Reliable Transport of Audio and Data Over IP

April 23, 2017

GatesAir Connect @ NAB Show 2017

Featuring GatesAir's

Keyur Parikh
Director, Intraplex

Reliable Transport of Audio and Data Over IP

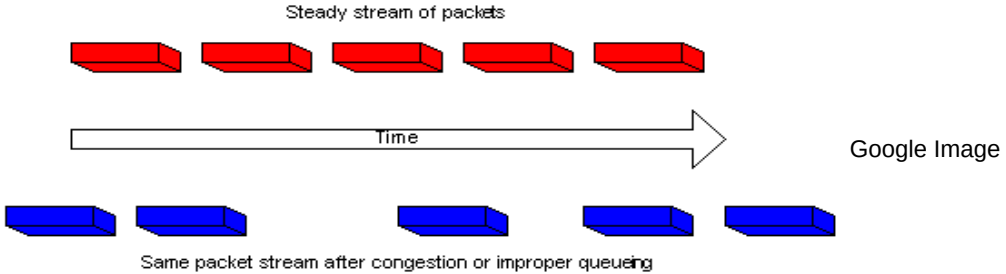
Keyur Parikh

Agenda

- Transport reliability
  - Review causes of packet losses
  - Review of media transport protocols
  - IP Link's methods for reliable IP transport for audio, FM MPX and control (GPIO, PAD)
- Network security
- Introducing Intraplex® IPConnect

Causes of Packet Losses

- Jitter: Variation in inter arrival time of a packet. Caused by queueing in network nodes.

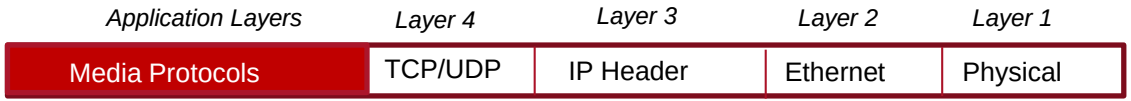


Google Image

  - *Solution*: Use Static or Dynamically sized De-Jitter buffer

- Various causes: link fades, route changes, congestion etc..
  - Patterns varies based on network quality – private Vs public
  - *Solution*: Several – depending on the pattern of losses

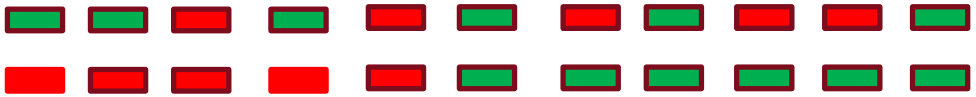
Media Transport Protocols



- TCP
  - Consumer streaming applications
  - Point to Point only, much higher playout delay, requires full duplex connection. Relies on retransmission of lost segments
  - Not suitable for broadcast application – no support for Multicast.
  - SHOUTcast/Icecast, RTMP, HLS, MPEG-DASH
- RTP over UDP
  - Broadcast application: 24/7 streams Vs on-demand
  - Most commonly used protocols for transport of VoIP, Audio and Video over IP. Standardized by both SMPTE and EBU for Audio and Video
  - Playout delay is controllable
  - Works with uni-directional network and Multicast
  - No retransmission of lost packets. Recovered outside of standard RTP/UDP protocol
- IP Link uses RTP/UDP as the main streaming protocol for Audio, MPX and PAD data transport

Packet Loss Recovery Techniques

- RTP level Forward Error Correction (FEC). Parity packets are used to recover lost packets. Very effective for Random/isolated pattern of losses



