Network Readiness Assessment for IP Video Surveillance

Contents

Objective 4

Overview 4

General Network Requirements 5

- Project Management 5
- Education and Training 5
- Documentation 5
- Network Services 5
- Network Management 6

Network Characteristics of IP Video Surveillance 7

- Bandwidth 7
- Packet Loss 7
- Latency 7
- Jitter 8
- Bursts 8
- Quality-of-Service (QoS) 9
- Video Surveillance Application Requirements 9
- Summary 10

Design Considerations 11

- LAN Switching Defined 11
- Switching Hierarchy 12
- Device Placement 13
  - IP Cameras 13
  - Media Server (VSMS) 14

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

Operations Manager (VSOM) 17
Viewing Station 18
Backup Media Server 18
Fibre Channel Attached Storage 18
Summary 19
Specific Network Requirements 20
Assessing Switching (LAN) Readiness 20
Inventory 21
Physical Connectivity 24
Environmental Statistics 26
CPU Utilization 27
Memory Utilization 27
Local Link Issues 28
Overall Capacity Assessment 30
Logging and Network Time Protocol 31
Summary 31
Assessing Routing Readiness 33
Inventory 34
CPU Utilization 34
Memory Utilization 34
Environmental Statistics 36
Buffer Tuning 36
Logging 36
Interfaces 37
Switching Path Analysis 40
Asymmetric Routing 41
Routed Protocol Analysis 41
Routing Protocol Analysis 41
Bridged Protocol Analysis 42
Summary 42
Service Level Assessments 43
IP SLA Control Protocol 45
Types of Probes 45
ICMP Echo Operation 45
TCP Connect Operation 48
HTTP Operation 50
UDP Jitter Operation 52
Summary 55
References 55
Security and Application Optimization Assessment 56

Access Control Lists (ACL) 56
Firewalls 56
NAT/pNAT 57
Segmentation 57
Application Optimization 57
Packet Shapers 57
Recommended Reading 57
Quality-of-Service (QoS) Assessment 58
Medianet Switches 58
References 58
Network Assessment Checklist 59
Appendix 64
show control-plane host open-ports 64
HTTP Connect Connections over Internet WANs 64
Residential DSL Broadband 64
Business Class Cable Broadband 65
Why Packet Loss Impacts IP Video Surveillance 68
Transport methods 68
Resolution is a Dominate Attribute 68
As Resolution Increases, the Drop Threshold Decreases 69
Summary 69
Troubleshooting Duplicate IP Addresses 70
Methodology 70
Address Resolution Protocol (ARP) Table 70
Show CDP neighbors 71
Displaying the MAC-Address Table (Static Entries) 71
Displaying the MAC-Address Table (Static Entries) 72
Summary 72
QoS Considerations for Backup Media Servers 73
LAN Switch Marking Example 73
Branch Router Sample Configuration 74
Verification 75
Asymmetric Routing 77
Switch Configuration—Reference Network Topology 79
Clearing Interface Counters 80
Q&A from Network Readiness Assessment for IPVS Webinar 81
References and Supplemental Reading 84

Objective

The objective of this document is to define best practices for assessing the existing or proposed network topology to transport IP video surveillance.

Overview

To successfully deploy the components of an IP video surveillance solution on a existing network, the physical security integrator and the network manager must work together to assess the existing network to determine if the infrastructure is capable of handing IP based video surveillance traffic.

This document consists of the following sections:

- General Network Requirements—Examines network requirements which are consistent with best practices for ongoing operation and support of a converge IP network. These are foundational requirements
- Network Characteristics of IP Video Surveillance—Discusses the bandwidth requirements as well as latency, jitter and loss in the context of the requirements specific to IP video surveillance.
- Design Considerations—Begins with a primer on campus network design and then illustrates the component devices which make up an IP video surveillance solution and the data flows between these devices.Bandwidth estimates for both high definition (HD) and standard definition (SD) camera as well as disk storage requirements for archive files are included. The current performance and internal disk storage guidelines for appliance-based Media Servers are included to help the assessment determine if sufficient network ports, bandwidth and storage are include in the bill of materials to support the business requirements.
- Specific Network Requirements—This section consists of the following subsections:
  - Assessing Switching (LAN) Readiness—Reviews the components of a LAN switch and provides insight into assessing the switch health as wells as the interfaces (ports) which provide connectivity to the component devices which comprise an IP video surveillance deployment
  - Assessing Routing Readiness—The same methodology is examined as Assessing Switching (LAN) Readiness, above.
  - Service Level Assessments—provides example configurations for using Cisco IOS IP Service Level Agreements (SLAs) commands to measure the existing network characteristics and gather baseline information to determine if the network meets the minimum requirements as defined in the Network Characteristics of IP Video Surveillance section.
  - Security and Application Optimization Assessment—Provides a high-level overview of issues which may impact a successful deployment when devices such as firewalls, packet shaping appliance or Cisco Wide Area Application Services (WAAS) appliances are present in the network.
  - Quality-of-Service (QoS) Assessment—Provides a similar overview specific to assessing the current state of QoS in the network under assessment
- Network Assessment Checklist—Provided to help organize the assessment efforts.
- AppendixA—Contains supplemental information and references to other whitepapers and design guides which explain in more detail those topics which may require further investigation.

General Network Requirements

These general network requirements outline the overall project management, training, documentation and other services that are required to ensure a timely deployment and successful ongoing operation of the network to support IP video surveillance.

Project Management

Depending on the size and scope of the deployment, either a full-time project manager is required, or for smaller deployments, an existing staff member must fill this role. The project manager must work with the stakeholders to set the scope of the project, develop a timeline to complete the implementation, and create a detailed plan. Additionally, they must monitor the progress of the plan, provide relevant updates to the stakeholders, and address any risks and roadblocks to completion.

Education and Training

IP video surveillance deployments are particularly challenging because historically, the physical security manager and the network manager had little reason to interact. In IP video surveillance, the dedicated COAX and twisted-pair cable plan is replaced by LAN switches and CAT-5 cable. The physical security integrator and operations staff must have a basic knowledge of networking to communicate their needs and objective to the network manager. Security integrators have the skill set that the network engineer does not possess, but do need to supplement this with network certifications such as a Cisco Certified Network Associate Routing & Switching (CCNA). Having a Cisco Certified Internetwork Expert (CCIE) on staff is a competitive differentiator.

Cisco recommends that any system integrator deploying Cisco's Physical Security Solutions complete the PSS ATP (Advanced Technology Program) curriculum.

Documentation

If an existing network infrastructure is used for a basis of the deployment, it must be adequately documented and an inventory of the components completed. The type, model number, and software/firmware releases of the switches and routers should be documented. In addition to a network topology diagram, the location and distances between IP cameras and the wiring closets must be determined. Because of the camera location requirements of video surveillance deployments, in some cases, twisted-pair cable needs to be supplemented with fiber due to distances. If in-house expertise is not available, a cabling contractor is needed.

Network Services

IP video surveillance has requirements for Network Time Protocol (NTP) services, Power-over-Ethernet (PoE), system logging (Syslog), File transfer (FTP/TFTP) servers, and Simple Network Management Protocol (SNMP) trap servers. An important part of the network assessment process is to identify and assess these services within the enterprise network or implement if none exist.

Network Management

The network management component is often overlooked, but a critical component for on-going success. The network management domains are Fault, Configuration, Accounting, Performance, and Security (FCAPS). Monitoring of the network for packet-loss on switch ports and server interfaces is a key element to ensuring acceptable video quality. Measuring network utilization trends is important to ensure the network performance characteristics remains consistent value suitable for transporting video.

Network Characteristics of IP Video Surveillance

Deploying video on an existing IP network often exposes network infrastructure issues that data traffic can tolerate while video cannot. Packet loss that may trigger a retransmission of an E-mail download often goes unnoticed, because the message text is not presented to the user until the download is complete. With IP video surveillance, however, the operator is watching the video in real-time and any loss is immediately recognizable.

Video surveillance network traffic can be characterized by the following:

- Bandwidth
- Packet Loss
- Latency
- Jitter
- Bursts

Bandwidth

Standard definition IP cameras using MPEG-4 for planning purposes assumes at least 1 to 2Mbps per camera, Motion JPEG at least 2 to 8Mbps per camera. For High Definition (1920/1080), using H.264 assumes at least 4 to 6Mbps per camera.

These are average values measured over the course of the time period of seconds to minutes. Because of the nature of MPEG-4 and H.264, the video feed will burst to much higher values when I-frames are generated. I-frames may be generated approximately every 4 seconds.

Packet Loss

With standard definition below 0.5 of 1 percent may be acceptable, but with high definition (HD) even 1/10th of 1 percent can be noticeable. For more information on packet loss and the impact on video feeds, refer to "Why Packet Loss Impacts IP Video Surveillance" section on page 68.

For practical purposes, packet loss in the network is noticeable in the video quality of MPEG-4 and H.264 video feeds. Packet loss is less of an issue for Motion JPEG, but impacts the usability of the video image. Because of the higher bandwidth and storage requirements of Motion JPEG versus MPEG-4 / H.264, it is assumed that Motion JPEG expected use is for analytics applications and lower frame rates and resolutions.

Latency

Latency depends highly on the transport protocol. MPEG-4/H.264 transported in a TCP session between a NDVR and a PC viewing station is more demanding than MPEG-4/H.264 transported in UDP/RTP between a camera and the NDVR. Two-way interaction for PTZ also requires lower latency. Latency in most LAN environments should routinely be less than 10ms. In a WAN environment, latency should be less than 50ms round-trip. Any WAN latency over 50ms round-trip may introduce poor video quality or issues with usability.

Jitter

Jitter generally increases as latency increases. If latency is less than 50ms round-trip, jitter should only be a few milliseconds at most. If jitter is high, latency is likely also an issue and should be addressed first. From an implementation standpoint, jitter is of little concern if sufficient bandwidth is available, latency is within the recommended values, and packet loss is approaching zero. Because of this, no specific range of jitter need be defined. As general rule, jitter should roughly be less than 10 percent of the measured latency value.

Bursts

Video traffic on the network is a series of video frames encapsulated in multiple IP packets. The size of the video frames and the resulting number of IP packets required to transport depends on how the video is encoded. However, resolution is the predominate factor. In MPEG-4 / H.264, the bursts are most apparent with the transmission of reference frames, also known as I-frames. These tend to be sent on a periodic basis, in many instances, approximately every 4 seconds.

Most IP surveillance cameras can be configured for a constant bit rate (CBR) value for network traffic. The encoder of the camera can vary the frame rate and the quantization of the video image to, on the average, send this amount of video traffic over the network.

The key here is *average*. Average over what time frame? Typically, it is calibrated in Megabits per second (Mbps). In looking at a 30-second H.264 traffic (configured for CBR of 4 Mbps) from an HD camera, a protocol analyzer reports 383 packets per seconds, with an average packet size of 1,397 bytes, at a rate of 4.3 Mbps.

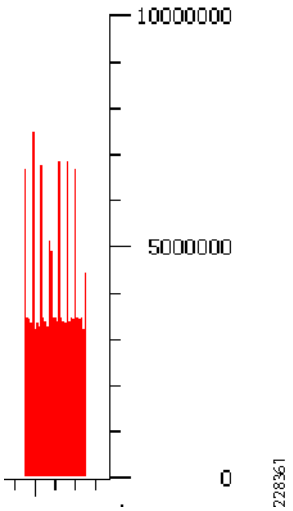
However, if we look at the data rate over a smaller interval, rather than an average normalized to a second, it is apparent that the actual data rate is much higher than the average of 4.3 Mbps during some periods of time and much lower over other intervals.

By graphing the 30-second time period, 1 second per tick mark, in bits per second, the graph illustrates that at some periods in time the load on the network is much higher than the 4 Mbps target. At 30 frames per second, this encoder generates an I-frame approximately every 4 seconds[1], if protocol analyzer used to graph the network load starting at the first IP packet of the I-frame, the network load approaches 100 Mbps for approximately 1/20th of a second (50 milliseconds). For routers and switches, 50ms is a fairly long period of time. When shaping traffic, routers may look at packet arrival rates in intervals as low as 4ms.

These bursts are much more pronounced from high definition (HD) IP cameras than from standard definition (SD) IP cameras. The number of IP packets required to send an I-frame from a SD camera is substantially less than that required for an HD camera, due to the higher resolution of the image. Figure 1 illustrates the I-frame bursts of H.264 HD video.

1. Group of Video (GOV) length of 128 at 30 frames per second is an I-Frame generated every 4.267 seconds

Figure 1 I/O Graph of H.264 High Definition Video (bits per second)



In a LAN network with IP cameras attached to the switch port at FastEthernet speeds with the Viewing Stations and Server attached at GigabitEthernet port speeds, these bursts are usually not an issue for the network. If packet loss is experienced in the network, it often will be associated with traffic bursts. However, it is important to understand the behavior and it is critically important to be aware of the increased network load when transitioning from SD IP cameras to HD IP cameras.

Quality-of-Service (QoS)

Because of the requirements for controlling IP packet loss and designing the network with sufficient bandwidth and appropriate WAN circuits to maintain latency and jitter within acceptable norms, the network must be provisioned with the appropriate QoS configurations on the LAN and WAN. QoS refers to techniques that manage access to network resources based on the requirements of the application. For example, video traffic must be given preferable treatment over data applications like file transfers or sending E-mail. For details of the requirements for video applications, including IP video surveillance, refer to the *QoS Design Recommendations for Medianets* at the following URL:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/qosmrn.html

This document shows the Cisco Differentiated Services (DiffServ) QoS recommendations for Medianets and how voice, video, and data applications should be identified to the QoS polices on the LAN and WAN.

Video Surveillance Application Requirements

The "Service Level Assessments" section on page 43 includes sample Cisco IOS IP service-level agreements (SLAs) router configuration commands to define and run probes within a Cisco network to help in evaluating if the network can meet the application requirements listed in the following table.

Table 1 Video Surveillance Application Requirements

Metric	Value
Latency (UDP/RTP Transport)	150ms one-way values or more may be acceptable if no two-way communication such as PTZ are required
Latency (TCP Transport)	Less than 50ms RTT
Loss (Standard Definition MPEG-4/H.264)	Less than 0.5% (1/2 of one percent)
Loss (High Definition MPEG-4/H.264)	Less than 0.05% (1/20th of one percent)
Jitter	Less than 10% of one-way latency

The "Performance Routing (PfR) Integration" chapter in the *IP Video Surveillance Design Guide* (http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/IPVS/IPVS_DG/IPVS_DG.pdf) discusses that connectionless IP video surveillance transport, such as with MPEG-4 or H.264 encapsulated in UDP/RTP between an IP camera and Media Server, does not negatively impact the video quality of the image. In fact, some vendor implementations actually buffer H.264/RTP video feeds for several seconds before displaying the video on the screen of a viewing station. For this reason, the latency requirement for connectionless transport is not particularly important.

However, if the video transport is MPEG-4 or H.264 encapsulated in TCP, as is the case with a viewing station watching a live or archived video feed from a Media Server, latency above 50ms can contribute to packets loss because of late arrival.

Absolute values for jitter are not specified. If latency and loss are within specification, jitter should not be an issue for IP video surveillance. If jitter is more than 10 percent of one-way latency, additional analysis may be required.

Loss is specified separately for SD and HD IP video surveillance. The higher the image resolution, the greater number of IP packets required to the transport reference frames for MPEG-4 / H.264. Refer to the Appendix section titled *Why Packet Loss Impacts IP Video Surveillance.*

Summary

While it is important to provision sufficient bandwidth on the LAN/WAN for the average rate if IP video surveillance traffic, packet loss may be an issue if the network cannot handle the bursts associated with MPEG-4/H.264 video. The bursts are typically associated with the transport of I-frames, also know as reference frames. If reference or incremental frames are corrupted due to packet loss, the video image may have artifacts in the image that linger for several seconds until a new reference frame is successfully received.

Design Considerations

This section addresses high-level design considerations regarding how and where the network devices that make up the components of an IP video surveillance solution should be placed in the overall topology. The LAN switch is the foundation building block of an IP network and this is especially true of IP video surveillance deployments. WAN bandwidth is costly compared to that of the LAN, and as such, the majority of video feeds will remain within the LAN environment. As a design goal, video feeds should remain within the LAN as much as practical and only transported across the WAN as necessary.

The LAN switch is the basic network device for connecting IP cameras, workstations, and the NDVR. In this section, the LAN switch is defined and some basic functions are reviewed. In order for LAN switching to scale and span distances between floors and buildings in a campus environment, they are deployed in a hierarchy. This hierarchical topology is illustrated. Additionally, a review of server (NDVR), camera, and viewing station placement within the network topology is reviewed.

An important part of the network assessment process is to validate that the network topology can support the bandwidth, power (PoE), and interface type and speeds required by the IP video surveillance solution. This section provides a foundational overview of the enterprise LAN to provide context to the more specific sections that follow the address assessing network specific readiness.

LAN Switching Defined

The most basic network component in today's network is the LAN switch. LAN switches operate at the data link layer. Ethernet hubs operate at the physical layer and were used to connect Ethernet devices before switches were commercially available. LAN switches are so economical today that no IP video surveillance deployment should contain Ethernet hubs.

LAN switches use memory buffers to store incoming packets from an Ethernet port, looks at the destination MAC address of the packet, references a table of MAC addresses to destination ports, and forwards the packet out the appropriate port. The destination port could be the port of the NDVR if attached to the same switch, or an uplink port to another switch connecting the NDVR.

Ethernet ports have various transmission speeds associated with them. Switches with ports rated for 10 Mbps/100 Mbps (Ethernet/FastEthernet) are designed for IP cameras, most cameras have a network interface that is 10/100. Ports used for connecting the viewing workstation and the NDVR should be capable of GigabitEthernet (1,000 Mbps). Most switches have a bus, or backplane, which connects the ports and memory buffers; the switching fabric. A fixed configuration, 24 or 48 port switch, a 32-Gbps switch fabric with two or more uplink ports is common in the industry. The switch should support IEEE 802.3af, the standard for PoE, to provide power to the IP cameras. The Cisco Catalyst 3750G-48PS-48 switch has these specifications.

In a small business deployment, the IP cameras, NDVRs, and viewing workstations can all connect to a single switch chassis. However, the length of copper twisted pair cable runs between the camera and switch is limited to 100 meters. The NDVRs and workstations may be located in an administration building across the campus, more than 100 Meters from the IP camera. Several switches are deployed in a hierarchy to aggregate switches at different locations and provide high-speed connectivity to the NDVRs.

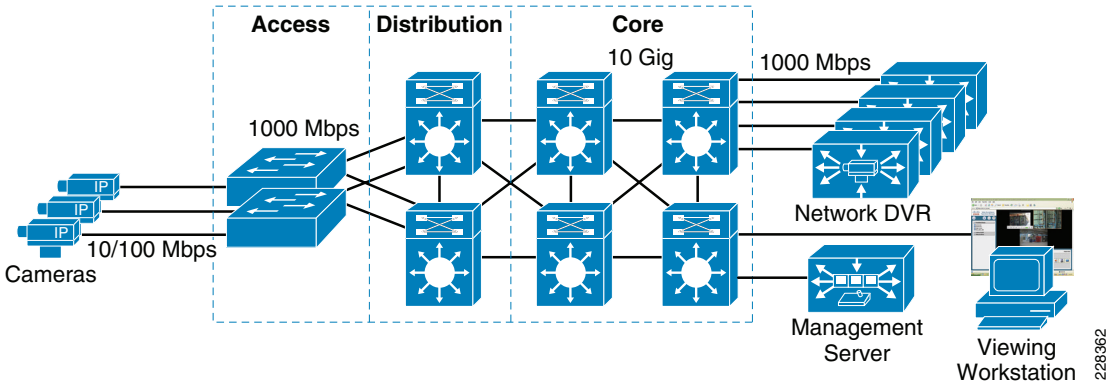
Switching Hierarchy

To scale IP networks, the network manager introduces hierarchy into the topology. The LAN switch for the wiring closed (access switch) is connected to distribution switches. These distribution switches provide uplinks to all the access switches in a building or floor. The link between the access and distribution switch is at a minimum 1 GigabitEthernet. The distribution switches then connect to core switches, often with 10 Gigabit links.

As a best practice, only Layer-2/Layer-3 switches are recommended because they eliminate the need to have a Layer-2 interface connecting the distribution layer switches. Additionally, a routed-access layer improves convergence times and enhances load sharing. For these and other reasons, many campus network deployments advocate using a Layer-3 connection to the access layer switch. For more information, refer to the *High Availability Campus Network Design—Routed Access Layer using EIGRP or OSPF* at the following URL: www.cisco.com/go/designzone.

The three tiers to this hierarch is shown in Figure 2.

Figure 2 LAN Switching Hierarchy



In Figure 2, the servers (Operations Manager/VSOM), NDVRs (Media Servers/VSMS) and viewing stations are connected to the core switches on GigabitEthernet ports. Including a server distribution layer in the topology is also an option. The hierarchical layers do not need to be distinct physical entities. Layers can be omitted, but hierarchy should be maintained for optimum performance.The IP camera port speed is 100Mbps, the uplinks are 1 Gigabit and 10 GigabitEthernet, and the NDVRs are 1 GigabitEthernet.

