Design Considerations for IP Video Surveillance Over a PIN Architecture

At-A-Glance

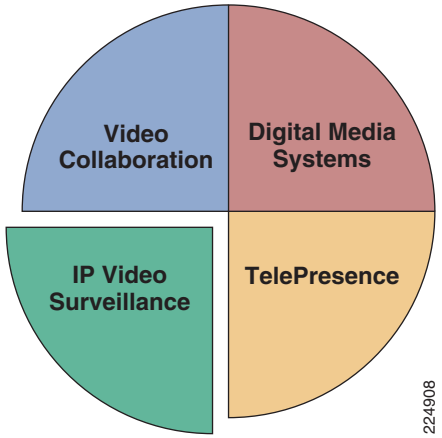
Benefits of Enabling IP Network-Based Video Surveillance

Video surveillance is a key component of the safety and security procedures of many organizations, providing real-time monitoring of the environment, people, and assets and providing recording for investigative purposes. The benefits of Cisco's Video Surveillance Solution include:

- Any-time, any-location access—Provides access to video at any time from any network location, within the constraints of available bandwidth, allowing remote monitoring, investigation, and incident response by remote physical security staff or law enforcement personnel
- Investment protection—Leverages existing investment in video surveillance and physical security equipment and technology.
- Network-wide management—IP cameras and servers are monitored and managed over a single network for fault, configuration, and centralized logging.
- Increased availability—IP networks offer a high level of redundancy that can extend to different physical locations.
- Scalability—The system can be expanded to new locations as business needs change.
- Efficient image processing—Digitized images can be transported and duplicated world-wide with no reduction in quality, economically stored, and efficiently indexed and retrieved.
- Interoperability—Employs an open, standards-based infrastructure that enables the deployment and control of new security applications from a variety of vendors.

The Cisco Video Surveillance Solution relies on an IP network infrastructure to link all components, providing high availability, Quality of Service (QoS), performance routing, WAN optimization, and privacy of data through IPSec encryption.

Figure 1 IP Video Surveillance

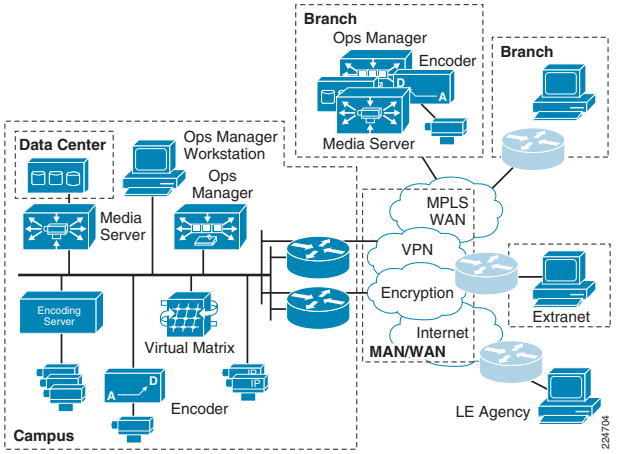


IP Video Surveillance Deployment Model

A typical IP Video Surveillance deployment in an enterprise network consists of one or more campus locations running Cisco Video Surveillance Media Server, Video Surveillance Operations Manager, and Video Surveillance Virtual Matrix on an Intel-based Linux Enterprise Server operating system. Deployment on stand-alone hardware is targeted at locations with more the 32 video surveillance cameras.

The branch locations are connected to the enterprise campus by WAN technologies, including Metro Ethernet, private line, the public Internet, or a MPLS VPN deployment. Cisco technologies, such as Dynamic Multipoint VPN (DMVPN), can overlay the WAN transport to provide data privacy and authentication by way of IPSec encryption. To ensure prioritization of voice, video, and mission critical applications over the WAN, QoS is deployed on the WAN; where multiple WAN links exist, Performance Routing (PfR) is enabled to provide intelligent path selection and the ability to route around brownouts and transient failures, beyond what can be provided by traditional routing protocols such as Enhanced IGRP (EIGRP).

Figure 2 IP Video Surveillance Deployment Model



Branches which have a requirement for 1-32 video surveillance cameras can incorporate the ISR Video Surveillance Modules to provide the Media Server and Operations Manager functionality in a network module form factor. Optionally, an Analog Video Gateway Module can be installed to support legacy analog cameras.

Branch offices and teleworker locations may view and administer the video surveillance system, as well as external organizations connected either through an Extranet or the public Internet, by way of a global IP connectivity and a Web browser. Figure 2 illustrates this topology and application services are described in more detail below.

IP Video Surveillance Application Services

The Operations Manager provides a Web-based browser console to configure, manage, display, and control video throughout a customer's IP network. Through this interface, one or more Cisco Video Surveillance Media Servers are managed, along with the definition of IP and analog cameras and scheduled and event-based video recording.

