Network Readiness Assessment for IP Video Surveillance

Updated 1 March 2010

Joel W. King
joel.king@cisco.com

A Powerpoint version is available by Emailing *ask-nra-ipvs@cisco.com*

Abstract

Network Readiness Assessment for IP Video Surveillance

One of the greatest challenges of deploying IP video surveillance is to assess if the existing network infrastructure, or proposed network topology, is capable of transporting IP video surveillance.

The current market space for IP video surveillance sales opportunities are typically small engagements managed by physical security integrators. These partners must be trained in IP networking to insure the implementation is successful. The outlook for growth of IP video surveillance (IPVS) is strong and continues to accelerate.

Joel King, Technical Leader for IPVS architectures in ESE, will discuss:

- best practices for assessing an existing or proposed network topology to transport IPVS
- explain the network characteristics of IPVS
- demonstrate how to design the network to address these characteristics
- Provide detailed 'how to' steps to Assessing Switching (LAN) and Routing Readiness
- How to configure Cisco IOS IP Service Level Agreements (SLAs) to assess the network
- Provide implementation checklists to help manage the deployment.

There is a companion white paper to the slides presented in the webinar. Questions during the presentation will be included in a Q&A section of the white paper.

Goals

- Define best practices for assessing an existing or proposed network topology to transport IP video surveillance
- Determine if the infrastructure is capable of handing IP video surveillance traffic
- Insure a timely deployment and successful ongoing operation of the network to support IP video surveillance

Agenda

- General Network Requirements
- Network Characteristics of IP Video Surveillance
- Design Considerations
- Specific Network Requirements
  - Assessing Switching (LAN) Readiness
  - Assessing Routing Readiness
  - Service Level Assessments
  - Security and Application Optimization Assessment
  - Quality of Service (QoS) Assessment
- Network Assessment Checklist
- Summary

General Network Requirements

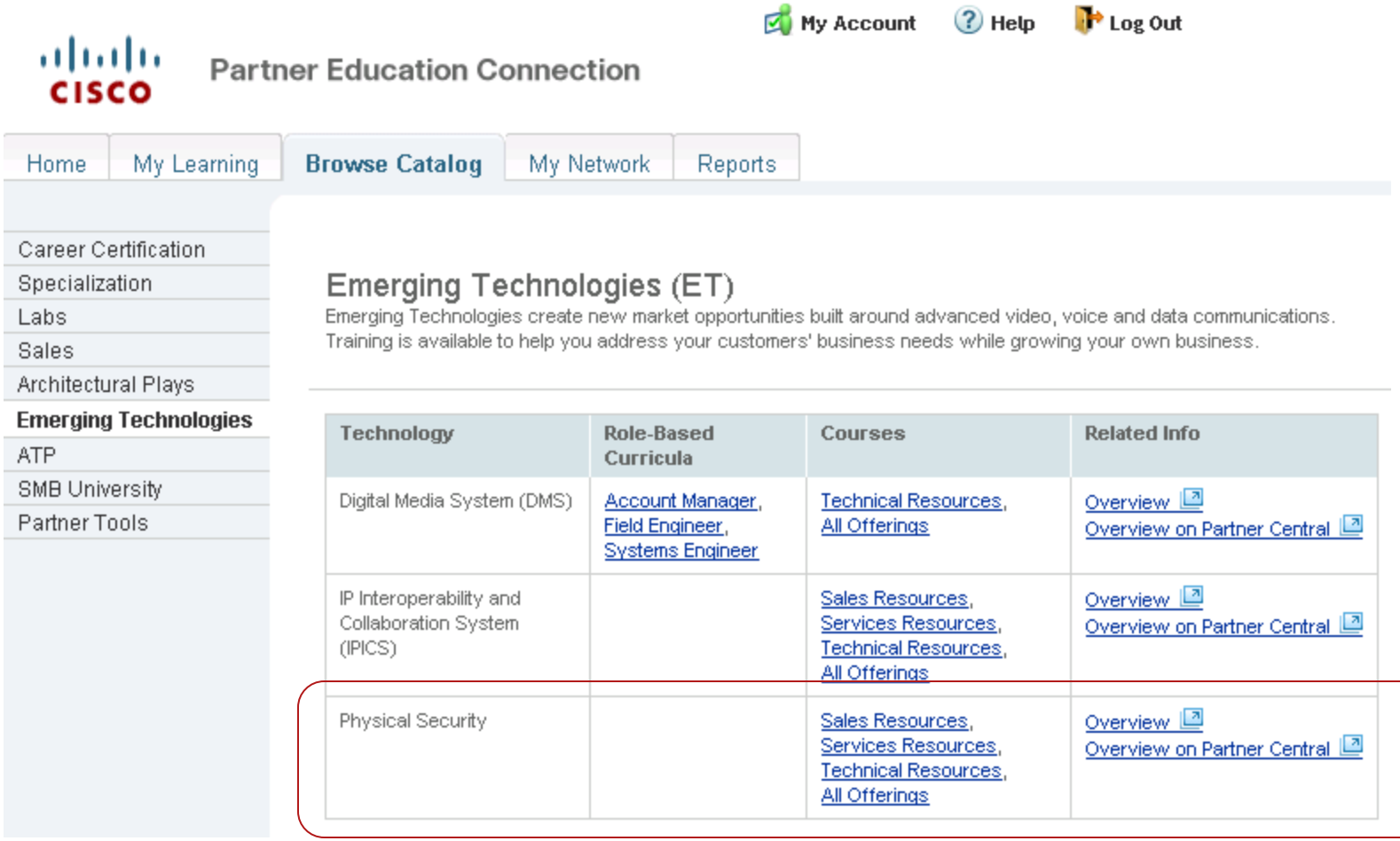
- Project Management
- Education and Training
- Documentation
- Network Services
- Network Management

Project Management

- Works with Stake Holders
- Defines the Scope of the Project
- Develops Timelines
- Coordinates Detailed Planning
- Monitors Progress
- Communicates Updates
- Addresses Risks and Roadblocks

Education and Training
http://cisco.partnerelearning.com/Saba/Web/Main

[insert training requirements for system integrators HERE]



Documentation
Physical Layout

- Physical Floor Plan of Camera Placement
- Location and Distances to wiring closets
- Document cabling distances to cameras
  - Twisted Pair
  - Fiber
- Power requirements
  - PoE
  - Street Power

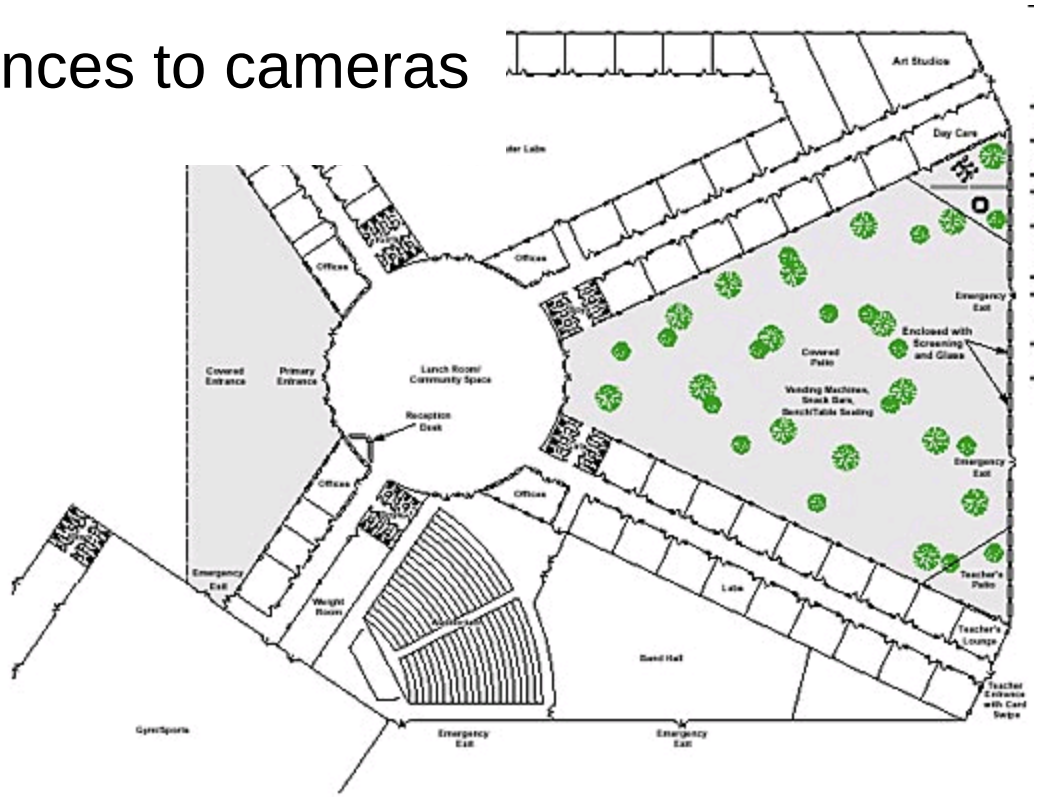
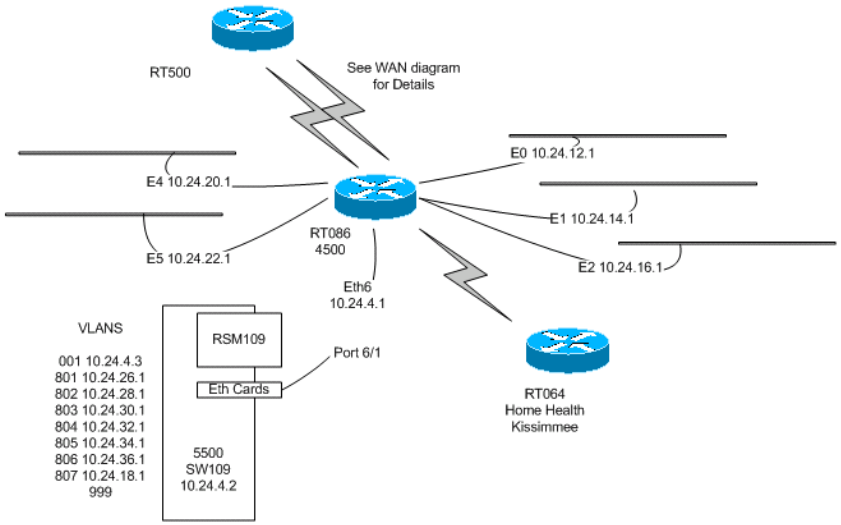


Exhibit 1.10. This drawing depicts a school design that incorporates some security-conscious features.