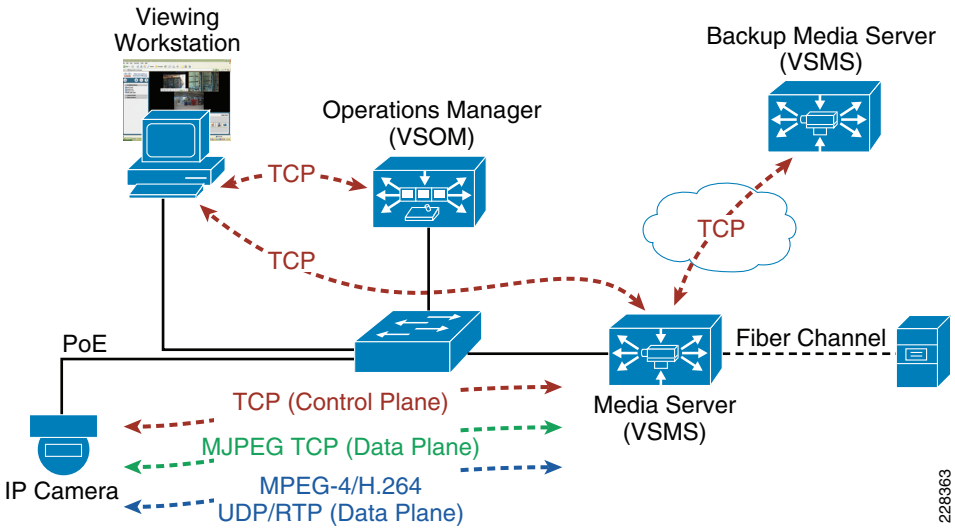
Assume that a single NDVR has sufficient disk space, memory, and CPU capacity to support 16 HD IP cameras. Video feeds are bursty by nature, and at times may send packets at line rate, (approaching 100Mbps) but for only a fraction of a second. HD IP cameras may send a H.264 reference frame every 4 seconds and this micro burst may occur for 1/20th of a second. While the likelihood that all 16 IP cameras will generate a reference frame within that same fraction of a second is slight; if it occurs, there likely will be packet loss at the port connecting the NDVR. If all the IP cameras and the NDVR are connected at 100Mbps speeds, oversubscription is likely. Attaching the NDVR at Gigabit Ethernet speeds helps to mitigate the potential for oversubscription.

For high quality, HD video surveillance, the LAN switching infrastructure must be designed to provide sufficient bandwidth at all points between the IP cameras and the NDVRs. If any of the ports between the camera and NDVR are oversubscribed, packet loss may occur and video quality is impacted. It is important to initially provision the network with sufficient capacity to minimize packet loss, but equally important is to monitor the network to ensure loss is not occurring on an ongoing basis.

Device Placement

The illustration in Figure 2 on page 12 shows IP cameras attached to the access layer and the viewing stations and servers attached to the core layer of the topology. This is a best practice deployment for a large enterprise campus. Figure 3 shows a small business deployment where all devices are attached to a single access-layer switch. Additionally, the topology shown in Figure 3 includes the sources and sinks (destinations) of the data flows between the components as well as the Layer 4 (transport) protocol used between the endpoints in a Cisco Video Surveillance Manager deployment.

Figure 3 Network Data Flows



The following subsections describe the application requirements associated with the flows in Figure 3 to provide a better understand of the network requirements of IP video surveillance.

All devices except IP cameras are attached to the switch on GigabitEthernet ports. The IP cameras are attached as FastEthernet. The topology in Figure 3 shows all devices attached to a single switch and the assumption is that all are on the same VLAN. Understanding the data flows between the devices is relevant to the single switch, single VLAN deployment, and a three-tier campus deployment.

IP Cameras

In a Cisco Video Surveillance Manager deployment, IP cameras are not viewed directly from a viewing station. The Media Server acts as a proxy between the IP camera and the viewing station. The Media Server (proxy) requests video from the IP camera at the configured frame rate/bit rate, video resolution and, protocol.

Control Plane

The control plane traffic is TCP-based and thus a two-way connection between the Media Server and the IP camera. Authentication step of the control plane is Hypertext Transfer Protocol Secure (HTTPS) and the video stream is initiated with Real-Time Streaming Protocol (RTSP). The control plan requires little bandwidth, only about 10 Kbps. In VSM Release 4.2/6.2, the camera feeds are initiated and streamed to the Media Server at all times. Even if an archive is not configured or an operator is not actively viewing the camera, the camera feed is streaming to the Media Server. This behavior is to reduce the amount of time to present a video feed to a viewing station once the camera is selected for viewing.

Data Plane

The data plane traffic between IP camera and Media Server is either TCP-based for Motion JPEG or UDP/RTP-based for MPEG-4/H.264. For planning purposes, consider the data plane traffic unidirectional, from the IP camera to the Media Server. The connectionless UDP/RTP-based MPEG-4/H.264 is solely unidirectional, with the TCP-based Motion JPEG, only the TCP acknowledgments flow from the Media Server to the IP camera. The bandwidth requirements for the data plane is a function of configured resolution, frame or bit rate and protocol (Motion JPEG or MPEG4/H.264). See Table 2.

Table 2 Per Camera Network Bandwidth Estimates

Camera	CODEC	Resolution	Frame Rate	Estimated Bitrate
CIVS-IPC-2500 (Standard Definition)	MPEG-4	D1 (720x480)	15 fps	1 Mbps
CIVS-IPC-2500 (Standard Definition)	MPEG-4	D1 (720x480)	30 fps	2 Mbps
CIVS-IPC-2500 (Standard Definition)	MJPEG	D1 (720x480)	5 fps	2.2 Mbps
CIVS-IPC-4300 or CIVS-IPC-4500 (HD)	H.264	HD (1920x1080)	30 fps	4-6 Mbps

Note The frame rate for MPEG-4/H.264 is a function of the constant bit-rate value configured. For a SD camera, a CBR rate >= 2Mbps is 30 frames per second. For the HD camera, a CBR rate >= 4Mbps is 30 frames per second.

Media Server (VSMS)

The Media Server receives video feeds from the IP cameras and streams camera feeds to viewing stations as requested. Media Servers must be connected to a GigabitEthernet switch port. However, for planning purposes, the maximum amount of I/O the chassis is capable of processing is less than the attached port speed. Table 3 represents an estimate of the Maximum I/O in Megabits per second for each chassis.

Table 3 Performance Guidelines

Server	Maximum I/O	Maximum Internal Storage
CIVS-MSP-1RU 1RU chassis	60 Mbps	4 Terabytes no RAID-5 (up to 4 750GB or 1TB SATA hard drives)
CIVS-MSP-2RU 2RU chassis	200 Mbps	12 Terabytes RAID-5 (up to 12 750GB or 1TB SATA hard drives)
CIVS-MSP-4RU 4RU chassis	200 Mbps	24 TeraBytes RAID-5 (up to 24 750GB or 1TB SATA hard drives)

Given a HD IP camera video feed at CBR 6Mbps and using the maximum I/O value of 200Mbps, it can be estimated that a 2RU/4RU chassis can support approximately 32 cameras. For every concurrent live viewing of camera feed, subtract one camera. The 1RU chassis could support up to 15 IP cameras at 4Mbps, less the number of concurrently viewed feeds.

Table 3 can be used to estimate the number of IP cameras that can be support from a network interface perspective. The storage requirements must also be estimated.

Disk Storage Requirements

The amount of disk storage required for archives is a function of the resolution, frame/bit rate, quality factors, scene complexity, and motion and retention period of the archive. Table 4 provides an estimate of the amount of disk storage required for 5 minutes of video archive. These estimates were derived from examining the file system of VSMS (Release 4.2/6.2) and averaging the file size of the individual 5 minute containers for the configured looping archives.

Table 4 Disk Storage Requirements

Camera Configuration	MegaBytes per 5 Minutes [approximate]
HD Camera H.264 1920x1080 CBR 4M (see Figure 4)	100
HD Camera H.264 1920x1080 CBR 5M (see Figure 5)	225
HD Camera H.264 1920x1080 CBR 8M (see Figure 6)	240
SD Camera MPEG-4 D1 (720x480) CBR 2M	76
SD Camera MJPEG D1 (720x480) 5 FPS (see Figure 7)	75
SD Camera MJPEG D1 (720x480) 10FPS	150

From Table 4, it is apparent that disk storage requirements are not solely a function of the constant bit-rate (CBR) parameter, even though all three cameras are 30 frames per second, using the same resolution and encoding, H.264. The scene complexity is also a factor in the storage requirements. Figure 4 and Figure 5 are relatively complex outdoor scenes with relatively little motion. The scene in Figure 5 is slightly more complex than Figure 4. Figure 6 is an indoor scene with little motion and a fair amount of spatial redundancy. Figure 7 is an example of a standard definition IP camera. The lower quality of the SD resolution is apparent when compared with the HD examples.

Note A *Cisco Video Surveillance Stream Manager Storage Calculator* is available on the internal Emerging Technologies Group Physical Security web page. Your Cisco support contacts can assist with this planning process.

Figure 4 HD Camera H.264 1920x1080 CBR 4M

Figure 5 HD Camera H.264 1920x1080 CBR 5M

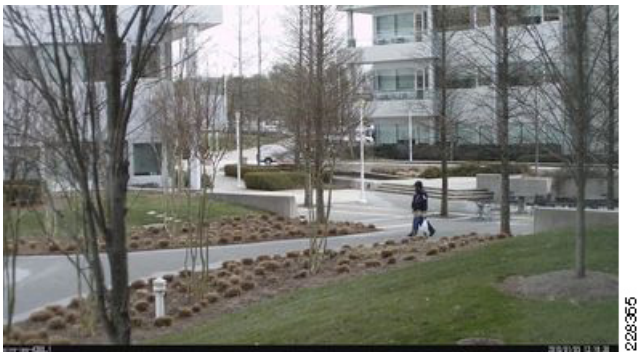
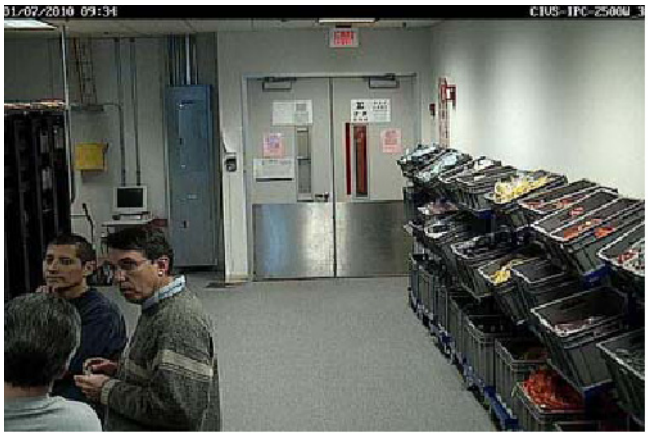


Figure 6 HD Camera H.264 1920x1080 CBR 8M

Figure 7 SD Camera 720x480 MJPEG 5 FPS



Calculating Storage Requirements

Given the 5-minute storage estimates, the disk space for a looping archive with a duration of one hour, one day or several days can be calculated. Given the 100 Mbytes for a 5-minute archive, the disk requirement for one hour is 1.2 Gigabytes (100MB * 12) and 28 Gigabytes per day (1.2 GB * 24).

Conversely, the daily disk storage requirements for the 240 Mbytes 5-minute archive setting would be approximately 70 GB per 24 hours.

Tip A Terabyte is 1,000 Gigabytes.

RAID-5 Capacity Calculations

RAID-5 combines three or more disks to prevent data loss if one disk fails. The Nevada Gaming Commission (NGC) standards and many others require RAID-5 capability. The RAID-5 algorithm stores parity bits across all disks and thus some storage capacity is lost to support fault tolerance. To calculate the effective capacity, use the following formula:

(*single drive capacity* * *number of drives*) * ((*number of drives* - 1) / *number of drives*)

Given a single drive of 640MB and 4 drives total, the calculation is as follows:

(640 * 4) * ((4 - 1) / 4) = 1,920 MB

The 2RU/4RU chassis support RAID-5, the 1RU chassis does not.

Note The more disks in the array, the less capacity loss as a percentage of total capacity is incurred.

Operations Manager (VSOM)

The bandwidth requirements between viewing station and the Operations Manager is minimal. During login and configuration of the IP cameras, there may be bursts of 1 to 2Mbps for a few seconds. However, from the standpoint of an operator viewing a live or archived video feed, the majority of the data traffic is from the Media Server and the control plane traffic from the Operations Manager IP address is minimal. Provided the latency and packet loss values are within the recommended interval, the bandwidth requirements are trivial.

Viewing Station

A viewing workstation must have sufficient CPU and video card performance to render the video feeds from the Media Server. Recall that the Media Server acts as a direct proxy between the IP camera feeds and the viewing station. From a planning standpoint, consider the amount of bandwidth required between the IP camera and the Media Server to also be available between the viewing station and the Media Server for those feeds being displayed.

As a best practice, the workstation is connected to a GigabitEthernet switch port. For displaying HD H.264 video, the workstation must meet the following system requirements:

- Windows XP with Internet Explorer 6.x, SP2 and above
- Intel Dual-Core 2.66-GHz or higher
- 1 GB of RAM or higher
- Nvidia Video card: EVGA 8600GTS 675MHZ 512MB 2.0GGHZ GDDR3 PCI-E DUAL DVI or similar

In testing for this document, a dual core 2.6 GHz AMD Opteron - 2 GB RAM PC with a GeForce 8800GTS (G92) 512MB 256-bit GDDR3 PCI Express 2.0 x16 HDCP Ready SLI Supported Video Card is deployed.

Note Video Surveillance Monitoring Workstation Baseline Specification is available internally at http://wwwin.cisco.com/etg/physec/files/vsm_clientspec.pdf. Please request a copy of this document from your normal support channels for more information.

Backup Media Server

In Figure 3 on page 13, a backup media server is shown in the topology. A Media Server at a central location can be defined as a backup Media Server in the VSOM administration section. Once defined to the system, when you create an archive (or edit an existing archive), you can see the **Backup** tab and can configure remote backups. The **Backup** tab includes a time of day specification for initiating the backup. The backup is started at the specified time and the backup files are transported from the remote Media Server to the backup Media Server over a TCP/HTTP session. The remote Media Server initiates the connection to TCP port 80.

The amount of data transported depends on the size of the archive, which is a function of resolution, frame or bit rate, encoding and length of the archive. The available bandwidth between the two Media Servers is a consideration when conducting a network assessment. For sample QoS configurations, refer to *QoS Considerations for Backup Media Servers* in "Appendix" section on page 64.

Fibre Channel Attached Storage

The MSP-1RU, MSP-2RU and MSP-4RU chassis all have the capability to supplement internal storage with external storage attached via Fibre channel. This optional interface is the CIVS-FC-1P PCI-e Fibre Channel. For more information on the Cisco Physical Security Multiservices Platform, see the following URL:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6918/ps9145/ps9152/product_bulletin_c25-490682.html

Summary

In planning the deployment of IP video surveillance, it is important to understand the video flows between the various components and ensure there is sufficient network bandwidth and switch ports of sufficient speed to connect all devices. Other than the IP cameras that are attached at FastEthernet speeds, all other servers and workstations are attached at GigabitEthernet.

Additionally, the number of IP cameras defined to each Media Server is a function of the amount of network traffic generated by the camera and this is directly related to the resolution, protocol and frame/bit rate configured for that camera. The amount of disk storage that must be available to the server is a function of the resolution, protocol and frame/bit rate configured for that camera(s) and the retention period configured in the video archive definition.

Specific Network Requirements

This section addresses how to assess specific aspects of the existing network. The goal is to determine what, if any, existing network deficiencies exist before implementing IP video surveillance on the network. Many of the topics discussed in this section are also useful to obtain basic and fundamental troubleshooting information for problems which may arise in a post implementation phase. This section has five main topics:

- Assessing Switching (LAN) Readiness, page 20
- Assessing Routing Readiness, page 33
- Service Level Assessments, page 43
- Security and Application Optimization Assessment, page 56
- Quality-of-Service (QoS) Assessment, page 58

The first two sections are focused on conducting a network inventory that should lead to a network topology diagram. High level capacity planning information should also be gathered during these two assessment steps. Of primary importance is to verify that no existing errors, capacity or resource constraints such as CPU or memory shortages exist in the network. If they exist, these issues must be addressed before implementing IP video surveillance.

"Service Level Assessments" section on page 43 provides example Cisco IOS IP Service Level Agreements (SLAs) commands that can be implemented on Cisco devices to measure the video surveillance application requirements for latency, loss, and jitter. This section is the toolset that can be used in a pre- and post- implementation of IP video surveillance.

Finally, the "Network Assessment Checklist" section on page 59 is provided to help complete a network assessment study in the proposed network.

Assessing Switching (LAN) Readiness

This section provides guidelines to the physical security integrator and network engineer for assessing the readiness of the LAN switches to transport IP video surveillance traffic. Recommendations are based on various interface counters and other statistics. Because of this, it is critically important to clear all switch interface counters in the network on a periodic basis. Clearing interface counters is accomplished by issuing the Cisco IOS privilege **clear counters** command manually on the command line or through some scripted or automated process. Ideally, this should be done weekly at the beginning of the business week. By scripting and automating this process, any interface statistics are consistent in timeframe between neighboring devices and provide a known point from the last time the counters were cleared. This greatly facilitates conducting the initial network assessment and on-going network troubleshooting and analysis.

This section addresses the following topics relating to conducting a network readiness assessment on the enterprise LAN network:

- Inventory—The model and software versions deployed on the network are to be documented
- Ports/Interfaces—To determine available capacity and type of interfaces in use and available
- VLANs—This information provides insight on how the physical switch is logically partitioned
- Power-over-Ethernet (PoE)—As many IP cameras require PoE, inventory available power capacity
- Physical Connectivity—In this section, an inventory of existing devices by port is determined
- Environmental Statistics—Display and record the power and cooling status of switches

- Memory Utilization—Display and verify all switches have sufficient memory
- Local Link Issues—Verification that no link errors or capacity issues exist on the network
- Overall Capacity Assessment—Capacity of trunks between switches and routers are examined
- Logging and Network Time Protocol—To aid in troubleshooting and as a network management best practice.

Tip Interface counters should be cleared every 7 days on a routine basis to aid in troubleshooting. The network assessment should be conducted between 5 and 7 days following the interface counters being cleared.

Inventory

As part of the planning process, the switch IOS version, model, uptime, reason for last reload, memory, and configuration register session should be obtained and documented for all switches in the network. The **show version** command can be used to obtain this information. The following is an illustration:

```
vpn2-3750-access#show version | include uptime|System|Confi|memory
Copyright (c) 1986-2009 by Cisco Systems, Inc.
vpn2-3750-access uptime is 21 weeks, 2 days, 7 hours, 28 minutes
System returned to ROM by power-on
System restarted at 10:05:23 edt Tue Aug 18 2009
System image file is "flash:c3750-ipservicesk9-mz.122-50.SE3.bin"
cisco WS-C3750G-24PS (PowerPC405) processor (revision F0) with 131072K bytes of
memory.
512K bytes of flash-simulated non-volatile configuration memory.
System serial number            : FOC1034Y1W6
Configuration register is 0xF
```

Ports / Interfaces

As part of the assessment, each switch in the network should be examined and documented for the total number of physical ports by type, speed (e.g., 100baseTX, FastEthernet twisted pair copper) and capability (e.g., PoE). The number of ports active and inactive should also be documented on a per switch basis. This provides an indication of the available port capacity in the network.

To facilitate the inventory assessment, the **show interfaces status** command provides a tabulation of the physical interface / port, description, status, VLAN, duplex, speed, and type for ports. Ports that have a status of connected are in use, the *notconnected* status shows ports that are available in the system. Sample output is shown as follows:

```
vpn2-3750-access#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/1   trunk to vpn1-2851 connected    trunk      a-full  a-100 10/100/1000BaseTX
Gi1/0/2   WireShark on PC un connected    208        a-full a-1000 10/100/1000BaseTX
Gi1/0/3   4300 IP camera 002 connected    220        a-full  a-100 10/100/1000BaseTX
Gi1/0/4   4300 IP camera 002 connected    220        a-full  a-100 10/100/1000BaseTX
Gi1/0/5   Viewing Station [L connected    220        a-full a-1000 10/100/1000BaseTX
Gi1/0/6   CIVS-IPC-2500 ESEL connected    206        a-full  a-100 10/100/1000BaseTX
Gi1/0/7   Linksys PVC2300-F4 connected    216        a-full  a-100 10/100/1000BaseTX
Gi1/0/8   Axis 207MW         connected    210        a-full  a-100 10/100/1000BaseTX
Gi1/0/9   CIVS-IPC-2500W_3   connected    220        a-full  a-100 10/100/1000BaseTX
Gi1/0/10  FlashNet vpn-jk2-f connected    156          full    100 10/100/1000BaseTX
Gi1/0/11  CIVS-IPC-4500-2    connected    220        a-full  a-100 10/100/1000BaseTX
Gi1/0/12  CIVS-IPC-4500-1    connected    220        a-full  a-100 10/100/1000BaseTX
Gi1/0/13  CIVS-IPC-4500-4 Po connected    220        a-full  a-100 10/100/1000BaseTX
```

```
Gi1/0/14  CIVS-IPC-4500-3    connected    220        a-full  a-100 10/100/1000BaseTX
Gi1/0/15  HD Compatable View connected    220        a-full a-1000 10/100/1000BaseTX
Gi1/0/16  ROOM150A camera fo connected    210        a-full  a-100 10/100/1000BaseTX
Gi1/0/17  ese-mediasvr-cc1   connected    220        a-full a-1000 10/100/1000BaseTX
Gi1/0/18  ese-vsom-vm-cc1    connected    220        a-full a-1000 10/100/1000BaseTX
Gi1/0/19  trunk to vpn1-3854 connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/20  trunk to vpn-jk2-7 connected    trunk      a-full  a-100 10/100/1000BaseTX
Gi1/0/21  trunk to vpn-jk2-7 connected    trunk      a-full  a-100 10/100/1000BaseTX
Gi1/0/22  trunk to vpn1-2851 connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/23  trunk to  vpn1-285 connected    trunk      a-full a-1000 10/100/1000BaseTX
Gi1/0/24                     notconnect   2            auto   auto 10/100/1000BaseTX
Gi1/0/25                     notconnect   2            auto   auto Not Present
Gi1/0/26                     notconnect   2            auto   auto Not Present
Gi1/0/27                     notconnect   2            auto   auto Not Present
Gi1/0/28  Trunk to vpn5-3560 connected    trunk      a-full a-1000 1000BaseSX SFP
vpn2-3750-access#
```

The *Name* column in the above output is derived from the interface description. This is manually entered by the network administrator who configured the switch. It is an optional field. The description for GigabitEthernet 1/0/14 is shown from the running configuration of this switch.

```
vpn2-3750-access# show run interface gigabitEthernet 1/0/14
!
interface GigabitEthernet1/0/14
 description CIVS-IPC-4500-3
 switchport access vlan 220
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 001e.bdfc.19c9
 load-interval 60
 mls qos trust dscp
 spanning-tree portfast
 spanning-tree bpdufilter enable
end
```

Tip The **show platform pm link-status** command also provides link state for each port number on the switch.

As a best practice, during the network assessment, an inventory of the existing network is an important step in determining the available physical capacity of the network.

