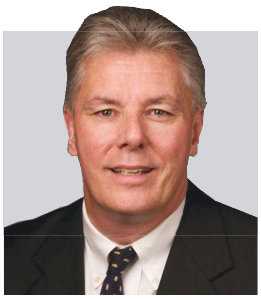
IT Intelligence

MAXIMIZING BANDWIDTH WITH MINIMAL NETWORK IMPACT

by Bob Stockwell



Bob Stockwell is Global Technology Leader for STANLEY Security. From 1997-2012, he was Niscayah's Director of Systems Operations.

bob.stockwell@sbdinc.com

Maximizing bandwidth and minimizing network impact is critical for a successful security system in today's environment. This month's tips mainly focus on video surveillance, which usually has the greatest impact on a network.Consulting IT personnel from the start provides valuable guidance and resources on how to best use the existing infrastructure and add to it, if necessary, as well as minimize potential for costly mistakes. Without the appropriate support, adding even just a few IP cameras could cause problems within a network.

When planning for a video system, carefully consider the following:

1. *How many cameras will be installed?*
2. *Where will they be installed? (Are there network connections nearby, e.g. 100 meters or less?)*
3. *Frame rate at which you will view*
4. *Frame rate at which you will record*
5. *Resolution in which you will view and record*
6. *Do the cameras support multiple video streams?*
7. *Does the network support multicast?*
8. *Encoding to be used (e.g. MJPEG, MP4, H.264, propriety)?*

After these questions have been considered, determine if the existing network infrastructure will support the new system, even beyond bandwidth capability. Today's systems begin at 100Mbps per port, and though this may seem sufficient for a 1.3-megapixel camera, there will be other traffic to consider (E-mail, VoIP, Web sites, application servers, etc.) unless you are running on an isolated network.

Next, evaluate the processing power of the data switches connected to the video system. Most data traffic comes in bursts, and data switches have buffers to handle overflow if too much information is received at once. However, video is a steady stream and does not stop, and if the video is sent faster than the switch can process, there's no chance to catch up, which is the case with normal data traffic. This can cause video loss, or even a switch to lock up.

Many cameras can send multiple video streams at once, but these streams add up quickly. In a system, there may be one stream for live view, another for recording, one for alarm and another for mobile viewing. This means a single 1.3-megapixel camera must now send up to four or more megapixels of data. Selecting the correct encoding type is also important. MJPEG formatting sends a very large stream and can consume a network quickly. H.264 formatting sends a much smaller stream and is more bandwidth efficient. But there's a catch: H.264 requires much more processing power to decode and view. Consider this efficiency example: Camera 1 with 720p @ 10 FPS using MJPEG = 8.72Mbps vs. Camera 2 with 720p @ 10 FPS using H.264 = 647Kbps.

Improper routing can be another pitfall, so consider where cameras are located relative to the recorders and monitoring stations. If the recorders are not located on the same network as the cameras, and data must travel through multiple switches or routers to get to the recorders, this can cause additional network traffic. Typically, WANs have slower connection speeds and are more vulnerable to congestion.

Next, gauge how the system handles video streams. Does the camera send a live stream to the customer and another to the recorder, or is it sent to the recorder and retransmitted to the customer? In some installs, these two streams can be on different networks, thus reducing the load on a single network. Multicast can also reduce usage in the right situation.

Consulting IT personnel from the start provides valuable guidance and resources on how to best use the existing infrastructure, as well as minimize potential for costly mistakes.

If multiple devices are accessing the same video stream, multicast sends one stream to multiple devices/customers.

Isolating video network traffic from business network traffic can also help maximize network usage. VLANs use the existing network to separate video network traffic from day-to-day data traffic through software configuration. Another method is to totally separate the security systems from the business network. Though a more expensive approach, this is also more secure.

Using QoS (Quality of Service) technologies will also allow the option to select and prioritize certain types of traffic over others, such as VoIP services over E-mail. With QoS, data packets are broken up into small, manageable packages for routing between endpoints. An E-mail is stored until all packets arrive before being reassembled and delivered. In a voice call and live video, packets must arrive in order, or the data will be jumbled. QoS allows the ability to specify which is most important.

All in all, maximizing network bandwidth relies on proper planning and having knowledgeable, consulting resources from the onset. ■