White Paper

IP Multicast Technical Overview

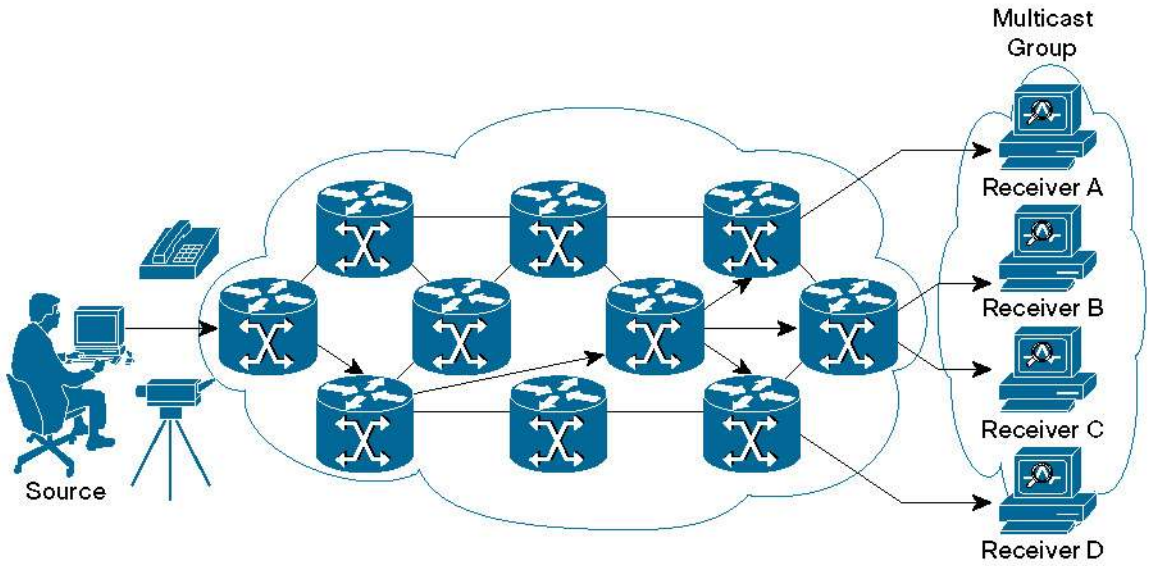
This paper provides an introductory overview of IP Multicast. It is assumed that the reader is familiar with TCP/IP and networking in general. Please refer to Beau Williamson's book, *Developing IP Multicast Networks, Volume 1* (Cisco Press, 1999), for additional information relating to the topics discussed in this overview.

INTRODUCTION

Traditional IP communications allow a host to send packets to another host (unicast transmissions) or to all hosts (broadcast transmissions). IP Multicast provides a third communication alternative: allowing a host to send packets to a group that is made up of a subset of the hosts on the network. IP Multicast is a bandwidth-conserving technology specifically designed to reduce traffic by simultaneously delivering a single stream of information to potentially thousands of corporate recipients or homes. By replacing copies for all recipients with the delivery of a single stream of information, IP Multicast is able to minimize the burden on both sending and receiving hosts and reduce overall network traffic. Within a multicast network, routers are responsible for replicating and distributing multicast content to all hosts that are listening to a particular multicast group (see Figure 1). Cisco® routers employ Protocol Independent Multicast (PIM) to build distribution trees for transmitting multicast content, resulting in the most efficient delivery of data to multiple receivers.

Alternatives to IP Multicast require the source to send more than one copy of the data. Traditional application-level unicast, for example, requires the source to transmit one copy for each individual receiver in the group.

Figure 1. Multicast Transmission to Many Receivers



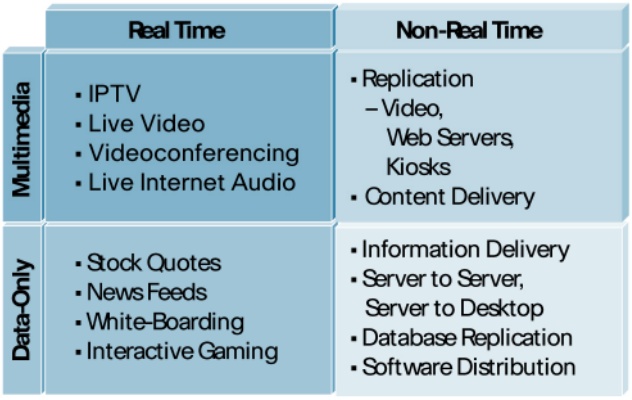
MUTLICAST APPLICATIONS AND ENVIRONMENTS

IP Multicast solutions offer benefits relating to the conservation of network bandwidth. In the case of a high-bandwidth application, such as MPEG video, IP Multicast can benefit situations with only a few receivers because a few video streams would otherwise consume a large portion of the available network bandwidth. Even for low-bandwidth applications, IP Multicast conserves resources when transmissions involve thousands of receivers. Additionally, IP Multicast is the only nonbroadcasting alternative for situations that require simultaneously sending information to more than one receiver.

