SCTE | STANDARDS

Network Operations Subcommittee

SCTE STANDARD

SCTE 168-7 2017 (R2021)

Recommended Practice for Transport Stream Verification in an IP Transport Network

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards and Operational Practices (hereafter called "documents") are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interoperability, interchangeability, best practices, and the long term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE members.

SCTE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

NOTE: The user's attention is called to the possibility that compliance with this document may require the use of an invention covered by patent rights. By publication of this document, no position is taken with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from the standards developer. SCTE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE web site at https://scte.org.

140 Philips Road
Exton, PA 19341

Document Types and Tags

Document Type: Specification

Document Tags:

☐ Test or Measurement	☐ Checklist	☐ Facility
☐ Architecture or Framework	☐ Metric	☐ Access Network
X Procedure, Process or Method	☐ Cloud	☐ Customer Premises

Document Release History

Release	Date
SCTE 168-7 2010	*3/15/2010*
SCTE 168-7 2017	*6/5/2017*

Note: Standards that are released multiple times in the same year use: a, b, c, etc. to indicate normative balloted updates and/or r1, r2, r3, etc. to indicate editorial changes to a released document after the year.

Note: This document is a reaffirmation of SCTE 168-7 2017. No substantive changes have been made to this document. Information components may have been updated such as the title page, NOTICE text, headers, and footers.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1.0 SCOPE

This Recommended Practice is to give guidance about detecting errors in the IP Transport network used for the delivery of media services including Video and Audio streams of data with the associated control information to provide MPEG transport through an IP network. The IP Transport Layer operates in conjunction with other Application and Physical component layers that could also generate network impairments, this document will focus on the effect these impairments have on the detection of the cause of problems in the delivery of media services. Common IP network events and failures are characterized with their impact on the MPEG transport stream in a functioning system. Every network layout is different and presents unique configuration challenges; this document does not provide guidance on configuration of the network but does provide background information on the individual components of the IP network as well how the IP transport network operates in a multimedia network.

This document describes the protocols within the IP network and the possible IP layer causes of media impairments but does not provide metrics that correlate specific IP failures to media impairments. Industry accepted metrics have been provided for IP packet loss, delay and jitter.

This background on the IP network layer provides guidance to operators who are planning to deploy or are currently deploying MMM systems and, where appropriate, refers to other SCTE documents that provide supplemental information about other network components outside of the IP Transport Network.

2.0 INFORMATIVE REFERENCES

The following documents may provide valuable information to the reader but are not required when complying with this standard.

2.1 SCTE References

[1] SCTE 142, Recommended Practice for Transport Stream Verification

[2] SCTE 168-6, Recommended Practice for Monitoring Multimedia Distribution Quality

2.2 Standards from other Organizations

[3] IEEE 802.3, Ethernet protocol family

[4] IETF RFC 791, Internet Protocol

[5] IETF RFC 2460, Internet Protocol Version 6 (IPv6) Specification

[6] IETF RFC 3031, Multiprotocol Label Switching Architecture

[7] IETF RFC 2236, Internet Group Management Protocol version 2 (IGMPv2)

[8] IETF RFC 3376, Internet Group Management Protocol version 3 (IGMPv3)

[9] IETF RFC 2710, Multicast Listener Discovery (MLD) for IPv6

[10] IETF RFC 3810, Multicast Listener Discovery Version 2 (MLDv2) for IPv6

[11] IETF RFC 4445, A Proposed Media Delivery Index (MDI)

[12] IETF RFC 2328, OSPF Version 2

[13] IETF RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments

[14] IETF RFC 1771, A Border Gateway Protocol 4

[15] IEEE 802.1d, Spanning Tree Protocol

[16] IETF RFC 3209, RSVP-TE: Extensions to RSVP for LSP Tunnels

[17] IETF RFC 3036, LDP Specification

[18] IETF RFC 2679, A One-way Delay Metric for IPPM

[19] IETF RFC 2362, Protocol Independent Multicast-Sparse Mode

[20] IETF RFC 3973, Protocol Independent Multicast - Dense Mode (PIM-DM)

[21] IETF RFC 2463, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)

3.0 DEFINITIONS AND ACRONYMS

ASM – Any Source Multicast

DSCP – Differentiated Service Code Points

EGRESS – Network traffic that is sent out of a router port for a destination outside of the router.

IGMP - Internet Group Management Protocol

INGRESS – Network traffic that originates from outside of a router which is processed by the router.

MLD - Multicast Listener Discovery

Policer – Policing, or rate limiting, enables you to limit the amount of traffic that passes into or out of an interface.

RTP – Real Time Protocol

SSM – Source Specific Multicast

4.0 INTRODUCTION

One of the challenges to detecting errors in the transport of MPEG streams is that these packets are carried in UDP, which is essentially connectionless. In order to determine that there is a failure there has to be a known metric by which to measure the traffic. In an IP Network there are specific network events that could lead to impairments or service degradation that would cause a perceived problem for the end user of a specific service such as watching a Video On Demand television program.

Work has been documented in SCTE 142 [1] to detail media impairment severity levels specific to the connection between the emission remultiplexer and the QAM modulator.

