TOMORROW starts here.
Network Design and Implementation for IP Video Surveillance

BRKEVT-2311

Lionel Hunt TME
Abstract

BRKEVT-2311 - Network Design and Implementation for IP Video Surveillance

This session discusses the fundamentals of deploying IP video surveillance. It provides a foundation on selecting the type of IP cameras, the placement, field of view, resolution and frame rate to address the safety and security requirements of the organization.

The network characteristics of IP video surveillance and the demands video encoding, resolution, image quality, and frames per second for both standard and high definition IP cameras place on the network.

It details industry best practices to design a network to support video surveillance in the LAN/WAN and how IP video surveillance is integrated into an enterprise Quality of Service (QoS) model. The session reviews what network services are required for a successful deployment.

The session discusses what tools and resources are available to conduct a network readiness assessment and includes customer case studies and remediation steps to address common deployment issues.

This session is an intermediate level session. A basic understanding of video surveillance and is helpful, but not required. Familiarity with the basics of IP internetworking technologies is recommended. It is targeted for participants considering or implementing IP Video Surveillance.
Agenda

- Fundamentals of IP Video Surveillance
- Network Characteristics
- Network Design Considerations
- Network Services and QoS
- Network Readiness Assessment
- Case Studies
- Summary
Fundamentals of IP Video Surveillance
Fundamentals of IP Video Surveillance

Business Objectives

- Traditionally realm of loss prevention, regulatory compliance
- Cameras are a crime deterrent tool but so much more too
- Extend manpower significantly – direct emergency responders
- Monitor Patients
- Successful implementations require planning, proper assessment and deployment, monitoring, staffing, education and training.
- Cameras are a Marketing tool

Moving video to the corporate IP network allows the adoption of risk mitigation strategies across all aspects of the business.
Barriers to Success

- In the past, the physical security manager and the network manager had little interaction.
- The physical security manager is incurring risk by migrating from analog based systems to IP based systems.
- Value Added Resellers (VARs) are generally not (yet!) experts in IP networking.
- Key elements of video surveillance—the 3 ‘R’s Resolution, Retention and Reliability.
Project Management

Key to successful deployments

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

• Resources available to plan and install effective surveillance systems

• Schools and Large Retail often have Extranets with local law enforcement and share video feeds

• Some markets have large installed base of analog systems

• Britain estimated to have 4.2 million surveillance cameras — one for every 14 people[*]

• Other markets have high growth potential

• University ‘x’ has 4,700 students, 75-100 buildings with 232 cameras in total.

• China estimated to have one for every 472,000 people.


Best Practices
Not every issue is network related

- Avoid backlit scenes
- Obstructed camera field of view
- Avoid glare from glass windows
- Image must be in focus! Focal plane / depth of field - hallways
- Many deployments are forensic only – is video actually being written to disk?
- Is there a sufficient number and type of cameras?
Glare / Reflection from window
Example of poor camera placement

- Move camera closer to glass to reduce reflections
Documentation

Physical Layout and Network Inventory

- Physical layout - Camera Placement
- Location and Distances to wiring closets
- Document cable runs
  - Twisted Pair
  - Fiber
- Inventory / assess network equipment
- Power Requirements (PoE)

http://www.jvsg.com/
Obstructed Field of View

Example of poor camera placement

- Reposition camera for unobstructed view of court
Camera Placement—Overview or Detail Influences codec, Frame Rate, Resolution

Overview
- Traffic cameras—viewing congestion
- Parking lots
- Single Megapixel or multiple SD cameras
- Wide angle lens

Detail View
- Point of sale transactions
- Face or license plate recognition
- Megapixel (HD) cameras
- Zoom lens
- Camera close to subject

www.wral.com/traffic/traffic_cams/
Detection and Identification - Large venues

- Detail view and overview cameras working together
Video Surveillance in some markets (public schools, higher education) is mainly for forensic – no live viewing, aka headless

Use of PTZ in these markets not ideal deployment – camera is typically facing the wrong direction!

Surveillance operators in gaming use PTZ for more pixels on target – ATM machines, table transactions

Advanced PTZ use detection and multiple presets

Monitor area for movement, then zoom to preset and return to home position to again monitor
High Definition vs. Megapixel

- HD video is megapixel video (1920x1080 = 1.9m pixel count)
- Megapixel is not HDTV – HDTV must meet these requirements
  - Aspect Ratio - 16:9
  - Minimum 25/30 frames per second (fps)
  - Resolution (1280 x 720 or 1920 x 1080)
  - Color Rendering / Standard
- Megapixel cameras commercially available at 29 megapixel (6576 x 4384) at 2 images per second - Lossless JPEG2000 compression
### Typical Resolutions

User Expectation of Image Quality is Increasing with Adoption of HDTV

<table>
<thead>
<tr>
<th>Size / Format</th>
<th>NTSC based</th>
<th>PAL based</th>
<th>Size / Format</th>
<th>Pixels</th>
</tr>
</thead>
<tbody>
<tr>
<td>QCIF</td>
<td>176 x 120</td>
<td>176 x 144</td>
<td>3M</td>
<td>2048 x 1536</td>
</tr>
<tr>
<td>CIF</td>
<td>352 x 240</td>
<td>352 x 288</td>
<td>HDTV</td>
<td>1920 x 1080</td>
</tr>
<tr>
<td>2CIF</td>
<td>704 x 240</td>
<td>704 x 288</td>
<td>2M</td>
<td>1600 x 1200</td>
</tr>
<tr>
<td>4CIF</td>
<td>704 x 480</td>
<td>704 x 576</td>
<td>1M</td>
<td>1280 x 1024</td>
</tr>
<tr>
<td>SD</td>
<td>720 x 480</td>
<td>720 x 576</td>
<td>1M</td>
<td>1280 x 960</td>
</tr>
<tr>
<td>D1</td>
<td>720 x 480</td>
<td>720 x 576</td>
<td>HDTV</td>
<td>1280 x 720</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>VGA</td>
<td>640 x 480</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>QVGA</td>
<td>320 x 240</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>QQVGA</td>
<td>160 x 120</td>
</tr>
</tbody>
</table>

Megapixel camera in MJPEG may be 4CIF resolution for MPEG-4

HD cameras in H.264 may be 4CIF for MJPEG

Read the Data Sheets!
Pixel per foot (ppf) requirements

- **Identification**
  - General 60
  - Face recognition 80-150
  - License plates 125 ppf

- **Recognition** – 40

- **Detection** – 20

- **Overview** - 10

Given a 7’ high doorway—resolution of 1050 pixels at 150 pixels per foot
Resolution and Aspect Ratio
IP Cameras More Optimal Than Analog

Wider Aspect Ratio – SD 4:3 while HD is 16:9

Axis’ Corridor Format monitoring aisles, hallways.
New installations - Should I deploy SD or HD?

