WIKIPEDIA

IP multicast

IP multicast is a method of sending Internet Protocol (IP) datagrams to a group of interested receivers in a single transmission. It is the IP-specific form of multicast and is used for streaming media and other network applications. It uses specially reserved multicast address blocks in IPv4 and IPv6.

Protocols associated with IP multicast include Internet Group Management Protocol, Protocol Independent Multicast and Multicast VLAN Registration. IGMP snooping is used to manage IP multicast traffic on layer-2 networks.

IP multicast is described in RFC 1112 (https://tools.ietf.org/html/rfc1112). IP multicast was first standardized in 1986.[1] Its specifications have been augmented in RFC 4604 to include group management and in RFC 5771 (https://tools.ietf.org/html/rfc5771) to include administratively scoped addresses.

Contents

Technical description

Overview

IP multicast is a technique for one-to-many and many-to-many real-time communication over an IP infrastructure in a network. It scales to a larger receiver population by requiring neither prior knowledge of a receiver's identity nor prior knowledge of the number of receivers. Multicast uses network infrastructure efficiently by requiring the source to send a packet only once, even if it needs

to be delivered to a large number of receivers. The nodes in the network (typically network switches and routers) take care of replicating the packet to reach multiple receivers such that messages are sent over each link of the network only once.

The most common transport layer protocol to use multicast addressing is User Datagram Protocol (UDP). By its nature, UDP is not reliable—messages may be lost or delivered out of order. Reliable multicast protocols such as Pragmatic General Multicast (PGM) have been developed to add loss detection and retransmission on top of IP multicast.

Key concepts in IP multicast include an IP multicast group address,[2] a multicast distribution tree and receiver driven tree creation.[3]

An IP multicast group address is used by sources and the receivers to send and receive multicast messages. Sources use the group address as the IP destination address in their data packets. Receivers use this group address to inform the network that they are interested in receiving packets sent to that group. For example, if some content is associated with group `239.1.1.1`, the source will send data packets destined to `239.1.1.1`. Receivers for that content will inform the network that they are interested in receiving data packets sent to the group `239.1.1.1`. The receiver *joins* `239.1.1.1`. The protocol typically used by receivers to join a group is called the Internet Group Management Protocol (IGMP).[4]

With routing protocols based on shared trees, once the receivers join a particular IP multicast group, a multicast distribution tree is constructed for that group. The protocol most widely used for this is Protocol Independent Multicast (PIM). It sets up multicast distribution trees such that data packets from senders to a multicast group reach all receivers which have joined the group. There are variations of PIM implementations: Sparse Mode (SM), Dense Mode (DM), source-specific multicast (SSM) and Bidirectional Mode (Bidir, or Sparse-Dense Mode, SDM). Of these, PIM-SM is the most widely deployed as of 2006; SSM and Bidir are simpler and scalable variations developed more recently and are gaining in popularity.

IP multicast operation does not require an active source to know about the receivers of the group. The multicast tree construction is receiver driven and is initiated by network nodes which are close to the receivers. IP multicast scales to a large receiver population. The IP multicast model has been described by Internet architect Dave Clark as, "You put packets in at one end, and the network conspires to deliver them to anyone who asks."[5]

IP multicast creates state information per multicast distribution tree in the network. If a router is part of 1000 multicast trees, it has 1000 multicast routing and forwarding entries. On the other hand, a multicast router does not need to know how to reach all other multicast trees in the Internet. It only needs to know about multicast trees for which it has downstream receivers. This is key to scaling multicast-addressed services. In contrast, a unicast router needs to know how to reach all other unicast addresses in the Internet, even if it does this using just a default route. For this reason, aggregation is key to scaling unicast routing. Also, there are core routers that carry routes in the hundreds of thousands because they contain the Internet routing table.

Routing

Each host that wants to be a receiving member of a multicast group (i.e. receive data corresponding to a particular multicast address) must use IGMP to join. Adjacent routers also use this protocol to communicate.

In unicast routing, each router examines the destination address of an incoming packet and looks up the destination in a table to determine which interface to use in order for that packet to get closer to its destination. The source address is irrelevant to the router. However, in multicast routing, the source address (which is a simple unicast address) is used to determine data stream direction. The

source of the multicast traffic is considered upstream. The router determines which downstream interfaces are destinations for this multicast group (the destination address), and sends the packet out through the appropriate interfaces. The term *reverse path forwarding* is used to describe this concept of routing packets away from the source, rather than towards the destination.