Documentation
Network Hardware

- Inventory existing network equipment
  - Model / Type of interfaces / Memory
  - Software Versions
- Overlay the Physical Inventory Requirements with the Network hardware
- Develop Bill of Materials
  - Cabling
  - Access, distribution and core switches
  - Routers, Firewalls
  - Media Servers
  - IP Cameras



Network Services

- IP video surveillance requires
  - Network Time Protocol (NTP) servers
  - Power over Ethernet,
  - system logging (Syslog)
  - File transfer (FTP/TFTP) servers
  - Simple Network Management Protocol (SNMP) trap servers.
- Network assessment process must identify and access these services within the enterprise network
- Implement servers which do not exist

Network Management

- Often overlooked but a critical component for on-going success
- Fault, Configuration, Accounting, Performance, and Security: FCAPS
- Monitor network devices for for packet loss, errors, memory and CPU utilization
- Measure network utilization trends

Network Characteristics of IP Video Surveillance

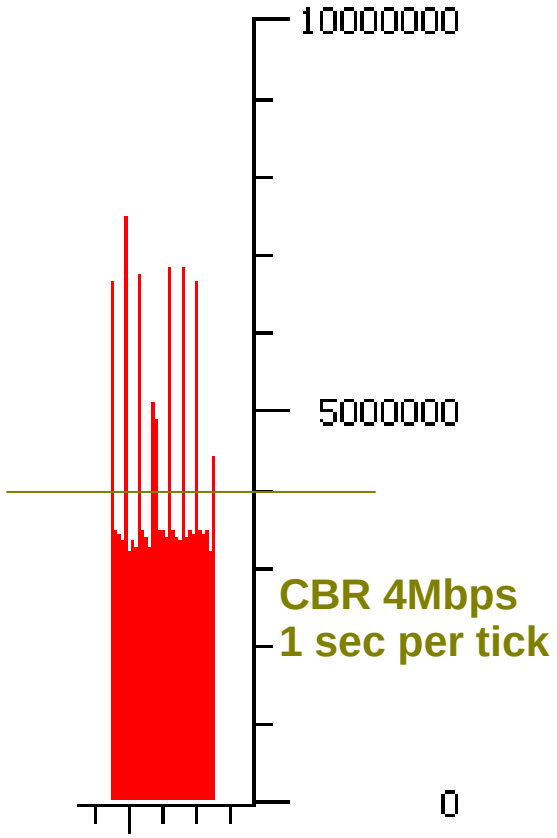
Network Characteristics of IP Video Surveillance

- Bandwidth
  - SD (4CIF/D1 MPEG-4 15fps **1Mbps** / 30fps **2Mbps**)
  - SD (Motion JPEG **2-8Mbps**)
  - HD (1920 x 1080 H.264 30fps **4-6 Mbps)**
- Bursts
- Packet Loss
- Latency
- Jitter
- Quality of Service (QoS)

HD Camera H.264 1920x1080 CBR 8M

Bursts

- In MPEG-4 / H.264, the bursts are associated with the transmission of reference frames, or I-frames.
- Standard Definition (D1) ~ 16-30 packets
- High Definition (1080p) ~300 packets
- As Image resolution and complexity increases, so does the number of IP packets necessary to transport slices



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

High Definition IP Cameras
Bursts

- I-frame generated every ~ 4 sec. (128 GOV /30 fps)
- CBR 4M = 383 pps and ave. packet size ~ 1,400 bytes
- Network load approaches 100Mbps during I-frame transmission – appx 50ms (1/20th second)
- P/B frames every 33ms

Note:
Video Surveillance images can be far more complex than Telepresence

Packet Loss

- Packet loss in the network will be noticeable in the video quality of MPEG-4 and H.264 video feeds.
- Standard Definition below ½ of 1% may be acceptable
- High Definition even 1/10th of 1% may be noticeable.

SD Camera MPEG-4 720x480 1% loss

Latency

- Depends on the transport protocol
- MPEG4 / H.264 transported in TCP is not tolerant of high latency
- IP cameras with two-way (PAN-TILT-ZOOM) need low latency
- MPEG4 / H.264 in UDP/RTP tolerant of high latency

Jitter

- Jitter generally increases as latency increases.
- If Jitter is high, latency will likely also be an issue
- Address the latency issue first - jitter will take care of itself
- Jitter is more of an issue with VoIP than with IP VS deployments
- IP Video Surveillance requires
  1. **Adequate Bandwidth**
  2. **No Loss**
  3. **Low / Reasonable Latency**

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 .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

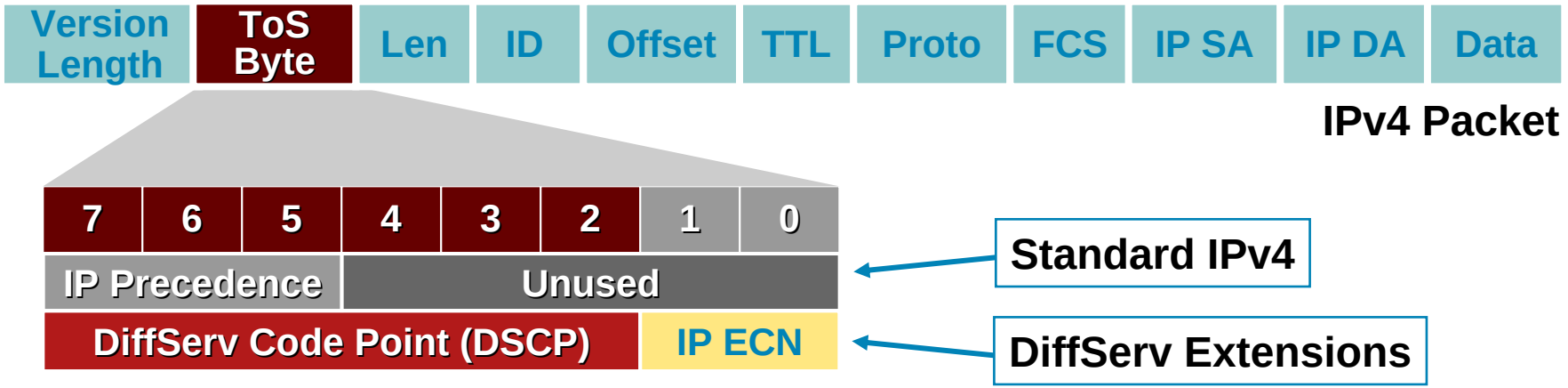
Quality of Service (QoS)

- On a converged VoIP, Data and Video Network QoS usually is required to allocate resources to transport Video with low loss.
- Marking can be done on IP Cameras, but also by routers and switches for servers and viewing workstations.
- *Cisco IP Video Surveillance Design Guide*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/IPVS/IPVS_DG/IPVS_DG.pdf
- *QoS Design Recommendations for Medianets*

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

Classification Tools
IP Precedence and DiffServ Code Points



- IPv4: Three most significant bits of ToS byte are called IP Precedence (IPP)—other bits unused
- DiffServ: Six most significant bits of ToS byte are called DiffServ Code Point (DSCP)—remaining two bits used for flow control
- DSCP is backward-compatible with IP precedence

Cisco medianet Application Classes

DiffServ QoS Recommendations (RFC 4594-Based)

Application Class	Per-Hop Behavior	Admission Control	Queuing & Dropping	Application Examples
VoIP Telephony	EF	Required	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
Broadcast Video	CS5	Required	(Optional) PQ	Cisco IP Video Surveillance / Cisco Enterprise TV
Realtime Interactive	CS4	Required	(Optional) PQ	Cisco TelePresence
Multimedia Conferencing	AF4	Required	BW Queue + DSCP WRED	Cisco Unified Personal Communicator
Multimedia Streaming	AF3	Recommended	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	CS6		BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
Call-Signaling	CS3		BW Queue	SCCP, SIP, H.323
Ops / Admin / Mgmt (OAM)	CS2		BW Queue	SNMP, SSH, Syslog
Transactional Data	AF2		BW Queue + DSCP WRED	Cisco WebEx / MeetingPlace / ERP Apps
Bulk Data	AF1		BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
Best Effort	DF		Default Queue + RED	Default Class
Scavenger	CS1		Min BW Queue (Deferential)	YouTube, iTunes, BitTorent, Xbox Live

Design Considerations

Overview

- Examine where IPVS Component devices are deployed in the network topology
- WAN bandwidth is costly compared to that of the LAN
- Video feeds on the LAN as much as practical
- Only transport across WAN as necessary
- LAN switch is the basic network device for connecting IP cameras, Workstations and NDVR (Media Server)

