Designing Cisco Video Surveillance VM Deployment on Cisco UCS Platforms, Release 7

Revised: April 25, 2014

This guide summarizes high-level design recommendations and best practices for implementing Cisco Video Surveillance (Cisco VSM) virtual machines (VMs) on the Cisco Unified Computing System (UCS) B-, C-, E- and Express Series platforms.

Tip See the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms for additional information.

Contents

This document includes the following sections:

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

Introduction

This guide summarizes high-level design recommendations and best practices for implementing Cisco Video Surveillance on the following platforms:

- Cisco UCS B- and C- Series platforms
- Cisco UCS Express and E- Series platforms on the Integrated Services Router Generation 2 (ISR G2)

Note This guide does not describe the configuration and operation of the Cisco Video Surveillance (Cisco VSM) products or the deployment of the Cisco VSM virtual machine images on the Cisco UCS platforms. For more information on these subjects, see the "Related Documentation" section on page 18.

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.

Figure 1 represents a virtualized VSM application running on a UCS B- and C- Series platform.

Figure 1 Cisco IP Video Surveillance on UCS B- and C- Series Platforms

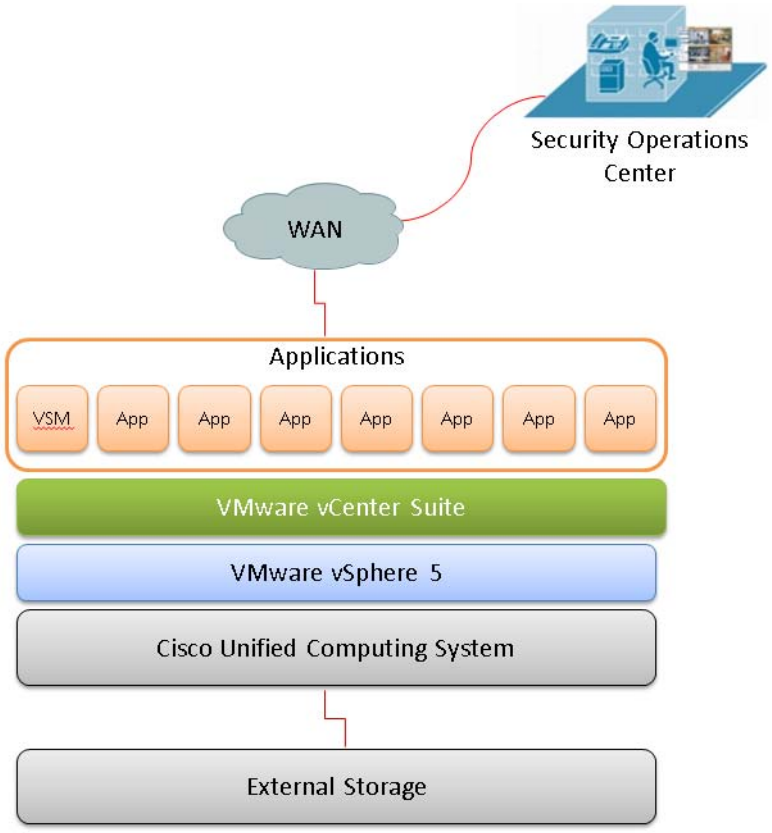
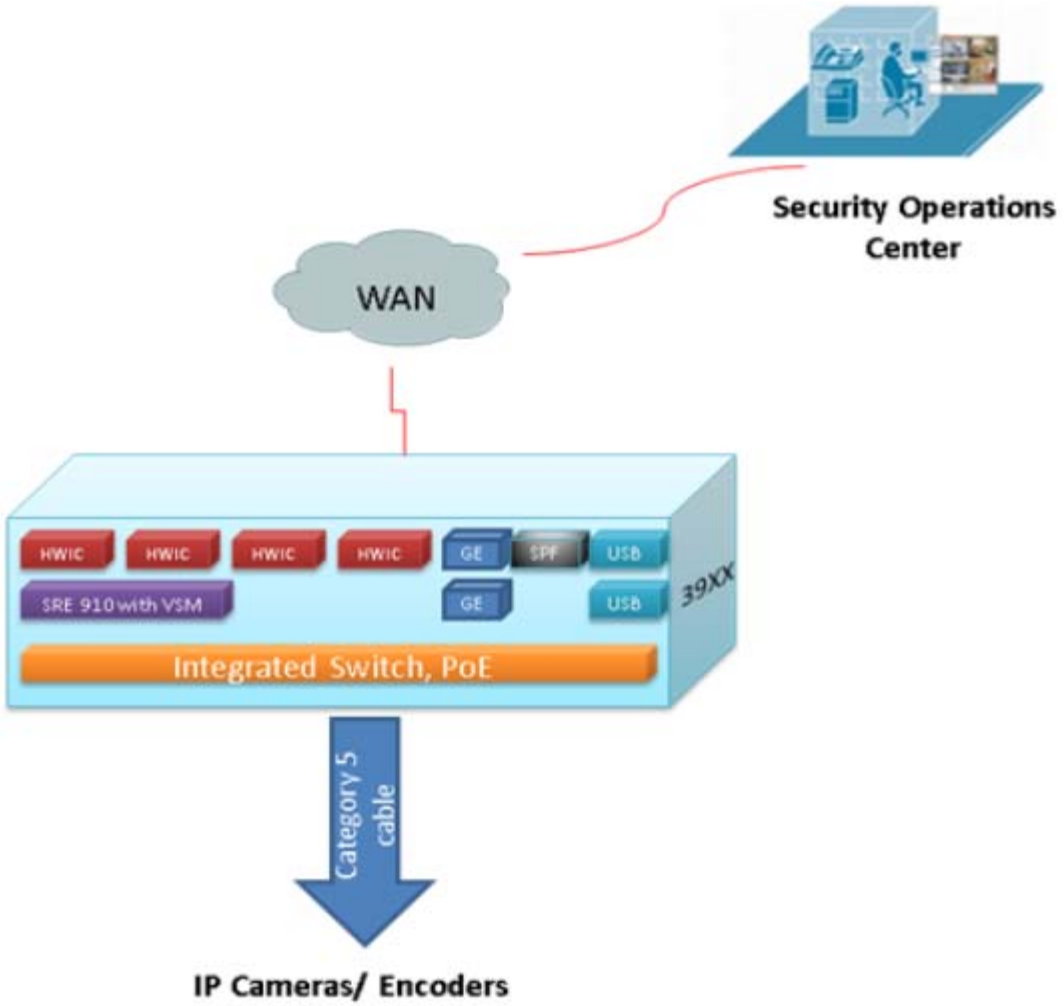


Figure 2 displays the Cisco ISR G2 platform integrating Cisco Video Surveillance on the UCS Express and E- Series platforms. This solution uses a single network access device for remote sites.

