Technical Disclosure Commons

Defensive Publications Series

August 28, 2019

DETECTING PACKET LOSS ON RTP STREAMS LEVERAGING CLOUD SCALE ASIC FLOW TABLES

Rahul Parameswaran

Ammar Latif

Roshini Paul

Sunil Gudurvalmiki

Sandeep Bharadwaj

DETECTING PACKET LOSS ON RTP STREAMS LEVERAGING CLOUD SCALE ASIC FLOW TABLES

AUTHORS:
Rahul Parameswaran
Ammar Latif
Roshini Paul
Sunil Gudurvalmiki
Sandeep Bharadwaj

ABSTRACT

A number of customers in, for example, the Service Provider segment, the Media and Entertainment industry, *etc*. use networks to transport audio and video signals. These audio and video signals include uncompressed video transported in accordance with the Society of Motion Picture and Television Engineers (SMPTE) ST 2110 standards, compressed video in accordance with the Moving Picture Experts Group (MPEG) standards, JPEG 2000 (J2K), *etc*., which may be User Datagram Protocol (UDP)/Real-time Transport Protocol (RTP) flows in a network.

Today, when there is packet loss, end customers/operators find it very difficult to determine where the packet loss is happening in the network as, at times, the flows traverse different geographic regions, different service providers, *etc*. The techniques presented herein leverage flow tables on vendor Cloud Scale application-specific integrated circuits (ASICs) to detect gaps in RTP flows (i.e., to detect RTP packet drops). As soon as RTP packet drops are detected, the networking device (e.g., switch with the Cloud Scale ASIC) can generate an alert notifying the end customer/operator of the packet loss, thereby enabling the end customer/operator to pinpoint exactly where the loss is occurring.

DETAILED DESCRIPTION

FIG. 1, below, is a schematic flow diagram illustrating conventional video troubleshooting. As shown, in conventional arrangements, the packet loss may occur anywhere in the network and the end customer/operator has no visibility as to where (i.e., at which networking devices) the packet loss is occurring. That is, today no network switches can detect loss at a per flow level. This is because most networking device ASICs only support sampled flow capture. The fact the flows are sampled means that data is lost

and, accordingly, so is the ability to detect granular packet loss. As such, when there is packet loss in conventional arrangements, an operator generally has to troubleshoot large portions of the network to identify the location of the packet loss. This can be a time consuming and tedious process.

Recently certain ASIC vendors have the ability to capture unsampled flow information, an example includes Cisco's Cloud Scale ASIC that is used in Nexus 9000 family of products. These Cloud Scale ASICs can inspect every packet of every flow (up to 24k per switch) and parse up to 128B of packet header to detect gaps in the RTP flows. As such, presented herein are RTP flow monitoring techniques that leverage the capabilities of Cloud Scale ASICs to detect gaps in RTP flows (i.e., detect RTP packet drops), including in uncompressed flows (e.g., SMPTE 2110-20) and in compressed flows (e.g., MPEG-4, H.264, *etc*.). As shown in FIG. 2, below, the RTP headers include a sequence number which can be used to track the packet loss.

FIG. 3 is a schematic flow diagram illustrating operation of the RTP flow monitoring techniques presented herein. As shown, an RTP flow can be transmitted from a source to one or more destinations via a network. In this example, the switches at a remote production site do not report any RTP packet drops. However, a border leaf switch at a media site reports RTP packet drops. With this reporting, the end customer/operator has data to indicating that the service provider is dropping packets, as well as data indicating exactly where this packet loss is occurring. As a result, the end customer/operator has direct visibility as to where (i.e., at which networking device(s)) the packet loss is occurring. FIG. 4 generally illustrates data that can be provided to end customer/operator upon detection of RTP drops (i.e., example RTP flow monitoring output).

FIG. 5 illustrates RTP flow monitoring with a network management platform, such as Data Center Network Manager (DCNM). That is, as shown, the networking devices with Cloud Scale ASICs can also stream the RTP flow monitoring (RTP packet drops) to an external controller, such as the DCNM Media controller, where an operator can visualize where the loss is occurring. The DCNM overlays the end to end path of flow and the point in the network where loss is detected can be immediately pinpointed, thereby reducing the time spent on troubleshooting flow loss from, for example, several hours to several seconds.