Recommended Practice SCTE 142 specifically refers to the MPEG Transport Stream and is independent of the underlying distribution system. Rather than using traditional ASI transport technologies, MPEG2 Transport Streams can be carried between the Head End System and a downstream Modulator over an IP-based network infrastructure such as that shown in Figure 1 with a simplified network view shown in Figure 2. When a packet network is used as the distribution system it could be non-deterministic and may cause errors that are reported at the transport stream layer when the SCTE 142 Recommended Practice has been implemented.

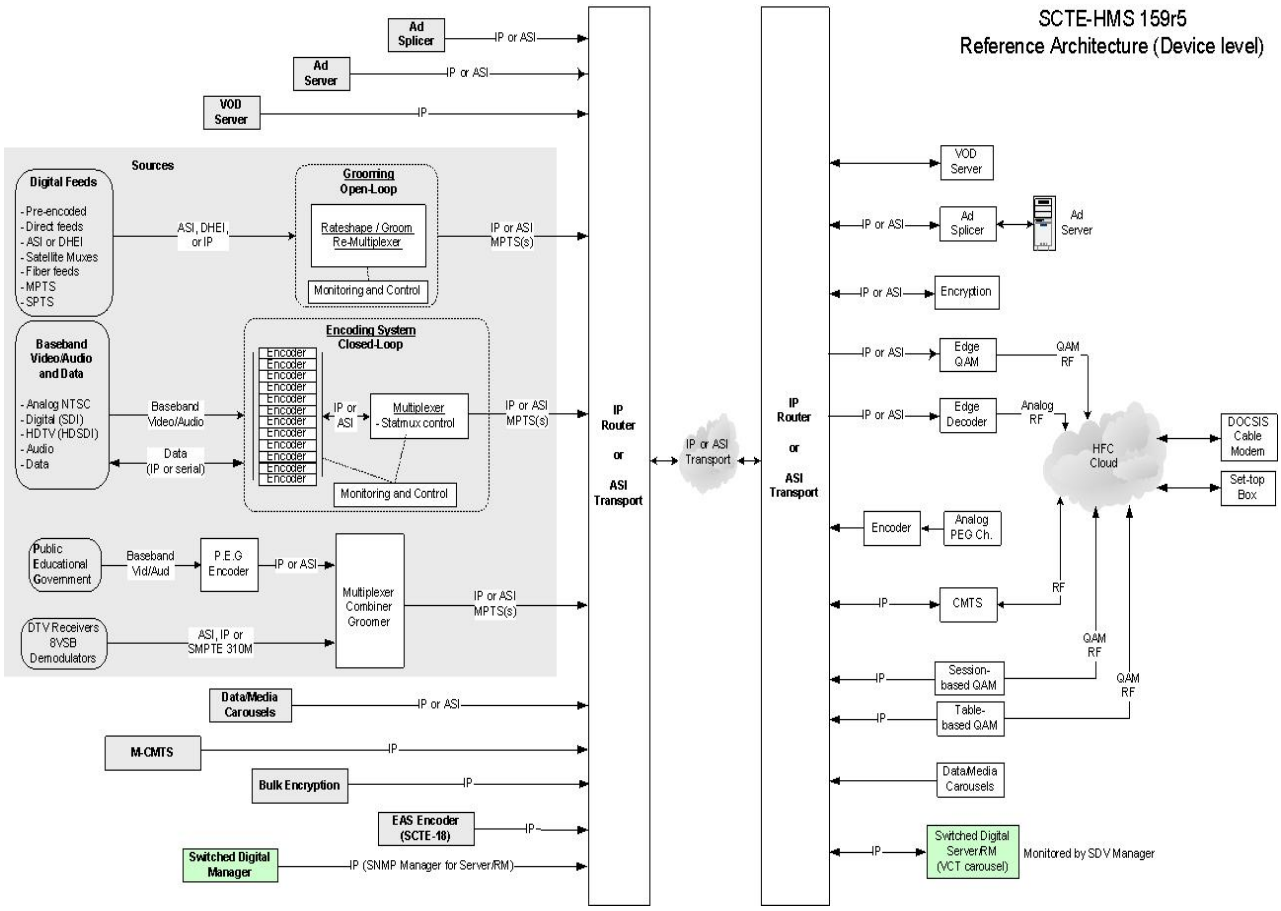

Figure 1 – Representative Cable Architecture

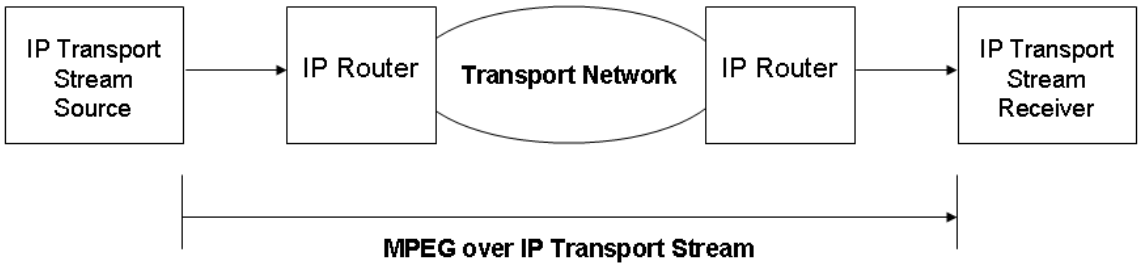

Figure 2 – Simplified View of IP Transport Network

To ensure a deterministic model for the packet network, the network must adhere to a set of IP metrics that induce little or no impact to the MPEG transport stream being carried across the network.

