

# An Introduction to Videoconferencing and Distance Learning

*Chris McCuller*

*Valdosta State University*

[chris.mcculler@gmail.com](mailto:chris.mcculler@gmail.com)

# **1. Introduction**

Distance Learning is a relatively new educational field that focuses on delivering classroom content/instruction to students who are not physically on site. Instead, teachers and students communicate either asynchronously (at a time of their own choosing via email or other text-based communication), or using technology that allows them to communicate in real-time (synchronously).

## **1.1 Current Methods**

Web-based classes are the most prevalent method of delivering distance classes today. These classes utilize various applications of the Internet (instant messaging, email, file upload/download, message boards, etc.) to distribute classroom materials and help students and teachers interact with one another. Commonly, specialized software packages that provide easy access to these functions are used to facilitate these classes. In some cases, students may connect to a live video feed of a live classroom streamed over the Internet. In these cases, a technology assistant is usually provided to provide interaction between the distance students and the instructor and on-site students.

## **1.2 Future Needs**

The advent of Web 2.0 brought dynamic content, easy syndication of content, and rich interactive experiences, along with raised expectations of distance learning classes. Both educators and students are asking for more interaction in the virtual classroom. The classroom is an active place, and live, real-time communications are needed to augment or replace the current standard of text-based, non-interactive classes.

## **1.3 Video Conferencing: Bridging the Gap**

With the explosion of bandwidth after the Dot-Com era, the resources are now available to provide more interaction in the virtual classroom via video conferencing. Using the various technologies available for video conferencing, educators can provide a more interactive distance learning experience by delivering real-time, bi-directional video, voice, and data communications to their distance students, rather than just the standard electronic media.

## 2. Technology

### 2.1 Communications Standards

Popular Communications Standards. For the purposes of this document, we will be focusing on H.323.

	<b>H.320</b>	<b>H.321</b>	<b>H.322</b>	<b>H.323 V1/V2</b>	<b>H.324</b>
<b>Approval Date</b>	1990	1995	1995	1996/1998	1996
<b>Network</b>	Narrowband switched digital ISDN	Broadband ISDN ATM LAN	Guaranteed bandwidth packet switched networks	Non-guaranteed bandwidth packet switched networks, (Ethernet)	PSTN or POTS, the analog phone system
<b>Video</b>	H.261 H.263 H.264	H.261 H.263	H.261 H.263	H.261 H.263 H.264	H.261 H.263
<b>Audio</b>	G.711 G.722 G.722.1 G.728	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.722.1 G.723 G.728 G.729 A/B	G.723
<b>Multiplexing</b>	H.221	H.221	H.221	H.225.0	H.223
<b>Control</b>	H.230 H.242	H.242	H.242 H.230	H.245	H.245
<b>Multipoint</b>	H.231 H.243	H.231 H.243	H.231 H.243	H.323	
<b>Data</b>	T.120	T.120	T.120	T.120	T.120
<b>Comm. Interface</b>	I.400	AAL I.363 AJM I.361 PHY I.400	I.400 & TCP/IP	TCP/IP	V.34 Modem
<b>Text Chat</b>	T.140	T.140	T.140	T.140	T.140
<b>Encryption</b>	H.233 H.234	H.233 H.234		H.235	H.233 H.234

### 2.1.1 The Audio Standards

---

**G.711:** Pulse Code Modulation of voice frequencies (PCM), where 3.1 kHz analogue audio is encoded into a 48, 56 or 64 kbps stream. Used when no other standard is equally supported.

**G.722:** 7 kHz audio encoded into a 48, 56 or 64 kbps stream. Provides high quality, but takes bandwidth.

**G.722.1:** 7 kHz audio encoded at 24 and 32 kbps for hands-free operation in systems with low frame loss.

**G.723:** 3.4 kHz dual rate speech codec for telecommunications at 5.3 kbps & 6.4 kbps.

**G.728:** 3.4 kHz Low Delay Code Excited Linear Prediction (LD-CELP) where 3.4 kHz analogue audio is encoded into a 16 kbps stream. This standard provides good quality results at low bitrates.

**G.729 A/B:** 3.4 kHz speech codec that provides near toll quality audio encoded into an 8 kbps stream using the AS-CELP method. Annex A is a reduced complexity codec and Annex B supports silence suppression and comfort noise generation.

