White Paper

Cisco Video Surveillance Manager: Realize the Promise of the "Internet of Everything" for Safety and Security

What You Will Learn

The Internet is becoming the Internet of Everything, connecting people, processes, data, and things at unprecedented scope and scale. This white paper, intended for safety and security and IT professionals in organizations of all sizes, explains new features of Cisco® Video Surveillance Manager that help you take advantage of the Internet of Everything to protect people, property, and assets:

- A choice of validated architectures helps provide end-to-end security support from dozens of cameras in one building to more than one million cameras providing coverage over an entire city or region.
- The same size IT team can support much larger deployments, using a visual management interface with medianet capabilities.
- Cisco Video Surveillance IP Cameras provide new capabilities, such as the ability to add additional functionality by installing applications or on-camera video storage for special deployments.

The Internet of Everything: How It Transforms Safety and Security

Traditionally, video surveillance cameras were connected to a separate network, increasing costs and restricting viewing of video feeds to consoles connected to the same network. More recently, organizations have begun connecting their cameras to their existing IP network. This is part of a global trend called the Internet of Everything, referring to burgeoning connections between people, process, data, and things, including video surveillance cameras and physical access controllers.

The Internet of Everything is transforming safety and security operations. For example, situational awareness improves because mobile personnel can receive alerts and view video from anywhere, on any device, including tablets and smartphones. In addition, you can automate response to events by integrating different safety and security systems connected to the same network—for example, by capturing video in response to gunshots or an opening door.

To capitalize on the potential of the Internet of Everything for video surveillance, you need:

- **A secure architecture that can adapt to evolving business needs.** This might include adding many more cameras, capturing high-resolution video to enable facial recognition, or storing video from vehicle-mounted cameras on the cameras themselves when the vehicle loses connectivity. Today, supporting requirements like these typically requires costly efforts such as rebuilding the infrastructure or replacing cameras.
- **Automated processes to minimize management overhead.** The challenge is not simply making the deployment work, but making it work with your existing resources. Adding ten times more cameras is not economically feasible if it requires ten times more staff.

- **Simplified troubleshooting and remediation.** To maintain high video quality, the IT team needs to find out about quality issues without having to wait for user reports, and needs easy-to-use tools to quickly pinpoint and remediate the source of the issue.

Cisco Video Surveillance Manager meets these requirements. It works with analog and digital cameras from any vendor, and provides even more advantages when used with Cisco Video Surveillance IP Cameras.

Following are major benefits of Cisco Video Surveillance Manager in the age of the Internet of Everything.

1. Connect a Practically Unlimited Number of Cameras, and Distribute Live Video to Mobile Security Officers in Any Location

Today's challenge: Today, most organizations cannot easily scale their video surveillance deployments. If you have media servers in multiple locations, safety and security officers probably need to log in separately to each location's media server to view video from that location. That means monitoring feeds from 50 sites requires logging in to 50 different servers. In addition, mobile security officers on their way to an incident scene cannot view live video, impeding situational awareness.

Solution: Proven, secure architectures for Cisco Video Surveillance Manager support any size deployment, from dozens of video surveillance cameras in a single building, to more than one million cameras providing coverage over an entire city, region, or country (Figures 1, 2, and 3). All architectures provide end-to-end security that includes role-based access, 802.1x authentication, traffic encryption, firewalling, and intrusion detection and prevention. Security personnel can view live video securely from anywhere with wireless coverage, using an Android tablet or smartphone with the Cisco Video Surveillance Operations Manager Mobile Viewer.

