White Paper

Multicast Services for IP Triple-Play Networks

At one time, networks were challenged to provide robust e-mail and high-speed data services. Then e-commerce became a primary focus, often mission-critical. Today, networks must reach people anywhere in the world with data, voice, video, and mobile services quickly and efficiently. Broadcast of IP video is a new frontier for enterprises and service providers that makes content delivery over the network a compelling proposition. Cisco Systems® has worked for more than a decade to perfect multicast forwarding and routing, making it the most efficient method of video broadcasting in networks today. Technologies in Cisco IOS® Software, Cisco® platforms, and triple-play (data, voice, and video) architectures make multicast applications over IP triple-play networks flexible, reliable, secure, and scalable to ensure a dependable, high-quality user experience.

This paper provides an overview of multicast services in IP triple-play networks. It includes a review of multicast applications, multicast varieties, relevant protocols and technologies, and architectural considerations for delivering scalable multicast traffic efficiently, securely, and economically.

SUMMARY

Increasingly, customers are relying on IP broadcasting to bring enhanced value to a broad new spectrum of platforms and applications—interactive videoconferencing, digital TV, digital audio, online movies and concerts, networked gaming, Internet-enabled PDAs and home appliances, content synchronization, and broadband access.

Multicast is a well-established bandwidth-conserving technology that reduces traffic by allowing a host to send packets to a subset of all hosts as a group transmission instead of having to send packets to every single user. IP Multicast delivers application source traffic to multiple receivers without burdening the source or the receivers while using a minimum of network bandwidth and enabling easily scalable and economical distributed applications. Multicast packets are replicated in the network at the point where paths diverge by Cisco routers enabled with Protocol Independent Multicast (PIM) and other supporting multicast protocols, resulting in the most efficient delivery of data to thousands and even millions of business or consumer users.

Common Multicast Applications in Triple-Play Networks

Multicast application types include *one to many* (such as IPTV, Internet radio, stock news), *few to few* (small video broadcasts or audio conferences), *few to many* (publishing), *many to many* (stock trading, gaming), and *many to one* (which involves a two-way request and response, such as polling or online auctions).

IPTV

IPTV is the broadcast of IP video, based on a few-to-many video multicast. It can include live or rebroadcast content or synchronized presentations. Many service providers are already offering IPTV. As millions of consumers enjoy IP video services in coming years, service providers and business enterprises are adding the necessary functionality between the video application and the network. Cisco has been working closely with leading video vendors and standards bodies such as the IETF, Digital Video Broadcasting (DVB) Forum, and Internet Streaming Media Alliance (ISMA) to define this internetworking layer, and Cisco has applied time-tested IP technologies for multicast, quality of service (QoS), and security to the video distribution process.

Building on extensive experience in developing triple-play residential Metro Ethernet architectures and solutions, Cisco has engineered the use of Cisco IP Multicast with Source Specific Multicast (SSM) to provide for bandwidth-efficient delivery of broadcast video while providing greater simplicity and inherent security than in previous versions of multicast routing. Cisco also has features useful for the control and authentication of multicast users and which IPTV channels they can tune into using multicast authentication, authorization, and accounting (mAAA). Also available is Multicast Admission Control, which includes a method to monitor the bandwidth utilized by a set of users watching standard and high-definition MPEG2 and MPEG4. This is a critical feature because an oversubscribed Ethernet link could affect the signal quality to users watching IPTV. IP QoS protects critical traffic from congested networks. The Cisco IOS Software IP service level agreement (SLA) feature in routers continuously monitors network performance, fast convergence, broadcast source redundancy for high availability, and load balancing for optimal use of available capacity on redundant links.

Hoot ‘n’ Holler over IP

Hoot ‘n’ holler applications date back 50 years, to when local concentrations of small, specialized businesses needed to communicate time-critical information. These networks functioned as early business-to-business intercom systems. They have since evolved into specialized, always-on, leased-line networks used by financial and brokerage firms to trade stocks and currency futures and to provide time-critical information such as market updates. Other users of hoot ‘n’ holler networks include news agencies, government and municipal emergency response agencies, and airlines.

Hoot ‘n’ holler in an IP triple-play network can be configured to support multiple “hoot groups” on a single connection, an example of one-to-many multicasting. Each hoot group represents a separate hoot ‘n’ holler session, which broadcasts and receives voice traffic to specific endpoints. Bandwidth-conserving technologies, including Bidirectional Protocol Independent Multicast (Bi-Dir PIM), standard voice over IP (VoIP), voice activity detection (VAD), and QoS, run the service with as little impact to other applications as possible.