A number of errors can happen if packets intended for unicast are accidentally sent to a multicast address; in particular, sending ICMP packets to a multicast address has been used in the context of DoS attacks as a way of achieving packet amplification.

On the local network, multicast delivery is controlled by IGMP (on IPv4 network) and MLD (on IPv6 network); inside a routing domain, PIM or MOSPF are used; between routing domains, one uses inter-domain multicast routing protocols, such as MBGP.

The following are some common delivery and routing protocols used for multicast distribution:

- Internet Group Management Protocol (IGMP)
- Protocol Independent Multicast (PIM)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Multicast Open Shortest Path First (MOSPF)
- Multicast BGP (MBGP)
- Multicast Source Discovery Protocol (MSDP)
- Multicast Listener Discovery (MLD)
- GARP Multicast Registration Protocol (GMRP)
- Shortest Path Bridging (SPB)

Layer 2 delivery

Unicast packets are delivered to a specific recipient on an Ethernet or IEEE 802.3 subnet by setting a specific layer 2 MAC address on the Ethernet packet address. Broadcast packets make use of a broadcast MAC address (FF:FF:FF:FF:FF:FF).

IPv4 multicast packets are delivered using the Ethernet MAC address range 01:00:5e:00:00:00–01:00:5e:7f:ff:ff (with an OUI owned by the IANA). This range has 23 bits of available address space. The first octet (01) includes the broadcast/multicast bit. The lower 23 bits of the 28-bit multicast IP address are mapped into the 23 bits of available Ethernet address space. This means that there is ambiguity in delivering packets. If two hosts on the same subnet each subscribe to a different multicast group whose address differs only in the first 5 bits, Ethernet packets for both multicast groups will be delivered to both hosts, requiring the network software in the hosts to discard the unrequired packets.[6]

For IPv6 multicast addresses, the Ethernet MAC is derived by the four low-order octets OR'ed with the MAC 33:33:00:00:00:00, so for example the IPv6 address FF02:DEAD:BEEF::1:3 would map to the Ethernet MAC address 33:33:00:01:00:03.[7]

If a switch does not understand multicast addresses then it will flood that traffic to all the members of a LAN; in this case the system's network card (or operating system) has to filter the packets sent to multicast groups they are not subscribed to.

There are switches that listen to IGMP traffic and maintain a state table of which network systems are subscribed to a given multicast group. This table is then used to forward traffic destined to a given group only to a limited set of hosts (ports). This process of listening to the IGMP traffic is called IGMP snooping.

Additionally, some switches with layer 3 capabilities can act as an IGMP querier. In networks where there is no router present to act as a multicast router, a switch with IGMP snooping querier enabled can be used to generate the needed IGMP messages to get users to subscribe to multicast traffic.

Wireless considerations

802.11 wireless networking uses the same range of MAC addresses as wired Ethernet to map IP multicast addresses. However, an 802.11 wireless network handles multicast traffic differently, depending on the configuration of delivery traffic indication message (DTIM), and beacon interval settings. If no stations within the basic service set are in power save mode, multicast packets are sent immediately when they arrive. If there are one or more stations in power save mode, access points then only deliver multicast traffic after each DTIM interval and transmit at one of the supported rates in the basic rate set. In most wireless access points, default configuration for this interval is either 102.4 ms (Beacon interval = 100ms, DTIM = 1) or 204.8 ms (Beacon interval = 100ms, DTIM = 2) and the transmit rate is either 1 Mbit/s or 6 Mbit/s, depending on the operating band and protection mode. The DTIM and beacon interval settings can be adjusted to improve multicast performance in wireless networks.[8]

Unlike Ethernet, most traffic in 802.11 is sent reliably using ACKs and NACKs so that radio interference doesn't cause unbearably high packet loss. However, multicast packets are sent once and are not acknowledged, so they are subject to much higher loss rates. There are various methods for coping with this, such as choosing to unicast multicast data repeatedly to each client, or requesting ACKs from each client.[9] Some methods require only modification on the access point, and are supported in some enterprise-class devices, while other improvements would require modifications to clients, and therefore have not seen widespread adoption.

Secure multicast

IP multicast is an internet communication method where a single data packet can be transmitted from a sender and replicated to a set of receivers. The replication techniques are somewhat dependent upon the media used to transmit the data. Transmission of multicast on an inherent broadcast media such as Ethernet or a satellite link automatically allows the data packet to be received by all the receivers directly attached to the media. In contrast, transmission of multicast on media that is point-to-point or point-to-multipoint requires the packet to be replicated for each link. The replication process should occur in an optimal manner where a distribution tree is built within the network. The packet can be replicated at each of the branches in the tree. This mitigates the requirement for the sender to replicate the packet once for each recipient.

