Optimised IP multicast architectures for real-time digital workflows

Thomas Kernen
Cisco
IP Multicast 101

- Single data stream generated at source
- Receivers subscribe to stream (group)
- Packets replicated by network elements
- Identical data to all receivers
  - Payload independent
- Beneficial for broadcast applications such as:
  - Essence delivery, synchronisation, QC, monitoring
IP Unicast vs. multicast

Source \[\rightarrow\] Router \[\rightarrow\] Unicast receiver

Source \[\rightarrow\] Router \[\rightarrow\] Multicast receiver
Source Specific Multicast

• Unlike Any Source Multicast:
  – Group and source awareness
  – No centralised Rendezvous Point mapping group to source
  – No initial setup via shared tree
  – Requires IGMPv3 at receiver

• Benefits:
  – No changes at source
  – No changes in network core
  – Direct tree/flow to receiver
  – SSM Mapping to support non SSM capable devices
Mcast Virtual Private Network models

Service
- Native
- mVPN

C-Multicast Signaling
- PIM
- BGP

Core Tree Signaling
- PIM (pt-mpt)
- MLDP (pt-mpt | mpt-mpt)
- P2MP TE (pt-mpt)

Encapsulation /Forwarding
- IP/GRE
- LSM
Malicious or misconfiguration?
Same security rules

• **Source Originating Threats:**
  – Protect First Hop Router from Denial of Service
  – Overloaded & creating state towards RP
  – IP Access lists to limit authorise sources/groups

• **Receiver Originating Threats:**
  – Prevent receivers from joining too many and/or unauthorised sources/groups
  – IP Access lists to limit authorise source/groups

• **Control Plane Policing:**
  – Limit maximum number of multicast routes per node
  – Filter Protocol Independent Multicast messages
Generic HW based Multicast Replication Architecture

Ingress Card

LC1

Fabric

LC2

Egress Card

LC3

Multicast Packet

Multicast Packet

Multicast Packet

Multicast Packet

Multicast Packet

Multicast Packet

Multicast Packet
Multicast Replication Throughput Performance

- 2000 multicast routes
- 64000 output interface list with receivers
- 10GE input
- 24 x 10GE ports
- 20 μs latency
Mitigate Quality of Service (QoS) scheduler inefficiency

- Classic (weighted) round-robin 8 queue model can result in traffic drops
- Enable Video priority queue (VPQ):
  - for all video traffic in IP transport network
  - VPQ ensures scheduler services video traffic with strict priority & 100% weight before another queue is serviced
- No drops under network congestion scenarios
Multicast Stream-Merge with Path Diversity

Multicast Source

Protection Domain

IP/MPLS Core

Multicast Receiver

Ingress Demarcation

Multicast Receiver

Egress Demarcation

IP/MPLS Core

Explicit Path Vector TLV

Explicit Path Vector TLV

(S,G)

(S1,G)

(S2,G)

R1

R2

R3
Inline Video monitoring
Payload Encapsulations
Vidmon RTP Metrics Use case

**Video Contribution**
- Uncompressed RTP (0,0,10)
- RTP (4,2,1,20)
- RTP (12,8,9,55)
- RTP (0,0,0,10)
- J2K (0,0,11)
- RTP (12,23,20)
- RTP (0,0,15)
- RTP (120,3,30)

**IP/MPLS Core**

**Video Distribution**
- Final Studio
- Super Head End
- Edge Distribution

- RTP (0,0,10)
- RTP (4,2,1,20)
- RTP (12,8,9,55)
Vidmon RTP Metrics Triggered Stream-Merge Failover

- Automated failover
  - Real-time on-path video quality metrics
- Trigger switchover based on set of metrics such as:
  - loss, jitter, video-glitch count, or video availability
- Failover in ~25msecs
Software Defined Networking

• New approach to networking
  – Normalisation of network configuration & control through open APIs
  – Topology virtualisation, and customised control planes
  – Controller/policy server directs network node functions
Sample use case: Low latency path for broadcast interview mode

- Correlate:
  - Capacity
  - Link cost
  - Reliability
  - Latency
  - Jitter
  - Congestion
  - ...