In summary, presented herein are RTP flow monitoring techniques that leverage flow tables on vendor cloud ASICs to detect gaps (packet loss) in RTP flows. As soon as gaps are detected, the networking device generates an alert to notifying an operator of the RTP packet loss, thereby enabling the operator to pinpoint exactly where the packet loss is occurring.

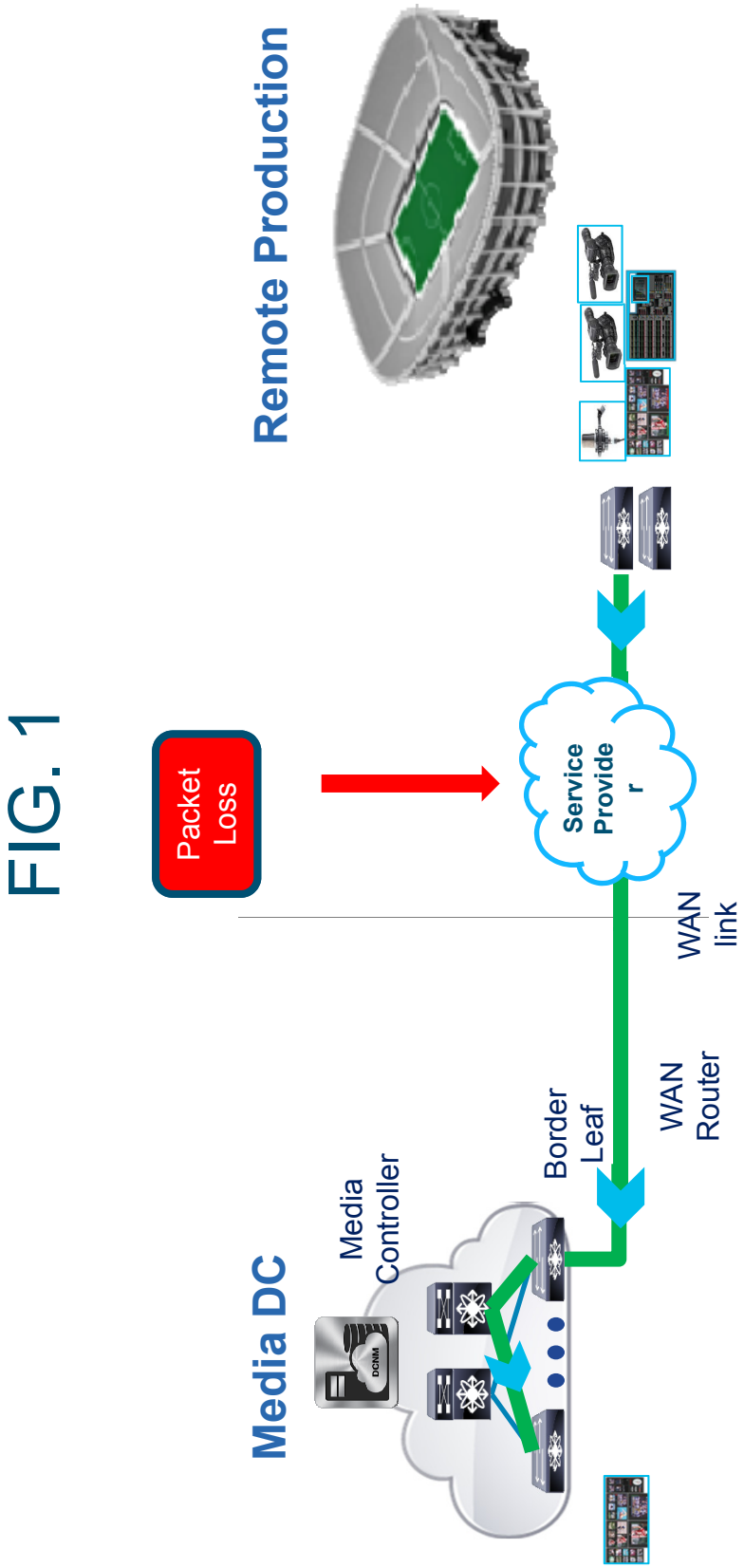
Remote Production
Packet Loss
Service Provide r
WAN link
WAN Router
Border Leaf
Media Controller
Media DC
DCNM