Camera feeds originate from both IP-based and analog cameras attached to stand-alone encoders or analog gateways. For example, the Cisco IP Video Surveillance Analog Video Gateway Module installed in the ISR branch router shown in Figure 2 can support up to 16 analog cameras. This branch router can also host a Cisco Video Management and Storage System Network Module to support both an Operations Manager and Media Server at the branch location.

In this remote branch location deployment, use of the VMSS provides efficiency; traffic only needs to traverse the network when requested by remote viewers. Branch office video remains localized and does not have to traverse wide area connections unless requested by users.

In this topology, physical security staff at the campus location, third-party location at an Extranet site, a separate branch, or even a remote teleworker location can configure, manage, and display the VMSS at the branch location. Video requests and video streams are delivered to the viewer using HTTP traffic (TCP port 80). Additionally, video surveillance archives can be captured and transferred to law enforcement agencies world-wide as still images or stored clips.

Network Protocols for Video Surveillance

Camera feeds traverse the IP network from the camera source to the Media Server either as Motion JPEG (MJPEG) or MPEG-4. MJPEG is typically transported via the TCP protocol. TCP provides guaranteed delivery of packets by requiring acknowledgement by the receiver. Packets that are not acknowledged are retransmitted. With MJPEG, each image stands alone, so the images that are displayed are of good quality.

MPEG-4 video is typically transmitted over UDP or Real-time Transport Protocol (RTP) or Real Time Streaming Protocol (RTSP). UDP does not guarantee delivery and provides no facility for retransmission of lost packets. UDP transport is most suitable for networks with very little packet loss and bandwidth that is guaranteed through QoS mechanisms. UDP transport does provide the option of IP Multicast (IPmc) delivery, where a single stream generated by the camera may be received by multiple endpoints, the Media Servers.

Branch/WAN and Campus PIN Design Considerations

Many of the existing network services deployed in the enterprise branch, MAN/WAN, and campus are applicable to IP Video Surveillance deployments. For example, in the campus, QoS marking at both Layer 2 (CoS) and Layer 3 (DSCP) can be enabled in the switching infrastructure to enhance the usability and quality of the video feeds. Cisco IP cameras support Cisco Discovery Protocol (CDP), Simple Network Management Protocol (SNMP), and Power-over-Ethernet (PoE), which simplify provisioning and device management. The cameras, servers, and encoders can be deployed on separate VLANs to provide isolation at Layer 2 and transported over the WAN with Layer 3 isolation over an MPLS VPN.

Such network fundamentals as QoS, path selection, optimization and rerouting by routing protocols such as EIGRP, OSPF, and Performance Routing (PfR) enhance the quality and guarantee a realistic video experience. IPSec technologies enable privacy, integrity, and authenticity of IP video surveillance data through encryption. Video services can also be secured behind firewalls. Application Networking Services, such as Wide Area Application Services (WAAS), are also a key element given that the transport for video viewing is TCP-based.

Video Storage Design Considerations

An archive is a collection of video data. The video source, a feed from a camera or encoder, can be stored in multiple locations and viewed at a later time. Archives are either One-Time, where the archive recording stops at a specified date and time, or Continuous Loop, where the archive continuously records. Loop archives reuse the disk space. Archives may also be scheduled to begin at a certain date and time and run using a recurring schedule.

The bit rate setting for MPEG-4 and frame rate settings for MJPEG specify the amount of bandwidth and storage space required for the video stream. The image size and quality also greatly influence these requirements. Bit rates for MPEG-4 range from 5Mbps to 56Kbps and frame rates for MJPEG range from 30 frames per second to over a frame per minute. Higher values generate more data every second, translating into smoother video and a more accurate representation of the field of view.

However, it also translates into larger archive file sizes. An 8-hour video feed with a target bit rate of 768kbps requires approximately 3 Gigabytes of disk storage.

WAN Bandwidth Design Considerations

Deploying a video surveillance solution through a WAN environment presents challenges that are not typically seen in a LAN. In a LAN environment it is common to see 1 Gbps and 10 Gbps of bandwidth, while in a traditional legacy WAN environment bandwidth is commonly less than 10 Mbps, with many locations operating on a single T1 (1.544 Mbps) or less.

However, by carefully considering the placement and bandwidth between the camera feeds and the Video Surveillance Media Server, it is possible to either archive the video data locally or, via high speed connectivity, to a central campus, while maintaining the ability to view cameras from any workstation within the enterprise network or globally through public Internet connectivity.

Summary

Access to video surveillance resources at any time from any network location is the driver for enabling the enterprise IP network to support video. Video surveillance traffic uses a combination of TCP and UDP as transport protocols and are easily provisioned by the enterprise QoS policies. Path selection and redundancy are optimized by features such as Performance Routing (PfR), while network services such as PoE, VLANs, and IPSec security simplify provisioning, isolation, and privacy of the video data. For more information, see: www.cisco.com/go/designzone