The use of IPsec as a communication link requires a point-to-point connection establishment. Usually, the security is required from sender to receiver which implies the sender must replicate the packet on each of the secure connections - one for each receiver. As the number of receivers grows, the sender must scale by replicating the packet to each of the receivers. The processing load placed on the sender can be high which limits the scalability of the sender. A new method was required to securely transmit multicast and this was referred to as Secure Multicast or Multicast Security.

The Internet Engineering Task Force (IETF) created a new Internet Protocol (IP) to securely transmit multicast traffic across a packet network. The protocol definition was developed in the Multicast Security Workgroup and led to several Request for Comments (RFC) that are now used as standards for securing IP multicast traffic. The protocol allowed a sender to encrypt the multicast packet and forward it into the packet network on the optimal distribution tree. The packet may be replicated at the optimal locations in the network and delivered to all the receivers. The receivers are capable of decrypting the packet and forwarding the packet in the secure network environment. The sender of a multicast packet does not know the potential receivers; therefore, the creation of pair-wise encryption

keys (one for each receiver) is impossible. The sender must encrypt packets using a shared key that all the legitimate receivers use to decrypt the packets. The security of the system is based on the ability to control the distribution of the keys only to those legitimate receivers. For this, the IETF created the Group Domain of Interpretation (GDOI) protocol defined in RFC-6407. The protocol allows the sender and receiver to join a key server where policies and keys are encrypted and distributed to the members of the secure multicast group. The key server can authenticate and authorize senders and receivers into a specific group where the shared key is used to encrypt and decrypt traffic between members of the group.

Reliable multicast

Multicast, by its very nature, is not a connection-oriented mechanism, so protocols such as TCP, which allows for retransmission of missing packets, are not appropriate. For applications such as streaming audio and video, the occasional dropped packet is not a problem. But for distribution of critical data, a mechanism is required for requesting retransmission.

One such scheme, proposed by Cisco, is PGM (originally Pretty Good Multicasting, but changed for trademark reasons to Pragmatic General Multicast), documented in RFC 3208. In this scheme, multicast packets have sequence numbers and when a packet is missed a recipient can request that the packet be re-multicast with other members of the Multicast group ignoring the replacement data if not needed. An expanded version, PGM-CC, has attempted to make IP Multicasting more "TCP friendly" by stepping the entire group down to the bandwidth available by the worst receiver.

Two other schemes documented by the Internet Engineering Task Force (IETF) are: the standards-track protocol NACK-Oriented Reliable Multicast (NORM), documented in RFC 5740 and RFC 5401, and the protocol File Delivery over Unidirectional Transport (FLUTE), documented in RFC 6726. Open-source, in addition to proprietary, implementations exist for these. Other such protocols exist, such as Scalable Reliable Multicast, and are defined by a variety of sources. Such protocols vary in the means of error detection, the mechanisms used in error recovery, the scalability of such recovery and the underlying ideas involved in what it means to be reliable. A list of reliable multicast protocols from the ACM SIGCOMM Multicast Workshop, August 27, 1996, documents a number of approaches to the problem.

Independent groups like the Internet Protocol Multicast Standards Initiative (IPMSI) have claimed that the lack of a truly scalable Secure Reliable IP Multicast protocol like the proposed Secure Multicast for Advanced Repeating of Television (SMART) have hampered the adoption of IP Multicast in inter-domain routing. The lack of a widely adopted system that has AES level security and scalable reliability have kept mass media transmissions of sporting events (like the Super Bowl) and/or breaking news events from being transmitted on the Public Internet.

Reliable IP Multicasting protocols, such as PGM and SMART, are experimental; the only standards-track protocol is NORM (the standards-track revision of RFC 3941 is specified in RFC 5401, the standards-track revision of RFC 3940 is specified in RFC 5740).

Multicast-based protocols

Since multicast is a different transmission mode from unicast, only protocols designed for multicast can be sensibly used with multicast. Most of the existing application protocols that use multicast run on top of the User Datagram Protocol (UDP).

In many applications, the Real-time Transport Protocol (RTP) is used for framing of multimedia content over multicast; the Resource Reservation Protocol (RSVP) may be used for bandwidth reservation in a network supporting multicast distribution. Multicast DNS (mDNS) can be used to resolve domain or host names without a dedicated DNS server by using multicast.

