outside. The technology continues to mature, but the fact that a standards-based firewall traversal solution is evolving and beginning to be supported by the major vendors in their latest hardware and software releases may lead to the improved stability and quality of H.323 IP video across firewalls and among institutions in many instances.

Comprehensive Firewall Port Listing:

The ports listed in Table 1 of Section 5.6 are based on a basic configuration for video conferencing over IP networks. Below is a comprehensive list of port usages, using the Polycom VSX endpoint product line as an example. Some of these ports may not be used in your configuration, and are listed here purely for informational purposes.
### Table 1: H.323 Port Usage

<table>
<thead>
<tr>
<th>Port Number:</th>
<th>Purpose:</th>
</tr>
</thead>
<tbody>
<tr>
<td>80-Static</td>
<td>TCP HTTP interface (optional)</td>
</tr>
<tr>
<td>389-Static</td>
<td>TCP ILS registration (LDAP - optional)</td>
</tr>
<tr>
<td>1503-Static</td>
<td>TCP T.120</td>
</tr>
<tr>
<td>1718-Static</td>
<td>TCP Gatekeeper discovery</td>
</tr>
<tr>
<td>1719-Static</td>
<td>TCP Gatekeeper RAS</td>
</tr>
<tr>
<td>1720-Static</td>
<td>TCP H.323 call setup</td>
</tr>
<tr>
<td>1731-Static</td>
<td>TCP audio call control</td>
</tr>
<tr>
<td>8080-Static</td>
<td>TCP HTTP server push</td>
</tr>
</tbody>
</table>

### Table 2: Ports for H.323 Audio/Video (bidirectional)

<table>
<thead>
<tr>
<th>Port Number:</th>
<th>Purpose:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024-65535 Dynamic</td>
<td>TCP H.245</td>
</tr>
<tr>
<td>1024-65535 Dynamic</td>
<td>UDP – RTP (Video data)</td>
</tr>
<tr>
<td>1024-65535 Dynamic</td>
<td>UDP – RTP (Audio data)</td>
</tr>
<tr>
<td>1024-65535 Dynamic</td>
<td>UDP – RTCP</td>
</tr>
</tbody>
</table>

Note: The ports listed in Table 3 can be set to fixed ranges on many Polycom video conferencing systems.

### Table 3: Fixed Port Assignments for Polycom Products

<table>
<thead>
<tr>
<th>Port Number:</th>
<th>Purpose:</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP: 3230-3235</td>
<td>H.245</td>
</tr>
<tr>
<td>UDP: 3230-3253</td>
<td>Audio/Video RTP and RTCP</td>
</tr>
</tbody>
</table>
### Table 4: Global Management System Port Usage

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Purpose:</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>FTP - Software upgrades and provisioning for endpoints</td>
</tr>
<tr>
<td>24</td>
<td>FTP - Telnet trace log</td>
</tr>
<tr>
<td>80</td>
<td>HTTP – Pulling endpoint system information</td>
</tr>
<tr>
<td>80</td>
<td>HTTP – Software upgrades iPower &amp; provisioning iPower</td>
</tr>
<tr>
<td>3601</td>
<td>Proprietary Data Traffic – GAB data</td>
</tr>
<tr>
<td>3603</td>
<td>TCP – Pulling ViaVideo Info</td>
</tr>
<tr>
<td>389</td>
<td>LDAP and ILS</td>
</tr>
<tr>
<td>1002</td>
<td>ILS</td>
</tr>
</tbody>
</table>

### Table 5: Other Ports Used by VSX Systems

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Purpose:</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>FTP – Software Upgrades and GMS provisioning</td>
</tr>
<tr>
<td>23</td>
<td>Telnet – for diagnostics</td>
</tr>
<tr>
<td>24</td>
<td>FTP – API control</td>
</tr>
</tbody>
</table>
Appendix D - Network Assessment Tools

There are many different features, tools, and applications you may find useful when troubleshooting, evaluating, and monitoring the activity of both your IP-based video conferencing endpoints and your network connectivity. What follows are a few examples of tools that are either present on video conferencing endpoints and PCs, or easily available to aid you in your IP video training, monitoring and troubleshooting efforts:

Section 1 - Using Endpoint Diagnostics

Modern video conferencing endpoints have built-in diagnostics that can help identify the presence of errors on a video connection or variations in call configurations that may provide clues to endpoint or network problems. An example Advanced Network Statistics screen is shown in Figure 4. For more information, refer to the Video Network Statistics or Diagnostics section of your endpoint's administrator's guide or user's manual.

Figure 4

Section 2 - Using the PING and Trace Route Utilities

For latency (delay) evaluation in round trip testing, the "PING" utility included with all TCP/IP enabled PCs and workstations can be used. PING uses the Internet Control Message Protocol, so ICMP must be enabled on network devices in order to use this utility. With "PING" a user can set the packet size and determine transit times to other nodes. Adjusting the "PING" packet size from 480 bytes to 640 to 880 to 1024 to 1280 to 1472 will generate packet sizes similar to those used in the video and audio data streams. Because H.323 video packets are usually larger than audio packets, differences in latency between packets of different sizes can cause trouble for IP-based video conferencing, and may point to packet prioritization configuration issues in network equipment. To determine latency by network "hop" (i.e. network segment), a simple method using Trace Route, represented by the command "TRACERT", is often utilized. Trace Route is another commonly used TCP/IP application. This tool outputs the number of network segments encountered en route to the target endpoint. Each network segment is identified by the name of the IP Gateway/Router that was involved in the packet forwarding process,
displaying the latency encountered to reach each segment all the way to the destination. Running this tool several times along the same path will give the average latency encountered when traversing the interim network segments. For more information about using the PING and TRACERT utilities, go to http://help.expedient.com/general/ping_traceroute.shtml or talk to your network administrator.