Figure 1. Centralized Data Center Architecture, Centralized Management

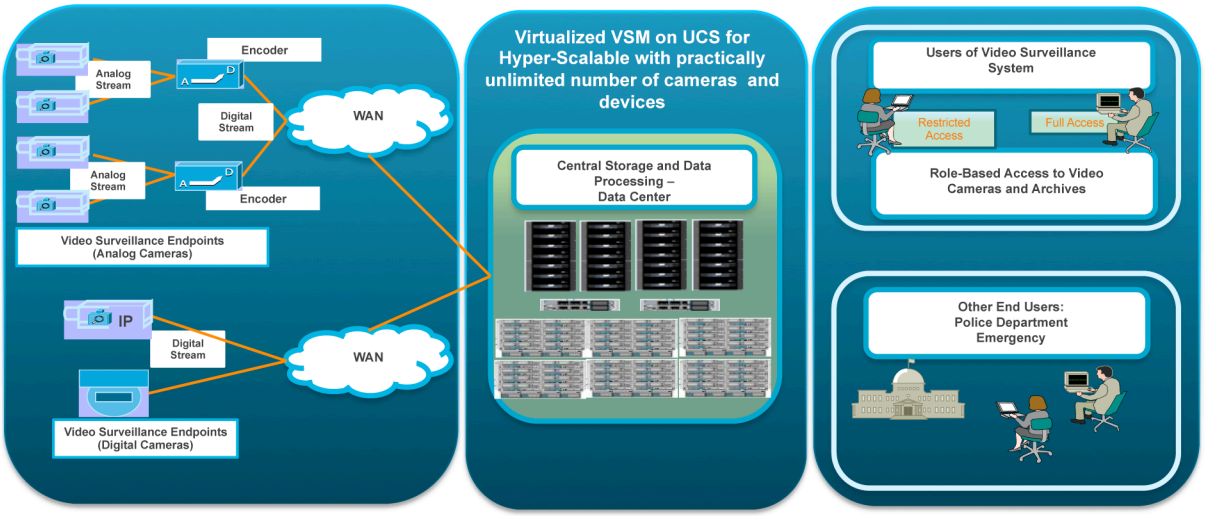


Figure 2. Distributed Architecture, Centralized Management

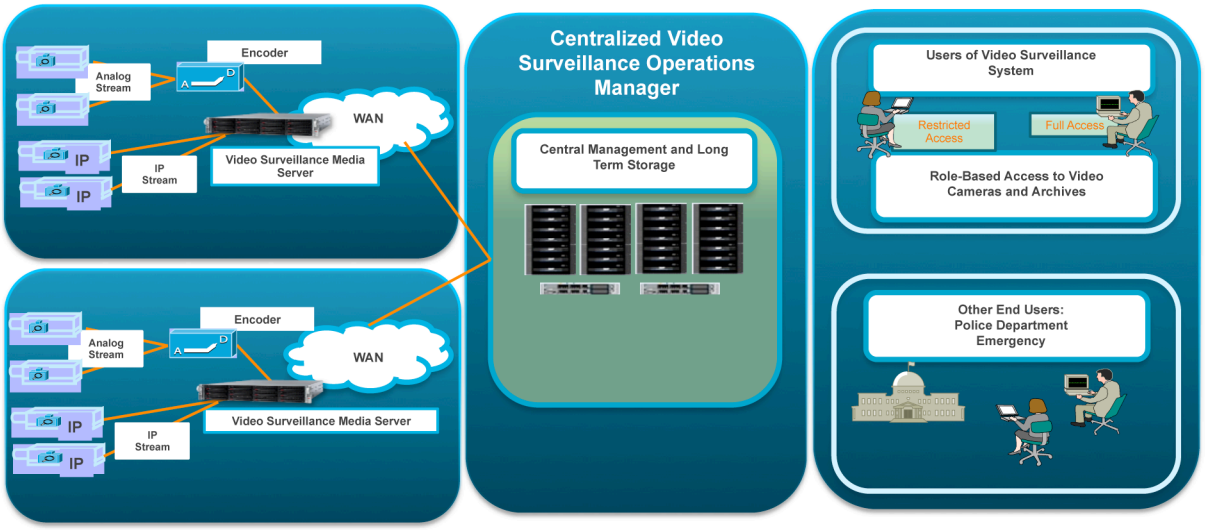
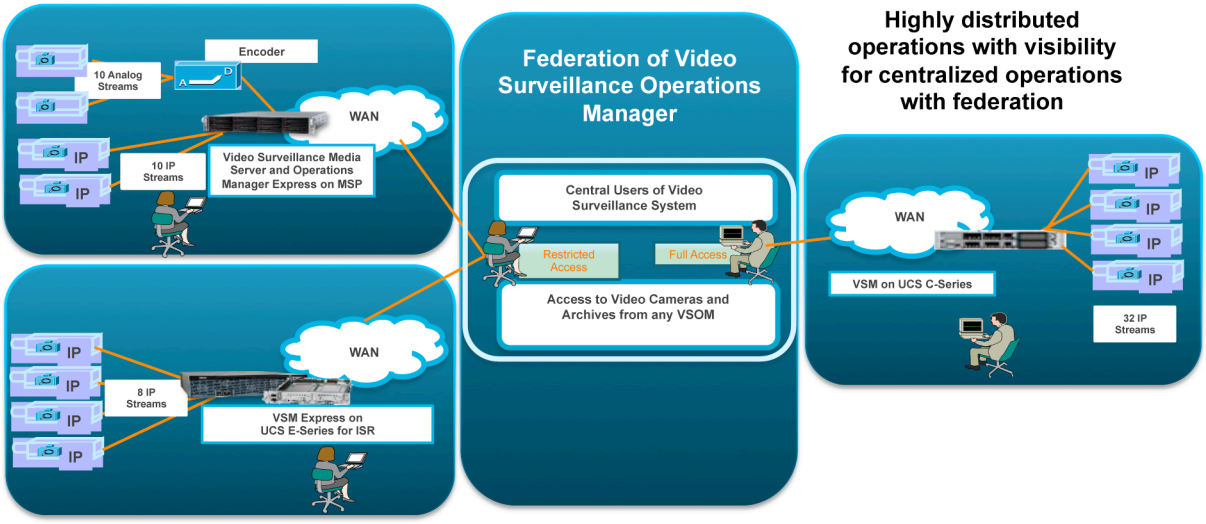