Deployment

IP multicast is widely deployed in enterprises, commercial stock exchanges, and multimedia content delivery networks. A common enterprise use of IP multicast is for IPTV applications such as live television distribution and televised company meetings.

In the hospitality industry IP multicast has become common for IPTV distribution in hotels, and in the retail sector IP multicast is now widely used for TV distribution and video advertising applications.

Pay-TV operators and some educational institutions with significant on-campus student housing have deployed IP multicast to deliver one-way streaming media such as high-speed video to large groups of receivers. Additionally, there have been some uses of audio and video conferencing using multicast technologies. These are far less prevalent and are most often relegated to research and education institutions, which often have a greater degree of network capacity to handle the demands. Some technical conferences and meetings are transmitted using IP multicast. Until recently many of the sessions at the IETF meetings were delivered using multicast.

Another use of multicast within campus and commercial networks is for file distribution, particularly to deliver operating system images and updates to remote hosts. The key advantage of multicast boot images over unicasting boot images is significantly lower network bandwidth usage.

IP multicast has also seen deployment within the financial sector for applications such as stock tickers and hoot-n-holler systems.[10]

While IP multicast has seen some success in each of these areas, multicast services are generally not available to the average end-user. There are two major, related, factors for this lack of widespread deployment. First, forwarding multicast traffic imposes a great deal of protocol complexity on network service providers. Second, core network infrastructure exposes a far greater attack surface, with particular vulnerability to denial-of-service attacks.

The large state requirements in routers make applications using a large number of trees unable to work while using IP multicast. Take presence information as an example where each person needs to keep at least one tree of its subscribers, if not several. No mechanism has yet been demonstrated that would allow the IP multicast model to scale to millions of senders and millions of multicast groups and, thus, it is not yet possible to make fully general multicast applications practical. For these reasons, and also reasons of economics, IP multicast is not, in general, used in commercial Internet backbones.

RFC 3170 (*IP Multicast Applications: Challenges & Solutions*) provides an overview of deployment issues.

History

Development

IP multicasting was first developed by Steve Deering while at Stanford University for which he received the IEEE Internet Award.[11]

The MBONE was a long-running experimental approach to enabling multicast between sites through the use of tunnels. While the MBONE is no longer operational, there is renewed interest in tunneling multicast traffic once again in order to make the service available to a wide array of end users.

CastGate

CastGate was an attempt from the ETRO-TELE research group at the Vrije Universiteit Brussel to adopt IP multicast on the Internet.[12]

Although multicast would have allowed an Internet user to receive rich media and other content without placing a high burden on the net, it was still unavailable to most Internet users. The CastGate project tried to fix this by allowing end users to connect through an automatically configured IP tunnel over networks which did not natively support IP multicast. The idea was that if more users have multicast capability, more content providers would see the benefit of streaming content over multicast. The hope was if enough content providers and users used this service, then more Internet service providers would enable IP multicast natively to their customers.[12]

CastGate supplied a software client for both Microsoft Windows and Linux to connect to the CastGate tunnel network. It also supplied tools to add tunnel servers and tools to receive Session Announcement Protocol announcements from the multicast network with video and audio streams.[13]

The project maintained a web site through 2007.[13]

Commercial deployment

Starting in 2005,[14] the BBC began encouraging UK-based Internet service providers to adopt multicast-addressable services in their networks by providing BBC Radio at higher quality[15] than is available via their unicast-addressed services. This has also been supported by a variety of commercial radio networks, including BBC, GCap Media, EMAP and Virgin Radio.[16]

The German public-service broadcasters ARD[17] and ZDF and the Franco-German network Arte offer their TV program multicasted on several networks. Austrian Internet service provider Telekom Austria offers its digital subscriber line (DSL) customers a TV set-top box that uses multicast addressing in receiving TV and radio broadcasts. In Germany, T-Home, a brand of Deutsche Telekom, offers a similar service.

