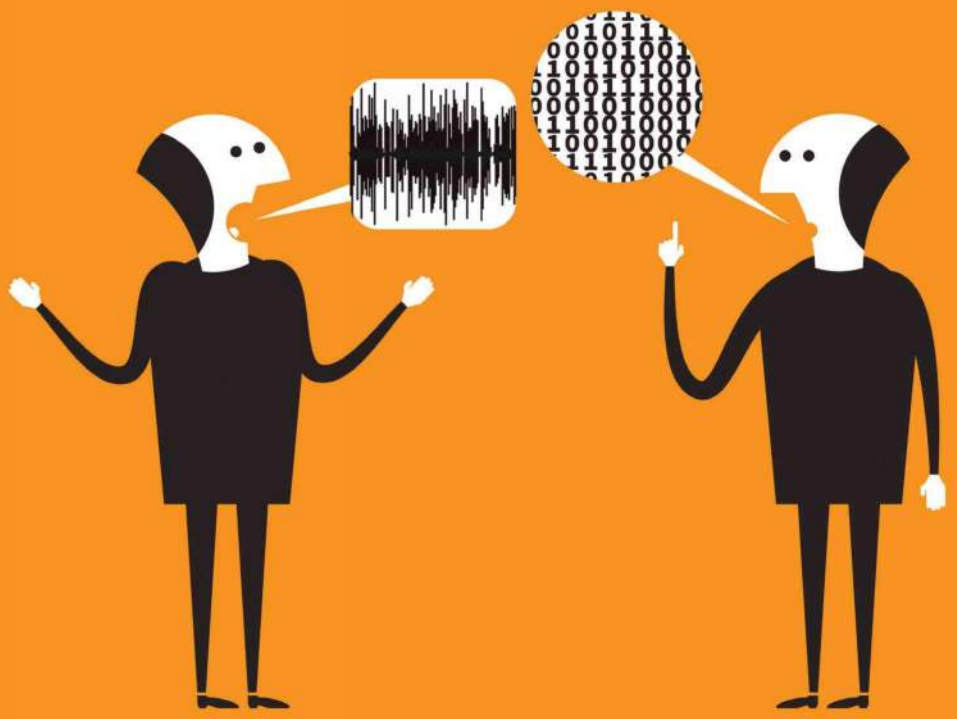
THE TECHNOLOGY MANAGER'S GUIDE TO

IT ESSENTIALS



Featuring:

- SPEAKING THE LANGUGE OF IT
- SAFEGUARDING AGAINST HACKS
- FOSTERING TWO-WAY CONVERSATIONS

from the editors of

AVTECHNOLOGY

sponsored by

ADDER®
THE IP KVM PEOPLE

HALL RESEARCH

Editor's Note

[**By** Cindy Davis]

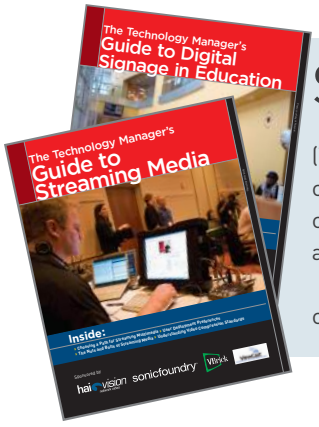
HOPPING ON THE BANDWIDTH WAGON

We've pushed the AV/IT envelope. The conversation has moved beyond the basics. Convergence has occurred, and we'll see more exhibitors than ever at InfoComm 18 showing full suites of networked AV solutions.

Savvy AV professionals are on board. Others are hopping on the bandwidth wagon. The following articles provide some much-needed structure and perspectives for approaching converged AV and IT, discussing it with the IT department, and avoiding the "not-on-my-network" response.

While we feel it is critical that all AV professionals have a basic understanding of networked AV principals and the impact it has on IT, it's equally important to know this is where you should rely on AV/IT technology consultants, integrators, and vendors.

Look for the acronyms defined in the glossary. As always, we welcome your feedback.