Figure 2 Cisco ISR G2 With the UCS Express and E- Series Platforms Integrates Video Surveillance on Single Network Access Device for Remote Sites



Solution Components

This guide assumes that the ESXi 5.0 Hypervisor is installed on the UCS server of SRE blade.

The required components for designing and deploying VSM on UCS B-and C–Series platforms include:

- **UCS B- and C-Series servers**—The Cisco UCS Servers can be deployed as rack-mount servers (C-Series) or blade servers (B-Series) running the ESXi 5.0 virtualization software.The B-Series servers deliver a scalable and flexible architecture to meet your data center needs while helping to reduce the total cost of ownership. The C-Series servers address fluctuating workload challenges through a varying balance of processing, memory, I/O, and internal storage resources.
- **UCS Express on a Cisco ISR G2 with SRE 900/910 blade**—The Cisco UCS Express is an SRE blade on an Cisco Integrated Services Routers Generation 2 (ISR G2) branch office router running the SRE-V (ESXi) virtualization software. The 2900 and 3900 series routers have up to four Gigabit Ethernet interfaces onboard, up to four Enhanced High-Speed Wide-Area Network (WAN) Interface Card (EHWIC) interface slots, and up to four service module slots (depending on the model). See the UCS Express Data Sheet for more information.
- **UCS E-Series on a Cisco ISR G2 with E140x or E160x single or double-wide blade**—Cisco UCS E-Series Servers are next-generation power-optimized general-purpose x86 64-bit blade servers designed to be deployed in Cisco ISR G2 branch office router running the SRE-V (ESXi) virtualization software. See the UCS E-Series Data Sheet for a list of the supported single-wide and double-wide blades.
- **Virtualized Video Surveillance Manager (VSM) software**— The VSM software is available as an Open Virtual Appliance (OVA) file on Cisco.com. The OVA package is a tar file with the Open Virtualization Format (OVF) directory inside. Apart from the OVA file, the Video Surveillance Operations Manager (VSOM) virtual machine (VM) License and Video Surveillance Media Server (VSMS) VM License are also required.
  - UCS B-or C-Series: This software runs on a UCS B-or C-Series server in a virtualized environment.
  - UCS Express and E-Series: This software runs on a Cisco ISR series SRE blade in a virtualized environment.
- **Cameras**—The Cisco IP video surveillance camera and analog cameras are attached to encoders, analog gateway network modules for the integrated services router, or third-party IP surveillance cameras.
- **Network**—This component is comprised of the enterprise network—the Media Ready Network. The primary focus of this design guide is to reference the existing design baselines of branch office and wide-area network (WAN) while building on this base of knowledge with IP video Surveillance requirements, best practices, and design recommendations.

Logical Network Topology

Figure 3 and Figure 4 illustrates the overall logical topology of the networking and video surveillance components, including a UCS B-Series containing the ESXi host running VSM and VSOM, various IP cameras, an external switch, and the operator workstations running the VSOM client.

Figure 3 UCS B- and C- Series Logical Network Topology

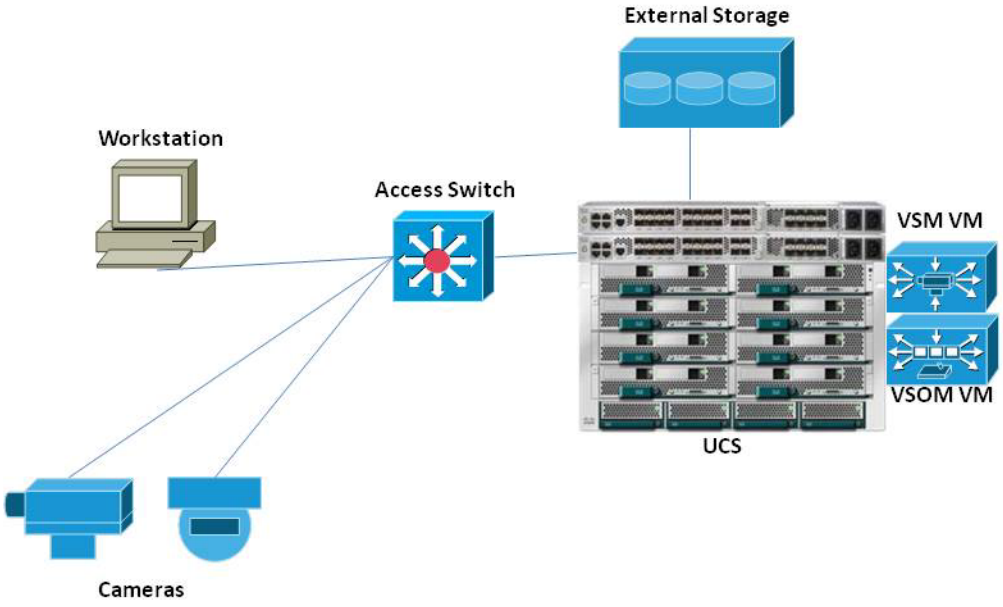
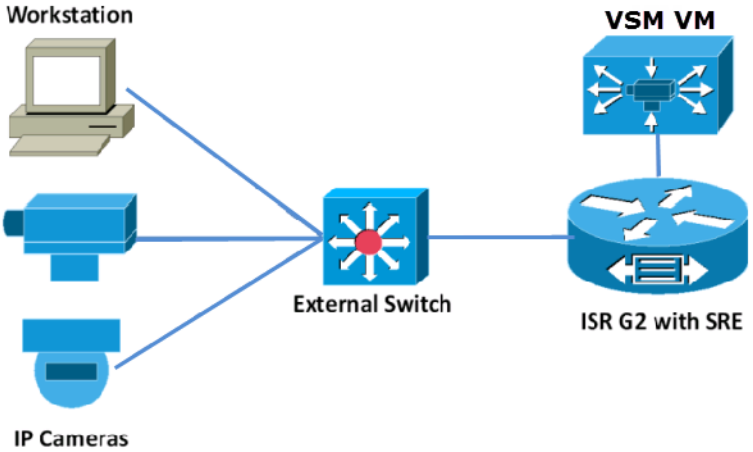


