Q&A | Video Surveillance

Q: What are the benefits of IP Video Surveillance?

In the old CCTV world, monitoring stations were fixed and hardwired; now they can be flexible and mobile. IP video systems are easy to install and are flexible to meet changing requirements. IP Video Surveillance systems are able to easily combine multiple locations to a single video security solution and can integrate to other security systems as part of a complete holistic security framework. The change to IP-based video surveillance has coincided with dramatic improvements in camera technology and the adoption of high definition video for surveillance use. High definition video not only improves the quality of the image but it also means that in many cases fewer cameras are needed for a particular coverage area.

Q: How much bandwidth will it require from my network?

The bandwidth requirement for any particular video stream is related to the quality and complexity of the image, and this can be configured to provide the right balance between bandwidth cost and video clarity. Good quality IP cameras can be configured to provide compressed video streams from less than 30Kbps up to 4Mbps (and more). A rough "rule of thumb" number: 200kbps is reasonable for standard definition and 1Mbps provides an excellent quality high-definition stream. Don't forget to consider the aggregate bandwidth usage for all hops on the network, as well as the bandwidth required for monitoring stations.

Q: If the network goes down, how do we ensure that our cameras stay live?

First, make sure that the edge power-over-Ethernet switches are properly protected with uninterruptible power supplies. Without this protection, even a small power interruption produces a significant interruption in video surveillance. All the normal techniques for providing reliable network connectivity apply to IP video surveillance. We can also strategically place the NVR servers in the network to provide continued service if particular network elements fail. Distributed video storage provides both improved uptime for network failures and reduces bandwidth requirement. For the ultimate in video surveillance up-time, cameras are available with the ability to locally store video for future retrieval. Combine this with a local battery backup for the camera and you can ensure complete recording even if the local cable is cut.

Q: Can the cameras be centrally managed if we have a multi-site deployment?

Yes. Ease of management and flexibility for multi-site deployment are key benefits to IP Video Surveillance. The fact that all three key elements (cameras, recording systems and monitoring stations) are on an IP network that can be securely accessed from anywhere for management means that administrators and technicians no longer need to be on-site to manage the systems. Furthermore, Video Management Systems (VMS) are able to provide an overlay solution to complement the individual components and provide a single integrated system, not just for system management, but for security operations too.

Q: How do you set up a multi-site deployment and manage it holistically?

Proper selection and implementation of the VMS simplifies management of the system with features like central access control, storage allocation tools and archive rules. These systems can also enhance the operational value of the system though integration to mapping and physical security management systems, video wall management, investigation tools and automated event handling.

Q: Can you talk about the tradeoffs when it comes to unicast routing versus multicast routing for IP video surveillance?

The tradeoff is bandwidth efficiency versus network administration complexity. This balance is currently shifting because new IP network solutions are dramatically simplifying network configuration for multicast deployment. Although multicast technology has been available for a long time it is not widely used because adding more bandwidth has been seen as a simpler and more reliable alternative, and before IP video there were not many bandwidth-hungry applications that would benefit from IP multicast. IP Multicast has the ability to reduce bandwidth requirements by providing a single data stream that is accessed by multiple devices. It is particularly useful for IP video surveillance when an organization has multiple monitoring stations on a multi-site system.

Q: How can I ensure that my video streams come in real-time from my remote monitoring stations?

Any application that needs real-time data should use a network that is configured for Quality-of-Service (QoS). Quality of service is a collection of network techniques used to ensure that the network provides particular applications (in this case video surveillance) with the end-to-end performance needed by the application. The performance of the network is measured in terms of packet latency (how much time a packet of data takes to traverse the network), packet jitter (how much this latency varies over time) and packet loss (how many packets don't make it to the destination). The actual value for latency is not that important, but keeping packet loss low is critical. One of the drawbacks of the compression algorithms used to compress the raw video stream data to a manageable bandwidth is that relatively low packet loss can produce a dramatic drop in video quality. So the question is not so much about real-time delivery to the monitoring stations, but about providing good quality video to the monitoring stations. The answer is the same: use QoS on the network.

Q: Do I need a dedicated network for IP video surveillance? What are the performance, scaling and security issues if I utilize my existing IT network?

There is a great parallel between IP telephones and IP video surveillance in this regard. Early IP telephone deployments were often deployed on a separate network but now it is completely commonplace to run IP telephones on the normal IT network. The same is true of IP video surveillance, although the trend is several years behind. Knowing that video can be a high-bandwidth application, many organizations are still not prepared to let that additional traffic on the IT network for fear that it will slow down other applications. However, the prevalence of gigabit and multi-gigabit networks with high throughput switches and routers means that many existing networks are capable of supporting the additional load of video surveillance systems. Quality-of-Service (QoS) must be implemented on a shared network to maintain performance for the video surveillance system.

Q: How can I secure my video streams if I put video surveillance over my existing IT network?

The security of the video surveillance data as it travels over the network can be maintained through typical network security methods. Just how these are used depends on the level of security required. Cameras have multi-level username and password authentication with IP address filtering to stop unauthorized access. Video data streams can use HTTPS to provide both data encryption and protection from man-in-the-middle connection attacks. The video network itself can be logically separated from the user network and firewalled off to further prevent unauthorized access. Also, the cameras can use 802.1X to authenticate with the network. This prevents anyone from using the camera's network connection, which may be outside the physical security boundary of the facility, to get unauthorized access to the network.

Q: How do I design the access portion of my network to eliminate single points of failure for cameras as well as VMSs?

The discussion of reliability for IP video surveillance systems again highlights the flexibility unlocked by using an IP-based system. All the technologies available to provide reliable data networks, servers and storage can be used by the IP video surveillance system to improve reliability and uptime. Networks with dual uplinks, switches with redundant power and supervisor modules, Dual NICs, RAID disk arrays and so on, all contribute to the robustness of the system. Best practice for the access edge where the cameras connect is to use two stacked PoE switches with multiple core links and pairs of cameras with overlapping coverage of key areas. And while thinking about system uptime, do not ignore the value of a properly implemented network management system to keep the network running smoothly.

About Jim Emerson

With over 25 years of industry experience in multiple communications and network technologies, Jim provides consulting, design and operational expertise to many Fortune 50 companies. Jim has been with Meridian IT for almost three years and has a degree in Applied Physics from Durham University.

Meridian IT Inc. is a member of Meridian Group International, a collection of companies engaged in technology and equipment leasing businesses. Since 1979, Meridian Group has been helping organizations optimize the strategic value of their IT investments. Learn more at www.onlinemeridian.com

Nine Parkway North, Suite 500 / Deerfield, IL 60015 USA / Tel. 847.964.2664
www.meridianitinc.com