SPEND A DAY IN OUR LIBRARY

(You don't have to whisper or leave your coffee at the door.) Stroll through the electronic corridors of AVNetwork.com and stop in our library of AV Technology Manager's Guides. Brought to you by our erudite editors and expert contributors, The Technology Manager's Guide to... series presents an in-depth look into the most important areas affecting your bottom line.

Explore our Guides to Boardroom AV, Streaming Media, Digital Signage in Education, and many more. Our Guides are completely free to download and they are yours to keep. (And there is no late fee.)

Table of Contents

FEATURES

THE SEXTANT GROUP

The Sextant Group was responsible for audiovisual planning and design of Kiewit's new 62,000 square-foot training center, which features a variety of technology-intensive spaces including an auditorium, large and small classrooms, breakout rooms, and conference rooms.

What IT Needs to Know About Networked AV

Trying to communicate AV needs to the IT department using a common language might be easier than scaling Everest speaking Esperanto. We've gathered some wisdom from AV and IT industry veterans to help navigate the terrain.

By Cindy Davis

The operative word in networked AV is—you got it—network. At least that's how the IT department sees it. And let's face it: If you want to move your organization into 21st-century AV, your path goes straight through IT. You need to learn their language and understand why their first reaction is often "not on my network."

"There's a language barrier that isn't helped by the fact that there's not a published common set of AV standards that as an industry we can hand to people," said Jon Ottesen, senior technical director at Crestron Electronics. The IT world, on the other hand, references a 3-inch-thick book of standards from the Institute of Electrical and Electronics Engineers (IEEE).

Crestron can say a particular product supports 802.1X, an IEEE standard for port-based Network Access Control (PNAC). This provides an authentication mechanism to devices wishing to connect to a LAN or WLAN. "I am borrowing their language for my piece of equipment to express to them what's happening on my device in their stack," Ottesen said. "I'm using their language because they need to be confident that we're compliant."

AV manufacturers can support AV integrators and managers with the documentation to provide the IT department so they can make informed deci-

sions. "The AV industry does not have a set of definable published standards that create a common-criteria of behavior and language," Ottesen said.

AV STARTING POINTS FOR TALKING TO IT

Paul Zielie, manager of enterprise solutions for Harman Professional, recommends starting with an accurate scope of the project. Answer these questions first:

1. What is the business value, including the internal sponsorship the project brings?
2. How many devices need to be added to the network, and where they will physically reside?
3. Where will network traffic be required? Will admin or user computers need to access the devices? Will the devices need to get to the internet or the wide area?

"Brushing up on the language of an IT networking professional so you can fluidly communicate with them can help," said Mark Grassi CTS-D, principal consultant of The Sextant Group. "Remember, we are playing in their sandbox, and they are responsible for protecting the data of your enterprise, and every device that goes on the network is a risk."

Phil Hippensteel, an instructor at Penn State Harrisburg, said AV managers should have a good understanding of the following before going to the IT department:

1. How variable subnet masks work, e.g., 255.255.255.224;
2. The differences between TCP and UDP traffic;
3. How ARP, DNS, and DHCP work.

BE READY TO ARTICULATE WHY

An IT manager knows the network benefits of communications systems such as email and VOIP, as well as access to servers and printers. A convincing case for why AV belongs on the network will sell the "why" to the IT folks.

"There are two primary benefits to using networked AV products," said Harman's Zielie. First is the scalability and cost efficiency of using existing, standardized infrastructure to implement AV services. Second is reducing the operational costs and decreasing incident response times associated with the AV application by leveraging the ability to remotely access AV equipment and perform troubleshooting and maintenance. Standardized infrastructure and reducing operational costs are familiar IT concepts, so you're speaking their language.

The Sextant Group's Grassi added, "From the basic level, having networked AV products allow for centralized and streamlined control capabilities." Having each device on the network allows for easy deployment of code, firmware, and troubleshooting of devices.

"Taking that a step further, when we leverage the network for audio and video transport we open up what can be accomplished," Grassi said. Allowing for network-based transport allows us to scale systems beyond what is possible by having purpose-built, localized systems. "Once the audio or video is on the network it creates the ability to do resource sharing, which will ultimately drive down installation and equipment costs." Further, having transport on the network makes for better maintenance and service capabilities, which is familiar to IT departments.