<table>
<thead>
<tr>
<th>Cost Factor</th>
<th>Standard Definition</th>
<th>High Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation</td>
<td>No difference</td>
<td></td>
</tr>
<tr>
<td>Access Switch</td>
<td>No difference</td>
<td></td>
</tr>
<tr>
<td>Upgrade to HD</td>
<td>Install + camera</td>
<td></td>
</tr>
<tr>
<td>Camera and Lens Costs (MSRP)</td>
<td>~$1400</td>
<td>~$1700</td>
</tr>
<tr>
<td>Power (PoE) Consumption</td>
<td>5.28 Watts</td>
<td>6.2 Watts</td>
</tr>
<tr>
<td>Viewing station</td>
<td>Higher</td>
<td></td>
</tr>
<tr>
<td>Viewing station Requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server /Storage Req.</td>
<td></td>
<td>30% – 300% Higher</td>
</tr>
<tr>
<td>Average BW (CBR at 30fps)</td>
<td>&lt;= 2 Mbps</td>
<td>&gt;= 4 Mbps</td>
</tr>
</tbody>
</table>

**HD cameras can be deployed initially at SD (D1, 4CIF, CIF) resolutions**
Television has changed the perception of video surveillance.

By 2015 - 60% cameras sold are HD / megapixel

- Users want High Definition resolutions
- Expect Unlimited digital zoom
- Immediate forensic search results
- Project manager must manage user expectations
- Educate user on all aspects of system capabilities


CSI publicity photo/fair use
Key Points

- Implementations issues stem from variety of factors – technical issues are easiest to address
- Proper planning and project management key to success
- Proper documentation, floor plans, network assessment critical
- User expectations have increased making High Definition video a baseline requirement
Network Characteristics
Video Attributes Affecting Network Load

- Resolution (configurable)
- Encoder Implementation and CPU (fixed)
- Quality Factor (configurable)
- Frame Rate (configurable)
- Picture Complexity (some influence)
- Motion (some influence)

The number of IP packets per video frame (reference frame) is proportional to resolution.
Video Surveillance Acronyms

- **Cisco Video Surveillance Manager**

  - **VSMS**: Video Surveillance Media Server. Cisco term for a Network DVR. Manages IP camera video feeds and storage media.

  - **VSOM**: Video Surveillance Operations Manager. Provides a Web based interface for operator and administrator for configuration and management of the VSMS and endpoints.

  - **Viewing Station**: High-end Intel workstation for displaying live or archived camera feeds. Windows Windows 7 64Bit – Internet Explorer

- **Video Codecs**

  - M-JPEG: Motion – Joint Photographic Experts Group
  - MPEG-4: ISO/IEC Moving Picture Experts Group (Part 2)
  - JPEG 2000: Joint Photographic Experts Group (committee 2000)

- **Video Signaling and Transport Protocols**

  - HTTP: Hyper Text Transport Protocol
  - HTTPS: Secure HTTP
  - RTSP: Real Time Streaming Protocol
  - RTP: Real-time Transport Protocol
  - RTCP: Real Time Transport Control Protocol
Network Data Flows - Transport Layer Protocols

Media Servers maintain TCP session to Camera port 554 (RTSP)
Keepalive sent every 6 seconds
Bandwidth

- Media streams (data plane) consume the majority of bandwidth

- Media Servers proxy video for viewing

- Don’t archive packet loss!

- Decoder (viewing station) can also be the cause of poor video quality

Data Flows - MPEG-4 / H.264 with UDP Transport
### IP Cameras

#### Network Bandwidth and Disk Storage Estimates

<table>
<thead>
<tr>
<th>Camera</th>
<th>CODEC</th>
<th>Resolution</th>
<th>Frame Rate (fps)</th>
<th>Average Load Mbps</th>
<th>Disk Storage in Megabytes per 5 min of archive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 3k Series (SD)</td>
<td>MPEG-4</td>
<td>D1 (720x480)</td>
<td>15 / 30</td>
<td>1 / 2</td>
<td>35 / 76</td>
</tr>
<tr>
<td></td>
<td>MJPEG</td>
<td>D1 (720x480)</td>
<td>5 / 10</td>
<td>2.2 / 4.4</td>
<td>75 - 150</td>
</tr>
<tr>
<td>Cisco 4k/6k series HD</td>
<td>H.264</td>
<td>HD (1920x1080)</td>
<td>30</td>
<td>4 - 6</td>
<td>100 - 240</td>
</tr>
</tbody>
</table>

---

**TCP (control plane)**
- MJPEG TCP (data plane)
- MPEG-4 / H.264
- UDP/RTP (data plane)
# Video Surveillance Application Requirements

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latency (UDP/RTP Transport)</td>
<td>150ms one-way values or more may be acceptable if no two-way communication such as PTZ are required</td>
</tr>
<tr>
<td>Latency (TCP Transport SD)</td>
<td>Less than 80msRTT</td>
</tr>
<tr>
<td>Latency (TCP Transport HD 6MCR)</td>
<td>Less than 30msRTT</td>
</tr>
<tr>
<td>Loss (Standard Definition MPEG-4/H.264)</td>
<td>Less than .5% (1/2 of one percent)</td>
</tr>
<tr>
<td>Loss (High Definition MPEG 4/H.264)</td>
<td>Less than 0.05% (1/20th of one percent)</td>
</tr>
<tr>
<td>Jitter</td>
<td>Less than 10% of one-way latency</td>
</tr>
</tbody>
</table>
Quality of Experience
As resolution increases, drop threshold decreases

- IP packets transporting video frames are packed very close together
- Network drops are not uniformly distributed – when buffers fill, packets are tail dropped - all at once!

