CHAPTER 3

Solution Components

This guide is published at a point in time where video surveillance systems are no longer solely standalone, isolated, totally analog-based systems, nor fully integrated into the IP network and converged with other enterprise subsystems. The long-term goal of the industry is to move out of the targeted role of addressing the areas of loss prevention, regulatory compliance, and personal safety to providing a business value to the enterprise.

To increase sales and deployments of IP video surveillance equipment, the goal must be to move from targeting the physical security manager as the primary decision maker in the organization to the chief financial office and IT/technology officer.

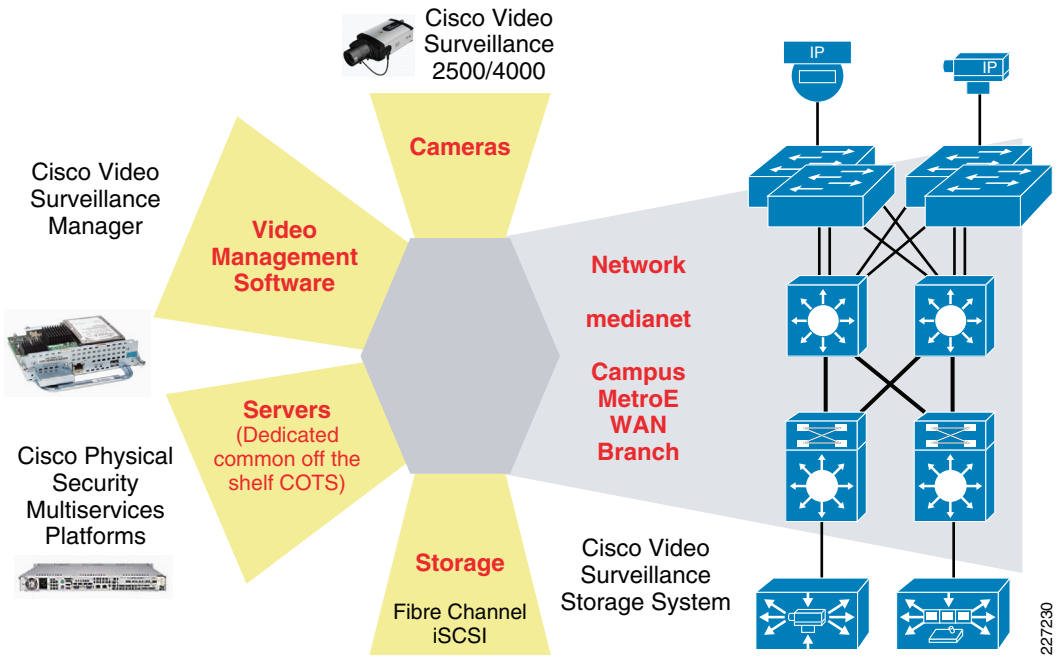
The true value in a converged physical security deployment is when the video data can be analyzed and the result of that analysis provides actionable information on increasing sales or reducing costs or legal liabilities to the enterprise. Increasing the return on investment (ROI) by lowering the costs of the video surveillance infrastructure through IP-enabling video surveillance is an initial goal. The goal is to reach the point where all aspects of the video surveillance system are IP-enabled and integrated on the IP network before moving on to subsequent objectives.

This guide addresses how to integrate a video surveillance onto the enterprise IP network. This is not the end goal, it is the first step. In this chapter, the various components and functions of an IP video surveillance deployment is discussed. Then, at an overview level, the IP network infrastructure key points of bandwidth, quality-of-service (QoS), security, network services, and virtualization are reviewed. The chapter concludes with the prospects of network management, integration with ancillary subsystems, and video data-mining and analytics.

Video Surveillance

Every video surveillance deployment is made up of cameras, video management software, servers, and storage. The IP network is then the fifth element that ties all these components into a converged network infrastructure. The relationship is shown in Figure 3-1.

