IP Video Surveillance 1.0 Solution Overview

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

This document summarizes high-level design recommendations and best practices to implement IP video surveillance on the enterprise network infrastructure. In some instances, existing network equipment and topologies have the necessary configuration and performance characteristics to support high-quality IP video surveillance. In other instances, network hardware might require upgrading or reconfiguration to support increased bandwidth needed to support video. Quality of service (QoS) techniques are important for any design because video has similar—in some instances, more stringent—requirements than VoIP for loss, latency and jitter.

IP video surveillance is a part of the medianet—a network initiative to incorporate all forms of video on the enterprise network. IP-based Video Surveillance is one of the four components of the medianet. These components consist of the following:

- TelePresence Network System
- Desktop Video
- Digital Media Systems
- IP Video Surveillance

This solution overview focuses on IP video surveillance while other overviews focus on the other three solutions. Not all forms of video on the enterprise network have the same requirements, given the diversity of transport techniques and user interfaces to the video feeds.

IP Video Surveillance Components

There are five components of all IP-based video surveillance solution. These are as follows:

- Cameras
- Video management software
- Servers
- Storage
- Network

The camera component is addressed by the Cisco Video Surveillance IP Camera, analog cameras attached to encoders, analog gateway network modules for the integrated services router, or third-party IP surveillance cameras.

The video management software is addressed by the Cisco Video Surveillance Manager (VSM) suite of software. This software runs on one or more standalone, Linux-based servers or on a Cisco Integrated Services Router (ISR) Series Video Management and Storage System network module.

The storage component is aligned with either the Data Center Architecture and the Cisco Video Surveillance Storage System, or with off-the-shelf iSCSI servers for archiving and storage of video feeds.

The network component is the enterprise network—the medianet. The primary focus of this document is to reference the existing Solution Reference Network Design baselines of Branch Office, Campus, WAN, and Metro Area Networks while building on this base of knowledge with IP video surveillance requirements, best practices, and design recommendations.

The IP video surveillance component of the medianet is integrated with the *Places in the Network* (PIN) architecture. along with the companion video components of the medianet.

Supporting Designs

Implementing IP video surveillance on an existing network is designed to overlay non-disruptively on other core Cisco PIN Architecture design elements. These include the following:

Each is summarized in the subsequent descriptions.

Quality of Service Design Considerations

QoS design is addressed in the *Enterprise QoS Solution Reference Network Design Guide Version 3.3* available at

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a008049b062.pdf

and should be considered a fundamental consideration for implementing video on any corporate network. Both voice and video are tolerant of some packet loss, latency, and jitter between the video end points; however, video is typically less tolerant to loss than voice over IP (VoIP). Depending on the type of video feed, the disruption of video quality might be evident for much longer periods of time than with VoIP.

Branch PIN Design Considerations

The Branch Architecture design collateral is organized under the Design Zone for Branch, which can be found at:

http://www.cisco.com/en/US/netsol/ns816/networking_solutions_program_home.html

From this web link, there are a number of branch-related PIN design guides which are applicable to implementing a branch router deployment. They include the following:

- *Enterprise Branch Architecture Design Overview*
- *Enterprise Branch Security Design Guide*
- *Enterprise Branch Wide Area Application Services Design Guide (version 1.1)*

The integration between IP video surveillance and the Enterprise Branch Architecture is targeted at integration of the Cisco ISR VS network modules. Enabling Branch Architecture services along with the Cisco ISR VS network modules is a key element of IP Video Surveillance 1.0

The Cisco Empowered Branch 4 marketing launch included the Cisco Video EVM-IPS-16A EVM Module featuring analog-to-IP encoding capabilities for existing analog cameras and the Cisco NME-VMSS Module which supports the Cisco Video Surveillance Manager (VSM) suite of software on the network module. The EVM-IPS-16A module is not required if the deployment is with all IP surveillance cameras.