LAN Switching Defined

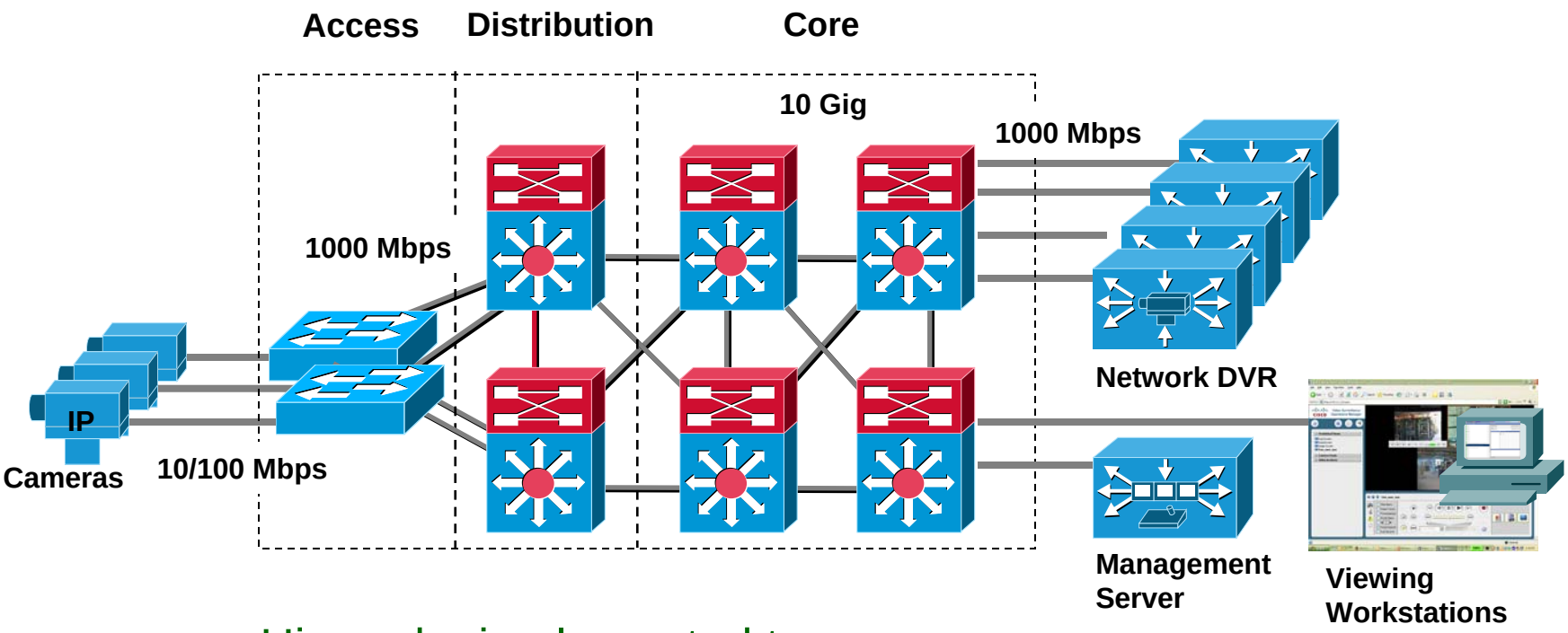
- LAN switches operate at the Data Link (Layer 2) network layer
- LAN switches
  - store incoming packets in buffers
  - looks up the destination (MAC) address in a table
  - forwards the packet out the appropriate port.
- Ethernet hubs operate a the physical layer (Layer 1)
- IPVS deployment should NOT contain Ethernet hubs!
- Hubs are repeaters, and simply extends segments all nodes (ports) 'see' all traffic.

Switch Port
Speeds and Feeds

- 10 / 100 Mbps (Ethernet / FastEthernet) Full Duplex – IP Cameras
- 10/100/1000 Mbps (Gigabit Ethernet) – Servers and Workstations
- Common - fixed configuration, 24 or 48 port switch w/ 32-Gbps backplane and two uplink ports
- IEEE 802.3af, the standard for Power over Ethernet (for IP Cameras)
- Cisco Catalyst 3560G-24PS or 3750G-48PS are examples

LAN Switching Hierarchy

Best practice deployment for a large enterprise campus



Hierarchy implemented to

- Scale
- Provide Redundancy
- Traverse Distance Limitations

Distances

- 100BASE-TX (100 Mbit/s over two-pair Cat5)
  - 100 meters
- 100BASE-FX SFP multimode fiber-optic (MMF)
  - 2 kilometers
- 100BASE-LX10 SFP single-mode fiber-optic (SMF)
  - 10 kilometers

Fast Ethernet

- 1000BASE-TX Twisted-pair cabling (CAT-6, CAT-7)
  - 100 meters
- 1000BASE-SX Multi-mode fiber
  - 220 meters
- 1000BASE-LX Multi-mode fiber / Single-mode fiber
  - 550 meters / 5 kilometers

Gigabit Ethernet

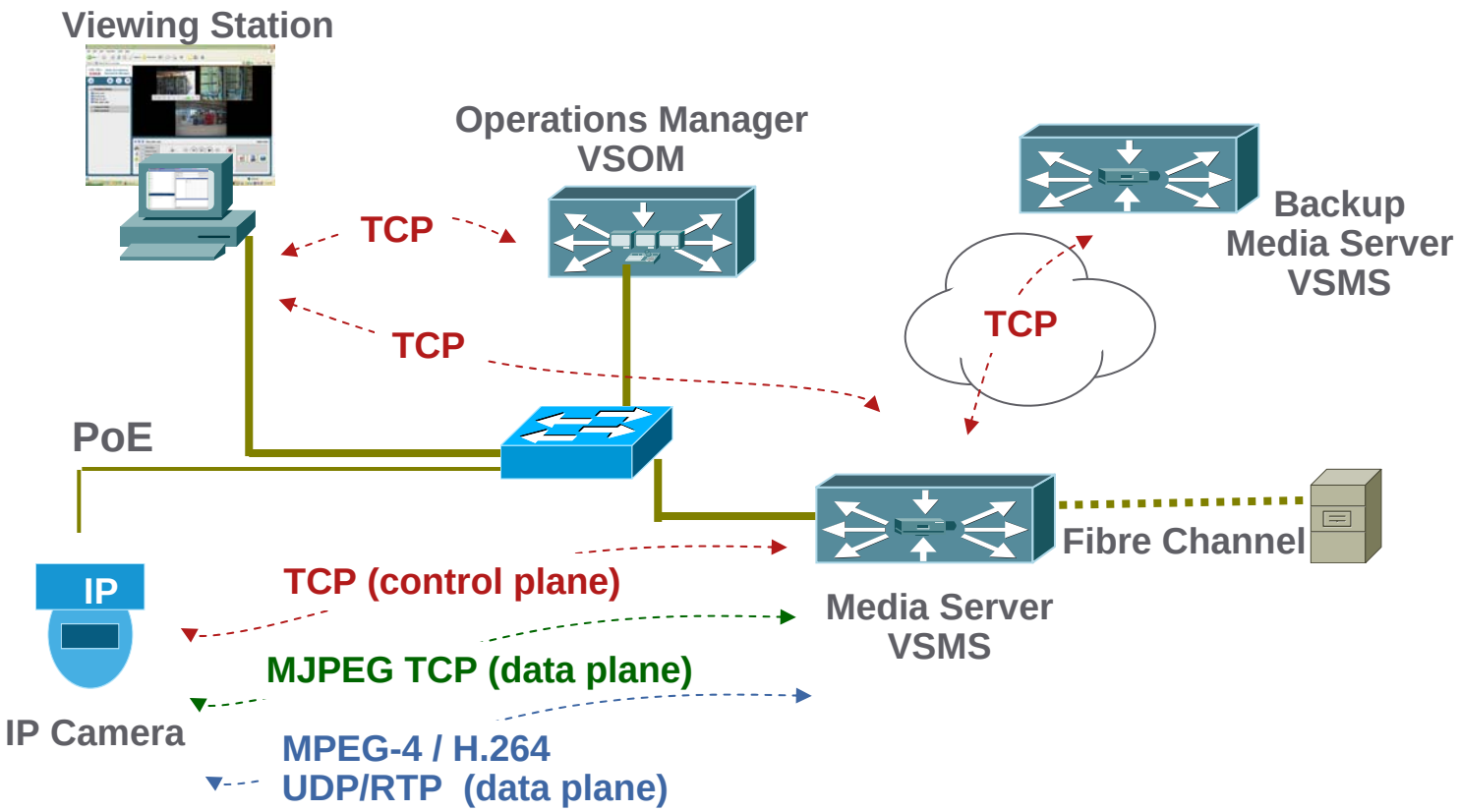
- 10GBASE-SR ("short range") OM3 multi-mode fiber (MMF)
  - 300 meters

10 Gigabit Eth

Small Form-factor Pluggable (SFP)

Network Data Flows - Transport Layer Protocols

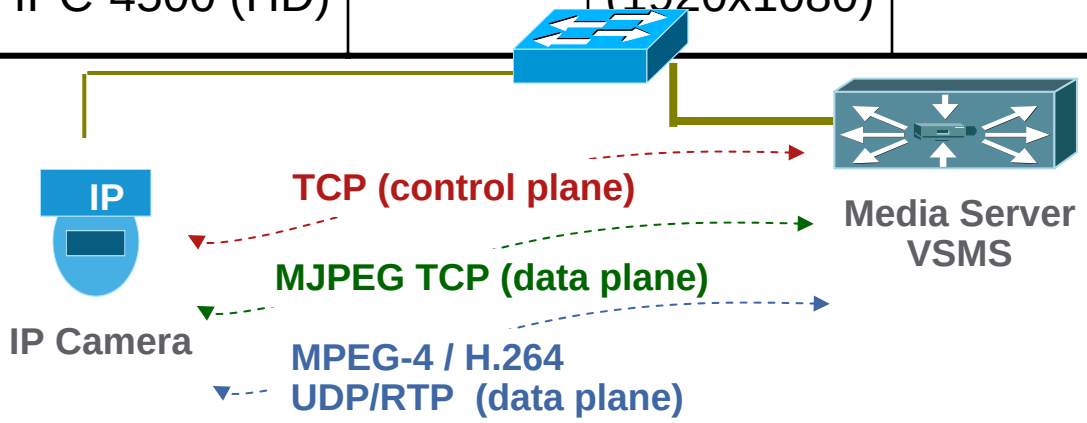
Small business deployment – single switch



Understanding the data flows is relevant to single switch or three tier campus deployment.