Build optimal path across SP network for real-time low latency, jitter and congestion free requirements
Conclusions

• Architecture simplification & performance:
  – SSM, line rate HW replication, stream-merge capabilities & priority queuing

• Security improvements:
  – Virtualisation of the network path (mVPN)
  – Traffic filtering enhancements

• Inline monitoring

• SDN: granular workflow control via APIs
Optimised IP multicast architectures for real-time digital workflows

Thomas Kernen, Consulting Systems Engineer
Cisco, Avenue des Uttins 5, 1180 Rolle, Switzerland, thkernen@cisco.com

Javed Asghar, Technical Marketing Engineer
Cisco, 725 Alder Drive, Milpitas, 95035, USA, jasghar@cisco.com

Written for presentation at the
2012 SMPTE Annual Technical Conference

Abstract. Across the entire broadcast chain from production to distribution, real-time digital workflows are now commonly being distributed over Internet Protocol (IP) networks. Many deployments are leveraging IP multicast to optimise the delivery from a source to a set of diverse end points (receiver) such as video servers, mixers, quality control units, video monitoring, time & synchronisation slaves, etc. These devices require reliable and deterministic network behaviour to ensure an optimal operating environment.

Technology developments in multicast-related protocols and architectures such as Source Specific Multicast, transport virtualisation, Fast Convergence, inline video monitoring metrics, combined with multicast hardware replication improvements in routers and switches, have significantly increased the reliability of the network layer transport for digital workflows.

By preventing bandwidth duplication or centralised congestion points, reducing outage duration by using dual paths between source and receivers, combined with protocol, hardware, monitoring and security improvements, the overall reliability of IP multicast networks has dramatically increased in the last decade.

Keywords. IP, multicast, security, network, workflows, monitoring, fast convergence, SDN
Introduction

Since the introduction of Internet Protocol (IP) -based networks for moving essence as part of digital workflows, many broadcasters and production facilities have embraced IP multicast technology to allow for better scaling of their IP network resources.

In contrast with a unicast mechanism, where a unique flow from any given source to any destination must to be set up for each and every destination, multicast offers the ability to distribute a single flow from a source to any number of destinations (known as receivers). By doing so, the same amount of data is sent from the source independently of the number of receivers that wish to subscribe to the flow. The IP network nodes, such as switches and routers, perform the flow replication where needed along the path between sources and receivers, as seen in Figure 1.

Broadcast related applications that may benefit from a multicast distribution are:

- Live essence from cameras or to/from video servers, mixers, slow-motion replay servers, slide store servers, etc;
- House clock and related synchronisation; and,
- In-house TV, live audio, intercoms.

Quality control and monitoring may also benefit from multicast, since those services could tap into any of the flows mentioned above at any multicast enabled point in the network, on demand, without introducing an additional load on the network.

With the introduction of 4K workflows, combined with 720p and/or 1080i/p uncompressed workflows whenever possible, IP network bandwidth requirements are rapidly growing across all parts of the broadcast industry.

Figure 1. Unicast vs. Multicast distribution.
In a properly designed IP multicast network, where all sources are multicast-enabled, this could simplify IP network resource management tremendously. Any new destination for an existing flow could be connected with minimal IP network planning and engineering, helping to keep bandwidth requirements under control.

In other industries, where reliability and efficiency is key, multicast is already used for financial market data distribution, high frequency algorithmic trading, and air traffic control.

Many devices already in use in the broadcast industry offer multicast capabilities. Unfortunately they do not often support, or have not been configured with, the optimisations offered by modern multicast implementations. The following sections of this paper highlight some of these optimisations, and ways in which real-time digital workflows can benefit from them.

When designing multicast networks, it is important to understand how the different protocols interact, and therefore how a change to a specific protocol may influence another protocol in the network stack. In particular, understanding how the network converges and how long it can take to recover from failure scenarios can be extremely important.