Other markets that use multicast applications include:

- Education
- Corporate communications
- Surveillance
- Childcare
- Healthcare
- The military

Key Protocols and Technologies for Delivering Multicast in Triple-Play Networks

Multicast technology and protocols must be present in the core, edge, and access layers of an IP triple-play network. Security must also be deployed throughout, along with a high-availability architecture end to end. IP Multicast can be packaged into two solutions from a functional standpoint: intradomain and interdomain multicast.

Intradomain Multicast Protocols

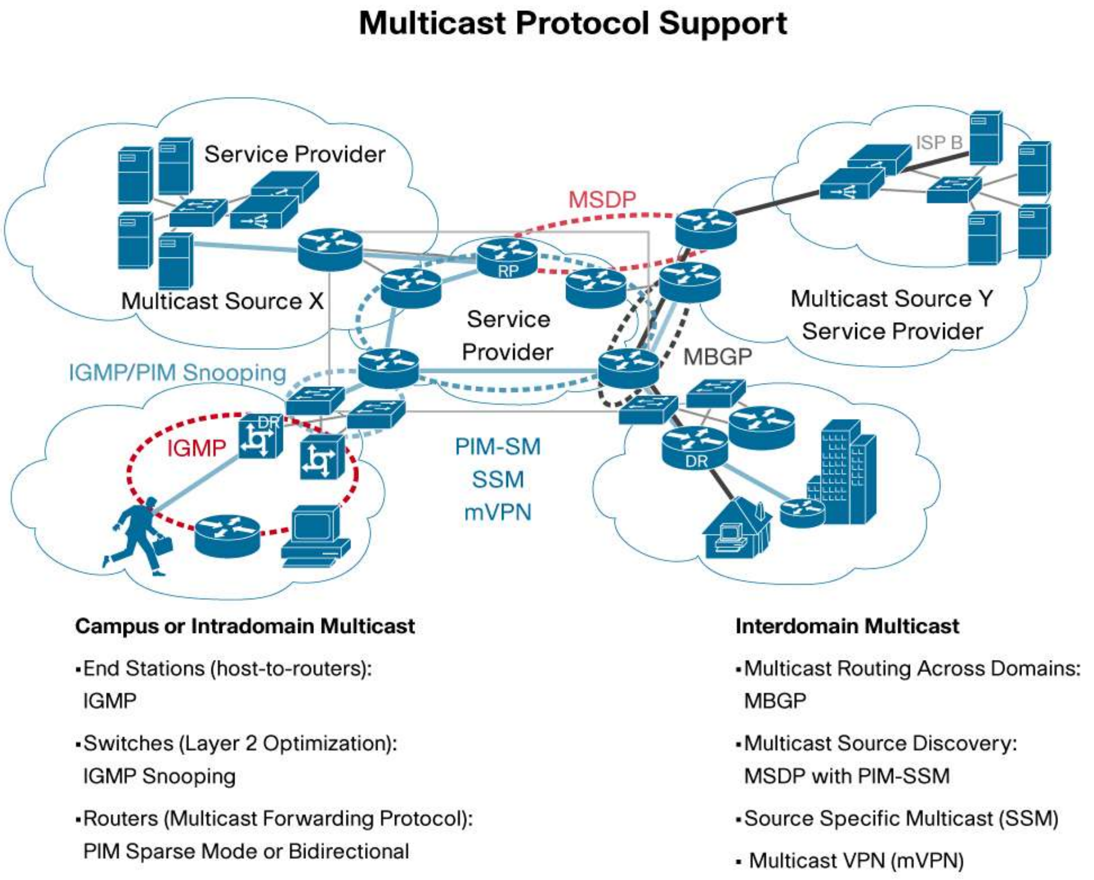
Intradomain or basic multicast supports multicast applications within an enterprise campus or WAN. Cisco IOS Software features these protocols to support intradomain multicast:

- Internet Group Management Protocol (IGMP) is present at the end stations, between the hosts and routers. It is used by hosts to inform routers of their need to receive data addressed to a specific multicast group. When a host wants to join a multicast group, it sends an IGMP “join” message to the network’s router. The router then uses a multicast routing protocol to inform other routers of its desire to receive packets destined for the multicast router. The router may also use IGMP to query the attached network segments for specific group members. IGMPv3 is the basis for SSM. IGMP snooping is a method by which a switch can constrain multicast to only those ports that have requested the stream.