"Articulating benefits of networked AV products is the same as articulating anything else—listen to the concerns of your clients, then address them one by one," said Sextant's Jesse Fishman CTS-D, DSCE, senior systems/GUI designer. If you don't have an answer for something, tell them you don't know, but can facilitate a conversation with the manufacturer. Once you've gotten the concerns out of the way, it becomes much easier to explain benefits such as saving physical space, cost, and scalability.

"Once the audio or video is on the network it creates the ability to do resource sharing, which will ultimately drive down installation and equipment costs."
—Mark Grassi, principal consultant, The Sextant Group

ADVICE FROM THE OTHER SIDE

Geordie Klueber recently joined Biamp Systems as a video and network specialist. He spent more than two decades at IBM and Sun Microsystems where he specialized in distributed computing systems, networking, and cloud computing. He was the "other side."

From an IT perspective, Klueber said the biggest concerns are: What resources will this need to use, statically, initially, and dynamically? What impact is it going to have on the other stuff that's going on my network right now—which may or may not have a higher priority than what you're asking me to support? And what is the security angle? "If the answer to any of those is presented negatively—it could be a show stopper," he said.

"I am borrowing their language for my piece of equipment to express to them what's happening on my device in their stack. I'm using their language because they need to be confident that we're compliant."
—Jon Ottesen, senior technical director, Crestron

If AV managers have some concrete answers for the IT department, it will go a long way toward making the sale easier. "Not just initially, but throughout the project," Klueber said. "So rather than going in and saying, 'I think it needs 400 IP addresses; I'm not quite sure how it works. And yeah, it uses 5Gb of video, and the vendor said it's secure, so I'm all set.' That's not a good approach in any situation.

"Instead, say, 'Here is what my AV system is going to consist of. I'm going to have X number of devices. Each one of those devices is going to require one IP address, and these devices will consume X amount of bandwidth, and the ports that are open per device are these, and only these.'"

All AV network companies will or should have this information available to provide, and this can often be found on their websites. Be proactive when you go to an IT person with this information. "They are going to feel a lot more comfortable about working with you," Klueber said. "Because that means that you understand their perspective."

In the end, "that means I'm not going to have to waste my time defending why I care about security because you already get it," Klueber said. "Which means that I'm going to be more likely to work better with you."

The Number-One Deal-Breaker

Toss everything you've learned about networked AV if you can't ensure IT security.

By Cindy Davis

You don't need to become a network security expert, but you do need to know how to help provide the right answers so IT departments can ensure security. "Fortunately, most manufacturers already account for this and list security measures for their products," said Jesse Fishman CTS-D, DSCE, senior systems/GUI designer at The Sextant Group.

Many include AES encryption, so signals can't be eavesdropped, 802.1X authentication to prevent products from being compromised, and secure shell protocol for protecting and encrypting communication between devices. "Sometimes additional security measures are used by manufacturers to make products even more secure," Fishman said.

THE ATTACK SURFACE

"Attack surface" seems like a military term, but according to Geordie Klueber, video and network specialist at Biamp Systems, "All it means is, am I giving a bad guy another platform on which to do something nefarious?" It might not be the security of the device itself, but if someone gets into that device, what can they do with it?

"Every network port my device opens is another vector that somebody can attack me with," Klueber said. One way to mitigate this is by hardening devices, also known as "locking them down." "This means turning off everything except that which is exactly and specifically needed."

From a networking device perspective, most enterprises are going to have a vetting process. Many IT departments insist products be fully tested to ensure security before it can be added to the network.

"The good news is that since these are appliances or dedicated function devices, it's easier to task and analyze stuff," Klueber said.

The biggest thing to understand is what needs to talk to what, said Paul Zielie, manager of enterprise solutions for Harman Professional.

At that point, it's important to know what services are available and what is being used in the application. "A service is when a device accepts a communication," Zielie said. "For example, if a device can be configured via a web browser, it is it is offering a web service. The browser itself is a client. The ports and protocols documentation will reveal the services."

