WHITE PAPER

IP MULTICAST IN CABLE NETWORKS

Joe Godas of Cablevision Systems Corporation; Brian Field, PhD. of Comcast Corporation;
Alon Bernstein, Sanjeev Desai, Toerless Eckert, and Harsh Parandekar of Cisco Systems, Inc.

ABSTRACT

IP multicast is as an integral technology in networked applications throughout the world. Any network application involving the transmission of the same information to multiple recipients can benefit from the bandwidth efficiency of multicast technology. Multicast represents a key inflection point for the cable industry. While multicast is being used in cable networks today, two key new technologies—the wideband protocol for a Data Over Cable Service Interface Specification (DOCSIS) network and Single Source Multicast (SSM)—are expected to dramatically accelerate multicast deployment.

These technologies will help operators dramatically incease the operational efficiency of the Hybrid Fiber Coax (HFC) network, create a mechanism to accelerate the delivery of advanced services, leapfrog recent announcements of fiber-to-the-x (FTTx) deployments and service, and drive industry agendas for years to come.

This paper is jointly authored by Cablevision Systems Corp., Comcast Corp., and Cisco Systems, Inc. The paper describes multicast deployments at Cablevision and Comcast, highlights other multicast applications, and discusses key challenges. The paper proposes enhancements to DOCSIS specifications that should significantly increase multicast deployments in cable networks.

INTRODUCTION

IP multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to potentially thousands of subscribers. Multicast routing establishes a tree that connects a source with receivers. Multicast delivery sends data across this tree towards receivers. Data is not copied at the source, but rather, inside the network at distribution branch points. Only a single copy of data is sent over links that lead to multiple receivers, resulting in bandwidth gains. Multicast packets are replicated in the network at the point where paths diverge by routers enabled with Protocol Independent Multicast (PIM), and other supporting multicast protocols. Unlike broadcast, the traffic is only received and processed by devices that are listening for it.

IP multicast was developed in the early 1990s and was first deployed in education and research networks. About 1997, multicast was deployed on a large commercial scale when stock exchanges required a fast, efficient method to send market data to many subscribers simultaneously. For the past few years, multicast has gained wider acceptance as enterprises and service providers have realized the benefits of the technology.

Two multicast service models are deployed today:

- **Any Source Multicast (ASM)** is the original model introduced in 1990 (RFC1112) where an interested receiver of a multicast session notifies the network via Internet Group Management Protocol (IGMP) that it is interested in joining a specific group associated with that multicast session. The receiver then receives content sent by any source sending to this group. This model is targeted to support dynamic multi-source sessions like conferencing and financial trading. The standard protocol set in support of ASM is IGMPv2 or IGMPv3 for hosts to join a group and Protocol Independent Multicast-Sparse Mode (PIM-SM), together with Multicast Source Discovery Protocol (MSDP), for interdomain operations and rendezvous point (RP) redundancy. Support for IGMPv2 and ASM is covered in DOCSIS 1.1.

- **Source Specific Multicast (SSM)** is a more recent model in which an interested receiver of a multicast session specifies both the group and the source (or sources) from which it would like to receive content. The SSM model is superior for services where sources can be well-known in advance of the multicast sessions. The SSM model is achieved through the use of IGMPv3 which allows the host to specify both the group and the sources of interest, as well as the PIM-SSM which generates S, G joins in direct response to the IGMPv3 reports.

SAMPLE APPLICATIONS UTILIZING IP MULTICAST

This section highlights solutions in which IP multicast is an important element of the network. The section details deployments at Cablevision and Comcast. The section also discusses multicast virtual private network (VPN) services. Figure 1 on the next page depicts a sample multicast-enabled network.

Multicast VPN services are offered primarily by telcos, but are of high value and interest to cable operators as well. The challenge for cable operators is to allocate enough spectrum and bandwidth to support these services. The wideband protocol for a DOCSIS network is the leading contender for providing this capacity. This section briefly describes the wideband technology and its relevance to cable operators as they converge IP services.