Figure 3. Distributed Architecture, Distributed Management



Safety and security personnel can monitor all camera feeds with a single sign on from the VSOM Federator. A federal government agency uses the VSOM Federator to monitor video surveillance cameras at approximately 1000 offices. Each office has its own Cisco Video Surveillance Operations Manager server so that it can continue collecting video if the network connection to headquarters is lost. From the Federated Server at headquarters, administrators can view video from any camera, in any office.

2. Simplify Troubleshooting and Issue Resolution

Today's challenge: Traditionally, IT departments found out about video quality issues only after the safety and security team reported them. Pinpointing the source of performance issues required time-consuming event correlation. Resolving issues required learning to use a complex command-line interface (CLI).

Solution: Use Cisco Video Surveillance Manager in conjunction with LiveAction software from ActionPacked Networks, a Cisco Developer Network partner. In the operations center, IT personnel receive alerts on the LiveAction console when latency, packet loss, or jitter dips below a specified threshold. LiveAction visually presents the end-to-end flows from the camera to the media server (Figure 4). The IT administrator can execute a Mediatrace on the affected flow by selecting it and choosing a command. LiveAction visually presents the results, using arrows to point to the network devices responsible for the congestion (Figure 5). Using the same user interface, IT personnel can use the LiveAction QoS Monitor to adjust the policy for bandwidth, shaping, or other QoS parameters, pushing them to the device nearest the congestion (Figure 6). LiveAction allows you to quickly identify the source of video quality issues and remediate them in minutes.

Figure 4. LiveAction Provides Visualization of End-to-End Flows, Accelerating Troubleshooting

