



Network Video Doesn't Have to Burden IT

Have you seen that vein bulge on your IT director's forehead when he hears you say "network video?" Learn to feel his pain and ease his mind with these tips.

By Randall R. Nason, PE

The IT transformation of the electronic security industry is evident in practically all recently completed and ongoing projects. What started out as a communication protocol to link a few research computers together has resulted in an essentially universally accepted digital communication standard.

The early adopters, the information technology (IT) professionals providing networked business services to their organizations, became the owners of the IT network landscape. Security departments, accustomed to owning and operating dedicated and isolated communications networks, quickly found themselves tenants on the corporate network. This carries a number of clear advantages, not the least of which is the luxury of having, on someone else's payroll, a trained staff dedicated to keeping the network healthy.

At the fundamental level, the goals of the IT and physical security groups are identical. My IT associates have three goals for their

networked systems. First, availability: IT professionals pride themselves on maintaining downtime benchmarks that are measured in minutes per year. Second, integrity: The data that leaves the source must arrive at the destination quickly and intact. Third, confidentiality: Transmission paths must be secure from unauthorized access, interception, observation, and interruption.

As security professionals, we would list all of the above attributes as non-negotiable requirements for our system communication networks. Sounds like a great marriage.

Still, the waters often churn when the prospect of a new or expanded network requirement is presented to the IT department by the security group.

IT's big concerns are always associated with the video portions of the proposed system. Network cameras are getting better, less expensive, and therefore more dominant in new and upgrade projects. They also place a

big demand on the network's bandwidth and storage.

How Much Bandwidth Do You Have?

Bandwidth is the first discussion point when a new or expanded security system is in view. Security designers must understand the finite nature of the existing IT infrastructure and the need for the IT group to continue to provide existing services to the using community without performance degradation or lapses.

As these designers begin to discuss gross and net bandwidth to determine the impact of the new system, you'll want to understand certain standards of transmission and cable nomenclature. You'll find a short

based on common assumptions about uncompressed video frame sizes. This provides a good beginning point to determining the bandwidth requirements of the new or upgraded system.

Unfortunately, in practice, determining the size of the video data stream is not quite that simple. A recent publication by Pelco, one of the leading manufacturers of digital video equipment, even says, "For years, the industry was fond of providing concrete numbers for average file size based on image size, resolution and record rate. Unfortunately, there are simply too many variables that affect this actual number."

This is borne out by a quick review of the specification sheet of a high-end digital CCTV encoder. For a 1CIF

(480 pixels) image, the range is given as 768 to 4096 kb/second, a factor of over four between the upper and lower estimates.

What Affects Compression Ratio?

Modern digital video equipment uses various compression algorithms in an attempt to reduce bandwidth consumption. While the best compression technique cannot necessarily be defined, the most widely used appears to be MPEG-4. The actual compression achieved by any technique is a function of the video scene. Particular factors affecting the compression ratio include:

Scene Detail. The size of the digital video file is affected by the amount of detail present. For example, a video frame of a cloudless sky is normally smaller than a frame of a parking lot. Conversely, a video scene with a wide variety of detail results in a larger file. A bright light in the video scene or multiple bright colors will keep the file size up.

Scene Movement. The bandwidth consumption of a video stream is also affected by the amount of change that is occurring in the scene. A static scene requires less bandwidth than a scene that is changing. This factor also comes into play if the camera moves, either through wind or other environmentally induced

Name That Cable

The Institute of Electrical and Electronics Engineers (IEEE) standard 802 specifies a number of Ethernet standards that use varying types of cable and support different bit rates. As you talk with your IT team, you'll probably want to have a baseline understanding of these specifications.

The name of each specification alone gives you useful information. The first number reflects the bit rate. For example, 10Base-2 supports a speed of 10 Mbps. The final letter or number reflects either the segment length (number) or type of cable (letter). Here's a short rundown:

10Base-2: 10 Mbps, coax	10Base-5: 10 Mbps, coax (RG-8)
10Base-T: 10 Mbps, twisted pair	100Base-T: 100 Mbps, UTP
100Base-FX: 100 Mbps, fiber-optic	1000Base-T: 1 Gbps, Cat-5 UTP
10GBase-X: 10 Gbps, fiber-optic	

overview in the box below. Another good resource for this information is Bruce Hallberg's *Networking, A Beginner's Guide*, published by McGraw Hill.

The majority of the installed networks are at the 100Base-T level, while new installations are trending toward the 1000Base-T level. The net or available bandwidth is a multi-variable function of existing traffic, necessary overhead, desired surge capacity, and contingency for growth.