Empowered Branch 4 also includes the Cisco 880 ISRs, which have sufficient performance characteristics to support the various forms of video at a Small Office/Home Office (SOHO) location. Many of the foundation architecture concepts from the *Business Ready Teleworker*

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008074f24a.pdf

The teleworker or SOHO deployment is applicable for addressing remotely located or isolated wired-IP cameras which in turn can be managed by a central or branch Video Surveillance Manager deployment. Video Surveillance Operations Manager viewing stations—PCs running an Active-X enabled web browser—may also be located at extranet or remote locations to allow physical security staff or law enforcement agencies to view live or archived video.

Application Networking Services (ANS), such as Wide Area Application Services (WAAS), are a key element given that the transport for IP video surveillance viewing stations is TCP-based.

WAN/MAN PIN Design Considerations

The WAN/MAN PIN Architecture reference is:

http://www.cisco.com/en/US/netsol/ns817/networking_solutions_program_home.html

There are several design guides within the Design Zone for WAN/MAN that describe foundation architectures for deploying IP video surveillance. The integration between IP video surveillance and the WAN/MAN Architecture is targeted at QoS, NetFlow, Network Based Application Recognition (NBAR), Ethernet access, Performance Routing (PfR) and implementing IP Security (IPSec) technologies to enable privacy, integrity, and authenticity of IP video surveillance data through encryption. Because of the focus on the Cisco ISR VS network modules in branch routers, the design guidance provided here relies heavily on integration of the WAN/MAN PIN.

If the branch office locations are implemented over a public network, the *Dynamic Multipoint VPN (DMVPN) Design Guide* provides important information on encrypting data between branch, SOHO, and central office locations. Because of the requirements for availability and selecting the optimal path among redundant links, the *Transport Diversity: Performance Routing (PfR) Design Guide* is also a key element in a successful deployment. Video requires much higher bandwidth than is required for a VoIP and data enabled branch location and the *Ethernet Access for Next Gen Metro and Wide Area Networks* might be applicable when implementing the branch office over a Metro Ethernet deployment or an Multiprotocol Label Switching (MPLS) Layer-2 pseudowire. Also applicable is the *Next Generation Enterprise MPLS VPN-Based MAN Design and Implementation Guide*.

Campus PIN Design Considerations

The Campus PIN Architecture reference is

http://www.cisco.com/en/US/netsol/ns815/networking_solutions_program_home.html

There are several design guides within this Design Zone for Campus that can provide guidance to the network manager in designing a campus medianet. These include the following:

- *Network Virtualization—Path Isolation Design Guide*
- *Network Virtualization—Services Edge Design Guide*
- *Campus Network for High Availability Design Guide*
- *Campus Design: Analyzing the Impact of Emerging Technologies on Campus Design*

The existing *Cisco Video Surveillance Manager Solutions Reference Guide* can be found at the following URL:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9145/ps9152/design_guide_c07-462879.pdf

That publication references the application recognition services, QoS marking, and design requirements for a campus-based Video Surveillance Manager deployment at a campus or central location. That existing design guide will be superseded by a IP Video Surveillance 1.0 design guide at a future date.

The integration between IP video surveillance and Campus PIN Architecture is a requirement because most IP network cameras support Power over Ethernet (PoE). PoE is important to facilitate installation of these cameras as a single Category 5 Ethernet cable can provide both Ethernet connectivity and power-reducing installation costs. The Cisco IP cameras support Cisco Discovery Protocol (CDP) and Simple Network Management Protocol (SNMP), which together help to simplify provisioning and device management.

In the campus, QoS marking at both Layer 2—class of service (CoS)—and Layer 3—Differentiated Services Code Point (DSCP)—can be enabled in the switching infrastructure to enhance the usability and quality of the video feeds.

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 virtual private network (VPN).