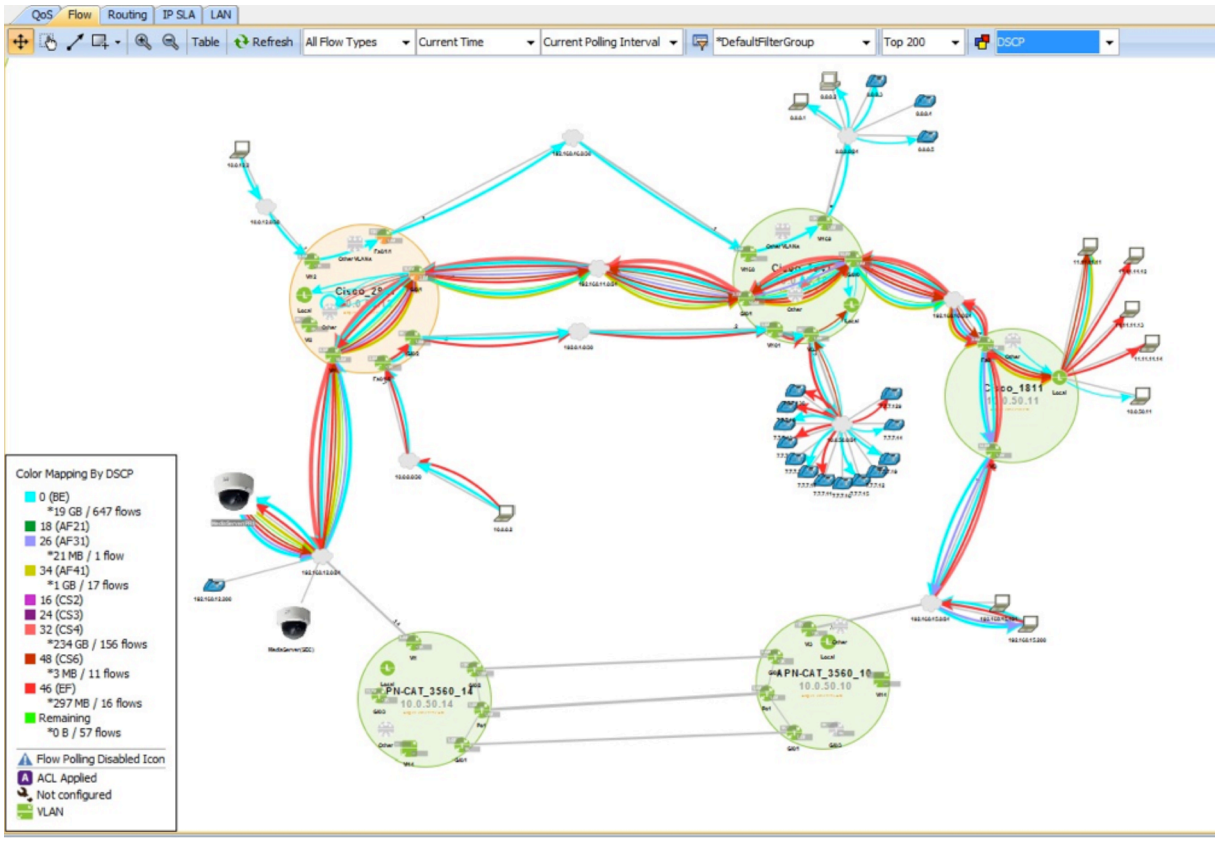


Figure 5. Quickly Identify the Source of Performance Issues with LiveAction Mediatrace Capability