VLANs

Virtual LANs (VLANs) are logical instead of physical connections. VLANs devices attached to ports of several physical switches can communicate at Layer 2 as if they were attached to the same physical switch. Trunk ports between switches transport packets between switches and use a tag (header) to associate the packets with their respective VLAN. The IEEE 802.1Q (typically referred to as *dot1q*)is the most common VLAN tagging standard in use today.

VLAN Trunking Protocol (VTP) is a Layer-2 messaging protocol that manages the addition, deletion, and renaming of VLANs on a network-wide basis. If VTP is running in the network and no pruning is taking place, all switches in the network (assuming the same domain) should have the same amount of VLANs defined. For more information on VTP, refer to *VTP Introduction* at the following URL*:* http://www.cisco.com/en/US/tech/tk389/tk689/tk706/tsd_technology_support_sub-protocol_home.html

One advantage of implementing Layer-3 connectivity to the access layer is to eliminate the need for Layer-2 trunks and the complexity of troubleshooting Spanning Tree issues and eliminating the need for defining VTP domains. However, many installations will have Layer-2 connectivity between switches and as part of the network assessment an inventory of the existing VLANs on all switches is required. To determine the number of VLANs on each switch, issue the **show vlan summary** command as follows:

```
vpn2-3750-access#show vlan summary
Number of existing VLANs           : 67
 Number of existing VTP VLANs      : 67
 Number of existing extended VLANs : 0
```

To determine what VLANs are configured on which port, the **show vlan brief** command can be issued to determine which ports are associated with a VLAN. If there are no ports listed for a VLAN, this is an indication that the VTP pruning feature can be implemented to restrict unnecessary VLAN traffic from entering a switch.

```
vpn2-3750-access#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
2    VLAN0002                         active    Gi1/0/24, Gi1/0/25, Gi1/0/26
                                                Gi1/0/27
90   vlan090                          active
206  vlan206                          active    Gi1/0/6
208  vlan208                          active    Gi1/0/2
210  vlan210                          active    Gi1/0/8, Gi1/0/16
216  vlan216                          active    Gi1/0/7
220  vlan220                          active    Gi1/0/3, Gi1/0/4, Gi1/0/5
                                                Gi1/0/9, Gi1/0/11, Gi1/0/12
                                                Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                Gi1/0/17, Gi1/0/18
230  VLAN0230                         active
353  vlan353                          active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

In the above example, VLAN 230 is active, but has no ports assigned to it on this switch, while VLAN 220 has eleven ports associated. VLANs that have no active ports could be pruned. As part of the network assessment, the VLAN names and intended use should be part of the assessment documentation. VLANs that are defined but not used should be noted and can be removed from the topology.

Power-over-Ethernet (PoE)

The following example shows how to verify the inline power configuration for the fixed configuration 3750 access switch. The summary of the available, used, and remaining Watts provide useful information for inventorying the existing power consumption and available capacity.

```
vpn2-3750-access#show power inline

Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1           370.0      111.4       258.6
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi1/0/1   auto   off        0.0     n/a                 n/a   15.4
```

```
Gi1/0/2   auto   off        0.0     n/a                n/a   15.4
Gi1/0/3   auto   on         13.0    CIVS-IPC-4300      3     15.4
Gi1/0/4   auto   on         13.0    CIVS-IPC-4300      3     15.4
Gi1/0/5   auto   off        0.0     n/a                n/a   15.4
Gi1/0/6   auto   on         9.0     CIVS-IPC-2500      3     15.4
Gi1/0/7   auto   on         15.4    Ieee PD            3     15.4
Gi1/0/8   auto   off        0.0     n/a                n/a   15.4
Gi1/0/9   auto   off        0.0     n/a                n/a   15.4
Gi1/0/10  auto   off        0.0     n/a                n/a   15.4
Gi1/0/11  auto   on         13.0    CIVS-IPC-4500      3     15.4
Gi1/0/12  auto   on         13.0    CIVS-IPC-4500      3     15.4
Gi1/0/13  auto   on         13.0    CIVS-IPC-4500      3     15.4
Gi1/0/14  auto   on         13.0    CIVS-IPC-4500      3     15.4
```

Physical Connectivity

IP cameras should be attached to a switch port that supports FastEthernet (10/100Mbps). The recommendation is a speed of 100Mbps, full duplex. If the cameras require PoE, the switch must support the IEEE 802.3af—PoE standard. The maximum cable length is 100 meters. The 100BASE-TX standard specifies a minimum of Category 5 copper cabling with two twisted pairs.

Client PCs (viewing stations) and all servers (VSMS Media Servers and VSOM Operations Manager) must be connected and configured for 1000Mbps (1 GigabitEthernet). While the GigabitEthernet standard requires auto-negotiation, when attached to a switch port, the speed must always negotiate to GigabitEthernet and the duplex setting always full duplex. The 1000BASE-T (also known as IEEE 802.3ab) standard is for GigabitEthernet over copper wiring. Each 1000BASE-T network segment can be a maximum length of 100 meters and must use Category 5 cable at a minimum. Category 5e cable or Category 6 cable can be substituted.

These physical connectivity requirements and the inventory of the existing network devices are important part of the network assessment to determine what, if any, additional switches must be ordered to support the implementation.

MAC Address Table

All Cisco IP cameras and those from other manufactures have the hardware address (MAC) printed on a label attached to the external housing. Using the MAC address as part of the description or name field when defining cameras to VSOM is a practical technique. Regardless of the IP address assigned to the IP camera, the MAC address remains the same. Capturing the MAC address as an identifier for the camera during deployment along with the type, model, and other information such as firmware version is useful information for on-going troubleshooting and support. The following commands illustrate how to use the **mac address-table** command on the switch to view the MAC address of the device attached to switch port g1/0/4. In this example, the device is a Cisco 4300 Series camera, which also supports CDP. However, IP cameras from other manufactures may not support CDP and displaying the **mac address-table** is one technique for identifying these devices.

```
vpn2-3750-access#show mac address-table  interface g1/0/4
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 220    0021.1bfd.df62    STATIC      Gi1/0/4
Total Mac Addresses for this criterion: 1

vpn2-3750-access#show cdp neighbors g1/0/4
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
```

```
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
00211BFDDF62     Gig 1/0/4         121               H    CIVS-IPC- eth0
vpn2-3750-access#sh run interface g 1/0/4
!
interface GigabitEthernet1/0/4
 description 4300 IP camera 0021.1bfd.df62
 switchport access vlan 220
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0021.1bfd.df62
 load-interval 60
 mls qos trust dscp
 spanning-tree portfast
 spanning-tree bpdufilter enable
end
```

The **show mac address-table** command has several subcommands that are useful for conducting the inventory and initial site survey. The form **show mac address-table vlan 220**, for example, can be used to list all the MAC addresses and ports associated with a particular VLAN; in this case, VLAN 220. To list all the ports on the switch which have port security enabled (an anti-tampering technique) use the following form of the command:

```
show mac address-table secure
```

One additional use is to identify switch ports that are connected to hubs or other switches.This is information must be captured during the initial site survey. Ports with multiple MAC addresses associated with a single VLAN on a port are non-trunk interfaces that are connected to another switch or hub. The following is an example:

```
vpn2-3750-access#show mac address-table interface g1/0/10
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 156    0001.c972.5408    DYNAMIC     Gi1/0/10
 156    0004.dd0d.fd4b    DYNAMIC     Gi1/0/10
 156    000a.8b7e.d408    DYNAMIC     Gi1/0/10
 156    000e.d756.7520    DYNAMIC     Gi1/0/10
 156    000e.d77b.04e0    DYNAMIC     Gi1/0/10
 156    000e.d77b.06c0    DYNAMIC     Gi1/0/10
 156    000e.d7a4.f340    DYNAMIC     Gi1/0/10
 156    000e.d7a5.4220    DYNAMIC     Gi1/0/10
 156    0013.808b.3930    DYNAMIC     Gi1/0/10
 156    0013.808b.39f0    DYNAMIC     Gi1/0/10
 156    0013.808b.3a10    DYNAMIC     Gi1/0/10
 156    0013.c403.d610    DYNAMIC     Gi1/0/10
 156    0015.2b6c.0f43    DYNAMIC     Gi1/0/10
 156    0015.c798.a000    DYNAMIC     Gi1/0/10
 156    001a.6c60.4c48    DYNAMIC     Gi1/0/10
 156    001a.6c84.a5a0    DYNAMIC     Gi1/0/10
 156    001a.6c84.a5b0    DYNAMIC     Gi1/0/10
 156    001a.6c84.a604    DYNAMIC     Gi1/0/10
 156    0022.90a4.5a12    DYNAMIC     Gi1/0/10
 156    0050.5480.8b22    DYNAMIC     Gi1/0/10
 156    0050.5480.8eda    DYNAMIC     Gi1/0/10
 156    00b0.64fd.5900    DYNAMIC     Gi1/0/10
 156    00b0.64fd.5908    DYNAMIC     Gi1/0/10
Total Mac Addresses for this criterion: 23
```

If multiple MAC addresses are leaned on a single port and more than one VLAN is represented, this is an indication of a trunk interface. The following is an example:

```
vpn2-3750-access#show mac address-table interface g1/0/1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 210    0005.0101.63cd    DYNAMIC     Gi1/0/1
 220    0005.0101.63cd    DYNAMIC     Gi1/0/1
 220    000e.d756.7521    DYNAMIC     Gi1/0/1
 220    0014.6a21.b06a    DYNAMIC     Gi1/0/1
   1    0005.0101.63cd    DYNAMIC     Gi1/0/1
   1    0005.0127.dbfb    DYNAMIC     Gi1/0/1
```

By using the **mac address-table** and the **show cdp neighbors** commands, the inventory collection phase of the network assessment can be completed and an accurate representation of the network topology can be documented.

Tip If no MAC address is learned on a port with a device attached, the following are possible explanations to consider: Are packets being received? Is the expected MAC address learned on another port? Check if dot1x is in use; if so, is the port authorized? Does port security allow more MAC addresses? Is the port in spanning tree forwarding?

Environmental Statistics

The **show environment** command is used to display environmental status information (power supply, fan status, and temperature information) and power input to the chassis. Power supplies and fans are frequently the root cause of switch failures because they may have a higher failure rate than other components that make up the switch.

As a best practice, all switches in the network should be checked to verify that the environmental statistics are within operating parameters. Switches with temperature or fan problems should be noted in the assessment and identified for more investigation.

```
vpn2-3750-access#show env all
FAN is OK
TEMPERATURE is OK
Temperature Value: 38 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 51 Degree Celsius
Red Threshold    : 61 Degree Celsius
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
 1  Built-in                                         Good

SW  Status          RPS Name          RPS Serial#  RPS Port#
--  -------------   ----------------  -----------  ---------
1   Not Present     <>
```

In the above sample output, the reported temperature value of 38 degrees is substantially lower than the warning (yellow) threshold of 51 degrees. Temperatures that are too high may be caused by a internal fan issue or airflow problem where the switch is mounted.

CPU Utilization

The main CPU is not used for normal switching of traffic between ports. CPU utilization can become high due to traffic sent to the CPU for processing or processes running on the CPU consuming resources. Switches have separate queues for different types of traffic that must be send to the main CPU for processing. Examples of traffic which must be sent to the main CPU are as follows:

- Routing protocol traffic
- traffic destined to the switch (tacacs, ssh, telnet, icmp)
- Spanning Tree traffic
- IGMP snooping
- CDP traffic

Packet drops in the spanning tree queue (dropped BPDUs) due to high CPU associated with spanning tree can lead to instability in the network. This is also true for routing protocol traffic processing. Spanning tree and routing protocol instability will lead to packet loss in the network which will degrade the video quality. Using CPU cycles in itself is not a problem, only if the CPU consumption is constantly high or excessive due to some network anomaly.

As a best practice, before implementing IP video surveillance on the network, the CPU utilization for the switches in the network should be examined to ensure there are no current network instability due to high CPU utilization. The **show processes** command should be used to identify switches that are encountering high CPU levels and these must be noted in the assessment audit.

```
vpn2-3750-access#show processes cpu  sorted
CPU utilization for five seconds: 8%/0%; one minute: 9%; five minutes: 9%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
 207   383244916 217671074       1760  3.03%  3.04%  3.03%   0 Spanning Tree
  96        1620       585       2769  0.47%  0.16%  0.07%   0 Exec
  63     5496701 671650611          8  0.15%  0.05%  0.00%   0 Fifo Error Detec
 147     4665843   2537655       1838  0.15%  0.02%  0.00%   0 HQM Stack Proces
   4    16559355   1523159      10871  0.00%  0.19%  0.18%   0 Check heaps
   5         954      1325        720  0.00%  0.00%  0.00%   0 Pool Manager
   6           0         2          0  0.00%  0.00%  0.00%   0 Timers
   3        4869       576       8453  0.00%  0.00%  0.00%   0 SpanTree Helper
```

Tip The **show processes cpu history** command is useful to look at CPU trends over time.

Memory Utilization

Memory utilization analysis is used to verify that switches are not low on memory. Switches that are have free memory less than 20 percent of the total value by memory category (processor, I/O, etc.) should me more closely monitored and considered candidates for upgrade or replacement.

Processor memory is used by Cisco IOS. For example, processor memory is used to store and execute the software imaged loaded on the switch. I/O memory is used for packets sent to the CPU. I/O memory is not used for normal packet switching between ports.

The memory inventory can be displayed by the following commands:

```
vpn2-3750-access#show version  | include memory
cisco WS-C3750G-24PS (PowerPC405) processor (revision F0) with 131072K bytes of
memory.
512K bytes of flash-simulated non-volatile configuration memory.
```

```
vpn2-3750-access#show memory statistics
                Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor    3F6E4B4    72264100    45076392    27187708    25570756    16768896
      I/O    6400000    12582912     8532852     4050060     3992492     4047808
Driver te    2C00000     1048576          44     1048532     1048532     1048532
```

Local Link Issues

Local link issues can be the cause of degraded video quality. It is important when deploying the components of the IP video surveillance solution that the individual ports and interfaces, including trunk interfaces connecting switch and routers do not encounter physical errors.

The error counters are reset by the **clear counter** command. It is highly recommended to routinely clear the interface counters on a weekly basis so any errors reported are relevant to the recent operation of the network. By clearing all the interface counters on the network at a predefined time, errors on adjacent routers and switches can be more apparent.

Errors

Examining the interface counters on a periodic basis, ideally a few days after the **clear counter** command is issued, is a best practice to determine if there are physical errors or capacity issues which may adversely impact video quality. Once the video surveillance system is deployed, examine the interface counter for signs of problems. Examples of the **show interfaces counters** command are as follow:

```
vpn2-3750-access#show interfaces counters errors

Port        Align-Err     FCS-Err    Xmit-Err     Rcv-Err  UnderSize  OutDiscards
Gi1/0/1             0           0           0           0          0         7774
Gi1/0/2             0           0           0           0          0            0
Gi1/0/3             0           0           0           0          0            0
Gi1/0/4             0           0           0           0          0            0
```

Alternately, more details on individual interfaces can also be viewed as follows:

```
vpn2-3750-access#show interface g1/0/2 counters errors

Port        Align-Err     FCS-Err    Xmit-Err     Rcv-Err  UnderSize  OutDiscards
Gi1/0/2             0           0           0           0          0 0

Port      Single-Col  Multi-Col   Late-Col  Excess-Col  Carri-Sen      Runs Giants
Gi1/0/2            0          0          0           0          0         0 0
```

- Alignment Errors—This column displays a count of the number of frames received that do not end with an even number of octets and have a bad CRC. This is an indication of a cable problem or a faulty transmitter on the network equipment connected at the other end. This count should either be zero or very low. When the cable is first connected, some errors may occur. Additionally, if there is a hub connected, collisions between other devices on the hub may also cause these errors. This column is representative of alignment errors relative to received frames.
- FCS Error—The Frame Check Sequence (FCS) Error% column count is the number of frames that were transmitted/received with a bad checksum (CRC value) in the ethernet frame. These frames are dropped and not propagated onto other ports. A few of these errors are OK, but could also be an indication of bad cables, NICs, etc.

- Undersize—Are frames received that are smaller than the minimum IEEE 802.3 frame size of 64bytes long (excluding framing bits, but including FCS octets) that were otherwise well formed; check the device sending out these frames.
- Xmit-Err and Rcv-Err—Indicates that the transmit or receive buffer is full.
- Out-Discards—If you have a large number of deferred frames or Out-Discard (also referred to as Out-Lost on some platforms), it means that the switch's output buffers have filled up and the switch had to drop these packets. This may be an indication that there is too much traffic that goes through this port.

Link Capacity

Even with all the interfaces in the network operating without any physical errors, capacity planning must be considered. There are a variety of free-ware and commercial software packages available to monitor interface utilization. However, as part the network assessment, and as a post deployment and ongoing management effort, the individual switches can be queried to provide a snapshot into current capacity. The **show controller utilization** command can be used to look at a summary of interface utilization.

```
vpn2-3750-access#show controller utilization
Port       Receive Utilization  Transmit Utilization
Gi1/0/1            2                    6
Gi1/0/2            0                    0
Gi1/0/3            6                    0
Gi1/0/4            2                    0
Gi1/0/5            0                    0
Gi1/0/6            1                    0
Gi1/0/7            0                    0
Gi1/0/8            0                    0
Gi1/0/9            4                    0
Gi1/0/10           0                    0
Gi1/0/11           8                    0
Gi1/0/12           2                    0
Gi1/0/13           6                    0
Gi1/0/14           8                    0
Gi1/0/15           0                    0
Gi1/0/16           2                    0
Gi1/0/17           0                    4
Gi1/0/18           0                    0
Gi1/0/19           0                    1
Gi1/0/20           2                    2
Gi1/0/21           0                    0
Gi1/0/22           0                    0
Gi1/0/23           0                    0
Gi1/0/24           0                    0
Gi1/0/25           0                    0
Gi1/0/26           0                    0
Gi1/0/27           0                    0
Gi1/0/28           1                    0

Total Ports : 28
Switch Receive Bandwidth Percentage Utilization  : 0
Switch Transmit Bandwidth Percentage Utilization : 0

Stack Ring Percentage Utilization : 0
```

Looking at an individual port provides more detailed information from the summary displayed above. In this deployment, a VSMS (Media Server) is attached to interface G1/0/17. There are six HD (1920x1080 resolution) IP cameras and one SD (D1 resolution) camera streaming to this Media Server. The images shown in "Disk Storage Requirements" section on page 15 are snapshots from this server. From the

summary screen above, the transmit utilization is 4 percent. This value is calculated from the interface counters. The details of the counters can be seen with the **show interface** command for that interface. Review the following output:

```
vpn2-3750-access#show interfaces g1/0/17
GigabitEthernet1/0/17 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 0019.2f98.0111 (bia 0019.2f98.0111)
  Description: ese-mediasvr-cc1
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 10/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:02, output hang never
  Last clearing of "show interface" counters 00:33:44
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  30 second input rate 172000 bits/sec, 308 packets/sec
  30 second output rate 41435000 bits/sec, 3649 packets/sec
     625513 packets input, 43812572 bytes, 0 no buffer
     Received 3 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     7282563 packets output, 10322427766 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

The *txload* value is 10/255 or 4 percent. The output rate is approximately 41 Mbps (41,435,000 bits/sec). It is a full-duplex Gigabit interface and the interface counters were cleared 33 minutes and 44 seconds earlier. There are no output drops on this interface and no errors since the interface counters were cleared. In Table 3 on page 14, estimates for server I/O targets are listed for the various appliances. By looking at the interface statistics above, actual I/O statistics can be measured against what was estimated during implementation planning.

Tip The **show controllers ethernet-controller gigabitEthernet 1/0/17** command can be used to view interface statistics including a breakdown of the size of frames sent and received on the interface.It also provides additional information on error counters.

Overall Capacity Assessment

Analyzing switch traffic on a node-by-node basis may not provide much value, but correlating it relative to the entire network can produce valuable results. The first step is to produce a topology diagram of the existing network that includes switches, routers, servers and end-node devices such as IP cameras. Then the amount of traffic that is traversing through the switches and routers in the network can be assessed at a point in time. This allows the network assessment to identify the busiest switches in the network as well as switches that have the most active ports based on the total traffic.

Logging and Network Time Protocol

Syslog and Network Time Protocol (NTP) are recommended configuration on all switches. This subject is also referenced and discussed in the "Assessing Routing Readiness" section on page 33. The following configuration is from a Cisco 3720 switch and shown as an example of the clock, NTP, and logging configuration.

```
service timestamps log datetime msec localtime show-timezone
!
clock timezone est -5
clock summer-time edt recurring
!
logging buffered 65536
logging trap debugging
logging 192.0.2.186
!
ntp server 172.26.156.1
```

With logging enabled, events such as link and line protocol up/down can be logged and identified. In this example, a viewing station Ethernet cable was removed and re-inserted:

```
Jan 14 10:49:45.953 est: %LINEPROTO-5-UPDOWN: Line protocol on
InterfaceGigabitEthernet1/0/5, changed state to down
Jan 14 10:49:47.950 est: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/5, changed state to
down
Jan 14 10:49:52.631 est: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/5, changed state to
up
Jan 14 10:49:52.639 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/5, changed state to up
```

By logging to the buffer and syslog server, events in the network can be identified and troubleshooting is facilitated. As a best practice, the network assessment should make note of the existing switch configuration and implement logging and NTP in the network as part of the site survey and assessment.

Summary

The purpose conducting a switch readiness assessment focuses on conducting an inventory of the switches in the network and providing this information to the documentation phase of the network assessment. By capturing a snapshot of the CPU, memory and interfaces statistics, the network manager can discover if any switches in the network need software or hardware upgrades. Additionally, any existing interface problems, whether they be hardware errors or capacity issues can be identified and addressed before video surveillance is implemented on the network.

By verifying that all the switches are logging both to their logging buffers as well as to a syslog server, with timestamps synchronized to a common clock source by way of NTP, problems in the network can more easily be identified and corrected. By identifying the total VLANs in use the network and which ports are associated with the specific VLANs, a logical topology diagram can be created as an overlay to the physical topology.