For low-bandwidth applications, an alternative to IP Multicast could involve replicating data at the source. This solution, however, can deteriorate application performance, introduce latencies and variable delays that impact users and applications, and require expensive servers to manage the replications and data distribution. Such solutions also result in multiple transmissions of the same content, consuming an enormous amount of network bandwidth. For most high-bandwidth applications, these same issues make IP Multicast the only viable option.

Today, many applications commonly take advantage of multicast, as shown in Figure 2.

Figure 2. Different Types of IP Multicast Applications



Other applications that take advantage of IP Multicast include:

- Corporate communications
- Consumer television and music channel delivery
- Distance learning (for example, e-learning) and white-boarding solutions
- IP surveillance systems
- Interactive gaming

IP Multicast is supported in:

- IPv4 networks
- IPv6 networks
- Multiprotocol Label Switching (MPLS) VPNs
- Mobile and wireless networks

IP Multicast capabilities can be deployed using a variety of different protocols, conventions, and considerations suited to the different network environments just mentioned. Multicast services can also be deployed across multiple protocol platforms and domains within the same network.

By implementing native IP Multicast functionality inside MPLS VPN networks, service providers can more efficiently deliver bandwidth-intensive streaming services such as telecommuting, videoconferencing, e-learning, and a host of other business applications. Cisco Multicast VPN technology eliminates the packet replication and performance issues associated with the traffic relating to these applications. Multicast MPLS VPNs further benefit service providers by:

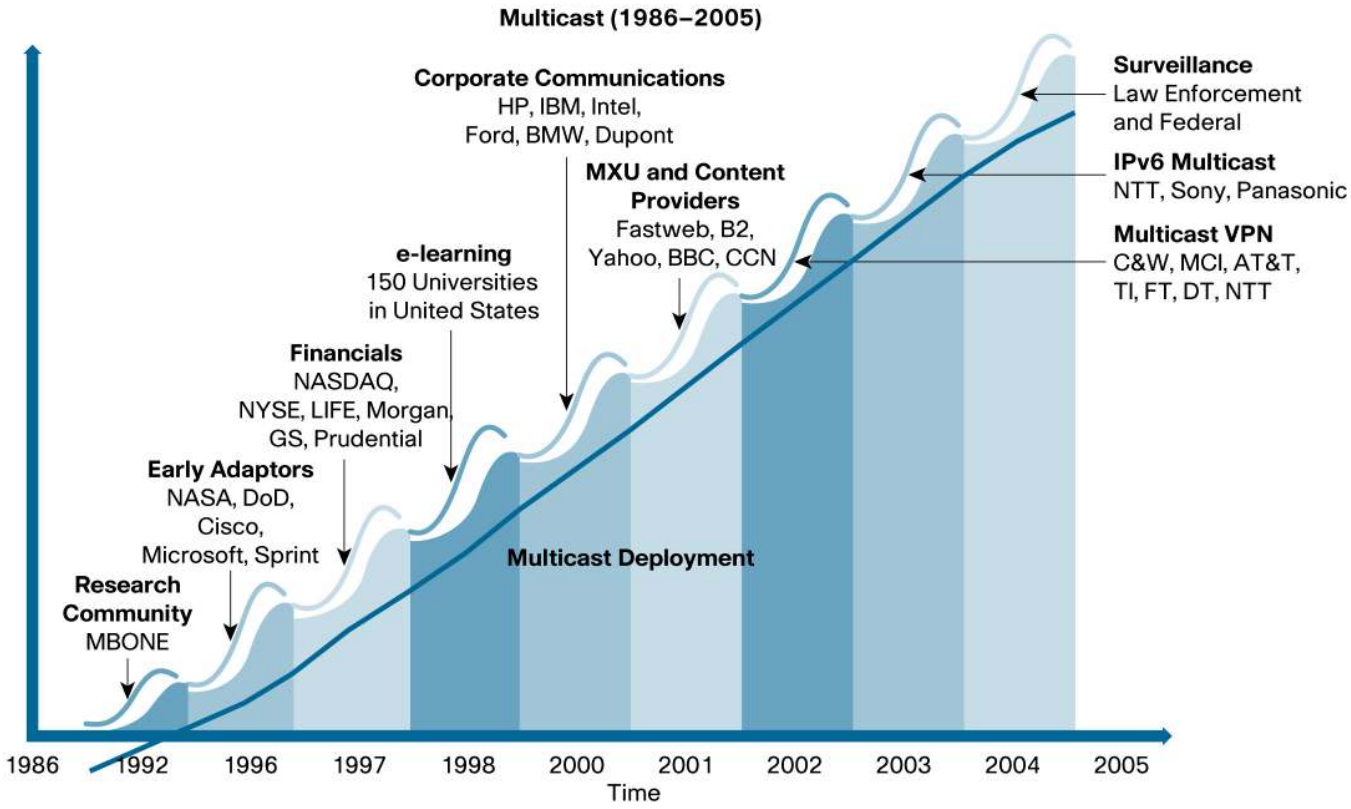
- Minimizing configuration time and complexity – configuration is required only at edge routers
- Ensuring transparency of the service provider network
- Providing the ability to easily build advanced enterprise-friendly services such as Virtual Multicast Networks
- Increasing network scalability