Figure 3-1 Components of IP Video Surveillance Deployments



In very small deployments, the video management software, server, and storage components can be as simple as a single PC, an IP camera, and a simple Ethernet hub. Very large deployments may encompass thousands of IP cameras, hundreds of servers, and a storage subsystem capable of hundreds of terabytes to a 1-petabyte (1024 TB). In the first case, the network requirements are trivial, in the second, substantial.

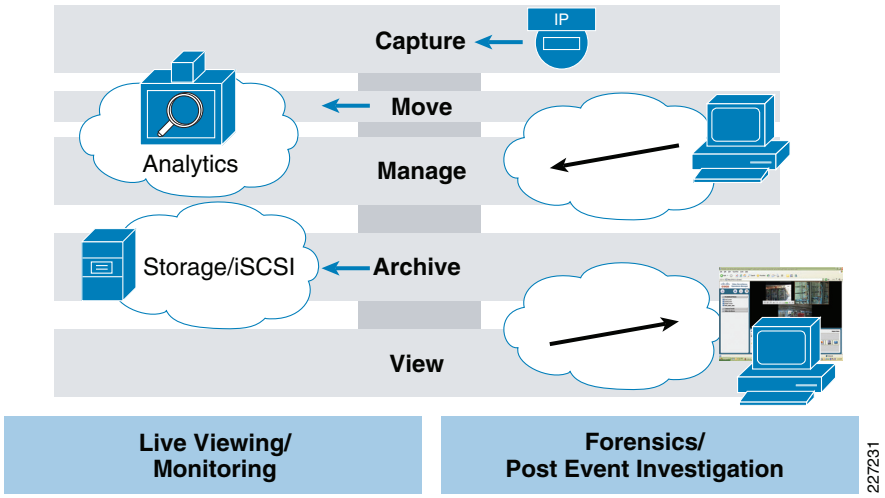
The IP video surveillance application intersects with the network infrastructure by connecting endpoints, IP cameras, workstations, servers and storage physically to the network. From a network planning and design standpoint, it is important to understand the flow of both media and command and control functions between the components. Video surveillance has two main baseline functions: live viewing and real-time monitoring of video feeds, and retrieval and viewing of video as a post-event investigation. Forensic video analysis is used to examine and analyze video for use in legal proceedings. Some video may require one type or the other, or both. Traffic cameras may have the sole purpose of identifying congestion and have no need for archive or retention of the video data. An enterprise video deployment may have both live viewing of selected cameras with all cameras being archived. Other deployments may be "*headless,*" meaning there is only archiving, but no living viewing.

The primary video surveillance functions are:

- *Capture*—Encoding video feeds for network transport
- *Move*—Camera feeds are moved from camera to one or more servers for processing
- *Manage*—Administration of cameras, setting up archives, configuring operator views, etc
- *Archive*—Storing real-time camera feeds to disk for later retrieval
- *View*—Viewing either live or archived feeds

These functions are shown in Figure 3-2.

Figure 3-2 LAN/ WAN/MAN Intersections to IP Video Surveillance Functions



Each of the above functions can intersect with the underlying IP network and, to properly design and implement the network, the requirements of the video surveillance application must be understood. To capture a video feed, the IP camera must be configured for resolution, frame rate, and server IP address; at least the frame rate and resolution could change at times throughout the day. Therefore, simply capturing data requires some control plane network traffic as well as keeping the clock of the camera in synch with a universal clock through protocols such as Network Time Protocol (NTP). While the bandwidth requirements of the function is small, the reliability and availability requirement is high.

Moving video feeds introduce a bandwidth load on the network. The cameras may be LAN- or WAN-attached. Understanding the collective bandwidth from a deployment of hundreds or thousands of cameras requires an understanding of the load placed upon the network. These media streams must also be protected against packet loss.

Managing the system also influences the network bandwidth requirements. If there is a requirement to schedule a backup of an archive, sufficient bandwidth must be available for this function to complete. The archive backup process is typically between a remote Media Server and a central Media Server and the limited bandwidth of the WAN must be considered.

