Media Flow Analytics

Using the Cisco Nexus 9000 for media flow health monitoring

Isolate traffic problems on an IP network

The media and entertainment industry is undergoing a massive transformation. Content production is rapidly moving from standard definition to high definition and ultra-high definition and beyond. To adapt to these changes, media companies have moved their production infrastructures from serial digital interfaces (SDI) to IP.

Although IP offers advantages and opportunities for the industry, the nature of the architecture makes it more difficult to isolate problems when they arise. When video flow is affected, such as when a packet is lost, the viewer sees a disturbance on the screen, but doesn't know why. However, using a combination of hardware and software telemetry, the Cisco Nexus 9000 can help you isolate traffic problems on an IP network, so you can resolve them in seconds, instead of hours.

Contents

The move to IP

In the past, the broadcast industry used an SDI router and SDI cables to transport video and audio signals. SDI cables carry only a single unidirectional signal, so a large number of cables, frequently stretched over long distances, are required. However, with an IP-based infrastructure, a single cable has the capacity to carry multiple bidirectional traffic flows and can support different flow sizes without requiring changes to the physical infrastructure. Media companies are moving to an IP-based infrastructure to meet the demands for more content and rich media experiences, including more camera feeds, higher resolutions, and virtual reality capabilities. An IP network architecture makes production options such as live production in studio, stadiums, and remote production feasible.

Because SDI architectures offered one-to-one connections, it was relatively easy to detect the source of a problem. But with an IP infrastructure the cable is common, which affects problem detection. The lack of visibility into the flow health of IP networks is a serious concern in the industry. In fact, it's one of the reasons some media and entertainment organizations are reluctant to move their production workflows to IP. Media businesses need to be able to efficiently operate their IP networks and ensure reliability. If video flow is degraded, you need to be notified proactively or in real time to minimize the effect on viewers.

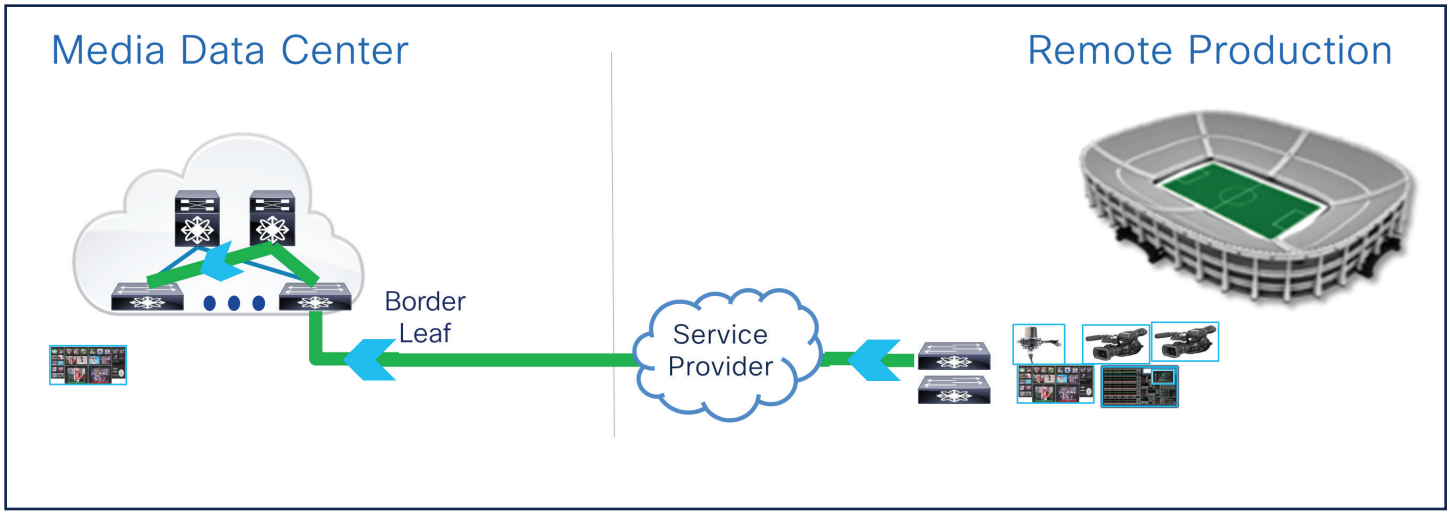
Operational challenges

Bad video on air is an operator's nightmare. Although IP networks are designed to ensure resiliency with multiple paths from source to destination, interface errors and drops are beyond an operator's control.