### 2.1.2 The Video Standards

---

**H.261:** Supports 352x288 (CIF or FCIF) and 176x144 (QCIF). DCT-based algorithm tuned for 2B to 6B ISDN communications

**H.263:** Much improved derivative of H.261, tuned for POTS data rates. Mostly aimed at QCIF and Sub-QCIF (128x96 – SQCIF), while providing better video than H.261 on QCIF and CIF.

**H.264:** Joint collaboration between ITU and ISO. Improved video over H.263 providing similar quality at half the bandwidth

### 2.1.3 The Control/Communications Standards

---

**H.221:** defines the transmission frame structure for audiovisual teleservices in channels of 64 to 1920 Kbps; used in H.320.

**H.223:** specifies a packet-orientated multiplexing protocol for low bit rate multimedia communications; Annex A & B handles light and medium error prone channels of the mobile extension as used in 3G-324M.

**H.225:** defines the multiplexing transmission formats for media stream packetisation & synchronisation on a non-guaranteed QoS LAN.

**H.230:** defines frame synchronous control and indication signals for audio visual systems.

**H.242:** defines the control procedures and protocol for establishing communications between audiovisual terminals on digital channels up to 2 Mbps; used by H.320.

**H.243:** defines the control procedures and protocol for establishing communications between three or more audiovisual terminals - H.320 multipoint conferences.

**H.245:** defines the control procedures and protocol for H.323 & H.324 multimedia communications.

## 2.2 Equipment

### 2.2.1 Video Conferencing

---

H.323 is essentially a set of standards that defines how communications between terminals and their respective IP-based networks occur. There are four basic components involved in H.323 communications: the required terminal, and the optional gatekeeper, gateway, and multipoint control unit (MCU). These components provide the majority of the interactivity in the distance classroom.

#### Terminals

An H.323 Terminal is an endpoint on a network which provides for real-time, two-way communications with another H.323 terminal, Gateway or Multipoint Control Unit. A terminal may provide speech only, speech and data, speech and video, or speech, data and video. Examples of terminals include a PC with H.323 software, such as Microsoft Netmeeting or Polycom PVX, a Tandberg 880, or a Polycom VSX7000.

#### Gatekeepers

A Gatekeeper is a very useful, but optional, component of an H.323-enabled network. The gatekeeper provides address translation and controls access to the network resources for H.323 terminals, gateways and MCU's.

An endpoint does register itself at a gatekeeper. All H.323 endpoints registered to a single gatekeeper build an H.323 zone. A gatekeeper provides several services to all endpoints in its zone. These services include:

- Address translation - a gatekeeper translates H.323 aliases into call signaling IP addresses (especially useful for endpoints with dynamic IP addresses). A gatekeeper maintains a database for translation between aliases (such as E.164 addresses) and network addresses.
- Admission and access control of endpoints - this control can be based on bandwidth availability, limitations on the number of simultaneous H.323 calls, or the registration privileges of endpoints.
- Bandwidth management - Network administrators can manage bandwidth by specifying limitations on the number of simultaneous calls and by limiting authorization of specific terminals to place calls at specified times.

- Routing capability - A gatekeeper can route all calls originating or terminating in its zone. Thus, accounting information of calls can be maintained for billing and security purposes. A gatekeeper can re-route a call to an appropriate gateway, based on bandwidth availability. Re-routing can be used to develop advanced services such as mobile addressing, call forwarding, and voice mail diversion.

There are several gatekeepers on the market, including proprietary hardware gatekeepers from Tandberg, Polycom, Cisco, and others, and software based gatekeepers such as GNUGK and DUAL Gatekeeper.

### **Gateway**

A Gateway is an optional component in an H.323-enabled network. When communication is required between different networks (e.g. between an IP-based network and PSTN) a gateway is needed at the interface. A H.323 Gateway is an H.323 endpoint that provides for real-time, two-way communications between terminals belonging to networks with different protocol stacks. For example, it is possible for an H.323 terminal to set up conference with terminals based on H.320 or H.324 through an appropriate gateway. A gateway provides data format translation, control-signaling translation, audio and video codec translation, and call setup and termination functionality on both sides of the network. Depending on the type of network to which translation is required a gateway may support H.310, H.320, H.321, H.322, or H.324 endpoints.