Because the type of media data in any given IP packet varies widely the effects of a single lost IP packet will vary. Most deployed networks do not prioritize specific packets based on content or handle packets with different content differently, and since any IP packet is expected to carry any mix of video, audio, or control information (PSI/SI tables), a single

packet loss might affect video, audio, or the ability of a decoder to make sense of the data being received. With every packet loss carrying the likelihood for audio and/or video corruption, it is critical that an operator be able to detect all packet losses on all flows throughout the network and be able to determine when and where such losses occur for quality assessment and fault isolation maintenance.

However, even though every IP packet loss is important to identify it is almost impossible to determine what type of media data was lost with that packet and thus very difficult to map a failure in the IP network to a specific MPEG error classification.

5.0 CHARACTERISTICS OF THE IP NETWORK

The IP network is fundamentally segmented into two functional layers as shown in Figure 3 below:

- Control Plane: The route processing used to create a forwarding topology across the end-to-end network allowing each node to make autonomous per-packet forwarding decisions for a packet to reach its destination. This plane consists of routing protocols such as BGP[14], OSPF[12], ISIS[13], and PIM[19,20]. This plane can also consist of RSVP-TE[16] and/or LDP[17] label switched paths (LSP).

- Forwarding Plane: The forwarding engine used in each node to bring a packet into the router, perform a route lookup to determine the egress interface(s), and provide other per-packet functions such as filtering, QoS, and accounting before sending the packet out the egress interface(s).

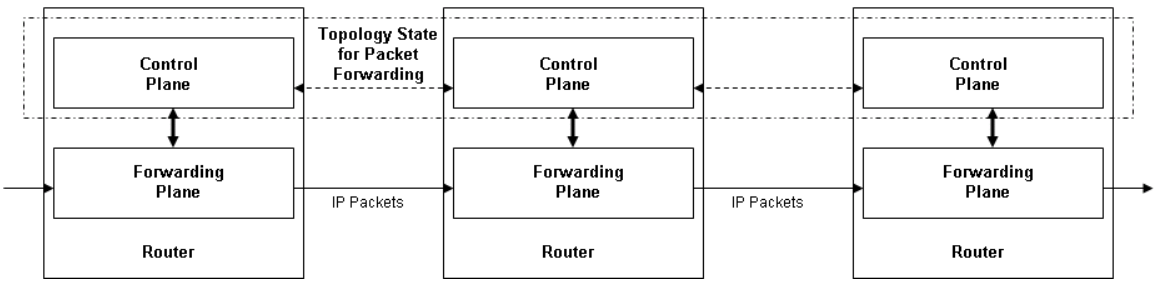

Figure 3 – Control and Forwarding Planes

A packet-based network makes use of two fundamental types of IP transport models: unicast and multicast.

* There is also a unique type of packet called a Broadcast packet which is not used specifically in the delivery of media packets.

Unicast is a single destination model where the destination address denotes the end receiver and is matched to a single next-hop egress interface. Unicast addresses are used for one-to-one communication. Multicast is a one-to-many model where the destination address is not the end receiver, but instead denotes a multicast distribution tree with one or more egress interfaces. Unicast and multicast, however, both contain a forwarding plane and control plane even though they are unique in terms of routing topology creation and packet forwarding. Correct network setup and addressing schemes are basic network configuration concepts that are outside the scope of this document, but are required for the correct transport of packets.

6.0 CONTROL PLANE CHARACTERISTICS

The router control plane creates a network topology map defining one or more egress interfaces for each packet. Defined egress data is then pushed down to the forwarding plane and is updated as the network topology changes. Topology changes can occur due to planned configuration changes or due to hardware failures in the network.

Well-known protocols such as OSPF, ISIS, BGP, and PIM are typical examples of the router control plane. For Ethernet switching, the Spanning Tree Protocol (STP) is a prime example of an Ethernet control plane protocol. Other protocols such as RSVP-TE and LDP may be used in MPLS network to create an end-to-end label switched path (LSP).

Since the forwarding plane depends on the state of the control plane, the control plane plays a major role in packet forwarding. The inability to match a destination address for a received packet will result in the packet being discarded, if a default router for non-matching entries is used, or possibly sent out an incorrect interface. It is critical to ensure that the control plane state matches the desired topology and forwarding behavior in the network.

Metric violations created by the control plane may inadvertently be attributed to the forwarding plane. Packet loss is a key example where routing entries do not exist for a specific destination resulting in packet discards. Thus control plane metric violations should be defined separately from forwarding plane packet drops that may occur due to a faulty interface or interface congestion.

6.1 Unicast Routing and Topology Control Plane

The network topology typically is based on the determination of connection paths by routing protocols for IP routing. Examples of routing protocols are OSPF [12], ISIS [13], and BGP [14]. These protocols are used to create forwarding entries for each IP subnet mapping to a next-hop or egress interface. If a packet enters the router and a lookup fails due to absence of a routing entry, the packet can be dropped or forwarded out an incorrect interface. Packets also could be forwarded out the incorrect interface if the ultimate route is lost from the routing table but a less specific route's next-hop is another interface.

Other types of topology control plane protocols such as spanning tree [15], RSVP_TE [16] and LDP [17] for MPLS [6] can impact path creation within the network resulting in packet forwarding error conditions.