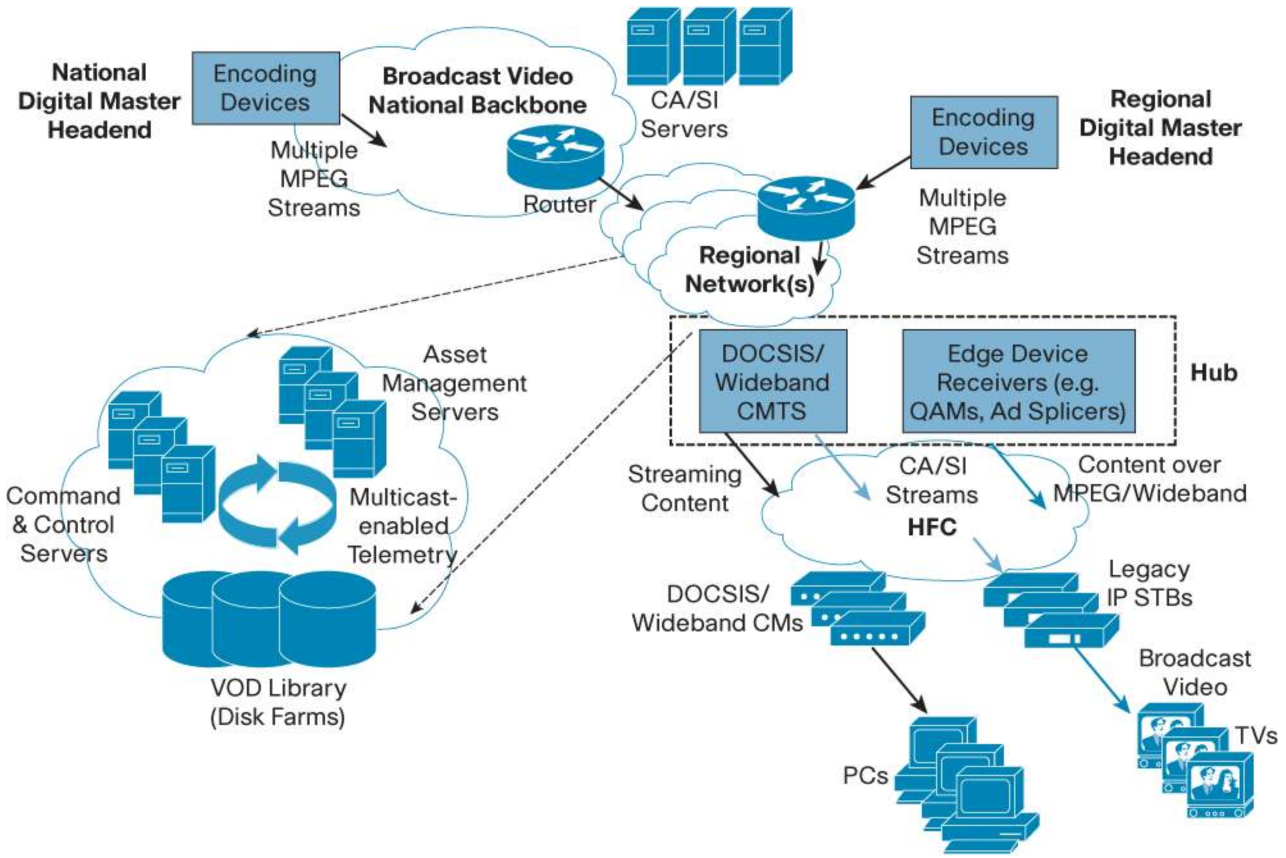
Digital Simulcast at Comcast

In Deployment

In today's broadcast video networks, proprietary transport systems are used to deliver entire channel line-ups to each hub site. These transport systems are often dedicated to broadcast, both digital and analog, video delivery and are not easily or economically extendable to other services.

By its very nature, broadcast video is a service well-suited to using IP multicast as a more efficient delivery mechanism. Comcast is in the process of moving its broadcast video service from a proprietary Baseband Video/Audio, IF, and DVB-ASI-based delivery system onto an IP network that is architected to support and deliver all Comcast-based services.