### **Multipoint Control Unit (MCU)**

MCU is an optional component of an H.323-enabled network that controls conferences between 3 or more terminals. It consists of:

- A mandatory *Multipoint Controller (MC)* - used for call signaling and conference control.
- An optional *Multipoint Processor (MP)* - used switching/mixing of media stream, and sometimes real-time trans-coding of the received audio/video streams

Although the MCU is a separate logical unit, it may be combined into a terminal, gateway or gatekeeper.

The MCU is required in a centralized multipoint conference where each terminal establishes a point-to-point connection with the MCU. The MCU determines the capabilities of each terminal and sends each a mixed media stream. In the decentralized model of multipoint conferencing, a MC ensures communication compatibility but the media streams are multicast

and the mixing is performed at each terminal.

### **2.2.2 Support Services**

---

The video conferencing equipment only makes up one part of the distance classroom. Another, important part are the support services that go along with each distance class. Educators need to have a way to efficiently distribute materials and assignments and provide feedback, and students need to have a way to submit assignments and interact with the educator and other students outside of the classroom. The biggest consideration is that of how the students will interact outside the classroom. Mediums for this interaction include web-based chat or message boards, email, or even video calls. Also, how will the students submit assignments to their instructor? Will they email the assignments, or put on some sort of shared server space that they all have access to? This all depends on how the class is setup, along with the infrastructure of the educational institution. Components that would need to be considered here include servers, storage, software, and technical support.

## **2.3 Network Infrastructure**

### **2.3.1 Bandwidth Requirements**

---

Institutions that plan on hosting any type of distance education class will most likely have the necessary bandwidth to serve the classes with minimal issues. A typical connection at a university is anywhere from 10 Mbit to 150 Mbit, depending on the size of the university. Either end of the spectrum is fine, though the amount of bandwidth available will affect the ability to scale classes based on the number of students. As is always true with network bandwidth, the more the merrier.

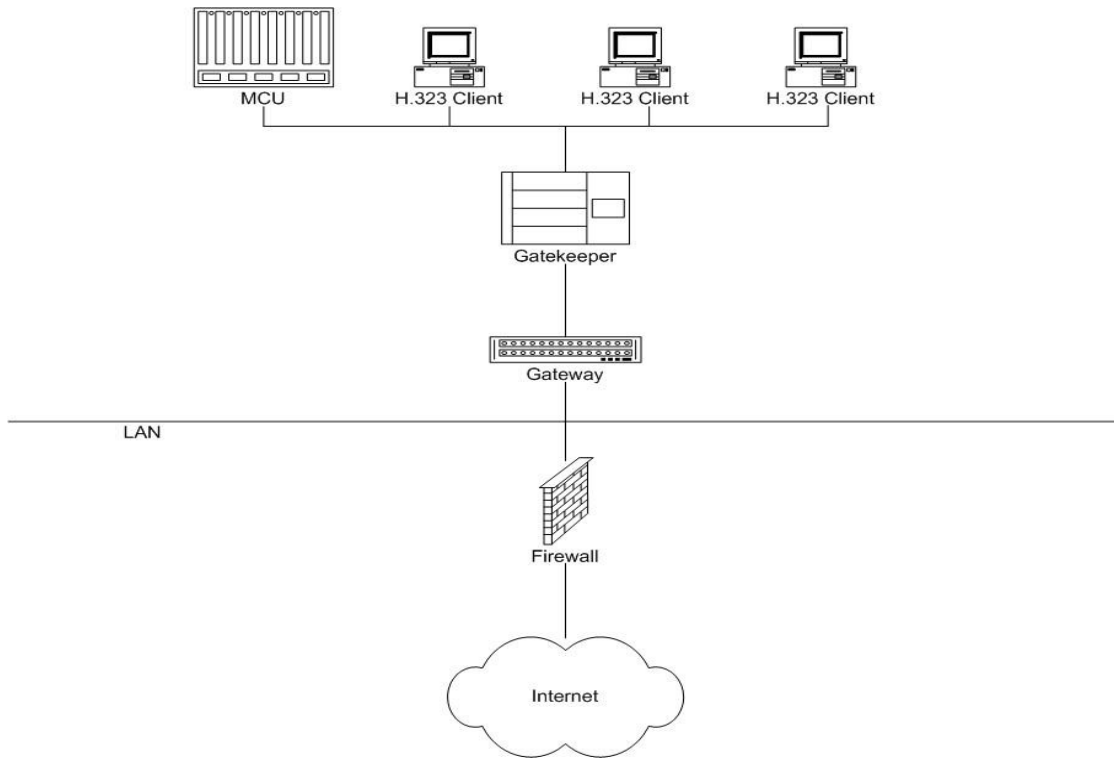
On the remote end, bandwidth is the number one external factor to focus on when dealing with distance education, especially if the class will have any sort of real-time interaction. When using video conferencing for interaction, each remote endpoint needs to have, at a bare minimum, a 256 Kbps download and upload rate. This means that the endpoints must be on a broadband connection of some sort, be it residential broadband (DSL, cable, ISDN), business-level broadband (DSL, cable, ISDN), or enterprise-level leased lines (T1, T3, etc). Specific bandwidth requirements depend on a number of factors which will be addressed later in this paper.