Random/isolated losses

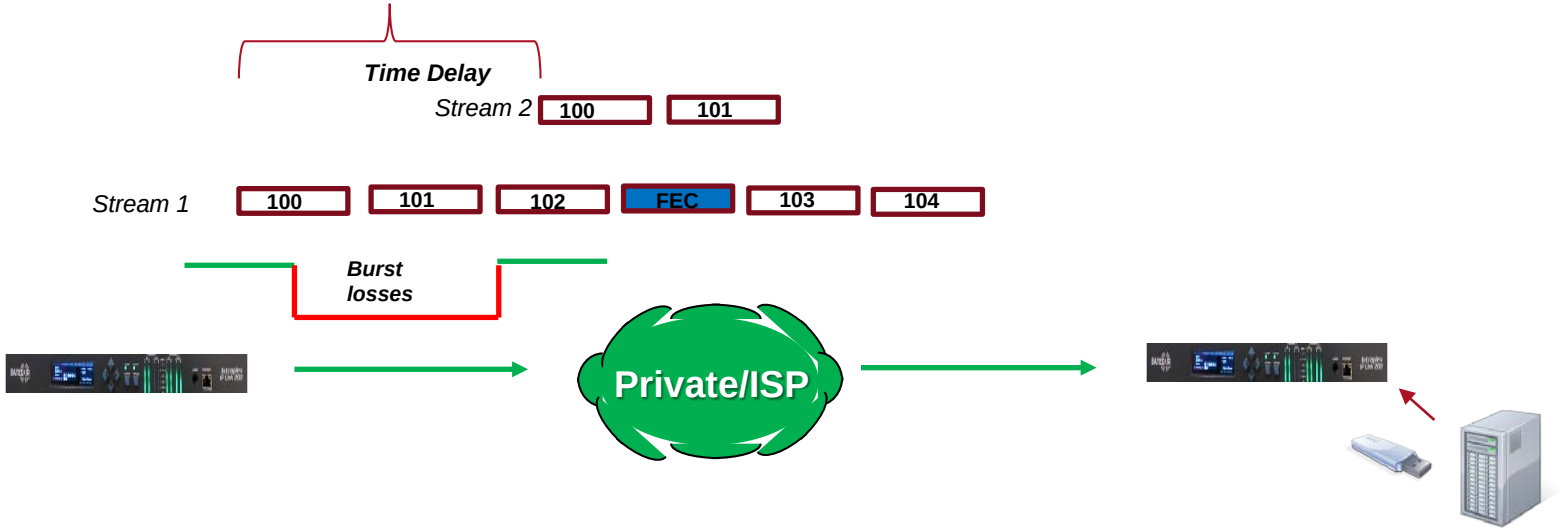
Burst losses

- Use Intraplex LiveLook to analyze the patterns of losses

- Stream Splicing – uses duplicate packets sent with time or network diversity. Very effective for burst packet losses. IP Link can use up to 3 network connections.

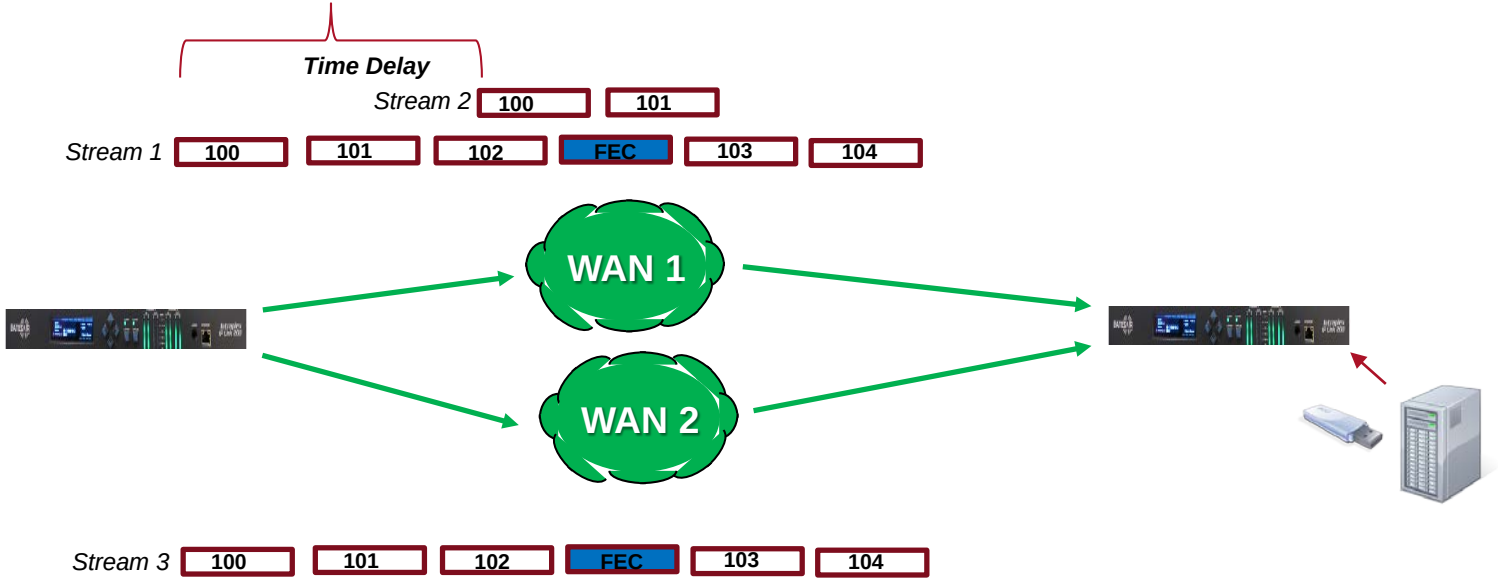
- Combination of FEC + Stream Splicing provides a scalable method for different network conditions