IP multicast software

- *Media Tools Repository* (https://web.archive.org/web/20070108230830/http://mediatools.cs.ucl.ac.uk/nets/mmedia/), UK: UCL, archived from the original (http://mediatools.cs.ucl.ac.uk/nets/mmedia/) on 2007-01-08 – a collection of tools for the MBone.
- VideoLAN – a free software multicasted video streaming application.
- *Xorp* (http://www.xorp.org/) – a free software router with multicast (IGMP, PIM) support.
- *Smcroute* (https://github.com/troglobit/smcroute) – a simple tool to manipulate multicast routes on the Linux kernel.
- *SSM-ping* (https://web.archive.org/web/20071126235623/http://www.venaas.no/multicast/ssmping/), NO: Venås, archived from the original (http://www.venaas.no/multicast/ssmping/) on 2007-11-26 – tool to test multicast connectivity.
- Wilbert, *IGMP v3* (https://web.archive.org/web/20070826161743/http://www.kloosterhof.com/~wilbert/igmpv3.html), Kloosterhof, archived from the original (http://www.kloosterhof.com/~wilbert/igmpv3.html) on 2007-08-26 – host implementation of IGMPv3 on FreeBSD.
- *IP multi* (ftp://parcftp.xerox.com/pub/net-research/ipmulti/) (software), Palo Alto: Xerox
- *Java Reliable Multicast Service* (https://archive.is/20130130204742/http://labs.oracle.com/techrep/1998/abstract-68.html), archived from the original (http://labs.oracle.com/techrep/1998/abstract-68.html) on 2013-01-30, retrieved 2012-09-08 - libraries and services for building multicast-aware applications

- *PIM implementation* (https://web.archive.org/web/20071224133547/http://netweb.usc.edu/pim/), USC, archived from the original (http://netweb.usc.edu/pim/) on 2007-12-24 – an implementation of the PIM protocol, now obsolete
- *qpimd – PIM Daemon for Quagga* (http://www.nongnu.org/qpimd/), GNU — PIM module for the Quagga Routing Suite.
- *GateD* (https://web.archive.org/web/20070909152315/http://www.nexthop.com/products/gated.html), Next hop, archived from the original (http://www.nexthop.com/products/gated.html) on 2007-09-09 – Unix implementation of routing protocols, including multicast.
- *PIM-DM code for GateD* (https://web.archive.org/web/20071015124705/http://antc.uoregon.edu/GATED/), University of Oregon, archived from the original (http://www.antc.uoregon.edu/GATED/) on 2007-10-15.
- *NORM* (http://cs.itd.nrl.navy.mil/work/norm/), NRL – Nack-Oriented Reliable Multicast from the U.S. Naval Research Laboratory, with an open source C++ implementation.
- *ecmh (Easy Cast du Multi Hub)* (http://unfix.org/projects/ecmh/), Unfix – IPv6 Multicast Daemon, allows IPv6 multicast to be used without the need for PIM.
- MRD6 – IPv6 multicast routing daemon
- UFTP – encrypted UDP based FTP with multicast
- GStreamer – a free software multimedia framework that supports multicast video streaming
- *Mcproxy (Multicast Proxy)* (https://github.com/mcproxy/mcproxy) – an IGMP/MLD Proxy that supports PMIPv6 multicast extensions

See also

- Core-based trees, a proposal for IP multicast scalability

References

1. RFC 988
2. RFC 5771
3. RFC 1112
4. "What Is My IP, Your Address IPv4 IPv6 Decimal on myip" (https://my-ip-is.com). *My Ip Is*.
5. 1968-, Taylor, Ian J. (2009). *From P2P and grids to services on the web : evolving distributed communities*. Harrison, Andrew B., Taylor, Ian J., 1968- (2nd. ed.). London: Springer. ISBN 9781848001220. OCLC 314174970 (https://www.worldcat.org/oclc/314174970).
6. RFC 1112 Section 6.4
7. RFC 2464
8. "802.11 Multicasting" (http://www.wireless-nets.com/resources/tutorials/802.11_multicasting.html). Wireless nets. Retrieved 2008-10-08.
9. "EURASIP Journal on Wireless Communications and Networking" (https://jwcn-eurasipjournals.springeropen.com/). *EURASIP Journal on Wireless Communications and Networking*.
10. *Speakerbus* (http://www.speakerbus.com/), a IP hoot-n-holler provider.
11. *Internet Award recipients* (https://web.archive.org/web/20120916115007/http://www.ieee.org/documents/internet_rl.pdf) (PDF), IEEE, archived from the original (http://www.ieee.org/documents/internet_rl.pdf) (PDF) on 2012-09-16, retrieved 2010-08-26.
12. Marnix Goossen; . Pieter Liefooghe; Arnout Swinnen (30 September 2006). "The CastGateproject: "Enabling Internet multicast for content distribution" " (https://web.archive.org/web/20110526111518/http://www.nordu.net/conference2006/presentations/We11_NORDUnet2006.pdf) (PDF). Archived from the original (http://www.nordu.net/conference2006/presentations/We11_NORDUnet2006.pdf) (PDF) on 26 May 2011. Retrieved 25 May 2013. Presentation at NORDUNET Conference

