Audio Over IP – Technology Considerations

September 12, 2015

IBC2015

Featuring GatesAir's

Keyur Parikh

Architect / Software Lead

GATESAIRCONNECT

Connecting What's Next

Audio Over IP – Technology Considerations

Sept 12, 2015

Using IP For Media Broadcasting

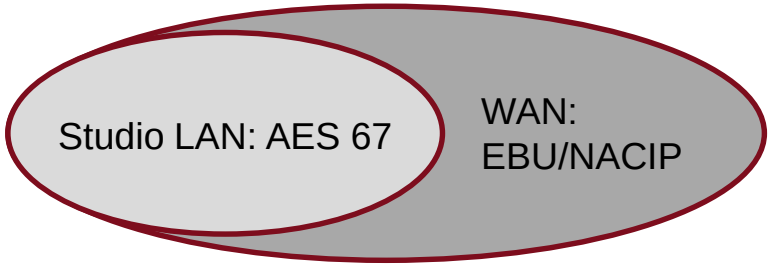
- Enabler
  - Advances in networking and computing technology coupled with lower cost – i.e low cost of high speed Ethernet switches, server technology, virtualization etc.
- Benefits
  - Reduces cost by using common IT infrastructure: switches, servers etc.
  - Reduces complexity of wiring: Physical audio interfaces are only needed at source and termination point, everywhere else it resides in the network
  - Enables Network Function Virtualization (NFV): i.e implementing functionality on off the shelf server technology
  - In the WAN transport, it significantly reduces re-occurring cost compared to circuit connection while increasing flexibility with site to site interconnection

Key Considerations for Audio Over IP

- Interoperability
  - Enables multi-vendor interworking
- Transport reliability
  - Overcome challenges posed by underlying IP network
- Network Security
  - Preventing unauthorized access to devices

Interoperability for Audio Over IP

- Enables customers to built multi-vendor ecosystem – buying “best of breed” solutions
- Need industry standards to ensure interoperability
- Vendors will be more willing to implement standards that are based on open internet protocols and technology
- Interoperability Standards
  - Audio in LAN: AES 67
  - Audio over WAN: EBU/NACIP



AES 67 – EBU/NACIP Differences

AES 67

- Specification for low delay, high fidelity audio in LAN. Only uses uncompressed audio format
- Sample rates greater 44.1 Khz (44.1, 48, 96 Khz) – high fidelity
- Primarily uses Multicast streams (even though Unicast streams are part of the standard)
- Precise synchronization is required between sender and receiver to achieve low latency
- Mandates PTPv2 (IEEE-1588): Ethernet based common timing reference