### **2.3.2 Security**

---

With all of the security concerns in today's digital world, nearly every network is protected by a firewall. Firewalls are great for keeping the bad people out, and letting the good people in, but can notoriously be a pain when it comes to multimedia applications. Video conferencing is no different. Things to be considered here include the type of firewall you purchase, the services you plan to offer, and what needs to be done in order to make sure those services are available when they are needed. Typically this involves the IP-addressing scheme of your network and what ports need to be opened on the firewall in order for the services to be accessed when needed.

### 2.3.3 A Sample H.323 Network (Video Conferencing only)



### 3. Technology Considerations

#### ***Network Bandwidth:***

#### **Host Institution:**

The host institution needs as much available bandwidth as possible to ensure the quality and reliability of the video conference. A general rule of thumb for bandwidth at the host institution is:

$$(number\ of\ sites * preferred\ callrate = amount\ of\ needed\ bandwidth)$$

If you wish to have 6 concurrent sites at a 384 kbps callrate, you would need ~2 Mbit of available bandwidth to make sure the call goes smoothly. This isn't 100% true, but it's a good guideline to go by.

#### **Remote Users:**

Bare Minimum:

384 kbps download

384 kbps upload

Recommended

Maximum download available

~1.5 – 3.0 Mbps on residential Cable/DSL connections

Maximum upload available

~512 – 768 kbps on residential Cable/DSL connections

Enterprise LAN connections vary depending on the organization, but typically run from T1/Business Broadband (1.5 Mbps up and down) levels in small-businesses to multiple T1/T3 (~ 3.0+ Mbps up and down) levels in educational institutions.

### **Remote Users Requirements and Considerations**

1. Bandwidth depends on the technology environment:

**a. Home Technology Environment:**

Residential Broadband connection (Cable/DSL)

**b. Enterprise Technology Environment:**

Enterprise Broadband Connection

2. Polycom PVX 8.0.x software

3. Webcam compatible with PVX software (we recommend the Logitech Quickcam Pro 4000 or 5000).

***PC Requirements\*:***

- ~1 GHz Processor (~1.2 GHz for H.264 video where supported)
- 256 MB RAM (512 MB recommended)
- ~100 MB hard drive space (varies with software)
- Windows XP SP1 (varies with software)
- 800x600 16-bit color SVGA display

## **Technology Environments**

### **Home Technology Environment**

*A conferencing environment where the user(s) are located in a residential environment that is not designed and/or optimized for video conferencing, has limited technical support available, and has limited technology resources.*

### ***Pros and Cons of the Home Technology Environment***

Pros:

- Convenient for the user (easier access to equipment)
- No enterprise-level firewall to deal with
- Much simpler network setup
- Easier to troubleshoot network issues off-site.
- Relative ease of solving hardware problems (when in doubt, just buy a new PC)

Cons:

- No trained IT support staff
  - Most users don't have the necessary skills to troubleshoot issues as they arise
- Much less control of the technology environment
  - WAN connection speeds vary depending on the type of connection, the time of day the call is placed (peak hours vs. quiet hours), and other factors out of our control. Peak usage hours typically are 6pm – 11pm Monday-Friday and 12pm – 4pm on weekends
  - Meeting minimum equipment requirements
  - Software issues
    - System Resource/Network Bandwidth Issues