There is a considerable resources available to the network engineer with best practice guidelines on campus LAN designs, best practices and troubleshooting. They include the following:

- Enterprise Campus 3.0 Architecture: Overview and Framework

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html
- *Cisco LAN Switching (CCIE Professional Development Series)* Publisher:Cisco Press; illustrated edition (September 5, 1999) by Kennedy Clark and Kevin Hamilton

The following Networkers 2009 sessions provide extensive troubleshooting information on Cisco Catalyst switches that comprise many network deployments:

- Troubleshooting Cisco Catalyst 3750, 3550, and 2900 Series Switches - BRKRST-3141
- Troubleshooting Cisco Catalyst 4500 Series Switches - BRKRST-3142
- Troubleshooting Cisco Catalyst 6500 Series Switches - BRKRST-3143

Note The introduction of Cisco Networkers Virtual (CNV), launched in January 2009, provides access to all Cisco Networkers content including, breakout sessions, techtorials and keynote presentations for customers and partners. Delegates who attended CNW2009 can access the online content free of charge however, there is a subscription fee to access the content for non-attendees. See the following URL for the CNV platform: http://wwwin.cisco.com/europe/tcmo/brandexperience/eventmarketing/customerevents/ciscone tworkers2009/resources/index.shtml

Assessing Routing Readiness

This section provides guidelines to the physical security integrator and network engineer for assessing the readiness of the routers and Layer-3 switches to transport IP video surveillance traffic. Historically, routers provided WAN connectivity only and switches or hubs provided LAN connectivity. In many network deployments, routing can be deployed in the LAN environment down to the access-layer switch infrastructure.

Routing at the access layer as described in the *High Availability Campus Network Design--Routed Access Layer using EIGRP or OSPF* (http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/routed-ex.html) is considered a best practice. By deploying routing to the access layer, this means that all of the LAN switching infrastructure is both a Layer-2 switch and Layer-3 router. This means that the routing readiness assessment is a key element and of prominent importance to deploying video surveillance, even if the video feeds never cross a WAN interface.

In this section, recommendations are based on various interface counters and other statistics.As a result, it is critically important to clear all router interface counters in the network on a periodic basis. Clearing interface counters is accomplished by issuing the Cisco IOS privilege command **clear counters** manually on the command line or through some scripted or automated process. Ideally, this should be done weekly at the beginning of the business week. By scripting and automating this process, the interface statistics are consistent in timeframe between neighboring devices and provide a known point from the last time the counters were cleared. This greatly facilitates conducting the initial network assessment and on-going network troubleshooting and analysis.

This section addresses the following topics relating to conducting a network readiness assessment on the enterprise network:

- Inventory—Collecting information on the model and software versions running in the network
- CPU Utilization—Collecting and understanding router CPU utilization
- Memory Utilization—Displaying and analyzing memory utilization
- Environmental Statistics—Displaying and recording power and cooling of high-end routers
- Buffer Tuning—Best practices on configuring IOS to tune buffers automatically
- Logging—Emphasis the importance of syslogs to aid in network troubleshooting
- Interfaces—A primer on interface statistics and what statistics are important to network health
- Switching Path Analysis—Includes recommendations on load sharing and asymmetrical routing
- Routed Protocol Analysis—Identify routed protocols on the network
- Routing Protocol Analysis—Identify what routing protocols are in use on the network
- Bridged Protocol Analysis—Identifying any bridged protocols on the network
- Summary—Includes general best practices recommendations

Tip Interface counters should be cleared every 7 days on a routine basis to aid in troubleshooting! The network assessment should be conducted between 5 and 7 days following the interface counters being cleared. For more information, see the "Clearing Interface Counters" section on page 80.

Inventory

As part of the planning process, the router's IOS version, model, uptime, reason for last reload, memory, and configuration register session should be obtained and documented for all routers in the network. The **show version** command can be used to obtain this information. Following is an illustration.

```
router#show version | inc uptime|System|Config|memory
Copyright (c) 1986-2008 by Cisco Systems, Inc.
ROM: System Bootstrap, Version 12.3(11r)T1, RELEASE SOFTWARE (fc1)
rtp5-esevpn-gw5 uptime is 30 weeks, 6 days, 23 hours, 54 minutes
System returned to ROM by Reload Command at 17:26:20 edt Fri May 1 2009
System restarted at 17:27:52 edt Fri May 1 2009
System image file is "flash:c3825-advipservicesk9-mz.124-15.T4"
Cisco 3825 (revision 1.0) with 1010688K/37888K bytes of memory.
250368K bytes of ATA System CompactFlash (Read/Write)
Configuration register is 0x2102
```

Most installations standardize on a release and version of Cisco IOS and deploy it on all the like routers in the network. The recommendation for configuration register is 0x2102.

CPU Utilization

Router CPU utilization may not provide a useful indicator of overall performance of the network. For example, the Cisco ASR 1000 Series routers have a distributed control plane architecture. A separate control processor is embedded on each major component in the control plane. One of which is the Route Processor (RP)—A general purpose CPU responsible for routing protocols, CLI, network management interfaces, code storage, logging, and chassis management. It also processes network control packets as well as protocols not supported by the Cisco ASR 1000 Series ESP.

Alternatively, the Cisco 3800 Series Integrated Services Routers use the main CPU for packet switching in addition to processing routing protocols, CLI and similar control plane functions. In these platforms, CPU utilization below 50 percent are ideal, and ranges from 50 to 80 percent for the 5-minute average should be monitored more closely. The **show processes cpu** command can be used to determine the overall CPU utilization. The **show processes cpu history** is also useful to look at CPU utilization over time.

Memory Utilization

As part of the network assessment, the status of the installed memory in all routers must be investigated and analyzed to verify that no router in the network is experiencing memory leaks or low memory conditions. The **show memory statistics** command is used to obtain information regarding the memory utilization of a router.

```
vpn-jk2-7206-1#show memory statistics
                Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor   65CCAF70   120802980    53249052    67553928    67405300    53694116
      I/O    E000000    33554432     8220096    25334336    24807280    24796028
Transient   6D000000    16777216       22332    16754884    16262604    16750836
```

Processor memory is the memory used by the Cisco IOS. The I/O memory allocation is shared between the CPU and interface controllers. I/O memory is used for all packet switching, either fast or process switching. Any buffer tuning commands, **buffers small permanent 400**, for example, will decrease the amount of available I/O memory. Buffers are allocated from I/O memory, not from processor memory on shared memory routers.

Beginning in Cisco IOS Release 11.0, if processor memory is exhausted (zero bytes free), Cisco IOS will begin to borrow, or allocate memory out of I/O memory to satisfy memory allocation requests. For example, if the OSPF process needs 36 bytes of memory and there is zero processor memory available, the allocation will come out of I/O memory. Thus, I/O memory is a backup pool for the processor pool. This explains how a router can continue to function with zero processor memory free.

Symptoms of Insufficient Free Memory

Expect to experience thee following symptoms on routers with insufficient memory.

- MALLOCFAIL (Memory Allocation Failure) messages on console or log:

```
Mar 16 15:55:53 est: %SYS-2-MALLOCFAIL: Memory allocation of 4856 bytes failed from
0x30D345C, pool Processor, alignment 0-Process= "OSPF Router", ipl= 0, pid= 1
```

- Telnet sessions refused, *% Connection refused by remote host*
- '*show proc mem*' command displayed no matter what command you type on console
- *%% Low on memory; try again later* messages on the console port
- *Unable to create EXEC - no memory or too many processes*' messages on console
- *% Configuration buffer full, can't add command:* after a 'wr t'
- Memory Corruption crash ('valiblock' in stack)—It might corrupt its memory and cause a memory corruption crash.

Of course, the memory allocation failures will influence the behavior of the processes requesting memory, loss of routes, corrupted OSPF data bases and will contribute to network instability.

Memory Leaks

If free memory is decreasing continuously, there is a memory leak. The **show processes memory sorted** command can be used to determine which process is holding the most memory, sorted in descending order. If Free Processor Memory is below 25 percent of the total memory installed, the router should be monitored closely. The Largest Block Free (Bytes) column refers to the largest block of contiguous memory. Values less than 250Kytes are cause for concern. The Largest column refers to the largest block of contiguous memory available. If this value is decreasing over time it means that memory is being fragmented. For routers that are up for more than a year may experience some memory fragmentation which can be addressed by a scheduled reload during a maintenance window.

Routers which are low on memory or have a memory leak can be forced to reload rather than function impaired due to memory allocation failures. Examples of these commands are as follow:

```
exception memory fragment {value}
exception memory minimum io {value}
exception memory minimum {value}
```

Values specified depend on the total memory installed.

If any router in the network is experiencing low memory conditions, the assessment should note this and the problem must be addressed before deploying IP video surveillance on the network.

Environmental Statistics

Environmental statistics include router air temperature, power supply statistics. For the high-end router platforms, both power supplies are monitored to validate normal operation. Typically, high-end routers only report environmental statistics. For example, the **show environment** command can be used on a 7200 Series to determine if all measured values are in the normal range. Actual temperatures and voltages can be displayed from their last measured value, as illustrated in the following sample output:

```
vpn-jk2-7206-1#show environment last
  I/O Cont Inlet     previously measured at 28C/82F
  I/O Cont Outlet    previously measured at 29C/84F
  NPE Inlet          previously measured at 31C/87F
  NPE Outlet         previously measured at 31C/87F
  +3.45 V            previously measured at +3.45
  +5.15 V            previously measured at +5.23
  +12.15 V           previously measured at +12.24
  -11.95 V           previously measured at -11.81
  last shutdown reason - power supply shutdown
```

Issues related to power supplies and air flow/cooling are important for high availability and must be monitored on an ongoing basis.

Buffer Tuning

In early versions of Cisco IOS, buffer tuning was a manual process by which the individual buffers were analyzed and the appropriate values changed to eliminate buffer failures and misses. Beginning in the 12.3(14)T version of Cisco IOS, this can be done automatically using the **buffers tune automatic** configuration command. The **show buffers tune** command shows what tuning happened and the old and new values.

It is a best practice and highly recommended that the **buffers tune automatic** configuration command be used where available.

Logging

Many network-related problems can be isolated and identified by viewing the system log and interface counters and statistics. As a best practice, routers should always log to the logging buffer and to a syslog server to assist with network diagnostic. The following commands are sample syslog related parameters.

```
service timestamps log datetime msec localtime show-timezone
logging buffered <logging buffer size>
logging trap debugging
logging source-interface GigabitEthernet0/0
logging 192.0.2.186
```

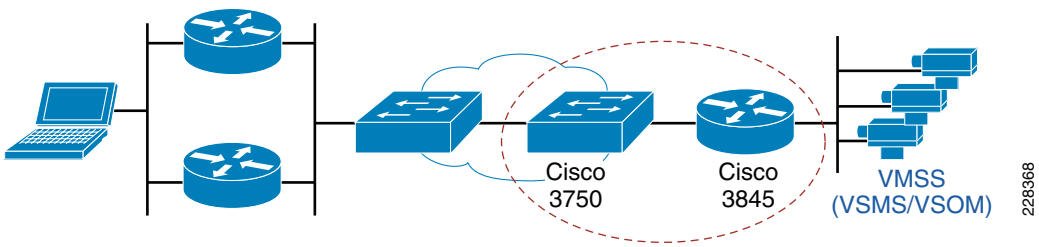
Including a timestamp in the log file is a best practice. There is an extensive example of using NTP for IP video surveillance deployments in the “Time Synchronization using Network Time Protocol” section of the *Cisco IP Video Surveillance Design Guide* at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/IPVS/IPVS_DG/IPVS_DG.pdf

Logging buffer size is configurable and ranges from a size of 4096 to 2147483647. A value of 65535 is a reasonable initial value and can be decreased or increased accordingly.

Interfaces

Many network-related issues can be addressed by analyzing the output from a **show log** and **show interface command.** Before deploying IP video surveillance on the network, a review of the interfaces that transport video traffic is highly recommended. In this section, an example of an interface transporting video surveillance traffic is examined.

Figure 8 Reference Network Topology



There are three aspects of the router interface that is examined; configuration, utilization and errors. As an example, a show interface command output is shown from the 3845 router in the previous illustration. Items of note are highlighted in blue and are discussed in the subsequent text.

Note The switch interface configuration and **show interface** command is available in "Switch Configuration—Reference Network Topology" section on page 79.

Show interfaces

When this command was issued, the viewing station was monitoring three video surveillance cameras through the VSOM server on the VMSS network module installed in the 3845 shown in the topology diagram.

```
vpn1-3845-1#show interfaces gigabitEthernet 0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is BCM1125 Internal MAC, address is 0022.55a9.5f51 (bia 0022.55a9.5f51)
  Description: Trunk
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 3/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is RJ45
  output flow-control is XON, input flow-control is XON
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 13800000 bits/sec, 1569 packets/sec
  30 second output rate 7436000 bits/sec, 965 packets/sec
     1896286283 packets input, 1145717374 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 66630131 multicast, 0 pause input
     0 input packets with dribble condition detected
     467392465 packets output, 911073511 bytes, 0 underruns
     2 output errors, 0 collisions, 1 interface resets
```

```
     0 babbles, 0 late collision, 0 deferred
     2 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
vpn1-3845-1#
```

Because the interface counters have not been manually cleared, the uptime of the router is relevant to understand the timeframe of the error counters.

```
vpn1-3845-1#show version | include uptime
vpn1-3845-1 uptime is 2 weeks, 3 days, 23 hours, 48 minutes
```

From this output, the context of the error counters is the past 2 1/2 weeks. If the interface counters have not been manually cleared or the router recently reloaded, the error counters lose their significance and relevance to the current state of the network.

Configuration

An important part of the network assessment is the documentation and inventory component and using the interface configuration information from the **show interfaces** command provides much useful information. In this example, we can see that the interface is GigabitEthernet, it has negotiated GigE speed and is correctly configured as full-duplex and is a 802.1Q trunk interface, connected to the switch port with a CAT5 copper cable as RJ45.

Tip The **show cdp neighbors g0/1 detail** command can be used to identify the Cisco switch interface this router interface is attached.

The network topology diagram should show the router interface, connected switch interface (port) and speeds, duplex and type of encapsulation.

Utilization

A snapshot of the current interface utilization can be seen from the *txload* and *rxload*, and the input and output rate values. The *txload* and *rxload* are determined from the observed data rates as a function of the implicit or explicitly configured bandwidth command on the interface. If the bandwidth configuration command is entered incorrectly, the txload and rxload values will be incorrect.

The input and output rates are calculated on a default basis of 5 minutes. This default interval can be changed with the *load-interval* interface configuration command. In this example, *load-interval 30,* is configured, which is why the rates are based on 30 second values.

Tip Observing the current interface utilization does not take the place of ongoing, long term capacity planning based on network management tools, which provide trend analysis and long-term historical data.

The loading is shown as a fraction with denominator of 255. Therefore 1/255 is the lowest reported loading value which is 0.39 percent. During the network assessment phase of the project, loads over 50 percent of the available bandwidth for the interface should be highlighted and monitored. For services which are provisioned over Ethernet handoff from the service provider, calculating the interface load may be more complicated than with a point-to-point serial interface because the committed data rate may be a fraction of the clock rate of the interface. For example, a service provider may provision a GigabitEthernet interface that is policed to 50Mbps on the customer premise switch.

For more information on issues around Ethernet handoff services, see the *Ethernet Access for Next Generation Metro and Wide Area Networks* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Ethernet_Access_for_NG_MAN_WAN_V3.1_external.html

Broadcasts and Multicasts

The broadcast counters should indicate no more than 10 to 20 percent broadcast packets to total packets received on the interface. One reason why broadcasts may be a high percentage would be if the link is receiving little or no end-user application traffic. Multicast traffic may be a high percentage of the total packets received on the link if the end-nodes are legitimately generating IP multicast (IPmc) feeds. For example, if a network camera is enabled for IPmc, then the multicast counter should be representative of this traffic.Routing protocols also generate IPmc traffic. For example, EIGRP uses both multicast and unicast packets between neighbors.

Error Counters

The error counters reported on the show interfaces command can be very useful in determining if any physical or data link errors exist which will adversely impact the quality of video feeds. The error counters are reset by the **clear counter** command. It is highly recommended to routinely clear the interface counters or a weekly basis so any errors reported are relevant to the recent operation of the network. By clearing all the interface counters on the network at a predefined time, errors on adjacent routers and switches can be more apparent.

Input and Output Errors, Resets

A common example of an input error is a CRC. Input errors are typically caused by a hardware error on the adjacent device. For example, a router may report input errors due to a faulty port on the switch port the router interface is connected. Output errors in many cases are indicative of hardware failures of the sending interface on the router. Output errors are incremented for any reason that prevented the final transmission of packets out of the interface. Any input error value for cyclic redundancy check (CRC) errors, framing errors, or aborts suggests some kind of link problem. Theses errors should be very low or zero and not increasing.

Resets occur if packets queued for transmission were not sent within several seconds time or the interface is manually reset.

As a best practice, CRC errors should not exceed one per million bytes of data transmitted.

Total Output Drops

This counter lists packets dropped on output. An interface showing output drops is not always a cause for concern, as packet drops by a QoS service policy on the interface are accumulated in this counter. Packet drops by QoS can be expected behavior, priortizing video and voice packets over data traffic. Interfaces with output drops require more investigation.

Input Queue Drops

Packets that are destined for the router itself (such as routing protocol packets) or packets which cannot be fast switched and therefore sent to process switching go through the input queue and could be dropped. Input queue drops should be low or zero and not increasing. As a general guideline, more than 50 per hour should warrant additional analysis. If input queue drops are rapidly increasing or excessive, refer to the *Troubleshooting Input Queue Drops and Output Queue Drops* for information on debugging this issue at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080094791.shtml#topic2

Switching Path Analysis

For IP protocols, Cisco Express Forwarding (CEF) is the preferred and default switching path. NetFlow switching has been integrated into CEF switching. For more information on switching paths on please refer to the *Cisco IOS Switching Paths Overview* at the following URL:

http://www.cisco.com/en/US/docs/ios/12_2/switch/configuration/guide/xcfovips.html

All routers in the network should have their switching path verified. This can be accomplished by using the **show ip interface** command. Sample command output is shown as follows:

```
vpn1-3845-1#show ip interface gigabitEthernet 0/1.342
GigabitEthernet0/1.342 is up, line protocol is up
  Internet address is 192.168.15.78/30
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is enabled
  IP CEF switching is enabled
  IP CEF VPN Flow Fast switching turbo vector
  VPN Routing/Forwarding "IPVS"
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, Flow cache, CEF, Full Flow
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
```

From the above output, it can also be verified that policy routing is disabled and that no NAT/pNAT is enabled on this IP interface. Additionally, the interface is in a VRF named IPVS. Because this interface is not in the global routing table, but rather the virtual routing table IPVS, the global routing table will not show this interface, routing protocol neighbors, or routes learned through the interface. The virtual routing table must be referenced instead.

Load Sharing

Load sharing is a function of the switching path, not the routing protocol. The routing protocol may insert two or more equal or unequal cost paths into the routing table, but it is a function of the switching path to use more than one next hop to reach the destination network. Two or more equal cost paths are

can be used to load share packets by Cisco Express Forwarding (CEF) and fast switching. CEF provides better granularity as it load shares on a per source, per destination basis while fast switching is based only on per destination. Per packet load-sharing can be accomplished by process switching or CEF per packet; however, this is not recommended for voice and video traffic. Using per packet load-sharing for voice and video (real-time applications) increases the likelihood of incurring out-of-order packets. Out-of-order packets are often dropped by the receiver because they arrived too late for playout.

Warning **Per packet load sharing is not recommended for voice or video applications.**

For more information and examples on load sharing, refer to the *V3PN: Redundancy and Load Sharing Design Guide* at the following URL:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008074f2cb.pdf

Asymmetric Routing

Asymmetric routing is when the network path from source IP address to destination IP address is different than the return path. Asymmetric routing is common on the Internet as well as enterprise networks with multiple paths for redundancy or load sharing. The "Asymmetric Routing" section on page 77 details how to enable multiple paths for redundancy but only use the backup path in the event of a path failure. This technique effectively eliminates asymmetric routing. Asymmetric routing may make troubleshooting more complicated. If there is asymmetric routing in the network, the assessment should note this and further analysis is required.

Routed Protocol Analysis

The term routed protocols define those network protocols that are routed at the network layer. Examples include Appletalk, DECnet, IP, IPX, and Vines. Most enterprise networks have standardized on IP and is the only routed protocol in use. If there are other routed protocols in use on the network, the assessment should note this and further analysis is required.

As a best practice, IP should be the only routed protocol on the network that transports video surveillance traffic.

Routing Protocol Analysis

A routing protocol sends routing information packets to adjacent routers and, in turn, receives routing information packets. A routing protocol is the control plane for a routed protocol. Examples of IP routing protocols are BGP, EIGRP, IGRP, IS-IS, RIP, and OSPF. Enhanced IGRP (EIGRP) can be used as the routing protocol for Appletalk and IPX as well as IP. Most enterprise networks use either EIGRP or OSPF as their interior gateway routing protocol. BGP is an exterior gateway routing protocols and is typically used on the Internet between enterprise networks and service provider networks. It is also used by service providers offering MPLS-based VPNs.

If any routing protocol other than EIGRP, OSPF, or BGP is used in the network, the assessment should note this and further analysis is required.

There are many texts available for a better understanding of routing protocols and their design and implementation. *Routing TCP/IP, Volume 1, 2nd Editio*n and *Routing TCP/IP, Volume II* by By Jeff Doyle, Jennifer DeHaven Carroll are examples.

Bridged Protocol Analysis

Bridged protocols include source-route bridging (SRB), Remote Source-Route Bridging (RSRB), Data Link Switching Plus (DLSw+), Synchronous Data Logical Link Control (SDLLC), and Transparent bridging. In general, DLSw+ is more scalable and easier to configure in the presence of 'any-to-any' SNA connectivity requirements. Data Link Switching is an open standard, while RSRB is Cisco proprietary. If there are any bridged protocols other than DLSw+, the assessment should note this and further analysis is required.

Summary

The purpose of the router readiness assessment is to provide an inventory of the routers in the network and include this information to the documentation phase of the network assessment. By capturing a snapshot of the CPU, memory, and interfaces statistics, the network manager can discover if there are routers in the network that need software or hardware upgrades. Additionally, any existing interface problems, whether they be hardware errors or capacity issues, can be identified and addressed before video surveillance is implemented on the network.