IP Multicast can work with Cisco Mobile Networks. An IP Mobility platform extends the network with traditional fixed-line access to an environment that supports mobile wireless access. Multicast, from the point of IP Mobility, is a network service or application. Within an IP Mobility environment, IP Multicast can be employed to deliver content to users with wireless devices. An example is the Cisco Mobile Networks Tunnel Template feature. Using this feature, service providers can configure multicast on statically created tunnels to be applied to dynamic tunnels brought up on the home agent and mobile router. A tunnel template is defined and applied to the tunnels between the home agent and mobile router. The mobile router can now roam and the tunnel template enables multicast sessions to be carried through to mobile users.

INCREASING DEMAND FOR IP MULTICAST

Over the past decade, enterprise and public sector adoption of IP Multicast-enabled applications has skyrocketed (see Figure 3), and service providers have responded by increasingly adding multicast VPNs to service portfolios. Today, any service provider with enterprise customers must support IP Multicast to remain competitive. The deployment of video services provides further incentives for the strengthening of a service provider's multicast platform, because it offers the most efficient, cost-effective means of supporting triple-play traffic (data, voice, and video).

Figure 3. Multicast Deployments



TECHNICAL OVERVIEW

Multicast Groups

Networks using IP Multicast deliver source content to multiple users (hosts or receivers) that are interested in the data stream. A multicast channel refers to the combination of a content source IP address and the IP Multicast group address to which the content is being broadcasted. Unlike unicast/broadcast addresses, multicast groups do not have any physical or geographic boundaries, and receivers interested in joining can be located anywhere on a network or the Internet as long as a multicast-enabled path has been established.

To receive a particular multicast data stream, hosts must join a multicast "group" by sending an Internet Group Management Protocol (IGMP) message to their local multicast router. Almost all networks and applications use either IGMP Version 2 or 3. IGMPv2/3 allows individual receivers to independently join or leave a group.

Content is identified by "(S,G)" where G is the multicast group and S is the sending source IP address. The multicast group address lies in the Class D IP address space. The content provider/owner and service providers select the multicast address based on the local multicast addressing policy (whether multicast applications are local or global in scope).

Multicast Forwarding and Distribution Trees

In a multicast network, routers are responsible for replicating source content and forwarding it to multiple recipients. Routers use the PIM protocol to build "distribution trees" for multicast routing in the network. Routers replicate source content at any point where the network paths diverge, and use Reverse Path Forwarding (RPF) techniques to ensure content is forwarded to the appropriate downstream paths without routing loops.

Multicast-capable routers dynamically create distribution trees that control the path the content travels through the network. PIM uses two types of multicast distribution trees: “shared trees” and “source trees.” Services and applications can exclusively use shared trees (Bidirectional [Bi-Dir]), exclusively use source trees (Source Specific Multicast [SSM]), or use a combination of the two (Any-Source Multicast [ASM]).