- Spyware/Adware
  - Viruses
  - Antivirus software
  - Pre-installed “junk” or evaluation software
  - Software firewalls
- Update/Patch level of the systems
- Proper configuration of network settings and software used for the call.
- Varying setups of the users LAN and it's components
  - Type of broadband connection (cable, xDSL, ISDN, etc)
  - Type of LAN access
    - Wired (10 Mbps, 100 Mbps, 1000 Mbps)
    - Wireless (A, B, G)
    - Combination
  - Type of router
    - Does it support user configuration and customization?
      - Custom port forwarding
      - Controlling the firewall
      - Ease of configuration
  - Number of routers
    - One primary router (usually the cable/DSL router)
    - Two or more routers
      - Primary router (Internet connection)
      - Secondary router (wireless or wired LAN access)
      - Require MAC cloning? (usually required for cable connections)
  - Addressing issues
    - Most home broadband connections rely on DHCP, although a static IP address can be obtained for a fee (varies depending on the provider)

### ***Common Issues***

- **Download and upload speeds are not synchronous.**

Most home broadband connections have a sufficiently fast download speed to allow for 20-30 fps calls to be delivered with no hassles. The issues arise when trying to upload that same quality of video, which is often times impossible with a standard home-based connection (3.0 Mbps download, 256 kbps upload). 256 kbps (most likely less, as some other applications, and even the router will be using some of that bandwidth for

mandatory communications. The end result is a smooth feed at one site and choppy feed at the other site. The only solutions are:

1. Increase your upload bandwidth (ideal solution).
2. Decrease your outgoing video quality.

Another issue that comes into play is that while providers offer a standard package of 3 Mbps down and 256 kbps up, most users are not getting that speed. A quote from the Wikipedia article on Broadband Internet access:

“In practice, the advertised bandwidth is not always reliably available to the customer; ISPs often allow a greater number of subscribers than their backbone connection can handle, under the assumption that most users will not be using their full connection capacity very frequently. This aggregation strategy works more often than not, so users can typically burst to their full bandwidth most of the time; however, peer-to-peer file sharing systems, often requiring extended durations of high bandwidth, stress these assumptions, and can cause major problems for ISPs who have excessively overbooked their capacity.”

The same can be said of videoconferencing, which requires a steady transmission rate rather than the standard burst transmission rate. The only surefire way to fix this is to provide a dedicated amount of bandwidth to the hardware – i.e. a dedicated line/network for the conference to take place. Unfortunately, this is cost prohibitive, as well as technically challenging, as everyone that wants to do conferencing can't have their own dedicated line.

### ***Enterprise Technology Environment***

*A conferencing environment where the user(s) are located in some sort of enterprise environment (educational, small business, corporate, etc) that is designed and/or optimized with videoconferencing in mind, has trained tech support readily available, and ample technology resources.*

### ***Pros and Cons of the Enterprise Technology Environment***

Pros:

- More control of the technology environment
- Typically higher-end equipment
- Trained IT support staff on hand for troubleshooting

- Better WAN connection speeds
  - Guaranteed bandwidth
  - Typically higher bandwidth, esp. upload speeds

Cons:

- More complex networks
  - More difficult to identify and solve network issues
  - Enterprise-level firewalls
    - As of this presentation, **SONICWall Firewalls WILL NOT work with H.323 or SIP based video conferencing** due to the way some incoming packets are flagged. SONICWall is aware of this issue, but there is no timetable on a resolution.
  - Updated software/firmware for network equipment
    - Many support contracts (which are required to most software/firmware updates) are too expensive for many K-12 systems. Often times technicians are using software that is 1-3 years old, and, as a result aren't getting the full benefit of the hardware.
- Availability/Over-extension of IT support staff
  - Most K-12 school systems employ a single network engineer, who is responsible for all network configuration throughout the system (firewall/router/switch configurations, LAN/WAN connections between sites, etc). Troubleshooting firewall configurations can be problematic due to over-extension of the network engineer.
  - Most K-12 school systems employ a single network admin, with a limited (often one or two full-time staffers) who are responsible for everything the network engineer is not (NOS maintenance, system maintenance and troubleshooting, hardware/software purchases, budgetary concerns, etc).
  - Most K-12 school system IT departments are under-staffed and over-extended.
- Training level of site support staff
  - Many IT support staffers located on-site are teachers/administrators who have some technology experience, but are not trained IT professionals.
  - This is not the fault of the staffer, but a result of budget strains in many school systems. Schools systems have to make due with what's available more often than not.
- Ease of resolution of some issues
  - Committees, paperwork, proper authorization, etc can lead to slow response times for issues that require immediate attention (ie a system upgrade to the local videoconferencing PC or maintenance of the dedicating videoconferencing

system).