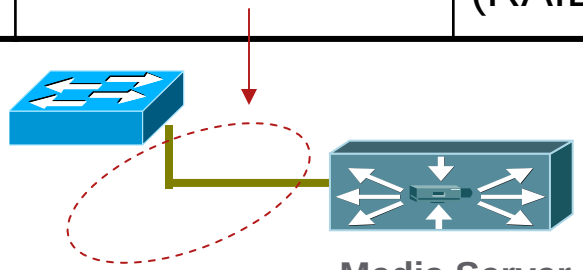
IP Cameras
Per Camera Network Bandwidth Estimates

Camera	CODEC	Resolution	Frame Rate	Average Load
CIVS-IPC-2500 (SD)	MPEG-4	D1 (720x480)	15 fps	1 Mbps
CIVS-IPC-2500 (SD)	MPEG-4	D1 (720x480)	30 fps	2 Mbps
CIVS-IPC-2500 (SD)	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



Media Servers

Server	Maximum I/O	Maximum Internal Storage
CIVS-MSP-1RU 1RU chassis	60 Mbps	**4 TeraBytes** (no RAID-5)
CIVS-MSP-2RU 2RU chassis	200 Mbps	**12 TeraBytes** (RAID5)
CIVS-MSP-4RU 4RU chassis	200 Mbps	**24 TeraBytes** (RAID5)



Media Server VSMS

HD IP camera - CBR 6Mbps - maximum I/O value of 200Mbps - estimated that a 2RU/4RU chassis can support approximately 32 cameras (minus number of feeds viewed live

http://wwwin.cisco.com/etg/physec/files/understanding_msp_performance.pdf

Disk Storage Requirements

Camera Configuration	Megabytes per 5 min. of archive (appx)
HD Camera H.264 1920x1080 CBR 4M	100
HD Camera H.264 1920x1080 CBR 5M	225
HD Camera H.264 1920x1080 CBR 8M	240
SD Camera MPEG-4 D1 (720x480) CBR 2M	76
SD Camera MJPEG D1 (720x480) 5 FPS	75
SD Camera MJPEG D1 (720x480) 10 FPS	150

Given the 100 Mbytes for a 5 minute archive, the disk requirement per day is 28 Gigabytes per day (100Mbytes * 12 * 24). 32 Cameras = **1TB per day**

Media Server
VSMS

HD Camera H.264 1920x1080 CBR 4M

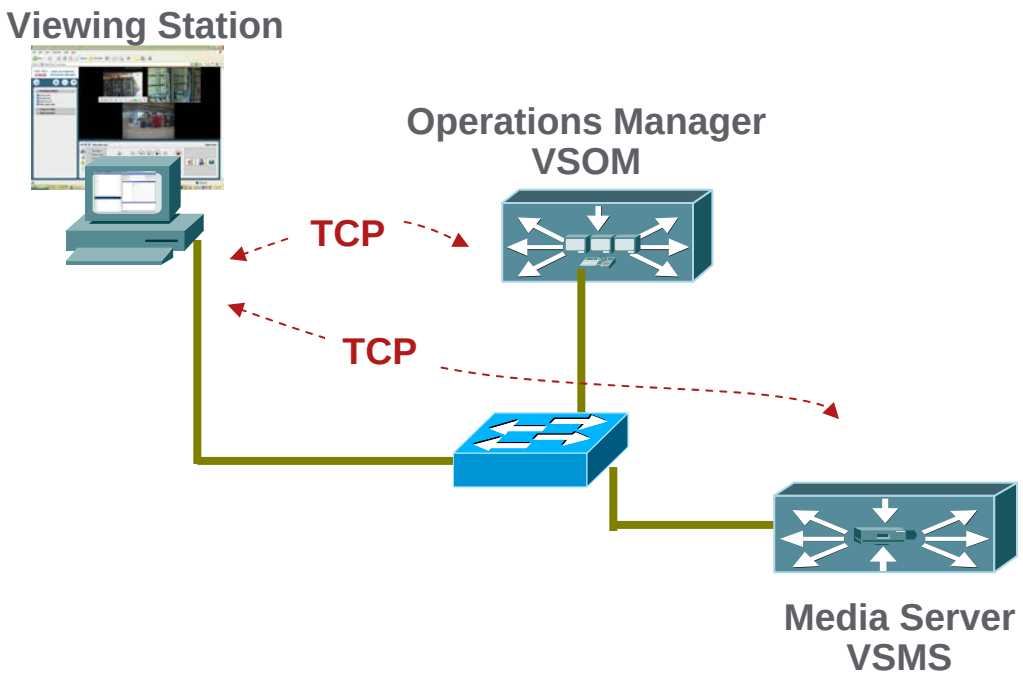
HD Camera H.264 1920x1080 CBR 5M

HD Camera H.264 1920x1080 CBR 8M

SD Camera 720x480 MJPEG 5 FPS

Operations Manager (VSOM) and Viewing Station

- BW between viewing station and the VSOM minimal
- Majority of the data traffic is from the Media Server
- Media Server acts as a direct proxy between the IP camera feeds



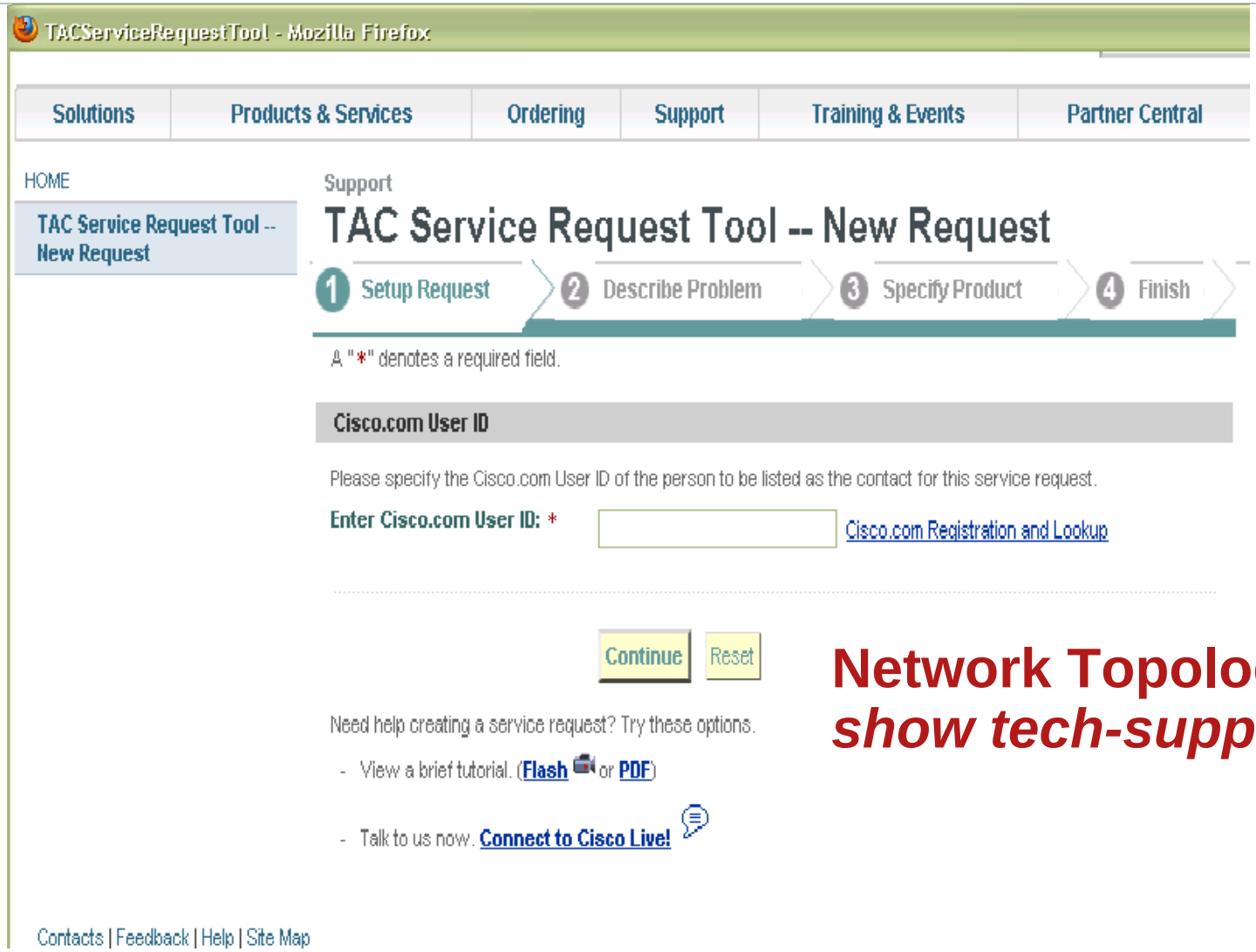
Note:
Workstation System and video card HW /SW requirements!

Summary

- Examined Interface/port requirements for LAN switches
- Importance of deploying a LAN Switching Hierarchy
- Listed Distances for various Ethernet port speeds
- Tracked Network Data Flows between components
- Looked at Bandwidth and I/O estimates
- Storage Requirements

Specific Network Requirements

Two key pieces of information
for resolving network related issues



Network Topology diagram
show tech-support

Assessing Switching (LAN) Readiness

Overview

- Guidelines for assessing the readiness of the LAN switches to transport IP video surveillance traffic
- Introducing video on the network illustrates many existing problems not apparent with data transport
- Based on NATkit Network Analysis Toolkit (Cisco) - LAN Switching Stability Audit
- Advanced Services
  http://www.cisco.com/en/US/products/svcs/ps2961/serv_category_home.html

Assessing Switching (LAN) Readiness

- Inventory - the model and software versions
- Ports/Interfaces- determine available capacity
- VLANs- how physical switch is logically partitioned
- Power over Ethernet
- Physical Connectivity- inventory of existing devices
- Environmental Statistics- power and cooling status of switches
- Memory Utilization- verify switches have sufficient memory
- Local Link Issues- any link errors or capacity issues?
- Overall Capacity Assessment- capacity of trunks / uplinks
- Logging and Network Time Protocol- aid in troubleshooting

Clearing Counters

- Recommendations are based on various interface counters and other statistics
- Many network problems can be resolved with a

  show log

  show interface
- If counters are never cleared, you don't have a reference point across all devices in the path
- Once a week, counters should be cleared across all devices in the network.
- Network Assessment conducted in 5-7 days after clearing counters

Inventory

- Switch IOS Version, model, uptime, reason for last reload, memory and configuration register
- Identifies if hardware or software need be upgraded
- Switch stability issues (uptime)

```
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

- Inventory number of physical ports by type, speed (eg. 100baseTX, FastEthernet twisted pair copper)
- Capability (eg. Power over Ethernet).
- Number of ports active and inactive

is this a problem?