Many newer video conferencing systems have limited support for “PING” and “TRACERT” built-in. Figure 5 shows how a “PING” command can be issued through a Polycom VSX endpoint’s network diagnostics menu.

Figure 5

The results of the ping will be displayed as shown in Figure 6:

Figure 6

Figure 7 shows the Trace Route feature as accessed through a VSX7000 endpoint’s network diagnostics menu.
Section 3 - Using Telnet

A Telnet session can be initiated to supply a log of video conferencing endpoint activity. The log shows basic information about an endpoint and can record information regarding errors encountered by the internal codec and other details that may be difficult to obtain from the standard diagnostic screens. This log also provides information that can be analyzed by vendor support and engineering teams in order to resolve difficult endpoint or network problems. One point to remember is that if you have disabled Telnet on your endpoint for security reasons, you may need to enable it in order to capture Telnet traces from the device. Figure 8 shows an example of the beginning of a Telnet trace for a Polycom VSX7000.

Telnet traces also contain other useful information, such as communication between an endpoint and the gatekeeper it is registered to, as shown in Figure 9 below.
For more information about using Telnet to evaluate video conferencing endpoint status, go to www.polycom.com and select Support from the menu at the top of the page. Conducting a search for ‘Telnet’ will bring up a number of articles about this topic.

Section 4 - The ntop Application

The ntop application is an open-source network traffic probe that provides information about network usage. It has the ability to sort traffic according to a long list of protocols, display network traffic statistics, identify source/destination entities, and analyze IP traffic. The group that developed NTOP recently released an updated version called ntopng. For more information about ntop, go to http://www.ntop.org/.

Section 5 - The Iperf Application

Iperf is an open-source tool used to measure maximum TCP bandwidth through a network. Iperf reports bandwidth, delay jitter, and datagram loss, and allows various parameters and UDP characteristics to be tuned. You can learn more and obtain instructions for downloading Iperf at http://kb.pert.geant.net/PERTKB/IperfTool.

Section 6 - The Wireshark Protocol Analyzer

Wireshark is a network protocol analyzer for UNIX and Windows that is open-source software and has many features including the ability to capture all the components of an IP-based H.323 call “off the wire” while it is taking place. Wireshark is an upgraded version of a very popular application that used to be called Ethereal. This tool can be useful for both close examination of IP video based calls and for training individuals or groups on the components of the H.323 suite and how they relate to each other. For more information about Wireshark and/or to download the required components, go to www.wireshark.org.
### Appendix E – IP Video Conferencing Implementation Checklist

<table>
<thead>
<tr>
<th>Activity:</th>
<th>Document Reference:</th>
<th>Completed:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meet regularly with IT, administrative, educational, and ITU staff</td>
<td>Section 5.1</td>
<td></td>
</tr>
<tr>
<td>Estimate bandwidth requirements</td>
<td>Section 5.3</td>
<td></td>
</tr>
<tr>
<td>Evaluate and prepare local network for IP video</td>
<td>Sections 5.4, 5.5, and 5.8</td>
<td></td>
</tr>
<tr>
<td>Review and optimize firewall/NAT settings for IP video</td>
<td>Sections 5.6 and 5.7</td>
<td></td>
</tr>
<tr>
<td>Assess endpoint needs and acquire new equipment</td>
<td>Section 7</td>
<td></td>
</tr>
<tr>
<td>Install and configure new IP video equipment</td>
<td>Section 8</td>
<td></td>
</tr>
<tr>
<td>Obtain IP endpoint number assignments from K-20</td>
<td>Sections 6 and 6.1</td>
<td></td>
</tr>
<tr>
<td>Register IP endpoints with the gatekeeper</td>
<td>Sections 6 and 6.1</td>
<td></td>
</tr>
<tr>
<td>Test IP video connectivity</td>
<td>Sections 10, and 11</td>
<td></td>
</tr>
<tr>
<td>Optimize IP video connection quality</td>
<td>Sections 9 and 11</td>
<td></td>
</tr>
<tr>
<td>Monitor and evaluate IP video network performance</td>
<td>Sections 5.3, 9 and 11</td>
<td></td>
</tr>
</tbody>
</table>

Note: This checklist may need to be customized to meet specific sector and/or institutional needs.
Appendix F – List of NTSC Video Working Group Members

Jeff Andrews – ESD 112
Tony Brownell – OSPI
Randy Cross – Washington State University
Don Laurance – ESD113
Carrie Sherman – ESD113
Edson Rodriguez – ESD189
Noah Pitzer – University of Washington
Peter Savin – State Board for Community and Technical Colleges
Cliff Smelser – ESD101
Michael Evans – K-20 Program Office