The typical use case for unicast routing in a media network is for the delivery of video on demand services. Video Servers and Resource Managers communicate over the IP network.

6.2 Multicast IGMP Control Plane

Receiver membership to a multicast tree is based on IGMP for IPv4 [7,8] or MLD for IPv6 [9,10,21]. *IGMP* is used as the general term for the multicast control plane protocol. IGMP consists of reporting messages termed *join* for requesting to be part of a multicast tree or *leave* when requesting to end membership to a multicast tree.

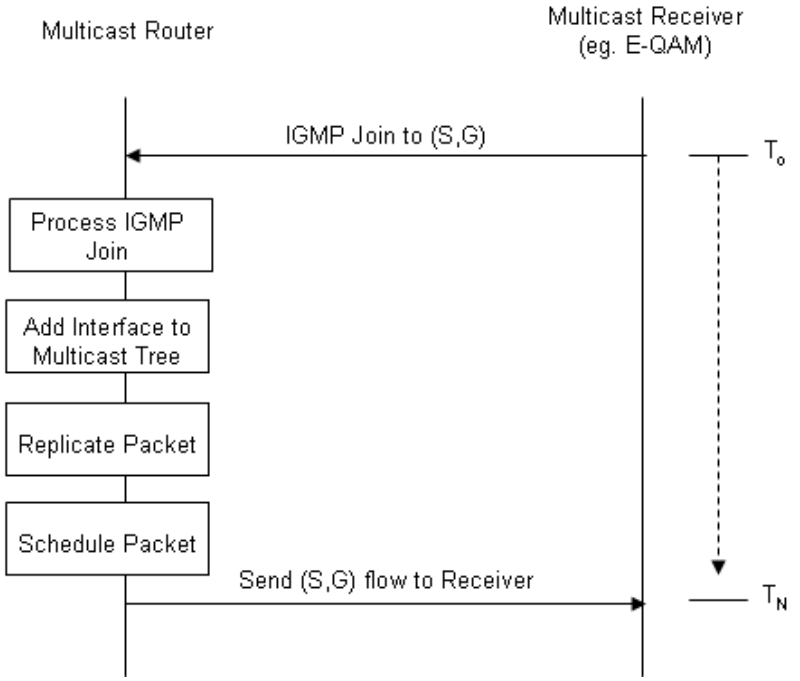

Figure 4 – Simple Model of an IGMP SSM Control Plane

Figure 4 shows a basic model for a multicast IGMP *join* sent between a multicast receiver and multicast router. There is a finite time delay between the receiver sending a *join* and the receiver receiving the multicast data stream. The time delay between these two events can impact the amount of time for a channel change event to occur and should be minimized.

The time delay can approach infinity if the IGMP *join* is not processed properly such that replication out an interface does not occur. This type of error condition will result in a perceived service outage.

For ASM deployments, the model is the same except that (*,G) messages are passed between the receiver and router instead of (S,G). In this case the receiver only requests the group address and will accept multicast traffic destined to that group from any multicast source.

6.3 Multicast PIM Control Plane

Router-to-router multicast tree construction is based on PIM as the multicast routing protocol. As with IGMP, PIM consists of reporting messages that will be termed *join* for requesting a branch to be added a multicast tree or a *prune* when requesting to remove a branch from the multicast distribution tree.

PIM requires both the formation of a neighbor relationship between routers and continue keep-alive *hello* messages to validate the existence of the neighbor.

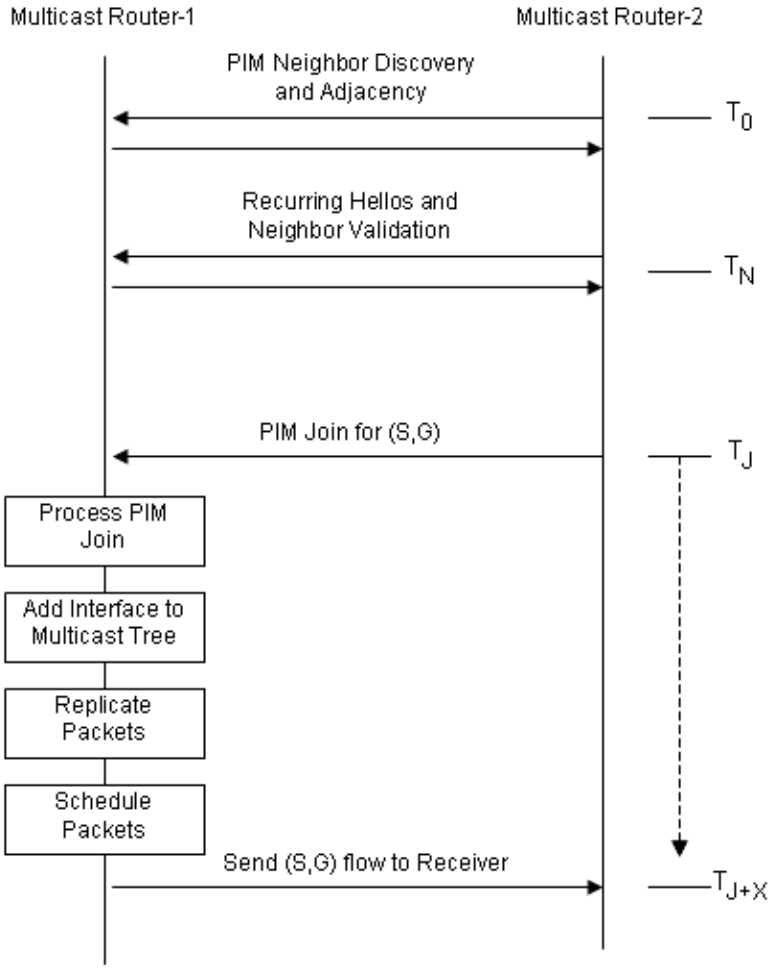

Figure 5 – Simple Model of a PIM SSM Control Plane

For proper creation of the multicast distribution tree within the network, all three stages of PIM are required:

1. Establish neighbor adjacency
2. Send and receive *hello* messages to/from each neighbor
3. Process PIM *join* messages per multicast group

This model is specific to SSM traffic. For ASM, a Rendezvous Router (RP) is used to construct the network topology. A (*,G) *join* is sent to the RP which has (S,G) entries. The RP will then forward the group(s) to the multicast router. Once the multicast router receives the (S,G) multicast groups it can then issue (S,G) *joins* towards the source to optimize the multicast tree.

7.0 FORWARDING PLANE CHARACTERISTICS

The forwarding plane role in each IP Router receives a packet, determines the output interface(s) of the packet, and sends the packet out that egress interface(s). This is not done on a stream-by-stream basis but packet-by-packet. The forwarding decision is made using a unique destination identifier in the packet header and may be based on various technologies such as Ethernet [3], IP [4,5], or MPLS [6] along the network path. The creation of the forwarding topology is dependent on the control plane protocols as discussed in Section 6.

For unicast delivery a single copy of the packet is received and ultimately sent out of the network node as shown in Figure 6. For multicast a single copy is received and the network node is responsible for making copies of, or *replicating*, the packets out the interfaces that are part of the multicast distribution tree.

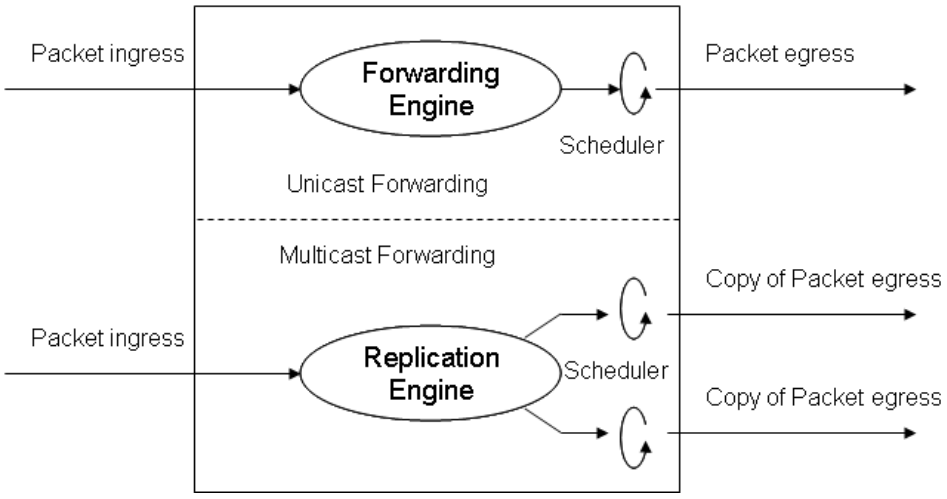

Figure 6 – Simple Model of a Node Forwarding Plane

The forwarding engine can provide functionality such as route lookups, packet filters, rate shaping, and other packet related requirements. The forwarding plane can impact the higher level transport stream by dropping packets (loss), adding delay between

ingress and egress (latency), having variable latency (jitter), and possibly reordering or duplicating packets. The larger the multicast tree, the more impact on the forwarding device. These impacts will be product specific.

7.1 Forwarding Plane Functional Layers

The forwarding plane itself can be broken into various layers each with various metric components or potential media impacts as shown in Figure 7. At the highest level, the network is portrayed as a single end-to-end system transporting the video. In reality, the network is comprised of per-hop nodes, each with physical link connectivity to adjoining nodes.

