

Changing the Conversation

I'm launching a personal crusade to get people to stop thinking that "voice is just another application on the data network." Let's be clear. In implementing VoIP, we need to *create a voice network* that happens to use packets, not tweak a data network to enable it to carry voice.

We all understand that voice traffic has characteristics that make it more sensitive to network perturbations than typical data traffic. But when we start with the notion of enhancing the data network, we set ourselves up for some potentially fuzzy thinking that's rooted in the history of how different network strategies evolved in the past.

No Margin of Error

Companies cannot afford to make a mistake with the quality of voice communications. At the core of our country's values is the right to life, liberty, and toll-quality service every time we pick up the phone. Well, at least, that's how most people see it. It is this requirement for every-time, always-available, high quality service that makes voice different than most other communications applications.

This requirement is even more stringent in the contact center, where revenue and customer retention are on the line every minute of every day. If voice quality is compromised, is management likely to accept the explanation that voice is just another application on the network and, therefore, they should expect delay and packet loss from time to time? I think not.

Potential compromises in quality will drive contact center management to resist a move to VoIP – and with good reason. We've seen it happen. Companies maintain an isolated, standalone TDM-based solution in the contact center, while the rest of the company moves to a new infrastructure. Besides adding ongoing support costs, keeping the legacy approach means losing the transformational opportunities that VoIP can bring, and the potential contributions to the business's bottom line.

Starting in the Wrong Place

Beginning with the wrong premise (that voice is an application on the data network) can lead to a number of problems. Some of the more obvious issues reflect all that well-documented mythology of the differences between voice folks and data folks – "five 9s of reliability" vs. "we'll just have the network down for a few minutes!" Like a lot of myths, this one is grounded in experience. But, while most companies today really do understand these distinctions and have worked around legacy thinking, there are plenty of examples where vestigial attitudes have caused embarrassing outages.

A more typical example is *after* the network is up and running. Unlike other applications on the IP network, keeping five 9s humming for voice is a continual, and sometimes hard, slog. The constantly changing nature of a shared network means that it must be continually monitored for the impact of configuration changes, new devices and applications, other technology additions, competing priorities, etc.

Too often companies moving to IP will have their vendors do a “network readiness assessment,” make all the necessary changes and upgrades, install the VoIP infrastructure, announce availability, and then break out the champagne. That’s consistent with the notion that it’s a voice application running over the data network. The application is tested and installed, and we can move on to other things with a minimal amount of ongoing monitoring of the state of the network’s health. But if the focus is that this is a *voice* network, then it’s more obvious that comprehensive, ongoing monitoring is needed.

Another example is security. One of the concerns that I hear about with voice over the network is the need to put in place extra security precautions. There are so many threats that simply didn’t exist on the old PSTN. The implication is that, if it weren’t for voice, we wouldn’t need to be concerned about these. Of course, managers realize that that isn’t the situation at all; it’s just that voice makes these issues more visible because a potential interruption is more obvious. There are good processes and devices available to provide the security needed. Mostly, it’s a matter of paying attention to a number of issues that weren’t previously on our radar. But, companies need to be putting these procedures in place anyway to secure the data on the network too.

Changing Attitudes

I recently talked about my crusade with the CIO at a major company who has made the transition to IP. He thought about it for a minute, and then said, “You’re right. Too much of our time we have spent complaining about how ‘this voice application’ is getting in the way of other things on our network. We need to revise our thinking. We need to view this as a voice network, not data.” A voice network with the requisite robustness, survivability, and quality built in from the ground up.

And, by the way, if you do it right, you can make that high-reliability, secure voice network available to data traffic, too.

Don Van Doren is president of Vanguard Communications, an independent consulting firm that helps clients achieve their business goals through better customer contact solutions. Contact Don at dvandoren@vanguard.net or visit Vanguard at www.vanguard.net.

Published in VON Magazine, December 2005