Data Center PIN Architecture

The Data Center PIN Architecture reference links can be found within the Design Zone for Data Centers at the following URL:

http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html

The integration between IP video surveillance and the Data Center PIN Architecture intersects notably at the storage requirements of an IP video surveillance system. 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 storage requirements for video archives can be substantial. For example, a High Definition (HD) surveillance camera recording at a rate of 10 motion JPEG frames per second with a resolution of 1600 x 1200 pixels can require up to 1GB of disk storage *per hour*. Retention of this archive for days or weeks, combined with a deployment of a hundred cameras will consume vast amounts of storage.

The *Cisco Video Surveillance Manager Solutions Reference Guide* addresses at a functional level the way in which the storage subsystem of the Cisco Video Surveillance Media Server can augment internal storage with direct-attached storage and storage area networks (SANs). Additionally, the Cisco ISR Series Video Management and Storage System network module supports an iSCSI interface for local storage in the branch office.

Technical Assistance Center (TAC

Technical Assistance Center (TAC) Technical Tips are a valuable sources of configuration examples for the technologies deployed in this design guide. Please refer to the Technical Tip section after logging on the Cisco TAC cisco.com page at http://www.cisco.com/tac.

Solution Description

In this section the, Cisco Video Surveillance Solution is described at a functional level given a deployment of the components on standalone workstations and appliances. In addition, the functional components are mapped to an implementation using the Cisco 2800/3800 ISR IP Video Surveillance Network Modules. The Cisco Video Surveillance Manager software is a common code base that is ported to run on the network module.

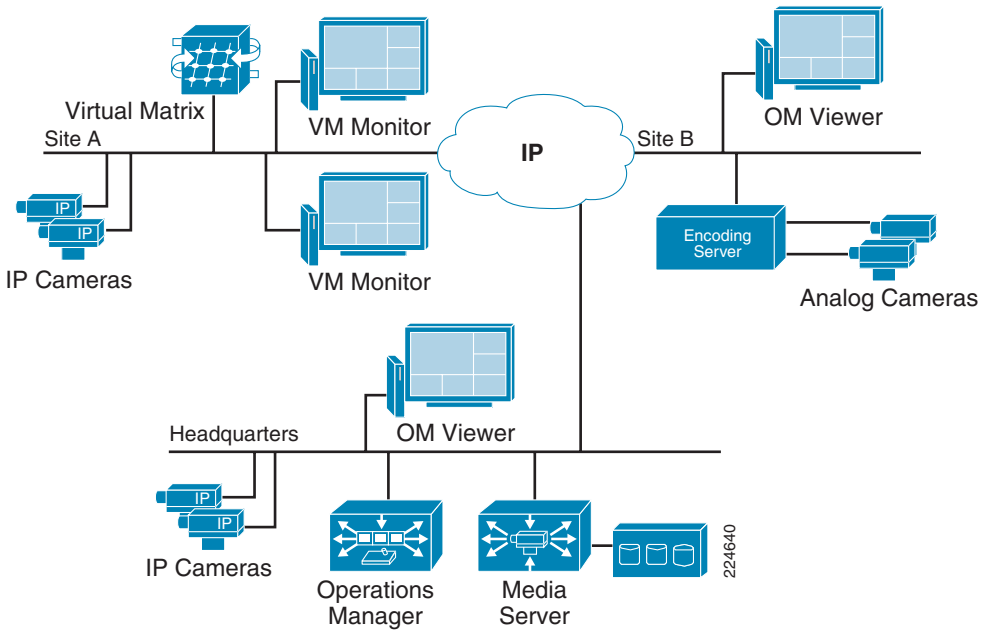
Cisco Video Surveillance Solution

The Cisco Video Surveillance Solution relies on an IP network infrastructure to link all components. The designs of a highly available hierarchical network have been proven and tested for many years and allow applications to converge on an intelligent and resilient infrastructure.

Cisco offers a unique approach to moving different proprietary systems to a common IP backbone. This approach leverages other Cisco technologies, such as network security, routing, switching, network management, and wireless. Video from IP cameras can now be truly converged into a robust network environment with the intelligence and flexibility provided by the Cisco infrastructure.