Routers may create shared trees so that a single distribution tree can be shared by all sources. Alternatively, a separate source tree can be built for each source. Source trees offer the most optimal paths (and least latency) for multicast traffic, whereas shared trees consume much lower router memory resources.

Because members of multicast groups can join or leave at any time, distribution trees must be updated constantly. When all the active receivers on a particular branch stop requesting traffic for a particular multicast group, routers along the path will “prune” that branch from the distribution tree and stop forwarding traffic down that branch. If one receiver on that branch becomes active and requests the multicast traffic, the router will dynamically modify the distribution tree and resume forwarding traffic over that branch.

Security Requirements

To protect multicast content and multicast service networks, network administrators should address the following security considerations:

- *Service-level security* – Networks using IP Multicast can use filtering mechanisms to ensure that data streams are sent (and new distribution tree branches created) only for legitimate receivers and requesting routers. Service providers may use SSM along with Extended ACL support for SSM, which requires that the source address be supplied by any host requesting to join a multicast group. Using this combination of SSM and Extended ACL for SSM protects the network from rogue senders that might try to inundate the network with unauthorized traffic.
- *Access and admission control* – IP Multicast networks should use access control mechanisms such as access control lists (ACLs) and IGMP access groups to control access to multicast-capable routers. Quality of service (QoS) policing and queuing mechanisms, as well as multicast route-limiting mechanisms, provide additional access control for multicast networks. Multicast authentication, authorization, and accounting (AAA) integration can also be used for user authentication purposes within a multicast context.
- *Policing multicast networks* – Multicast networks require mechanisms not only to recognize illegitimate multicast groups, but to disable unauthorized groups, group ranges, and, if necessary, network routers.
- *Firewall protection* – New Cisco PIX® security platforms (such as the Cisco ASA 5500 Series Adaptive Security Appliances running Cisco PIX Firewall Software Version 7.0) provide PIM support. This feature eliminates the need to “tunnel” multicast traffic through the firewall, which would otherwise circumvent security policies.
- *Native IP Multicast data encryption* – New Cisco IOS® Secure Multicast provides a set of hardware and software features necessary to secure IP Multicast group traffic originating on or flowing through a Cisco IOS device. It combines the keying protocol Group Domain of Interpretation (GDOI) with IP Security (IPsec) encryption to provide users an efficient method to secure IP Multicast group traffic. With Cisco IOS Secure Multicast, a router can apply encryption to IP Multicast traffic without having to configure generic routing encapsulation (GRE) tunnels.

High-Availability Considerations

To ensure that critical multicast applications are reliable and highly available, network administrators delivering IP Multicast services should:

- *Eliminate any single point of failure* – Multicast networks should be architected to protect the entire path, from the source all the way to every receiver. The loss of any single router should not result in a disruption to the multicast stream at any point in the network.

- *Design networks that can dynamically respond to problems* – Network architects should use multicast protocols and strategies, such as "anycast" techniques for source redundancy, network topologies that provide path redundancies, and route processor redundancy in each node. These features ensure that the multicast network can immediately and automatically respond to the loss of any single source or network segment, and rapidly rebuild multicast trees as needed.
- *Build scalability into the network* – IP Multicast networks should be able to absorb growth dynamically, to ensure that usage spikes do not overwhelm the system.
- *Employ high-availability techniques* – Network architects should use mechanisms such as stateful switchover (SSO) and Cisco In-Service Software Upgrade (ISSU) support to help ensure availability in multicast IPv4, IPv6, and VPN environments.

Managing Multicast Networks

To effectively manage multicast environments, network administrators can use the following technologies:

- *Multicast MIBs*, which can be used with Simple Network Management Protocol (SNMP) tools to assess multicast network performance, identify issues and potential issues, and plan for network growth
- *Multicast traps* that can notify SNMP tools of multicast problems and errors such as invalid PIM messages and group changes
- *Multicast "heartbeat" mechanisms*, which confirm traffic stream activity and help prevent critical sections of a multicast group from being cut off from the data stream
- *Multicast Syslog and NetFlow mechanisms*, which provide Syslog and NetFlow information for large-scale network management tools and network event correlation engines
- *Cisco Multicast Manager software*, which provides a Web-based network management interface for multicast monitoring, diagnostics, health checks, and reporting

CISCO IP MULTICAST TECHNOLOGY LEADERSHIP

Cisco Systems® was an early innovator of IP Multicast, and has provided IP Multicast technology for more than a decade. The table in Figure 4 highlights important Cisco contributions to multicast technology between 1994 and 2004.