Figure 1. Network Diagram



The IP multicast delivery of broadcast video works as follows. Encoding devices in digital master headends, encode one or more video channels into a Moving Pictures Expert Group (MPEG) stream which is carried in the network via IP multicast. Devices at each hub site are configured by the operator to request the desired multicast content via IGMP joins. The network, using PIM-SM as its multicast routing protocol, routes the multicast stream from the digital master headend to edge device receivers located in the hub sites. These edge devices could be edge QAM devices which modulate the MPEG stream for an RF frequency or ad insertion devices which splice ads into the MPEG stream and then re-originate the ad zone-specific content to a new multicast group. Edge devices within the ad zone would use IGMP joins to request this ad zone-specific multicast content.

Futures

National Backbone

Comcast is in the process of deploying a backbone designed to support Comcast’s specific service needs. This backbone will be multicast-enabled and be able to deliver broadcast video content to Comcast regional networks. Having a multicast-enabled IP backbone that is able to deliver broadcast video has a number of economic benefits, including the ability for the backbone to act as the backup origination location to the regional networks for core video channels. The cost of deploying high-quality video-encoding equipment in a backbone backup facility can be more easily justified as its expense is offset by reduced redundant encoding equipment needs in Comcast regional networks.

SSM

While multicast, as available today, is a useful technological solution for a number of cable service applications, there are areas in which further enhancements to multicast, multicast's interaction with the rest of network routing protocols, and with devices which participate in multicast, may be useful. One enhancement to multicast relates to using SSM instead of ASM. With today's ASM/IGMPv2-based service with PIM-SM and IGMPv2, the complexity of IP multicast in the network is larger than necessary for applications with one or few (redundant) sources like DOCSIS Set-top Gateway (DSG) and Digital Simulcast. Migrating to PIM-SSM and IGMPv3 reduces this complexity, and thus, lowers the cost of operations. The challenge to adopting this technology lays primarily in edge device support like quadrature amplitude modulation (QAM) devices.

Challenges

Main challenges of this application are quality and availability. This translates into the applications and network redundancy design and failover times.

Better Overall Service Quality

As broadcast video is the core service offered by Comcast, the video service delivered via the IP transport network must be as good, if not better, than what is provided via existing legacy systems. Thus, it is critical that network and edge devices are highly available; the encoded video content is of very high quality; sufficient redundancy exists when a hardware failure occurs to enable the video service to recover quickly. Cable operators, therefore, have a number of design decisions to make regarding the level of device and network redundancy needed to support the real-time broadcast video service requirements.

Redundant Sources

For critical channels or content, a cable operator may choose to have dual origination points in the network. If the primary facility becomes unavailable due to a catastrophic failure or unplanned maintenance, the content can be multicast from the backup location. The operator can opt to have this backup stream always "on" and immediately available to devices in the network. This mode results in fast service recovery, but at the expense of using more bandwidth in the network.

On the other hand, since losing the primary facility should be an uncommon event, upon losing the primary facility, the operator may opt to manually enable the backup feed. This reduces the amount of bandwidth needed in the network. The service recovery time, however, will be greater.

Fast IP Unicast Convergence

Since multicast relies on the underlying IP routing infrastructure to build the multicast distribution trees, the time to rebuild the multicast tree when a failure occurs in the network, is in part dependent on how quickly the unicast routing protocols re-converge. Only when the unicast routing protocols have converged can PIM begin to rebuild the multicast trees. Thus, for real-time multicast applications, it is important that the operator's network design enables—and corresponding unicast and routing architectures—support fast network re-convergence.

Multicast at Cablevision

In Deployment

System and Conditional Access Information Distribution to STBs

Cablevision currently uses IP multicast to drive the conditional access (CA) and system information (SI) carousels to their set top boxes (STBs). Their first advanced STB had a single out-of-band tuner which acted as both as an interactive and out-of-band (OOB) management interface. Cablevision originally supported DOCSIS and Digital Audio Visual Council (DAVIC) delivery mechanisms, but quickly adopted a DOCSIS-only approach once multicast robustness was demonstrated. Cablevision's newer STBs use DOCSIS to carry vital SI streams. Both CA and SI will be carried over into any DSG deployments that Cablevision evolves to in the future.

IP multicast is delivered via PIM-SM for all applications. The system and conditional access distribution itself does not rely on IGMP signaling from the STBs, but instead statically joins and forwards the traffic from the cable modem termination system (CMTS). Depending on the STB system, the packet flow ratios will be approximately 50 pps @ 300 kbits/sec or 110 pps @ 430kbits/sec.

