Voice and Video over IP: Concept Guide

This guide provides technical background information about the voice and video over IP technologies that are monitored by CA Unified Communications Monitor (UC Monitor). This guide helps you understand the challenges of delivering a high-quality experience to the users who access your unified communications system.

Unified Communications and the IP Network

The definition of *unified communications* is evolving. For UC Monitor, the term refers to integrated applications that enable communications that use existing IP network infrastructure and extend beyond telephone service. Unified communications represent the convergence of multiple modes of communication within applications and infrastructure to allow people, teams, and organizations to communicate more effectively.

The IP network provides the unifying factor for unified communications. Unified communications rely on a converged network, often with multiple and diverse applications vying for the same network resources. Therefore, network performance is a critical enabler for all unified communications applications. Assessing user quality of experience when interacting with unified communications system components is the key to the delivery of these services.

UC Monitor monitors unified communications applications and devices, and measures their performance from a user perspective.

VoIP Performance on the Network

Many businesses lose sales opportunities when the phones go down for even a few minutes each month. VoIP traffic requires premium handling for the following reasons:

- Network users are accustomed to excellent performance from their telephone service, which has been excellent since they first picked up a telephone in their homes. They notice, and probably complain, when the quality of their VoIP calls dips even slightly.

- VoIP is a real-time application. As such, it is sensitive to latency, jitter, and packet loss. The network infrastructure is not designed to carry real-time application traffic.

VoIP still behaves like an emerging technology. Standards are still adopted and challenged. Multiple vendors still sell components that do not work together. These factors can create major application performance issues on converged networks. As a result, even a limited VoIP deployment requires ongoing, VoIP-specific monitoring, frequent call quality evaluation, trending, and troubleshooting.

Unique Characteristics of VoIP Traffic

VoIP traffic has several unique characteristics:

- VoIP is a significant consumer of bandwidth. Application performance deteriorates when VoIP traffic runs on the same network because VoIP sends data at a fixed rate, with no throttling mechanism.
- VoIP has a fair amount of header overhead and sends data continuously in two directions. Depending on several factors, such as the codecs you use and the levels of phone usage, VoIP traffic can really fill up your network. Your TCP applications gracefully back down under conditions of congestion. VoIP can starve them out.
- VoIP uses the Real-time Transport Protocol (RTP), which rides on top of the User Datagram Protocol (UDP). RTP applications typically send packets at a fixed rate, and because UDP is a connectionless protocol, there is no retransmission or reordering of data. When a packet is dropped, it is gone. The signal cannot be retransmitted. If a whole group of packets is dropped at once, entire portions of a conversation between two IP phones are lost.

Think of VoIP as an application that is highly delay-intolerant, and whose quality depends on delivery with minimal latency, jitter, and packet loss.

Video Performance on the Network

Maintaining user Quality of Experience (QoE) is immensely challenging for video applications because it is difficult to measure success in delivering high-quality video. Video applications do not have a widely accepted video quality standard equivalent to the MOS for audio. Video quality is more subjective than audio quality, and it is more complicated to implement.

Video is finicky. Like VoIP, it has stringent performance requirements. Its real-time, streaming behavior resembles VoIP, but some of the performance metrics that affect VoIP call quality have a more powerful effect on video. For example, packet loss causes a syllable or two to drop out of a call. For a viewer of a video, packet loss causes pixelation and probably slow or frozen images. Jitter on a call makes the audio sound scratchy or garbled. Jitter during a video conference both distorts the image and scrambles the speech. The effects are both more noticeable and more annoying. Video requires a network that is expertly tuned, adequately or even over-provisioned, and carefully monitored.

Video applications have a much greater throughput requirement than VoIP. Video packets are large to begin with, and a key point to remember is that a video conference also has an audio component. One video stream takes from 300 to 400 kbps in each direction. Add the audio, and you have more than 800 kbps for combined video and audio streams.

On the LAN, video performs well. However, a desktop video deployment means that some video streams are sent point-to-point, between a pair of users. Others are multicast, for a video conference or webcast, for example. A slow link or busy interface presents a potential issue for these users. Using desktop video conferencing enables cross-site collaboration, which usually means video calls must travel across WAN links to reach remote offices. When they compete for bandwidth with other application traffic, these data streams can create bottlenecks on WAN links and WAN-LAN interfaces.

Challenges of VoIP and Video Deployments

The primary challenge in maintaining a unified communications system is minimizing network *delay.* Delay is the latency from infrastructure components such as:

- packet queues
- QoS queues
- firewalls
- NAT
- encryption

Properly configured QoS policies ensure that other data applications do not contend with voice-allocated bandwidth, but they can add delay. Encryption technologies introduce more latency by ignoring priority flags (ToS) and adding additional header information, such as IPsec headers.

Non-uniform packet delays, or *jitter*, are often more detrimental to VoIP and video call quality than latency. When it is not affecting every voice packet in a stream, delay creates jitter. Jitter affects call quality as the signal starts to sound or look garbled. Jitter can also cause packets to arrive out of order, which introduces additional latency at the application layer when reassembly of the signal occurs.

VoIP-endpoint buffers, network devices that support QoS, and RTP header compression can minimize jitter. But there is always a tradeoff. RTP header compression, for example, adds latency due to the extra processing that is required on the routers.

Packet loss can also result from excess latency or jitter. VoIP and video are also more sensitive to packet loss than other network applications. Loss rates greater than three percent are considered intolerable when compared to plain old telephone service (POTS) calls.

Finally, specialized VoIP equipment presents its own monitoring and maintenance challenge. Test and monitor your call servers to ensure they can handle voice traffic and can route it properly.