Figure 4 UCS Express and E- Series Logical Network Topology (External or Internal Switch in ISR)



IP Network Infrastructure

Table 1 IP Network Infrastructure Considerations for VM Deployment

Requirement	Description	More Information/Detailed Requirements
Virtual Machine Considerations for the UCS Express	The SRE 900/910 service module must be dedicated to the VSM VM, because the computing requirements for VSM are high. Deploying other VMs on the same SRE 900/910 service module are not recommended and not supported.	*Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms*
Bandwidth	Bandwidth refers to the raw capacity available on a particular transport medium, and is dependent on its physical characteristics and the technology used to detect and transmit signals. The amount of available bandwidth on a network segment directly impacts the quality and performance of the IP Video Surveillance solution and as such should be carefully considered. High-bandwidth, low-delay networks typically do not encounter much performance degradation over time. Low-bandwidth, low-delay networks on the other hand typically experience packet loss due to congestion. High-bandwidth, high-delay networks (so-called Long Fat Networks), such as satellite links, would typically experience significant performance degradation due to the latency.	Cisco Video Surveillance Solution Reference Network Design Guide
Quality of Service (QoS)	QoS refers to the ability of the network to provide special or preferential service to a set of users or applications or both to the detriment of other users or applications or both. Proper design of QoS in an IP Video Surveillance environment is crucial as video transport places unique demands on the network infrastructure to ensure that it is usable, reliable and available to media servers and end-users.	Cisco Video Surveillance Solution Reference Network Design Guide
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 can expose the enterprise to financial loss and compromise personal safety. This design guide illustrates how to transport video traffic over LAN and WAN with IP security encryption, and also implement administrative controls on who has access to the network.	Cisco Video Surveillance Solution Reference Network Design Guide
Network Services	One advantage of the any-to-any aspect of IP networks is resource and system access. Examples include the Network Time Protocol (NTP), Dynamic Host Control Protocol (DHCP), Power-over-Ethernet (PoE) and the Cisco Discovery Protocol (CDP) both lower the cost of installation and facilitate troubleshooting.	Cisco Video Surveillance Solution Reference Network Design Guide

Table 1 IP Network Infrastructure Considerations for VM Deployment (continued)

Requirement	Description	More Information/Detailed Requirements
Network Management	In order to have an effective IP Video Surveillance solution that meet expectations, the video endpoints, server applications and client endpoints need to be managed on a common network framework, to allow for device and platform health monitoring, fault isolation and resolution.	Cisco Video Surveillance Solution Reference Network Design Guide
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. To achieve the goal of a fully-converged network, the other Building Management Systems (BMSs), 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 achieving 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 BMSs are very trivial to that of video surveillance, the end users of the data often report to the same organization heads and the likelihood of system integration (now or in the future) is high.	Cisco Video Surveillance Solution Reference Network Design Guide

Table 1 IP Network Infrastructure Considerations for VM Deployment (continued)

Requirement	Description	More Information/Detailed Requirements
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 video surveillance application can 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 use data mining techniques to detect patterns in data. Video analytics may be performed 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 analysis output of video data can be more economically valuable than the loss prevention role of video surveillance to many retail organizations.	To configure analytic rules on the camera, see the camera product documentation. To configure the actions that are triggered in Cisco VSM when an analytic event occurs on a camera, see the "Advanced Events" section of the Cisco Video Surveillance Operations Manager User Guide.
NTP Considerations	NTP must be configured on the VM and ESXi host. Time sync on VMware tools should be disabled on the VM.	Detailed instructions are available in the Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms.

Performance and Scalability

For performance and scalability information for the Cisco Video Surveillance Manager servers, see the Cisco Video Surveillance Manager Release 7 Server Performance Guidelines.

Describes the core capabilities and performance of a supported Video Surveillance Manager server for use when designing and deploying Cisco Physical Security solutions.

This document provides the scalability limits for server platforms supported in Cisco Video Surveillance Release 7.0.1 and higher.

Storage Considerations

Media Server VMs running on the UCS platforms support the following storage sources:

- UCS Express and E-Series platforms can access internal storage and iSCSI external storage.
- UCS B- and C- Series platforms can access internal storage, and external storage from Fiber Channel-based SAN storage, such as the Cisco Physical Security Storage System 4RU (CPS-SS: 4-RU) and the Cisco Physical Security Storage System 4RU-EX.

The usable storage is based on the redundant array of independent disks (RAID) level used. For more information, see the following:

Table 2 Related Documentation for VM External Storage

Information Source	Description
Cisco Video Surveillance Storage System documentation	Instructions to install, configure and administer the Cisco Physical Security Storage System.
Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms.	Instructions to associate external storage with a VM running on the Cisco UCS Series platforms, and how to add media partitions to a Cisco VSM VM