- Protocol Independent Multicast (PIM) is available in sparse, dense (used for Auto-Rendezvous Point) bidirectional, and SSM modes and provides intradomain multicast forwarding support for all underlying unicast routing protocols. Sparse mode relies upon an explicit joining method before attempting to send multicast data to receivers of a multicast group.
- Pragmatic General Multicast (PGM) is a reliable multicast transport protocol for applications that require ordered, duplicate-free multicast data delivery. PGM guarantees that a receiver in a multicast group either receives all data packets from transmissions and retransmissions or can detect unrecoverable data packet loss. It also manages retransmission of lost packets in a scalable fashion.
- Multicast Virtual Private Network (mVPN) makes it possible for a native IP or Cisco IP Multiprotocol Label Switching (MPLS) backbone to support multiple multicast services across any existing access technology, such as ATM, Frame Relay, or Ethernet. Cisco IP/MPLS mVPN technology allows for a single multicast source stream to be replicated in a network with precision and security. With the Cisco mVPN technology, enterprise networks and service providers can dynamically instead of manually provide multicast support over MPLS networks.

As shown in Figure 1, IGMP is a Layer 2 end station management or host-to-router protocol that requests admission to join or leave multicast groups. IGMP snooping handles switch membership management, ensuring that the switch intelligently handles multicast forwarding without flooding the network and lets the broadcast go only to those ports that requested it. At Layer 3, multicast routing protocols are required to build the multicast tree in an optimal fashion across the network. To accomplish this, Cisco designed PIM, a multicast routing protocol designed to operate over an IP network. PIM sparse mode ensures that the network has appropriate information necessary to forward multicast packets down a multicast distribution tree from source to destination.

Figure 1. Two Basic Multicast Topologies and Associated Protocols


Multicast Protocol Support
Service Provider
Multicast Source X
MSDP
ISP B
RP
Service Provider
Multicast Source Y Service Provider
MBGP
IGMP/PIM Snooping
DR
IGMP
PIM-SM
SSM
mVPN
DR
Campus or Intradomain Multicast
▪End Stations (host-to-routers): IGMP
▪Switches (Layer 2 Optimization): IGMP Snooping
▪Routers (Multicast Forwarding Protocol): PIM Sparse Mode or Bidirectional
Interdomain Multicast
▪Multicast Routing Across Domains: MBGP
▪Multicast Source Discovery: MSDP with PIM-SSM
▪Source Specific Multicast (SSM)
▪ Multicast VPN (mVPN)

Interdomain Multicast Protocols and Features

Interdomain routing and source discovery for multicast applications across domains comprising an enterprise and service provider networks are supported by protocols in Cisco IOS Software that include:

- Multiprotocol Border Gateway Protocol (MBGP) is a Border Gateway Protocol (BGP) extension that handles multicast routing policy throughout the Internet and connects multicast topologies within and between BGP autonomous systems.
- Multicast Source Discovery Protocol (MSDP) allows multiple PIM sparse mode domains to share information about active sources. It also announces active sources of multicast transmissions to MSDP peers and interacts with MBGP for interdomain operations.
- Source Specific Multicast (SSM) enables data forwarding based on both group and source addresses. With SSM, multicast packets originating in only a specific source address can be delivered to any receiver that requests it. It limits the original multicast model to one host, simplifying the requirements on the network, including security requirements. With SSM the receivers must specify the source address using IGMPv3 or Multicast Listener Discovery (MLD) in IP Version 6 (IPv6).
- The mVPN Interautonomous System (Inter-AS) feature allows multicast distribution tree tunnels to be set up between the provider edge routers of different service providers without the need to share routing information between them.

Another Cisco innovation that increases the efficiency of multicast transport and is important for residential providers is Multicast Virtual LAN Registration (MVR). MVR involves the creation of separate, dedicated virtual LANs (VLANs) constructed specifically for multicast traffic distribution. Each Cisco Catalyst® switch that receives an MVR stream examines each multicast group and internally bridges the multicast VLAN traffic to a particular subscriber that has requested the multicast stream. This is yet another feature Cisco has developed to help providers offer new and incremental services to their customers.