**Multicast transport models**

In the original Any Source Multicast (ASM) model the receiver is only aware of the multicast group (G) that he wishes to subscribe to, and not of the source (S) transmitting that group. The receiver relies on his directly attached (designated) router (DR) to discover which sources (S) are sending to the multicast group (G) of interest. The receiver relies on the IGMPv2 (or MLDv1 for IPv6) protocol to request the (*,G) membership. In order for the router to discover the source of the group in question, there is a need for a Rendezvous Point (RP), to allow for the source discovery to occur. The RP will handle the initial request from the receiver, set up the multicast tree, known as the shared tree, and forward the flow from any source via the RP to the receiver.

Once the receiver’s DR knows the source, it will set the direct multicast tree from the source to the receiver, and switch over the active stream to the new path known as the source or shortest path tree (SPT). The shared path between the receiver and the source (via the RP) is then torn down. This means that all new flows will initially transit the RP before the source path is set up.

**Source Specific Multicast**

Source Specific Multicast (SSM) greatly simplifies the above process versus the ASM model, especially for architectures with a large numbers of flows from limited number of sources to a large number of receivers as typically found in a broadcasting environment. It allows for a receiver to subscribe directly to a specific source by specifying both the source (S) and the multicast group (G) it wishes to receive from, hence the name Source Specific. No changes are required at the source, whilst the receiver and directly connected router must support IGMPv3 (or MLDv2 for IPv6) to allow for (S,G) membership reports. The receiver application must also be written to send source (S) and group (G) to a well-defined API that is present in all modern IP protocol stacks. Therefore, only the source/shortest path tree needs to be set up; this is done directly without the need for a Rendezvous Point. SSM also provides additional security whereby, in case multiple multicast sources are distributing content to the same group address, there is no stream overlap, since the source address remains unique. IETF RFC 4607 standardised SSM in 2006.
SSM Source Mapping

For legacy receivers that may not be able to support SSM, due to a lack of IGMPv3/MLDv2 in the IP network stack, or the previously mentioned API calls at high layers, SSM Source Mapping offers a migration solution.

SSM Source Mapping works by deploying SSM at the network edge close to the multicast receivers. IGMPv2/MLDv1 (*,G) membership reports from IGMPv2/MLDv1 receivers are mapped to specific source IP addresses. This mapping can be provided statically (from the local router configuration file), or dynamically (using a well known address lookup mechanism known as DNS). This enables managed IP networks to offer SSM services to both IGMPv2/MLDv1 and IGMPv3/MLDv2 receivers, and provides a smooth transition path from ASM to SSM, without the need to implement Rendezvous Points for legacy receivers.

Virtualised mVPN transport models

One of the strengths of IP is the ability to build virtual private networks (VPN) on top of a common infrastructure. Such VPNs provide the necessary security mechanisms to enforce the isolation in the transport of IP traffic within a given virtual domain, yet provide full transparency between the devices within the VPN, as if they were on a dedicated physical network infrastructure. Depending on the type of VPN requirements (emulation of a Layer 2 network bridge interconnect or a Layer 3 routed environment), a set of network signalling options are available to instantiate those networks. Those VPNs also have the ability to provide multicast replication as part of the VPN services as detailed in Figure 3.

The virtual network tunnels are set up using Label Switched Multicast (LSM). Core tree signalling can use Multicast Label Distribution Protocol (mLDP) or Resource Reservation Protocol (RSVP) Traffic Engineering (TE), depending on various options. Finally, the multicast signalling is triggered by the Border Gateway Protocol (BGP) routing protocol.
With this wide set of mVPN options to support common network topologies, multicast distribution within a virtual domain can meet most deployment requirements.

Security
When operating any type of network, an understanding of the infrastructure and how to secure it against a number of potential attacks, either malicious or due to misconfiguration, is necessary. In the world of IP networks, both the control plane (managing the inter node protocol exchange) and the forwarding plane must be protected.

Source Originating Threats
First hop attacks can occur, for example, if a source attempts to flood the network with many flows. These should not be forwarded by the first hop router (FHR) where the host is attached in the absence of any receivers. This attack may still overload the router with demands for multicast forwarding state creation. This can in turn cause a Denial of Service (DoS) condition for any legitimate traffic.