Figure 1 shows the Cisco Video Surveillance Manager solution using an Intelligent IP infrastructure as a transport.

Figure 1 Cisco Video Surveillance Solution



Solution Components

The following components make up the Cisco Video Surveillance Solution:

- *Cisco Video Surveillance Media Server*—As the core component of the network-centric VSM, this software manages, stores, and delivers video for the network-centric video surveillance product portfolio.
- *Cisco Video Surveillance Operations Manager*—The Operations Manager authenticates and manages access to video feeds. It is a centralized administration tool for management of Media Servers, Virtual Matrixes, cameras, encoders, and viewers—and for viewing network-based video.
- *Cisco Video Surveillance Virtual Matrix*—The Virtual Matrix monitors video feeds in command center and other 24-hour monitoring environments. It allows operators to control the video being displayed on multiple local and remote monitors.
- *Cisco Video Surveillance Encoding Server*—This single-box solution encodes, distributes, manages, and archives digital video feeds. Each server encodes up to 64 channels and provides up to 12 TB of storage.
- *Cisco Video Surveillance Storage System*—This complementary component allows the Media Server's internal storage to be combined with direct-attached storage (DAS) and storage area networks (SANs). The storage system allows video to be secured and accessed locally or remotely.

Cisco 2800/3800 ISR IP Video Surveillance Network Modules

In addition to the standalone dedicated implementation of the Cisco Video Surveillance Solution on Linux servers, the Cisco 2800 and Cisco 3800 ISRs support the necessary components of the solution to implement a self-contained instance at the branch location.

The Cisco Video Management and Storage System (VMSS) Network Module implements the Operatons Manager and Media Server functions for the branch. It supports IP based video cameras as well as analog cameras attached to the Analog Video Gateway Module.

The Analog Video Gateway Module installed in the Cisco ISR branch router provides support for analog cameras, analog Pan Tilt Zoom (PTZ), alarm input and control relay output. It supports up to 16 analog cameras. This module supports RS-485 on two serial interfaces, which controls analog Pan Tilt Zoom (PTZ). The module also supports event alerts by way of alarm input and control-relay output serial connections. The Analog Video Gateway Module is optional if these functions are not required.

A branch with all IP cameras and no analog requirments need only the VMSS network module. The NME-VMSS-16 and NME-VMSS-HP16 support up to 16 cameras, the NME-VMSS-HP32 is licensed to support up to 32 cameras.

The Virtual Matrix component is not supported on the Cisco ISR Video Surveillance Modules.