Design Recommendations for Deployment Models

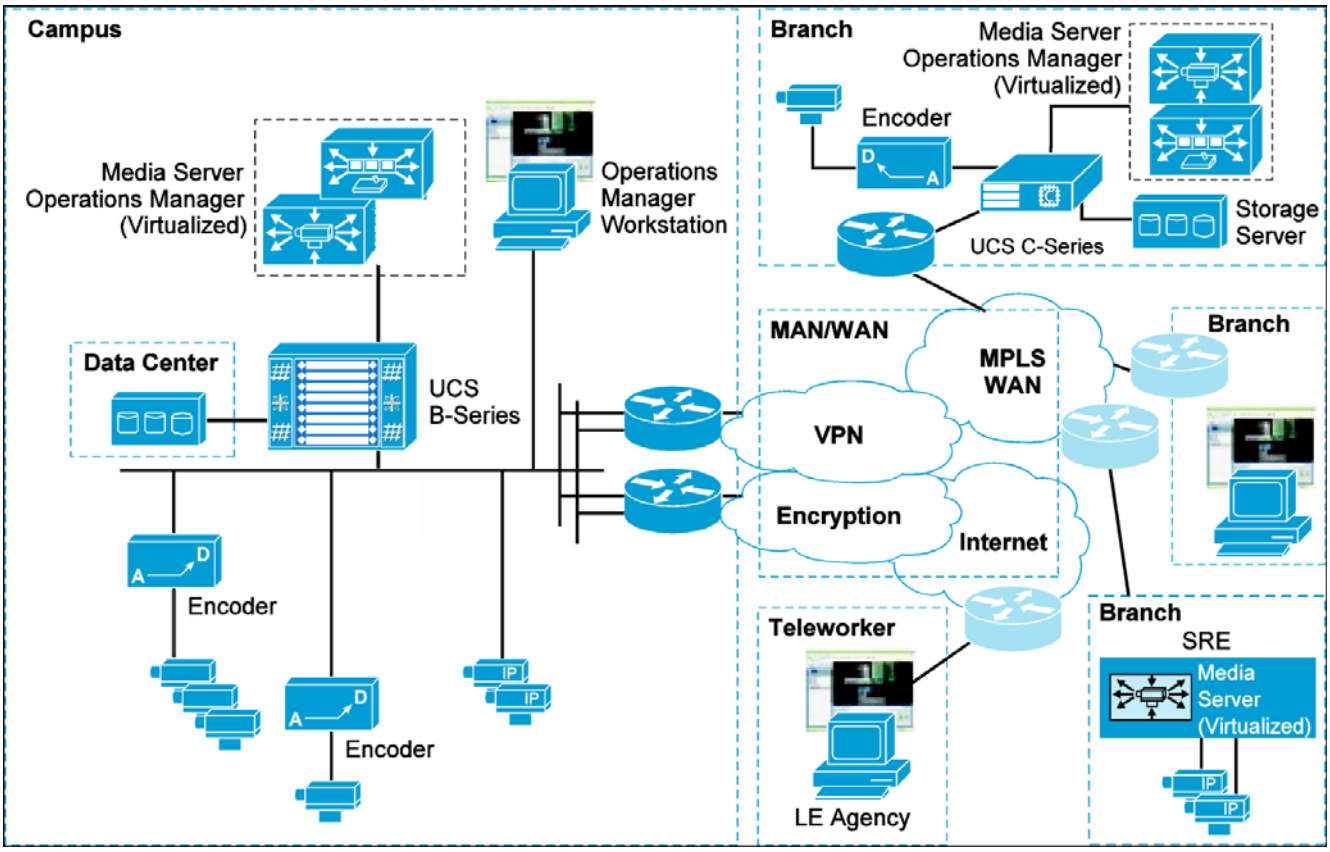
A typical IP video surveillance deployment in an enterprise network consists of one or more campus locations running a Cisco Video Surveillance Media Server and a Video Surveillance Operations Manager on an Intel-based Linux Enterprise Server OS (Cisco Physical Security Multiservices Platform or Cisco UCS Platform).

Recommendations

- Deploy Cisco VSM on UCS Express or E-Series platforms only if you plan to record up to 32 streams 1 M or 15 streams @ 2 M or 7 streams @ 4 M.
  - For the UCS Express, consider dedicating the entire SRE 9xx for video surveillance.
  - UCS Express or E-Series platforms are deployed on the Cisco Services Ready Engine (SRE) with ESXi running a video surveillance virtual machine (VM). The VMs can run the Cisco Video Surveillance Media Server and Video Surveillance Operations Manager software.
- Locations with more than 32 video surveillance cameras can be deployed on standalone hardware or the UCS C-Series server running a video surveillance virtual image.
- For enterprise-level deployments, we recommend to use the UCS B-Series servers in the data center.
- 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 bandwidth costs.
- A typical enterprise deployment consists of one or more campus locations running the Cisco Video Surveillance Media Server.
- Branch offices and teleworker locations may view and administer the video surveillance system
- External users and external organizations can also access the system using an Extranet or the public Internet and a web browser.

Figure 5 illustrates the topology and application services deployed in an enterprise-wide implementation of IP-based video surveillance.

Figure 5 VSM Deployment Models



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 Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) deployment. With a Layer-2 MPLS deployments (Pseudowire), IP cameras can be Ethernet-attached to a remote switch and can transport images through the carrier network, provisioned and managed by the Video Surveillance Operations Manager, either at a branch location or a central location. Branches attached through 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 Dynamic Multipoint Virtual Private Network (DMVPN), can be overlaid on to the WAN transport to provide data privacy and authentication by way of IP security (IPsec) encryption. To ensure the 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) 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 the Enhanced Internal Gateway Routing Protocol (EIGRP).

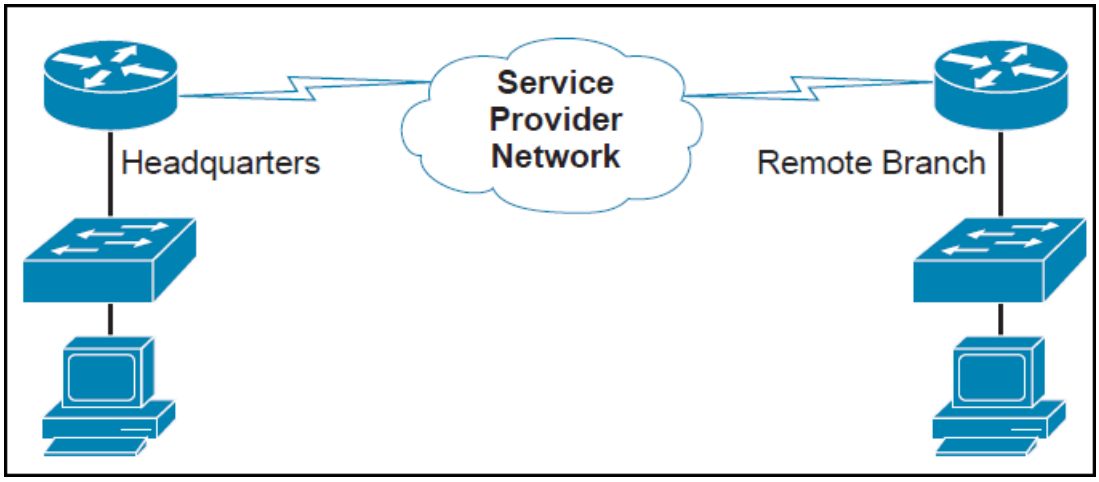
The decision as to whether a specific environment should implement the Cisco Video Surveillance on UCS Express or E-Series platforms at a branch location and archive data at the branch—or provision cameras off the campus implementation of the Cisco Video Surveillance Manager—depends on the number of cameras, the resolution, frame or bit rate of the camera, quality factors of the cameras, and the bandwidth cost and availability at the remote locations.

WAN Considerations

WAN is used to connect different LANs and typically includes a broad geographic area. WAN services are leased from service providers who provide different speeds and connectivity options.

Figure 6 illustrates how a remote branch office relies on the connectivity provided by a WAN service provider.