* Random Early Detection (RED) influences this behavior

Given 300 IP packets per i-frame - one percent loss means every i-frame is impacted
Packet Loss
*Introduced at .1% to .03%*

1080p / H.264 / 30 fps - 4MCBR (appx 380 pps)
Drop configured for 1 packet every 1000 to 3000 IP packets
Latency Video Surveillance Manager

- Depends on the transport protocol
- MPEG4 / H.264 transported in TCP is not tolerant of high latency
- MPEG4 / H.264 in UDP/RTP tolerant of high latency
- Network is only one component of the total latency budget
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
Characteristics of MPEG-4 / H.264 Video Frames

- Periodic resynchronization—complete image sent as reference: *aka* key frame, (I-frame)
- Predicted frames (P/B) built upon reference frame – changes transmitted
- Typically encapsulated in UDP/RTP—connectionless!
- As image size and complexity increases, so does the number of IP packets necessary to transport frame
- Reference frames 30-300 IP packets
- Predicted frames *may* be a single IP packet—usually one or more
- Average packet >1,000 bytes
- RTP header has a packet sequence number—loss detection
- Packet loss *will* degrade image appearance
Encoder Terminology

Frame Types
- I Frames: Fully Reference Frame, Time independent
- P Frames: Predicted Picture, progression since last frame
- B Frames: Bi-predictive picture,

Data compression over time
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) 70-300 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)*
Frequency of I-frames
Group of Pictures (GOP) / Group of Video (GOV)

1,000 ms = 1 second
Variable Bit Rate vs. Constant Bit Rate

- Variable Bit Rate (VBR)
  - Pre-defined image quality (low normal high very-high)
  - Scene complexity and motion will influence bandwidth consumption
  - More difficult to provision / estimate network bandwidth

- Constant Bit Rate (CBR)
  - Bandwidth consumption is deterministic (over seconds)
  - Either image quality and/or frame rate may change
  - Average bandwidth consumption can be estimated
  - Network traffic is still bursty – due to I-frame transmission
  - Image quality may be noticeably degraded – see next slide
In this example, the resolution size is fixed at 1920x1080, the encoder changed the quantization, lowering the quality of a portion of the screen to meet the bandwidth target (4Mbps CBR).
VBR – Variable Bit Rate

Storage reduction – static scenes

- MPEG-4 - 4CIF – Quality 80% - 15 fps
### H.264 Encoder Comparisons

**CPU Load increases with higher temporal compression**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Video Surveillance 4500E</th>
<th>TelePresence</th>
<th>GO Pro Hero Naked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Load</td>
<td>1080p ~ 4-6 Mbps at 30fps</td>
<td>1080p ~ 4 Mbps per camera (*)</td>
<td>15 Mbps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>720p Lite &lt;2 Mbps</td>
<td></td>
</tr>
<tr>
<td>Resolution / frame rate</td>
<td>1080p or 720p / 30 (or lower)</td>
<td>1080p or 720p / 30</td>
<td>1080p / 30</td>
</tr>
<tr>
<td>MSRP</td>
<td>$1,805 (w/ lens)</td>
<td>CTS-500 $33,900</td>
<td>$129</td>
</tr>
</tbody>
</table>

**WAN Friendly** - Low Scene Complexity due to lighting, background, limited movement - Quality and VoIP/UC integration (*) CTS-3000 about 15.3 Mbps

**Price / Quality** - Battery life

**Price - Quality – Frame rate - Power draw (PoE)**
IP Video Surveillance
Primary Compression codecs—Motion JPEG

- MJPEG (Motion JPEG)
- Transport Protocol
  - Typically TCP protocol—HTTP port 80/443
  - Cisco cameras - TCP 554 (RTSP interleaved frames) RFC 2326 section 10.12
    - control and data same session
- Compresses every frame and streams the data
- Image quality is not compromised by loss / latency – frame loss makes video ‘jumpy’.
- For given resolution requires twice the bandwidth for ¼ frame rate than MPEG-4 / H.264
- JPEG2000 used for multi-megapixel (11-16) at 3-5 fps
Motion JPEG
Every frame is a reference frame

Resolution 1280 x 720
Axis 207MW Motion JPEG
7 fps – Quality 50

Camera to Media Server

1 second per tick

1/100th sec (10ms) per tick
Deployment scenario
Motion JPEG

- Bandwidth constrained environments
- High latency / loss networks
- Standard Definition resolution at low frame rate

Latency 800-1000 ms
Bandwidth 256-512K
1/10th frame per second
1 frame every 10 seconds
Alarms / Events

- IP Cameras initiate control plane traffic
  - Video Analytics – Event counting, abandoned object, etc
  - Anti-spray alert (open cover, spray paint or movement)
  - Motion Detection – movement / lighting changes within window(s)

- Domes/enclosures limit tampering at the camera
  - Domes commonly stolen, camera field of view re-positioned

- Alarms generated by camera to management software or NMS host
  - FTP, SMTP, TCP session to configured port for notification
Key Points

- Bandwidth requirements based on average data rates but also to accommodate i-frame bursts
- Latency requirements transport protocol dependant
- Network latency is only one component of the total latency budget
- Poor video quality is likely due to network packet loss or video frames arriving too late
- Video feeds may be transported in TCP or UDP and either MJPEG or MPEG-4 / H.264 depending on camera model and manufacture
Network Design Considerations
<table>
<thead>
<tr>
<th>Physical Security LAN / WAN Deployment Models</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical Isolation</strong></td>
</tr>
<tr>
<td>Market: Gaming and single building deployment - smaller deployments may be all Layer-2 - may need to redesign as network grows</td>
</tr>
<tr>
<td><strong>Converged Network</strong></td>
</tr>
<tr>
<td>Market: Public Schools – Typically 2 tier – Layer-2 - VoIP and Data – QoS may be inadequately implemented – MetroE or dark fiber between buildings.</td>
</tr>
<tr>
<td><strong>Virtualization, Isolation and Encryption of Converged Facilities</strong></td>
</tr>
<tr>
<td>Market: Enterprise – with large geography WAN – not currently a target customer for PHYSEC – Complexity may retard adoption</td>
</tr>
</tbody>
</table>
General Considerations
**Speeds and Feeds**