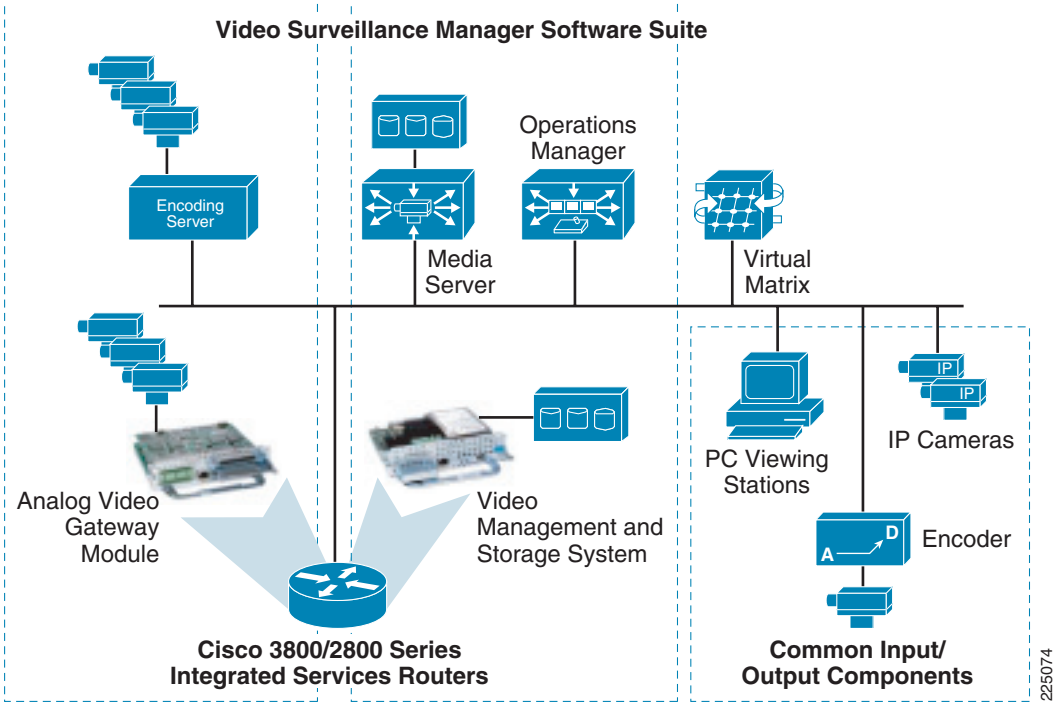
The Operations Manager provides a web-based browser console to configure, manage, display, and control video supported at the branch location. The Operations Manager and the Media Server share the same IP address configured on the logical interface of the Integrated Services Network Module. One or more Cisco Video Surveillance Media Servers are managed through this interface. The Operations Manager web interface is where the physical security administrator configures IP and analog cameras and where video feed archives are secheduled and managed.

In this remote branch location deployment, use of the Cisco 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. An external iSCSI device is attached to the GigabitEthernet port on the network module in order to supplement the disk storage on the VMSS module.

In this topology, physical security staff at the campus location, a 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 via Hypertext Transfer Protocol (HTTP) which uses Transmission Control Protocol (TCP) port 80.

In Figure 2, the Video Surveillance Manager Software Suite components for both the Linux deployment and the Cisco ISR IP Video Surveillance Network Module deployment are shown.

Figure 2 Video Surveillance Manager Software Suite Components



At the branch location, the Analog Video Gateway Module provides a similar function to the encoding server. The Media Server and Operations Manager, along with storage, are supported on the VMSS network module. The Virtual Matrix function is not supported on the Cisco ISR Video Surveillance Modules. The IP cameras, analog cameras attached to dedicated IP encoders, and the PCs used as viewing stations are common to both implementations.

Solution Benefits

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

- Provides access to video at any time from any network location within the constraints of available bandwidth, allowing remote monitoring, investigation, and incident response via remote physical security staff or law enforcement personnel.
- 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.
- Digitized images can be transported and duplicated worldwide with no reduction in quality, economically stored, and efficiently indexed and retrieved.
- 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, QoS, performance routing, WAN optimization, and privacy of data through IPSec encryption.

Solution Scope

This publication will be extended and updated over time as capabilities expand the addressable market. The associated design guide focuses on the following:

- Video Surveillance Manager solution overview (as presented in this publication)
- Implementing the Cisco ISR Video Surveillance Modules
- Video surveillance traffic flows
- QoS for IP video surveillance
- Bandwidth and archival planning and provisioning
- Protocols and features
- PfR of video surveillance
- WAAS optimization of IP video surveillance
- Application requirements
- Network deployment models
- Video storage requirements
- IP based surveillance camera deployment and provisioning

Other features that were not evaluated for initial revision of the associated design guide include the following:

- The Stream Manager product offering is covered in other design guides. These design guides can be found at www.cisco.com/go/designzone.
- Wireless deployments of IP cameras based on IEEE 802.11 wireless LANs
- Audio surveillance
- IP Multicast based deployment scenarios

Solution Overview and Best Practices

This section presents a high-level overview of an IP Video Surveillance deployment to give the reader a quick reference as to the capabilities of this solution. The associated design guide will then go into detail on planning, design, product selection, and implementation of an IP Video Surveillance deployment.