By verifying that all the routers are logging both to their logging buffers as well as to a syslog server, with timestamps synchronized to a common clock source by way of NTP, problems in the network can more easily be identified and corrected. By identifying the routed, bridged, and routing protocols used on the network, an assessment is made on the currentness of the applications and protocols used.

There are many books available that provide the network engineer with best practice guidelines on network design and implementation. They include, but are not limited to the following:

- *Cisco IOS Management for High Availability Networking: Best Practices White Paper* at the following URL: http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800a998b.shtml
- *Cisco ISP Essentials* by Barry Raveendran Greene, Philip Smith was published in 2002 and may be out of currently out of print. Enterprise network managers can benefit from reading this text as well as the target audience; Internet service providers. Some online version of this documentation may be available as an Internet resource under the heading of "Essential IOS Features Every ISP Should Consider."
- *Advanced IP Network Design* by Alvaro Retana (Author), Don Slice (Author), Russ White

Service Level Assessments

This section addresses the recommended tools and techniques that are available to determine the functional characteristics of the network transporting IP video surveillance. Given that video feeds are sensitive to loss and latency, some consistent method to monitor and measure these values is required. Ping, or ICMP echo, is commonly used as the utility, in some form, exists on most every IP-based operating system. Ping can report both round trip latency and packet loss. The **ping** command is available on routers, switches, Unix and Linux workstations and Apple and Microsoft based laptops and PCs.

While ping is commonly available, the accuracy and consistently from platform to platform may vary widely. If the target IP address of a ping request is a Cisco router, the ICMP packet must be handled in process switched mode by the main CPU. Responding to ICMP requests is not the primary function of the router. ICMP has been used as the basis for many denial-of-service attacks on routers and other hosts, responding to them may be rate limited, further skewing the reported results.

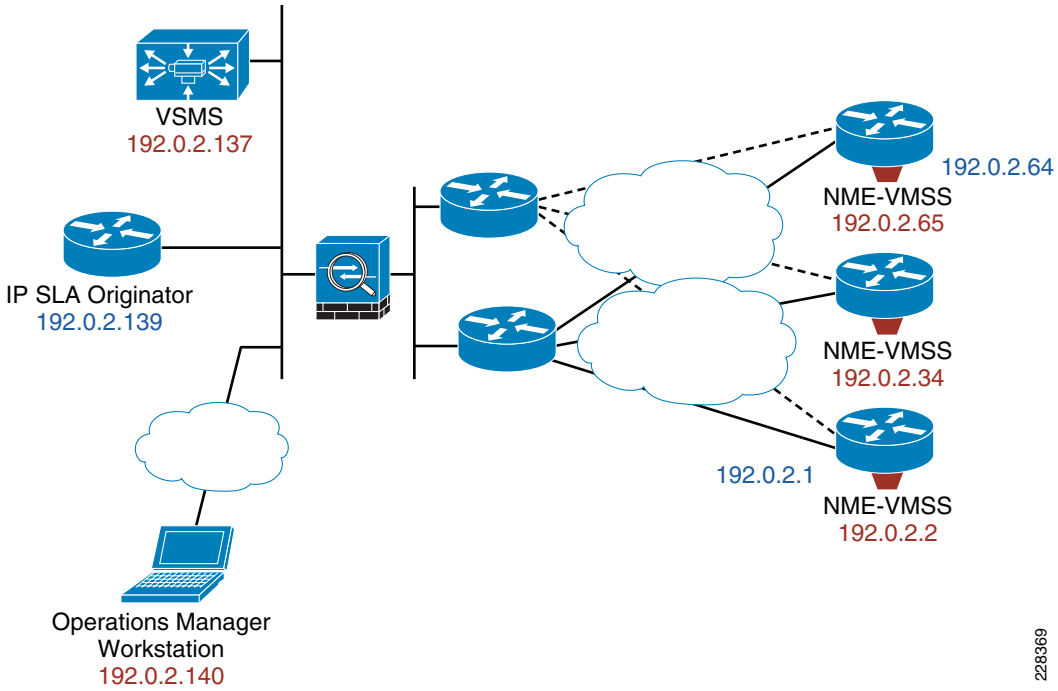
Tip Ping should only be used as a screening tool, providing only a preliminary assessment of the characteristics of the network.

The recommended tool for measuring overall network performance is Cisco IOS IP Service Level Agreements (SLAs). Cisco IOS IP SLAs uses probes, (traffic generated by the source router) to provide a predictable and consistent measurement of network performance. Many large enterprise network deployments implement IP SLA on routers dedicated solely for generating and responding to the probes. They are also called dedicated (shadow) SLAs routers. These are typically called *one-arm* routers, meaning they have a single network interface, by which they receive and generate packets originating from the router itself. IP SLA is included in most all Cisco IOS images, the one-arm routers are deployed to use this IOS feature and are not otherwise part of the network path. Typically, shadow routers deployed in this manner are low-end and less costly routers. Examples are Cisco 880 or 1800 Series routers.

While a router in the Cisco 881 or 1811 Series is cost effective, many deployments may not afford to dedicate a router at each branch location. An alternate solution is to deploy an originating IP SLA router in the main command center, and use the branch router and/or hosts at the branch to respond to the probes. Some probes must have a Cisco IOS IP SLAs *responder* to answer the probe, while other probes can be answered by most any IP-based operating system. The example probe configuration in this section is shown configured on the originating IP SLA router. These samples are marked indicating if they require a *Cisco IOS IP SLAs Responder* or any host can respond- *IP Host Responde*r.

Figure 9 is used to illustrate the network topology. IP addresses shown in blue are *Cisco IOS IP SLAs Responders,* while any *IP Host Respond*ers are shown in red.

Figure 9 Service Level Assessment Sample Topology



In the topology shown in Figure 9, Cisco IOS IP SLA probes are originated from the router at 192.0.2.139. The target of the probes are the VSMS server on the same subnet, as well as the Operations Manager workstation that is attached to the subnet by a MPLS Pseudo wire WAN. The latency of the WAN network which connects this viewing station is evident in the sample output shown later in this section. There is an ASA firewall connecting the command center LAN to the corporate network. There are three remote branch offices each with a Cisco ISR router and NME-VMSS (Video Management and Storage System network module). The branch offices are MetroEthernet attached and the video is accessed through a DMVPN encrypted tunnel. The NME-VMSS modules run a Linux operating system with the VSOM and VSMS sharing the same IP address of the module.

Table 5 illustrates these IP addresses, device or host, and if the IP address is owned by Cisco IOS and can therefore supports an IP SLA responder.

Table 5 Service Level Assessment Device Table

IP Address	Device/Host	ip sla responder
192.0.2.139	vpn-jk3-2651xm-9 Cisco IOS router (originating probes)	Yes, also source
192.0.2.137	VSMS - Media Server	No
192.0.2.1	Cisco IOS Router	Yes
192.0.2.2	NME-VMSS (Linux)	No
192.0.2.34	NME-VMSS (Linux)	No
192.0.2.64	Cisco IOS Router	Yes
192.0.2.65	NME-VMSS (Linux)	No
192.0.2.140	Windows PC	No

IP SLA Control Protocol

Cisco IOS IP SLA incorporates a patented control protocol between the source and destination devices. This control protocol is required for UDP jitter operations and optional for UDP echo and TCP connect operations. The control protocol is enabled by including the **ip sla responder** command in the configuration of the target router. As a best practice, include the **ip sla responder** command in all routers in the network to facilitate troubleshooting.

With the control protocol enabled, prior to sending a probe packet, the initiating router sends a control message that includes information such as protocol, port number, and duration. When the responder receives this control message, enables the specified UDP/TCP port for a specified duration and listens for probes. Once it responds to the probes, or the specified duration expires, the ports used by the probes are disabled. For added security of Cisco IOS IP SLAs control messages, MD5 authentication can be configured.

The **show ip sla responder** command can be used to verify the **ip sla responder** command is included in the configuration and that the target router is receiving probes.

```
vpn1-3845-1#show ip sla responder
IP SLAs Responder is: Enabled
Number of control message received: 3457 Number of errors: 0
Recent sources:
        192.0.2.139 [09:45:19.157 est Tue Dec 22 2009]
        192.0.2.139 [09:40:19.150 est Tue Dec 22 2009]
        192.0.2.139 [09:35:19.143 est Tue Dec 22 2009]
        192.0.2.139 [09:30:19.135 est Tue Dec 22 2009]
        192.0.2.139 [09:25:19.128 est Tue Dec 22 2009]
Recent error sources:
```

The control protocol listens on UDP port number 1967. Any firewalls between the source and destination routers must have a rule to permit communication on UDP 1967 as well as the ports and protocols used by the probes themselves. The network administrator can verify the ports the router is listening on by using the **show control-plane host open-ports** command. Output from this command is shown in the "Appendix" section on page 64.

Types of Probes

Cisco IOS IP SLA can be configured to generate several different types of probes. Of the probes that are supported, several have application to the IP video surveillance deployment. They are as follows:

- ICMP Echo Operation
- TCP Connect Operation
- HTTP Operation
- UDP Jitter Operation

Each operation is discussed as to its application to the IP video surveillance deployment and sample configurations are shown.

ICMP Echo Operation

The ICMP echo operation is fundamentally a ping issued by way of the Cisco IOS IP SLA subsystem. Because ICMP echo request/response is implemented by most IP-based operating systems, this probe has application to most all hosts. However, the accuracy of Cisco IOS IP SLAs is much better than ICMP ping between two routers, if the Cisco IOS IP SLAs responder is enabled on the target router.

Many IP video surveillance cameras may have access control lists enabled that may block network traffic from some hosts. Also host-based firewalls may also block ICMP packets. Cisco IOS routers may rate limit ICMP responses or respond only on a best effort basis.

In the sample configuration, the viewing station, a Windows PC at IP address 192.0.2.140, is the target host. The protocol data size in the payload is set at 1400 bytes. This size is configured as it is a typical packet size for video feeds to a viewing station. The Type of Service byte (ToS) is configured as decimal value of 96. This value is the marking used for control plane traffic and is equivalent to IP Precedence value of 3 or DSCP value of CS3. The probe timeout value, the number of milliseconds the operation waits to receive a response from its request packet, is set at 200ms. The tag value is simply a text label. The probe identifier is 8140, which is simply a numerical identifier of the probe.

One advantage of Cisco IOS IP SLA over a PC or workstation originating the ICMP echo request is the ability to maintain a history of the success or failure of the probe and the reported round trip times. The sample probe has a frequency, is generated, every 30 seconds and the history commands are included to maintain a history table in memory of the originating router.

```
ip sla 8140
 icmp-echo 192.0.2.140
 request-data-size 1400
 tos 96
 timeout 200
 tag PC_Viewing_Station
 frequency 30
 history lives-kept 1
 history buckets-kept 60
 history filter all
ip sla schedule 8140 life 86400 start-time now
```

This probe is scheduled to start immediately (now) and has a life of 86400 seconds, or 24 hours. Following the expiration of the lifetime, the probe remains in the configuration of the router but is not initiated.

Intended Use Case

This probe has considerable application for diagnosing network connectivity issues that may be intermittent and not currently demonstrated. For example, assume the workstation operator is reporting loss of video feeds to the viewing station for short periods of time. By configuring this probe along with the history command, the date and time of probes that are lost or exhibit long round trip times can be documented. By having the workstation operator note the date and time of the reported outages, it can be determined if the outage is network related or application related.

The most recent probe operation can be displayed with the **show ip sla statistics** command as shown in the following example:

```
vpn-jk3-2651xm-9#show ip sla statistics 8140

Round Trip Time (RTT) for       Index 8140
        Latest RTT: 56 milliseconds
Latest operation start time: 10:54:04.522 est Thu Dec 10 2009
Latest operation return code: OK
Number of successes: 39
Number of failures: 1
Operation time to live: 84809 sec
```

The above output demonstrates a probe with 56ms round trip time and the latest probe was successful. By displaying the history table, the success or failure of past probes can be examined. In the following output, bucket index number 1 has a 48ms RTT. Bucket number 21 has a Sense code of 4 with no CompT listed, meaning the probe failed, perhaps due to packet loss.

```
vpn-jk3-2651xm-9#show ip sla history 8140
        Point by point History
Entry    = Entry number
LifeI    = Life index
BucketI  = Bucket index
SampleI  = Sample index
SampleT  = Sample start time
CompT    = RTT (milliseconds)
Sense    = Response return code

Entry LifeI      BucketI    SampleI    SampleT    CompT      Sense      TargetAddr
8140  1          1          1          6288527    48         1          192.0.2.140
8140  1          2          1          6291527    52         1          192.0.2.140
8140  1          3          1          6294528    53         1          192.0.2.140
8140  1          4          1          6297527    48         1          192.0.2.140
8140  1          5          1          6300527    48         1          192.0.2.140
8140  1          6          1          6303528    48         1          192.0.2.140
8140  1          7          1          6306528    48         1          192.0.2.140
8140  1          8          1          6309527    52         1          192.0.2.140
8140  1          9          1          6312528    48         1          192.0.2.140
8140  1          10         1          6315528    48         1          192.0.2.140
8140  1          11         1          6318527    48         1          192.0.2.140
8140  1          12         1          6321527    48         1          192.0.2.140
8140  1          13         1          6324528    52         1          192.0.2.140
8140  1          14         1          6327528    49         1          192.0.2.140
8140  1          15         1          6330527    48         1          192.0.2.140
8140  1          16         1          6333528    44         1          192.0.2.140
8140  1          17         1          6336528    52         1          192.0.2.140
8140  1          18         1          6339527    52         1          192.0.2.140
8140  1          19         1          6342527    48         1          192.0.2.140
8140  1          20         1          6345528    48         1          192.0.2.140
8140  1          21         1          6348527    0          4          192.0.2.140
8140  1          22         1          6351527    48         1          192.0.2.140
8140  1          23         1          6354528    44         1          192.0.2.140
8140  1          24         1          6357528    52         1          192.0.2.140
8140  1          25         1          6360547    200        1          192.0.2.140
8140  1          26         1          6363528    48         1          192.0.2.140
8140  1          27         1          6366528    48         1          192.0.2.140
8140  1          28         1          6369527    48         1          192.0.2.140
8140  1          29         1          6372527    48         1          192.0.2.140
8140  1          30         1          6375528    48         1          192.0.2.140
8140  1          31         1          6378527    48         1          192.0.2.140
8140  1          32         1          6381527    48         1          192.0.2.140
8140  1          33         1          6384528    48         1          192.0.2.140
8140  1          34         1          6387528    48         1          192.0.2.140
8140  1          35         1          6390527    48         1          192.0.2.140
8140  1          36         1          6393527    49         1          192.0.2.140
8140  1          37         1          6396528    48         1          192.0.2.140
8140  1          38         1          6399527    48         1          192.0.2.140
8140  1          39         1          6402527    52         1          192.0.2.140
8140  1          40         1          6405528    56         1          192.0.2.140
8140  1          41         1          6408528    48         1          192.0.2.140
```

The default tabular option is useful for identifying trends. For example, if the listed RTT values are within a few milliseconds in the reported value and there are no lost probes (Sense code '4'), it is usually an indication of a stable, consistent network connection. If the listed RTT values vary widely and there are frequent lost probes, the network may be experiencing congestion or some interface error condition which is influencing the delay and loss of the probes. Consequently, video feeds will likely be experiencing similar delay and loss as are the probes, albeit on a more pervasive basis, given the number of packets per second of video data is likely substantially higher than the probes generated.

Individual history entries can be viewed with the **full** option. This output is useful for associating a date and time with an individual probe history row.

```
vpn-jk3-2651xm-9#show ip sla history 8140 full
Entry number: 8140
Life index: 1
Bucket index: 1
Sample time: 10:34:34.525 est Thu Dec 10 2009
RTT (milliseconds): 48
Response return code: OK

Life index: 1
Bucket index: 2
Sample time: 10:35:04.526 est Thu Dec 10 2009
RTT (milliseconds): 52
Response return code: OK

Life index: 1
Bucket index: 3
Sample time: 10:35:34.527 est Thu Dec 10 2009
RTT (milliseconds): 53
Response return code: OK
```

The date and time stamps are from the system clock on the router initiating the Cisco IOS IP SLA probes. This router must be configured to peer with an NTP time source so the time is synchronized with a universal clock.

Tip Use ICMP echo with a history table to aid in identifying intermittent network outages that cause packet loss. The history helps identify how consistent the round trip times are to each branch location. Every Branch router can each be configured to generate a probe to the IP address of the dedicated Cisco IOS IP SLA router, or the dedicated router can configure a probe each branch.

TCP Connect Operation

The TCP connect operation makes a TCP connection to the target IP address and port number and reports the time it takes for the connection setup. The target IP address can be a Cisco IOS IP SLA responder or any IP host. Disable the control protocol (using the **control disable** command) in the configuration, if the latter is used.

Referring to *Figure 9*, the IP SLA originating router at IP address 192.0.2.139 is configured to issue a TCP connect to each VMSS network module at the branch locations. Video Surveillance Operations Manager (VSOM) listens on TCP port 80 on these network modules. There are three probes configured, labeled as 92, 933, and 964, as shown below:

```
ip sla 92
 tcp-connect 192.0.2.2 80 source-ip 192.0.2.139 source-port 21877 control disable
 tos 160
 timeout 100
 tag VSOM_Site130
```

```
ip sla schedule 92 life forever start-time now

ip sla 933
 tcp-connect 192.0.2.34 80 source-ip 192.0.2.139 source-port 11091 control disable
 tos 160
 timeout 100
 tag VSOM_Site150
 frequency 300
ip sla schedule 933 life forever start-time now

ip sla 964
 tcp-connect 192.0.2.65 80 source-ip 192.0.2.139 source-port 22574 control disable
 tos 160
 timeout 200
 owner jimroy
 tag VSOM_Site140
ip sla schedule 964 life forever start-time now
```

All three probes are scheduled to start immediately and run continuously. The default frequency is every 60 seconds, but the frequency can be specified in the configuration. A **frequency 300** value in seconds specifies the probe starts every 5 minutes. The timeout value is specified in milliseconds. As a best practice for IP video surveillance deployments setting the timeout value between 100 and 500 (1/10th to 1/2 second) is a reasonable value for TCP connections. If the target host does not respond to a TCP connection in 500ms, there is either a network outage or the server is slow or not responding. In either of these cases, a failure should be noted.

The Type of Service byte (ToS) is configured as decimal value 160. This value is the marking used for video surveillance traffic and is equivalent to IP Precedence value 5 or DSCP value of CS5. By setting this value, any QoS policy in the path will treat the probes with the same policy as a video feed being viewed through the web server on the branch VSOM server.

The *owner* and *tag* values are simply means of documenting and identifying the probes in the configuration.

Intended Use Case

This probe has considerable application for diagnosing network connectivity issues as well as identifying any Media Server or Operations Manager server outages. One other use for this probe is to assist in configuring the security policies on firewalls and access control lists. For example, if the network manager is configuring access lists to permit the security operations staff at a remote location to initiate a connection to a Operations Manager server behind the firewall, enabling a TCP connect operation on the branch router supporting the remote location is a means of testing the access lists.

Additionally, the statistics for this probe include the latest round trip time (RTT). The RTT includes both network latency and processing delay of the target host responding to the TCP connect request.This probe, therefore, provides an indication of network and server latency, packet loss in the network or server outages, as well as verification of any security policies implemented on the network.

The statistics for the three TCP connect probes configured previously are shown as follows:

```
vpn-jk3-2651xm-9#show ip sla statistics 92

Round Trip Time (RTT) for       Index 92
        Latest RTT: 4 milliseconds
Latest operation start time: 10:49:23.788 est Thu Dec 10 2009
Latest operation return code: OK
Number of successes: 28
Number of failures: 0
Operation time to live: Forever
```

```
vpn-jk3-2651xm-9#show ip sla statistics 933

Round Trip Time (RTT) for       Index 933
        Latest RTT: 4 milliseconds
Latest operation start time: 10:47:14.815 est Thu Dec 10 2009
Latest operation return code: OK
Number of successes: 5
Number of failures: 0
Operation time to live: Forever


vpn-jk3-2651xm-9#show ip sla statistics 964

Round Trip Time (RTT) for       Index 964
        Latest RTT: 4 milliseconds
Latest operation start time: 10:50:44.883 est Thu Dec 10 2009
Latest operation return code: OK
Number of successes: 23
Number of failures: 0
Operation time to live: Forever
```

These probes are reporting very low latency (4 ms) because the branches in the topology are connected through a low-latency MetroEthernet services.

HTTP Operation

The HTTP operation measures the round-trip time (RTT) between the Cisco IOS IP SLA originator and an HTTP server to retrieve a web page. The HTTP server response time measurements (RTT) consist of three types:

- DNS lookup—RTT taken to perform domain name lookup.
- TCP connect—RTT taken to perform a TCP connection to the HTTP server.
- HTTP transaction time—RTT taken to send a request and get a response from the HTTP server. The operation retrieves only the home HTML page.

The DNS lookup step is optional. If an IP address is used in the URL and the **no ip domain lookup** command is configured on the originating router. If the viewing stations specify a domain name in the URL for connecting to VSOM, using the DNS lookup step is recommended. DNS-related issues can contribute to perceived network latency issues.

The TCP connect operation is next and connects to port 80 of the target HTTP server. In the previous section, a TCP connect operation was configured to connect to TCP port 80. From a practical standpoint, if the target port number is 80, then the HTTP operation should be configured rather than a TCP connect, as the HTTP operation provides more data points. The TCP connect operation can be configured to connect to ports other than 80, and the target can be a IP SLA responder or an IP host. The control messages can be enabled or disabled with TCP connect. With an HTTP operation, there is no control message support.

Finally, the HTTP request is issued to retrieve the home HTML page from the server. The RTT to retrieve the home page is measured and also a measurement of the time to receive the first byte. This measures the time from the start of the TCP connect operation to the first HTML byte retrieved by the HTTP operation. The total HTTP RTT is a sum of the DNS RTT (optional), the TCP connect RTT, and the HTTP RTT.