Packet Loss Protection – 1 WAN Network



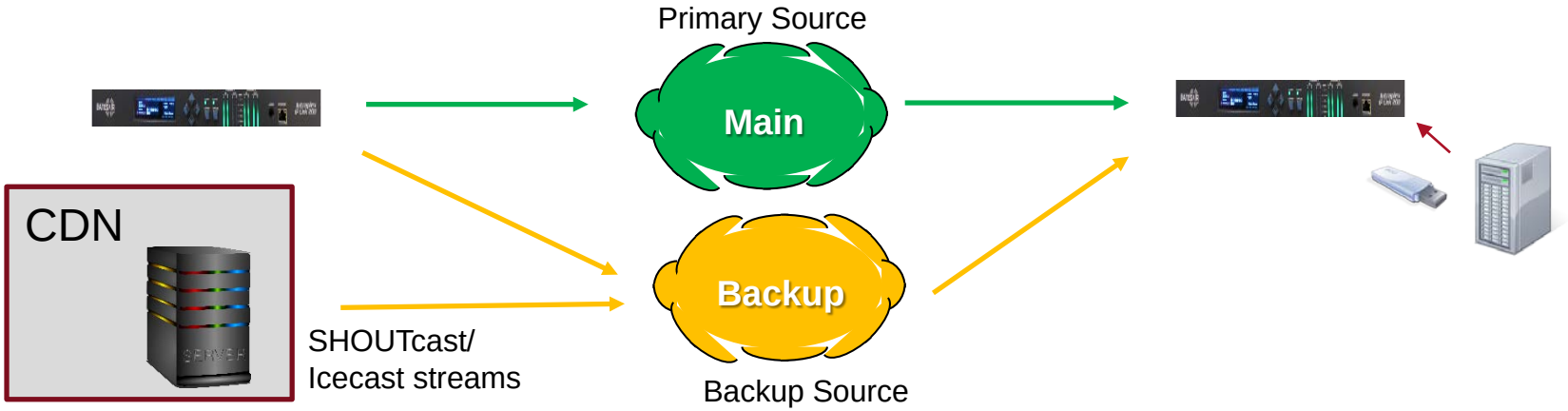
- Multiple streams (up to 12) in a group with programmable time delay. Very effective for burst packet losses
- Time delay value can be recommended by LiveLook
- FEC can be added to any stream for added protection
- Falls back to local audio source (USB, local feed)