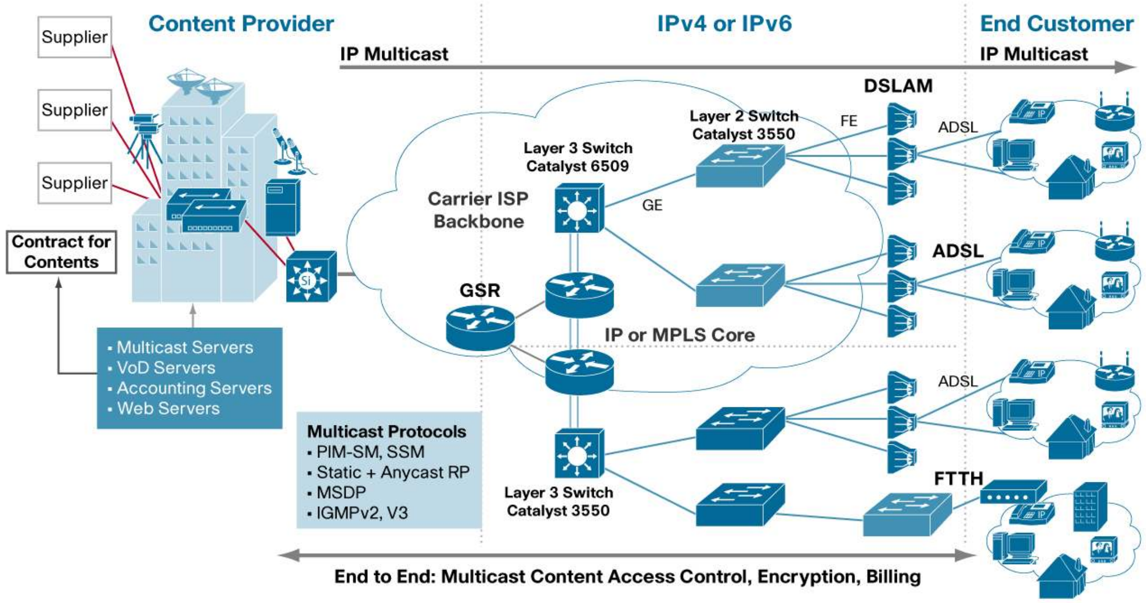
These multicast features and others in Cisco IOS Software allow IP triple-play networks to efficiently deploy, scale, and manage secure distributed group applications across the Internet. For every market, Cisco has multicast solutions that are designed to save network costs by conserving bandwidth and server processing, to apply QoS and admission control parameters, and to be flexibly managed with device-level instrumentation and other powerful management applications.

CHALLENGE

Service providers offering triple-play services must be able to scale broadcast video to hundreds, thousands, or millions of receivers, necessitating fast convergence in the core and edge and fast channel changes for PCs, video phones, television set-top boxes, and other devices at the access layer.

Upstream and downstream speeds alone are no longer enough to satisfy consumer expectations. Given the extremely delay-sensitive nature of video—where more than one error in one million packets may be noticeable to viewers—coupled with its bandwidth-intensive nature, service providers must design their triple-play networks with technologies that can differentiate between each service and apply appropriate QoS and priority to video. Networks must be flexible enough to enable multiple content source injection points from different content suppliers (Figure 2).

Figure 2. IP Multicast in a Triple-Play Architecture



Multicast applications must be able to run over IPv4, IPv6, or dual-stack networks, as the transition to IPv6 moves forward. Additionally, the full complement of control, security, and provisioning functions must be available.