For example, suppose content that is captured at a stadium is transported to a production facility across a service provider network (see Figure 1). When a problem arises, it's difficult for the network operations team to pin-point the source of the problem. The network operator has complete control over the network in the production facility but may not have any visibility over the IP network in the stadium or the service provider.

If the video on screen goes bad because of packet loss, the loss could be happening at the stadium, at the service provider, or at the production facility itself. Isolating where the loss is taking place involves long hours of troubleshooting. Problems like these can lead to a loss of revenue and affect the entire business. Sometimes, the issue may disappear before troubleshooting is complete, which makes it impossible to determine the cause of the failure.

Figure 1. Remote production example

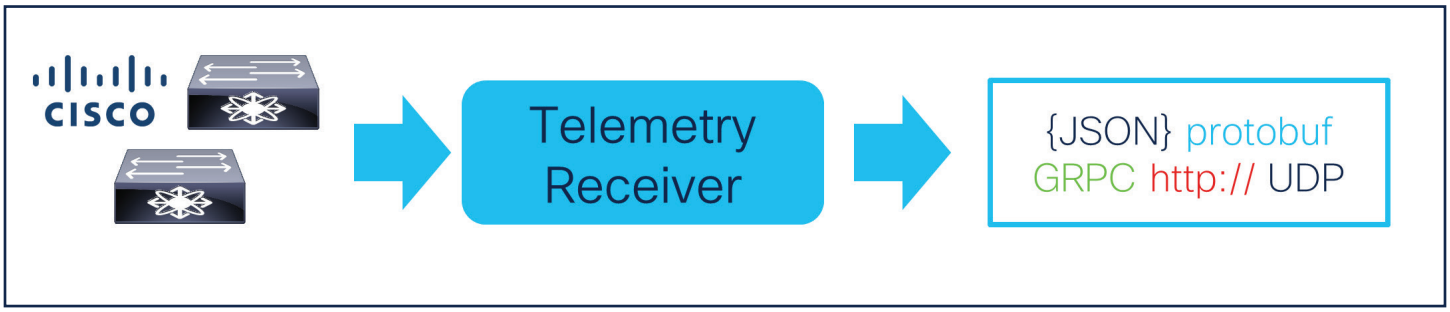


Telemetry with the Cisco Nexus 9000 and NX-OS

The traditional means of checking network health involved polling each network element for link errors, usage, and resource utilization. Because of the nature of periodical polling, often the information isn't captured in real time, so you can miss events that occur between polling intervals. The information returned from the network could indicate issues such as packet loss on an interface, but it never provided deeper insights into what traffic or application was affected.

Rather than polling the network, the Cisco Nexus 9000 uses hardware and software telemetry to proactively notify operators of traffic problems (see Figure 2). Because you find out about problems more quickly, this proactive notification can reduce the mean time for resolution from hours to seconds.

Figure 2. Hardware and software telemetry with Nexus 9000 and NX-OS

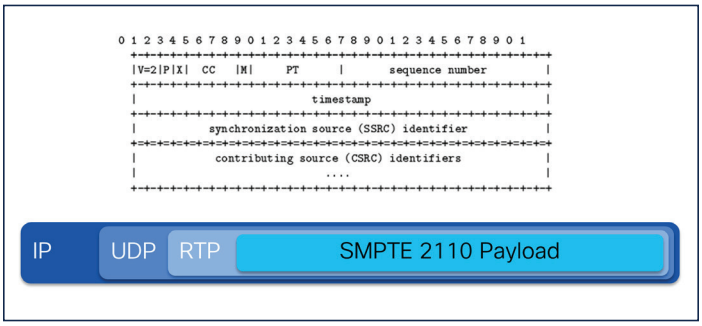


Flow health monitoring

Almost all of the applications where video is delivered over IP use real-time protocol (RTP) over UDP. These applications include uncompressed video such as ST2110, Aspen, or compressed video like MPEG and H.261. Each packet in an RTP flow has a sequence number from 0 to 65535 (see Figure 3). When the Nexus 9000 is used for video transport, it inspects every packet of every RTP flow that is traversing the switch. The flow table on the Cisco Cloud Scale application-specific integrated circuit (ASIC) powers the Nexus 9000. The Nexus 9000 switch is the first in the industry that can examine unsampled flow information. Using this feature, the Nexus 9000 can detect a gap in an RTP flow and generate an alert to notify the operator that packet loss has occurred.