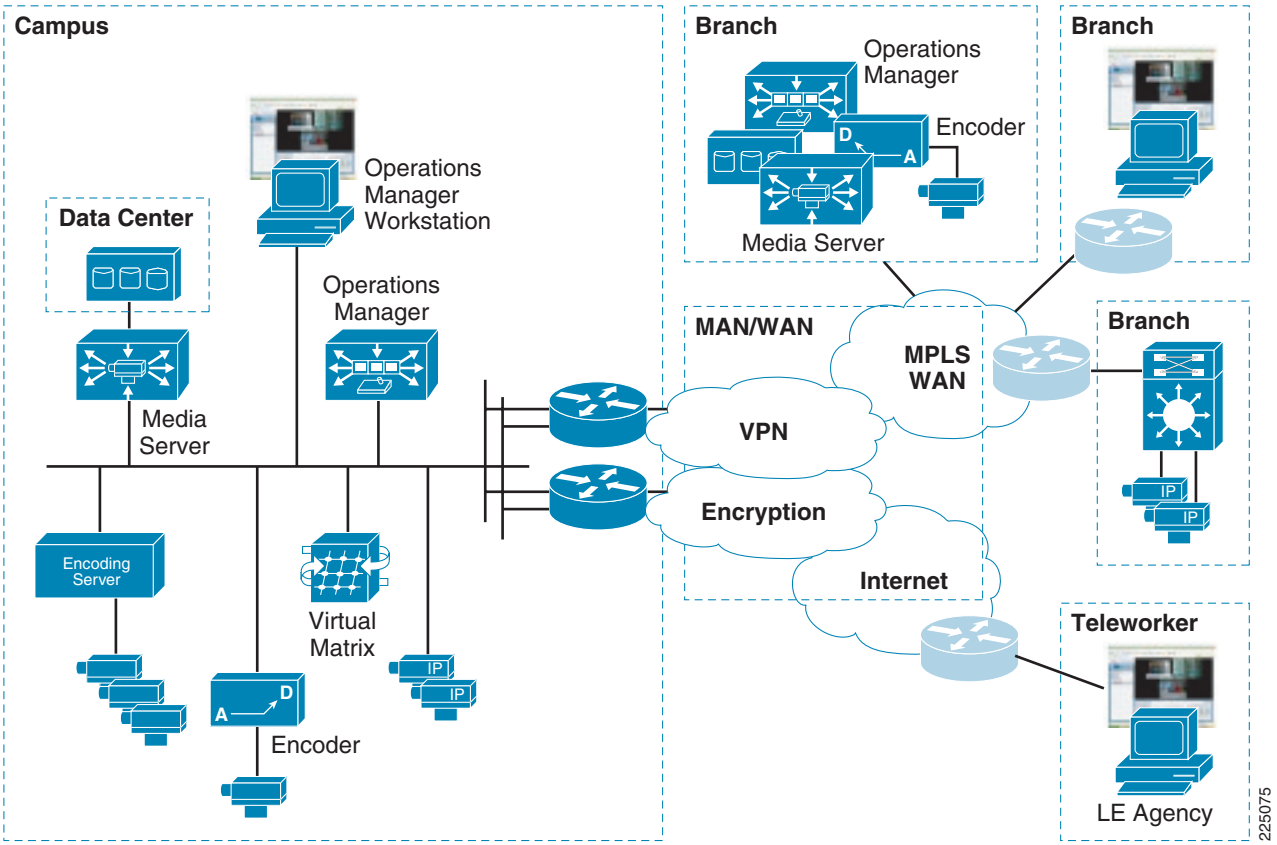
Deployment Model

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 standalone hardware is targeted at locations with more than 32 video surveillance cameras.

