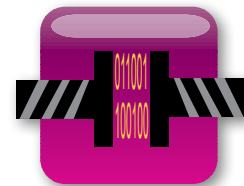


Video Conferencing 101

In the simplest terms, a videoconference happens when audio and video is exchanged between two stations in real time. That sounds pretty easy right? “But what about bitrates, frame rates, ports, codecs, routers, NAT, and standards like H.323, ” you ask. You are right, this is where it gets tricky. All the jargon can be daunting and it is constantly changing; however, when you stick to the four basic concepts, the whole process can easily be understood:



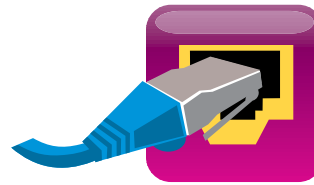
Audio & Video Capture



Data Compression



Communication



Network



Capturing audio and video data

In desktop videoconferencing, video and audio is captured by external devices and streamed into the computer via a USB or AV port. The videoconferencing software is able to obtain these streams and use them.



Compressing the data for transport

Once the software has the digital stream of 0s and 1s that describe the audio and video, it compresses this data using a mathematical process that keeps only the most essential information. This is to make the amount of information that you have to send over the network as small as possible while still maintaining the best quality.

These mathematical gymnastics are referred to as algorithms or codecs. There are standard and proprietary versions of them. Some examples are H.261, H.263, and H.264 for video and G.711, G.723 for audio. Each codec has unique properties and performs best given a certain set of circumstances. Some are best when you need a really small size with marginal quality that is good for sending over slower networks. While others are best when you have a fast network and demand superior audio and video. So no one codec is best for all situations and this is why there are several to choose from.

This process of choosing the best setting for a situation that may be changing all the time is nearly impossible. Therefore, it is important to select a videoconferencing application that can automatically monitor the conditions to provide the best overall quality given the changing network environment.



Communication between two computers

Having a language that the stations understand

Exchanging audio and video over a network requires that the videoconferencing stations speak a common language. H.323 is that “language”. It is the set of rules used to videoconference over an computer network. These standardized rules have been set up so that you can call other H.323 stations regardless of vendor. This is mostly true; however, there are nuances. It is always a good idea to test call a variety of stations early on to make sure that you can connect successfully.

Being able to send these messages to the right location

The second component that is critical to communications is locating the station that you want to connect to. Luckily, this piece of the puzzle is the fundamental foundation of all computer networks. Just like your phone has a unique phone number, each computer device on a network has a unique address made up of a series of four numbers called the “IP Address”. All communications directed to a specific computer are sent to its IP address.

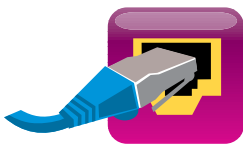
When you consider public, private, static and dynamic IPs, things can get more complicated. However, for the sake of understanding the big picture, simply know that videoconferencing stations talk to other stations by sending messages and data to their IP Address.

Receiving messages and responding

Typically, people understand the idea of having standardized messaging and being able to send messages to a unique address. However, they often get hung up on the idea of receiving the data via specific computer ports. In addition, users tend to get nervous when instructed to configure a router and open ports in the firewall.

You can think of opening ports like you are opening phone lines to your computer. When you open lines to your computer, messages can be sent over them. Videoconferencing applications have “receptionists” that listen on these lines for messages and respond accordingly.

But you ask, “Isn’t this risky? What if the receptionist allows the bad guys in by accident?” This does seem plausible; however, in the world of videoconferencing, this doesn’t happen. The videoconferencing “receptionists” are the only people listening on these ports and they only understand a few phrases. Anything coming over these ports other than these phrases are ignored. This virtually guarantees that only properly formatted data will be processed by the application.



Network path that the data will travel

The network is pretty straightforward. It is the path or highway that the data travels on. As easy a concept as it is to understand, it can be one of the most high-impact and unpredictable pieces of the videoconferencing puzzle. The quality of a videoconference is 100% dependent on data being able to travel from sender to receiver without any loss or delay.

Picture your video and audio being a physical package that you are sending on a truck to a destination. You decide to send the maximum quality, which requires a 10-foot wide truck. If that truck is traveling on a 15ft wide road, everything is fine. However if at some point during the trip, the truck has to pass down a 10-foot wide road. The truck has to slow and squeeze through, causing delay. This would be just fine if the package didn’t have to arrive exactly on time as is the case with email. However, when you are talking about sending questions and answers in a “real-time” conversation, even minimum delay causes clumsy communication and perhaps even misinterpretation.

Through the combination of choosing the right technology to compress the data (codec choice) and the amount of data sent in a stream (video bitrate and frame rate), videoconferencing applications strive to send the perfect amount of data given the network conditions. Be aware that unless you have unlimited bandwidth, you often have to strike a balance between video and audio quality and having all the data arrive on time and intact.