How Big Are Your Images?

The critical parameter the IT staff will need from you is the size of the data stream presented by the security-related cameras and associated devices. Unfortunately, this is an elusive parameter to determine. Table 1 at right shows some simple calculations

Table 1: Uncompressed Video Bandwidth Requirements

Frame Rate fps	Frame Size ¹ kB	Byte Rate kB/s	Bit Rate ² kb/s	Bit Rate Mb/s ³	Cameras on 100 Base T Network
30.00	15.00	450.00	3,600.00	3.52	23.70
15.00	15.00	225.00	1,800.00	1.76	47.41
10.00	15.00	150.00	1,200.00	1.17	71.11
5.00	15.00	75.00	600.00	0.59	142.22

¹ "Video Compression for Surveillance," Dr. Bob Banerjee, *Cygnus Security CCTV Supplement*, Feb. 06

² Don't confuse bits and bytes. 1 byte (B) = 8 bits (b).

³ Conservatively assumes 20% overhead

(Common Interchange Format, 352 x 240 pixels) image, the estimated bandwidth requirement ranges from 512 to 1024 kb/second, a factor of two between the upper and lower estimates. Similarly, for a 4CIF (720 x

motion, or as a result of programmed tour movement.

Camera Noise. Camera noise typically occurs when there is inadequate scene lighting and the auto gain circuits

are active in order to compensate. This type of noise affects the whole video scene and appears as movement.

Some video analytics developers have implemented advanced algorithms to reduce file sizes even beyond what is normally achieved through conventional compression techniques. Very simply, one manufacturer has implemented an algorithm that separates the moving

This dedicated portion of the network can be designed to accommodate the bandwidth and recording demands of the security video system. The subnet is normally isolated from the balance of the organization's network through appropriate application of router and firewall functions. Depending on the application, this configuration may require specific access procedures as an authorized user moves from the

appropriateness of the assumptions is then determined over time, through experience. If it turns out that the video file sizes are larger than anticipated, several system parameters can be adjusted, usually on a per camera basis, such as frame rate and compression ratio. As a final solution, additional storage capacity can be installed.

The storage concern has been diminished somewhat as digital security video hardware manufacturers have begun to provide modular high-end RAID 5 network storage devices specifically focused on security video applications. This industry focus includes the ability to match the particular compression algorithm implementation that is used throughout the rest of the system.

When You Design, Keep IT in Mind

- *Use local recording*
- *Isolate security on a subnet or dedicated network if necessary*
- *Adjust video parameters to maximize storage*
- *Choose optimized hardware*



Problems are Surmountable

Digital CCTV implementation represents new territory for most individuals and organizations. The advantages are overwhelming when the camera and analytical software are viewed in the context of providing definitive, actionable information to the responsible parties. These advantages come with a level of uncertainty with regard to network requirements and impact, but problems are imminently solvable through consultant support, conservative assumptions, and cooperative effort from all affected departments. **ST&D**

target from the relatively static background. This technique achieves its highest efficiency when the identified target represents a relatively small portion of the video frame.

How to Design for Bandwidth

There are a couple of network design features that can reduce digital video's burden on the existing network infrastructure.

A common design approach that has been in use since the VCR days is local recording. In systems where there may be concentrations of video resources, recording and storing the video information locally will eliminate the need to transport large quantities of real-time video over the network infrastructure, thus avoiding burdening the common network and the associated potential network performance impacts. Stored video information can be retrieved over the network as needed by the security administrators and monitoring staff.

Another approach is to isolate all security-related functions on one or more subnets that are logically isolated from the common network.

common network to the logically isolated security network.

A third approach is to establish a dedicated network that is physically isolated from the remainder of the common network. Referred to as the air-gap approach, this is used when the confidentiality of the security data or the burden on the balance of the network is such that physical isolation from the rest of the users is considered necessary.

Ease Their Minds on Storage

Beyond bandwidth, the IT manager is concerned about the storage space required to archive the video that is streaming across the network. The uncertainty in the size of the video stream clearly affects this topic as well. Fortunately, there is usually some flexibility on the storage parameters.

Most projects start off with a specified video archive period that ranges from days to months depending on the industry and organizational risk profile. Storage sizing calculations are normally made with conservative (high rather than low) assumptions regarding video file sizes. The



Randall R. Nason, PE, is a corporate vice president as well as manager of the Security Consulting Group of C.H. Guernsey & Company. His experience includes a broad spectrum of the security profession, including threat assessment, vulnerability analysis and site surveys through complete system design and construction management. Mr. Nason's current and recent projects focus on critical infrastructure protection.