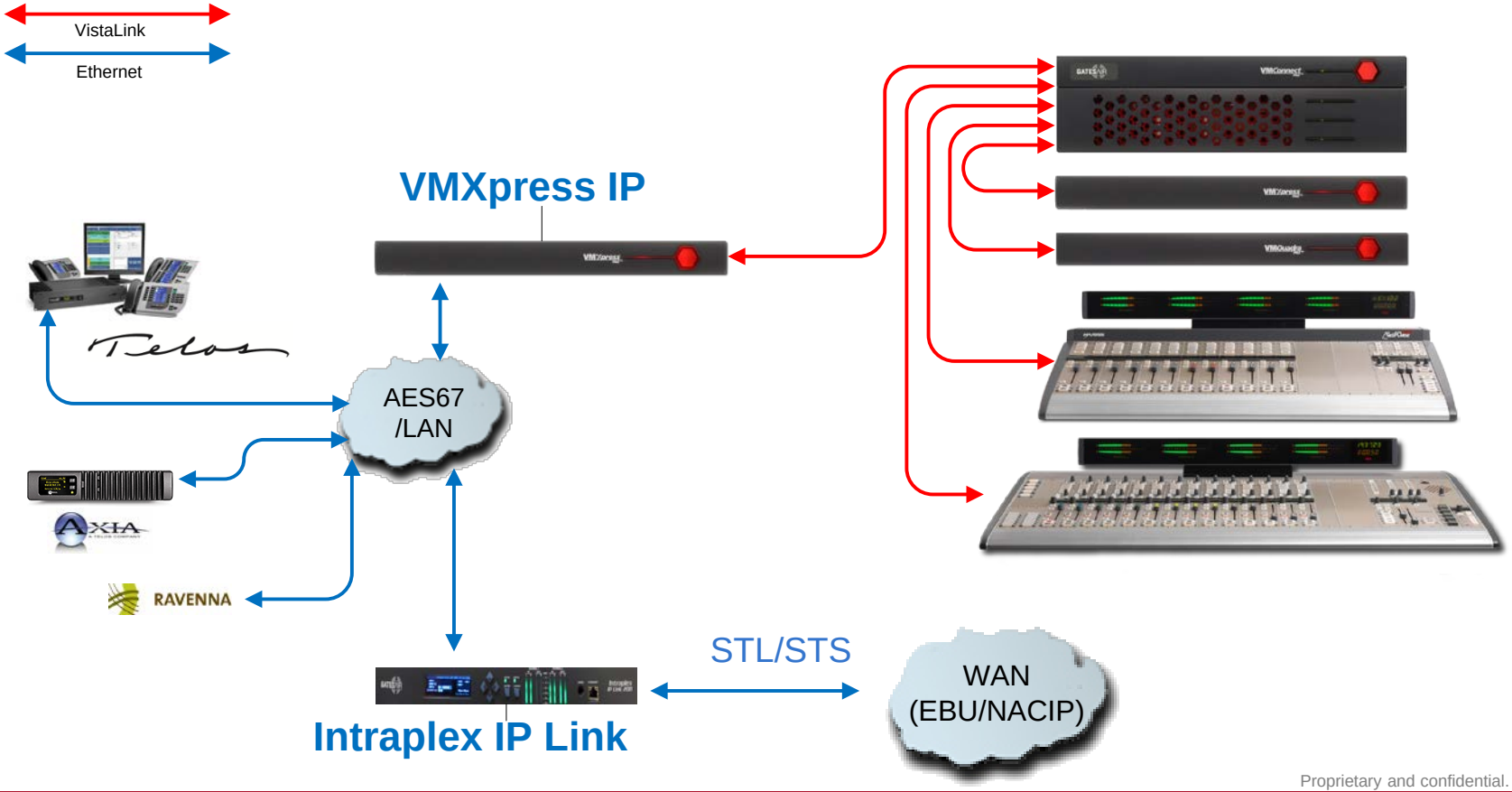
EBU/NACIP

- Specification for WAN environment. Specifies use of uncompressed and compressed audio formats (AAC, MP3, Opus etc.)
- Supports Sample rates from 8 to 48 KHZ
- Use of Unicast streams is more prevalent
- Precise synchronization is not required between nodes
- PTPv2 or other common reference is not mandated. Synchronization is achieved using incoming AoIP packets