Packet Loss Protection – Multiple Networks



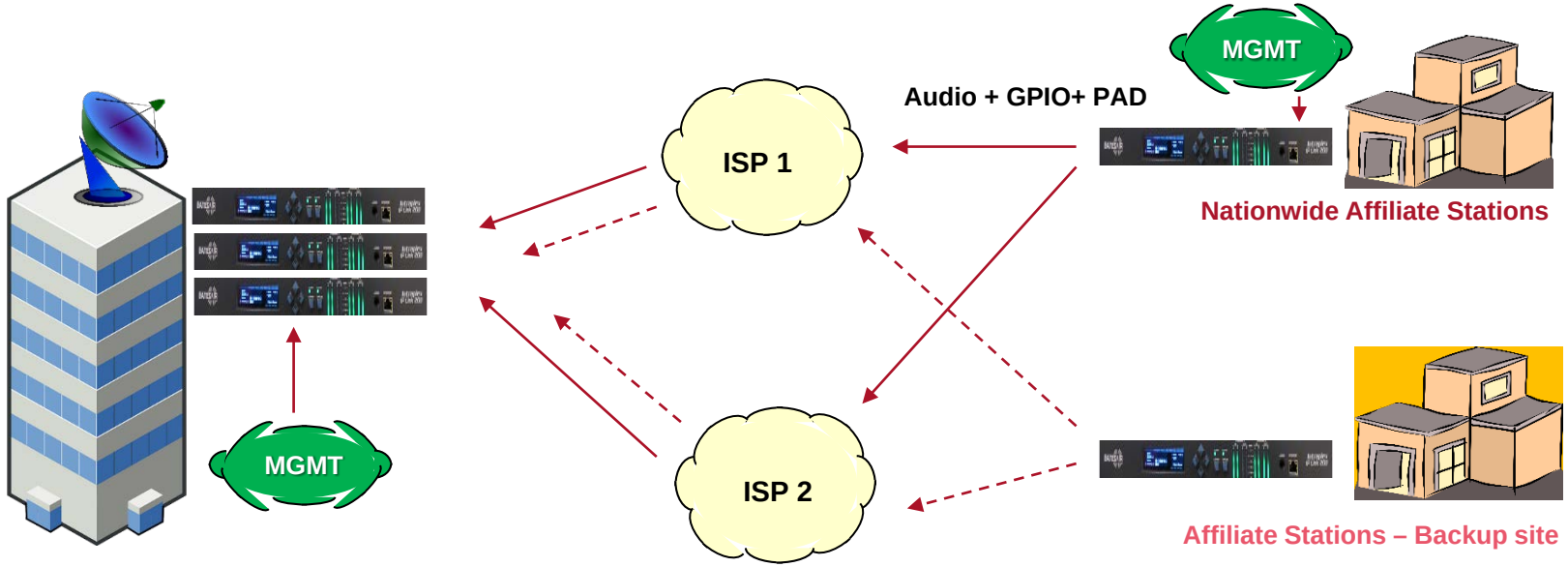
- Grouped streams sent across diverse network paths.
- Scalable protection: group of streams consisting of time diversity, network diversity and FEC
- “Hitless” operation as long as one network is available
- USB or local source as backup source

Main and Backup Networks



- Send high fidelity stream over main path (e.g. high speed microwave) as primary
- Send compressed stream from the same or different encoder, or an Internet server as a backup source
- Backup stream can be always ON or turned ON when required – useful for using LTE/Cellular as backup
- Failover criteria: Network loss at receiver, AES signal or silence at the encoder

Network Reliability Use Case – NPR



NPR – Hub Site (Washington DC)

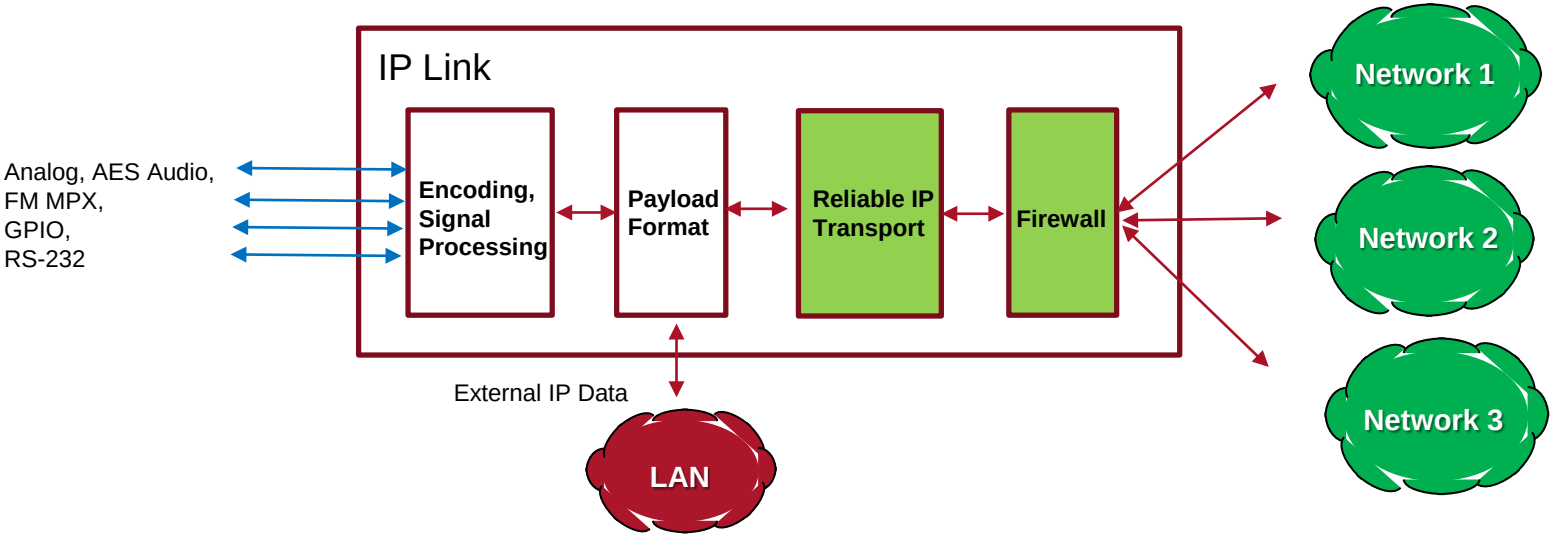
Capabilities used:

- 3 network ports to securely isolate networks
- Streaming splicing with 2 different ISPs
- Decoder at the hub site failover to backup site
- Reliable transport of GPIO and PAD, aligned to audio frame

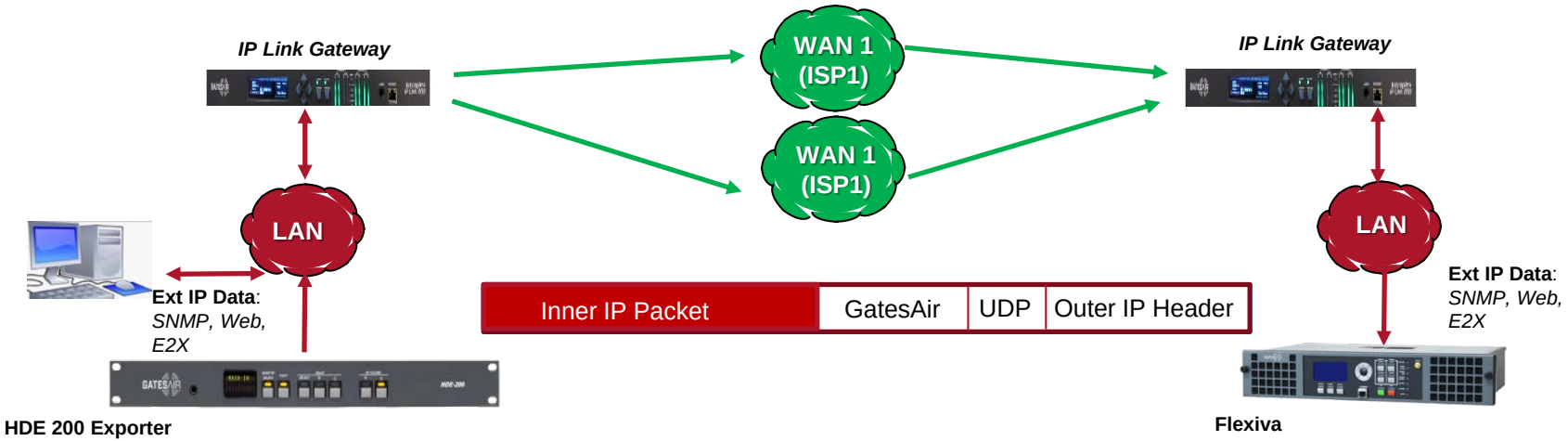
Network Security

- Common threats: hacking and misconfiguring system, DoS, wrong content on the air
- Leaving the default password has been the most common mistake
- IP Link forces the user to change the password out of the box
- IP Link's 3 network ports will physically isolate trusted from untrusted networks
- IP Link's layer 3 and layer 4 firewall capability restricts traffic based on source IP and type of traffic
- Support of secure Web (SSL) and SNMP (v3)
- 2-factor web authentication – password and answer to secret question to protect against user account hacking
- Smart web cookies to track if a user session has been hijacked by another computer
- RTP stream authentication to ensure that the stream is coming from the approved encoder