```
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
...
Gi1/0/23 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
```

show platform pm link-status command also provides link state for each port.

VLANs

Virtual LANs (VLANs) are logical connections

- Trunk ports use tags (headers) to associate packets and the VLAN - IEEE 802.1Q - *dot1q*
- VLAN Trunking Protocol (VTP) manages VLANs between switches
- Configuring Layer-3 links between access and distribution layer switches minimizes VLAN complexity

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

```
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
```

Power over Ethernet

- Most IP cameras require IEEE 802.3af standard PoE
- Look at the available, used and remaining Watts

```
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

vpn2-3750-access#show interfaces g1/0/7 | inc Desc
  Description: Linksys PVC2300-F491
```

Physical Connectivity

- IP Cameras
  - FastEthernet (10/100Mbps) Full Duplex
  - IEEE 802.3af—Power over Ethernet
  - Cable runs 100 meters - 100BASE-TX
- Client Viewing Stations
  - 1000Mbps (1 Gigabit Ethernet)
- VSMS Media Servers and VSOM Operations Manager
  - 1000Mbps (1 Gigabit Ethernet)

Environmental Statistics

- Display environmental status information
  - power supply
  - fan status
  - temperature
  - power input to the chassis

```
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
```

Looking for fan issues or airflow problem

CPU Utilization

- Main CPU is not used for normal switching of traffic between ports.
- Traffic sent to the main CPU - Routing protocol traffic, tacacs, ssh, telnet, icmp, Spanning Tree traffic, etc.
- High CPU packet drops by spanning tree queue, RP queue will cause network instability

```
vpn2-3750-access#show proc cpu sorted
CPU utilization for five seconds: 10%/0%; one minute: 9%; five minutes: 9%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
 207   445172402 241709276       1841  3.03%  2.99%  3.03%   0 Spanning Tree
   4    20706009   1768355      11709  1.27%  0.28%  0.20%   0 Check heaps
  60     4069450 363677323         11  0.31%  0.07%  0.01%   0 RedEarth Tx Mana
```

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

Memory Utilization

- Verify that switches are not low on memory
- Free memory less than 20% of the total value by memory category (Processor, I/O, etc) - monitor / upgrade / replace
- Processor memory is used by IOS
- I/O memory is used for packets send to the CPU

```
vpn2-3750-access#show version | include memory
cisco WS-C3750G-24PS (PowerPC405) processor (revision F0) with 131072K bytes…
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    45140356    27123744    25505200    16768896
      I/O    6400000    12582912     8532852     4050060     3992492     4047808
Driver te    2C00000     1048576          44     1048532     1048532     1048532
```

Local Link Issues

- Local link issues one cause of degraded video quality
- Goal is to identify any physical errors on ports
- Error counters are reset by the *clear counter* command

```
show interfaces counters errors

Port        CrcAlign-Err Dropped-Bad-Pkts Collisions   Symbol-Err
...
Fa3/12               117                0          0            0
Fa3/13                14                0          0            3
Fa3/14              3857                0          0            0
Fa3/15               276                0          0            0
Fa3/16                 1                0          0            1
Fa3/17                 0                0          0            0
Fa3/18               799                0          0            2
Fa3/19             59993                0          0            1
```

Likely a module-wide HW problem

show interface g1/0/2 counters errors

Link Capacity
Individual Ports and Trunk Capacity

```
vpn2-3750-access#show interfaces g1/0/17
GigabitEthernet1/0/17 is up, line protocol is up (connected)
  Description: ese-mediasvr-cc1
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 11/255, 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 00:00:01, output hang never
  Last clearing of "show interface" counters 2w6d
  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 174000 bits/sec, 310 packets/sec
  30 second output rate 43490000 bits/sec, 3829 packets/sec
```

```
vpn2-3750-access#show controllers utilization
Port        Receive Utilization  Transmit
Utilization
Gi1/0/1              2                    6
Gi1/0/2              0                    0
Gi1/0/3              6                    0
...
Gi1/0/17             0                    4
```

43 Mbps to this Media Server

Logging and Network Time Protocol

- Sysloging / NTP configured as best practice

```
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
```

```
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
```

Summary

- Focus is on existing inventory, HW and SW versions
- Documentation of existing network topology
- Logical and Physical Interface connectivity
- Determine any existing interface errors
- Capacity issues (pre and post implementation)
- Logging and NTP configuration for ongoing support

Assessing Routing Readiness

Overview

- Historically, routers provided WAN connectivity - switches LAN
- Today routing deployed in LAN to access layer (wiring closet)
- *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
- Switches may be deployed as CPE devices by MAN/WAN service providers

What is one advantage of deploying L2/L3 switches and routing the access layer?

Assessing Routing Readiness

- Inventory- model and software versions in the network
- CPU Utilization - understanding router CPU utilization
- Memory Utilization - displaying and analyzing memory utilization
- Environmental Statistics - power and cooling
- Buffer Tuning - tune buffers automatically
- Logging - aids in network troubleshooting
- Interfaces - primer on statistics - what statistics are important to network health
- Switching Path Analysis - also load sharing / asymmetrical routing
- Routed Protocol Analysis - Identify routed protocols
- Routing Protocol Analysis – What routing protocols are used
- Bridged Protocol Analysis - Identifying any bridged protocols

Clearing interface counters
Command Scheduler

- Feature Introduced 12.3(1)
- Schedule some EXEC command-line interface (CLI) commands to run at specific times / intervals.

```
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
!
show kron schedule

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

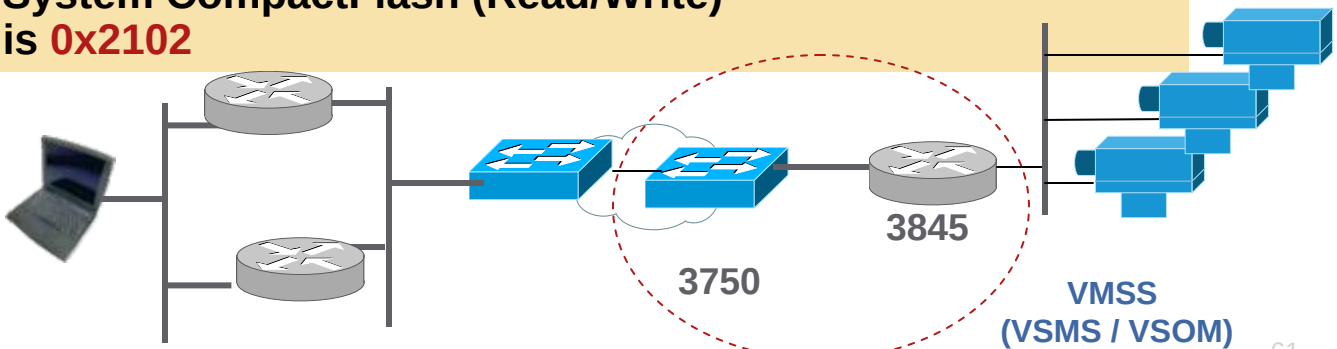
```
vpn1-2851-1#show interface g0/0 | include GigabitEthernet|counter
GigabitEthernet0/0 is up, line protocol is up
  Last clearing of "show interface" counters 00:17:37

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
```

http://www.cisco.com/en/US/docs/ios/12_3/feature/guide/g_kron.html

Inventory

- Router IOS Version, model,
- uptime and reason for last reload
- memory and configuration register value

```
vpn1-3845-1#show version | inc uptime|System|Config|memory
Copyright (c) 1986-2008 by Cisco Systems, Inc.
ROM: System Bootstrap, Version 12.4(13r)T10, RELEASE SOFTWARE (fc1)
vpn1-3845-1 uptime is 10 weeks, 5 days, 23 hours, 48 minutes
System returned to ROM by reload at 11:21:03 est Thu Nov 19 2009
System restarted at 11:22:59 est Thu Nov 19 2009
System image file is "flash:c3845-adventerprisek9-mz.124-15.T5"
Cisco 3845 (revision 1.0) with 1000448K/48128K bytes of memory.
250880K bytes of ATA System CompactFlash (Read/Write)
Configuration register is 0x2102
```



Router CPU Utilization

- CPU utilization may not be indication of network performance
- Cisco ASR 1000 Series Routers - distributed control plane architecture
- Separate Route Processor (RP)—responsible for routing protocols, CLI, network management, etc.
- Cisco 3800 Series Integrated Services Routers utilize the main CPU for packet switching
- In these platforms, CPU utilization below 50% are ideal, and ranges from 50% to 80% for the five minute average should be monitored more closely.

show processes cpu and ***show processes cpu history***

Memory Utilization

- Verify no memory leaks or low memory conditions
- Configure router to reload rather than ‘hang’ on memory issues.
- Note any memory issues in the assessment

```
exception memory fragment 32768
exception memory minimum io 262144
exception memory minimum 1048576
```

```
vpn1-3845-1#show memory statistics
                Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor   66DEB060   909201308    62356844   846844464   840913552   499864828
      I/O   2D100000    49282560    22457876    26824684    26750384    26812828
```

Troubleshooting Memory Problems
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6f3a.shtml

Environmental Statistics

- On two PS systems, one on street power, one UPS

```
vpn1-3845-1# show environment all

SYS PS1 is present.
      Fan status: Normal
      Input Voltage status: Normal
      DC Output Voltage status: Normal
      Type: AC
      Thermal status: Normal

SYS PS2 is present.
      Fan status: Normal
      Input Voltage status: Normal
      DC Output Voltage status: Normal
      Type: AC
      Thermal status: Normal

AUX(-48V) PS1 is present.
      Status: Normal

AUX(-48V) PS2 is present.
      Status: Normal
Compliance Mode: IEEE 802.af non-compliant

Fan  1 Normal
Fan  2 Normal
Fan  3 Normal

Fan Speed is Normal

Alert settings:
Intake temperature warning: Enabled, Threshold: 55
Core temperature warning: Enabled, Threshold: 70
(CPU: 90)

Board Temperature: Normal
Internal-ambient temperature = 35, Normal
CPU temperature = 47, Normal
Intake temperature = 28, Normal
Backplane temperature = 26, Normal

Voltage 1(3300) is Normal, Current voltage = 3284 mV
Voltage 2(5150) is Normal, Current voltage = 5153 mV
Voltage 3(2500) is Normal, Current voltage = 2501 mV
Voltage 4(1200) is Normal, Current voltage = 1203 mV

Nominal frequency
```

Buffer tuning / Logging

- In early versions of Cisco IOS, buffer tuning was a manual process
- Beginning 12.3(14)T can be done automatically use '*buffers tune automatic*‘ and ‘*show buffers tune*’
- Logging (buffered and syslog) should include timestamps – See Cisco IP Video Surveillance Design Guide at

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/IPVS/IPVS_DG/IPVS_DG.pdf.

```
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
```

Router Interface Statistics

- Three aspects of the router interfaces - configuration, utilization and errors.
- Network topology diagram - show the router interface, connected switch interface (port) speeds, duplex and type of encapsulation
- *show cdp neighbors {interface} detail* - Identify neighboring switch
- Utilization and Error analysis is used to avoid / detect packet loss at the interface level

Show interfaces

Configuration

Utilization

Input Errors

Output Errors

```
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 2/255
  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 3w2d
  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 11218000 bits/sec, 994 packets/sec
  30 second output rate 146000 bits/sec, 261 packets/sec
     2132971992 packets input, 865332148 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, 85688469 multicast, 0 pause input
     0 input packets with dribble condition detected
     748197230 packets output, 530484737 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
```