FIG. 1

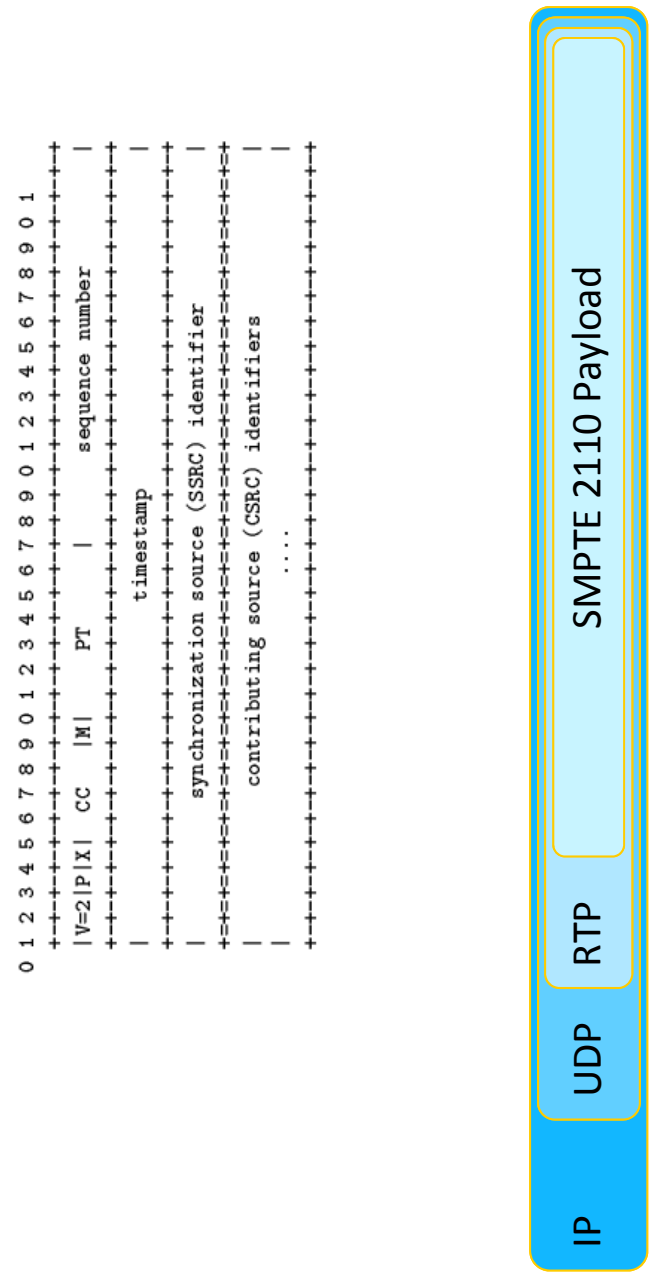
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|V=2|P|X| CC |M| PT | sequence number |
timestamp
synchronization source (SSRC) identifier
contributing source (CSRC) identifiers
....
IP
UDP
RTP
SMPTE 2110 Payload