Similarities between AES 67 and EBU/NACIP

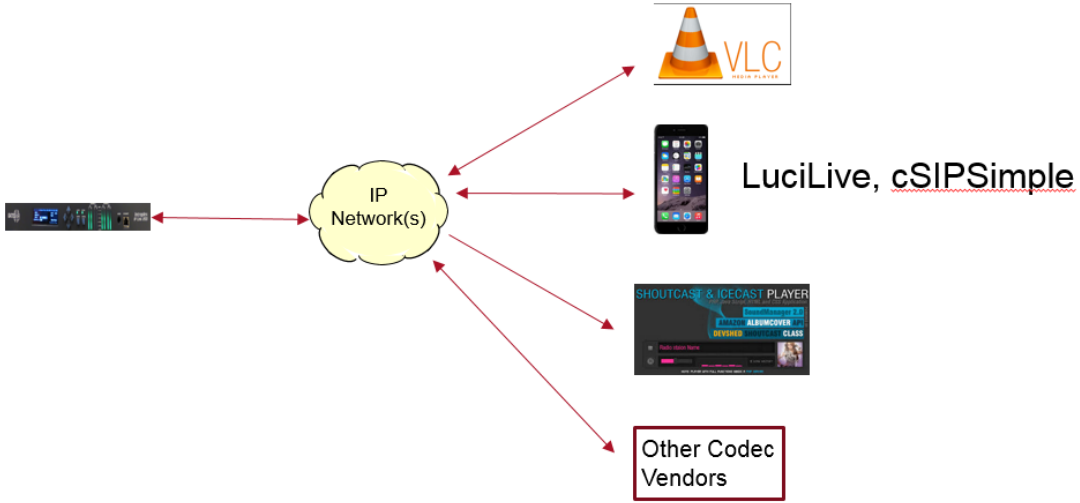
- Both specifies open Internet protocol - Real Time Protocol (RTP) to transport audio. RTP runs over UDP, so no re-transmission of lost packets
- Both specifies use of Unicast (Point to Point) and Multicast (Point to Multi-Point) audio streams. As of now AES 67 only uses Multicast. Unicast is prevalent with EBU/NACIP for remote contribution
- Both specify use of Session Initiation Protocol (SIP) to setup Unicast streams.
- Minimal Interworking between EBU/NACIP and AES 67:
  - EBU node should be able to receive a Multicast stream from AES 67 with 4 msec packet time. PTP based timestamps in the incoming RTP packets are ignored by the EBU node
  - AES67 cannot receive a stream from EBU node due to lack of PTP timing requirement

Interoperability – GatesAir's support



Interoperability – Intraplex IP Link

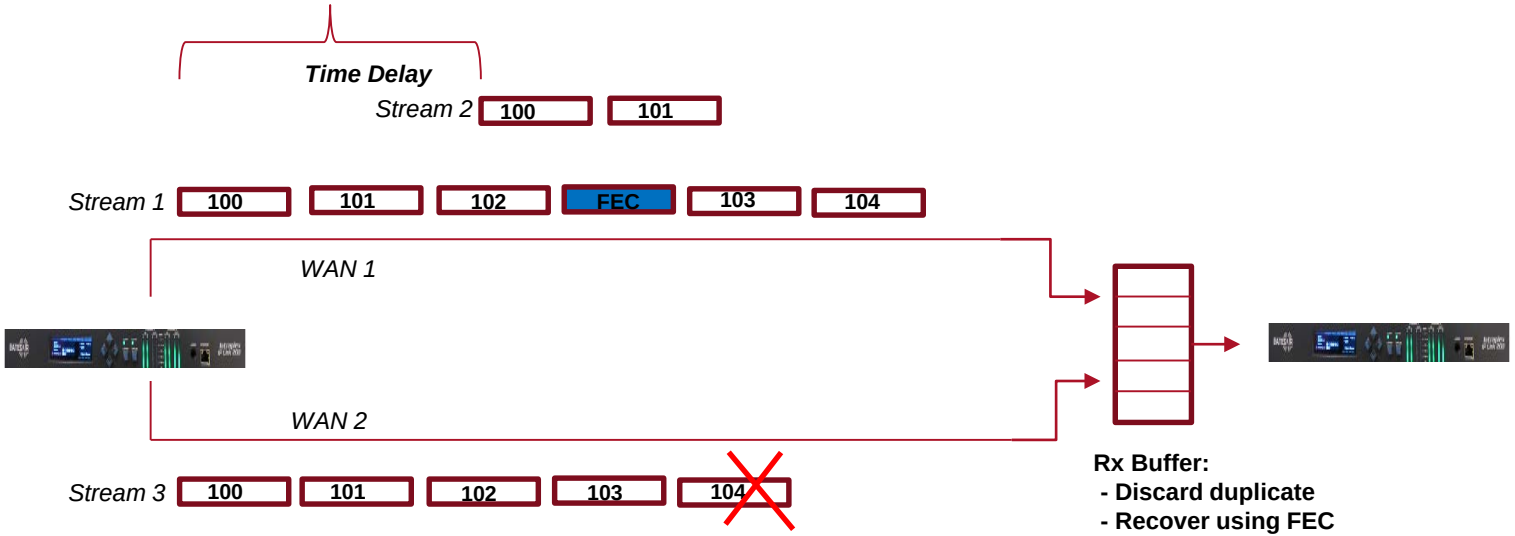
- IP Link supports EBU/NACIP standard with all required codecs
- IP Link interoperates with number of hardware and software codecs including:
  - Comrex, TieLine, LuciLive etc.
- Audio streams can be exchanged between VLC and IP Link