Branches which have a requirement for 1-to-32 video surveillance cameras can incorporate the Cisco 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 may external organizations connected either through an Extranet or the public Internet by way of a global IP connectivity and a web browser. Figure 3 illustrates the topology and application services deployed in an enterprise-wide implementation of IP-based video surveillance.

Figure 3 Video Surveillance Solution Master Architecture Diagram



The branch locations are connected to the enterprise campus by WAN technologies, including Metro Ethernet, private line, the public Internet, or a Layer-2 or Layer-3 MPLS VPN deployment. With a Layer-2 MPLS deployments (*Pseudowire*), IP cameras may be Ethernet-attached to a remote switch and have images transported through the carrier network and provisioned and managed by the Operations Manager at either a branch location or a central location. Branches attached by way of a Layer-3 MPLS network, leased line, or over the Internet can support viewing stations and IP cameras that can be managed by either the campus or branch deployment.

Cisco technologies such as DMVPN can be overlaid onto 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, PfR can be enabled to provide intelligent path selection and the ability to route around brownouts and transient failures, thereby enhancing what can be provided by traditional routing protocols such as Enhanced Internal Gateway Routing Protocol (Enhanced IGRP).

The decision as to whether a specific environment should implement the Cisco ISR Video Surveillance Modules at a branch location and archive data at the branch—or provision cameras off the campus implementation of the Cisco Video Surveillance Manager—depends on the number of cameras, the resolution, frame or bit rate of the camera, quality factors of the cameras, and the cost and availability of bandwidth at the remote locations. In cases where implementing cameras is the only requirement, it may be practical to transport the camera feeds across the WAN for archiving. However, in most deployments, local storage is necessary due to the bandwidth required and the costs associated with this bandwidth.

Solution Characteristics

Table 1 represents the general solution characteristics for an IP video surveillance deployment

Table 1 Solution Characteristics Summary

Solution Characteristics
An IP network infrastructure is required to link all components.
IP cameras are under the control of and feed Media Servers. The VSOM interface is the viewing station portal into the video archives and live feeds.
The amount of disk storage for archiving camera feeds depends on factors that include the retention period requirements, image resolution, image quality, format and encoding. Storage requirements might be difficult to plan and predict.
Encryption through IPSec may be implemented between video endpoints to insure data privacy, integrity, and authentication.
VRF-lite, VLANs, and other network virtualization techniques may be used to segment the video endpoints and servers.
Viewing stations are PCs running Internet Explorer (IE) with Active-X controls. The PC must have a sufficient CPU clock rate to decode the video feeds.
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 the User Datagram Protocol (UDP), 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 provides the option of IP Multicast (IPmc) delivery, however is not universally supported.
Deploying a video surveillance solution through a WAN environment presents challenges that are not typically seen in a LAN. WAN bandwidth is most costly and the available transport types are dependent on the service provider offering available in the geographic area.

General Best Practices Guidelines

Table 2 presents a list of best practices that have been established through a combination of design experience, scalability and performance evaluation, and internal Cisco trials.

Table 2 IP Video Surveillance Best Practices Guidelines Summary

Best Practices Guidelines
Network Time Protocol (NTP) must be configured for an accurate and consistent time source for all video surveillance devices in the network.
Camera feeds for MJPEG can be reduced to save bandwidth and disk storage. For example, 30 frames per second (fps) can be configured from camera to Media Server, while two archives for this feed can be configured; one at 10 fps and a second at 1 fps. These archives can have different retention periods.
Access control techniques to limit the workstations that are allowed to configure and view an IP camera directly should be implemented.
Where possible, use PoE for IP cameras. It simplifies installation.