Figure 6 Service Provider Network



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 WAN environment, most connections are less than 10 Mbps; many remote connections operate on a single T1 (1.544 Mbps) or less.

These inherent bandwidth constraints require careful evaluation of the placement of cameras and Media Servers, and how many viewers can be supported at remote sites simultaneously. By using child proxies, bandwidth requirements can be reduced to transport video streams across WAN connections.

The placement of recording devices also becomes important. The video can be streamed to a central site using lower frame rates or resolution, but another attractive alternative is to deploy Media Servers at the remote sites and stream the traffic using the LAN connectivity within the remote site.

A point-to-point or leased line is a link from a primary site to a remote site using a connection through a carrier network. The link is considered private and is used exclusively by the customer. The circuit usually is priced based on the distance and bandwidth requirements of the connected sites.

Technologies, such as Multilink Point-to-Point Protocol (PPP), allow several links to be bundled to appear as a single link to upper routing protocols. In this configuration, several links can aggregate their bandwidth and be managed with only one network address. Because video surveillance traffic requirements tend to be larger than other IP voice and data applications, this feature is attractive for video surveillance applications.

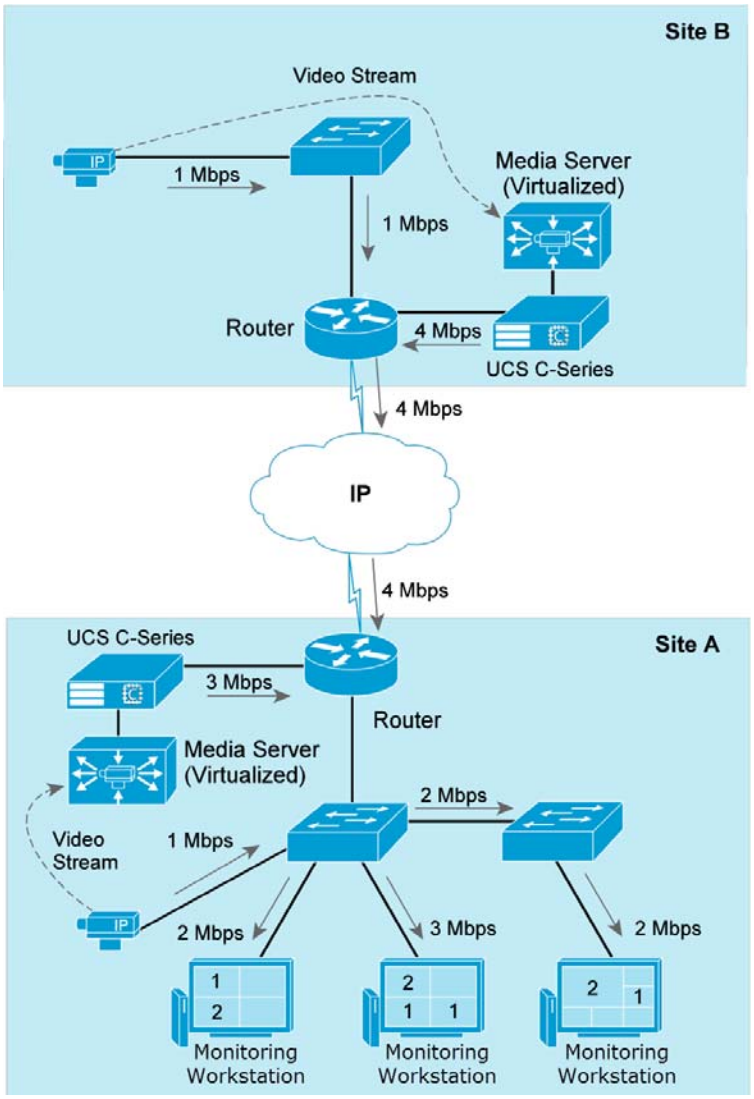
Hub-and-spoke, also known as star topology, relies on a central site router that acts as the connection for other remote sites. Frame Relay uses a hub-and-spoke topology predominantly due to its cost benefits, but other technologies, such as Multiprotocol Label Switching (MPLS), have mostly displaced Frame Relay.

Example 1—Network Bandwidth Usage

Figure 7 and Figure 8 illustrate a simple scenario with two sites. Each site has a Media Server and each is the direct proxy for an IP camera. Three video monitoring workstations are active in Site A and each IP camera generates 1 Mbps of network traffic.

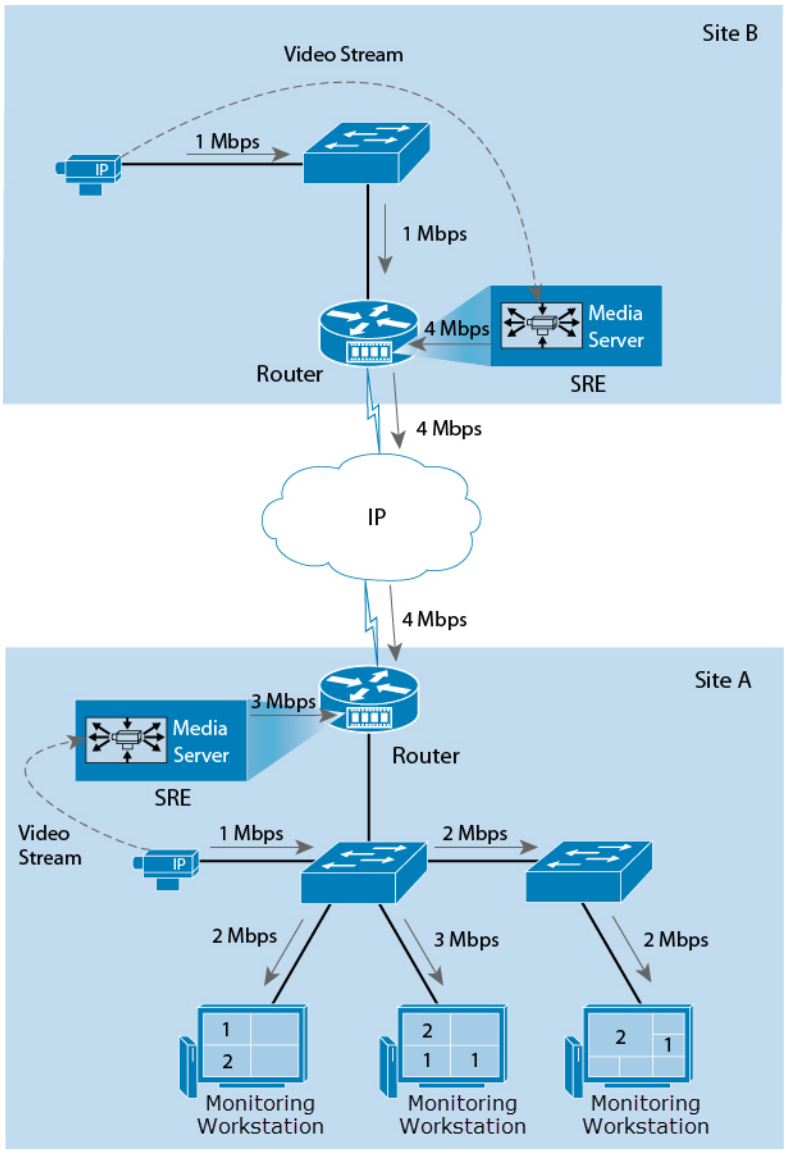
Two monitoring workstations display video streams from Camera 1 and Camera 2, while one monitoring workstation displays three video streams: two streams from Camera 1 and one stream from Camera 2. The network bandwidth required to display video streams for Camera 2 in Site A is relatively small for a LAN environment, but the traffic from Camera 1 can be significant for WAN environments because four different 1 Mbps streams must traverse the WAN locations.