IP Link: Internal Data Flow



Intraplex IPConnect



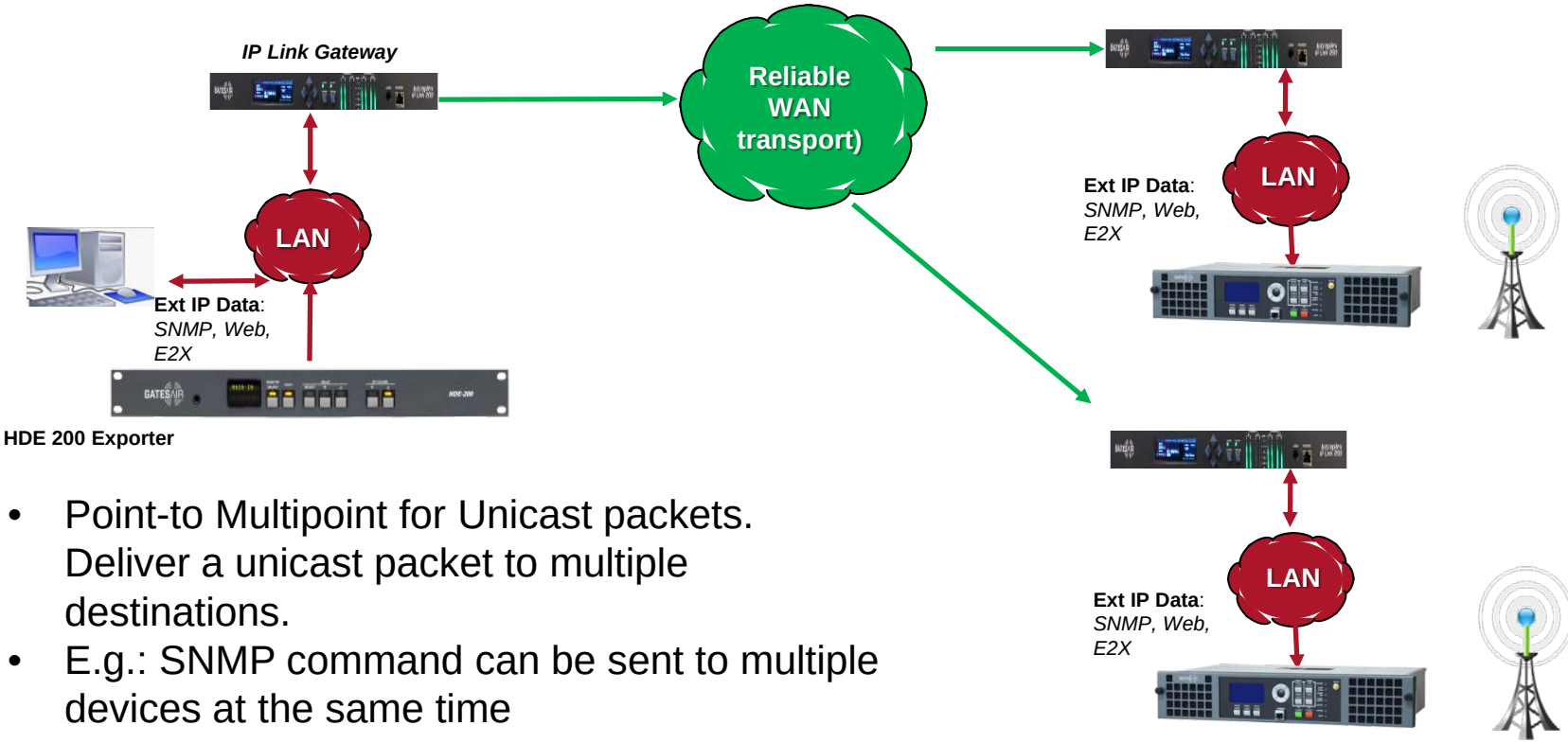
- Integrated IP Gateway software to reliably transport external IP datagrams
- Leverages IP Links network reliability and security capabilities
- Included on all models of IP Links (100, 100p, 200, MPX)