FIG. 2

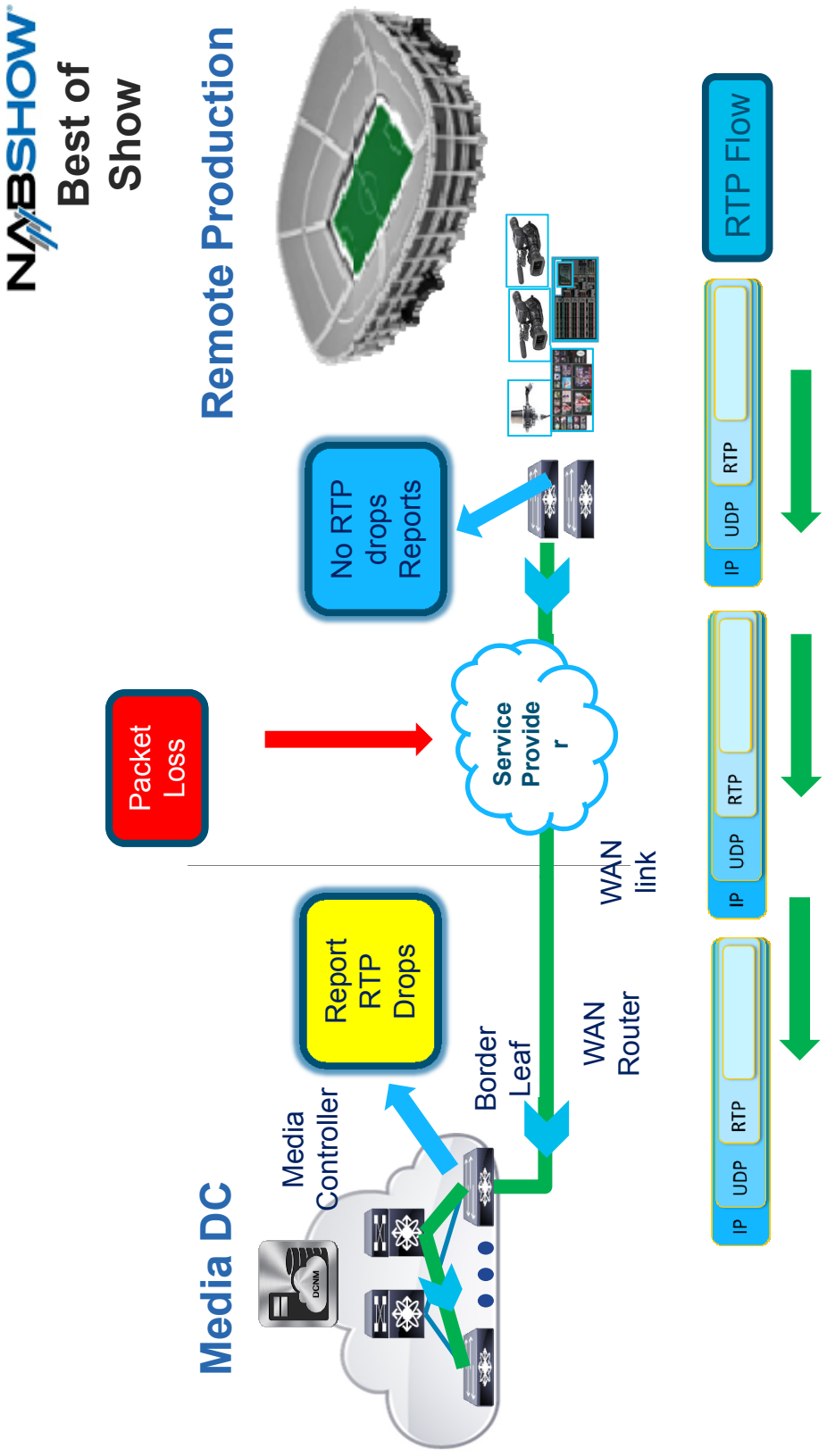
NABSHOW
Best of Show
Remote Production
Media DC
Media Controller
DCNM
Border Leaf
WAN Router
WAN link
Service Provide r
Packet Loss
Report RTP Drops
No RTP drops Reports
RTP Flow
IP
UDP
RTP

FIG. 3

FIG. 4

```
!Configuration
feature netflow
ip flow rtp
```

```
show flow rtp details  -- Displays all active flows detected by the ASIC

RTP Flow timeout is 1440 minutes
IPV4 Entries
SIP             DIP             BD ID   S-Port  D-Port  Intf/Vlan Name      Packet Count     BytesPerSec  FlowStart
192.168.21.2    239.20.13.1     4139    5500    20000   Ethernet1/34        181699102492     157943157    22:25:08 UTC May 22 2019
192.168.100.164 239.101.160.22  4138    50000   20000   Ethernet1/33        41719636319      76983505     06:21:29 UTC May 30 2019
192.168.21.2    239.30.21.1     4141    5500    20000   Ethernet1/36        1388462946       299999       22:25:10 UTC May 22 2019
192.168.21.2    239.40.21.1     4141    5500    20000   Ethernet1/36        84118756         30686        22:25:11 UTC May 22 2019
```

```
show flow rtp errors active - Displays flows currently impacted

RTP Flow timeout is 1440 minutes
IPV4 Entries
SIP             DIP             BD ID   S-Port  D-Port  Intf/Vlan Name      Packet Count     BytesPerSec  FlowStart                Packet Loss Loss Start              Loss End
192.168.21.2    239.20.13.1     4150    5500    20000   Ethernet1/50        99709154952      157932128    06:21:22 UTC May 30 2019 56853       04:18:34 UTC Jun 08 2019 N/A
```

```
Leaf1# show flow rtp errors history -- Displays historic information of flows that where impacted and the time of impact (24hr on box history)

RTP Flow timeout is 1440 minutes
IPV4 Entries
SIP             DIP             BD ID   S-Port  D-Port  Intf/Vlan Name      Packet Count     BytesPerSec  FlowStart                Packet Loss Loss Start
Loss End
192.168.21.2    239.20.13.1     4150    5500    20000   Ethernet1/50        99713271686      157931882    06:21:22 UTC May 30 2019 307773      04:18:34 UTC
Jun 08 2019  04:19:02 UTC Jun 08 2019
192.168.21.2    239.20.13.1     4150    5500    20000   Ethernet1/50        97761927229      157931915    06:21:22 UTC May 30 2019 27295       00:07:48 UTC
Jun 08 2019  00:07:48 UTC Jun 08 2019
```