WAN Reliability

- IP based WAN have advantages, but need to overcome network impairments for broadcast quality
- Packet Loss Mitigation
  - Need a scalable set of technique to address wide range of network topologies
- Backup network and audio sources
  - Need ability to failover to low speed backup network or local audio sources in case of emergency
- Ability to monitor and analyze network quality to optimize codec performance
  - Monitor SLA of ISP
  - Analyze Packet Loss patterns: Random Vs Burst

Intraplex IP Link – Stream Splicing Technique

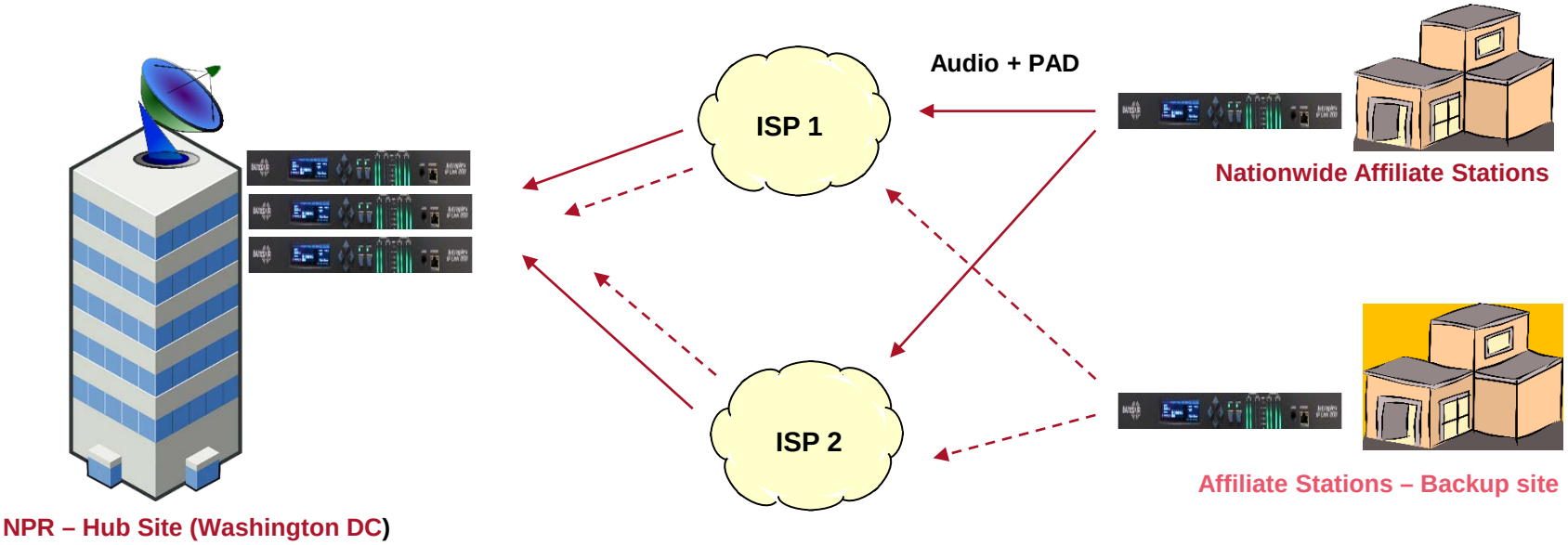


Stream 1: FEC enabled

Stream 2: Grouped with Stream 1. Delayed version of Stream 1 on same network. Time Delay value calculated by LiveLook report

