How to Use Wireshark to Analyze Video
Betty DuBois, Sr. Manager, Product Marketing
Endace a division of Emulex
http://tinyurl.com/tcpctraces
Why care about video?

According to Cisco Visual Networking Index
Why care about video?

Global Business Service Adoption Trends

By 2017, Business Mobile SMS will have 537 million users, ranking as the highest penetrated service among all business service categories (data & mobile).

- Business Location-based Services (LBS) will be the second fastest growing business service category from 2012 to 2017. ▲ 32.9% CAGR

- Business IM will have 703 million users, ranking as the business service category with the largest number of users.

- Desktop Video Conferencing will be the fastest growing service across all business service categories (data & mobile) from 2012 to 2017. ▲ 51.7% CAGR

According to Cisco Visual Networking Index
Why care about video?

- According to Cisco Visual Networking Index
Just how much bandwidth?

• **Netflix**
  – 1 Mbps for viewing on a computer
  – 2 Mbps for SD video on a TV
  – 4 Mbps for 720p HD video
  – 5 Mbps for "the best video and audio experience" (according to Netflix)

• **Hulu**
  – 1 Mbps for SD video
  – 2 Mbps for 720p video
  – Over 3.2 Mbps for best quality HD video and audio

• **Vudu** - Note: All Vudu movies are streamed with Dolby Digital Plus 5.1 audio.
  – 1.0 - 2.3 Mbps for SD video
  – 2.3 - 4.5 Mbps for 720p video
  – 4.5 - 9.0 Mbps for HDX 1080p video
  – Over 9 Mbps for 3D HD movies

According to www.hometheater.com
Where do I start?

• Use policies
  – What can you block

• Business approved
  – How much bandwidth is it really taking – capacity planning
  – How much packet loss is there – capacity planning & troubleshooting
  – What QoS is in place – is that what I designed
  – How much jitter
What are the common protocols?

Compression
- MPEG4
- MPEG2
- H.264

Transfer
- RTP
- RTCP
- RTSP
- RTMP
RTSP

- Real Time Streaming Protocol
- The protocol is used for establishing and controlling media sessions between end points
- Similar to HTTP
  - DESCRIBE responses will show media type
RTSP – TrendnetViaServer.pcap

- Telephony | RTSP | Packet Counter | Create Stat
- Filters:
  - rtsp
  - sd.p.media.media="video"
  - rtsp.status>299

<table>
<thead>
<tr>
<th>Topic / Item</th>
<th>Count</th>
<th>Rate (ms)</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total RTSP Packets</td>
<td>13</td>
<td>0.000142</td>
<td></td>
</tr>
<tr>
<td>RTSP Request Packets</td>
<td>7</td>
<td>0.000076</td>
<td>53.85%</td>
</tr>
<tr>
<td>DESCRIBE</td>
<td>2</td>
<td>0.000022</td>
<td>28.57%</td>
</tr>
<tr>
<td>SETUP</td>
<td>2</td>
<td>0.000022</td>
<td>28.57%</td>
</tr>
<tr>
<td>PLAY</td>
<td>2</td>
<td>0.000022</td>
<td>28.57%</td>
</tr>
<tr>
<td>TEARDOWN</td>
<td>1</td>
<td>0.000011</td>
<td>14.29%</td>
</tr>
<tr>
<td>RTSP Response Packets</td>
<td>6</td>
<td>0.000066</td>
<td>46.15%</td>
</tr>
<tr>
<td>???: broken</td>
<td>0</td>
<td>0.000000</td>
<td>0.00%</td>
</tr>
<tr>
<td>1xx: Informational</td>
<td>0</td>
<td>0.000000</td>
<td>0.00%</td>
</tr>
<tr>
<td>2xx: Success</td>
<td>6</td>
<td>0.000066</td>
<td>100.00%</td>
</tr>
<tr>
<td>3xx: Redirection</td>
<td>0</td>
<td>0.000000</td>
<td>0.00%</td>
</tr>
<tr>
<td>4xx: Client Error</td>
<td>0</td>
<td>0.000000</td>
<td>0.00%</td>
</tr>
<tr>
<td>5xx: Server Error</td>
<td>0</td>
<td>0.000000</td>
<td>0.00%</td>
</tr>
<tr>
<td>Other RTSP Packets</td>
<td>0</td>
<td>0.000000</td>
<td>0.00%</td>
</tr>
</tbody>
</table>
RTP

- Real Time Protocol
- Used for voice or video
- For video transfers, RTP most commonly used in video conferencing
- Check QoS
  - Apply as column
  - Does the value change as travel through the environment?

Differentiated Services Field: 0xb8 (DSCP 0xe: Expedited Forwarding; ECN: 0x00: Not-ECT (1011 10.. = Differentiated Services Codepoint: Expedited Forwarding (0xe))
  .......00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
RTP – TrendnetViaServer.pcap

- Telephony | Show All Streams
- How much loss?
  - Packet loss is determined by the sequence numbers, much like TCP
Telephony | Stream Analysis
If loss is greater than 1%, how is the loss spread?
Wrong timestamps?
RTP – VLC_rtp_stream.pcap

- UDP???
  - Wireshark doesn’t realize it is RTP because it is a stream
  - there is no control protocol
  - Or control protocol is missing (in other examples)
  - Decode as RTP
    - Show Current
    - Save to Profile
RTMP – WSB_live.pcap

• Real Time Messaging Protocol
• Flash video streaming
• Message flow:
  – Handshake
  – Connection parameter exchange
  – Play video – createStream
• Troubleshoot like any other TCP stream
H.264

- Most common high definition video compression
- Used by Vimeo, YouTube, iTunes, Flash Player, Silverlight and Blu-ray discs
Trendnet_h264.pcap

- Filter http.content contains video
- 500,000Bps = 3.8Mbps
Video Stream in HTTP

- Example is a .swf file
- Users complaining of video pausing
- Packet loss and TCP recovery issue – yet because it is video, it is infinitely more noticeable to the user
- Sort by TCP delta time
Questions?