Design Speed Mismatches as we Aggregate

- **IP Cameras**
  - FastEthernet - FDX
  - IEEE 802.3af—PoE

- **Viewing Stations**
  - Gigabit Ethernet

- **Servers**
  - Gigabit Ethernet

- **IP Cameras**
  - Fast Ethernet - FDX
  - Gigabit Ethernet
  - 10 Gigabit Ethernet
  - Gigabit Ethernet
  - 10 Gigabit Ethernet
  - Gigabit Ethernet
  - Gigabit Ethernet
  - Gigabit Ethernet
  - Fast Ethernet
  - Gigabit Ethernet

---

<table>
<thead>
<tr>
<th>Video Stream Bit Rate</th>
<th>Number of Camera Streams per VM</th>
<th>Number of VMs per Blade</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Mbps</td>
<td>250</td>
<td>4</td>
</tr>
<tr>
<td>2 Mbps</td>
<td>130</td>
<td>4</td>
</tr>
<tr>
<td>4 Mbps</td>
<td>66</td>
<td>4</td>
</tr>
</tbody>
</table>

---
Three Tier Model

Needed when size and distance increases

- Core: 4500-E
- Distribution: 4500-E
- Access: 3750X-48PS, 3750X-48PD

- Core: 2 - 10G, 24 - 10/100/1000
- Distribution: 2 - 10G, 24 - 10/100 PoE, 6 - 10G, 24 - 1G
- Access: 10Gig, 1 Gig, 10/100 PoE
Two Tier Model
Co-located Core and Distribution Layer

Typically deployed where the organization occupies a single building

Multiple IDFs to address cable distance limitations
# Access to Distribution Layer Uplink Options

<table>
<thead>
<tr>
<th>Layer-2</th>
<th>Logical Layer-2</th>
<th>Layer-3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Load Sharing</strong></td>
<td><strong>None</strong> forwarding or blocking</td>
<td><strong>Ether Channel</strong> port-channel load-balance</td>
</tr>
<tr>
<td><strong>Control Plane</strong></td>
<td><strong>Spanning Tree plus proprietary extensions - eg. UplinkFast</strong></td>
<td><strong>8 physical links per Port-channel</strong> maximum-paths default 4, up to 6</td>
</tr>
<tr>
<td><strong>Chassis Limits</strong> 4, 1 Gig or 2, 10 Gig Uplinks</td>
<td><strong>Routing Protocol</strong> EIGRP - OSPF</td>
<td><strong>Sub-second L1/L2 3-5 seconds L3</strong></td>
</tr>
</tbody>
</table>

- Default configuration ~ 40 seconds (*)
- **UplinkFast** Sub-second
Frequency of I-frames
How quickly must the network converge?

1,000 ms = 1 second

packet loss

Clearing I-frame resolves packet loss
H.264 – 1080p – 30 fps – 4Mbps CBR

Drop one packet every 1500 to 3000 IP packets -- average .04% loss
Access to Distribution Layer
Uplink Options

- Routed Access layer – all links can forward traffic

Interface | Role | Sts | Cost | Prio.Nbr | Type  
----------|------|-----|------|----------|-------
Po1       | Root | FWD | 4    | 128.1    | P2p   
Po2AltnBLK | 4    |     | 128.27|          | P2p   

EIGRP learned routes

D 10.40.1.0/26 [90/3328]
   via 10.40.248.45, 6d03h, GigabitEthernet0/52
   [90/3328] via 10.40.248.43, 6d03h, GigabitEthernet0/51
   [90/3328] via 10.40.248.41, 6d03h, GigabitEthernet0/50
   [90/3328] via 10.40.248.39, 6d03h, GigabitEthernet0/49
Failed Primary Link – the SD camera lost 27 packets out of 190 pps

me-westipvs-2#
Jan 25 14:06:40.423 est: %SPANTREE_FAST-7-PORT_FWD_UPLINK: VLAN0066GigabitEthernet0/3 moved to Forwarding (UplinkFast).
Jan 25 14:06:41.429 est: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

Media Server ims.log

2011-01-25 14:06:40.431 [ proxy(3770).p_s1_me-westvsms-8_me-c523_1GL_UTIL=1 <Mpeg4Parser.cxx:1147> ] ERROR: missed 27 RTP packet(s) [prev=34285, curr=34313]
Routed Access Layer

- Fault detection primarily through L1/L2 remote fault detection
- EIGRP hello and hold times can be tuned lower also – 3 second hold time and 1 second hello
- Test case will fail physical link
  - Administratively shut link
  - Physically remove fiber cable
- Less than 1 second video lost

```!
interface GigabitEthernet2/1
description vpn7-3560g-1
no switchport
dampening
ip address 10.40.248.3 255.255.255.254
ip hello-interval eigrp 64 1
ip hold-time eigrp 64 3
carrier-delay msec 0
end
```
Routed Access Layer

- View media server ims.log file for packet loss
- Administratively shutting down interface on 4506
  - Disconnecting cable from switch port on 4506

```plaintext
[ proxy(3819).p_s1_dome-cam-3_1 GL_UTIL=1 <H264Parser.cxx:2087> ] ERROR: missed 136 RTP packet(s)
[ proxy(3822).p_s1_dome-cam-4_1 GL_UTIL=1 <H264Parser.cxx:2087> ] ERROR: missed 186 RTP packet(s)
  - Disconnecting cable from switch port on 4506

[ proxy(3819).p_s1_dome-cam-3_1 GL_UTIL=1 <H264Parser.cxx:2087> ] ERROR: missed 159 RTP packet(s)
[ proxy(3822).p_s1_dome-cam-4_1 GL_UTIL=1 <H264Parser.cxx:2087> ] ERROR: missed 129 RTP packet(s)
```

```
vpn7-3560g-1#show interfaces g0/3 | include rate |Desc

Description: 5000 Series HD IP Dome Cameras
1 minute input rate 4893000 bits/sec, 468 packets/sec
1 minute output rate 0 bits/sec, 0 packets/sec
```

Less than ½ second video lost – no failure on recovery
Why Segment IPVS traffic?