The alert also includes the flow that was impacted, its IP address, and its UDP port. The alert can be sent to a syslog or be streamed using streaming telemetry to an external collector.

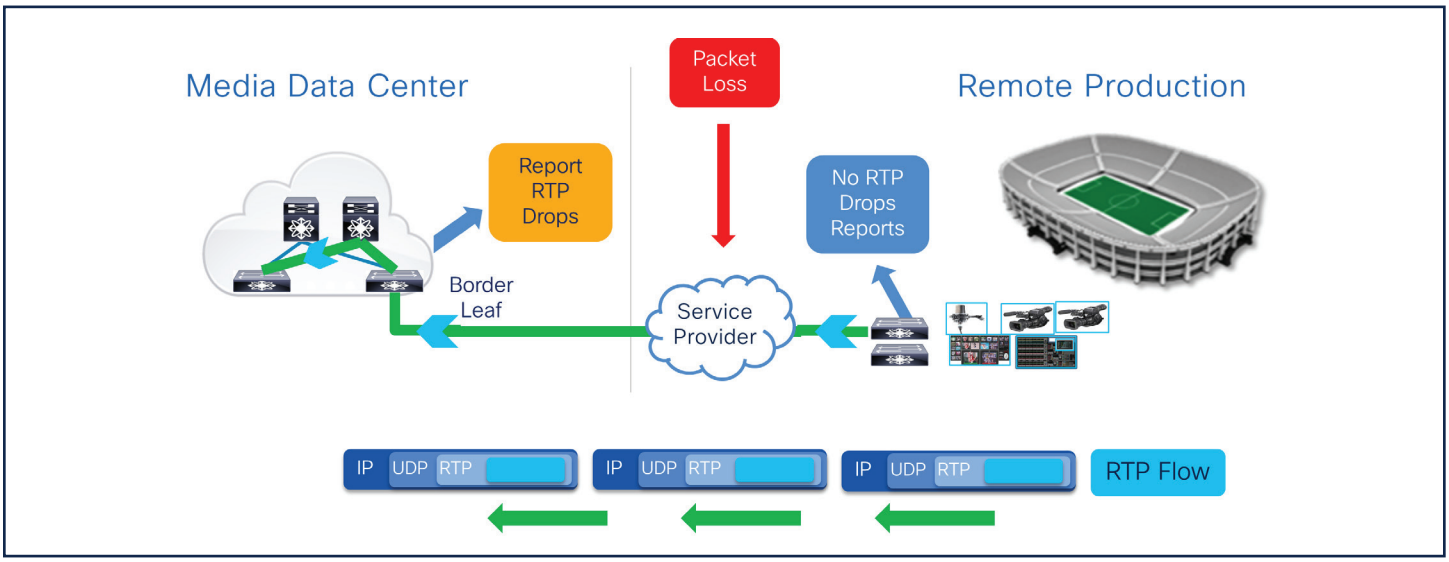
Figure 3. RTP header



Feature in action: remote production use case

In the remote production example described earlier, suppose the IP network has a Cisco Nexus 9000 at the stadium and one at the production network. When bad video appears on screen, the RTP flow analytics feature is activated and tells the operator where the issue is taking place. If the Nexus 9000 at the stadium reports no issues, but the Nexus 9000 at the production edge toward the service provider does report an issue, you can conclude that the service provider is dropping the packet. Tracking down and isolating a problem like this one no longer takes several hours of troubleshooting; it only takes a matter of seconds (see Figure 4). The capability is available on Nexus 9300-FX/FX2/FXP switches running NX-OS 9.3(1). For details on how to configure the feature, refer to the Media Flow Analytics configuration guide.

Figure 4. Detecting packet loss in real time



Learn more

To discover how you can move to IP while preserving the quality and robustness the media market demands, visit the IPFM use case page.

New architectures require new tools

As you transition your workflows to IP, you need new solutions. In the past, networks lacked the ability to provide granular information on flow health or the ability to see problems in real time. Cisco offers the media industry a reliable, scalable, and flexible network and provides the tools you need to efficiently operate that network. Cisco is uniquely positioned in the networking industry with intelligent ASICs that are complemented with innovative software.