savvius™ | TECH BRIEF

Isolating and Improving Unified Communications in the Enterprise

Unified Communications (UC) applications such as VoIP and video have been used in the enterprise setting for well over a decade, yet they continue to cause some of the biggest and most persistent IT headaches for network engineers.

One explanation for this is that most networks are configured to prioritize TCP traffic, which is used by email and other non-real-time applications. By contrast, UC-related network traffic typically relies on a best-effort protocol such as UDP, which doesn't allow for all of the acknowledgements and re-transmission of packets enabled by TCP. So, if UDP packets don't arrive in time, or come out of order, they cannot simply be added back into the data stream. This makes UC applications like VoIP particularly prone to poor quality and a frustrating user experience due to underlying issues on the network such as packet loss, latency, and jitter. Bringing wireless connectivity into the mix only exacerbates these problems due to the possibility of introducing additional interference.

Forcing Analog into a Digital World

We've all experienced those annoying VoIP calls and live video streams where sound quality was poor or where there was a half-second delay in the conversation, making natural dialog very difficult. The fact is that we live in an analog world, but we force UC applications to work on our networks by converting them into digital streams of packets. Natural conversations are fluid and continuous; they don't have time to 'buffer' or be re-assembled, so real-time applications such as VoIP and video need their data to be transmitted immediately, not seconds or even milliseconds later. Even small inconsistencies in packet delivery cause noticeable, annoying issues, as well as making communication more difficult.

One of the biggest distinctions between UC applications and other applications on the network is the source of the data. Rather than being generated digitally, the origin of UC data is a fluid and continuous analog stream. For that reason, data from UC applications like VoIP need to be dealt with in real time. Unfortunately, as digital files are transferred over any network, it's normal for some of those packets to fall out of order, even by a fairly significant amount. Although VoIP devices use buffers to help smooth packet influx, the buffer can only do so much before we begin to hear static, dropped syllables, and even cases of more severe quality degradation.

The difference between TCP and UDP protocols causes a fundamental change in the way data is sent and received. TCP is a very reliable packet delivery protocol that has the flexibility to deal with widely varying packet spacing while handling packets of many sizes. Thanks to TCP's built-in checks, balances, and acknowledgements, packets that don't reach their intended destination in the form they were sent will be retransmitted and put back in their proper order. This isn't the case for UDP, which is a best-effort protocol. UDP is characterized by regularly spaced, small, and consistently-sized packets. Once a UDP packet has been sent, there is no mechanism to acknowledge or retransmit that packet if it gets delayed or corrupted due to issues such as latency, jitter, and packet loss. This reliance on consistency is perhaps the biggest weakness of UC applications on the network today.

The Impact of Latency, Jitter, and Packet Loss on UC Applications

If you've ever experienced a delay during a VoIP call, then you've probably been a victim of latency. Even delays of half a second quickly cause an unnatural cadence that results in people unintentionally talking over one another. Likewise, jitter on a network causes packets to be delivered out of order, causing strange sound effects such as static, uneven audio, and jerky video feeds. TCP's non real-time design deals with jitter well, but a UC decoder doesn't have time to put packets back in the right order, so it cannot afford to have a jitter buffer longer than 50 or 60 milliseconds. Anything longer than 100 milliseconds will simply cause packets to drop. Last, but definitely not least, packet loss is due to physical layer corruption. It can typically be found in systems that experience congestion but lack adequate provision for Quality of Service (QoS). Packet loss results in missing sounds, syllables, words, or phrases. While there are DSP algorithms that compensate for up to 30 milliseconds of missing data, anything above that threshold will be noticed by the listener.

Actionable Data to Resolve any UC Issue

Tools like the VoIP dashboards in Savvius Insight Plus, and the powerful diagnostics and analytics tools built into Savvius Omnipeek®, make it possible to quickly visualize and troubleshoot any UC application issue.

The ELK VoIP dashboards (Calls and Media) in Savvius Insight Plus™ are extremely useful for monitoring and trouble-shooting VoIP traffic: use the Calls dashboard to see the number, duration, endpoints and gatekeeper of the call, the overall quality of calls, and more. For even more detail, the Media dashboard provides access to all available quality scores for each media flow. Analyze MOS and R Factor scores, one-way delay, packet loss, and jitter.

Omnipeek offers several dashboards that are optimized for traffic over TCP, UDP, and any other encoding or decoding protocol. These dashboards allow network engineers to use any number of measurements or standardized call quality metrics such as Mean Opinion Scores (MOS) or R-Factors to quickly determine the root cause of network issues that may be impacting VoIP and video quality.

For example, Omnipeek's Voice & Video dashboard allows network engineers to compare packet utilization with VoIP utilization to quickly drill down to individual calls and look at qualitative metrics, such as MOS scores, to identify and investigate specific calls for troubleshooting and resolution.

Another tool is Omnipeek's Expert view. These views give users the freedom to classify data by a variety of categories such as QoS, making it possible to rapidly filter results and investigate specific calls that showed poor results. In addition, Omnipeek's Media view can be used to reveal other details about UC applications, including how well data is flowing from either direction of a VoIP call.

The core strength of Omnipeek in UC application troubleshooting lies in its ability to provide complete visibility, packet by packet, into any aspect of the application's data traveling across the network. Whether it be the management or config and control packets used to set up a call, to information about jitter and latency, or the MOS and R-Factor, all of that information is right at the user's fingertips. This allows users to quickly identify problems and work rapidly to resolve any lingering issues.

Conclusion

UC and other real-time protocols don't reside in a vacuum. For that reason, troubleshooting UC applications requires network engineers to look at the network as a whole. Rather than showing network engineers what's happening solely from a UC perspective, Savvius Insight Plus and Omnipeek provide the critical visibility to see UC applications in relation to all of the other traffic on the network. That is the only truly effective and long-lasting way to troubleshoot, analyze, and resolve UC application issues on any shared network.

We often fall into the trap of thinking about networks in terms of bandwidth, where more is better. However, in practice, the quality of network traffic is much more important than the quantity when it comes to UC applications. Many high-performance networks regularly experience large spikes or bursts of traffic that impact real-time applications like VoIP and Video far more than they affect non-real-time applications. One of the best ways to deal with these issues is to establish an accurate baseline that captures long-term trends together with short-term peaks and dips. This combination gives network engineers a much more balanced view of averages over an extended period of time, where even millisecond spikes can matter on the network. Armed with all of the information from Savvius Insight Plus and Omnipeek, network engineers can proactively resolve most UC issues well before they are even noticed by the enterprise's users and clients.

Savvius and the Savvius logo are trademarks or registered trademarks of Savvius and/or its affiliates in the U.S. and other countries. All registered and unregistered trademarks are the sole property of their respective owners. The use of the word partner does not imply a partnership relationship between Savvius and any other company.