In terms of separation, Cablevision's high speed data (HSD) customers are shielded from seeing these STB multicasts via standard DOCSIS cable modem filters which are established by the configuration from the cable modem's Trivial File Transfer Protocol (TFTP) boot file. These filters also prohibit unintended sources from hijacking or disrupting multicast flows. In addition, Cablevision prohibits IGMP from cable modems in the upstream direction through configuration on the CMTS. Only the groups of the streaming audio/video service (described as follows) are allowed for subscriber cable modems of that service.

VoD Server Resource Management Telemetry

Cablevision's video on demand (VoD) resource management telemetry currently occurs over IP multicast, with a future eye on utilizing reliable multicast for content distribution to disk farms. The telemetry messaging is constant and averages close to 184 pps @ 458kbits/sec.

The command and control servers are a suite of servers that talk to clients and servers in the VoD cluster. The asset management component of the system must know what resources are available on each server in order to know if it has additional disk space and streaming capability. These status messages are carried over a proprietary multicast messaging system (developed by Seachange).

The basic network design consists of centrally located asset management and command and control servers that speak to remotely located VoD disk farms that communicate over the multicast network. Newer network design models and data transmission capabilities have enabled Cablevision to centralize the VoD disk farms. This in turn lends itself to a reduced need to route the VoD multicasts.

Streaming Audio/Video to Cable Internet Customers

This year, Cablevision is beginning a trial of real-time multicast video streaming to HSD users. This is meant to differentiate and add value to Cablevision's data service, promote loyalty, and reduce churn. Cablevision will start by porting selected Interactive Optimum (iO)—Cablevision's Video Service—content/functionality to Optimize Optimum Online (OOL)—Cablevision's cable modem service—for use exclusively by subscribers to both iO and OOL services. Video and audio content will be offered. Rates for video will approach 500 kbps and 55 pps per stream. The same sparse-dense mode network used for STB's SI will be used. The encoding is Windows Media version 9 (WM9), but alternative encodings are also being investigated—specifically for future content over the wideband protocol for a DOCSIS network.

Futures

Looking to the future, Cablevision sees the use of multicast as a delivery mechanism for push-VoD models where content is streamed to a group of PCs for viewing at a later time. Cablevision's VoD libraries can be leveraged, in addition to third-party content providers.

Beyond that, Cablevision sees their switched broadcast architecture incorporating IP multicast to help drive the efficient delivery of popular content across the video backbone and down the respective QAM devices—be they traditional MPEG or IP over DOCSIS.

Challenges

While Cablevision has been successful with the systems and services it has deployed to date, the company needs to continue to refine its network strategy and fine tune its architectures to address ongoing changes and challenges. Some of these challenges include:

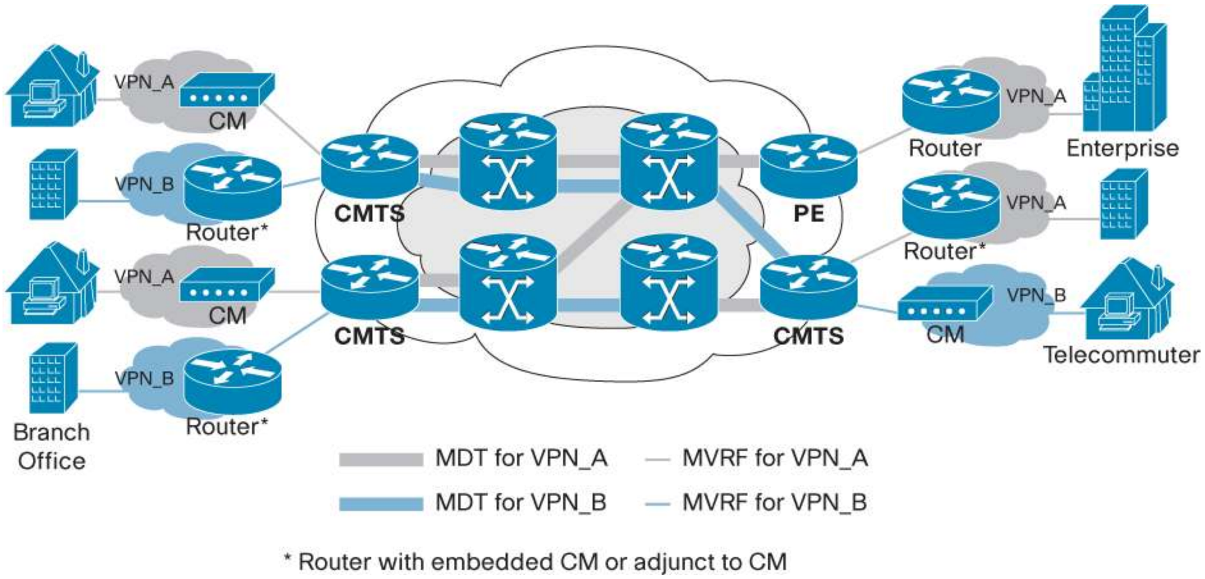
- DOCSIS 1.1 support is a necessity so that multicast flooding does not occur in a customer's home network.
- Enhancements to DOCSIS must be made such that multicast can be reliably scheduled and assigned a priority on DOCSIS segments.