13. "CastGate: Enabling Internet Multicast" (https://web.archive.org/web/20070928013753/http://www.castgate.net/). Archived from the original (http://www.castgate.net/) on 28 September 2007. Retrieved 25 May 2013.
14. "Rugby union", *News* (http://news.bbc.co.uk/sport1/hi/rugby_union/4290396.stm), UK: The BBC.
15. *Multicast services* (http://bbc.co.uk/multicast), UK: The BBC.
16. "Radio", *Multicast* (https://www.bbc.co.uk/multicast/radio/), UK: The BBC Research & Development, retrieved 19 April 2012
17. *IPTV* (http://www.ard-digital.de/empfang--technik/dvb-t-satellit-kabel-iptv---die-ard-auf-allen-wegen/alles-ueber-iptv), DE: ARD, retrieved 2015-05-17.

External links

- *Multicast over TCP/IP* (http://www.tldp.org/HOWTO/Multicast-HOWTO.html) (Howto), The GNU/Linux documentation project, Mar 1998. Describes Multicast in the Linux kernel, although some sections (specially multicast programs) is outdated and does not cover recent software.
- *Reliable Multicast Transport (rmt)* (https://web.archive.org/web/20071203150138/http://www3.ietf.org/html.charters/rmt-charter.html) (working group), IETF, archived from the original (http://ietf.org/html.charters/rmt-charter.html) on 2007-12-03.
- *Multicast & Anycast Group Membership (magma)* (https://web.archive.org/web/20071214221047/http://www.ietf.org/html.charters/magma-charter.html) (working group), IETF, archived from the original (http://ietf.org/html.charters/magma-charter.html) on 2007-12-14.
- *Protocol Independent Multicast (pim)* (https://web.archive.org/web/20071202041753/http://www.ietf.org/html.charters/pim-charter.html) (working group), IETF, archived from the original (http://ietf.org/html.charters/pim-charter.html) on 2007-12-02.
- *Source-Specific Multicast (ssm)* (https://web.archive.org/web/20070127090246/http://www.ietf.org/html.charters/ssm-charter.html) (working group), IETF, archived from the original (http://ietf.org/html.charters/ssm-charter.html) on 2007-01-27.
- *Multicast Security (msec)* (https://web.archive.org/web/20071216145244/http://www.ietf.org/html.charters/msec-charter.html) (working group), IETF, archived from the original (http://ietf.org/html.charters/msec-charter.html) on 2007-12-16.
- *Multicast* (http://www.sockets.com/ch16.htm#Multicast), Sockets. IP details.
- *IP-Ethernet multicast* (http://www.firewall.cx/multicast-intro.php) (tutorial), CX: Firewall.
- *IP Multicast* (http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html) (video), Cisco.
- "Overview of Reliable Multicast methods", *ACM SIGCOMM Multicast Workshop* (http://www-net.cs.umass.edu/sigcomm_mcast/talk1.html), University of Massachusetts, August 27, 1996.
- Floyd, *A Reliable Multicast Framework for Light-weight Sessions and Application Level Framing* (http://www.icir.org/floyd/srm-paper.html), ICIR. The paper defining Scalable Reliable Multicast.
- *An Analysis of Multicast Methods* (http://tech-talk.wikidot.com/an-analysis-of-multicast-methods), Wikidot, retrieved 2019-05-03.
- Noormohammadpour, Mohammad; Raghavendra, Cauligi S.; Rao, Sriram; Kandula, Srikanth (2017), *DCCast: Efficient Point to Multipoint Transfers Across Datacenters* (https://www.researchgate.net/publication/316921061), USENIX Association, arXiv:1707.02096 (https://arxiv.org/abs/1707.02096), Bibcode:2017arXiv170702096N (https://ui.adsabs.harvard.edu/abs/2017arXiv170702096N), retrieved 2019-05-03.
- *Overview of the Internet Multicast Routing Architecture* (https://tools.ietf.org/html/rfc5110). January 2008. doi:10.17487/RFC5110 (https://doi.org/10.17487%2FRFC5110). RFC 5110 (https://tools.ietf.org/html/rfc5110).