Remote Tech in a Modern World

By: Jacob Daniluck
Technical Sales Specialist, Americas
Broadcast Remote Solutions

• Software Based Codecs & Hardware Based Codecs
• Advancements in Technology implemented in remote solutions
• Few troubleshooting techniques
Software based Audio Codec

- Software Packages that are based around live streaming:
  - LUCI
  - ipDTL
  - Cleanfeed
  - Skype
  - Report-IT
  - Field Tap
  - Etc...
RTP with a Software Unit

• Things to know
  • Cheaper than Hardware based solutions
    • Note that some software based solutions do require a monthly/annual subscription
  • Technical support may be limited
  • At the mercy of the operating system
    • Think of Windows Dreaded Updates
    • Higher-Propriety Task taking CPU Cycles
    • Virus Protection
    • Power Redundancy
    • Network Redundancy
  • Auto-Reconnect may not be fully implemented
Hardware Solutions

• Hardware Manufactures throughout the industry
Hardware Solutions

• Benefits of using hardware based codecs
  • Forward Error Correction
  • Packet Level Duplication
    • Tieline’s SmartStream PLUS
    • Comrex’s Crosslock
    • Worldcast Surestream
  • Network Bonding
  • Power Redundancy
  • Transport Failover for connectivity
  • Adaptable Jitter Buffer
Hardware Solutions

• Additional Benefits overlooked
  • Typically DSP Based Architecture – Provides low latency options for processing digital signals and more flexibility from Manufacturer
    • Digital Audio Routing
    • Audio Encoding/Decoding
    • Less of a restriction on the CPU
  • Audio Input/Output Circuits designed for broadcast quality audio
  • Mixer & Connectivity Options Built-in to a single unit
  • Technical Support is supported by the manufacturer
Hardware Solutions

• Things to keep in mind
  • Hardware Solutions are typically use-case specific
    • Remote Broadcast Codec, is either a codec (or perhaps a mixer as well)
  • Cost – Typically more expensive then software based solutions
Primary and Backup Solutions

**Hardware Solutions** should be the primary means for remote broadcasts
- Designed for the purpose of broadcasting in a remote environment
- Designed to be simply and easy for talent to use
- Normally multiple layers of redundancies built-in

**Software Solutions** should be setup as a backup solution for remotes
- Requires a PC to operate
- Requires CPU management to ensure CPU cycles are not taken
- At the mercy of the audio input/output device
- May have longer delays
- At the mercy of dependences
  - WebRTC – Maintained by Google, Mozilla, Opera
  - SIP EBU 3326 Maintained by the Internet Engineering Task Force
Modern Features

• Forward Error Correction
• Quality of Service
• Packet Replication
• Network Diversity
• Time Diversity
Forward Error Correction

• Act of embedding an additional data-correction stream from the transmitter unit.

• The data-correction stream is designed to operate to “help” correct missing data received at the decoder.

• This technique does require additional throughput, but can be useful when no other options are available.
Quality of Service

- Quality of Service
  - Differentiated Services (DiffServ) – RFC 2474
    - Class Based Mechanism for Traffic Management over a Network Interface
    - This mechanism acts as a framework to provide internet routers the ability to differentiate types of traffic based on their class.
Quality of Service

• Quality of Service
  • DiffServ Classes
    • Default Forwarding – Typically uses a “Best-Effort” forwarding characteristics
    • Expedited Forwarding – Provides Low-Delay, Low-Loss, and Low-Jitter Characteristics
    • Assured Forwarding – Provides assurance of delivery as long as traffic doesn’t exceed some subscribed rate. This Class has subgroups built-in for priority on dropping packets
    • Class Selector – Used prior to Differentiated Services. This uses a simpler version of DiffServ
### Quality of Service

<table>
<thead>
<tr>
<th>Application</th>
<th>CoS=IPP</th>
<th>AF</th>
<th>DSCP</th>
<th>EXP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best Effort</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Scavenger</td>
<td>1</td>
<td>CS1</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>1</td>
<td>AF11</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AF12</td>
<td>12</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AF13</td>
<td>14</td>
<td>1</td>
</tr>
<tr>
<td>Network Mgmt.</td>
<td>2</td>
<td>CS2</td>
<td>16</td>
<td>2</td>
</tr>
<tr>
<td>Transaction Data</td>
<td>2</td>
<td>AF21</td>
<td>18</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AF22</td>
<td>20</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AF23</td>
<td>22</td>
<td>2</td>
</tr>
<tr>
<td>Call Signaling</td>
<td>3</td>
<td>CS3</td>
<td>24</td>
<td>3</td>
</tr>
<tr>
<td>Mission-Critical</td>
<td>3</td>
<td>AF31</td>
<td>26</td>
<td>3</td>
</tr>
<tr>
<td>Streaming Video</td>
<td>3</td>
<td>AF32</td>
<td>28</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AF33</td>
<td>30</td>
<td>3</td>
</tr>
<tr>
<td>Interactive Video</td>
<td>4</td>
<td>CS4</td>
<td>32</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AF41</td>
<td>34</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AF42</td>
<td>36</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AF43</td>
<td>38</td>
<td>4</td>
</tr>
<tr>
<td>Voice</td>
<td>5</td>
<td>CS5</td>
<td>40</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EF</td>
<td>46</td>
<td>5</td>
</tr>
<tr>
<td>Routing</td>
<td>6</td>
<td>CS6</td>
<td>48</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CS7</td>
<td>56</td>
<td>7</td>
</tr>
</tbody>
</table>
Packet Replication