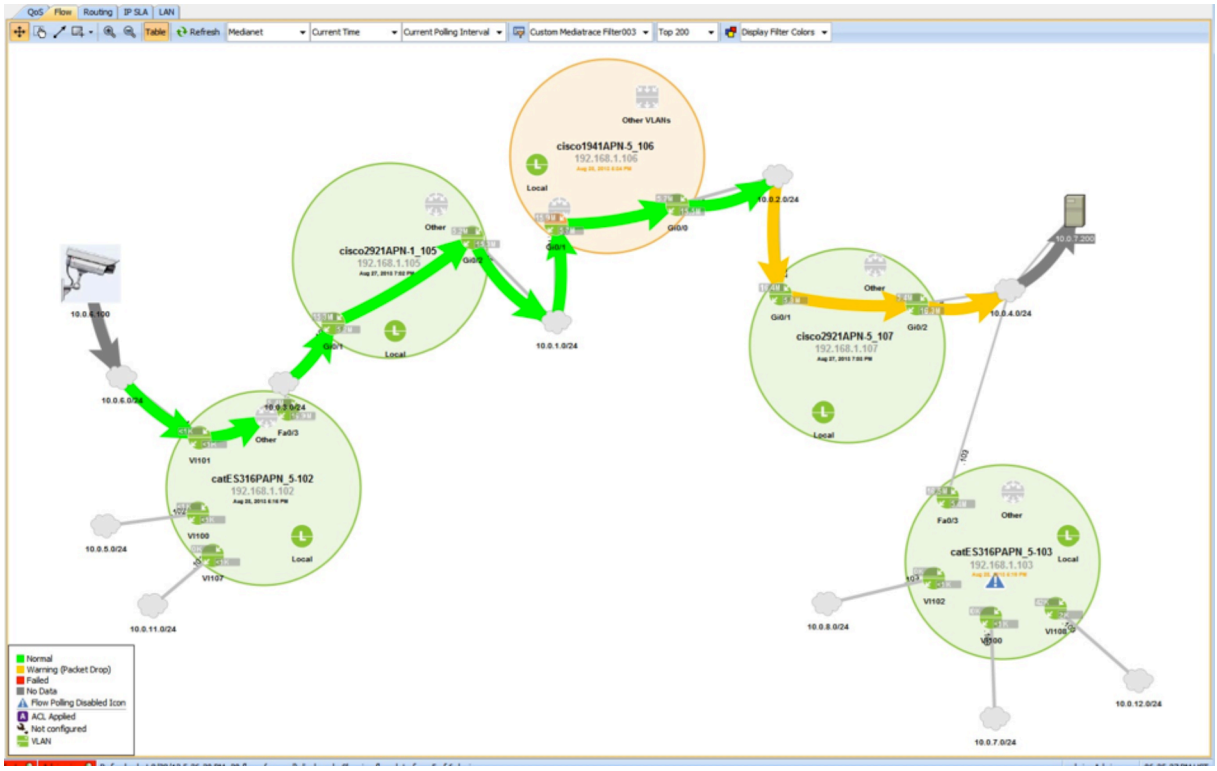
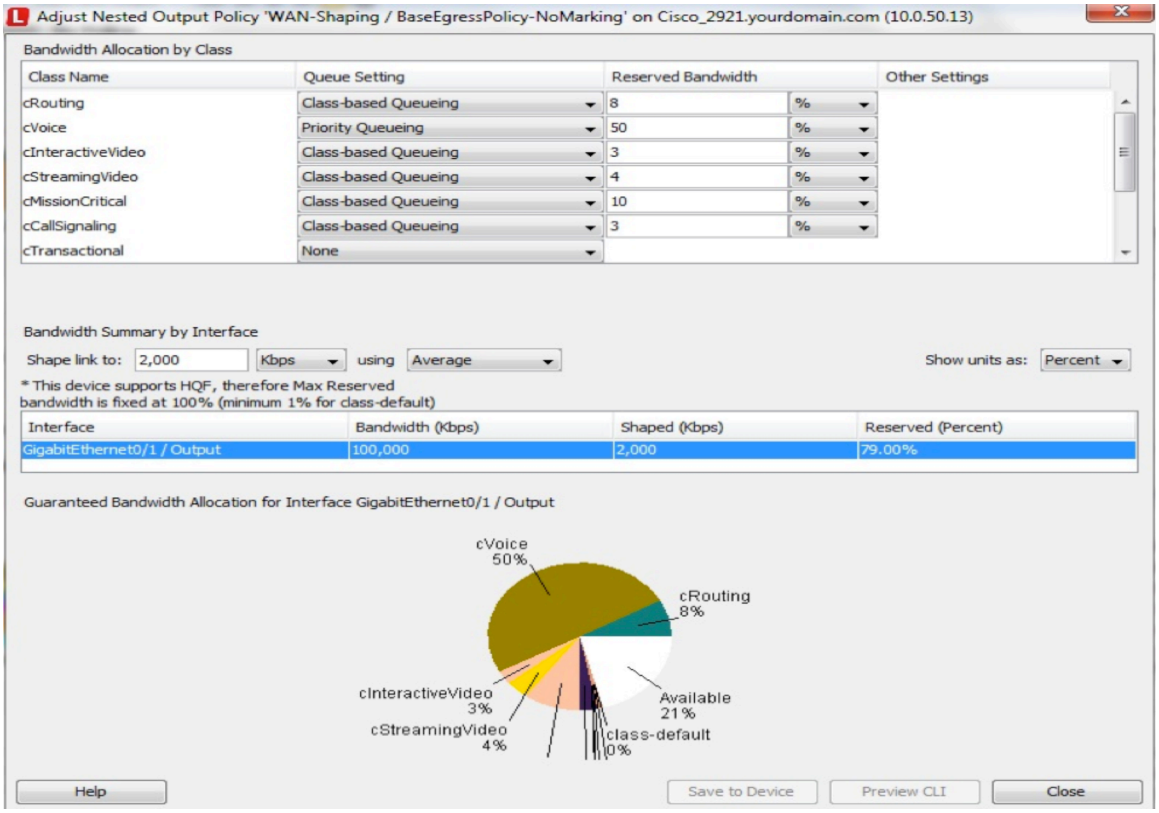