- Minimize exposure to security flaws, worms, viruses for video endpoints
- Need to know – access to video feeds typically limited to small population of users
- IPVS, Facilities Management (heat, light power) and Access Control may share same segments
- Outages to these systems may incur fines, safety issues or penalties by regulating authorities
Means of Achieving Virtualization

- **Policy-based Network Virtualization**
  - Restricts the forwarding of traffic to a specific destination
  - Rule based, an administrative policy.
  - Independent of the control plane – destination is reachable, but administratively prohibited.
  - Example: Access Control Lists, Firewalls

- **Control plane-based network virtualization**
  - Restricts the propagation of routing information
  - Routing Tables are Virtualized
  - IP Networks are segregated by their respective virtual routing table VRF
  - Example: VPN Routing and Forwarding (VRF)

Typically both methods are implemented as synergist approach to the network design
Cisco IP Cameras
Policy Based Features

- HTTPs
  - Secure HTTP to protect from eavesdroppers and other attacks

- IP address filtering
  - Use IP address filtering to either allow or deny access to a Cisco IP camera from specific IP addresses

- User access rights
  - The camera administrator can create up to 20 roles and configure rights for each user
  - User types: administrator, root, user
Segmentation - *Layer-2 with policy-based Layer-3*

hostname vpn7-3560e-1

interface GigabitEthernet0/1
description CameraQ1755
switchport access vlan 128
mls qos trust dscp
spanning-tree portfast
spanning-tree bpdudfilter enable

interface GigabitEthernet0/2
switchport access vlan 2

interface Vlan2
description IDFA.4 - DATA VLAN
ip address 10.40.33.193 255.255.255.192

interface Vlan128
description IDFA.4 - FACILITY-MANAGEMENT
ip address 10.40.0.193 255.255.255.192
ip access-group FACILITY_MANAGEMENT_in in

ip access-list extended FACILITY_MANAGEMENT_in
permit udp any eq ntp any eq ntp
permit udp any eq snmp any
permit udp any eq domain any
permit ip 10.40.0.0 0.0.7.255 any
IP Multicast (IPmc)
Redundant archives for disaster recovery

- Define same IP camera two media servers using IPmc transport
- Archives defined to both VSMS
- Both live feeds/archives viewable thru VSOM
- Other clients may join IPmc group as well
- Can Also be Achieved in VSM7 with Dual Streaming
Embedded Medianet Capabilities
Auto-configuration—simplifying deployment

**Without Medianet**
- Multiple skillsets actively needed for every new camera deployed (networking plus security)
- Manual and error prone process

**With Medianet**
- Auto-Discovery, and Auto-Configuration with the network
- Faster, simplified deployment Reduce 10s of minute to 10s of seconds
Two key medianet features:

Automatically identifies IP Cameras and flows
Automatically assigns network services
Auto configuration

Medianet Service Interface (MSI)

- Intent to ease administrative burden
- Catalyst switch detects medianet device
- FCAPS – configuration mgmt
  - Auto smart port
  - Civic location

Detection –
- Cisco Discovery Protocol (CDP)
- Link-Level Discovery Protocol (LLDP)
- MAC address vendor code

- Not all Cisco camera series support CDP

Key Points

- Network topology must address bandwidth required by IP video surveillance
- Be sufficiently modular to grow without redesign
- Have sufficient redundancy to provide high availability
- Not be overly complicated or difficult to manage
- Ensure video feed is not compromised / disrupted
Network Services and QoS
Transport Services
Quality of Service—Optimization

- Video Surveillance is only one type of video on the network; also TelePresence, Digital Media, Collaboration, Enterprise TV

- Network load of video much higher than VoIP and data

- QoS classification (marking) done by end-stations, routers and switches

- Improperly implemented, QoS can have a detrimental effect on network traffic
# Cisco medianet Application Classes

## DiffServ QoS Recommendations (RFC 4594-Based)

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

Cisco Camera CIVS-IPC-4500
Ingress Marking
Servers and Workstations

class-map match-all HTTP_acl
match access-group name HTTP
!
policy-map VSMS
  class HTTP_acl
  set dscp cs5
  class class-default
  set dscp cs3
  !
ip access-list extended HTTP
permit tcp any eq www any
!
interface GigabitEthernet1/0/4
  description
  switchport access vlan 220
  switchport mode access
  priority-queue out
  spanning-tree portfast
  spanning-tree bpdufilter enable
  service-policy input VSMS

BRKEVT-2311  © 2013 Cisco and/or its affiliates. All rights reserved.
Ingress Marking
Servers and Workstations

class-map match-all HTTP_acl_client
match access-group name HTTP_client
!
policy-map Viewing_Station
class HTTP_acl_client
set dscp cs5
class class-default
set dscp cs3
!
ip access-list extended HTTP_client
permit tcp any any eq www
!
interface GigabitEthernet1/0/5
description Viewing Station
switchport access vlan 208
switchport mode access
priority-queue out
spanning-tree portfast
spanning-tree bpdufilter enable
service-policy input Viewing_Station
Trust DSCP and Ingress / Egress Queuing
IP Cameras and trunks

- CS5 by default in Ingress-PQ

```plaintext
interface GigabitEthernet1/0/11
description CIVS-IPC-4500-2
switchport access vlan 220
switchport mode access
switchport port-security
switchport port-security mac-address sticky
mls qos trust dscp
spanning-tree portfast
spanning-tree bpdufilter enable

interface GigabitEthernet1/0/1
description trunk to vpn1-2851-1
switchport trunk encapsulation dot1q
switchport mode trunk
priority-queue out
mls qos trust dscp
```

