Is the Network Ready for Video?—Network Assessments

The surveillance industry is using the IP network as the foundation for new video surveillance deployments. While every major vendor is focused on delivering both standard and high-definition IP cameras, servers, and viewing workstations, the role of assessing the network infrastructure falls on the security integrator. Often, the success or failure of the installation, and the resulting perception of the capabilities of the integrator, is dependent on the capabilities of the network.

Cisco is offering new tools and resources to successfully deploy IP video surveillance on complex networks.

Figure 1.   Cisco Video Surveillance 5000 Series HD IP Dome Camera (1080p) H.264


Is the Network Ready for Video?

An IP-based video monitoring system that uses the existing network infrastructure provides a cost advantage over a traditional analog-based system. Existing IP networks already support voice (VoIP) and data applications. Networks that are enabled for VoIP often have medianet-ready access layer switches installed that support Power over Ethernet (PoE), quality of service (QoS), and Auto Smartports. Attaching IP video surveillance cameras to PoE switches is more cost effective than using externally powered, analog-based systems. Typically around 80% of the long-term costs of any system are operational. Converged IP networks can deliver operational savings immediately and throughout the much longer life of a networked IP-based video surveillance system. Standalone video surveillance systems are more costly to operate, maintain, integrate, and upgrade over time, and become obsolete more quickly.

While controlling costs is a key consideration, increased image quality is driving the adoption of IP-based video surveillance. When presented with a video image at high-definition (HD) resolution, few people will find standard-definition video acceptable. A recent public school deployment initially specified 278 total cameras, 36 of which had HD resolution. During the implementation, the requirements were amended and upon completion, 363 of the 376 cameras were HD.

If a network supports VoIP and data today, will it also support IP-based video? It might, but some additional analysis is required. VoIP requires less bandwidth than video and may be more tolerant of packet loss. A single VoIP-encoded (G711/G729) call generates 50 packets per second with a network load between 30 and 90 Kbps. VoIP packet loss concealment is effective at masking occasional loss. With voice calls, not all parties are speaking continuously. Packet loss during lulls in conversation incurs no audible distortion.

With video surveillance, there is no lull in a conversation; video is streamed over the network 24x7. The HD camera snapshot shown in Figure 2 (1080p, 30 frames per second, H.264, 6 Mbps CBR, packet loss induced at 0.04%) is generating 575 IP packets per second—almost 30 times the number of IP packets as a VoIP phone. The image illustrates how even 0.04% packet loss can distort video. The details and clarity of people moving through the field of view is obscured by the packet loss. For a video surveillance implementation to be successful, the network must deliver IP packets with very low loss thresholds while maintaining acceptable latency and jitter.

Figure 2.   Cisco Video Surveillance 5000 Series HD IP Dome Cameras—Packet Loss Induced at 0.04%
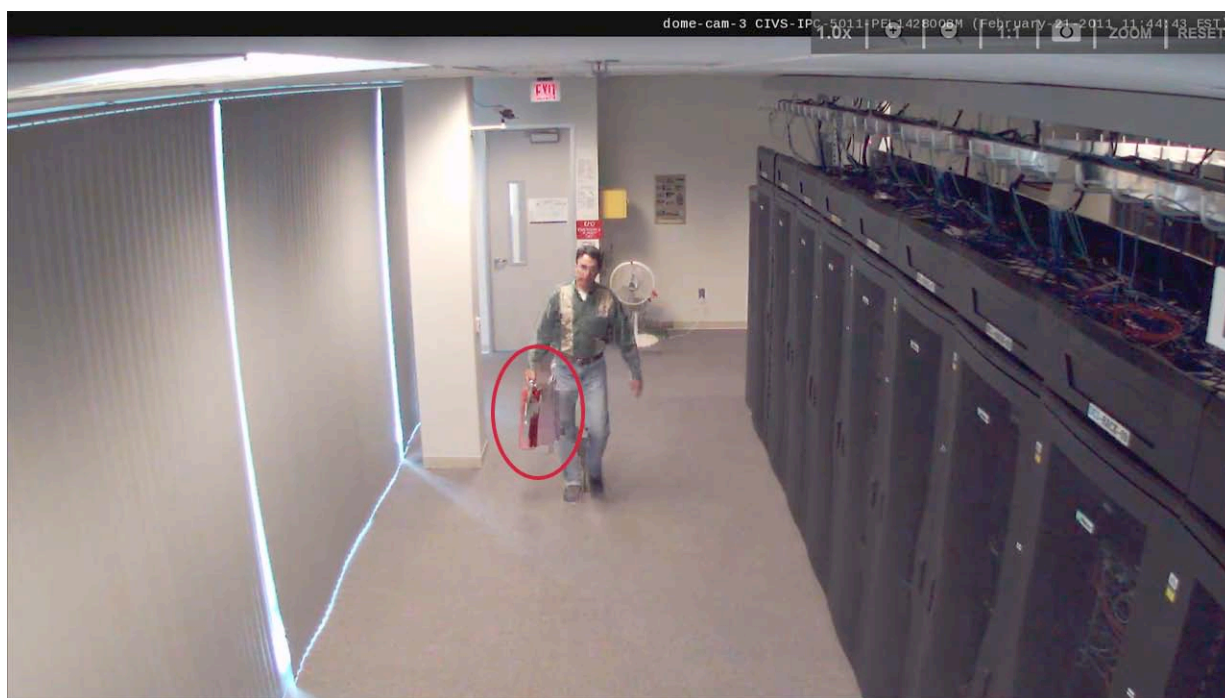
The goal in assessing the network prior to deploying video is to ensure the quality of experience of the video surveillance deployment to meet the safety, security, and loss prevention needs of the organization.

Who Can Assess My Network?

It depends on the complexity of the network and how it is supported. Small, single-site, video surveillance deployments can be assessed quickly. In some cases, these deployments may be implemented with switches that are dedicated to support video endpoints such as standard-definition IP cameras, servers, and workstations. A Cisco Authorized Partner uses a checklist to assess the installation.

Cisco Authorized Technology Provider (ATP) partners can assess larger, more complex implementations that use high-definition IP cameras, that may include locations connected through a metropolitan or wide area network (MAN/WAN), and that typically also support VoIP and data applications. Cisco ATP partners have the training and knowledge to analyze, inventory, and assess the network and remediate any network design or capacity issues prior to deploying video. These partners will work with an organization's network administrator and deliver a report documenting their analysis of the network that includes performance graphs from the Cisco Video SLA Assessment Agent (VSAA) tool.

For network deployments with large numbers of IP cameras deployed in diverse topologies at many campuses, a Network Consulting Engineer from Cisco Advanced Services can be engaged to work directly with the network administrator. These Cisco engineers are skilled in implementing complex network and physical security deployments.

If you have questions or need additional information, please contact us at physec-questions@external.cisco.com.

Collateral

The following collateral provides guidance on routing, switching, and design requirements to best support IP-based video surveillance.

Network Readiness Assessment for IP Video Surveillance

- White paper (HTML; PDF available):
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/IPVS/IPVS_Network_Assessment.html
- Webinar (83 minutes):
  https://cisco.webex.com/ciscosales/lsr.php?AT=pb&SP=EC&rID=42300707&rKey=7d3276e94cf7fcdb
- Presentation (PDF):
  http://www.cisco.com/en/US/docs/solutions/enterprise/video/IPVS/IPVS_network_assessment_presentation.pdf

For more information, contact your Cisco account team.