SOLUTION

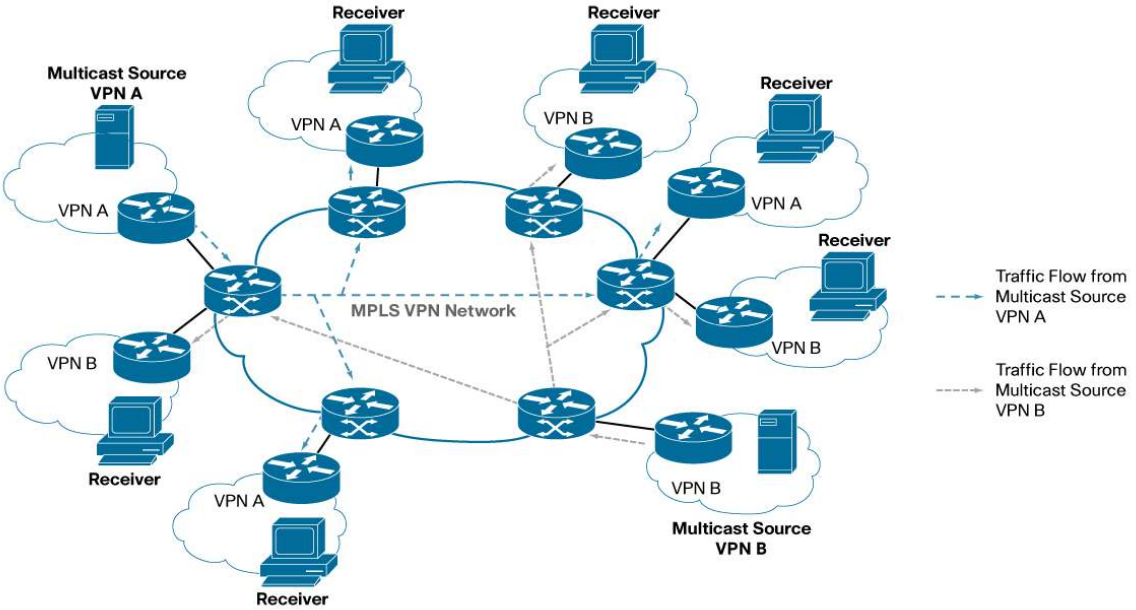
Cisco IOS Software multicast solutions for IP triple-play networks provide customers with a variety of options, based on their specific requirements. Robust security, management, troubleshooting, and deployment tools are all available as well.

Multicast provides interactive, reliable campus multicast for interactive distance learning, corporate videoconferencing, inventory updates, software and content distribution. Core Multicast, which includes PIM, IGMP, and Pragmatic General Multicast (PGM), provides interactive Internet multicast across domains for network gaming, intercompany conferencing, Internet software distribution, and extranet content distribution. Enhanced Multicast includes MBGP, MSDP, and all of the protocols supported in Core Multicast.

Multicast VPNs

A Cisco native IP or Cisco IP Multiprotocol Label Switching (MPLS) backbone can support multiple multicast networks through multicast virtual private networks (VPNs), which allow enterprises and service providers to offer IP Multicast services across any existing access technology, such as ATM, Frame Relay, or Ethernet (Figure 3). Instead of delivering multicast to multiple recipients through a point-to-point mesh of tunnels and sending multiple copies of the same multicast data across the network backbone, Cisco IP/MPLS multicast VPNs transmit a single multicast source stream, and this stream is replicated in the network where paths diverge with routers enabled with intradomain multicast protocols. MVPN uses PIM protocols, which have proven scalability, having been deployed in networks for customers that include financial institutions with critical market data and a large number of endpoints.