The first level of security is to make sure the services are secure enough for the organization, Zielie said. "This could be by turning them off—for instance turning off the http service but leaving on the https. This could be by configuring them [by] setting up user and password access. Or, this could be by limiting the access through the network (by blocking the port), only allowing computers in the service group to access the web interface, but no other computers."

And, a reminder from Phil Hippensteel, an instructor at Penn State Harrisburg: "Never, ever leave a device with the default password."

Typical Security Documentation Include

HARDWARE AND SOFTWARE INVENTORY

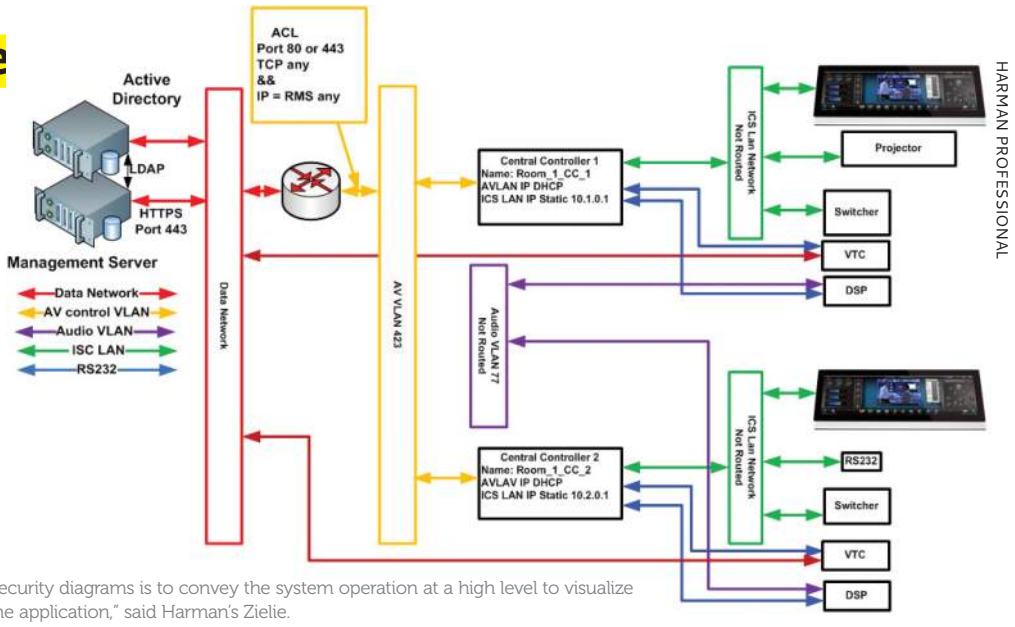
* Ports, Protocols, and Services
* OS and Package Versions Network Topology

NETWORK TOPOLOGY

* High-Level Network Diagram
* Logical Topology
* VLAN Assignments
* Physical Topology
* Connection Points
* Traffic Flow
* Access Control Lists