CS5 by default in Egress priority queue (PQ)
IP Cameras TCP/IP stack setting DSCP - switch trusts the DSCP markings
IP Network Services for Video Surveillance

Advantages over Analog Systems

- IP network—access to video feeds, any time from any place
- Video transport over redundant and reliable IP infrastructure
- Leverage existing network management services
  - HTTP/web-based configuration management
  - Dynamic Host Configuration Protocol (DHCP)
  - Cisco Discovery Protocol (CDP)
  - Power over Ethernet (PoE)
  - Simple Network Management Protocol (SNMP)
  - Syslog protocol
  - Network Time Protocol (NTP)
Most IP cameras default to DHCP, then fixed IP address.
Site installer mounts/focus camera via local LAN attachment.
Central site technician configures via IP network.
Advanced Setup—Cisco IP Cameras
Cisco Discovery Protocol (CDP) Enabled by Default

Device ID: 00:1E:BD:FC:19:86
Entry address(es):
   - IP address: 10.194.31.35
   - IPv6 address: FE80::200:FF:FE00:0 (link-local)
Platform: CIVS-IPC-4500, Capabilities: Host
Interface: FastEthernet0/5, Port ID (outgoing port): br0
Holdtime: 129 sec

Version:
2.4.0-271

advertisement version: 2
Duplex: full
Management address(es):
### Power over Ethernet

**CCTV analog usually 24 VAC 3.5 AMP**

- Most IP cameras require IEEE 802.3af standard PoE
- Distance is 100 meters, same as Fast Ethernet
- Devices which support CDP can lower the power level

```text
<table>
<thead>
<tr>
<th>Module</th>
<th>Available (Watts)</th>
<th>Used (Watts)</th>
<th>Remaining (Watts)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>370.0</td>
<td>111.4</td>
<td>258.6</td>
</tr>
</tbody>
</table>
```

```text
<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin</th>
<th>Oper</th>
<th>Power (Watts)</th>
<th>Device</th>
<th>Class</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>auto</td>
<td>off</td>
<td>0.0</td>
<td>n/a</td>
<td>n/a</td>
<td>15.4</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>auto</td>
<td>off</td>
<td>0.0</td>
<td>n/a</td>
<td>n/a</td>
<td>15.4</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>auto</td>
<td>on</td>
<td>13.0</td>
<td><strong>CIVS-IPC-4300</strong></td>
<td>3</td>
<td>15.4</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>auto</td>
<td>on</td>
<td>13.0</td>
<td><strong>CIVS-IPC-4300</strong></td>
<td>3</td>
<td>15.4</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>auto</td>
<td>off</td>
<td>0.0</td>
<td>n/a</td>
<td>n/a</td>
<td>15.4</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>auto</td>
<td>on</td>
<td>9.0</td>
<td><strong>CIVS-IPC-2500</strong></td>
<td>3</td>
<td>15.4</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>auto</td>
<td>on</td>
<td>15.4</td>
<td>IEEE PD</td>
<td>3</td>
<td>15.4</td>
</tr>
</tbody>
</table>
```

```
vpn2-3750-access#show interfaces gi1/0/7 |
inc Desc
Description: **Linksys PVC2300-F49I**
```
Network Time Protocol (NTP)

- Synchronizes camera clocks to common time source
- Local time displayed on video image by IP camera
- Timestamps may be compared across cameras
Cisco routers send syslog messages to their logging server with a default facility of ‘local7’

Cisco IP cameras use facility of ‘user’

To include messages of level ‘debug’ and above

Restart your syslog process

```
/etc/syslog.conf
#
local7.debug /var/adm/logs/cisco.log
user.debug /var/adm/logs/cisco.log
```

# kill -HUP `cat /etc/syslog.pid`


Key Points

- VoIP and Video equally important
- QoS policy must address requirements of Voice, Video and Data
- DSCP values set on both end-points and on network ingress
- IP cameras are Linux hosts on the network capable of DHCP, DNS, NTP, CDP, Syslog, HTTP – plan accordingly
Network Readiness Assessment
Is the network all that important?

*IP Video Transport requires a network that …*

- Has sufficient available **capacity** (bandwidth) to transport video
- Exhibits very low / **no loss** of IP video packets
- Network **latency** is within the range suitable for the transport protocol (eg. TCP/UDP) of the video feed
- Provides **high availability** – network redundancy
- Meets the **network security (and services) requirements**
Network Readiness Assessment for IP Video Surveillance

Reference guide of processes and information to be collected to conduct a thorough network assessment

Goal to insure a successful IP


Webinar

https://cisco.webex.com/ciscosales/lsr.php?AT=pb&SP=EC&rID=42300707&rKey=7d3276e94cf7fcdb
Raising Awareness
Assess the Network before Deploying Video


Is the Network Ready for Video?—Network Assessments

The surveillance industry is leveraging Internet Protocol (IP) networks as the foundation for new video surveillance deployments. While every major vendor is focused on delivering both standard and high-definition IP cameras, servers, and viewing workstations, the role of assessing the network infrastructure falls on the security integrator. Often, the success or failure of the installation, and the resulting perception of the capabilities of the integrator, is dependent on the capabilities of the network.

To support video on increasingly complex networks, Cisco is now offering new tools and resources to successfully deploy IP video surveillance.