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.
- *Cisco IOS Switching Paths Overview* at

  http://www.cisco.com/en/US/docs/ios/12_2/switch/configuration/guide/xcfovips.html
- Verify switching path *show ip interface*

```
vpn1-3845-1#show ip interface GigabitEthernet0/1.342 | include switching|VPN
  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
```

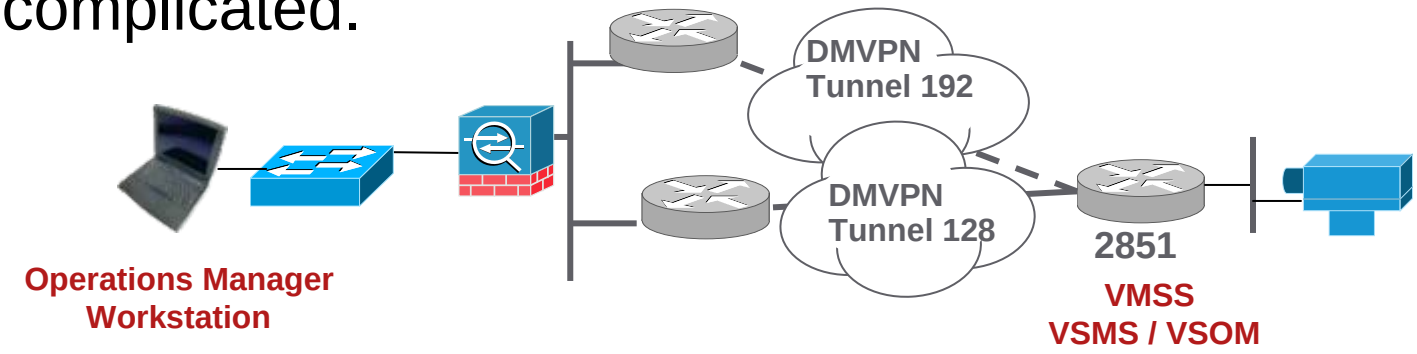
Load Sharing

- Routing protocol may insert two or more equal or unequal cost paths into the routing table
- The switching path determines load sharing
- Process switching or CEF can load share per packet
- Per packet load sharing is NOT recommended for voice or video applications
- Why? Increases the likelihood of out-of-order packets.

Network Assessment Topology Diagrams - document redundant paths

Asymmetric Routing

- Asymmetric routing - the network path from source IP address to destination IP address is different than the return path
- Asymmetric routing is common on the Internet
- Possible where multiple paths exist for redundancy or load sharing
- Asymmetric routing may make troubleshooting more complicated.



See *Asymmetric Routing in the* companion whitepaper for more details

Routed / Routing and Bridged
Protocol Analysis

- Routed protocols - define those network protocols which are routed at the network layer.
  - Appletalk, DECnet, IP, IPX, and Vines
  - Ideally only IP present in proposed network
- A routing protocol is the control plane for a routed protocol
- A routing protocol sends routing information packets to adjacent routers and, in turn, receives routing information packets.
  - Examples are BGP, EIGRP, IGRP, IS-IS, RIP, and OSPF
  - Ideally EIGRP, OSPF or BGP is used
- Bridged Protocol Analysis
  - Source-route bridging (SRB), Remote Source-Route Bridging (RSRB), Data Link Switching Plus (DLSw+), Synchronous Data Logical Link Control (SDLLC), and Transparent bridging.
  - Ideally no bridged protocols are in use

Summary

- Network assessment documentation
- Snapshot CPU, memory and interfaces statistics, discover if hardware / software upgraded are needed
- Hardware errors or capacity issues can be identified before IPVS deployment
- Verify (logging buffer / syslog) SNMP traps, and NTP services
- Identify the routed, bridged and routing protocols in use

Service Level Assessments

Service Level Assessment

- Need consistent tool to measure latency, loss, availability, etc.
- Ping (ICMP echo) is commonly used, widely available
- Accuracy and consistency across platforms vary
- Recommended tool is Cisco IOS IP Service Level Agreements (SLAs) (IP SLA)
- Some IP SLA probes must have a Cisco IOS IP SLAs *responder* to answer the probe
- Many can be answered IP based operating system

Shadow Routers

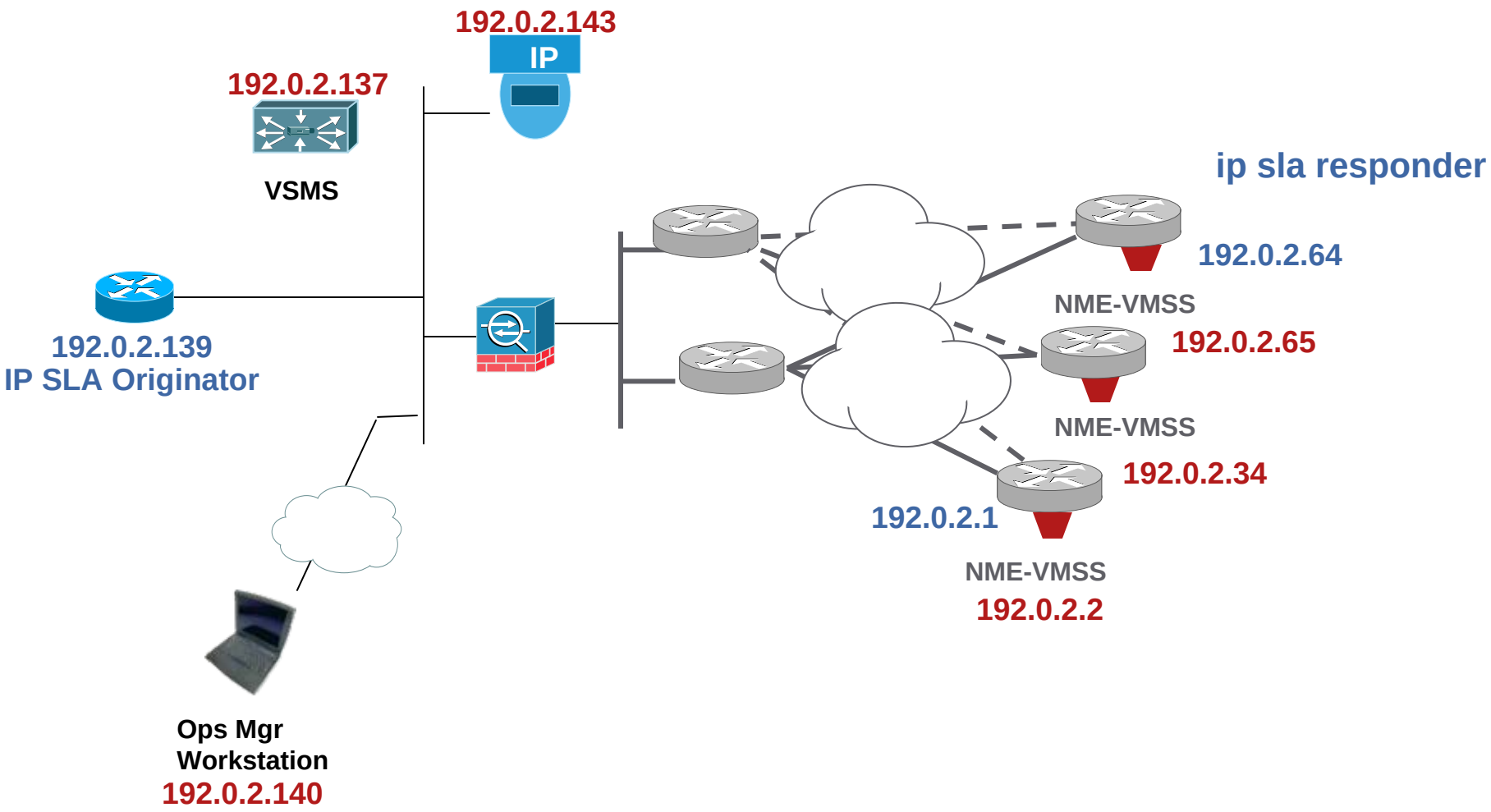
- Dedicated (shadow) SLAs routers can be deployed permanently or temporarily during the assessment
- 871 / 881 or 1800 / 1900 series routers are excellent shadow routers – low cost & small footprint
- Consider deploying IP SLA router at command center
  - IP SLA originator
  - Remote access to customer network via VPN
  - NTP local clock source for network (Internet reference clock)
  - DHCP server

IP SLA Responder
control protocol

- Some probes require use of IP SLA responder and control protocol
- Control protocol is required for UDP Jitter operations
- Best practice, include the *ip sla responder* in all router configurations
- Control protocol listens on UDP port 1967
- IP SLA responder gets control message, enables the specified UDP/TCP port for a specified duration and listens for 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:
```

IP SLA Testing
Topology



Cisco IOS IP Service Level Agreements (SLAs)

- Cisco IOS IP SLA can be configured to generate a variety of probes
- Probes with application to the IP video surveillance deployment.
  - ICMP Echo Operation
  - TCP Connect Operation
  - HTTP Operation
  - UDP Jitter Operation

ICMP Echo Operation
Diagnose Network Connectivity (Loss / Outages)

- Windows PC (viewing station) IP address 192.0.2.140
- ToS byte is decimal ’96’ or DSCP value CS3
- Frequency of 30 seconds, History is maintained

```
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
```

```
router#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
```

ICMP probe with history
CIVS-IPC-4500


```
vpn-jk3-2651xm-9#show ip sla history 343
…
Entry LifeI      BucketI    SampleI    SampleT    CompT      Sense      TargetAd
dr
343   1          1          1          438796893  0          4          192.0.2.143
343   1          2          1          438797893  3          1          192.0.2.143
343   1          3          1          438798393  4          1          192.0.2.143
343   1          4          1          438798893  4          1          192.0.2.143
343   1          5          1          438799393  4          1          192.0.2.143
                                                                        192.0.2.143
                                                                        192.0.2.143
                                                                        192.0.2.143
                                                                        192.0.2.143
                                                                        192.0.2.143
                                                                        192.0.2.143
                                                                        192.0.2.143
                                                                        192.0.2.143
                                                                        192.0.2.143
                                                                        192.0.2.143
343   1          18         1          438805893  1          1          192.0.2.143
343   1          19         1          438806393  1          1          192.0.2.143
343   1          20         1          438806893  1          1          192.0.2.143
```