## **Common Issues**

- **Firewall Compatibility**

The bandwidth issues of the home technology environment are replaced by network hardware issues in the enterprise technology environment. The most common hardware problems occur with the firewall. There are literally hundreds of firewalls available, and none of them configure the same way. They all, however, support the same basic features. The problem is having someone with enough knowledge to figure out what needs to be done to the firewall in order to make it work for videoconferencing. At VSU, we have a standard set of rules implemented at the firewall for any video conferencing devices. These rules are:

<b><i>Port(s)</i></b>	<b><i>Protocol</i></b>	<b><i>Direction</i></b>	<b><i>Purpose</i></b>
1503	TCP/UDP	In/Out	T.120 Data Sharing
1718-1720	TCP/UDP	In/Out	Q.931 Call Setup
2326-2373	TCP/UDP	In/Out	Video/Audio/Data (Tandberg)
3230-3237	TCP/UDP	In/Out	Video/Audio/Data (Polycom)
5555-5560	TCP/UDP	In/Out	H.245 Call Setup
9940	TCP/UDP	In/Out	iVisit

As long as the software/codec and the firewall on the remote end are configured to use these ports (specifically 1718-1720 and 3230-3235), conferencing should go smoothly. The only hitch is with SONICWall Firewalls, which hasn't been resolved to our knowledge. Newer ITU standards such as H.460.17, H.460.18, and H.460.19, which allow for NAT/firewall traversal may circumvent these issues as well as make using a standardized set of ports irrelevant.