ACCESS CONTROL

* Roles and Permissions
* Password Policies



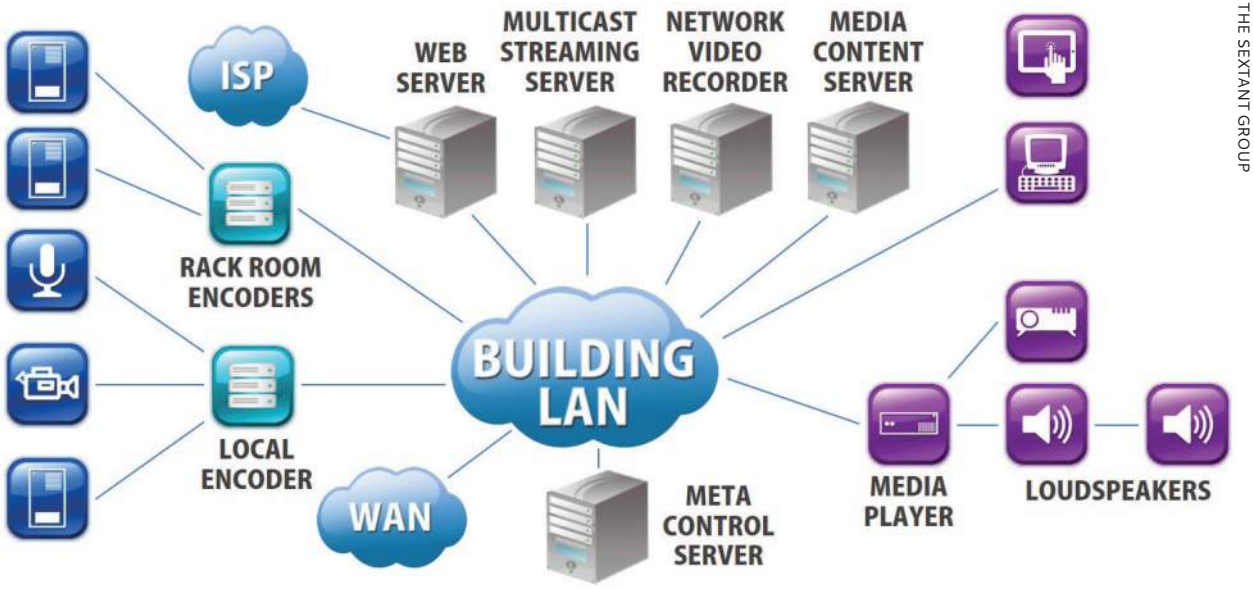
"The purpose of security diagrams is to convey the system operation at a high level to visualize and understand the application," said Harman's Zielie.

Articulating Networked AV Needs

AV on the network needs to be two-way conversation with the IT department. Here's how to prepare.

By Cindy Davis

One of the least-understood concepts by AV designers and managers is how AV traffic affects other corporate traffic, but it is the single most important issue for IT folks. It is imperative to have at least a basic understanding of the network to have informed conversations about networked AV. This is also where you should rely on the expertise of AV/IT technology consultants, integrators, and vendors.



Elements of an AV-over-IP network

THE SEXTANT GROUP

"We as an industry are asking to live on the IT network," said Mark Grassi CTS-D, principal consultant, The Sextant Group. "IT professionals will not be too receptive to this if we cannot articulate our needs to them."

Grassi offers the following as helpful information you should bring to the IT department to have a constructive conversation:

- A basic network diagram of what you are trying to accomplish;
- Network ports that need to be open on the network for proper communication;
- Necessary VLAN configurations in order for proper isolation of communication protocols;
- Bandwidth requirements necessary at the local network switch and between network switches;
- A network risk assessment document detailing the security protocols of the various equipment being placed on the network;
- Is any special network hardware required? For instance, in the case of AVB, particular network switches must be used to handle the AVB traffic;
- An IP scheme concept for the equipment and an understanding of what devices are capable of doing. For instance, can a DNS name be set? Is the device capable of being set to a static IP address? How must other devices communicate with this device?

Network services are helper applications that give your devices the information they need to do their jobs, like the time or IP address of a URL.

NAVIGATING

"You need to be able to understand and describe where the network traffic needs to go," said Paul Zielie, manager of enterprise solutions for Harman Professional. Think of where the network traffic will be required—just between devices? Will admin or user computers need to access the

Ports and protocols, the sub-addresses of network communications, and the types of communications are vital when the traffic needs to leave the local network.

devices? Will the devices need to get to the internet or the wide area?

"VLAN and multicast route requirements come out of the understanding of where network traffic will be required, possibly combined with the need for security or bandwidth control," Zielie said. "Your network people should be able to help you come up with the right combinations."

Ports and protocols, the sub-addresses of network communications, and the types of communications are vital when the traffic needs to leave the local network, especially if security rules block traffic and bandwidth becomes crucial. This information should be available from the equipment manufacturer. "At that point you need to figure out which ports and protocols are associated with which portion of the application," Zielie said. "For example, you may need the ability to control or configure a network video device from an admin computer, but not require the video stream to be accessible from that computer. Those two parts of the application have separate ports and protocols."

Bandwidth becomes important when traffic needs to leave the local switch. "If I have 15 800Mbps video sources on a switch, it will not be a problem to have them sending traffic to the appropriate ports with receivers connected to the same switch," Zielie said. "However, if I send multiple video streams out a single port to multiple receivers on another switch, I will quickly run out of bandwidth."