In an ASM architecture using RPs, state is still created for each new flow, which may lead to resource exhaustion on the RP. Source registration filters on the RP ensure that only valid sources are registered, and rate limiting the registration rate for new groups from the FHR towards the RP further reduces the risk. In an SSM architecture there is no RP, hence this attack vector isn’t applicable.

To prevent sources spoofing valid sources by announcing multicast groups in use by others, an IP access list designed to only allow authorised sources for any given host can be applied to the FHR.
**Receiver Originating Threats**

A receiver generating multiple requests for a large set of multicast groups may also exhaust the resources of the directly connected router by creating unneeded state for many bogus entries, and/or overload the available bandwidth upstream by requesting too many sources. Enabling IP access lists in the local router for the specific range of groups that receivers are authorised to subscribe to would reduce the potential load due to such attacks.

**Control Plane Policing**

Whilst not being interface specific, it is also important to protect the global resources of any network node to prevent further attack vectors from being exploited. Limiting the global number of multicast routes per node to a known value reflecting how the network may operate when at full planned capacity would help prevent rogue devices from directly impacting multicast state replication in those devices.

Interfaces that aren’t members of the multicast infrastructure should not be sending Protocol Independent Multicast (PIM) messages to their neighbours. An IP access list filtering PIM messages from such neighbours should be implemented on those interfaces.

**Distributed Hardware Multicast Replication**

**MRIB and MFIB Table Data-Structures**

A multicast router or switch capable of multicast replication in hardware (HW) uses two important data-structures, the Multicast Routing Information Base (MRIB) table and the Multicast Forwarding Information Base (MFIB) table. All multicast control plane information (Join, Prunes, and multicast protocol updates) is maintained centrally in the MRIB table on the central router CPU. The MRIB table is downloaded to each line card (LC) in a router to create the MFIB table. Each line card maintains its own MFIB, table that is programmed into the hardware for multicast lookups and replication. A typical MFIB entry in hardware consists of the multicast route (*,G)/(S,G), the input interface (RPF), the fan-out replication interface list (output-interface-list) and a set of multicast flags that describe the properties of the multicast route.

**Generic Hardware Multicast Replication Model**

Hardware multicast replication is a mandatory requirement for video contribution/production networks, as the video flow bandwidth dimension can range from a few hundreds of Mbit/sec to a few Gbit/sec. These video flows need to be replicated at line rate within a few microseconds over 1GE, 10GE, 40GE or 100GE interfaces. In contrast, a software based replication model uses the central CPU for multicast replication suitable only for low bandwidth (a few Mbit/sec) video flows with limited multicast fan-out, but will this in any case result in high latency depending on CPU utilization.

Figure 4 describes generic distributed hardware based multicast replication model which is an industry standard. In this model, the multicast packet replication architecture is summarised in the following steps:

1. When a multicast packet arrives at the ingress line card Network Processor (NP), a MFIB HW lookup is performed to determine the output interface list of the multicast packet. The ingress line card will then program a fabric replication bit-map into the multicast packet. The fabric replication bit-map consists of egress slots in the system. A single copy of multicast flow is sent in to the fabric. (Note: the ingress line card doesn’t perform replication at this stage)
2. The fabric crossbar replicates the multicast packet towards each egress line card, based on the fabric replication bit-map of the multicast packet. That is, the fabric replicates only 1 copy of the multicast flow towards each egress line card that has an interested multicast receiver attached. If a line card doesn’t have an interface receiver, the fabric will not replicate to that line card.

3. Each egress line card NP performs a 2nd MFIB HW lookup of the multicast flow to determine the number of the local multicast output interfaces list, and then the NP replicates and forwards the multicast flow to those multicast receiver interfaces.

![Figure 4: Generic Hardware based Multicast Replication Architecture](image)

**Hardware Multicast Replication Model Throughput Performance**

The multicast replication performance of the hardware-based replication model is described in Figure 5. In this performance test, 2’000 multicast routes with a 64’000 output interface list of interested multicast receivers was validated. The input bandwidth of aggregate multicast traffic was 10G input and output replication fan-out to 24x10G ports. The X-axis shows the Ethernet frame size of the IP/MPLS multicast packet. The left Y-Axis shows the bandwidth in Gbit/sec, and right Y-Axis shows the bandwidth in Mframe/sec.