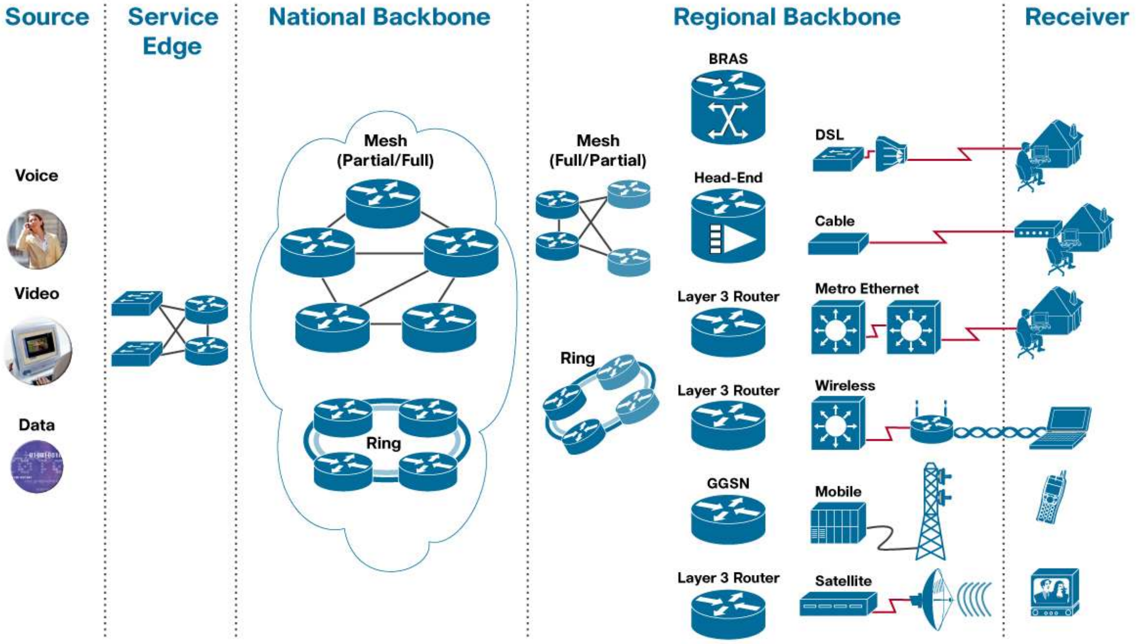
Figure 3. Multicast VPN



Architectural Considerations for Multicast

Cisco IOS Software multicast technologies are flexible to fit a variety of different network architectures and topologies. Many cable service providers have ring topologies in the backbone and in the distribution layer (Figure 4). Other providers and enterprise networks may have a hub-and-spoke architecture. Regardless of the topology, multicast must be deployed throughout the network. Different types of multicast applications are more suited to different architectures.

Figure 4. Multicast in Triple-Play Networks



In point-to-multipoint applications, for example, a single multicast stream is replicated at “branch points” in a switched hub-and-spoke network to reach multiple viewers. This is useful for unidirectional, live broadcasts such as corporate communications or media events. It is also useful for content distribution from a central server to collocated servers or software distribution from a data center to multiple end station PCs or servers. In certain cases the data flow may also be bidirectional, such as multiple distance-learning connections to a single classroom.

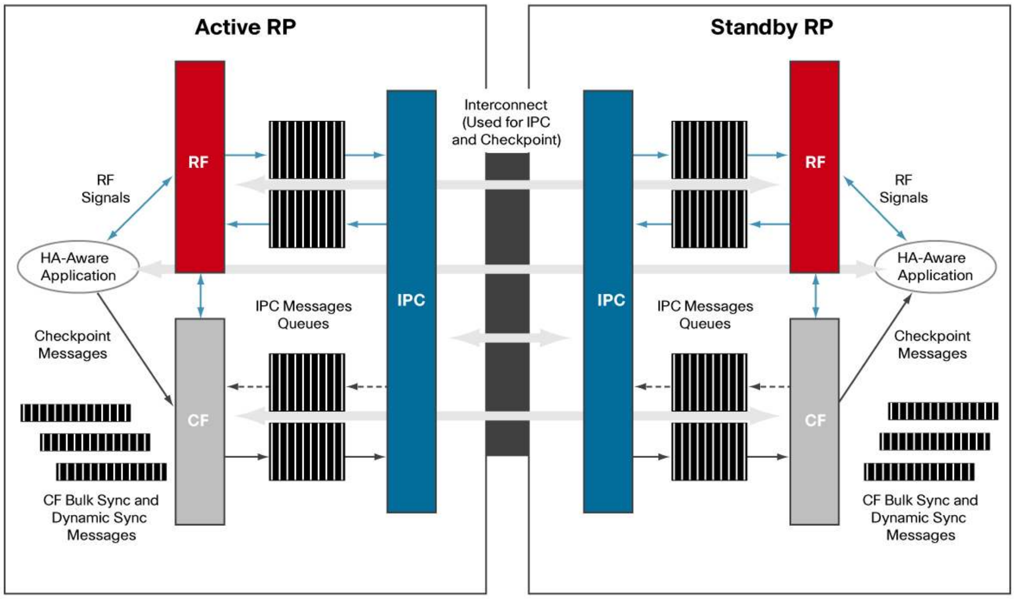
In multipoint-to-multipoint applications, a bidirectional hub-and-spoke architecture in which a multipoint controller unit (MCU) receives and redirects signals from each member of a multicast conference is optimal. This is useful for videoconferences in which all participants collaborate or for online gaming services.

Other multicast applications shown in Figure 4 are video broadcasts to residential users through a broadband remote access server on a DSL connection, a headend router to a cable connection, and a Layer 3 router to a Metro Ethernet connection. Wireless video broadcasts are also possible with a Layer 3 router and a wireless card or a Gateway General Packet Radio Service (GPRS) Support Node (GGSN) interface over a cell tower to a phone or over a satellite feed from a Layer 3 router to a television.