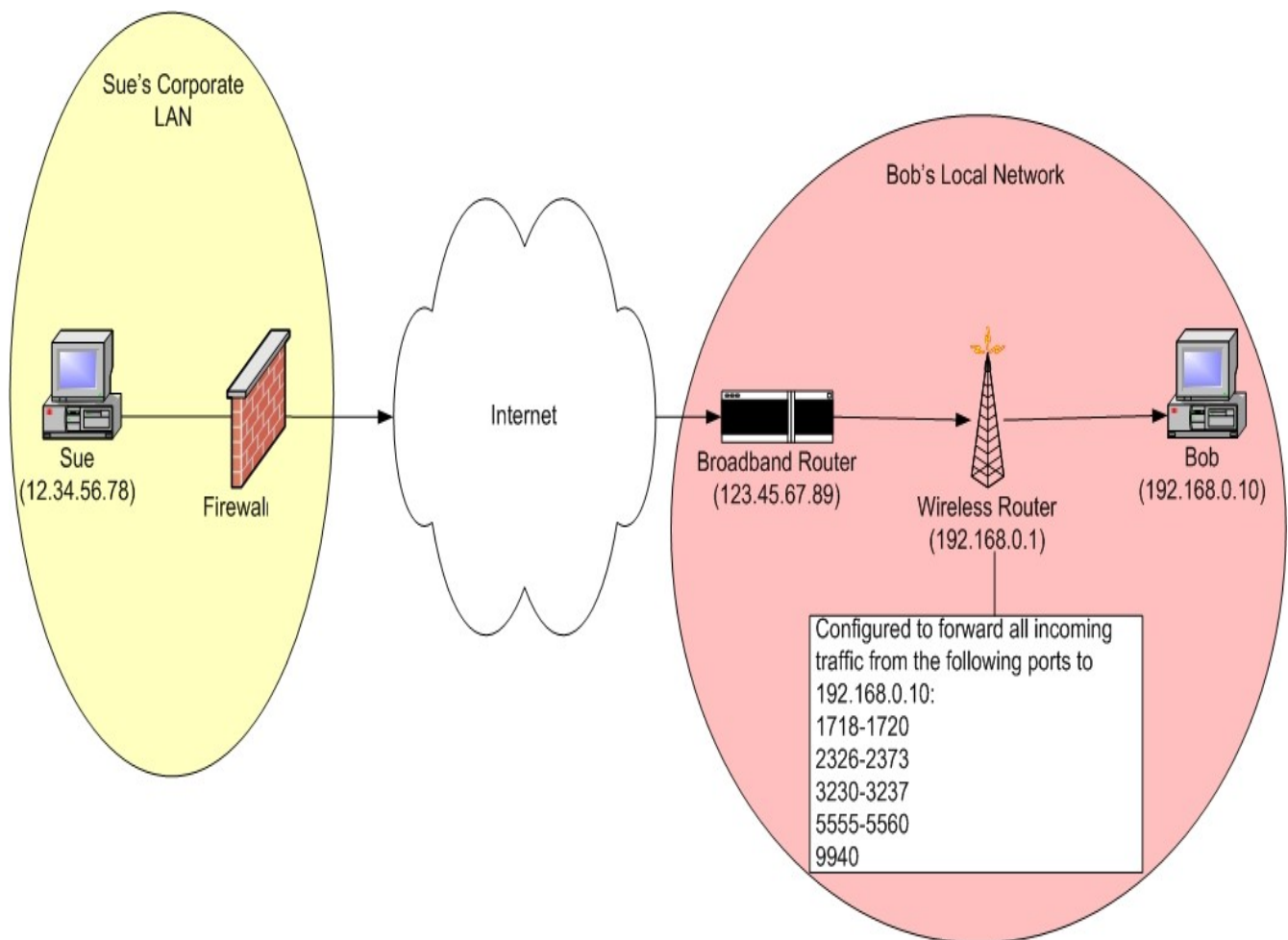
## Direct IP Dialing

### Description:

Direct IP dialing is the simplest form of communications between two H.323 devices. One device simply dials the other devices IP address, and the call is established. There is no need for a Gatekeeper, and no need for a Gateway as long as the devices are on the same kind of network (IP-to-IP, ISDN-to-ISDN, etc).

### How it Works:

Sue wants to call Bob.



1. Sue dials Bob's IP public address (123.45.67.89).
2. Bob sees Sue's incoming call and answers it.
3. The call is established.

## **Considerations:**

### **1. Where are the devices located on their respective networks?**

This is a big consideration when it comes to video conferencing. IP addressing schemes (public vs private) and network security (primarily firewalls) must be addressed before video conferencing can successfully occur.

In this case, Bob was behind a wireless router that handled IP addressing on his local network. Sue had to dial the IP address of Bob's broadband router (123.45.67.89) because his local network address (192.168.0.10) is not accessible to the public internet. Bob had previously enabled port forwarding for the proper ports on his router to his local IP address so he could receive calls.

Sue was located on a corporate LAN protected by a firewall that had been configured to allow video conferencing to her host (which was on public IP address 12.34.56.78).

### **2. What is the connection speed of the respective networks?**

In order for H.323 video conferencing to be reliable, a broadband connection is required. This means a bare minimum download and upload rate of 256 kbps, though slow of a connection over a standard IP network will have major issues with call quality, jitter, and packet loss. Recommended network speeds would be at 1.5 Mbps download, and as much upload as you can get.