Referring to *Figure 9*, the IP SLA originating router at IP address 192.0.2.139 is configured to issue an HTTP GET to the router at 192.0.2.1, the VSOM web server at 192.0.2.2, and a third connection to a Media Server in the command center at 192.0.2.137. This configuration is shown below.

```
ip sla 2100
 http get http://192.0.2.2
 tos 160
 timeout 200
 tag VSOM_Site130_HTTP
 frequency 300
ip sla schedule 2100 life forever start-time now

ip sla 2101
 http get http://192.0.2.1
 tos 160
 timeout 200
 tag Router_Site130_HTTP
 frequency 300
ip sla schedule 2101 life 86400 start-time now

ip sla 2137
 http get http://192.0.2.137
 tos 160
 timeout 200
 tag Media_Server_command_center
 frequency 300
ip sla schedule 2137 life forever start-time now
```

In each of the three configured probes, the IP address, rather than the host name are specified in the URL. The frequency of the probes are configured for 300 seconds, or 5 minutes. As shown in the previous sections, the ToS byte is configured for DSCP value CS5. The timeout values are set at 200 milliseconds.

Tip Because the total RTT includes three components, DNS, TCP and HTTP, the timeout values may need to be increased from values used by probes which are simply measuring the network RTT. See the "HTTP Connect Connections over Internet WANs" section on page 64 for additional examples.

Intended Use Case

This probe has considerable application for diagnosing network connectivity issues, identifying network latency, and server outages or slow performance of DNS and Web servers. Because the Media Servers and VSOM both support their application interfaces by way of Web servers, these probes are useful for identifying the availability and response time of both the network and applications.

Example output for HTTP GET of VSOM at the branch location:

```
vpn-jk3-2651xm-9#show ip sla statistics 2100 details

Round Trip Time (RTT) for       Index 2100
        Latest RTT: 75 milliseconds
Latest operation start time: 10:50:04.411 est Thu Dec 10 2009
Latest operation return code: OK
Over thresholds occurred: FALSE
Latest DNS RTT: 0 ms
Latest TCP Connection RTT: 7 ms
Latest HTTP time to first byte: 74 ms
Latest HTTP Transaction RTT: 68 ms
Latest HTTP Status: 302
Latest HTTP Message Size: 216
Latest HTTP Entity-Body size: 0
Number of successes: 5
```

```
Number of failures: 0
Operation time to live: Forever
Operational state of entry: Active
Last time this entry was reset: Never
```

Example output for HTTP GET of Cisco 2851 router at the same branch location:

```
vpn-jk3-2651xm-9#show ip sla statistics 2101 details

Round Trip Time (RTT) for       Index 2101
        Latest RTT: 21 milliseconds
Latest operation start time: 10:51:17.640 est Thu Dec 10 2009
Latest operation return code: OK
Over thresholds occurred: FALSE
Latest DNS RTT: 0 ms
Latest TCP Connection RTT: 8 ms
Latest HTTP time to first byte: 20 ms
Latest HTTP Transaction RTT: 13 ms
Latest HTTP Status: 401
Latest HTTP Message Size: 173
Latest HTTP Entity-Body size: 18
Number of successes: 5
Number of failures: 0
Operation time to live: 85083 sec
Operational state of entry: Active
Last time this entry was reset: Never
```

Example of HTTP GET from HP ProLiant DL380 (3.0GHz Dual-Core Intel Xeon 5160 Processor) running SuSe Enterprise 10 SP1+ and Cisco Video Surveillance Manager 4.2/6.2:

```
vpn-jk3-2651xm-9#show ip sla statistics 2137 details

Round Trip Time (RTT) for       Index 2137
        Latest RTT: 68 milliseconds
Latest operation start time: 11:13:41.834 est Wed Dec 23 2009
Latest operation return code: OK
Over thresholds occurred: FALSE
Latest DNS RTT: 0 ms
Latest TCP Connection RTT: 11 ms
Latest HTTP time to first byte: 67 ms
Latest HTTP Transaction RTT: 57 ms
Latest HTTP Status: 200
Latest HTTP Message Size: 1483
Latest HTTP Entity-Body size: 1181
Number of successes: 9
Number of failures: 0
Operation time to live: Forever
Operational state of entry: Active
Last time this entry was reset: Never
```

These three use cases all illustrate LAN/MAN attached response times. For sample output of these problems an a Internet WAN environment, see the "HTTP Connect Connections over Internet WANs" section on page 64.

UDP Jitter Operation

The IP SLAs UDP jitter operation was primarily designed to diagnose network suitability for real-time traffic applications such as voice and video over IP. One key element of the UDP jitter operation is its ability to report on jitter encountered by IP packets in the network. The UDP jitter operation is a very

useful measuring tool in that it also reports latency and jitter in each direction and packet loss. It also calculates a Mean Opinion Score (MOS), a subjective measure of audio fidelity for VoIP. The scores range from 1 (poor) to 5 (perfect). In most networkers, with sufficient bandwidth for the video feeds, MOS scores reported above 4.0 are a good general indication the network is capable of transporting IP video surveillance.

UDP jitter operation requires IP SLAs Responder be enabled on the target device. Typically, a standalone IP SLA originating router is configured to initiate UDP jitter probes with the remote router acting as the responder. UDP jitter operation does not support the IP SLAs History feature due to the large amount of data collected with each initiation. Time synchronization (via NTP) is required between the source and the target device in order to provide one-way delay (latency) measurements. If the time is not synchronized the one-way delay measurements are reported as '0' values.

The UDP jitter operation is a comprehensive tool for determining network suitability of video transport. If the network manager only has resources to become familiar and implement one type of probe for network assessment and on going troubleshooting, this is the probe to use.

Referring to Figure 9, the IP SLA originating router at IP address 192.0.2.139 is configured to issue a UDP jitter probe to the remote branch router at 192.0.2.64.

```
ip sla 864
 udp-jitter 192.0.2.64 16394 codec g711alaw codec-numpackets 30 codec-interval 33
codec-size 1300
 tos 160
 timeout 100
 threshold 200
 tag Router_Site140_udp-jitter
 frequency 300
ip sla schedule 864 start now lifetime 86400
```

In the configuration, the values for codec-size and interval are modified from the default values. A interval of 33 milliseconds equates to 30 packets per second. Video frame rates are commonly configured for 30 frames per second. In most instances, more than one IP packet is required to transport a video frame however. The codec size parameter is set at 1300 bytes, which is similar to the average payload size of MPEG4 / H.264 or MJPEG encoded video. The number of packets is set to 30, and given the interval of 33ms, this probe runs for one second, every 5 minutes (frequency 300 seconds).

By changing the default values, the probe is more representative of a video feed than the VoIP call it is initially modeled after.

Intended Use Case

This probe can identify network connectivity issues and both one-way and round trip latency. The latency, jitter and loss are reported in both directions, source to destination and destination to source. the source the originating Cisco device. Sample command output is as follows:

```
vpn-jk3-2651xm-9#show ip sla statistics 864

Round Trip Time (RTT) for       Index 864
        Latest RTT: 4 milliseconds
Latest operation start time: 10:49:56.218 est Thu Dec 10 2009
Latest operation return code: OK
RTT Values:
        Number Of RTT: 30               RTT Min/Avg/Max: 3/4/5 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 30
        Source to Destination Latency one way Min/Avg/Max: 3/3/4 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 1/1/2 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 29
        Number of DS Jitter Samples: 29
```

```
        Source to Destination Jitter Min/Avg/Max: 0/1/1 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/1/2 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0           Loss Destination to Source: 0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 1
MOS score: 4.34
Number of successes: 6
Number of failures: 0
Operation time to live: Forever
```

In the output, the number of jitter probes is always one less than the number of latency probes (samples). This is expected and intentional, jitter is based on the proceeding packet. The first packet has now proceeding packet to reference jitter.

This probe can report packet loss, but the accuracy of reporting packet loss is based on the number of samples. Given that packet loss is customarily measured in packets per million, it is unlikely that a sample size of 30 packets, as in this example, will provide a useful gauge of packet loss.

As mentioned previously, jitter is often a function of the network latency. The higher the latency the more likely jitter is also high. However, to some extent, the impact of jitter is also a function of the inter-packet interval. Jitter of 2ms when the interval is expected to be 20ms (VoIP is typically 50 pps) as opposed to jitter of 2m when the interval is expected to be 33ms. Also, recall that VoIP is always encapsulated in a single IP packet. Video may require several hundred IP packets for an MPEG4/H.264 I-frame using High Definition resolutions. Jitter therefore is more relevant to VoIP deployments than to Video deployments.

The MOS score value is a useful value to determine overall network performance. MOS scores below 4.0 should warrant additional scrutiny.

WAN Internet Broadband Example

As a point of reference, the configuration and output from the business class cable deployment described in the "HTTP Connect Connections over Internet WANs" section on page 64 is included for reference. This access circuit is 15M/2M and the WAN transport is encrypted DMVPN over the Internet. The configuration of the IP SLA originating router located at the DMVPN aggregation head-end routers is as follows:

```
ip sla 1864
 udp-jitter 10.81.7.25 16394 codec g711alaw codec-numpackets 30 codec-interval 33
codec-size 1300
 tos 160
 tag business_class_cable_broadband
 frequency 300
ip sla sched 1864 start now life 86400
```

The sample statistics are as follows:

```
rtp-esevpn-saa_MC#show ip sla statistics 1864

Round Trip Time (RTT) for       Index 1864
        Latest RTT: 23 milliseconds
Latest operation start time: 11:50:12.529 est Wed Dec 23 2009
Latest operation return code: OK
RTT Values:
        Number Of RTT: 30               RTT Min/Avg/Max: 18/23/38 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 30
```

```
        Source to Destination Latency one way Min/Avg/Max: 16/20/36 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 1/3/12 milliseconds
Jitter Time:
        Number of Jitter Samples: 29
        Source to Destination Jitter Min/Avg/Max: 1/3/14 milliseconds
        Destination to Source Jitter Min/Avg/Max: 1/3/10 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0           Loss Destination to Source: 0
        Out Of Sequence: 0      Tail Drop: 0    Packet Late Arrival: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 1
MOS score: 4.34
Number of successes: 3
Number of failures: 0
Operation time to live: 85701 sec
```

In this example, the RTT is 23 ms with jitter averaging 3ms.

Summary

This section demonstrates how to use and configure four types of Cisco IOS IP Service Level Agreements (SLAs) problems: ICMP Echo, TCP Connect, HTTP, and UDP jitter. While all four probes have application to a video surveillance deployment, the UDP jitter operation provides the most useful data points to determine if the network topology is suitable for deploying video.

While the probes themselves should be marked with the same QoS DSCP values of the traffic they are intended to emulate, the probe output cannot directly determine if three is sufficient bandwidth capacity in the network. Other capacity planning tools and the **show** commands described in both the switch and router assessment sections must also be used to verify that sufficient bandwidth is available to implement IP video surveillance.

References

- Cisco IOS IP Service Level Agreements (SLAs)

  http://www.cisco.com/en/US/products/ps6602/products_ios_protocol_group_home.html

Security and Application Optimization Assessment

When evaluating an existing network for supporting IP video surveillance, the assessment must take into consideration any existing network security polices and devices. Policy-based security implementations are most common and they protect resources by restricting the forwarding of traffic to a specific destination based on some rule or administrative policy. Firewalls and access control lists are examples.

If no access control lists, firewalls, packet shapers or packet optimization devices (such as Cisco Wide Area Application Services (WAAS)) exist in the existing or proposed network, the assessment simply should note this fact in the assessment. Because access-control lists are often implemented on routers and Layer-3 switches, the configuration files of these devices must be examined for the related access-control list configuration commands. Firewall functionality can also be implemented in software on a router, or as an appliance.

Access Control Lists (ACL)

Access control lists are lists of permissions (or explicit denies) which govern if packets are allowed to be forwarded to the intended destination. These lists can be written very generally, to permit an entire network to communicate with another network, or very specific, specifying both source and destination address, protocol and port number.

In the *Cisco IP Video Surveillace Design Guide*, section *Required TCP/UDP Ports* (page 4-11) specifies what ports and protocols are used to communicate between the various components of the Cisco Video Surveillance Manager (VSM). Also in that document, the section *Controlling Access to IP Video Surveillance* (page 6-80) provides a high-level overview of how to control access using policy-based access-control.

When deploying IP video surveillance on an existing network, any access control lists must be noted in the network assessment and indicated on the topology diagram. Updates to the access control lists may be required for the components of the video surveillance system.

Firewalls

Firewalls can be implemented as a software configuration to a Cisco IOS router, or can be a standalone devices. The software implementation is introduced *Cisco IOS Firewall Context-Based Access Control (CBAC): Introduction and Configuration* at the following URL: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080094e8b.shtml. This document shows how to implement an inspection policy and ACL policy combined to define firewall policy.

Zone-Based Policy Firewall (ZFW) introduced in Cisco IOS Software Release 12.4(6)T introduced a new configuration model for the Cisco IOS Firewall feature set. Policies are applied to traffic moving between zones, not interfaces. The Cisco IOS configuration model is more aligned with the PIX or ASA firewall configuration commands. *The Cisco IOS Firewall Zone-Based Policy Firewall Design and Application Guide* is a good reference document and can be found at the following URL: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml

NAT/pNAT

Network Address Translation/Port Address Translation (NAT/pNAT) is often implemented in conjunction with a firewall configuration, but can also be implemented on a Cisco IOS router. The location of any NAT/pNAT functionality must be noted on the network topology diagram. Typically, if the NAT/pNAT devices is implemented to allow viewing stations access to the Internet, there is no implication to the IP video surveillance deployment. However, additional analysis and configuration may be needed if NAT/pNAT is implemented between components of the IP video surveillance deployment. Note any NAT/pNAT in the network topology diagram.

Segmentation

Network segmentation is commonly implemented with VRF-Lite, VLANs and some firewall in the topology to allow the segmented networks to communicate. The *Cisco IP Video Surveillace Design Guide* includes a detailed chapter on *Virtualization, Isolation and Encryption of IP Video Surveillance* on page 6-87. If deploying the video surveillance solution on an existing network with end-to-end segmentation implemented, note this in the network assessment and further analysis is required.

Application Optimization

Many organizations implement application optimization appliances to accelerate network performance, especially in the WAN. The Cisco WAN optimization product Wide Area Applicatio*n Services (WAAS) was deployed and tested in the Cisco IP Video Surveillace Design Guide in section Wide Area Application Services (WAAS) Integration* on page 6-61.

In general, WAAS is not as optimal in optimizing video surveillance feeds as it is with data applications. In many deployments, real-time traffic like VoIP and video is not designated for optimization by the network administrator. Any WAN or application optimization appliance in the network should be noted in the network assessment for further analysis.

Packet Shapers

Packet shapers are Layer-7 application shaping. They may be implemented as an appliance and not part of the Qos policy implemented on a router or switch. These application shapers identify traffic on the network and allow the network administrator to define a policy to control the flow (transmission) rate for each particular type of traffic. Applications like YouTube or MySpace are often candidates for rate limiting. Any packet shaping appliances should be noted in the network assessment, as packet shaping video surveillance traffic may contribute to video quality issues.

Recommended Reading

There are many on-line resources available which describe in detail all aspects of security and application optimization. Some titles include:

- *Firewall Fundamentals* by Wes Noonan, Ido Dubrawsky
- *Deploying Cisco Wide Area Application Services*, 2nd Edition by Zach Seils, Joel Christner, Nancy Jin.
- *Cisco ASA: All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance*, 2nd Edition by Jazib Frahim, Omar Santos.

Quality-of-Service (QoS) Assessment

An important aspect of the IP video surveillance network assessment is to determine what, if any, QoS features have been implemented on the network. QoS is disabled by default on most routers and switches or some general QoS configuration is implemented by default. An example of this is the Cisco Catalyst C3750 family of switches. While QOS is disabled, resources are configured using values that are not modifiable by the end user and all traffic is treated as if it were classified the same. If the network deployment is solely to support IP video surveillance, no VoIP or application data exists outside the applications which make up the video surveillance solution, then leaving QoS disabled may be a practical option if no other QoS features are needed.

It is a common mis-conception that enabling QoS will improve throughput. If QoS is enabled by a global **mls qos** configuration command, but with no additional configuration, applications may experience worse throughput rather than better.

Medianet Switches

The Cisco Catalyst 2975, 3560G, 3750G, 3560-E, and 3750-E family of switches are access-layer switches that can be used for IP Video Surveillance deployments. These are considered medianet switches, meaning that they include GigabitEthernet interfaces and implement in hardware a strict priority queue with at least three additional queues.

The network assessment process must determine the following points in regards to QoS for the existing or proposed network topology:

- Is IP video surveillance the only network traffic on the network or is the network a converged network with other data or VoIP applications?
- As part of the network inventory assessment, are the existing or proposed network devices *medianet ready*, as defined in the initial paragraph of this section?
- Is QoS currently enabled end-to-end and in a consistent manner on all routers and switches in the exiting network?
- As part of the "Assessing Switching (LAN) Readiness" section on page 20 and "Assessing Routing Readiness" section on page 33, are output interface queue drops being encountered in the existing network topology.

By assessing the network and answering these questions, an action plan can be developed to replace any network hardware that is not *medianet ready*. It also allows a determination to be made as to the need for enabling QoS in the existing or proposed network. Even if the network is not a converged network, the best practice is to deploy switches that are *medianet ready* to take advantage of the GigabitEthernet interface support in the topology. QoS can then be implemented at a later time if additional applications are added to the network.

If QoS is currently enabled on some devices, but not all, or implemented inconsistently, or there are interfaces which are experiencing congestion, the network assessment must include this as an action item to ensure a successful video surveillance deployment. There are several documents that can be referenced to better understand the concepts and configuration of QoS in both the LAN and WAN to support IP video surveillance. They are listed below.

References

- Video in Campus

  http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns815/landing_cVideo.html

- Medianet Campus QoS Design 4.0

  http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html

- The *Cisco IP Video Surveillance Design Guide* includes a chapter on *Configuring Quality-of-Service (QoS) for IP Video Surveillance* beginning page 6-21

Network Assessment Checklist

This section is a network assessment checklist that can be used to develop the overall assessment document. Each table (see Table 6 to Table 10) references a section in this document and the category relates to topics discussed in their respective session. The descriptions are a series of questions that should be answered to better understand the action items needed to successfully implement IP video surveillance in a new or existing network.

As part of the overall project plan, these items should be reviewed with the project stakeholders, which include the physical security manager, network manager and administrators, and any systems or support personnel.

Table 6 General Network Requirements

Category	Description
Project Management	Has a project manager been identified? Are the roles and responsibilities of the team members been clearly defined? Are sufficient resources allocated to complete the project within the expected timeframe?
Education and Training	What training is required for the users operating the video surveillance system? What network related training is required of the persons installing the cameras and servers? Has time and budget been allocated for training?
Documentation	Does network topology documentation currently exist? As part of the specific network assessments, the LAN and WAN topology must be verified and the document updated as required.
Network Services	IP Video Surveillance systems require NTP, Syslog, FTP/TFTP, and Network Management servers. Do these systems exist in the network currently?
Network Management	Does the enterprise currently have any network management resources? Has the network administrator been involved of the planning process and understand the requirements of the physical security department
Network Characteristics of IP Video Surveillance	The Service Level Assessment section demonstrates how to measure the network for latency, jitter and loss. Review the section on Video Surveillance Application Requirements to understand the thresholds needed by IP video surveillance.
Design Review / Device Placement	Does the overall network design, including the placement of IP cameras, servers and viewing workstations align with network design best practices? Has the existing network capacity been evaluated?
Customer Remediation Agreements	The assessment should indicate any area that the customer is unwilling or unable to remediate prior to deployment. Ideally, obtain written agreement from the customer that they understand that by not remediating where needed can adversely impact the functionality and performance of the IP Video Surveillance deployment?

Table 7 Design Considerations

Category	Description
LAN switching requirements	Has the deployment been evaluated for how many cameras are required at each physical location? Is there a physical map available of the proposed locations? Are the distances indicated? Does the cabling exist or need be run? Are the cameras powered by the switch (PoE) or from building power?
Switching Hierarchy	Based on the size of deployment and physical distances, how many layers of switching hierarchy are required? Where are the servers going to be located in the hierarchy?
Device Placement	Has a logical topology overview of the devices in the deployment been produced? Are the cameras standard or high definition? Have the frame rates and bit rates been included in the logical overview to estimate uplink capacity? How many media servers and the number of cameras per Media Server been considered? Have estimates of disk storage been produced for each Media Server? Will the Operations Manager (VSOM) be implemented on a dedicated server or co-located with the Media Server?
Viewing Stations	Will viewing station hardware (including graphics cards) need be ordered?
Backups and Attached Storage	Will a backup Media Server be deployed or is the storage attached externally through Fibre Channel? If external, have the devices been appropriately sized for the storage requirements of the deployment?
WAN Design	Is the WAN topology appropriate in order to carry all the intended IP Video Surveillance traffic? Has the customer ordered an appropriate amount of bandwidth from their Service Provider?
High Availability	Does the LAN and WAN design provide for sufficient redundancy to provide for high availability?
IP Addressing	Have the appropriate IP Addresses been assigned for the IP Video Surveillance components?

Table 8 Switching (LAN) Assessment

Category	Description
Inventory	Assess the model and software versions of existing switches. Verify if they are medianet ready. Upgrade hardware and software as required.
Memory and CPU Utilization	Verify current memory and CPU characteristics as part of the switch inventory assessment
Ports / Interfaces	Verify sufficient ports of the correct speed are available on existing switches. Are all the network interfaces set at an adequate speed for their function and expected load within the topology?
VLANs	Inventory the VLAN assignments on existing switches and incorporate into overall plan for VLAN to IP network mapping

Category	Description
Power over Ethernet	Determine how IP cameras will be powered. Verify sufficient PoE capability exists on existing switches.
Physical Connectivity	Document what devices are attached to which ports. Update *description* in interface configuration as required.
Layer-2 Topology	Have you validated that the Layer 2 path(s) through the LAN matches the expected path in the network design?
Environmental Statistics	Verify power and cooling requirements of existing switches to identify any airflow or power issues. For switches which have redundant power supplies, verify they are attached to different circuit breaker panels or optimally one on street power, one on UPS power
Local Link Issues	Verify no interface errors on existing network, both individual interfaces and uplinks. Post implementation and pre-production, verify all links are running clean.
Overall Capacity Assessment	Determine if any existing capacity issues exist and during the implementation phase, again verify prior to production implementation. Capacity should be examined on a link-by-link and interface-by-interface basis. Note any capacity issues as part of the assessment and how they will be addressed.
Network Management Services	Verify switches (as well as servers and IP cameras) have the appropriate SNMP trap server configuration, NTP and syslog server configuration.
Clearing of Interface Counters	Develop a plan to clear and inspect interface counters weekly

Table 9 Routing Assessment

Category	Description
Inventory	Collect model and software version of all routers in the network. Create physical and logical topology diagram of existing routers and switches in the network. Upgrade software and hardware as required.
CPU and Memory Utilization	Determine existing resource utilization and address any deficiencies
Environmental Statistics	Verify power and cooling requirements of existing switches to identify any airflow or power issues. For switches which have redundant power supplies, verify they are attached to different circuit breaker panels or optimally one on street power, one on UPS power
Buffer Tuning	Configure routers to automatically tune buffers.
Network Management Services	Verify switches (as well as servers and IP cameras) have the appropriate SNMP trap server configuration, NTP and syslog server configuration.