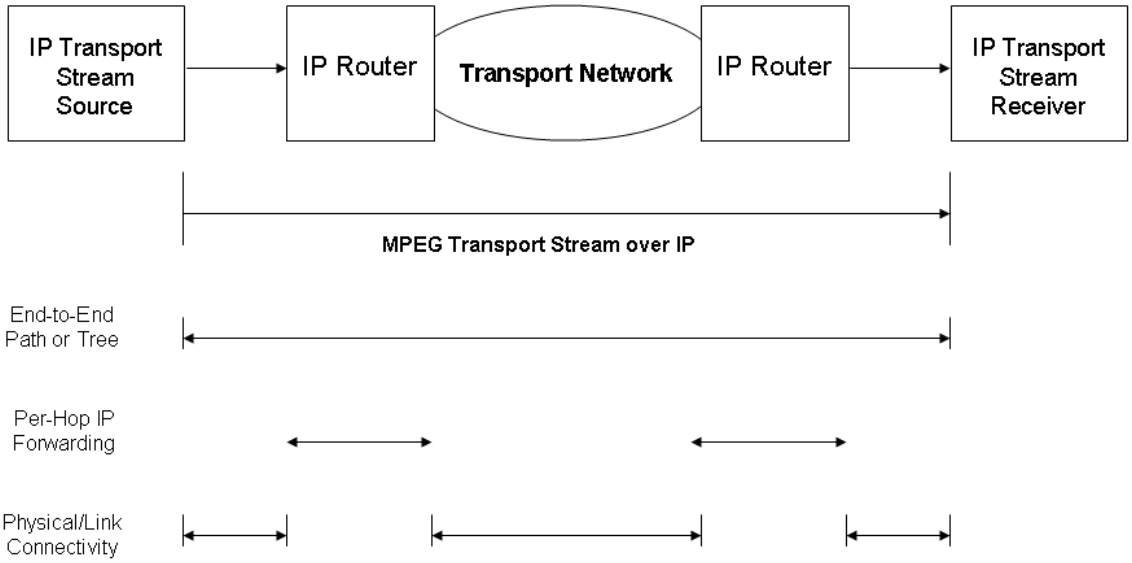

Figure 7 – Coupled Layers in the IP Transport Network

The network must be characterized as discrete layers to understand metric requirements per layer. Inherent coupling between layers can cause a lower layer fault to potentially impact higher layer functionality whereas higher layer faults are typically non-impacting to lower layers.

Metrics for the forwarding plane can be considered per bit (BER values) or per packet (PER) and can be measured per link, per router, or per end-to-end system. More specific information is contained in section 9.1.

7.2 IP Connectivity

In an IP network special treatment can be applied to packets at the router to limit the rate at which they are sent or received, if they are forwarded or dropped and if they are given priority over other packets within the router before they are forwarded.

An IP policer can limit the rate at which the IP packets are sent or received and as such can introduce network delay and jitter into the MPEG Transport Stream if the parameters of the policer are set inappropriately or exceeded.

Filters can be applied to IP packets for many reasons. Examples include filter based forwarding to override the route table, dropping all packets originating from a specific source or even something as insignificant as merely counting the packets. IP filters can cause many unintended consequences in the IP network that may cause impairments to the media stream.

DiffServ Quality of Service (QoS) provides a mechanism for classifying and managing traffic within the router by queuing and forwarding packets based on the DSCP code bits in their IP header. Generically these queues can be classified as best-effort (BE), Assured Forwarding(AF), and Expedited Forwarding (EF). Based on their header information the router can forward some packets before others based on their header information. Too many of one traffic type could keep the other queues from emptying. Misclassifying the video stream can introduce into the network potential IP delay, jitter and packet loss.

There are other QOS protocols such as RSVP that may impact the delivery of the media service in an IP network.

It is important to note that an IP router may be exhibiting the correct behavior and yet cause transport failures. This could stem from a misconfigured router or another device on the network. For example, if an IP packet with a TTL set to 2 ingresses a network with multiple hops, after that packet is forwarded two hops it will always be silently discarded before reaching its ultimate destination.

Specific thresholds for IP connectivity issues are given in section 8.

8.0 METRICS CHARACTERIZATION

The IP infrastructure does not distinguish between different types of media packets or have awareness of the payload information contained within each media packet. Therefore there is typically no correlation between a network element transient impairment and a particular impact to the higher layer TS payload.

The error characterization of the network layer is limited to the following metrics that, when they occur or exceed a boundary value, may in turn result in impairments to the transported media streams. These metrics can be impacted by Physical Connectivity, Forwarding Plane, or Control Plane characteristics.

Table 8.1 Network Level Metrics and Impacts

Metric Name	Description	Physical Link	Forwarding Plane	Control Plane
Packet Loss	Packets Sent- Packets Received	X	X	X
Delay	Latency (ms)	X	X	X

Delay Variation	Jitter (ms)		X	
Packet Sequence Violation	Packet reordering or duplication		X	
IGMP Control Plane Delay	IGMP Join/Leave latency (ms)			X
Failed Multicast Replication	Packet not replicated out interface		X	X

8.1 Packet Loss

Packet loss is measured as a packet that is not forwarded across the network. Loss can occur due to node congestion resulting in queue drops within an interface scheduler, corrupted packets, packet filters/firewalls, and routing black holes among other issues. Loss can also occur due to improper configuration of the network elements or due to lower layer impairments.

Loss has the most direct impact to Transport Stream quality. The magnitude of the perceived video and/or audio impairment is proportional to the number of packets lost and the particular video, audio, and/or control information in the packets' payload.

Ideally within the IP transport network, no packet loss should occur. Therefore any packet loss can be considered as an error condition.

In special cases, the media layer is able to recover from packet loss conditions where the network sees loss but the end user does not experience any degradation in media quality. One technique is forward error correction (FEC) to allow the media receiver to recover from loss conditions. Another is active-active (redundant) transport of the media stream over diverse network paths to a receiver that is capable of monitoring each stream and using the stream that does not have quality impairments. Since these recovery techniques occur at the application layer, they are beyond the scope of network transport metrics' discussion.

Since packet loss is a primary cause of media impairments, Appendix A is used to define common network level impairments that can result in media packet loss.

Without RTP, or other means to detect packet sequence, packet loss is immeasurable without analyzing the MPEG header, within the IP packet payload, described in 168-6 [2]

The following table from SCTE 168-6 (formerly HMS-168-6) [2] details acceptable metric thresholds for the cable environment.