Ensuring High Availability

Besides general network best practices for high availability, Cisco has engineered high availability for multicast services into specific router and switch platforms through device redundancy and Cisco IOS Software failover features. Since video is extremely delay sensitive, high availability is critical to the user experience. In platforms such as the Cisco 7600 Series routers that support dual route processors—which are router modules or cards that collect routing-table information and then update the router’s line modules or cards with the information—a failure in one route processor triggers a failover mechanism through the Stateful Switchover (SSO) feature in Cisco IOS Software, where an adjacent, redundant route processor takes over (Figure 5). SSO synchronizes IP communications (IPC) between the route processors. If the active route processor fails or is removed from the networking device or is manually taken down for maintenance, a switchover from the active to the standby route processor occurs so traffic continues flowing. Without this failover feature, the multicast distribution tree would have to be rebuilt, and the time delay would create an unacceptable wait or restart during which packets would be lost. Another Cisco IOS Software feature called Nonstop Forwarding (NSF) brings switchover features to Layers 1, 2, and 3 at the service provider edge.

Figure 5. SSO Maintains the Session State Between Redundant Route Processors



Cisco NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With Cisco NSF, peer networking devices do not experience routing flaps, reducing loss of service outages for customers. SSO and NSF together enable routers and switches to perform nonstop or to switch over to backup route processors in the event of a failure and with zero or nearly zero packet loss.

Providing Quality of Service for Multicast Traffic

Packets can be classified in a variety of different ways, from input interface to Network-Based Application Recognition (NBAR) for difficult-to-classify applications to arbitrary access control lists. Classification is the first component of the Modular QoS Command Line Interface (MQC), the simple, scalable, and powerful QoS framework in Cisco IOS Software. The MQC allows for the clear separation of classification from the policy applied on the classes of service to the application of a QoS policy on an interface or subinterface. Creating policies through access control lists or MQC enables the blocking of all unwanted IP Multicast traffic destined for the core on all ingress ports of the control plane. Control plane policing using MQC utilizes modular QoS attributes, providing filtering and rate limiting for control plane packets, matching criteria for many attributes, multiple match criteria within a class map, and consistency across platforms.

Source Redundancy

Many Cisco service provider customers who have implemented triple-play metropolitan area networks have video distribution environments using IP Multicast from a video headend. As video services grow in popularity, customers are focusing on ensuring that the video source is highly available. Cisco has engineered a highly resilient headend solution with a redundant topology called Anycast Source.

The Cisco Anycast Source solution assigns duplicated addresses to the redundant multicast sources. The concept is to announce the availability of the MPEG video stream to the streaming device’s address over the first-hop routers closest to the source using IP reachability information. The effect on the IP Multicast forwarding path is that it is entirely possible for a pair of receivers to be joined to different sources at the same time for the same stream.

The streaming device is connected to the router with a turnaround cable and a single virtual LAN (VLAN) is assigned to this port. Then the “redistributed connected” command is used so that the route to the source is advertised only when the interface is up. Thus, if the streaming device fails, the route will be withdrawn, and the network will converge on the other streamer.

Additionally, as a video headend might be using a single IP Multicast streaming device to packetize multiple MPEG video streams coming from different paths and using different components (each of which is subject to failure before reaching the streaming device), it is not efficient to shut down an entire IP streamer if one of the MPEG video streams has failed. Since any of the MPEG video streams may fail discretely, a way of identifying each stream independently is required. Historically, video equipment vendors have identified the individual multicast video streams by using a unique multicast group address for each stream. But what is required here is that the headend and streamer be able to individually address each stream with a unique logical IP source address, even though each stream is being forwarded into the network from the same physical interface.