Figure 4. Cisco Multicast Industry Contributions

Multicast Protocol Support: 10-Year History

10 Years of Cisco IOS IP Multicast	
1994	PIMv1 SM/DM, IGMPv1/v2, DVMRP Interoperability
1995	Fast-Switching, SAP/SDR, PIM/IGMP/Cisco-IPMRoute MIB, Mtrace, NBMA Mode
1996	AutoRP, CGMP, CMF
1997	MDFS, RFC2337 ATM MPS
1998	PIMv2 SM/DM, BSR, IPMRoute MIB, MBGP, Multicast Source Delivery Protocol (MSDP)
1999	MMLS, MRM, PGM Router Assist, IGMP/Tunnel UDLR, NTP Multicast, Multicast NAT, Multicast TAG Switching, UDPTN
2000	SSM (IGMPv3, IGMPv3lite, URD), Bidir-PIM, MSDP MIB, PIM-DM SR, Heartbeat, RGMP, MVoIP, HW IGMP Snooping, IGMP MRoute Proxy
2001	Cisco PIM Traps, MSDP SA Limits, IGMP-STD MIB
2002	MVPN/VRF-lite (PIM-DM/SM/Bidir, AutoRP/BSR, IGMPv3, MSDP, Default/Data-MDT), Multicast/PIM Scalable Convergence, IGMP Limits, MRoute-STD MIB
2003	IPv6 Multicast (MRIB/MFIB, PIMv2 SM, SSM, MLDv2) SSM Mapping, NetFlow v9 Multicast, Mobile-IP + Multicast, PIM Snooping
2004	RPF-Vector, Inter-AS MVPN, MVPN MIBS, RFC3618 MSDP, MSDP MD5, IPv6 BSR, IPv6 Bi-Dir-PIM, SSM Filtering

More recent Cisco IOS Software multicast innovations include:

- SSM Mapping for IPv4 and IPv6 Multicast (DNS-based)
- Multicast High Availability: Triggered PIM Join
- Multicast High Availability: IGMP High Availability
- Multicast Subsecond Convergence
- Multicast Fast Join/Leave for Faster Channel Change
- Multicast Source Redundancy
- Multicast AAA Integration
- NetFlow Data Export (NDE) v9 for Multicast
- IGMP Static-Group Range support
- Ability to disable multicast group ranges
- Extended ACL support for IGMP to support SSM
- Per-Interface Mroute State Limits
- SSM (S,G) filtering support on multicast boundary
- Multicast Source Discovery Protocol (MSDP) Message Digest Algorithm 5 (MD5) password authentication
- No Dense Mode Fallback after Rendezvous Point (RP) information loss
- IGMP/MLD Limit Command(s)

DELIVERING MULTICAST SERVICES WITHIN A CISCO IP NEXT-GENERATION NETWORK

To effectively respond to changing market and changing customer demands, service providers require an innovative, converged infrastructure that can accommodate multicast capabilities. A Cisco IP Next-Generation Network (NGN) provides the:

- *Mobility* of a cellular network, allowing extensive roaming of all its services
- *Bandwidth* of an optical network, transparently supporting any type of service
- *Flexibility* of Ethernet, so that it can be deployed quickly and used easily
- *Security* of a private network, protecting traffic even when a service traverses a public network

A Cisco IP NGN also allows service providers to achieve:

- *Levels of service awareness*: Recognizing the type, priority, and needs of a service
- *Service richness*: The ability to manage many different and distinct services simultaneously, with the ability to add more as needed
- *Service flexibility*: The ability to deploy and offer the service in different ways to match the needs of the customer

For customers, a Cisco IP NGN can deliver a better experience by providing a much broader range of on-demand services, tailored to their unique needs. At the same time, it simplifies the service provider's operational responsibilities while providing them the means to earn more revenue and increase brand awareness and customer loyalty.

By providing a highly efficient, cost-effective, and secure means of delivering innovative enterprise applications and consumer triple-play services, Cisco IP Multicast technologies represent a critical component of the Cisco IP NGN vision. By employing innovative Cisco IP Multicast strategies, service providers can immediately enhance service delivery while laying a robust foundation for future services and applications.

FURTHER READING

Developing IP Multicast Networks, 1999, Cisco Press:
http://www.cisco.com/en/US/tech/tk828/tk363/tsd_technology_support_sub-protocol_home.html

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.com 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

Printed in USA C11-355686-00 06/06