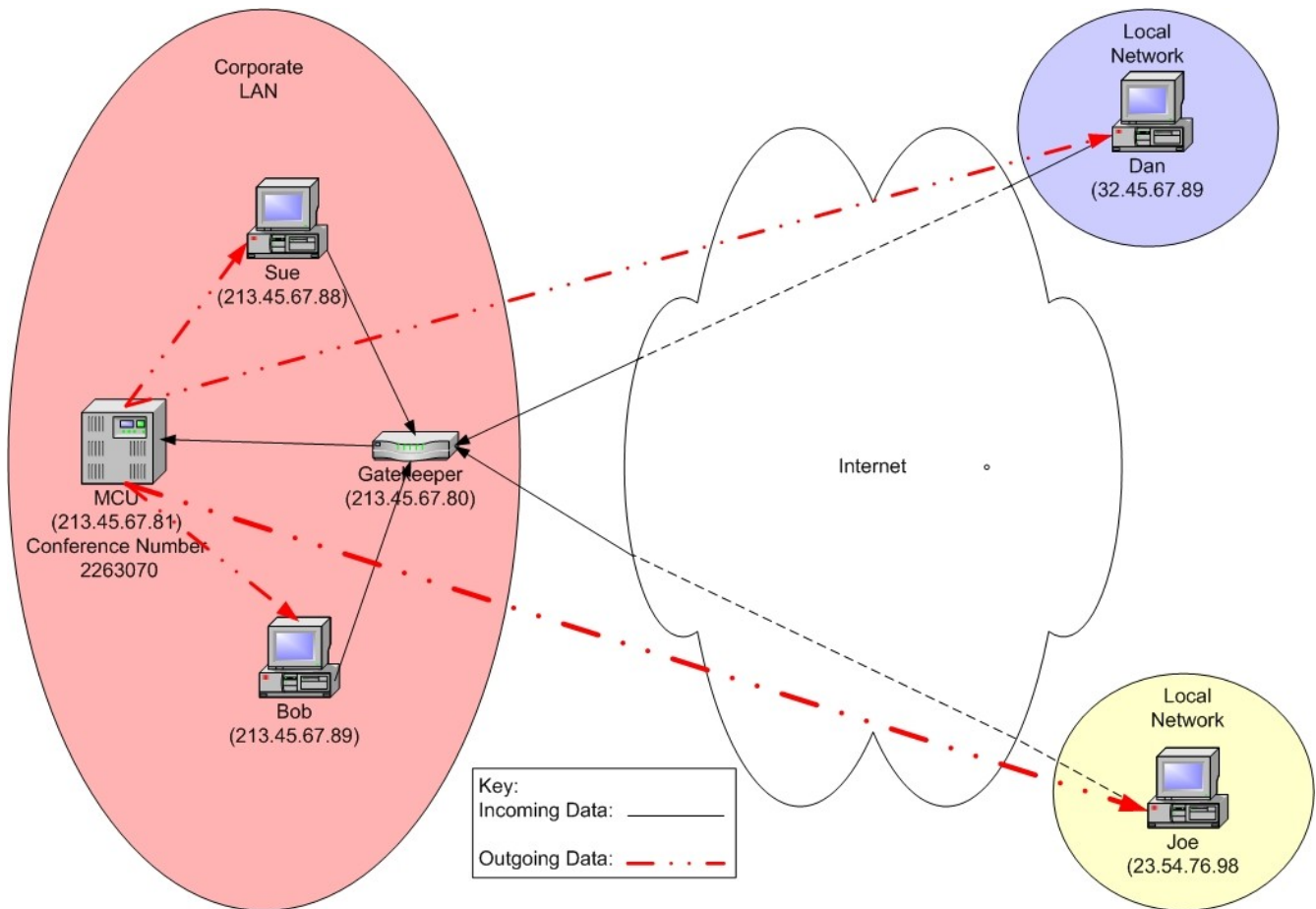
## Routed Dialing

### Description:

This method is more complex than direct IP dialing because it adds at least a Gatekeeper to the mix, if not a Gateway and MCU as well. The Gatekeeper acts like an operator, storing a table with a client's IP address and its corresponding E.164 number. The Gateway, if needed, acts as a translator by helping two different networks communicate with each other. The MCU is like the party host. It hosts all the calls, each identified by their own, unique number.

### How it Works:

Bob, Sue, Joe, and Dan are meeting in a conference call. Please note that ALL units participating in this call MUST be registered to the Gatekeeper before the call can take place.



1. A conference is setup on the MCU with the number 2263070
2. Bob and Sue, both of whom are on the local network with the Gatekeeper and MCU, dial the conference.

3. The Gatekeeper recognizes the number dialed as belonging to the MCU, and that both Bob and Sue are registered endpoints, and routes the calls appropriately.
4. Dan and Joe, who are on their own remote networks, call the conference.
5. The Gatekeeper, recognizing Dan and Joe as a registered endpoints, routes their calls to the MCU.
6. The call is established.

**Considerations:**

Throughout this process, the Gatekeeper is constantly routing calls between the MCU and the three endpoints. The Gatekeeper has a record of each endpoints IP address and it's corresponding E.164 number, and knows where and how to route each message.

1. Things to consider are firewall traversal (static ports vs. dynamic ports).
2. IP addressing scheme (public vs. private), and
3. The E.164 dialing plan for each institution (if one exists).
4. Bandwidth is also a concern as you must have enough available to handle all the calls (number of sites \* preferred callrate = amount of needed bandwidth). So if you wish to have 6 sites at 384 kbps, you would need ~2Mbit of bandwidth (download and upload) to be sure the call would go relatively smoothly.