PRO TIP 1

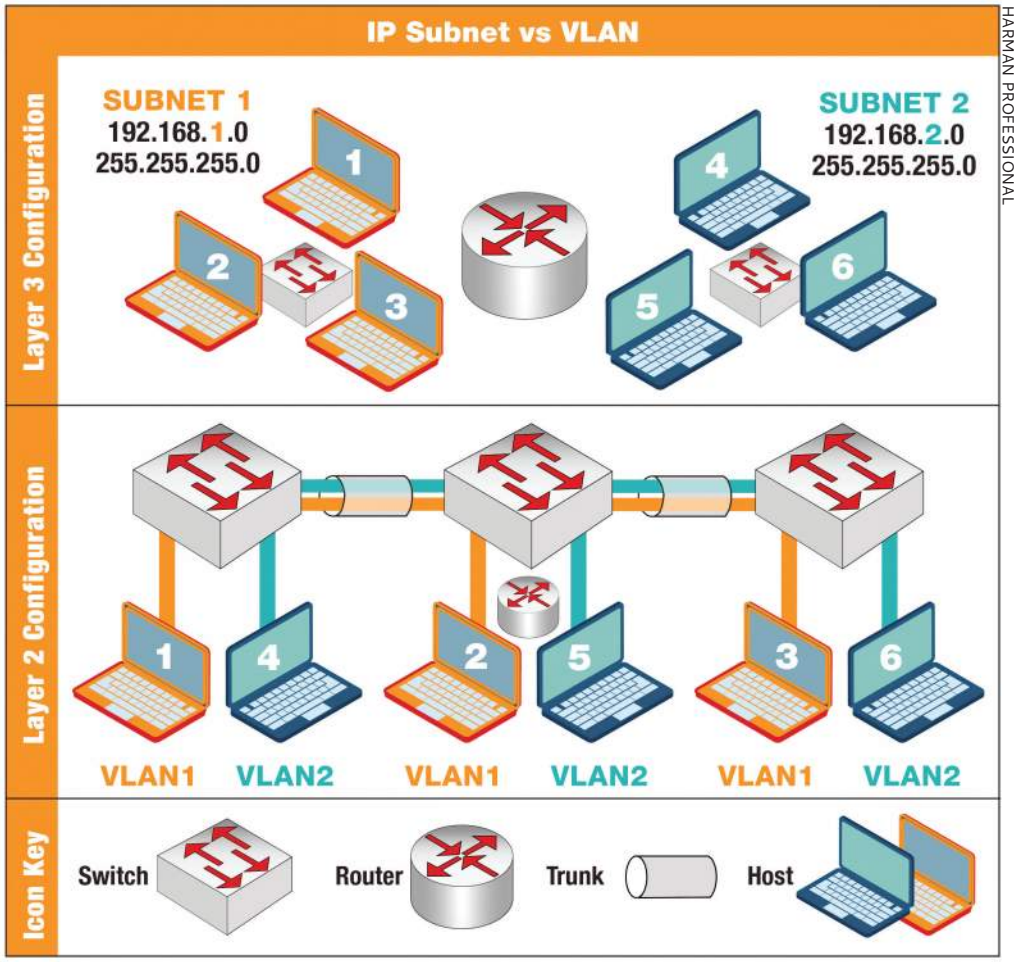
The network will not stop the transmitters from trying to send more bandwidth than a downstream link will handle. If your application requires a limited number of streams at a time, you should put in an AV control method that keeps track of the bandwidth being sent across a link and does not allow additional transmitters to start sending if the bandwidth isn't available.

PRO TIP 2

Be very careful when you "daisy-chain" switches together and you have multiple video-over-network sources.

Even if your application is not allowing too much bandwidth across a link, that link can be flooded. "If you are using multicast with IGMP

Open Systems Interconnection (OSI) Models Define a networking framework to implement protocols in layers, with control passed from one layer to the next.