Compression Type	**Resolution (bitrate)**	**Max Error Frequency**	**Max # IP Packets Per single Error**
MPEG 2	SD	1 per Hour	7 IP packets

MPEG 2	HD	1 per 4 Hours	27 IP packets
MPEG 4 AVC/VC1	SD	1 per Hour	5 IP packets
MPEG 4 AVC/VC1	HD	1 per 4 Hours	17 IP packets

8.2 Delay and Delay Variation

Delay can be measured as one-way (latency) and two-way (roundtrip delay) within the network. Latency can impacted by geographical distance, node forwarding delays, network congestion, among others. The variation between latency values is also termed jitter. IP Jitter is typically introduced by the variation of the processing time of a packet within the router and is also introduced due to node congestion and varying queue hold times. Network events that cause excessive IP control plane traffic may cause media packets to be queued longer due to the higher priority of control packets. Link failure on a router causing a reroute may cause the media stream to traverse a longer path through the network, thus inducing delay in the IP packet or IP packet loss if the new path does not provide end-to-end connectivity.

Delay may not have any impact on the quality of a media stream but can impact service quality for 2-way interactive services such as VoD pause and rewind.

IP Jitter can impact stream quality if jitter values exceed the accepted values used for device buffer management.

Further information for one-way delay can be found in RFC 2679[18].

The following tables, taken from SCTE 168-6 (formerly HMS-168-6) [2], provide recommended thresholds for IP delay and jitter. The Loss Distance and IP Video Stream Packet Loss Rate columns are not germane to this discussion.

Transport Stream bit rate (Mbps)	***Latency***	***Jitter***	***Loss Distance***	***Corresponding Average IP Video Stream Packet Loss Rate***
SD/MPEG 2 *3.75 Mb/s*	*<200 ms*	*<50 ms*	*1 error event per hour*	*<=7.8E-07*
HD/MPEG 2	*<200 ms*	*<50 ms*	*1 error event per 4 hours*	*<=4.9E-08*

15.0 Mb/s				
SD/MPEG 4 *2.0 Mb/s*	*<200 ms*	*<50 ms*	*1 error event per hour*	*<=1.5E-06*
HD/MPEG 4 *8.0 Mb/s*	*<200 ms*	*<50 ms*	*1 error event per 4 hours*	*<=2.4E-08*

Recommended Minimum Transport Layer Parameters for Satisfactory QoE for SD and HD services for cable

This can be still further simplified as shown below:

Transport Stream bit rate (Mbps)	***Loss Distance***
SD/MPEG 2 *3.75 Mb/s*	<24 errored Seconds / day
HD/MPEG 2 *15.0 Mb/s*	<6 errored Seconds / day
SD/MPEG 4 *2.0 Mb/s*	<24 errored Seconds / day
HD/MPEG 4 *8.0 Mb/s*	<6 errored Seconds / day

8.3 Packet Sequence

It is possible for the IP infrastructure to reorder packets along the path between ingress and egress. This can occur within a single node or across the entire transport network if load sharing is allowed packet-by-packet and not stream-by-stream.

Packet duplication may also occur where the network sends multiple copies of a media stream to a receiver. As an example, multicast can send the same group address to a receiver from unique sources. Although not a violation of multicast transport, there may be application level errors upon receipt of multiple MPEG transport streams.

Unlike RTP and TCP, UDP does not have the ability to sequence. A data network can reconstruct out-of-order packets but due to the real-time nature of audio and video, MPEG2 TS packets arriving out of order are typically discarded.

8.4 IGMP Control Plane Delay

The speed of the router to process IGMP *join* and *leave* messages can resort in IGMP *join* and *leave* delay. The speed for processing *joins* can impact channel change delay in a switched media environment. Minimizing *leave* delay is critical in cases with limited network resources to rapidly open up capacity by removing an endpoint from a specific multicast tree.

Further information on channel change times is detailed in SCTE 168-6 (formerly HMS-168-6) [2], section 4.3.2.

8.5 Failed Multicast Replication

If a multicast tree branch is not formed and MPEG streams are not sent out an interface, this is a failed multicast replication. This could be due to a software error or a lost IGMP *join* message between the receiver and the router control plane.

9.0 MULTICAST EVENTS IMPACTING MPEG TRANSPORT STREAM

The following section details network events specific to multicast transport of MPEG transport streams. These events can be correlated to metric violations listed in the previous section such as packet loss, excessive latency, or IGMP join delay. In many cases these events are part of the normal processing of multicast in the network layer so no alarms are present. However, log events or MIB updates can be provided for offline forensics and fault correlation or converted to alarm conditions as needed.

9.1 List of Multicast Events within the Network

The events listed below use terms specific to IPv4 multicast but can be expanded to IPv6 as the technology becomes deployed.

MC-E1: Loss of Source: The router is no longer receiving traffic for a specific multicast group.

MC-E2: PIM Neighbor Event: A PIM event such as *prune*, *join*, or neighbor failure that has impacted the creation of the multicast distribution tree. In the case of a PIM neighbor event, multiple multicast groups can be impacted.

MC-E3: Packet TTL Expiration: An IP packet received with TTL (time to live) value that drops to zero along the path of the multicast distribution tree causing the packet to be dropped by the router as part of IP loop prevention.