Category	Description
Interface Counters and Statistics	Identify on the network topology diagram the adjacent router or switch for each interface. Update the IP address and VLAN inventory to show all addresses and VLANs in use. Identify any interface utilization issues, output drops or errors on all interfaces. Identify what Qos policies are enabled on router interfaces and verify if consistent with switch configurations and overall network policies.
Switching Path Analysis	Verify the switching path is appropriately configured. Best practice is CEF and NetFlow switching for IP.
Redundant Links	Identify and document redundancy in network. As part of the Service Level Assessment, characterize latency and loss for redundant links. Address any anomalies. Consider implementing a primary and backup path rather than equal cost load sharing.
Routed Protocol Analysis	Identify any routed protocols in use on the network other than IP
Routing Protocol Analysis	Identify and review what routing protocol(s) are in use. As a best practice, EIGRP and OSPF are optimal for internal routing and BGP or statics for Internet and external gateway routing.
Bridged Protocol Analysis	Identify if any bridges protocols are in use. Optimally these should be eliminated or minimized.
Clearing of Interface Counters	Develop a plan to clear and inspect interface counters weekly

Table 10 Specific Network Requirements

Category	Description
Service Level Assessment	Configure Cisco IOS IP SLAs to determine loss, latency and jitter for the various paths in the network between IP cameras, servers and viewing stations. Determine if the existing network meets or exceeds the specified requirements.
Access control lists	Verify if any access control lists are present in the existing network which may cause connectivity failures between the video surveillance components
Connectivity	Has the routing (and connectivity) between the IP Video Surveillance component(s) been validated?
Firewalls	Locate any existing firewalls and identify on the network topology diagram. Review the configuration with the security administrator to ensure the ports and protocols needed by IP video surveillance are authorized. Are network security boundaries appropriate as it relates to the IP Video Surveillance component devices?
NAT/pNAT	Determine if any NAT/pNAT is present in the network and indicate on the network topology diagram
Segmentation	Review any segmentation requirements for the video surveillance system and update network topology diagram accordingly.
Application Optimization and Packet Shapers	Note any application optimization appliances in the existing network.

Category	Description
Quality-of-Service (QoS)	As part of the network topology and inventory assessment determine what, if any, QoS is enabled on the existing network. Determine if QoS policies need to be updated to support the IP video surveillance needs or implemented according to the documentation links referenced in this document. Has QoS been enabled on the routers and switches in the topology? Is IPVS traffic being marked appropriately by either the end device or on ingress to the network?
Service Provider QoS	If a Service Provider is transporting IPVS traffic between locations, is the QoS marking properly retained and applied when traversing the Service Provider portion of the network?
Service Provider Provisioning	Has it been validated that the Service Provider has configured the site circuits as per the customers' order as it relates to QoS and Bandwidth?
Network Infrastructure Software Readiness	Is there a defined standard for the versions of IOS/CatOS that they have implemented on the network devices? Are there any known issues with any of the IOS/CatOS versions currently implemented?

Appendix

show control-plane host open-ports

The **show control-plane host open-ports** command can be used to identify what ports the router is listening. UDP Port 1967 is used for Cisco IOS IP SLA control protocol.

```
vpn1-3845-1#show control-plane host open-ports
Active internet connections (servers and established)
Prot        Local Address      Foreign Address                  Service    State
 tcp                *:22                *:0               SSH-Server   LISTEN
 tcp                *:23                *:0                   Telnet   LISTEN
 udp              *:64723               *:0                  IP SNMP   LISTEN
 udp                *:321               *:0         IOS host service   LISTEN
 udp                *:67                *:0            DHCPD Receive   LISTEN
 udp                *:68                *:0             BootP client   LISTEN
 udp                *:123               *:0                      NTP   LISTEN
 udp                *:161               *:0                  IP SNMP   LISTEN
 udp                *:161               *:0                  IP SNMP   LISTEN
 udp                *:162               *:0                  IP SNMP   LISTEN
 udp                *:162               *:0                  IP SNMP   LISTEN
 udp               *:1967               *:0              RTR control   LISTEN
 udp              *:51262               *:0                IP SNMPV6   LISTEN
```

HTTP Connect Connections over Internet WANs

As a point of reference, two tests are shown below using Cisco IOS IP SLA probes (HTTP GET and ICMP-ECHO) between a campus headend IP SLA originator and the remote locations. The remote routers are Cisco 881w routers connected to the campus over DMVPN encrypted tunnels using broadband Internet connectivity.

Residential DSL Broadband

In this example, the he target IP address is a Windows XP PC running Apache/2.2.8 (Win32) web server. the broadband connections is residential aDSL trained at 1.4M/256K (downlink/uplink). With this connection, it is possible to view a single standard definition camera (4CIF) at CBR rates in the 768K/1Mbps range.

The IP SLA originating router is at the campus data center co-located with the DMVPN head-end aggregation routers. There two probes are configured as follows:

```
ip name-server xx.xxx.6.247
!
ip sla responder
ip sla 2101
 http get http://rtp-esevpn-76.cisco.com
 tos 160
 timeout 1000
 tag PC_HTTP
ip sla schedule 2101 life 86400 start-time now
!
ip sla 2102
 icmp-echo 10.81.7.76
 timeout 1000
 tag PC_ICMP
```

```
ip sla schedule 2102 life 86400 start-time now
!
end
```

The URL of http://rtp-esevpn-76.cisco.com resolves to IP address 10.81.7.76, the IP address of the remote Windows XP PC and Apache Web server. The RTT of this WAN connection is approximately 100ms, as shown:

```
rtp-esevpn-saa_MC#show ip sla stat 2102

Round Trip Time (RTT) for       Index 2102
        Latest RTT: 104 milliseconds
Latest operation start time: 15:20:09.123 est Tue Dec 22 2009
Latest operation return code: OK
Number of successes: 1
Number of failures: 0
Operation time to live: 86391 sec
```

The total RTT for the HTTP GET operation is 942 milliseconds. Note in the following output that the TCP connection RTT is 98ms, which is consistent with the ICMP RTT. The HTTP and DNS portion of the total RTT contributed to the majority of the 942ms RTT. The HTTP transaction RTT is 759ms.

```
rtp-esevpn-saa_MC#show ip sla stat 2101 details

Round Trip Time (RTT) for       Index 2101
        Latest RTT: 942 milliseconds
Latest operation start time: 15:21:47.689 est Tue Dec 22 2009
Latest operation return code: OK
Over thresholds occurred: FALSE
Latest DNS RTT: 85 ms
Latest TCP Connection RTT: 98 ms
Latest HTTP time to first byte: 726 ms
Latest HTTP Transaction RTT: 759 ms
Latest HTTP Status: 200
Latest HTTP Message Size: 1752
Latest HTTP Entity-Body size: 1429
Number of successes: 11
Number of failures: 0
Operation time to live: 85783 sec
Operational state of entry: Active
Last time this entry was reset: Never
```

Tip Configuring a HTTP GET operation in conjunction with an ICMP-ECHO request can aid in determining if performance issues are network related or server related.

Business Class Cable Broadband

This example is a business class cable broadband connection. It is provisioned at 15M/2M and the WAN transport is also a DMVPN-encrypted tunnel on the same head-end aggregation routers and IP SLA originating router as the previous example. The remote router is also a Cisco 881W. This network topology was used in developing the *Implementing TelePresence over Broadband* at the following URL: http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/TNS_x_BB_whitepaper.html

The target IP address is a Cisco Unified IP Phone CP-7970G. The Cisco IP phones support a web server and therefore can be used as a target for the HTTP Get and ICMP echo operations. The probes are similarly configured to the previous example.

```
ip sla 2501
 http get http://rtp-esevpn-28.cisco.com
 tos 160
 timeout 1000
 tag PC_HTTP
ip sla schedule 2501 life 86400 start-time now
!
ip sla 2502
 icmp-echo rtp-esevpn-28.cisco.com
 timeout 1000
 tag PC_ICMP
ip sla schedule 2502 life 86400 start-time now
!
```

The RTT of the ICMP-ECHO for this connection is substantially lower than in the previous example. The reported RTT is 16 milliseconds.

```
rtp-esevpn-saa_MC#show ip sla statistics 2502

Round Trip Time (RTT) for       Index 2502
        Latest RTT: 16 milliseconds
Latest operation start time: 16:57:47.179 est Tue Dec 22 2009
Latest operation return code: OK
Number of successes: 1
Number of failures: 0
Operation time to live: 86343 sec
```

There are two primary reasons the RTT of this probe is much lower than the previous example. The clock rate of the access circuit is considerably faster than the previous example. We are comparing an access circuit of aDSL at 1.4M/256K to a Cable link at 15M/2M. There is less serialization delay with the faster clock rate of the access circuit. Also to some extent, the number of Internet routers between the remote cable router and the DMVPN head-end is less than with the aDSL link.

The total RTT for the HTTP GET operation is 907 milliseconds. Note in the following output that the TCP connection RTT is 26ms, which is consistent with the ICMP RTT. The DNS RTT is similar to the value from the previous example. The DNS query from the IP SLA originator does not traverse the WAN, it is internal to the corporate network. The HTTP transaction time of 793 ms is higher than the previous example of 759 ms. This difference can be contributed to the main CPU performance of the IP phone versus a 2.20Ghz PC.

The items of note are highlighted in the following output:

```
rtp-esevpn-saa_MC#show ip sla statistics 2501 details

Round Trip Time (RTT) for       Index 2501
        Latest RTT: 907 milliseconds
Latest operation start time: 16:57:46.734 est Tue Dec 22 2009
Latest operation return code: OK
Over thresholds occurred: FALSE
Latest DNS RTT: 88 ms
Latest TCP Connection RTT: 26 ms
Latest HTTP time to first byte: 771 ms
Latest HTTP Transaction RTT: 793 ms
Latest HTTP Status: 200
Latest HTTP Message Size: 4907
Latest HTTP Entity-Body size: 4682
Number of successes: 1
Number of failures: 0
Operation time to live: 86367 sec
Operational state of entry: Active
```

```
Last time this entry was reset: Never
```

The key point of this illustration is that total application response time is a function of the network bandwidth and latency, but also of the server and applications being accessed by the end-user. By using probes that can measure network latency and compare that to the total latency of the application, a better root cause analysis can be conducted.

Why Packet Loss Impacts IP Video Surveillance

Success in deploying IP Video Surveillance on an existing network is dependent on the network's ability to transport the IP encapsulated video feeds between camera and the Network Digital Video Recorder (NDVR) without loss. Packet loss in campus and high-speed WAN backbones is measured in drops per million packets and typically is less than 1/10th of 1 percent. When drops occur, they are usually grouped together as opposed to be randomly distributed throughout the day.

Packet loss can be attributed to such factors as over subscription of a network interface, drops due to temporary buffer exhaustion, hardware failures or misconfiguration. One common example of a mis-configuration error is a duplex mismatch between two Fast Ethernet ports. This error occurs when either the network administrator, or the auto-negotiation between switch port and the IP camera, results in one side being configured as full and the other half duplex.

Transport methods

There are two primary transport methods for IP video surveillance. Transmission Control Protocol (TCP) and User Datagram Protocol/Real-time Transport Protocol (UDP/RTP). Between a camera and the NDVR, usually Motion JPEG (MJPEG) video is transported in TCP while MPEG-4 and H.264 are transported in UDP/RTP. Between the NDVR and a workstation viewing video feeds, the transport for both MJPEG and MPEG-4/H.264 may be TCP. The critical path is between the camera and the NDVR; if packets are lost here, the video image cannot be recovered. Once a high quality image is safely stored on disk, there is more tolerance for loss because we are viewing a recorded image.

Each MJPEG frame is complete into itself, packet loss will not degrade the video image, but movement will appear more choppy as the video frames per second is decreased from loss or lack of available bandwidth.

MPEG-4/H.264 is transported as a reference frame (I-frame) and incremental updates as P/B-frames. Lost packets are detected through the encoding of a sequence number in the RTP header, but are not re-transmitted. When packet loss occurs, the MPEG-4/H.264 image will be degraded until a complete I-frame is received successfully. This may take several seconds or longer and the artifacts are visible in the image.

Resolution is a Dominate Attribute

Video traffic on the network appears as a series of video frames transported in multiple IP packets.

The size of each video frame is variable and partially determined by how the video is encoded. The reference (I-frames) for MPEG-4/H.264 may require, at a minimum, ten or more IP packets for transport.

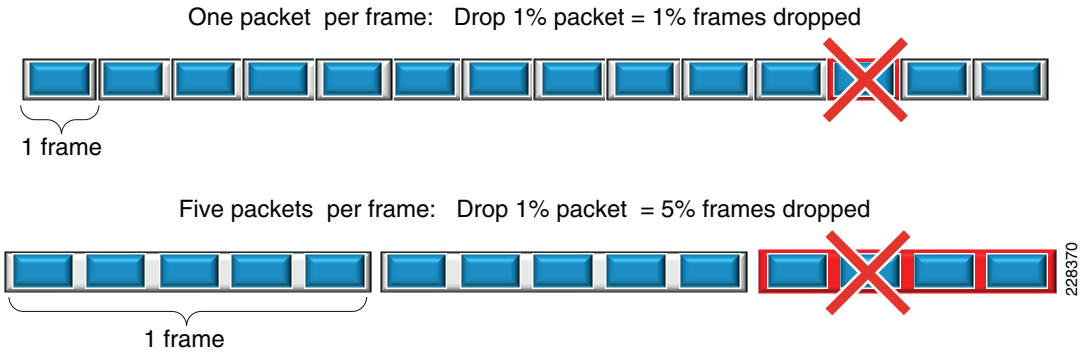
Video on the network, even when configured for a Constant Bit Rate (CBR), appears as a variable bit-rate stream with periodic bursts. As the video resolution increases, the number of IP packets required to transport the reference frame may increase dramatically.

Compare a standard definition camera at D1 resolution (720x480 NTSC 30fps) MPEG-4 using a CBR of 2Mbps versus a high definition camera at 1080P resolution (1920 x 1080p 30fps) H.264 using a CBR of 4Mbps. Both cameras have a similar average packet size; over 1,300 bytes per packet. The first reference frame for this SD camera is 16 packets while the HD camera generates 304 packets. The incremental frames from the SD camera range from 5 to 8 packets and the HD camera incremental frames are 2 IP packets. Because both cameras are generating 30 frames per second, the video frames are generated approximately every 33ms. These characteristics are from observed with WireShark (www.wireshark.com).

As Resolution Increases, the Drop Threshold Decreases

Higher resolution provides more useful video, but it has much more stringent requirements of the network. If the goal is to have less than 1% video frame drop rate at 5 packets per frame then your IP packet drop rate must be 1/5th that or less than 0.2 percent. Figure 10 illustrates this concept.

Figure 10 Factor of Dropped Frames



From the HD camera example, dropping one IP packet from the 304 packet HD reference frame invalidates the entire video frame, but it translates to a drop rate of only 3/10th of 1 percent of the packets.

Summary

Motion, picture complexity, encoder implementations, frame rates, and quality factors are video attributes that affect the load on the network. The camera resolution, however is the biggest factor in determining network load. As the resolution increases, the number of IP packets required to transport the reference frame also increases. Correspondingly, the IP packet drop rate must be monitored and controlled to insure good quality high definition video.

Troubleshooting Duplicate IP Addresses

This section illustrates how to determine if a duplicate IP address exists on the network. It also provides sample output from routers and switches to illustrate how to determine the MAC address associated with a switch port.

Methodology

One problem which occurs on IP networks are duplicate IP addresses. The symptoms of duplicate IP addresses include: connectivity is intermittent to the target host, some hosts can connect to the target host while other cannot.

To determine if a duplicate IP address is present on the network, complete the following tasks:

Step 1 Disconnect the Ethernet cable from the target host.

Step 2 Log on a router or workstation on the same LAN segment

Step 3 Clear the Address Resolution Protocol (ARP) table as follows:

*router#***clear arp**

c:\ arp -d *

Step 4 Ping the IP address of the target host from a router or workstation

Tip Because the ARP table is cleared, the first ping will usually timeout (fail). Issue a **ping** command with at least 5 iterations.

If the ping is successful and you receive responses, from the IP address, then a device is found with the IP address of the server you removed from the network and a duplicate IP address exists. If there is no response, then no duplicate IP address exists at this time.

Address Resolution Protocol (ARP) Table

The following is the arp table from a router. IP address 192.0.2.19 was the target IP address of a ping. There was no response to the ping and because of this the Hardware Address is shown as incomplete in the table. The hardware address column is populated from a successful Address Resolution Protocol (ARP) request. The ARP protocol is used to learn the Ethernet address of a device for a given IP address. In our example give above, the instructions were to clear the ARP cache and then ping the target IP address. Before the ping (ICMP) packets can be sent to the host, a ARP request and reply must be received and the ARP table of the sending router or workstation must be populated. If the ARP request fails, the ARP table is listed as incomplete and it is an indication that this IP address is not in use, as would be the case if the Ethernet cable is removed from that device from the switch port.

```
vpn1-2851-1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.0.2.1              -   0015.627f.ae20  ARPA   Integrated-Service-Engine1/0
Internet  192.0.2.2              0   0016.9d38.cabb  ARPA   Integrated-Service-Engine1/0
Internet  192.0.2.5              -   0015.627f.ae28  ARPA   Video-Service-Engine2/0
Internet  192.0.2.6              0   001b.54bc.ead0  ARPA   Video-Service-Engine2/0
Internet  192.0.2.17             -   0015.627f.ae10  ARPA   GigabitEthernet0/0.206
Internet  192.0.2.19             0   Incomplete      ARPA
Internet  192.0.2.20             0   001d.e5ea.7999  ARPA   GigabitEthernet0/0.206
```

The IP address of 192.0.2.20 is a Cisco IP camera connected to VLAN 206 with Ethernet MAC address 001d.e5ea.7999.

Show CDP neighbors

The IP camera at address 192.0.2.20 is attached to the G1/0/6 port on a Cisco 3750 access-layer switch. Because CDP is enabled on the camera by default, showing the CDP neighbor for that port with the detail option provides a verification of the Ethernet MAC address and IP address of the camera.

```
vpn2-3750-access#show cdp neighbors g1/0/6 detail
-------------------------
Device ID: 001DE5EA7999
Entry address(es):
  IP address: 192.0.2.20
Platform: CIVS-IPC-2500,  Capabilities: Host
Interface: GigabitEthernet1/0/6,  Port ID (outgoing port): eth0
Holdtime : 121 sec

Version :
2.1.2

advertisement version: 2
Duplex: full
Power drawn: 9.000 Watts
Power request id: 4732, Power management id: 4
Power request levels are:9000 0 0 0 0
Management address(es):
  IP address: 192.0.2.20
```

Using CDP is also a means to verify the duplex configuration of the neighbor. The duplex value of the IP camera is shown in the above display output.

Displaying the MAC-Address Table (Static Entries)

The Cisco 3750 switch interface port configuration includes port-security with the sticky option. The sticky option stores the first MAC address it learns in the configuration and it also becomes a static MAC addresses in the switch MAC-address table.

```
interface GigabitEthernet1/0/6
 description CIVS-IPC-2500 ESELAB
 switchport access vlan 206
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 001d.e5ea.7999
 load-interval 60
 mls qos trust dscp
 spanning-tree portfast
 spanning-tree bpdufilter enable
end
```

Because the sticky option creates a static MAC address in the mac-address table, the *static* option must be used to verify the CAM table for a port so configured. This is shown in the following output:

```
vpn2-3750-access#show mac address-table static int g1/0/6
          Mac Address Table
-------------------------------------------
```

```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 206    001d.e5ea.7999    STATIC      Gi1/0/6
```

Displaying the MAC-Address Table (Static Entries)

As a further illustration, a port on the same switch which is not configured with port security is also shown.

```
!
interface GigabitEthernet1/0/13
 description CIVS-IPC-4500-4
 switchport access vlan 220
 switchport mode access
 load-interval 60
 mls qos trust dscp
 spanning-tree portfast
 spanning-tree bpdufilter enable
end
```

Because no port security exists, the MAC address of the IP camera is learned dynamically and entered into the MAC-address table as a dynamic entry. This command format is shown below.

```
vpn2-3750-access#show mac address-table dynamic int g1/0/13
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 220    001b.53ff.6cb9    DYNAMIC     Gi1/0/13
```

Summary

In this section, a methodology for determining if a duplicate IP address exists on the network. Additionally, the ARP table on the router is shown, illustrating the relationship between the IP network address (Layer 3) and the Ethernet MAC address (Layer 2). Additionally, sample switch port configurations are shown with and without port security. The mac-address table for both static MAC addresses and dynamic MAC addresses is shown. The CDP neighbor command is used to demonstrate how CDP can be used to also verify the IP network address and the Ethernet MAC address in use by a Cisco IP camera. The MAC address is printed on the housing of many IP cameras, using this unique value is useful in identifying these devices on the network.

QoS Considerations for Backup Media Servers

Backup Media Servers (VSMS) can be defined in the Operations Manager (VSOM) administration configuration section. The backup files are transported from the remote Media Server to the backup Media Server over a TCP/HTTP session. The remote Media Server initiates the connection to TCP port 80.

The DiffServ QoS (RFC 4594-based) recommended marking for backups, E-mail and other File transfer applications is DSCP AF1 and referred to as High-Throughput applications. These types of data flows are long lived file transfer type applications. In testing, the backups were observed to run for a duration of over an hour for backups of standard definition IP cameras on LAN links shaped to 30Mbps.