Stream 3: Grouped with Streams 1 and 2. Same as Stream 1 but using different network. Network diversity provides hitless protection

Network Reliability Use Case – NPR (USA)



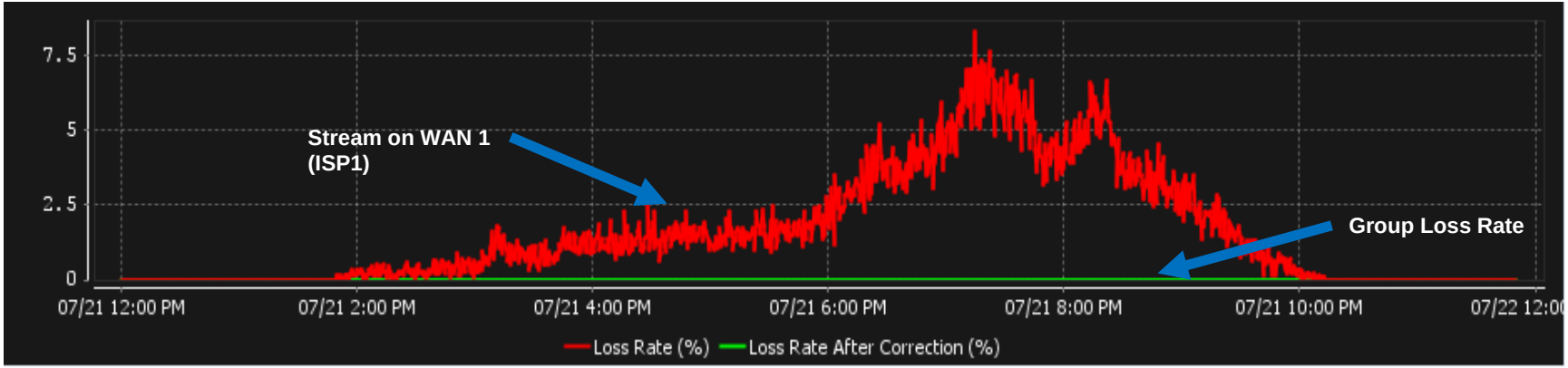
Capabilities used:

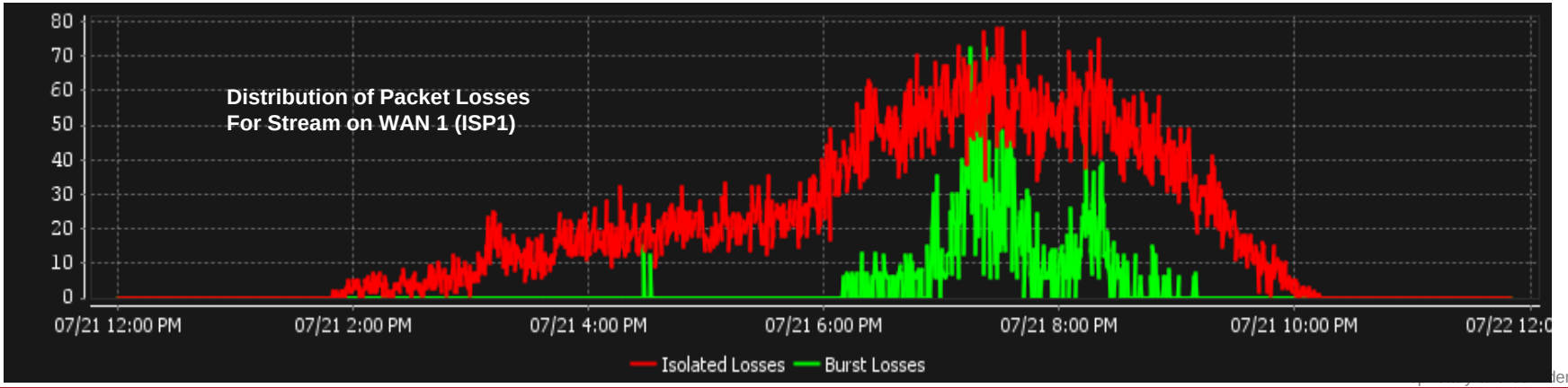
- Streaming splicing with 2 different ISPs
- Automatic failover to Backup site when Primary fails
- PAD aligned to audio spurt