MC-E4: Packet RPF violation: The RPF (reverse path forward) check against the source IP address fails causing the router to drop the multicast packet

MC-E5: IGMP version mismatch: The multicast receiver and router may be configured with different versions of IGMP not supporting backwards compatibility. An IGMPv3 receiver may also attempt to use SSM (source specific multicast) that is not supported by an IGMPv2 network.

MC-E6: RP failure: The event is catalogued when an RP outage prevents creation of the multicast distribution tree. In many networks the multicast tree can be rebuilt to a secondary RP but the failure should be captured since a momentary outage can occur.

MC-E7: Duplicate ASM Trees: When using Anycast multicast, it is possible for multiple sources to use the same multicast group address. This is a valid configuration, but when a receiver issues a *join* for (*,G) the receiver may receive multiple or duplicate application flows from two or more sources when only a single source is desired.

9.2 Impact of Network Events to the Media Layer

When a network event listed in the previous section occurs, the impact to the MPEG transport stream(s) can vary. The table below summarizes the severity of each event type.

Note: The table below gives impacts to packet flow for each multicast event but no direct correlation to SCTE-142 type error metrics. For example, extensive packet drops that result in Program Off Air (POA) can be caused by multiple network events in the control plane, IP forwarding, or physical link problem.

Table 9.1 Multicast Event Impacts

Event ID	Description	Impact	Recovery
MC-E1	Loss of Source	Multicast tree may exist but no packet counters are incrementing at ingress of the tree for one or more multicast groups	Ensure the source is transmitting multicast into the network with proper source and group configured
MC-E2	PIM Neighbor Event	The multicast tree cannot be formed between two adjacent PIM routing nodes resulting in a broken or sub-optimal multicast tree for all multicast groups requiring this branch	Validate that a PIM adjacency has formed between the two routing nodes and prune messages are accepted by the upstream router
MC-E3	Packet TTL Expiration	Packets are dropped within the multicast distribution tree due to TTL expiration of one or more multicast	Validate the TTL value at the video source and ensure sized to reach across all IP hops within the multicast distribution tree
MC-E4	Packet RPF violation	Packets are dropped at the ingress router for any multicast traffic coming from a source IP address that is not recognized as a valid reverse path subnet	Ensure the IP routing table is correct for the IP address of the multicast source or ensure the source address is configured properly
MC-E5	IGMP version mismatch	The interface connected to the multicast receiver will not be added to the multicast distribution tree since joins are not processed	Validate that the IGMP version numbers are correctly configured on the multicast routers and receivers. IGMPv3 is required for SSM (S,G) join requirements

MC-E6	RP failure	A multicast router cannot join to (*,G) tree(s) due to lack of communication with the RP. The RP is required for ASM trees since the router cannot join towards the source as with SSM implementations	Validate that the RP is receiving multicast groups with (S,G) entries and has a communication path to the multicast routers in the network
MC-E7	Duplicate ASM Trees	The multicast receiver is receiving multiple video streams or data sets for each (*,G) join creating an application layer failure	Validate that only a single (S,G) is sent into the (*,G) tree for each receiver. If multiple sources exist for a single (*,G) then network segmentation may be required or SSM deployed in the network

To properly capture event data, the router must understand and record network events that correlate to the defined multicast events. This data is typically collected as syslog events or through standard multicast MIBs as defined by the IETF.

APPENDIX A: COMMON PACKET LOSS CONDITIONS

Since packet loss plays the most critical role in media quality, the conditions leading to this condition are further detailed. This is not an all-inclusive list and does not include product defect conditions such as hardware failures, router design, or software bugs although these can lead to metric violations for any of the metrics listed in this document.

Physical Interface Errors

Physical connectivity from the router can be into an optical or copper network. These connections can become loose or faulty causing transmit or receive packet errors. These errors can also be introduced over any network infrastructure such as an Optical Transport Network (OTN) connecting two routing nodes.

In newer router platforms, connectors, such as SFP or XFP are used so that replacement is possible without removing other router components.

Interface Congestion

Since an egress interface on a router can receive packets from multiple ingress interfaces, it is possible that the outbound packet bandwidth is greater than the physical interface speed. An example is trying to send 2Gbps of media out of a 1Gbps interface. To alleviate this congestion condition, packets are queued in memory and a packet scheduler is used to determine which queued packets to forward out the interface.

If the number of packets to be queued exceeds the buffer memory, packets must be dropped from the queue resulting in dropped packets or packet loss. Where packets are not dropped, queue hold-times can impact latency and jitter.

Multiple queues per interface can be used to raise the priority of the more latency and loss sensitive traffic. In some cases, the traffic may incorrectly be configured to use the wrong queue, leading to service class congestion.

Interface Policers and Filters

Interface cognition on a router can include rules such as policers and packet filters to control traffic. Incorrect configuration of bandwidth allocation for policing can lead to packet drops by the router. Packet filters applied for security reason, if set incorrectly can also cause the router to drop media packets.

Routing Protocol Errors or Misconfiguration

Routing Protocols build routing topology in the network. These protocols share IP subnet and topology information between routing nodes. If a router is incorrectly configured or is not sharing all routing information, certain router hops may create a “black hole” situation where it receives packets but has no next-hop interface map. In this case, the router will drop the packet.

Note that a router acts opposite that of a switch. A switch floods traffic to all interfaces when an unknown outgoing interface exists while a router drops packets with an unknown outgoing interface.