LAN Switch Marking Example

The following configuration represents a LAN access switch (Cisco Catalyst 3750 Series) marking the backup traffic as AF11, the live or archive video traffic from the VMSS server as DSCP CS5 and the control plane traffic as DSCP CS3. The IP addresses (192.0.2.2, 192.0.2.34 and 192.0.2.65) referenced in the access-list VSMS_BACKUP are the branch office Media Servers initiating the backups.

```
!
hostname vpn2-3750-access
!
class-map match-all VSMS_BACKUP
 match access-group name VSMS_BACKUP
!
class-map match-all HTTP_acl
 match access-group name HTTP
!
policy-map VSMS
 class VSMS_BACKUP
  set dscp af11
 class HTTP_acl
  set dscp cs5
 class class-default
  set dscp cs3
!
!
interface GigabitEthernet1/0/17
 description ese-mediasvr-cc1
 switchport access vlan 220
 switchport mode access
 load-interval 30
 priority-queue out
 mls qos trust dscp
 spanning-tree portfast
 spanning-tree bpdufilter enable
 service-policy input VSMS
!
ip access-list extended VSMS_BACKUP
 permit tcp any eq www host 192.0.2.2
 permit tcp any eq www host 192.0.2.34
 permit tcp any eq www host 192.0.2.65
!
ip access-list extended HTTP
 permit tcp any eq www any
!
end
```

It is assumed that intermediate routers and switches are configured to apply the appropriate queueing strategy for packets marked AF11. An example queueing configuration is shown in the next section.

Branch Router Sample Configuration

The branch router has a Cisco Video Management and Storage System Network Module (VMSS) in interface Integrated-Service-Engine3/0 and two uplinks GigabitEthernet0/1.342 and GigabitEthernet0/1.343. This configuration illustrates marking on ingress from the VMSS network module and a hierarchical CBWFQ service policy on the output interfaces shaping these Ethernet handoff interfaces to 30Mbps. The ingress service policy marks HTTP traffic destined to the backup Media Server at IP address 192.0.2.137 as AF11. This bandwidth class is called HIGH-THROUGHPUT-DATA and during congestion is limited to four percent of the shaped bandwidth value of 30Mbps. The recommendation of DiffServ QoS (RFC 4594-based) is to apply DSCP-based Weighted random early detection (WRED) to the class and this optional configuration command (**random-detect dscp-based**).

```
hostname vpn1-3845-1
!
class-map match-any HIGH-THROUGHPUT-DATA
 match ip dscp af11  af12  af13
!
class-map match-any VMSS
 match access-group name HTTP
!
class-map match-any VSMS_BACKUP
 match access-group name VSMS_BACKUP
!
policy-map INGRESS_VMSS
 class VMSS
  set ip dscp cs5
 class VSMS_BACKUP
  set ip dscp af11
 class class-default
  set ip dscp cs3
!
policy-map IPVS_BRANCH
 class BROADCAST-VIDEO
  bandwidth percent 40
 class VOICE
  priority percent 10
 class LOW-LATENCY-DATA
  bandwidth percent 4
 class HIGH-THROUGHPUT-DATA
  bandwidth percent 4
  random-detect dscp-based
 class MULTIMEDIA-CONFERENCING
  bandwidth percent 4
 class SCAVENGER
  bandwidth percent 1
 class OAM
  bandwidth percent 1
 class NETWORK-CONTROL
  bandwidth percent 1
 class CALL-SIGNALING
  bandwidth percent 1
 class class-default
  fair-queue
policy-map 30M
 class class-default
```

```
  shape average 30000000
  service-policy IPVS_BRANCH
!
ip access-list extended HTTP
 permit tcp host 192.0.2.65 eq www any
ip access-list extended VSMS_BACKUP
 permit tcp any host 192.0.2.137 eq www
!
interface Integrated-Service-Engine3/0
 description NME-VMSS-HP32
 ip vrf forwarding IPVS
 ip address 192.0.2.64 255.255.255.254
 ip flow ingress
 ip route-cache flow
 load-interval 30
 service-module external ip address 192.168.11.2 255.255.255.0
 service-module ip address 192.0.2.65 255.255.255.254
 service-module ip default-gateway 192.0.2.64
 no keepalive
 service-policy input INGRESS_VMSS
!
interface GigabitEthernet0/1.342
 encapsulation dot1Q 342
 ip vrf forwarding IPVS
 ip address 192.168.15.78 255.255.255.252
 ip summary-address eigrp 65 192.0.2.64 255.255.255.192 5
 service-policy output 30M
!
interface GigabitEthernet0/1.343
 encapsulation dot1Q 343
 ip vrf forwarding IPVS
 ip address 192.168.15.90 255.255.255.252
 ip summary-address eigrp 65 192.0.2.64 255.255.255.192 5
 service-policy output 30M
!
end
```

Verification

To verify the QoS marking on both the remote router and switch at the backup Media Server are marking traffic correctly, a WAN router with NetFlow enabled can be used to view the backup flows from two branch routers (192.0.2.2 and 192.0.2.65) to the backup Media Server at IP address 192.0.2.137. NetFlow displays the Tos byte in hexidecimal. The value of 0x28 is binary 00101000 which is DSCP value AF11.

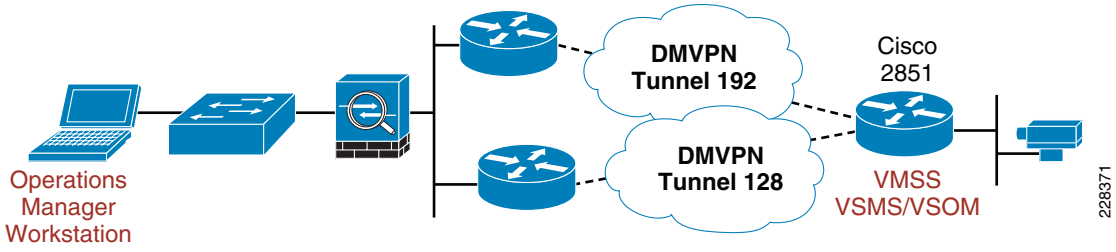
```
vpn-jk2-7206-1#show ip cache verbose flow
...
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Fa0/1.342      192.0.2.65      Fa0/1.91       192.0.2.137     06 28  18      21K
82F7 /0  0                     0050 /0  0     0.0.0.0              1419    10.0
Fa0/1.91       192.0.2.137     Fa0/1.342      192.0.2.65      06 28  10      60K
0050 /0  0                     82F7 /0  0     0.0.0.0                54    46.9
Fa0/1.91       192.0.2.137     Tu128          192.0.2.2       06 28  10    5445
0050 /0  0                     8C04 /0  0     0.0.0.0                54    47.6
Tu128          192.0.2.2       Fa0/1.91       192.0.2.137     06 28  10    3192
8C04 /0  0                     0050 /0  0     0.0.0.0              1400    15.6
```

One other observation that can be made from this sample output is the average number of bytes per packet for the archive backup is 1419 and 1400. One branch router is WAN attached through a DMVPN encrypted tunnel (192.0.2.2) and the other branch (192.0.2.65) is connected to the command center through an Ethernet LAN topology.

Asymmetric Routing

Asymmetric routing is very common in networks with redundant paths. For example, in the *IP Video Surveillance Design Guide* (http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/IPVS/IPVS_DG/IPVS_DG.pdf) one reference topology connected branch routers with VMSS network modules to a Metro Ethernet WAN and transported the video surveillance network traffic in encrypted DMVPN tunnels. Each branch router was configured with two tunnel interfaces; tunnel192 and tunnel128. This is shown in Figure 11.

Figure 11 Asymmetrical Topology



Two tunnels are used to provide high availability. The WAN links transporting the tunnels could be provisioned through separate service providers, and terminating the tunnels on separate DMVPN head-end aggregation routers allows the network manager to take one of theses routers out of service for software upgrades or maintenance without interrupting connectivity between the central site command center and the video feeds from the remote branch office.

It is very possible that the TCP connection to the HTTP server on the VMSS network module traverses tunnel 128 from PC to HTTP server while the return path for that connection traverses tunnel 192. Of course, if one of the DMVPN aggregation routers is taken out of service, only one path exists between the operations manager workstation and the remote HTTP server and no asymmetrical routing can happen.

The network engineer can implement high availability and at the same time configure the network so asymmetrical routing does not exist. In other words, the alternate path is only used during a failure of the primary path in both directions. This is the case with the reference topology. The Firewall is configured with a default gateway using the Hot Standby Router Protocol (HSRP) IP address shared between the two DMVPN WAN aggregation routers. The HSRP priority is configured so that the DMVPN WAN aggregation router for tunnel 128 is normally the active router. This will route traffic from the operations manager workstation to the branch router by way of tunnel 128.

The DMVPN WAN aggregation router for tunnel 192 is configured to advertise routes through tunnel192 with an offset-list applied to the metrics of the routes advertised. The offset-list command adds a constant value to the metric to make the routes appear less desirable even though they may be of equal cost to the routes learned through the alternate tunnel, tunnel128. The branch router has two routes in the EIGRP topology table, but only inserts one route into the routing table.

By using these two techniques, HSRP priority and EIGRP offset-lists, the network engineer has provided redundancy in the network while eliminating asymmetrical routing.

Following are **show** commands with comments to provide detailed information on the topology. First, the BW and DLY values of the tunnel interface are shown to be the same for the two tunnels.

```
vpn1-2851-1#show interfaces tu128 | inc MTU
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
vpn1-2851-1#show interfaces tu192 | inc MTU
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
```

EIGRP uses a composite metric based on the cumulative delay and minimum bandwidth. Tunnel interfaces by default use a bandwidth of 9Kbit, even though the actual bandwidth of the physical interface in this example is gigabitEthernet. Because the values are the same, they are not relevant in the composite metric. By showing the routing table for network 192.0.2.0 (the command center network address that supports the operations manager workstation in the illustration) only one route to that network is present in the virtual routing table of the branch router.

```
vpn1-2851-1#show ip route vrf IPVS 192.0.2.0 255.255.255.0
Routing entry for 192.0.2.0/24
  Known via "eigrp 65", distance 90, metric 297247232, type internal
  Redistributing via eigrp 65
  Last update from 192.168.15.129 on Tunnel128, 2w4d ago
  Routing Descriptor Blocks:
  * 192.168.15.129, from 192.168.15.129, 2w4d ago, via Tunnel128
      Route metric is 297247232, traffic share count is 1
      Total delay is 500110 microseconds, minimum bandwidth is 9 Kbit
      Reliability 255/255, minimum MTU 1400 bytes
      Loading 1/255, Hops 2
```

However, the EIGRP topology table has both paths, tunnel128 and tunnel192.

```
vpn1-2851-1#show ip eigrp vrf IPVS topology 192.0.2.0 255.255.255.0
IP-EIGRP (AS 65): Topology entry for 192.0.2.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 297247232
  Routing Descriptor Blocks:
  192.168.15.129 (Tunnel128), from 192.168.15.129, Send flag is 0x0
      Composite metric is (297247232/28416), Route is Internal
      Vector metric:
        Minimum bandwidth is 9 Kbit
        Total delay is 500110 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1400
        Hop count is 2
  192.168.15.193 (Tunnel192), from 192.168.15.193, Send flag is 0x0
      Composite metric is (297248232/29416), Route is Internal
      Vector metric:
        Minimum bandwidth is 9 Kbit
        Total delay is 500149 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1400
        Hop count is 2
```

Note that the composite metric value for tunnel192 is a value 1,000 higher than tunnel128. Now looking at the configuration for the DMVPN WAN aggregation router owning tunnel192, the *offset-list* in the EIGRP configuration specifies a value of 1,000 to be added to routes advertised from this router.

```
!
interface Tunnel192
 ip vrf forwarding IPVS
 ip address 192.168.15.193 255.255.255.192

!
router eigrp 65
 redistribute eigrp 64 metric 1000 100 255 1 1500 route-map DEFAULT
 network 192.168.15.0 0.0.0.63
 no auto-summary
 !
 address-family ipv4 vrf IPVS
  redistribute static metric 1000 10 255 1 1500 route-map COMMAND_CENTER
  offset-list 0 out 1000
```

```
  network 192.168.15.64 0.0.0.63
  network 192.168.15.192 0.0.0.63
  distribute-list route-map Branch_Net_vrf_IPVS_RT in
  no auto-summary
  autonomous-system 65
 exit-address-family
!
```

On this same router, the HSRP priority is defined as 90, the alternate router uses the default value of 100, which makes it the preferred HSRP router.

```
interface FastEthernet0/1.91
 description ASA DMZ vrf IPVS
 encapsulation dot1Q 91
 ip vrf forwarding IPVS
 ip address 192.168.15.98 255.255.255.248
 ip flow ingress
 standby 0 ip 192.168.15.102
 standby 0 priority 90
 standby 0 preempt delay minimum 60
!
```

In this example, therefore, the alternate router configuration for both HSRP and EIGRP controls the forward path and return path to eliminate asymmetrical routing. The primary router uses default configuration values for both EIGRP and HSRP.

Asymmetrical routing typically is not an issue in networks although some functions like NAT/pNAT and stateful firewalls may not function as expected when the return path is not through the same devices supporting these functions.

Switch Configuration—Reference Network Topology

This is the switch configuration from Figure 8.

```
!
interface GigabitEthernet1/0/19
 description trunk to vpn1-3845-1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 load-interval 60
 priority-queue out
 mls qos trust dscp
end

vpn2-3750-access#show interfaces gigabitEthernet 1/0/19
GigabitEthernet1/0/19 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 0019.2f98.0113 (bia 0019.2f98.0113)
  Description: trunk to vpn1-3845-1
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 3/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:42, output 00:00:00, output hang never
  Last clearing of "show interface" counters 4w6d
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  1 minute input rate 7395000 bits/sec, 957 packets/sec
  1 minute output rate 13809000 bits/sec, 1600 packets/sec
     1551434217 packets input, 164895982301 bytes, 0 no buffer
```

```
Received 4597730 broadcasts (4596423 multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 4596423 multicast, 107 pause input
0 input packets with dribble condition detected
5149780746 packets output, 7273624088578 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out
```

Clearing Interface Counters

Beginning in Cisco IOS Release 12.3(1), the ability to schedule some EXEC command-line interface (CLI) commands to run at specific times/intervals was introduced. This feature provides similar functionality to the Cron (time-based job scheduler) in Unix-like computer operating systems.

The following sample configuration is used to schedule a **clear counters** command weekly on Wednesdays at 11:00am,

```
no kron occurrence clrcntr at 11:00 Wed recurring
kron occurrence clrcntr at 11:00 Wed recurring
 policy-list clrcntr
exit
!
kron policy-list clrcntr
 cli clear counter
exit
!
```

The current schedule can be displayed with the **show kron schedule** command.

```
router#show kron schedule
Kron Occurrence Schedule
clrcntr inactive, will run again in 6 days 23:59:51 at 11:00 on Wed
```

The console output shown below is from a time period before and after the 11:00 initiation of the scheduled job to clear the interface counters.

```
vpn1-2851-1#show interface g0/0 | include GigabitEthernet|counter
GigabitEthernet0/0 is up, line protocol is up
  Last clearing of "show interface" counters 00:17:37

vpn1-2851-1#
Feb  3 11:00:34.698 est: %CLEAR-5-COUNTERS: Clear counter ….

vpn1-2851-1#show interface g0/0 | include GigabitEthernet|counter
GigabitEthernet0/0 is up, line protocol is up
  Last clearing of "show interface" counters 00:00:13
```

Automating the **clear counter** command with this configuration can be a useful tool to assist with the network assessment tasks and ongoing network troubleshooting.

For more information, see the following URL:
http://www.cisco.com/en/US/docs/ios/12_3/feature/guide/g_kron.html

Q&A from Network Readiness Assessment for IPVS Webinar

Q&A from the Webinar Network Readiness Assessment for IP Video Surveillance (session number 202239128) on Tuesday, February 23, 2010. The 1 hour and 23 minute recording is available for playback, Click the link below to play it:

https://cisco.webex.com/ciscosales/lsr.php?AT=pb&SP=EC&rID=42300707&rKey=7d3276e94cf7fcdb

---

Q. Some of our clients balk at switch upgrades. How can this be addressed?

A. I put the upgrades in terms of health and human safety. Since many clients are using this for police or public safety surveillance, the switch is now in the “critical path” just as a patrol car, a security officer, etc. This tends to put the cost of the upgrade into perspective.

Q. Many customers have switches from vendors other than Cisco, will the readiness plans provide for assessment of non-Cisco deployments?

A. The network assessment should apply to video in general, regardless of vendor. However, the commands used to collect information from the switch will differ.

Q. Does Cisco have a standard service called IP VS Assessment service?

A. There are plans to train and assist third-party companies to conduct assessments as part of their service offerings.

Q. Where can we find detailed documentation regarding network management instrumentation included in Cisco's IPVS and EAC devices and applications? Need MIB info, SYSLOG messages and what they mean, etc.

A. There is a chapter on SNMP Monitoring in the *Cisco Video Surveillance Media Server User Guide* at the following URL:
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_surveillance.html

Q. When comparing IPVS HD camera feeds to TelePresence, what is the bitrate used by Telepresence?

A. TelePresence goes up to 4 Mbps in 1080p per camera. A CTS-3000 with network overhead uses about 15.3 Mbps.

Q. Are bursts seen only with Cisco HD cameras? Is this something common with other cameras as well?

A. All video is sent as frames. Also there are always reference frames an non-reference frames. Therefore, all video is more or less bursty. High definition video sends more information per frame; therefore, the bursts are more of an issue.

Q. If we have 22 HD and 14 SD cameras, considering their bit rate, what would be an ideal storage to archive 30 days of history? Do we have a tool that can help us calculate the storage needs in such a situation?

A. A *Cisco Video Surveillance Stream Manager Storage Calculator* is available on the internal Emerging Technologies Group Physical Security web page. Your Cisco support contacts can provide you with this planning process.

Q. On the slide 'LAN Switching Hierarchy Best practice deployment for a large enterprise campus', why are we putting DVR and Management Server/VSOM in the core? Why not the classic model using the server block?

A. You could deploy a server distribution layer and attach these servers as you indicate. The hierarchical layers do not need to be distinct physical entities. Layers can be omitted, but hierarchy should be maintained for optimum performance. The number of servers required in the deployment would determine if a separate server distribution layer is required. For only a few server, the costs associated with the additional chassis would be prohibited.

Q. Would we discuss video camera deployment city-wide?

A. This presentation is more geared toward a traditional enterprise network, versus a city wide deployment, but great question. Many of the issues with regard to packet loss, latency, and jitter still apply however.

Q. In terms of access switch and core, is Virtual Switching System (VSS) recommended for core for low latency?

A. VSS is a means to provide network system virtualization. It does not reduce LAN latency, which is minimal, a few milliseconds at most.

Q. How much overhead does a VPN add? Are we dealing with separate sites or HIPAA control issues?

A. For a discussion on encryption overhead for TelePresence in the Implementing TelePresence over Broadband, refer to the following URL:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/TNS_x_BB_whitepaper.html

With IP Video Surveillance as well as TelePresence, assume 6 to 7 percent for planning purposes.

Q. Is QoS implementation required to have VS traffic on the network?

A. It is certainly recommended. It can be argued that if you overprovision your network enough such that congestion never occurs anywhere, then QoS is not needed. In reality, congestion does momentarily occur in almost all networks.

Q. How do you analyze the data generated by the IP SLA?

A. Typically directly via show commands on the device...but there is some ability to set thresholds and generate SNMP traps based on those thresholds. Also, for long-term collection, trend analysis and graphing, CiscoWorks Internetwork Performance Monitor (IPM) can configure probes and collect the output.

Q. Does the router record the IP SLA data to the log? Can we use syslog to offload the data to a server?

A. You can log against thresholds, the configuration is at the following URL:

http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsthresh.html

If the history option is enabled, the history table is stored in memory.

Q. Do you recommend running the IP SLA continuously or just for troubleshooting purposes? Does it have an impact on the network if it runs all the time?

A. It is recommended both running continuously and also configure probes to help diagnosis individual problems. There are several sessions at Cisco Live and Cisco Networkers 2010

http://www.cisco.com/web/learning/le21/le34/learning_networkers_home.html

- BRKNMS-1204—Introduction to Network Performance Measurement with Cisco IOS IP Service Level Agent
- TECNMS-2005—IP Service Level Agreements—How To Do It!, which provide more education on IP SLA

Q. Does MPEG4 UDP include a sequence number to track for losses?

A. RTP (over UDP) has a timestamp and sequence number.

Q. Can you talk of asymmetric routing potential impact on video transmission.

A. Video by itself (UDP/RTP) is a one-way flow, as is QoS. Where there is a feedback loop such as TCP video, or RTCP, then the return path may play a role, especially if there are drops. For more information, refer to "Asymmetric Routing" section on page 77.

Q. Can you give an example of how QoS can make things worse. Some people are now recommending not enabling QoS, which might be due to lack of not knowing how to use it.

A. There are some default settings of QoS on switches that are not optimal for how we recommend deploying IPVS.We recommend enabling QoS on switch and router platforms to ensure proper operation with IPVS. One example is enabling QoS on the switch globally (**mls qos**), configuring the IP cameras to mark their media feed CS5, and then not enabling the **priority-queue out** command on the interface connecting the media server.

Q. Is there white paper on implementing QoS with video and voice? This is a reoccurring theme with our clients.

A. QoS documentation on Design Zone for Video are found at the following URLs:

http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/qosmrn.html

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html

References and Supplemental Reading

- How Does H.264 Work? Understanding video compression with a focus on H.264

  http://www.salientsys.com/files/Understanding%20H.264.pdf
- Troubleshooting Cisco Catalyst 2960, 3560, 3560e,3750 and 3750e, Series Switches (BRKRST-3141)

  http://vsearch.cisco.com/main.cfm?m=browse.course&cid=3130#
- Troubleshooting TCP/IP

  http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1907.html
- Cisco IOS IP Service Level Agreements User Guide

  http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_white_paper09186a00802d5efe.html
- How LAN Switches Work

  http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a00800a7af3.shtml
- Cisco Catalyst 3750 Data Sheet

  http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps5023/product_data_sheet0900aecd80371991.html
- Troubleshooting Tools

  http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1902.html