- More multicast-aware customer premises equipment (CPE) gear: home routers and home wireless gear must continue to evolve to better support IGMP snooping, IGMP relay and firewall configurations that allow multicast streams to make it to intended destinations without allowing users to cannibalize their own experience. For example, a wired client on a home router should not be able to cause a multicast flood of his own wireless spectrum, if no wireless clients are requesting the flow.
- IGMPv3 and source-specific multicast (SSM) support
- More bandwidth: Cablevision must select their content carefully since there is a tight bandwidth budget with respect to the quality of the streams they want to offer. Cablevision is encouraged by the progress of the wideband protocol for a DOCSIS network and feels they will be able to exploit these opportunities further once larger backbones and modem contracts can be configured to handle cost-effective high-bandwidth services.

Multicast VPN Services

Commercial services over DOCSIS are steadily gaining traction in the cable environment—both in the U.S and abroad—because of strong revenue potential. One such service is VPN which allows businesses to connect multiple remote sites or devices over either a Layer 3 or Layer 2 VPN. Figure 2 on the next page depicts a multicast VPN service architecture.

Figure 2. Multicast VPN Services



For a Layer 3 VPN, the provider network is involved in the routing of traffic inside the VPN. A Layer 2 VPN provides a bridging transport mechanism for traffic between remote sites belonging to a customer. While these services are just gaining momentum in the cable world, they are quite pervasive in the telco world. In the telco VPN environment, enterprises have shown significant interest for native multicast support in the service provider's network. Current estimates are that ten to forty percent of VPN customers want IP multicast support in their VPN service to transport traffic for one or the other enterprise multicast application.

When VPN services are offered, multiple system operators (MSOs) will see the need to support IP multicast on these services. Typical enterprise multicast applications include NetMeeting, video conferencing, corporate communications, and finance-specific applications.

To support multicast over Layer 3 VPNs, each VPN receives a separate multicast domain with an associated multicast VPN routing and forwarding (mVRF) table maintained by the provider edge (PE) router. In the cable environment, the PE router can be a routing CMTS. The provider network builds a default multicast distribution tree (Default-MDT) for each VPN between all the associated mVRF-enabled PE routers. This tree is used to distribute multicast traffic to all the PEs. For high-bandwidth multicast traffic that has sparsely distributed receivers in the VPN, a special MDT group called a Data-MDT can be formed to avoid unnecessary flooding to dormant PE routers.

IP multicast can also be supported in Layer 2 VPNs via IGMP and/or PIM snooping in the provider's network. L2VPN services can be provided by configuring the CMTSs for point-to-point tunneling or for multipoint bridging. Depending on the configuration, snooping takes place on the external Layer 2 aggregation device or on the CMTS. Based on the snooped messages, the multicast traffic can be forwarded only to those customer edge (CE) devices that are interested in that traffic, versus flooding it to all the CE devices.

Security and data privacy are of primary concern in a VPN environment. The service provider network, including the CMTS, must be able to distinguish between multicast sessions that belong to different VPNs. On the shared cable downstream, packets belonging to separate VPNs must be encrypted using separate BPI keys. Since group addresses used within different VPNs can overlap, multicast support in VPNs can be complex without the right support in DOCSIS.