The result was that for every packet size the hardware replication model could always replicate multicast packets at line rate. The average latency of full replication in this test was approximately 20 microseconds. In contrast, a software based replication model can only replicate at Mbit/sec with high latency and jitter.

Therefore, we only recommend a hardware-based multicast replication model for video transport networks, instead of a software-based replication model.
Figure 5: Multicast Replication Throughput Performance

**Video Priority Queue**

The typical queuing model used in an IP/MPLS video transport network is typically based on a flat 8 queue model, which uses the Differentiated Services Code Point (DSCP), or MPLS EXP bits for classification to enqueue video packets and other traffic into queues. The queuing scheduler may service the queues in a round-robin or in a weighted round-robin fashion, which can result in video traffic getting dropped, or experiencing higher latency and jitter.

To mitigate Quality of Service (QoS) scheduler inefficiency, a video priority queue solution should be adopted for all video traffic in a video transport network.

Under congestion, the video priority queue ensures the scheduler will service the video traffic with strict priority and 100% weight before another queue is serviced.

By implementing a video priority queue in a video network, the network will not drop any video traffic under network congestion scenarios.

**Multicast Fast Convergence**

*Multicast Stream-Merge with Path Diversity*

This solution is designed to provide predictable multicast convergence (i.e. \(~25\text{msec}\)) by using 2 spatially diverse primary and backup multicast trees to transport high-bandwidth video flows from the first-hop multicast router to the last-hop multicast router. The last-hop multicast router receives 2 copies from the IP/MPLS core, and will replicate 1 copy to the multicast receiver. When the primary multicast tree fails, the last-hop multicast router detects the failure in the forwarding plane and will failover to the backup multicast tree from which the multicast traffic is replicated towards the multicast receiver. Multicast stream-merge is agnostic to IPv4 or IPv6.

This solution is illustrated in Figure 6. The video multicast sources could be single homed or dual-homed to the first-hop multicast router.
Constructing Path Diverse Multicast PIM Trees

Using Figure 6 as a reference architecture, the following steps illustrate how the path diverse multicast PIM trees are built for multicast stream-merge:

1. Last-hop-multicast router receives an IGMP/MLD/PIM Join (S,G) from the multicast receiver.
2. Multicast stream-merge function will clone 2 copies of (S,G) to (S1,G) and (S2,G) into core protection trees.
3. (S1,G) core tree represents the primary multicast tree and (S2,G) core tree represents the backup tree.
4. The last-hop-multicast router will insert an explicit-path-vector TLV stack (IETF RFC 5496) in the PIM join attribute of the primary tree (S1,G) and backup tree (S2,G).
5. The explicit-path-vector TLV is used for traffic engineering the path of the PIM multicast tree by overriding the routing protocol computed RPF path of the multicast PIM Join message.
6. Spatially diverse primary and backup trees are constructed from the last-hop multicast router to the first-hop multicast router over the IP/MPLS multicast core, where both trees do not intersect.
7. The video multicast sources could be single homed or dual-homed to the first-hop multicast router.

Stream-Merge Failover

Using Figure 6 as a reference architecture, the following steps illustrate how stream-merge failover is performed for deterministic multicast fast convergence (i.e. ~25msec).

1. The video source sends high bandwidth multicast video flow (S,G) into the first-hop multicast router.
2. In the forwarding plane, the first-hop multicast router replicates (S,G) flow to primary flow (S1,G) and backup flow (S2,G), and forwards each flow along the primary and backup path diverse trees.
3. At the last-hop multicast router, stream-merge function selects the primary (S1,G) flow and replicates it towards the multicast receiver by translating the source address of (S1,G) core flow to (S,G) receiver flow.
4. If there is a failure along the primary tree path, the stream-merge function at the last-hop multicast router will detect that failure and failover to the backup flow (S2,G).
5. Stream-merge will replicate (S2,G) towards the receiver by translating the source address of (S2,G) core flow to (S,G) receiver flow.
6. The total detection and failover time is ~25msec.