```
ip sla 343
 icmp-echo 192.0.2.143
 tos 96
 frequency 5
 history lives-kept 1
 history buckets-kept 60
 history filter all
ip sla schedule 343 life 86000 start-time now
```

Individual history entries can be viewed with the *full* option

TCP Connect Operation
Diagnose Network Connectivity & Server Outages

- Target IP address 192.0.2.65 is VMSS Network Module (VSOM)
- ToS byte is configured as decimal ‘160’ or DSCP CS5
- *owner* and *tag* values are simply documentation
- Control protocol disabled (optionally enabled)
- Port may be any TCP port which server is listening

```
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
```

TCP Connect Operation
Intended Use Case

- Diagnosing network connectivity issues
- Media Server or Operations Manager server outages
- Aids in configuring the security policies on firewalls and access control lists - means of testing the access lists.
- The RTT includes both network latency and processing delay of the target host responding to the TCP connect request

```
router#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
```

HTTP Operation
Intended Use Case

- DNS lookup—RTT for domain name lookup (optional)
- TCP Connect—RTT to perform a TCP connection
- HTTP transaction time—RTT to send a request and get a page from the HTTP server

```
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
```

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.

HTTP Operation
Media Server

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

Business Class Cable Broadband
15M/2M with DMVPN (crypto) to Cisco RTP Campus

- *Implementing TelePresence over Broadband*

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

- Target IP addr is a Cisco Unified IP Phone CP-7970G. Cisco IP phone is a Web server

```
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
!
```

Business Class Cable Broadband
Internet Transport Sample Output

```
router#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 se
Operational state of entry: Activ
Last time this entry was reset: N
```

```
router#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
```

UDP Jitter Operation

Reports latency and jitter and loss in each direction

- UDP jitter operation requires IP SLA Responder
- Does not support the IP SLAs History feature – use CiscoWorks IPM for trending and history
- Calculates a Mean Opinion Score (MOS) for VoIP
- This probe is your multi-tool !

```
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
```

www.gerbergear.com

UDP Jitter Operation

```
Round Trip Time (RTT) for      Index 864
        Latest RTT: 19 milliseconds
Latest operation start time: 15:24:49.596 est Fri Jan 29 2010
Latest operation return code: OK
RTT Values:
        Number Of RTT: 30              RTT Min/Avg/Max: 15/19/27 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 30
        Source to Destination Latency one way Min/Avg/Max: 3/4/9 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 12/14/23 milliseconds
Jitter Time:
        Number of Jitter Samples: 29
        Source to Destination Jitter Min/Avg/Max: 1/2/6 milliseconds
        Destination to Source Jitter Min/Avg/Max: 1/2/8 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: 1
Number of failures: 0
Operation time to live: 86368 sec
```

CSCtf04341

Video Surveillance Packet Loss Reporting Enhancement

CSCtf04341 **Video Surveillance Packet Loss Reporting Enhancement**

Externally found enhancement (Sev6) bug: N-New

Notes and Attachments [3]: [Expand all enclosures] [Collapse all enclosures] [Sort alphabetically] [Sort chronologically]
General [3]: Description Documentation CAP-Info
Service Requests [1]:
Cap [1]: CAP002213

[Unwrap text] [Edit this enclosure]
Documentation: Added 02/15/2010 11:04:03 by joeking

CSCtf04341 Video Surveillance Packet Loss Reporting Enhancement
==========

As part of the Physical Security Strategic Improvement Process (SIP
Readiness Assessment (NRA) document and supporting collateral has b

These documents are available at:

Network Readiness Assessment for IP Video Surveillance
http://wwwin-eng.cisco.com/Eng/ESE/Video/IPVS/IPVS network assessment joeking.ppt
Doc No: EDCS-846081

Network Readiness Assessment for IP Video Surveillance
http://wwwin-eng.cisco.com/Eng/ESE/Video/IPVS/Network Readiness Assessment for IP Vide o_Surveillance.zip
Doc No: EDCS-845082

The NRA documents describe best practices for network design and troubleshooting and
the use of Cisco IOS IP SLAs (IP SLA) to measure the network for latency, loss and jitter.

Packet Loss
==========

Packet loss in the network is perhaps the key problem which causes poor video quality.

Packet Loss is not reliably detected by probes because of the small number of probe packets compared to the media stream itself.

The Video endpoints (Media Servers) must report packet loss such that the problem can be identified and corrected.

Summary

- Demonstrated use/ configuration of four types of IP SLA probes
- UDP Jitter operation provides most useful data points
- Probes are marked with QoS DSCP values of the traffic they are intended to emulate
- Probe output does not measure bandwidth capacity!
- Reference

  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

Security and Application Optimization Assessment

- Policy-based security implementations block traffic specific destination based on some rule or administrative policy
- Firewalls and access control lists (ACLs)
- Network Assessment should identify Firewalls and access-control lists on routers and Layer-3 switches
- Firewall functionality can be implemented in software on a router, or as an appliance.
- If no access control lists, firewalls, packet shapers or packet optimization devices exist – note on topology / inventory

Access Control Lists (ACL)

- Lists of permissions (or explicit denies) which govern if packets are allowed to be forwarded to the intended destination.
- *Cisco IP Video Surveillance Design Guide*, section *Required TCP/UDP Ports* on page 4-11 specifies what ports and protocols between the various components of the Cisco Video Surveillance Manager (VSM)
- Network Assessment should note access control lists on the topology diagram.

Firewalls and NAT/pNAT

- Zone-Based Policy Firewall (ZFW) introduced in Cisco IOS Software Release 12.4(6)T
- ZFW is more aligned with the PIX or ASA firewall configuration commands
- Network Address Translation / Port Address Translation (NAT/pNAT) very common on FW configuration
- Additional analysis and configuration may be needed if NAT/pNAT is implemented between components of the IP video surveillance deployment

Application Optimization / Packet Shapers

- Wide Area Application *Services (WAAS) shown in the Cisco IP Video Surveillance Design Guide Wide Area Application Services (WAAS) Integration* on page 6-61
- WAAS does not optimize video surveillance feeds to the extent it does data applications.
- Packet Shapers are layer 7 application shaping
- Application shapers identify traffic and define a policy to control the flow (transmission) rate
- Packet shaping video surveillance traffic may contribute to video quality issues.

Quality of Service (QoS) Assessment

“ For those situations where the vast majority of user traffic is the same COS, then going with QOS disabled may be a viable option (and assuming no other QOS features are needed) ”

“ If all you do is enable QOS with “msl qos” command then, the switch is likely to have worse performance rather than better. ”

Medianet Switches

- Have Gigabit-Ethernet interfaces
- Implement in hardware a strict priority queue with at least three additional queues.
- Cisco Catalyst 2975, 3560G, 3750G, 3560-E, and 3750-E family of switches
- Best practice is to deploy switches which are *medianet ready*
- Do not implement (and look to replace) any switches which are solely 10/100 Mbps switches!

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

Network Assessment Checklist
See whitepaper for individual items

- ***General Network Requirements***
- ***Design Considerations***
- ***Switching (LAN) Assessment***
- ***Routing Assessment***
- ***Specific Network Requirements***

Appendix

Appendix
These topics are included in the whitepaper

- **HTTP connect connections over Internet WANs**

  Demonstrates Cisco IOS IP SLA probes over Internet

- **Why Packet Loss Impacts IP Video Surveillance**

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

- **Troubleshooting Duplicate IP Addresses**

  How to determine if a duplicate IP address exists on the network

- **QoS considerations for Backup Media Servers**

  Archives copied from remote Media Server to the backup Media Server over a TCP/HTTP session.

- **Asymmetric Routing**

  Asymmetric routing is very common in networks with redundant paths

- **References and Supplemental Reading**

Summary

Summary

- Plan – define the scope, coordinate and communicate!
- Document – what equipment exists today? Is the bandwidth available?
- Inspect – are problems systemic or do isolated, individual, problems exist?
- Measure – initial and ongoing analysis of network performance
- Design – does the network design lend itself to video transport?

Case Study

Problem Statement

Backup of Video Archive taking almost 12 hours

- **Analog Camera Attached to an Analog Video Gateway Network Module**
- **H.264 encoding Target Bit Rate 1024K (1Mbps)**
- **Resolution 704 x 480 – NTSC or 4CIF (15 fps)**
- **Step through verifying if this elapsed time is expected for completing the archive**

Backup Details

Each 5 minutes of video require ~ 41Mbytes

Backup Details
Name: a_p_AutoDome-12_-_a_AutoDome-12
Status: Succeeded
Start Time: 2010-01-25 11:15:01
End Time: 2010-01-25 23:14:43
Log:
Job started at Mon Jan 25 11:15:01 2010
Processing job for archive: a_p_AutoDome-12_-_a_AutoDome-12
Backup Name: a_s_192_0_2_2_a_p_AutoDome-12_-_a_AutoDome-12_bk
Remote Host: 192.0.2.137

Archive Start Time: Wed Oct 21 10:58:18 2009
Archive End Time: Ongoing
Backup Period (after archive start/end time and last backup file time filtering):
Sun Jan 24 11:15:00 2010
Mon Jan 25 11:14:00 2010

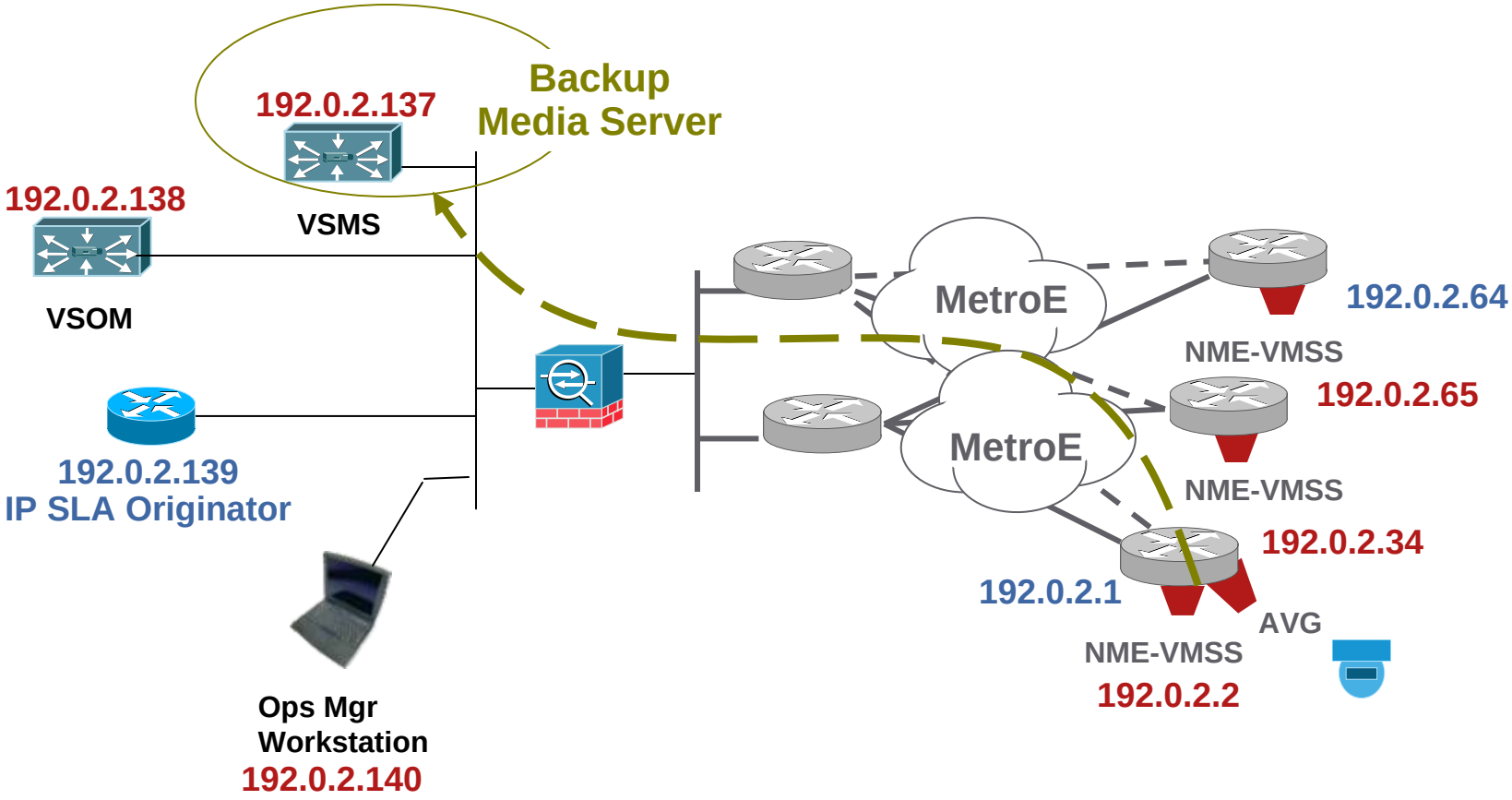
Found file entry /media0/1000/20100125/4b5cdfc6.smd size 41035420
…
Sending file /1000/20100125/4b5dc0c6.smd: Sent
Sending file /1000/20100125/4b5dc1f2.smd: Sent

Sent 289 files

executeJob returned: CURL succeeded
…

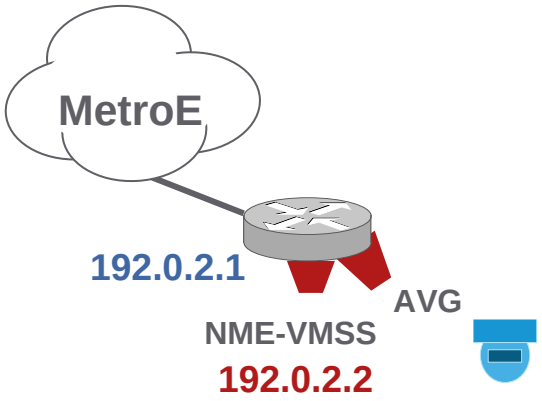
the file size looks reasonable based on the calculations of the stream from camera

Backup Archive
Topology



Troubleshooting Steps

- Check the Network Path the Backup is taking
- Look at the interface data rates while the backup is running
- Determine QoS settings



Check Network Path