High-Speed IP over Cable with the Wideband Protocol for a DOCSIS Network

Cable operators are now entering the third phase of service convergence as they increasingly add IP video services to existing data and voice IP offerings. Service delivery requirements are rapidly evolving. A significant percentage of traffic will shift from broadcast video to per-user streams as deployment of network VoD services enables consumers to move to a user-controlled "watch whenever" viewing paradigm.

In the short term, the transition to per-user video streams is largely taking place in the MPEG domain. VoD and personal video recorder (PVR) services are being delivered to conventional STBs via MPEG transport streams. Over the longer-term, more of the video content will be delivered via an end-to-end IP infrastructure—directly to televisions and PCs in the home. Therefore, the infrastructure deployed must be capable of evolving into an all IP network. The wideband protocol for a DOCSIS network, along with multicast and IP Version 6 (IPv6), are key ingredients of this evolution.

The wideband protocol, which is under evaluation for inclusion in pending DOCSIS 3.0 specifications, allows cable operators to make the leap to IP video faster and cheaper than telco companies. The technology supports bonding multiple channels to allow cable operators to add downstream channels, independently of upstream channels. The technology enables operators to leverage previously deployed DOCSIS CMTSs and take advantage of declining prices for external edge QAM devices. It will allow operators to use the same edge QAM pool for both data and video services. The technology provides plenty of bandwidth for multiple standard-definition digital and HDTV channels, IP telephony and data offerings, with a capacity of up to 640 Mbps.

TECHNICAL CHALLENGES

While there are numerous challenges overall, this section concentrates on what we consider to be the top two challenges:

- Issues with ASM
- Limitations in DOCSIS 1.1

Issues with ASM

Three basic issues with ASM and its protocols exist:

Address Assignment

In ASM, only one application can use a group address G at a time. As long as multicast applications only need to run between participants within a single administrative entity, this is manageable. A single administrative entity can construct an address plan of RFC1918 type IP multicast group addresses (from 239.0.0.0/8). But this requires operational coordination which adds cost. If on the other hand, multicast traffic is to be transported across domains—for example from a content provider onto one or more cable operator or telco network—then coordination of IP multicast group addresses becomes an almost unsolvable problem.

Denial of Service Attacks

The ASM service model is prone to attacks by unwanted sources, because receivers do not specify which source(s) they want to receive traffic from. While it is possible in a walled garden network to provide additional network-based access control, the operational cost of such control rises as more and more multicast applications are deployed in the network.

Complexity of Provisioning and Operations

Unlike older multicast protocols, the PIM-SM/MSDP protocol provides efficient delivery of traffic and high availability. This comes at the cost of adding many protocol elements which increase the complexity of the network. Amongst these are:

- Placement of RPs, operations, and troubleshooting of RPs
- Operations of BSR or Auto RP protocols for RP redundancy
- Alternatively, static configuration of RPs and set up of MSDP-mesh groups for anycast-RP
- Operations of MSDP between administrative domains
- Troubleshooting of PIM-SM protocol elements such as RPT/SPT switchover and register tunnel encapsulation

Limitations in DOCSIS

Current DOCSIS specifications define several hooks for enabling multicast on the RF. These include:

- Baseline Privacy Interface (BPI) extensions that allow encryption of multicast sessions
- IGMP snooping in the cable modem (CM) that is used to trigger the BPI exchange for multicast.

The purpose of IGMP snooping is to restrain multicast traffic and specify how a host can register a router to receive specific multicast traffic. These specifications leave a wide range of issues unaddressed. These are discussed below:

- **Aliasing of Traffic—**According to RFC1112, aliasing of traffic may happen because only the lower order 23 bits of an IP multicast address are mapped to a multicast Ethernet address. For example, a CM configured to receive traffic for group 224.1.2.3 will accept traffic for 239.1.2.3. This is particularly an issue with VPN and SSM support.
- **Limited Support for Multicast Protocols—**DOCSIS 1.1 does not have IGMP support for IGMPv3 and SSM, Generic Attribute Registration Protocol (GARP), GARP Multicast Registration Protocol (GMRP) or Multicast Listener Discovery (MLD).
- **IPv6—**No support for IPv6 multicast since IPv6 has a dedicated control plane for multicast.
- **PacketCable Multimedia (PCMM)—**PCMM does not yet define how multicast is to be supported.
- **Lack of Explicit Tracking of Multicast Listeners—**Because of IGMP v1/v2 report suppression, the CMTS cannot track which hosts are actually listening to a given session and cannot support fast-leave for multicast sessions.
- **Quality of Service—**QoS for Multicast flows is not defined
- **Routed Networks on the CPE Side—**The network cannot easily support routers connected in the CPE network that run PIM instead of IGMP.
- **JOIN Acknowledgment—**There is no way for a CM or CPE to make sure a multicast session is successfully activated since there is no explicit acknowledgment in IGMP V2.

SOLUTIONS

SSM

Solving ASM Issues

SSM solves several problems with the ASM service model:

- **Network-wide Group Address Allocation—**In SSM, the multicast group G does not need to be unique over the network because only (S, G) channels need to be unique. Groups can be reused.
- **DoS Attacks—**Receivers will only receive traffic from the source which was explicitly indicated in their IGMPv3 joins.
- **Simplified Operations—**In PIM-SM, a receiver host joins to a group G. The network builds a delivery tree towards an RP (the RP tree) and sources register to the RP via an encapsulation tunnel. Then, the RP joins to the source to receive traffic from the source and sends it down the RP tree. Once the router connected to the receiver sees packets from a new source S arriving on this tree, it joins to this source via the Shortest Path Tree (SPT)—also called the (S, G) tree.

In contrast, with PIM-SSM, the IGMPv3 (S,G) report from the host allows the router connected to the receiver to bypass all the initial steps involving an RP and start out immediately by establishing the SPT for (S, G).

SSM with IGMPv3 and PIM-SSM is an evolutionary technology because PIM-SSM is a subset of PIM-SM. Routers that support PIM-SM also support PIM-SSM. Applications supporting SSM with IGMPv3 will also work in an existing PIM-SM IGMPv2 network, because IGMPv3 is automatically backwards compatible with IGMPv2.

Challenges of SSM Deployment

The challenges in deploying SSM are adoption and support of IGMPv3 with (S, G) receiver reports in applications and appliances; for example, STBs, PCs or QAM devices.

SSM mapping can be used as a transition strategy. In SSM mapping, the router connected to receivers is seeded with the source address belonging to groups G. While the receivers only send IGMPv2 reports for groups G, the router itself adds the source address and then continues to use PIM-SSM.

DOCSIS 3.0 Multicast Proposal

Multicasting on the RF can save bandwidth on the RF interface. Currently, however, DOCSIS RFI specifications do not fully address multicast. A DOCSIS 3.0 specification proposal has been submitted to CableLabs to address current DOCSIS limitations on multicast.

It suggests the following framework:

- Multicast flows are signaled in the same way that unicast flows are—through registration or DSx message exchange. They use the same TLV unicast flows use—an admission control function to keep track of the fact that multicast flows do not consume additional bandwidth once the first one is established.
- The multicast control plane handling is moved to the CMTS.

The list below outlines current issues with DOCSIS multicast support, and explains how the multicast proposal addresses these issues:

- **Aliasing of Traffic—**Current DOCSIS specifications support only RFC1112 mapping of multicast addresses. With this mapping, two separate groups can be mapped to the same MAC address. The proposal recommends setting a multicast media access control (MAC) address from a CMTS-allocated pool of multicast MAC addresses outside of the RFC1112 MAC address range. The CM can later replace this locally assigned address to a standard RFC1112.
- **Limited Support for Multicast Protocols—**Current DOCSIS specifications use “IGMP snooping” to detect that an IGMP was sent from the CPE. By moving the IGMP control plane processing to the CMTS, the system is not limited to “snooping” multicast and inherent problems associated with snooping. Instead, the end point that was supposed to receive the multicast—the CMTS—is the one responding to it.

