Monitoring SMPTE 2110 and IPMX Networks

Introduction

In the evolving world of broadcast and professional AV (Audio/Video) systems, the transition from traditional SDI-based infrastructures to IP-based media transport has been a significant development. Two major standards that have emerged to facilitate this transition are SMPTE 2110 and IPMX (Internet Protocol Media Experience). While SMPTE 2110 is primarily used in broadcast environments, IPMX is designed to meet the needs of the Pro AV industry. The most significant difference between the two standards is that SMPTE 2110 uses Precision Time Protocol (PTP) for its timing synchronization while IPMX uses RTCP packets.

Even though SMPTE 2110 and IPMX networks are different they both have the common requirement that monitoring is essential for ensuring the reliability, performance, and efficiency of IP-based media transport. Here are the key reasons why monitoring is crucial:

1. Ensuring Stream Integrity

SMPTE 2110 and IPMX separate video, audio, and metadata into different streams, making it vital to monitor each component for packet loss, jitter, and synchronization issues.

2. Maintaining Low Latency

SMPTE 2110 support live production environments that require ultra-low latency. Similarly low latency is critical for IPMX applications such as live presentations, conferencing, and digital signage. Monitoring helps detect delays or network congestion that could impact real-time operations.

3. Synchronization and PTP Monitoring

SMPTE 2110 relies on PTP for synchronization. Any deviation in timing can cause drift or loss of sync, affecting live broadcasts. IPMX allows for simpler timing methods and monitoring synchronization ensures that audio and video remain in sync, preventing lip-sync issues or dropped frames.

4. Troubleshooting and Fault Detection

Issues such as packet drops, incorrect stream configurations, and network congestion can disrupt broadcasts. Monitoring provides real-time alerts and diagnostic tools for quick troubleshooting.

5. Bandwidth Optimization

SMPTE 2110 and IPMX allow both uncompressed and compressed streams, which can

heavily impact network bandwidth. Monitoring helps optimize network usage, balance network load and prevent bottlenecks.

6. Security and Anomaly Detection

IP-based networks are vulnerable to cyber threats. Monitoring helps detect unauthorized access, unusual traffic patterns, and potential security breaches.

7. Scalability and Future-Proofing

As networks grow, continuous monitoring ensures scalability while maintaining performance, helping broadcasters plan for future expansions.

By actively monitoring SMPTE 2110 or IPMX networks, organizations can prevent disruptions, maintain high-quality service, and ensure a seamless transition to IP-based workflows.

SMPTE 2110 Monitoring Finds Intermittent Issue

A national broadcaster detected a video issue on their SMPTE 2110 network couldn't resolve since it occurred infrequently and seemed intermittent.

The broadcaster connected the PacketStorm VIP-Monitor (monitors video, audio, and ancillary streams) to their SMPTE 2110 network and the monitor detected the video issue. The VIP-Monitor has sixteen different alarm types with user settable thresholds. The monitor displays any flow issues on its top page (see Figure 1). The Red line indicates an error and the error was occurring approximately every fifteen hours or so.

Figure 1 – Flows Monitor Display

Upon detecting the error, the monitor logs and describes the error. The VPI-Monitor described the error as an invalid RTP Timestamp.

Upon detecting the error, the monitor captures fifty packets before and after the error (see Figure 3). The packet capture shows the RTP Sequence numbers are good but there is a five second interval between packets 49 and 50.

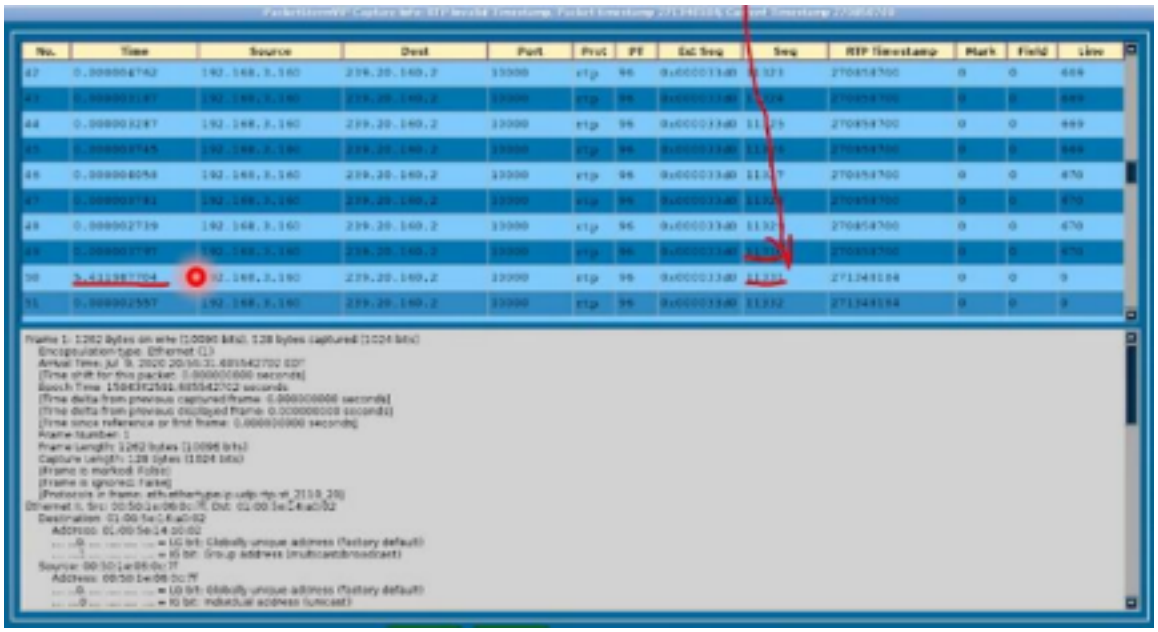

Figure 3 – Packet Capture before & after Error

There are three possibilities for causing errors: sender, network, and receiver. The monitor found flows with the same error from multiple senders which indicates the issue is mostly likely the network. The monitor acts as a receiver and detected the five second interval which means the receiver is not at fault. Upon debugging the network, it was discovered the PTP clock on a boundary clock switch would become unlocked once every fifteen hours or so. When the PTP clock became unlocked the sender would stopped sending flows until the clock came back.

About PacketStorm Communications

PacketStorm Communications, Inc. develops multiple media monitors, capture and replay systems, IP network emulators, and stream replicators. By developing proprietary hardware and software, PacketStorm has created test equipment that can be used to extensively test networking applications that are available today as well as future technologies that have yet to be deployed

PacketStorm is a privately held company founded in 1998 by a team of engineers and managers from the prestigious Bell Laboratories. With extensive backgrounds and experience in both network development and testing, PacketStorm continues to focus on the needs of IP developers and network managers. PacketStorm's world headquarters in New Jersey handles product engineering, marketing, and customer support.

Headquarters

PacketStorm Communications, Inc.

65 Oak Street

Norwood, NJ 07648

Phone: (732) 840-3871

Website

www.PacketStorm.com