IPConnect

- Encapsulates local IP traffic

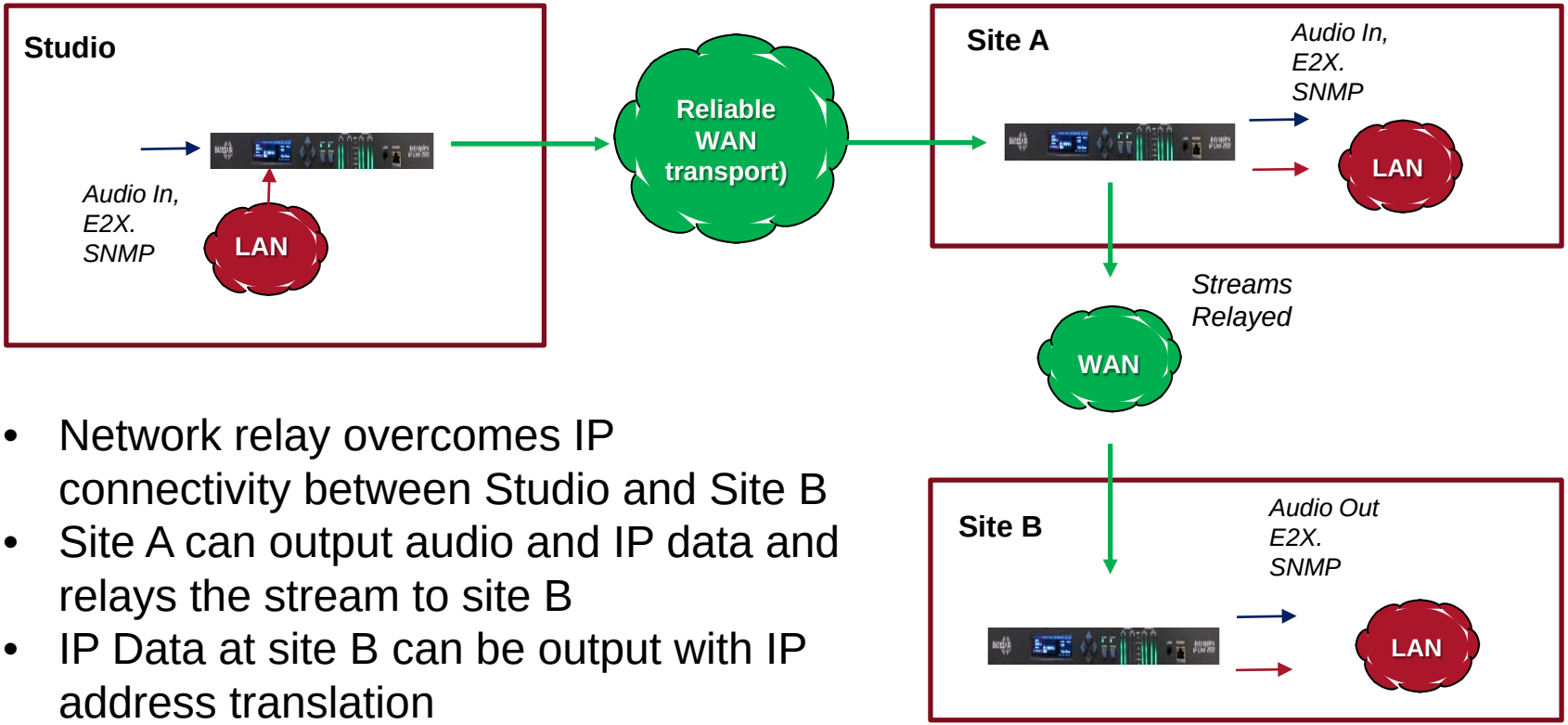
- Bridges Local IP traffic across WANs
- Application agnostic. Transports E2X, Web, SNMP traffic across STL . Future platform will increase capacity to transport video
- Provides specialized gateway functions typically not found on commodity routers