- **PCMM—**Currently there is no PCMM definition on how multicast can be handled. Since the multicast proposal to CableLabs treats multicast as unicast in terms of flow definition and setup, then PCMM will tie seamlessly into this framework.
- **Limited Monitoring on the CMTS—**An explicit signaling for multicast flow set up will allow for deterministic tracking of multicast users, instead of relying on "report suppression"
- **Quality of Service (QoS) Definitions—**Current DOCSIS specifications have a rich set of methods to define QoS. However, these are tied to a specific modem. The proposal allows these definitions to be re-used for multicast as well.
- **Routed Networks on the CPE Side—**If PIM is running between the CMTS and a customer's router, the CMTS can trigger a multicast DSx based on the PIM state machine.
- **JOIN Acknowledgment—**Currently, there is no explicit response to an IGMP v2 JOIN. If the JOIN triggers a DSx message exchange, the DSx-RSP will return specific error codes if the multicast session cannot be established.

SUMMARY AND CONCLUSIONS

IP multicast has a wide range of applications for current and future cable operations.

Cable-specific applications (to QAM devices or STBs) include:

- Digital simulcast of live TV via IP multicast (e.g., Comcast)
- Switched video/TV broadcast (dynamic overprovisioning to save bandwidth)
- DSG/proprietary STB system information and crypto key distribution (e.g., Cablevision)
- VoD server resource management (e.g., Cablevision)

"Enterprise" applications include:

- Reliable content/software distribution/preprovisoning with Pragmatic General Multicast (PGM) or other multicast transport to VoD or Web servers
- VoIP: multicast music on hold, voice conferencing (Hoot & Holler)
- Enterprise corporate communications, video conferencing, corporate event broadcasting, and training
- Financial applications including stock trading and market data distribution
- Retail including warehouse-distributed applications (e.g., with TIBCO middleware) (typical drivers for VPN customers asking for multicast)

DOCSIS 1.1 applications include:

- Live audio/video streaming to HSD customers (e.g., Cablevision)
- L2/L3 VPN services: delivering "enterprise" multicast applications

Wideband Protocol for DOCSIS Network applications include:

- Higher bandwidth applications, more customers/content, and HDTV
- Key to migrate cable-specific applications to IP (with an IP STB that supports the wideband protocol)

While cable operators may start with as little as one application, they will likely need to support multiple applications over time. This leads to the conclusion that IP multicast will be one of the core capabilities of a cable operator's IP network for the foreseeable future and will help operators unleash the full power of their HFC network and architecture.

But before this promise can be fulfilled, there are a number of items that must be considered and decisions to be made. The two most important network technologies that cable operators must consider in conjunction with IP multicast are SSM and the wideband protocol for a DOCSIS network.

SSM can be deployed today. The challenge is to ensure it is supported in applications and appliances such as STBs.

The wideband protocol for a DOCSIS network will expand cable operator service profiles in the IP/data arena. Its challenge, in conjunction with IP multicast, is to ensure improved support for several elements in IP multicast (like SSM), as outlined in our DOCSIS 3.0 proposal.

REFERENCES

ASM

Host Extensions for IP Multicasting, RFC1112, S.E. Deering. Aug. 1989

IGMPv3

Internet Group Management Protocol, Version 3, RFC3376, B. Cain, S. Deering, et. al., Oct. 2002

PIM-SM

Protocol Independent Multicast—Sparse Mode (PIM-SM) Protocol Specification (Revised), draft-ietf-pim-sm-v2-new-11.txt, PIM-WG, Oct. 2004.

SSM

H.Holbrook, B.Cain, *Source-Specific Multicast for IP*, draft-ietf-ssm-arch-*.txt, Sept. 2004

IGMPv3 SSM

Using IGMPv3 and MLDv2 for Source-Specific Multicast, draft-holbrook-idmr-igmpv3-ssm-08.txt, H. Holbrook et. al, Oct. 1, 2004

DOCSIS 3.0 Proposal

Multicast Proposal for DOCSIS 3.0, Submitted to CableLabs by Cisco Systems, Inc., Dec. 10, 2004

Wideband Proposal for DOCSIS 3.0, Submitted to CableLabs by Cisco Systems, Inc., Dec. 10, 2004

Reprinted with permission of NCTA, from the 2005, NCTA Technical Papers™

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

205283.E_ETMG_SH_7.05

Printed in the USA