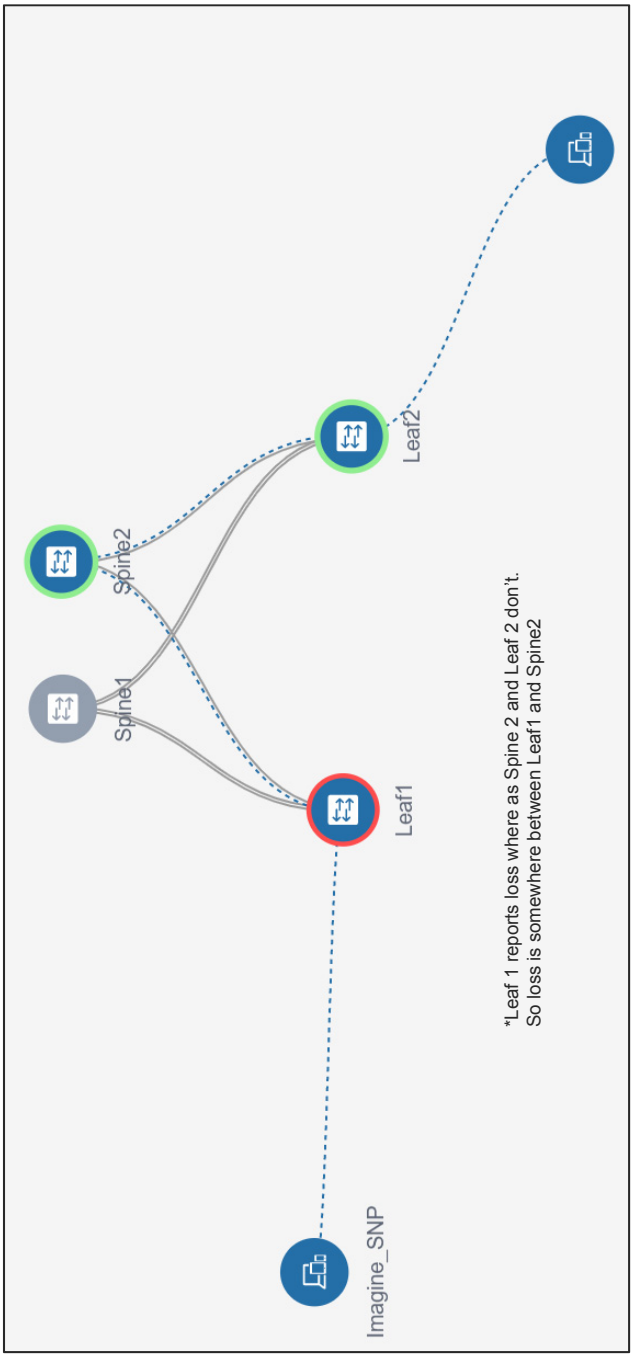
Spine2
Spine1
Leaf2
Leaf1
Imagine_SNP
*Leaf 1 reports loss where as Spine 2 and Leaf 2 don't.
So loss is somewhere between Leaf1 and Spine2

FIG. 5