IPConnect: Replicate & Translate



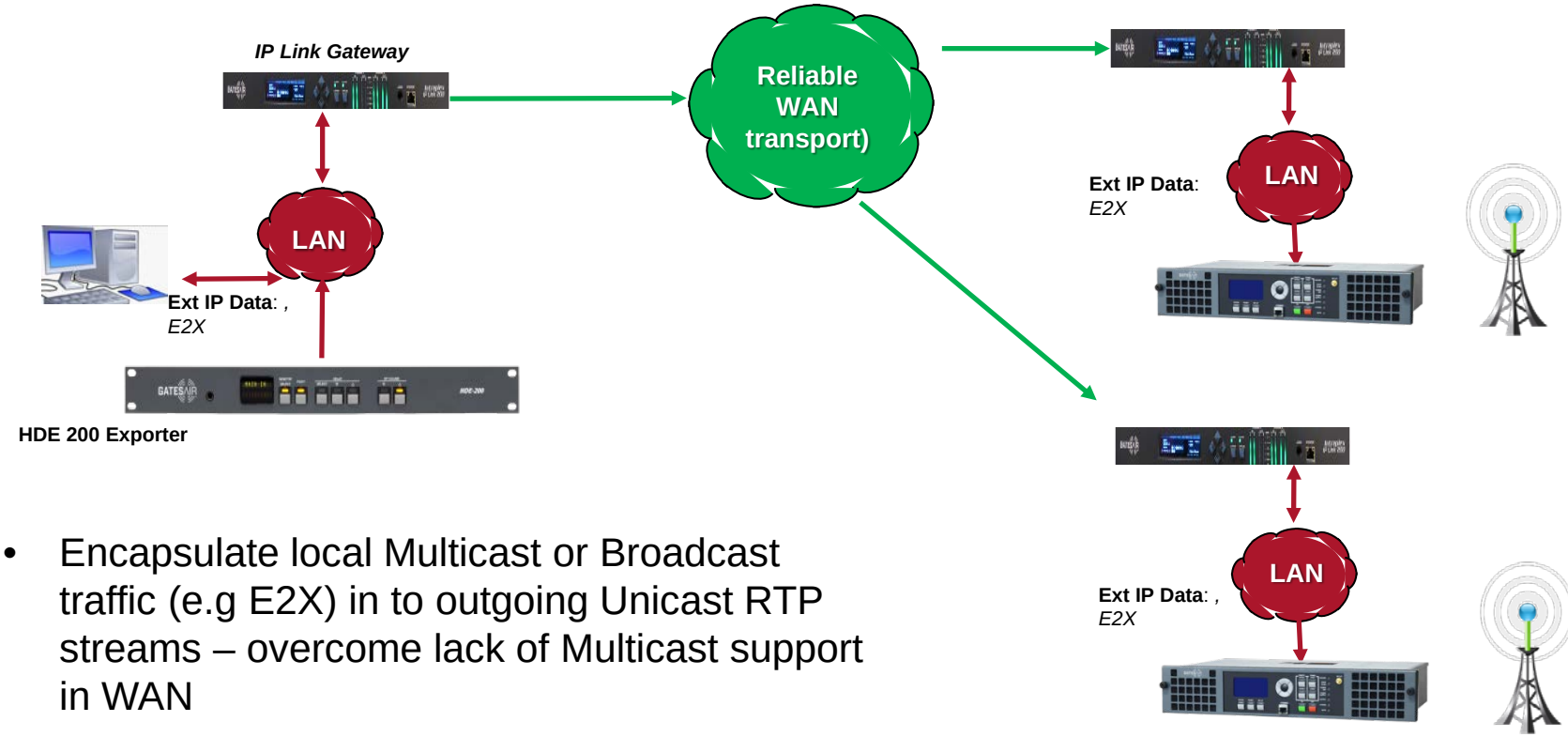
- Point-to Multipoint for Unicast packets. Deliver a unicast packet to multiple destinations.
- E.g.: SNMP command can be sent to multiple devices at the same time

IPConnect: Network Relay



- Network relay overcomes IP connectivity between Studio and Site B
- Site A can output audio and IP data and relays the stream to site B
- IP Data at site B can be output with IP address translation

IPConnect: Multicast ←→ Unicast



- Encapsulate local Multicast or Broadcast traffic (e.g E2X) in to outgoing Unicast RTP streams – overcome lack of Multicast support in WAN

Thank You!

Keyur Parikh
Director, Intraplex Business Unit