Intraplex® LiveLook For IP Link

- Real-time graphical network analytics and monitoring tool
- Analyzes packet loss patterns and recommends which packet loss recovery technique will be most effective on a connection
- Logging capability helps with trouble shooting and SLA monitoring
- Single point to monitor state of all audio streams with optional Email notification

Use Case of LiveLook – KCLM Los Angeles

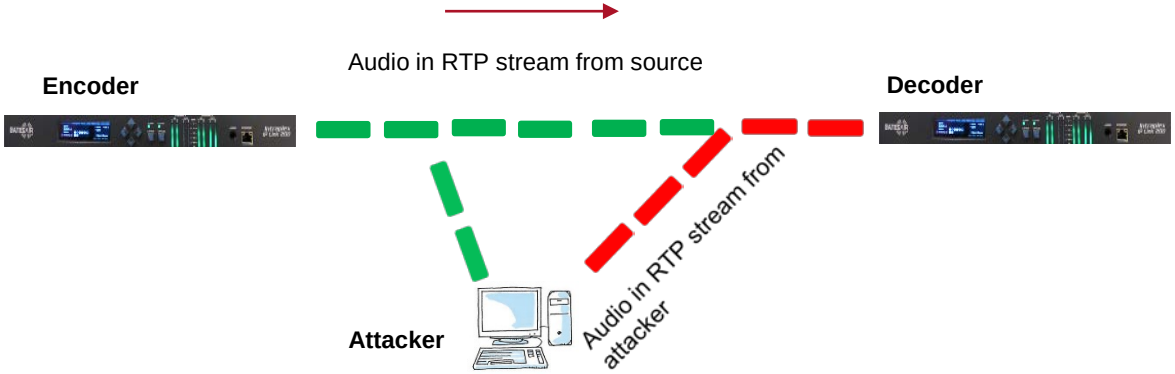




Network Security

- Use of ISPs and open Internet protocols make the system vulnerable to external threats
- Service Disruption threats
  - Unauthorized access via Web interface – Brute force attack to hack username/password
  - Unauthorized access via protocol services: SNMP, FTP, SIP
  - DoS (Ping Flood, TCP Syn Attack, IP Fragmentation attack)
- Media Plane threats
  - Use of standard encoding algorithms and protocols (RTP) posses threat of eavesdropping as well content replacement
  - Content replacement is where the attacker hijacks the media stream and play unauthorized content

Network Security – Content Replacement



- Decoder uses packet sequence number in RTP to detect duplicate
- Attacker can precede sequence number from Encoder
- Decoder accepts packets from attacker, as they arrive early
- Decoder discards packets from Encoder as duplicate

Network Security - Mitigation

- VPN/Firewall devices will protect against most threats, however open service ports can allow attackers to penetrate
- AoIP Codecs should have minimum set of security measures to protect both the management and media plane
- Access Control capability to restrict both management and media traffic should be included
  - IP Link provides both protocol and IP address level access control
- Web access should be protected with 2nd level authentication in case repeated login failures are detected.
  - IP Link requires an answer to a secret question with repeated login failures
- Media traffic in RTP should be authenticated
  - IP Link supports authentication of RTP packets with user defined passkey

Thank You!