**Inline Video Monitoring Metrics**

In any IP/MPLS video network, most service providers deploy off-path appliance devices to measure video payload quality. The off-path video monitoring solution is CAPEX intensive, therefore it is deployed at selective video sources and receiver sites, providing partial visibility of the video quality of video flows. An alternative solution is an Inline Video Monitoring (Vidmon) solution providing on-path video payload quality monitoring in a router port along an entire multicast flow path in the network.

**Inline Vidmon Architecture**

An inline Vidmon solution provides on-path video traffic payload quality monitoring capability in an IP/MPLS multicast network natively on router ports.

All Vidmon metrics are computed in hardware, where the micro-code parses all RTP or MPEG-2 Transport Stream (MPEG-2 TS) headers of every video packet, and then computes the video quality metrics at the end of the monitoring interval. Since the router is parsing and not buffering or queuing Vidmon flows, there is no latency or jitter added by Vidmon to the video flows being measured.

A video service provider can trigger on-path alarms to a network management station when the Vidmon metrics exceed a pre-defined error threshold.

Table 1, describes the Vidmon metrics available in most router or switches.

<table>
<thead>
<tr>
<th>Vidmon Metric Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDI MPEG-2 TS Metrics</td>
<td>Measures these MPEG2-TS statistics:</td>
</tr>
<tr>
<td></td>
<td>• Video packet loss</td>
</tr>
<tr>
<td></td>
<td>• Video loss rate</td>
</tr>
<tr>
<td></td>
<td>• Video glitch counter</td>
</tr>
<tr>
<td></td>
<td>• Video jitter profile</td>
</tr>
<tr>
<td></td>
<td>• Video flow availability</td>
</tr>
<tr>
<td></td>
<td>• Video flow stop event</td>
</tr>
<tr>
<td>RTP-JPEG2K Metrics</td>
<td>Measures these RTP statistics:</td>
</tr>
<tr>
<td>RTP-Uncompressed Metrics</td>
<td>• Video packet loss (16-bit, 32-bit seq. no.)</td>
</tr>
<tr>
<td>RTP-MMR Metrics (Microsoft Media Room)</td>
<td>• Video loss rate</td>
</tr>
<tr>
<td></td>
<td>• Video glitch counter</td>
</tr>
<tr>
<td></td>
<td>• Video jitter profile</td>
</tr>
</tbody>
</table>
Video flow availability
• Video flow stop event

Video Transport Availability
Measures video flow uptime and downtime

Video Jitter
Instantaneous max of RFC-3550 PPDV

Video Stop Events
Critical alarms when video servers doesn’t transmit video

Table 1: Vidmon Metrics

Figure 7, describes the video payload encapsulations applicable to Vidmon metrics.

Vidmon use case in Video Contribution/Production Networks
Vidmon RTP metrics can measure video SLA of uncompressed or JPEG2000 (JPEG2K) compressed video payloads in a video contribution/production network.

Figure 8 describes two Vidmon use cases where the red IP/MPLS multicast tree is transporting uncompressed video, while the purple multicast tree is transporting JPEG2K compressed video between video sources and receivers. The router ports along the entire path of each multicast tree are measuring RTP Vidmon metrics every 10 seconds. Vidmon RTP metrics are measured at:

1. The first-hop root multicast IP/MPLS tree router ports;
2. The core multicast tree transit or branching router ports; and,
3. The last-hop multicast router ports.

In the example illustrated in Figure 8, RTP Vidmon metrics diagnose the root cause and location of the video degradation in the network within a monitoring interval of 10 seconds.
1. At the multicast root node the Vidmon RTP flow metrics are green which implies the SLA is in-contract.

2. In the core, the multicast branching node replicates 2 copies, one branch towards the studio receiver (RTP Vidmon metric is green, SLA is in-contract) and a second branch towards the video edge receivers (RTP Vidmon metric is red, SLA out-of-contract).

3. At the last-hop multicast router, Vidmon RTP metrics show perfect video quality for the studio receivers, while Vidmon RTP metrics show poor lossy video quality for the video edge receivers.