Archiving the data through a directly attached point-to-point Fibre Channel between server and storage unit is very straight forward, but what if Fibre Channel switches are deployed or iSCSI?

The viewing function shares similar network requirements as the move function, because the client workstation is retrieving the same video feed from the server as was transported from the camera to the server originally.

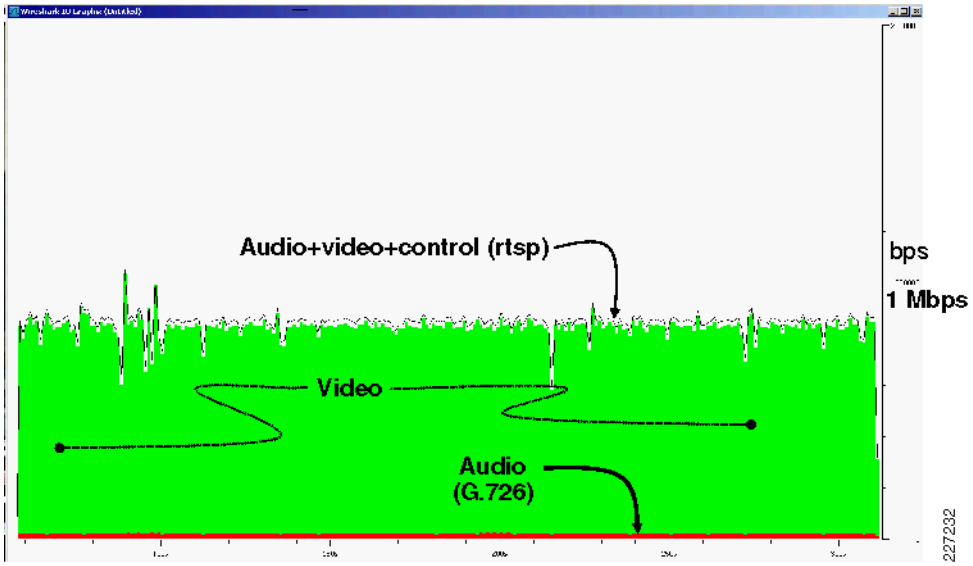
IP Network Infrastructure

The areas of bandwidth, QoS, security, network services, and virtualization are key elements of provisioning the enterprise IP network to support video.

Bandwidth

The bandwidth requirements for all video, but video surveillance in particular, is substantial compared to VoIP. Common codecs used in VoIP deployments, (G.711, G.729,G.726) use between 8 and 64Kbps for the voice encoding. A packet capture from a Cisco 2500 Series IP Camera configured at a CBR target of 1M for the MPEG4 feed with audio-enabled on the camera. Control traffic (HTTP/RTSP) is also captured. The relationship between the amount of audio, video, and control plane is obvious. See Figure 3-3.

Figure 3-3 Audio and Video Network Load



The bandwidth requirement for the video media stream is orders of magnitude higher than Audio (VoIP) and Signaling (RTSP) for video in the enterprise network.

While provisioning for this bandwidth requirement is a key element in planning for video in the enterprise network, there are other network requirements to be considered. For example, will the video traffic be segmented on both the LAN and WAN from other user traffic either logically or physically? Is the video deployment an overlay on an existing network infrastructure or is a entirely new deployment? Is IPSec encryption currently implemented? These factors must also be taken into consideration along with the bandwidth requirements.

QoS

QoS is a key element to managing network congestion during periods where bandwidth is constrained. QoS, however, does not eliminate bandwidth constraints; it manages the access to bandwidth by competing applications through prioritizing one application over another. QoS manages unfairness. Because the video quality for MPEG-4 and H.264 is highly dependent on little or no packet loss, IP video surveillance traffic must not be dropped by the enterprise QoS policy. Motion JPEG-based video does not suffer a degradation in the image with packet loss due to lack of bandwidth, but the smoothness of motion is compromised. Several frames or even several seconds of video may be missing with no indication of the loss. Because many video surveillance deployments are 'headless', and first time the video is viewed may be days or weeks after capture. If the quality is poor due to packet loss in the network, there is no recourse and the video data is worthless.