Figure 7 UCS B- and C- Series: Network Bandwidth Requirements



Note For simplicity, the Operations Manager has been removed from Figure 7 and Figure 8.

Figure 8 UCS Express and E- Series: Network Bandwidth Requirements



Example 2—Sites with Remote Storage

Figure 9 and Figure 10 display how Media Servers can be deployed at different WAN locations to minimize the bandwidth requirements. By deploying the Media Servers close to viewers and edge devices, the network traffic remains local to each site. Archiving video streams at each location is also an attractive solution to minimize the network traffic between sites.

In this example, Site A and Site C have Media Servers acting as direct proxies and archives for the IP cameras. Because both sites archive and distribute video to the monitoring workstations locally, the network traffic remains local to each site.

Site B can function without a local Media Server, but all video streams must traverse the WAN connections. Because Media Server A is the direct proxy for Camera B, the 1 Mbps stream must reach Media Server A before reaching any monitoring workstation. A total of 3 Mbps would be required for both monitoring workstations in Site B to receive video from Camera B.

Figure 9 UCS B- and C- Series: Sites with Remote Storage

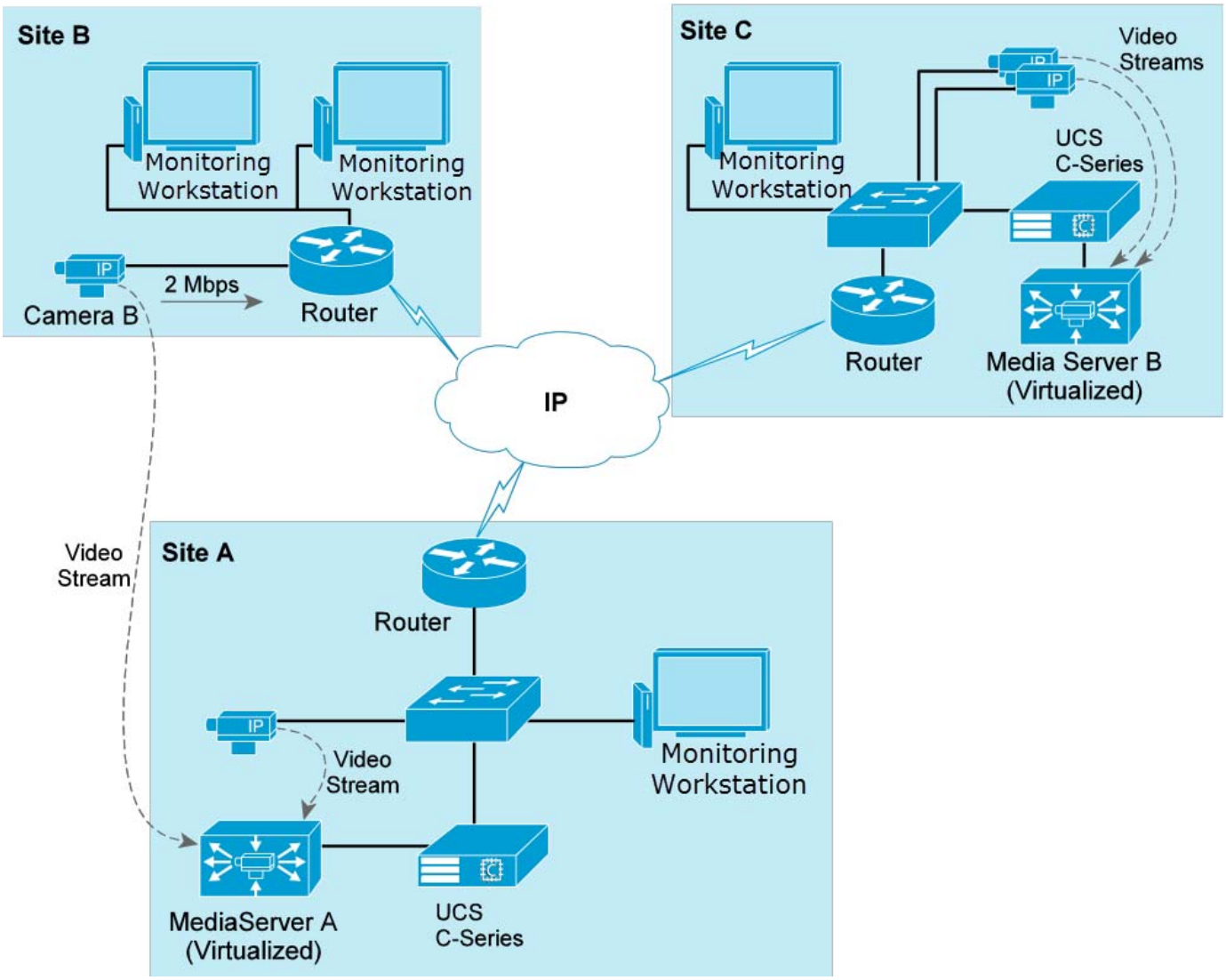
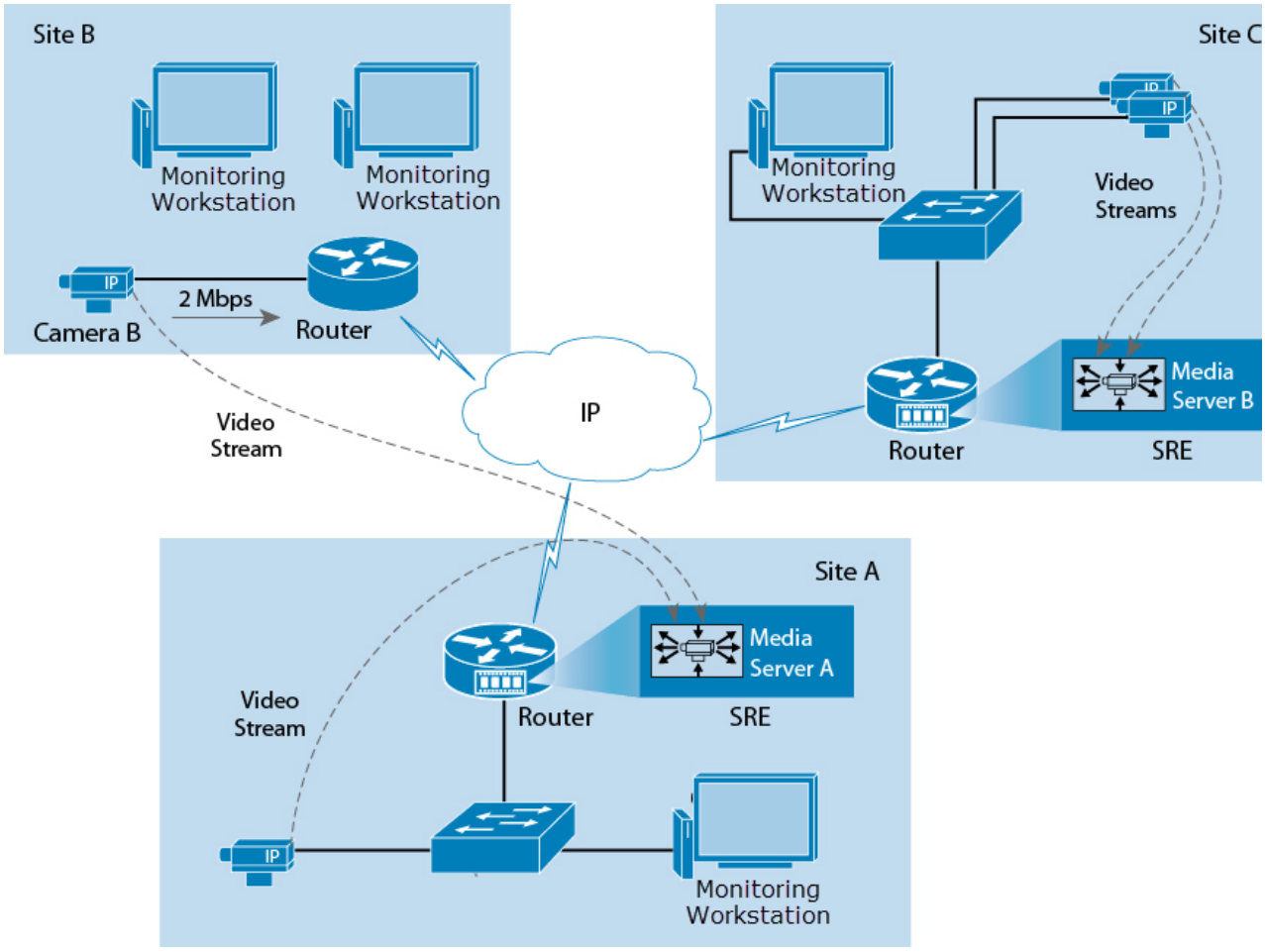