**Figure 1**  Cisco Video Surveillance 5000 Series HD IP Dome Camera—H.264—1080p at 30 Frames per Second—4Mbps CBR—No Packet Loss
Capacity Analysis of Uplink(s)

Network Assessment versus Capacity Analysis

- 3560E w/ GigE and TenGig
- 47 High Def (4000 series)
- 8 HD - traffic generation
- GigE uplink sufficient

47 HD Cameras
(100 Mbps)
Average 6.8 Mbps per camera

me-westipvs-1#show int gigabitEthernet 0/49
30 second input rate 35554000 bits/sec, 3581 packets/sec
30 second output rate 374600000 bits/sec, 33327 packets/sec
Test objectives

- No reported loss from 55 HD
- Tool identified loss during reload
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!

```bash
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
```
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
IPSLA Video Operation – IPSLA VO
Emulates UDP/RTP traffic

- Pre-packaged traffic profiles
  - IPTV
  - TelePresence
  - IP Video Surveillance

- No Round Trip Time (RTT) traffic – one-way only

- Network Time Protocol (NTP) sync required

- Supported on Cisco devices capable of generating platform-assisted video traffic and reflection
  - 3750/3560 - 3750G/3560G - 3750X/3560X - 3750E (recommended)

- Cisco IOS 12.2(58)SE1
IP SLAs video operations support only one-way traffic

```
ip sla 264
  video 192.0.2.129 42266 source-ip 10.40.1.1 source-port 42266 profile IPVSC
duration 300
tag camera_to_commandcenter
frequency 600
!
ip sla group schedule 1 264,300 schedule-period 2
frequency 600 start-time now life 84200

ip sla 300
  udp-jitter 192.0.2.129 16384 source-ip 10.40.1.1 source-port 16384 codec g711alaw codec-numpackets 3000
tos 184
tag camera_to_commandcenter_VoIP
frequency 600```

For Your Reference
VPN7-3560G-1#show ip sla stat
IPSLA's latest operation statistics

IPSLA operation id: 264
Type of operation: video
Latest operation start time: 10:01:05 EDT Thu Jun 23 2011
Latest operation return code: OK
Packets:
  - Sender Transmitted: 90654
  - Responder Received: 90634
Latency one-way time:
  - Number of Latency one-way Samples: 90634
  - Source to Destination Latency one way Min/Avg/Max: 0/100/500 ms
  - NTP sync state: Sync
Inter Packet Delay Variation, RFC 5481 (IPDV):
  - Number of SD IPDV Samples: 90610
  - Source to Destination IPDV Min/Avg/Max: 0/6/123 milliseconds
Packet Loss Values:
  - Loss Source to Destination: 40436
  - Source to Destination Loss Periods Number: 0
  - Source to Destination Loss Period Length Min/Max: 0/0
  - Source to Destination Inter Loss Period Length Min/Max: 0/0
  - Out Of Sequence: 0 Tail Drop: 0
Number of successes: 2
Number of failures: 0
Operation time to live: 83072 sec
IPSLA Video Operation – IPSLA VO
Sample Output – UDP-jitter operation

IPSLA operation id: 300
Type of operation: udp-jitter
  Latest RTT: 84 milliseconds
Latest operation start time: 09:55:19 edt Thu Jun 23 2011
Latest operation return code: OK
RTT Values:
  Number Of RTT: 2603  RTT Min/Avg/Max: 1/84/372 milliseconds
Latency one-way time:
  Number of Latency one-way Samples: 2603
  Source to Destination Latency one way Min/Avg/Max: 1/82/370 milliseconds
  Destination to Source Latency one way Min/Avg/Max: 1/1/4 milliseconds
Jitter Time:
  Number of SD Jitter Samples: 2588
  Number of DS Jitter Samples: 2602
  Source to Destination Jitter Min/Avg/Max: 0/17/129 milliseconds
  Destination to Source Jitter Min/Avg/Max: 0/1/4 milliseconds
Packet Loss Values:
  Loss Source to Destination: 14
  Source to Destination Loss Periods Number: 50
  Source to Destination Loss Period Length Min/Max: 1/33
  Source to Destination Inter Loss Period Length Min/Max: 3/32
  Loss Destination to Source: 0
  Destination to Source Loss Periods Number: 0
  Destination to Source Loss Period Length Min/Max: 0/0
  Destination to Source Inter Loss Period Length Min/Max: 0/0
  Out Of Sequence: 0  Tail Drop: 89
  Packet Late Arrival: 0  Packet Skipped: 605

Voice Score Values:
  Calculated Planning Impairment Factor (ICPIF): 1
  MOS score: 4.34

The root cause of the problem is a QoS policy on the distribution switch shaping traffic to a 3.2Mbps rate toward the Media Servers!
Key Points

- Document Network
- 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
- Use IP SLA probes to measure network performance
Case Studies
Housekeeping

Which would you rather troubleshoot?
Location *The Rock*

Network upgrades not finished before video deployed

- Network assessment (VSAA) run to identify perceived video quality issues
- School had multiple video issues-
  - Camera Focus Issues
  - Bandwidth - CBR value too low for configured resolution (HD)
- Switch Chassis – legacy base mode 4500
- Access switch (2950) ‘discovered’ in network topology by tracing cables
- Need network upgrade and accurate topology diagrams
Unknown 2950 Switch in topology
Found by tracing cables!

Average Video Loss 0.242%
Maximum Video Loss 2.63%
Location *The Beach*
*Public school with VoIP and Data on MetroE*

- Assessment and *show tech* indicated packet loss in MAN network – approximately 5%
- Video quality perceived good by user
- Upon investigation – cameras configured as Motion JPEG (4CIF) 8 fps – archiving at 4 fps.
- MAN is Verizon Transparent LAN Service (*TLS*) – Network diagram indicates all locations at 100Mbps
- Unknown if QoS is deployed in MAN – Customer says VoIP preferred over Video

Motion JPEG will consume 2x the Bandwidth at ¼ the frame rate at 4CIF resolution than MPEG-4

Impairment is missing frames not video ‘quality’ issues
Loss
Consistent - approximately 5%

Discovered that Archive Backups running over MAN during assessment execution
What can be learned from this output?