```
vpn1-2851-1#show ip route vrf IPVS  192.0.2.137
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, 7w0d ago
  Routing Descriptor Blocks:
  * 192.168.15.129, from 192.168.15.129, 7w0d 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
```

Verify Tunnel Interface

```
vpn1-2851-1#show interfaces tunnel 128
Tunnel128 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.15.130/26
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 255/255, rxload 255/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 192.168.15.46 (GigabitEthernet0/1.332), destination 192.168.15.40
  Tunnel protocol/transport GRE/IP
    Key 0x80, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "IPVS_Branches_ipsec_profile")
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters 2w1d
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 12113
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 75000 bits/sec, 117 packets/sec
  5 minute output rate 2355000 bits/sec, 218 packets/sec
     81154962 packets input, 2154058051 bytes, 0 no buffer
     ...
```

Verify Path of Tunnel 128

```
vpn1-2851-1# show ip cef exact-route 192.168.15.46 192.168.15.40
192.168.15.46   -> 192.168.15.40  : GigabitEthernet0/1.332 (next hop 192.168.15.45)
vpn1-2851-1#show ip route 192.168.15.40
Routing entry for 192.168.15.40/32
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 192.168.15.45
      Route metric is 0, traffic share count is 1

vpn1-2851-1#show run | inclued ip route
…
ip route 192.168.15.40 255.255.255.255 192.168.15.45 name vpn-jk2-7206-1_Loopbac k_0
```

Examine Interface QoS Service Policy

```
vpn1-2851-1#show run int GigabitEthernet0/1.332
!
interface GigabitEthernet0/1.332
 encapsulation dot1Q 332
 ip address 192.168.15.46 255.255.255.252
 service-policy output PER_CLASS_SHAPING
end
```

```
policy-map PER_CLASS_SHAPING
 class REAL_TIME
  set cos 5
    police 40000000 conform-action transmit  exceed-action transmit
 class GOLD
  shape average 2500000
  set cos 6
 class BRONZE
  shape average 2500000
  set cos 1
 class class-default
  set cos 0
  shape average 5000000
```

Verify Physical Interface

```
vpn1-2851-1#show interface GigabitEthernet0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is MV96340 Ethernet, address is 0015.627f.ae11 (bia 0015.627f.ae11)
  Description: Outside
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is T
  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 2w1d
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 17771
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 130000 bits/sec, 129 packets/sec
  30 second output rate 2500000 bits/sec, 219 packets/sec
     97309142 packets input, 3233588385 bytes, 0 no buffer
     Received 15768139 broadcasts, 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
     153379000 packets output, 2157098764 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
```

```
vpn1-2851-1#show policy-map interface GigabitEthernet0/1.332
 GigabitEthernet0/1.332

  Service-policy output: PER_CLASS_SHAPING

    Class-map: REAL_TIME (match-any)
      13210351 packets, 17257679558 bytes
      30 second offered rate 0 bps, drop rate 0 bps
...
   Class-map: GOLD (match-any)
     592255 packets, 64934600 bytes
     30 second offered rate 0 bps, drop rate 0 bps
...

    Class-map: BRONZE (match-any)
      138605017 packets, 199560741994 bytes
      30 second offered rate 2498000 bps, drop rate 0 bps
      Match: ip dscp af11 (10) af12 (12) af13 (14)
        138604907 packets, 199560729894 bytes
        30 second rate 2498000 bps
      Match: ip dscp cs1 (8)
        110 packets, 12100 bytes
        30 second rate 0 bps
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
          2500000/2500000   15000  60000     60000     24        7500

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        -      38        138587208 1967408200 138032050 1147442972 yes
      QoS Set
        cos 1
          Packets marked 138605017
  Class-map: class-default (match-any)
    10970 packets, 846954 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: any
```

```
vpn1-2851-1#show policy-map interface integrated-Service-Engine 1/0
 Integrated-Service-Engine1/0

  Service-policy input: INGRESS_VMSS

    Class-map: VSMS_BACKUP (match-any)
      138703648 packets, 190288370736 bytes
      30 second offered rate 2379000 bps, drop rate 0 bps
      Match: access-group name VSMS_BACKUP
        138703648 packets, 190288370736 bytes
        30 second rate 2379000 bps
      QoS Set
        dscp af11
          Packets marked 138703648

    Class-map: VMSS (match-any)
      13210371 packets, 16410427050 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: access-group name HTTP
        13210371 packets, 16410427050 bytes
        30 second rate 0 bps
      QoS Set
        dscp cs5
          Packets marked 13210371

    Class-map: class-
      1006321 packets
      30 second offere
      Match: any
      QoS Set
        dscp cs3
          Packets marked 1006321
```

```
vpn1-2851-1#show access-lists VSMS_BACKUP
Extended IP access list VSMS_BACKUP
    10 permit tcp any host 192.0.2.137 eq www (166129091 matches)
```

Verify from CPE Switch for SP

```
vpn1-2851-1#show cdp neighbors gigabitEthernet 0/1
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
vpn2-3750-access Gig 0/1           167          S I      WS-C3750G Gig 1/0/23
```

```
vpn2-3750-access#show int g1/0/23 | inc rate|errors
  Queueing strategy: fifo
  1 minute input rate 2494000 bits/sec, 221 packets/sec
  1 minute output rate 152000 bits/sec, 162 packets/sec
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 output errors, 0 collisions, 0 interface resets
```

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

Round Trip Time (RTT) for      Index 92
        Latest RTT: 4 milliseconds
Latest operation start time: 16:04:54.69
Latest operation return code: OK
Number of successes: 41
Number of failures: 0
Operation time to live: Forever


vpn-jk3-2651xm-9#show ip sla stat 210

Round Trip Time (RTT) for      Index 21
        Latest RTT: 21 milliseconds
Latest operation start time: 10:27:48.53
Latest operation return code: OK
Latest DNS RTT: 0 ms
Latest TCP Connection RTT: 8 ms
Latest HTTP Transaction RTT: 13 ms
Number of successes: 12
Number of failures: 0
Operation time to live: 0
```

```
vpn-jk3-2651xm-9#show run | beg ip sla 92
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 2101
 http get http://192.0.2.1
 tos 96
 timeout 200
 tag Router_Site130_HTTP
 frequency 300
ip sla schedule 2101 life 86400 start-time now
```

Key Items

- In this case, the network was functioning *as designed*
- QoS Policy matching backup traffic and setting DSCP to AF11
- Output QoS policy shaping traffic on a per-class basis – which is per the Service Provider MAN contract.
- Consider the BE needed to archive versus the BW available to backup – in this case backups running ½ the time
- Troubleshooting tips:
  - Don't assume anything
  - Verify the network paths
  - Review the current configuration
  - Use all the tools available (eg. IP SLA probes)