Figure 10 UCS Express and E- Series: Sites with Remote Storage



Example 3—Distributed Media Servers

Figure 11 and Figure 12 display a deployment with several remote sites, each with a local Media Server acting as the direct proxy and archive for local IP cameras. In this scenario, all recording occurs at the remote sites and live video streams are viewed by OM viewers and VM monitors (video walls) at the headquarters.

The Media Server at the headquarters could also have Parent-Child proxies to each remote Media Server and request the remote streams only when required at the headquarters. This would have less bandwidth impact when the same stream is requested by more than one viewer because the traffic would be contained locally in the headquarters LAN.

Figure 11 UCS B- and C- Series: Distributed Media Servers

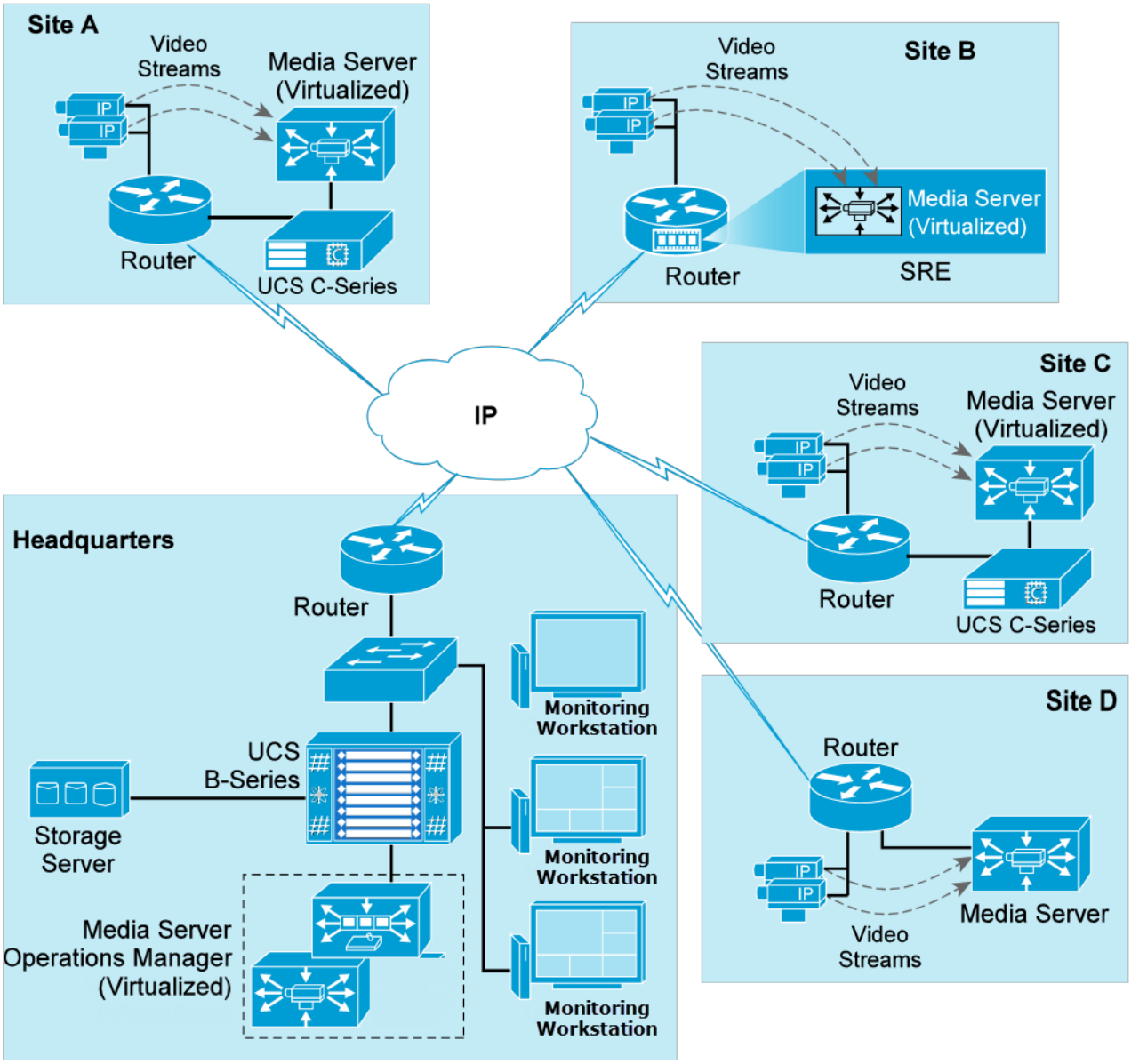
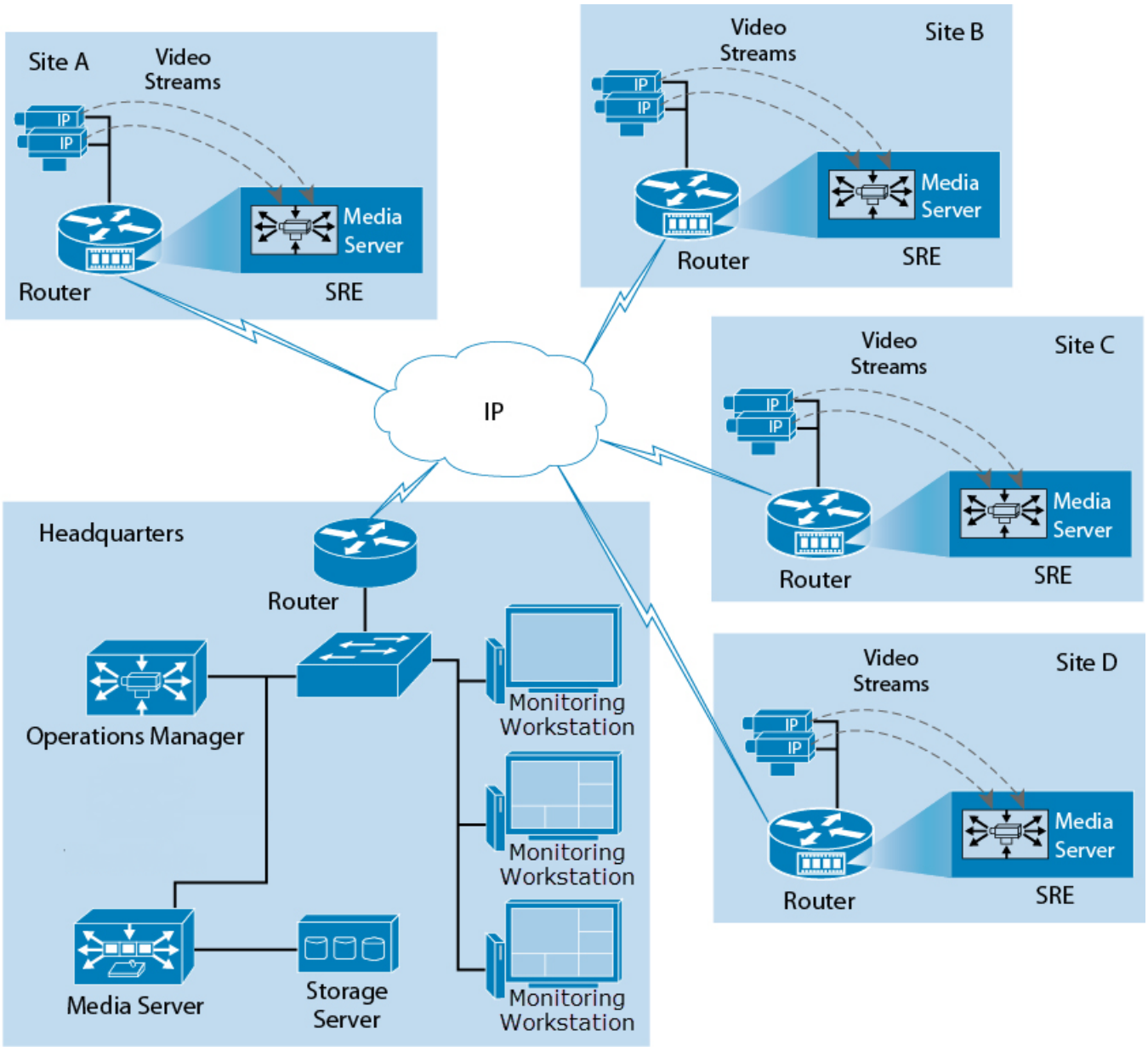


Figure 12 UCS Express and E- Series: Distributed Media Servers



High Availability

In Cisco VSM release 7, Media Server high availability is achieved using Media Servers that are configured as Redundant, Failover, or Long Term Storage servers. See the Cisco Video Surveillance Operations Manager User Guide for more information.

For Operations Manager high availability (when Operations Manager is deployed as a VM on the Cisco UCS platform), see the Cisco Video Surveillance Solution Reference Network Design Guide.

Related Documentation

Use one of the following methods to access the Cisco Video Surveillance (Cisco VSM) documentation:

- Go to the Cisco Video Surveillance documentation web site.
- See the Cisco Video Surveillance 7 Documentation Roadmap for descriptions and links to Cisco Video Surveillance documentation, server and storage platform documentation, and other related documentation.