**Figure 8: Vidmon RTP Metrics Use case**

**Vidmon Quality Triggered Stream-Merge Failover**

Vidmon metrics are also used to trigger stream-merge failover at the edge egress multicast router for video flows that exceed the Vidmon in-contract SLA alarm threshold. The benefit of this approach is that the stream-merge failover is selected based on the real-time on-path video quality metric statistics.

Figure 9 describes how a video network can automate the stream-merge failover, by using actual video quality provided by Vidmon metrics on the port. For example, the Vidmon RTP metric alarm threshold conditions (loss, jitter, video-glitch count, or video availability) trigger stream-merge failover from primary-path to back-up within ~25msecs and vice versa.
Software Defined Networking

Software Defined Networking (SDN) is a new approach to networking, complementing traditional network architectures. SDN aims at the normalisation of network configuration and control through open application programmatic interfaces (API) to individual network devices as well as to the whole network. SDN incorporates concepts for network and network topology virtualisation, and enables customised control planes. The latter allows close alignment of the network forwarding logic to the requirements of applications. A controller/policy server directs the functions of a network node through a secure channel that can be domain/context specific. Multicast benefits from these new developments for broadcast related applications.

Video Capacity planning, automated optimal path discovery and provisioning

Leveraging SDN APIs to extract the information from the network nodes offers additional capabilities when modelling workflow capacity planning between a given set of receivers and sources. By correlating a number of data sets (current and planned capacity availability, cost of links, reliability, latency, jitter, congestion…) collected via the APIs from the network nodes, the SDN policy server can provision the optimal path whenever new multicast flows are being triggered by a receiver subscribing to a group. This enables an additional level of decision making, beyond the common network topology metrics: focused on shortest path routing. The network nodes provide the controller/policy server with the metrics, which are then computed to set up the new optimal path for a given type of service. Leveraging all paths in the Service Provider (SP) network, the broadcaster can set up a low-latency transport path between studios A and B for real-time interview as shown in Figure 10. Another scenario could be a high-speed path for a faster than real-time workflow transfer.
SDN Optimal Path Computation Using Vidmon Metric Analytics

In a SDN environment, Vidmon metrics are now providing video quality analytics visibility that was not possible in an IP/MPLS network. The SDN controller is using the Vidmon metric analytics to compute and dynamically provision:

1. Optimal unicast forwarding paths or multicast forwarding trees that result in in-contract Vidmon SLA at the least possible cost.
2. Resilient backup forwarding paths are pre-provisioned at the least possible cost.

Conclusion

The architecture and performance of IP multicast networks has undergone major changes since originally designed back in 1985. These changes enable real-time digital workflows to deliver scalable performance and a deterministic behaviour.

The simplification of the multicast architecture through the use of SSM, line rate hardware based multicast packet replication, stream-merge capabilities and priority queuing ensure that even under severe load, high resolution/high frame rate workflows such as 4K and 8K will be given the service level guarantees they require. Those service level agreements can be verified and troubleshooted via inline monitoring capabilities.

Infrastructure level hardening and virtualisation of the network path (mVPN) enhance the security of workflows against a range of threats.

Whilst already demonstrating applicability for some workflow use cases, SDN is a new technology still undergoing research and standardisation. This field should be revisited over the course of the coming years to see how it evolves and provides additional solutions for the broadcast industry.

Acknowledgements

The authors wish to thank Steve Simlo for his help with reviewing this paper.
Reference and Bibliography


Steve Simlo, Michael Behringer, "Multicast Security Tool Kit", Cisco


Robert Doverspike, Guangzhi Li, Kostas Oikonomou, K. K. Ramakrishnan and Dongmei Wang, "IP Backbone Design for Multimedia Distribution: Architecture and Performance" AT&T Labs Research

IETF RFC 3569, "An Overview of Source-Specific Multicast (SSM)", July 2003

IETF RFC 3678, “Socket Interface Extensions for Multicast Source Filters”, January 2004

IETF RFC 4607, “Source-Specific Multicast for IP”, August 2006


IETF RFC 5880, “Bidirectional Forwarding Detection (BFD)", June 2010