• Packet Replication:
  • The process of copying an IP Packet and sending it out any network interface, first used on Cisco Switches
  • This process typically requires a secondary stream to be established between the “Server” and “Client”
  • This process can provide a second copy of the audio data packet

• Why Should you use Packet Replication?
  • As IP Packet Data is sent across the Public Internet, there can sometimes be collusion on Routing Servers that will have to drop the Packet at certain times.
  • Therefore, the idea of a second identical packet being dropped is small
Network Diversity

• Network Diversity:
  • The process of using a secondary network with Packet Replication
  • This is not a failover technique
  • For a Audio IP Path to be truly diverse, the network paths provided must be unrelated
    • ISP A and ISP B could be running two different forms of communication, but share a common drop point in the real world
      • Both lines are running across the same phone pole
      • Both lines share a common path
    • Example of recommended setup
      • Fiber Path for Primary
      • Cable, DSL, or Private IP link for Secondary

• Why should you use Network Diversity?
  • This technology is designed to provide not only a reliable link, but a redundant link.
  • When setting up a Network Diverse connection with your IP Audio equipment, this will create a secondary link through a separate network to your end point destination
Time Diversity

• Time Diversity:
  • The process of using Packet Replication at a slightly longer delay (ms) than the original stream

• Why should you use Time Diversity?
  • The same principles of using Packet Replication are applied. If you are sending out a secondary stream the chances of a router dropping a packet are small.
  • Adding in a secondary stream at a slightly longer delay will decrease the chances of dropping audio packets even more.
Tools to Troubleshoot IP Audio

• 3rd Party Software Tools
  • iPerf3 (www.iperf.fr)
    • Great application for testing LAN/WAN throughput between two locations
    • Provides stats for throughput and bandwidth available
    • Useful for testing both TCP and UDP services
  • Wireshark (www.wireshark.org)
    • Great application for debugging packet level problems
  • Simple Network Management Protocol (SNMP)
    • Great protocol to use to simply keep you informed on what is happening with your network
    • Can be used with any IP system that supports SNMP
3rd Party Tools - iPerf

• iPerf is a network throughput tool
• This application tool requires the use of a server and client (i.e. two installations)
• This application does require proper network forwarding.
• Provides throughput for both TCP and(or) UDP traffic
3rd Party Tools – Using iPerf

• Command Line Interface tool
• Some Graphical User Interfaces are available for specific OS
  • Linux: jPerf
  • Windows: Opensource GitHub Development
  • Windows: WindowsPerf (Paid License – Not Tested)
  • Limited in how much throughput is achievable
3rd Party Tools – Using iPerf
# 3rd Party Tools – Using iPerf

## iPerf Output

```
3rd Party Tools – Using iPerf

```
3rd Party Tools – Wireshark

- A Tool designed to act as an oscilloscope for IP Data
- Formerly called a packet capture device
- Allows for a laptop/desktop to intercept packets from the network and capture them in a log
- The data captured is maintained in its packet form
- Wireshark also provides some tools to decode packet data (i.e., turning raw AES67 traffic into a playable audio stream)
3rd Party Tools – Using Wireshark

• Wireshark is designed as a universal tool. It can be installed on multiple operating systems (Windows, macOS, Linux-Based OS)
• Comes complete with a Command Line Toolkit
• Also, comes complete with a GUI toolkit
3rd Party Tools – SNMP

- Simple Networking Management Protocol
- Not an application, but a protocol defined for the internet
- This protocol provides management tools to be alerted and set specific settings on network devices
- Not all network devices support a SNMP Agent
- SNMP has multiple versions (i.e. SNMPv1, SNMPv2, SNMPv3)
  - SNMPv1 – Basic Original Design
  - SNMPv2 – Adds some enhancement, and introduced the SNMP “Inform”
  - SNMPv3 – Adds Security to SNMPv2
3rd Party Tools – Using SNMP

• SNMP has a lot of terms that are specific to using SNMP
  • Set – Set a command on the SNMP Agent
  • Traps – Information being sent from the SNMP Agent
  • Informs – Information that is sent from the SNMP agent, but issues a confirmation that the data has been received/acknowledged.
  • Etc....

• As SNMP is a protocol it requires the use of an SNMP Manager
  • Multiple SNMP Managers are available – Ranging from Open Source to Paid Managed Licenses
Review

• Knowing a little bit about Audio over IP can help in the long run
• Understanding manufactures equipment can help increase the reliability of remote broadcasts, or even IP Audio STL solutions.
• Understanding 3rd party tools can help track down problems.
Review

• Primary and Backup Solutions
• Technology options to consider for the future