Figure 6. Dynamically Adjust QoS Policy to Resolve Video Quality Issues



3. Enable Multiple Viewers to View the Same Live Video Feed without Degrading Video Quality

Today's challenge: During events like robberies or disasters, multiple people at headquarters might want to simultaneously monitor real-time video from a single branch office. Today, however, quality worsens with each new video stream flowing over the WAN, and some people might not be able to view the stream at all.

Solution: Deploy Cisco Dynamic Proxy at the central site. When the first person requests a live stream, Dynamic Proxy retrieves it. When other people at the same location subsequently request the stream, Dynamic Proxy distributes it over the local network. Using a proxy preserves video quality by not overloading either the media server or the WAN.

Unlike multicast, which can take months of fine-tuning to work properly, Dynamic Proxy typically begins working within an hour. You simply select the option and answer a few questions.

4. Operational Efficiency Through Analytics

Challenge: Today, acquiring new analytics capabilities requires adding analytic software to existing video surveillance systems or purchasing new cameras with onboard analytics, which can be difficult to cost-justify. For this reason, many organizations have put off adoption of valuable new safety and security innovations such as video analytics, audio and location-based analytics, and metadata analytics. The use of metadata information within a video surveillance system enables innovative applications and the ability to share intelligence across connected people, processes, data, and things.

Solution: Video Surveillance Manager provides the ability to generate motion metadata on post recorded video and making it searchable for the user. This will speed up the time it takes to investigate any incident across a large number of cameras and recorded video.

5. Add Intelligent Cameras

Today's challenge: Video surveillance cameras on vehicles, such as buses, trains, law enforcement vehicles, or a Cisco Networked Emergency Response Vehicle (NERV), occasionally lose their wireless connection. Failure to store the video for later retrieval can lessen situational awareness, hamper incident review, and prevent public safety agencies from defending themselves in lawsuits.

Solution: To store video captured from vehicles when connectivity is absent, deploy Cisco Video Surveillance IP Cameras. When these cameras move out of the mobile coverage range, they store video locally. When connectivity resumes, they automatically transmit the stored video to the media server. You can configure the cameras to transmit stored video over either a Wi-Fi or 3G/4G cellular connection, or only over a Wi-Fi connection.

Onboard camera storage is supported with all models of the Cisco cameras. The Cisco 6050 is a 1080p, compact camera suitable for transportation applications such as buses, trains, and other vehicles. The camera is IP67 rated and designed to withstand shock, vibration, humidity, and dust, maintaining stable and reliable video during vehicle movement. Furthermore, the IK10 rated metal housing effectively provides robust protection from vandalism. The combination of high-resolution imaging and protective housing gives the Cisco 6050 the rugged reliability required to maximize passenger safety and optimize mobile surveillance.

Additionally, Cisco IP Cameras are much more than just cameras. Cisco offers a software development kit that allows the development of applications that can be run directly on the cameras. Application such as simplified video analytics, audio analytics, and IP telephony clients add intelligence at the edge and reduce the need for dedicated personnel to monitor video data. Applications will all be tested and certified by Cisco and can be managed on the camera directly or through VSM.

Conclusion

Today's Internet of Everything gives organizations an opportunity to increase the efficiency and effectiveness of their safety and security operations by bringing together more people, process, data, and things. New capabilities in Cisco Video Surveillance Manager help you realize the promise. Proven architectures with end-to-end security support a practically unlimited number of cameras. Safety and security personnel can monitor video from any camera with a single sign on, or use a mobile app on a smartphone or tablet. And as your deployment grows, you can manage it without a large increase in IT staff. Easy-to-use management tools harness medianet technologies to simplify troubleshooting and issue resolution, helping to provide the high-quality video needed for incident detection and informed response.

For More Information

Please visit, http://www.cisco.com/en/US/products/ps10818/index.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-729589-00 09/13