Security

Security focuses on controlling what users have access to a resource while in transit, at the originating node, or when it is processed or stored on a server. One aspect of IP networking is the any-to-any connectivity between networks and users. This strength is also a flaw. There is a certain population of users on the network that must have access to the video surveillance system, but many cannot be trusted to access this data. Video surveillance data is particularly sensitive because access to the system by unscrupulous individuals may expose the enterprise to financial loss and compromise personal safety. This guide illustrates transporting video traffic over LAN and WAN with IP security encryption and also implements administrative controls on who has access to the network.

Network Services

One advantage of the any-to-any aspect of IP networks is access to resources and systems. NTP and Syslog messages are examples of network services that IP cameras can request data from and send data to, which are either not available with analog-based systems or are more costly to implement. Additionally, local utilities like Power-over-Ethernet (PoE) and Cisco Discovery Protocol (CDP) both lower the cost of installation and facilitate troubleshooting.

Virtualization

Through virtualization techniques, the routers and switches can be configured to provide access to a common network infrastructure while maintaining a separate address space, broadcast domain, and separation of one user group from another. IP video surveillance is one application that is a prime candidate for virtualization as the end-user population is very small, the endpoints (IP cameras) may be distributed on a large number of routers and switches in the enterprise, and the data (video feeds) contain information that may be sensitive. This guide provides a detailed discussion of implementing virtualization of both routers and switches.

Network Management

Network management applications and protocols are discussed under the section on network services where IP service level agreements (IP SLAs), Syslog, CDP, and Simple Network Management Protocol (SNMP) are shown in relation to video surveillance deployments. Enterprise networks vary in degree of sophistication and maturity of network management. IP video surveillance, however, is one application that can greatly benefit from a proactive approach to the Fault, Configuration, Administration, Performance, and Security (FCAPS) model. For example, in headless deployments (video feeds that are not actively monitored by a person), the availability and network performance is critical to ensuring quality video recordings. The network management platforms and processes of the enterprise can help the physical security manager in detecting and reacting to an endpoint or network transport issues that could impact video quality.

Integration with Ancillary Subsystems

Physical security is one component of facilities management in many large organizations. Other components include door access control, which is often closely linked with video surveillance as a key component to the safety and security missions. In order to realize the goal of a fully-converged network, the other building management systems (BMS) such as fire alarms, elevator control (to park elevators in the event of a fire), air quality monitoring (carbon monoxide and smoke detection), and lighting and heating/cooling must be able to communicate with the video surveillance systems.

The first step in realizing this goal is to IP-enable these devices and provide the network infrastructure to support their effective communication between systems. For example, if virtualization is enabled on the IP network to support video surveillance, a practical approach is to also include the BMS devices on the same address space, and in the same network segments, as the video surveillance devices. Typically, the bandwidth requirements of BMS systems are very trivial to that of video surveillance, the end-users of the data are often report to the same organization heads and the likelihood of system integration now or in the future is high.

Video Data-Mining and Analytics

The end-goal of migrating from analog-based systems to IP-enabled video surveillance is to move the application from targeting loss prevention, compliance, safety, and security to obtain a greater business value by increasing sales and reducing expenses and exposure to liability. Data-mining is the process of detecting some pattern in data. One application to video surveillance may be to analyze video feeds to detect certain colors or articles of clothing to identify groups of gang members among patrons at a shopping mall. Video analytics uses data mining techniques to detect patterns in data. Video analytics may be preformed at the endpoint (IP camera) on specialized digital signal processors (DSPs) by a third-party analytics vendor or by servers within the enterprise data center. One application of video analytics is to detect the queue length of checkout lines and inform management to increase or decrease the staffing at cash registers to more fully use staff.

In the future, the output of the analysis of video data may be more economically valuable than the loss prevention role of video surveillance to many retail organizations.