HARMAN PROFESSIONAL

Harman's Paul Zielie stresses the importance of understanding and describing where network traffic needs to go.

snooping and have multiple switches connected, all the video streams are forwarded to the switch which has the IGMP querier," Zielie said. "There is nothing you can do about it; this is how the technology works. The topology must be designed to avoid this."

Network services are helper applications that give your devices the information they need to do their jobs, like the time or IP address of a URL. This information should be in the product documentation. "Often this information is handed out with the IP address and will not be an issue, but if any services are a requirement it is best to verify their availability," Zielie said.

What about AV devices that integrate with cloud services? "In that case you've just opened up another avenue for all of the other issues," said Geordie Klueber, video and network specialist at Biamp Systems. If you need access to the internet, you need to know how much bandwidth is needed, identify the security model, and how it is going to be authenticated, among other things. "These are all kinds of questions that are going to come from the IT side of the house," Klueber said. "If you give them a preconfigured list and anticipate what they're asking for, it's going to go a long way toward assuaging their fears."

HOMEWORK HELPER

AV managers need more than a superficial understanding of technical acronyms. "For example,

The Latency Discussion

Anything below 13 milliseconds of latency is considered imperceptible by mere mortals. Numerous terms are used to describe what is nearly imperceptible by the human brain in the sub-50-millisecond range. Some call this "near-real time," while others call it "zero latency."

Everything in nature takes time, said Geordie Klueber, video and network specialist at Biamp Systems. "This is an important point because in the IT space, latency is much less sensitive than it is in AV. So, if it takes you an extra five minutes to get an email, does it really bother you? Probably not."

This is where AV managers need to help IT departments understand the importance of low latency in each application. Conversely, AV managers need to understand where latency is added on the network. "In many cases, latency is not the primary factor in choosing a video transport method," said Paul Zielie, manager of enterprise solutions for Harman Professional.

Klueber suggested that latency and bandwidth are directly related, but often at odds with each other. "I can make a network that is very, very high bandwidth, but a result of that is that the latency is very, very high."

Many factors come into play when low latency is required. Before you design and buy products to build a solution that depends on low latency, it is essential to understand the full picture. "Depending on the network design, adding a single network router to the network can increase latency by hundreds of milliseconds," Klueber said.

Having a relationship between AV and IT is crucial, so each side has an understanding of the current operational capacity of the network. "They may have plenty of bandwidth, but the way the network is architected, if you need 20 milliseconds of latency to go from the New York office to the Chicago office, that's just not going to happen."

Simple conversations can avoid a lot of finger pointing.

a critical difference is the one between TCP and UDP," said Phil Hippensteel, an instructor at Penn State Harrisburg. "These are the protocols chosen by the video application that almost completely determines how that traffic will behave on the IT network and how it will interact with the network conditions and other traffic."

We have an amazing resource for you! Go to avnetwork.com, and search "Phil Hippensteel." For more than 10 years, Hippensteel has been providing "Byte-Sized Lessons for Technology Managers."

You'll learn what you need to know if an IT person asks about variable subnet masks, VLAN trunks, or ARP broadcasting.

"If you give them a preconfigured list and anticipate what they're asking for, it's going to go a long way toward assuaging their fears."
—Geordie Klueber, video and network specialist, Biamp Systems

Or what happens if DNS response times doubles? What apps are affected and how? Understand how the TCP/IP environment really works, and so much more.

QUICK GLOSSARY

Address Resolution Protocol (ARP): A protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

Domain Name System (DNS): The internet's equivalent of a phonebook containing a directory of domain names and translating them to Internet Protocol (IP) addresses.

Dynamic Host Configuration Protocol (DHCP): A network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network.

Internet Group Management Protocol (IGMP): A communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast.

Open Systems Interconnection (OSI) Model: Defines a networking framework to implement protocols in layers, with control passed from one layer to the next.

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP): The two most common protocols of the Internet protocol (IP) suite. Both protocols use port numbers as their addressing scheme.

Transmission Control Protocol/Internet Protocol (TCP/IP): A suite of communication protocols used to interconnect network devices on the internet.

Virtual Local Area Network (VLAN): A way of partitioning a physical network into smaller networks.