Table 2 IP Video Surveillance Best Practices Guidelines Summary

Best Practices Guidelines
IP video surveillance traffic is to be marked with the QoS DSCP value of CS5 and provisioned in either a priority or bandwidth queue.
Cisco IP Video Surveillance (IPVS) Utilities for the Cisco ISR Analog Gateway Module can be accessed with the following URL: http://*ipaddress*/ipvs/login.html, where *ipaddress* is the IP address of the analog network module. This utility facilitates implementation of analog cameras, RS-485 devices, alarms and contract relays.
In most instances, configuring a camera feed constant bit-rate (CBR) value of 1024Kbps is an acceptable starting value for reasonable video quality.
Most implementations will require at least 4CIF or D1 video resolution for reasonable video quality.
MPEG-4 over RTP/UDP is relatively intolerant to packet loss; however, latency and jitter cause less degradation because the Media Server functions as a dejitter buffer (due to the storage and replication of the camera feed to the viewing station). Manage WAN links to minimize loss, even at the expense of latency and jitter. Round Trip Times (RTT) of 300 msec might be acceptable.
Latency between client viewing station and VSOM should be less than 80 msec RTT for best results.
Many IP cameras can be configured as both MJPEG or MPEG-4 codec technology. Both have advantages and disadvantages. A mixture of these codecs on certain cameras might be desirable.
In most instances, the only manual CLI configuration required on the Cisco ISR Analog Gateway Module would be text descriptions of the physical ports. VSOM will provide all the configuration necessary for operation of this module when adding cameras or alarm events.

General Solution Caveats

Table 3 presents a list of caveats for the solution described in this solution overview.

Table 3 IP Video Surveillance Solution Implementation Caveats

Solution Implementation Caveats
The available disk storage for video archives on the Cisco ISR Video Surveillance Modules is approximately 100 GB. In most deployments, external disk archives storage is required.
Not all features of the Cisco 2500 Series Video Surveillance IP camera are supported by Cisco VSM. For example, the IP camera supports IP multicast, but VSM does not. QoS can be enabled on the IP camera by configuring the camera directly through a supported web browser, but the QoS parameters cannot be configured from VSM.
Some HD cameras only support the higher definition resolution on MJPEG.
The latency of video encoders used in some IP cameras might exceed 500 msec, and values of 2,000 to 3,000 msec have been observed. This presents usability issues when using the audio and speaker jacks of the camera or with PTZ controls.
When defining analog cameras under VSOM using the Cisco ISR Analog Gateway Module, the Encoder Channel field is not zero relative. In other words, Encoder Channel 1 is coax cable 0 on the CAB-EVM-IPVS-16A.
When defining alarms/control relay events in the Cisco ISR Analog Gateway Module, VSOM port COM1 equates to S0, while COM2 equates to S1. Contact closure port 0 equates to Channel 1in VSOM.
When defining PTZ analog cameras in VSOM, *Chain Number* equates to the RS-485 address switch value on the camera.
When defining Bosch Autodome analog cameras with PTZ on the Cisco ISR Analog Gateway Module, use *Pelco Analog Camera (D protocol)* rather than selecting *Autodome Analog Camera*.

Table 3 IP Video Surveillance Solution Implementation Caveats

Solution Implementation Caveats
The PTZ analog device is intermittently unresponsive to joystick movements from the Video Surveillance Operations Manager (VSOM). See CSCsk21927.
Symptom—Video image does not load on the upper first pane on various layouts with VMR enabled. *Workaround*—Disable VMR mode in the VSOM under *Settings* if this problem occurs.
In some instances, there may be a delay of several seconds, up to a minute, from the time an operator selects a camera feed to view, until the video feed is displayed. It may require several mouse clicks on the camera feed to initiate viewing.
Cannot configure VSVM on the Cisco ISR Video Surveillance Modules. Error “Cannot connect to server at 192.0.2.2:8086” is displayed. VSVM is not supported on the network module implementation.
There are incompatibility issues when a NAT/pNAT device is located between the client viewing station and the VSOM.
In VSOM, previews are displayed when you configure JPEG but not with MPEG-4.
Recurring archives might stop initiating if the disk media becomes full.

References

Refer to the medianet documents at:

www.cisco.com/go/designzone