**Capacity Issue on Metro Ethernet - MAN**

beach-DO-6509#show tech

GigabitEthernet5/2 is up, line protocol is up (connected)
- Hardware is C6k1000Mb 802.3, address is 0024.1499.9aa9 (bia0024.1499.9aa9)
- Description: #### TLS WAN LINK ####
- MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
  - reliability 255/255, txload 41/255, rxload 251/255
- Encapsulation ARPA, loopback not set
- Keepalive set (10 sec)
  - Full-duplex, 100Mb/s
- Media-type configured as RJ45 connector
- input flow-control is off, output flow-control is on
- Clock mode is auto
- ARP type: ARPA, ARP Timeout 04:00:00
- Last input 00:00:05, output 00:00:40, output hang never
- Last clearing of "show interface" counters 14w5d
- Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 24033698
- Queueing strategy: fifo
- Output queue: 0/40 (size/max)
  - 5 minute input rate 98450000 bits/sec, 9673 packets/sec
  - 5 minute output rate 16387000 bits/sec, 6548 packets/sec
Electrostatic Discharge (ESD)

Biggest factor you control to increase availability

- ESD - the rapid movement of a charge from one object to another.
- ESD event may not show up for weeks or months in electrical components – Latent Failure Mode - responsible for 90% of all component failures
- Components in ESD protective packaging can be handled by people who are not grounded.
- When servicing - utilize a static dissipative mat and wrist strap

- ESD Training Program -
  http://www.cisco.com/web/learning/le31/esd/WelcomeP.html
Key Points

- Most deployment issues are a combination of small problems

- Typical issues
  - Lack of education and training
  - Poor planning - lack of project management
  - Network has existing problems – video will uncover and graphically illustrate

- User expectations must be managed
Summary
Key Takeaway Items

- Bandwidth for standard definition video is much higher than VoIP, and is compounded for high definition
- IPVS BW consumption is generally unidirectional
- Surveillance integrators will require more IP networking expertise than they have in-house today
- Today video surveillance is mainly reactive, forensic
- As video integrates with other systems, it becomes more proactive and adds value to the business
- Video surveillance - *any time, any place*, will drive future WAN BW requirements
<table>
<thead>
<tr>
<th>Session ID</th>
<th>Start Time</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCEVT-2981</td>
<td>Sunday, 08:00</td>
<td>Architecture for Interactive Video Communication</td>
</tr>
<tr>
<td>LTEVT-2301</td>
<td>Sunday, 08:00</td>
<td>TelePresence Integration Lab - The Next Generation of Collaboration Solutions</td>
</tr>
<tr>
<td>BRKEVT-2814</td>
<td>Monday, 08:00</td>
<td>Troubleshooting TelePresence Call Failures</td>
</tr>
<tr>
<td>BRKEVT-2800</td>
<td>Monday, 10:00</td>
<td>Overview of Cisco TelePresence Solution and Deployments</td>
</tr>
<tr>
<td>BRKEVT-2801</td>
<td>Monday, 13:00</td>
<td>Cisco Telepresence: best practices for call control integration</td>
</tr>
<tr>
<td>LTEVT-2300</td>
<td>Monday, 13:00</td>
<td>Enterprise Medianet: Video Applications and Network Design Lab</td>
</tr>
<tr>
<td>COCEVT-3431</td>
<td>Tuesday, 08:00</td>
<td>Inside Cisco IT: Offering Video as an IT Service...How to Fund, Justify and Enable</td>
</tr>
<tr>
<td>BRKEVT-2311</td>
<td>Tuesday, 08:00</td>
<td>Network Design and Implementation for IP Video Surveillance</td>
</tr>
<tr>
<td>DISIoT-1005</td>
<td>Tuesday, 12:30</td>
<td>Integrated Plant: Secure and Remotely Accessible M2M Connected Production Environment/Video Analytics</td>
</tr>
<tr>
<td>BRKEVT-2807</td>
<td>Tuesday, 12:30</td>
<td>Enterprise Video Network Performance Analysis with Medianet</td>
</tr>
<tr>
<td>BRKEVT-2812</td>
<td>Tuesday, 15:00</td>
<td>Bringing Webex meetings and Telepresence together - WebEx TelePresence Integration</td>
</tr>
<tr>
<td>BRKEVT-2810</td>
<td>Wednesday, 08:00</td>
<td>Deploying Jabber Video for Telepresence(Movi)</td>
</tr>
<tr>
<td>BRKEVT-2806</td>
<td>Wednesday, 13:30</td>
<td>Troubleshooting Network Impairments in Enterprise TelePresence Deployments</td>
</tr>
<tr>
<td>BRKEVT-2803</td>
<td>Wednesday, 16:00</td>
<td>Designing and Deploying Multipoint Conferencing for Telepresence Video</td>
</tr>
<tr>
<td>BRKEVT-2813</td>
<td>Wednesday, 16:00</td>
<td>Using Video Analytics to Improve Safety, Security, and Business Intelligence</td>
</tr>
<tr>
<td>BRKEVT-2802</td>
<td>Thursday, 08:00</td>
<td>Deploying TelePresence and Video Endpoints on Unified Communications Manager</td>
</tr>
<tr>
<td>COCEVT-3432</td>
<td>Thursday, 08:00</td>
<td>Inside Cisco IT: Do's, Don'ts and Lessons Learned during 5 Years of Video Deployment</td>
</tr>
<tr>
<td>BRKEVT-2811</td>
<td>Thursday, 10:00</td>
<td>Deploying Telepresence &amp; Video endpoints</td>
</tr>
<tr>
<td>COCEVT-3430</td>
<td>Thursday, 10:00</td>
<td>Inside Cisco IT: Video Interoperability...Not Just a Dream</td>
</tr>
<tr>
<td>BRKEVT-2815</td>
<td>Thursday, 12:30</td>
<td>Medianet Traffic and Device awareness for intelligent services (2)</td>
</tr>
<tr>
<td>BRKEVT-2319</td>
<td>Thursday, 16:00</td>
<td>Business to Business Video</td>
</tr>
</tbody>
</table>
Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Cisco Daily Challenge points for each session evaluation you complete.
- Complete your session evaluation online now through either the mobile app or internet kiosk stations.

Maximize your Cisco Live experience with your free Cisco Live 365 account. Download session PDFs, view sessions on-demand and participate in live activities throughout the year. Click the Enter Cisco Live 365 button in your Cisco Live portal to log in.