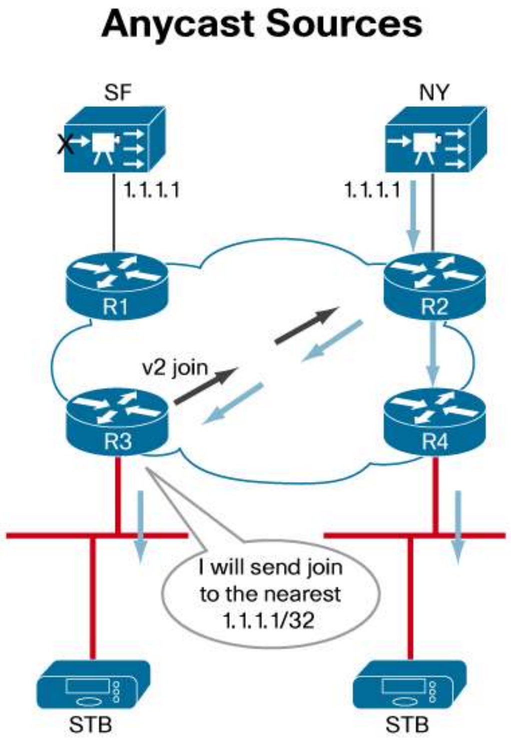
To signal the network using source reachability information, the streaming device must be able to detect when an incoming MPEG stream has failed and to provide some sort of up or down signal to the router so that source reachability can be signaled into the network.

The easiest way of announcing source reachability is by using a Routing Information Protocol Version 2 (RIPv2) host route. If an MPEG video stream is active, the streaming device is configured to announce the route with a hop count. If the MPEG video stream goes inactive, the streaming device is configured to announce the route with an infinite metric (that is, a hop count of 16). The RIP route is redistributed into the Interior Gateway Protocol (IGP) of the network as a /32 host route. PIM will then use that route in deciding the Reverse Path Forwarding (RPF) interface for “joins/prunes”.

There is no need for the streaming device to implement complete RIP router functionality to provide the desired signaling. All that is required is that the streaming device generates the appropriate RIP announcements to mirror the MPEG video stream availability. This does not depend at all on any special software on the receiver and works with Cisco IOS Software in network devices. The option should work with IGMPv2 Any-Source Multicast (ASM) and IGMPv3 SSM on the receiver.

As shown in Figure 6, SSM is enabled on all routers. Router 1 (R1) and Router 2 (R2) advertise the same prefix for each source segment. Router 3 and Router 4 follow the best path towards the source, based on IGP metrics. If R3's best path to San Francisco is through Router 1, when the source in San Francisco suddenly fails, R3's IGP will reconverge and trigger SSM joins toward R2 in New York.

Figure 6. Multicast Source Redundancy Using Anycast Sources



IGMPv3 Explicit Tracking

In networks where bandwidth is constrained between multicast routers and hosts (as in xDSL triple-play deployments), fast channel changes can easily lead to bandwidth oversubscription, resulting in a temporary degradation of traffic flow for all users. An efficient solution to this problem is to reduce the leave latency during a channel change by extending the IGMPv3 protocol.

The explicit tracking feature of IGMPv3 enables a multicast router explicitly to track the membership of all multicast hosts in a particular multiaccess network. This enhancement to the Cisco IOS Software implementation of IGMPv3, first introduced in Cisco IOS Software Release 12.0(29)S, enables the router to track each individual host that is joined to a particular group or channel. The main benefits of this feature are that it provides minimal leave latencies, faster channel changing, and improved diagnostics capabilities for IGMP.

The router in this implementation tracks both the user and the channel or channels being watched. When a user leaves a channel that no one else is watching, the router immediately prunes the channel off the interface. This would otherwise take up to three seconds with IGMPv2 and up to 180 seconds with IGMPv1.

Delivering Multicast Services Securely in Triple-Play Networks

Distributed-denial-of-service (DDoS) attacks, IP packet-based attacks launched at the network infrastructure to compromise network performance and reliability may result in network outages that destroy the network video experience for consumers. Cisco has engineered a multifaceted approach to multicast security that includes protection throughout the network, in the control plane, data plane, and infrastructure and through access and admission control.

Control Plane Security

Control plane security for IP Multicast is the implementation of security features in multicast routing protocols used in the distribution and reception of multicast data. With SSM, multicast traffic from each individual source is transported across the network only if it was requested from a receiver, inhibiting DDoS attacks from unauthorized sources. PIM neighbor filters prevent unknown routers from participating in PIM and potentially becoming a “designated router,” which is responsible for sending PIM registers, building the multicast tree, or performing a shortest path tree switchover. PIM register rate limiters limit the number of PIM register messages that designated routers are allowed to send for each group. Performed at the processor level, PIM registers set a limit that helps protect CPU utilization on the designated router and rendezvous point when there are many multicast transmissions that require PIM register processing at the same time. IP Multicast route (mroute) limits also can be used to limit the number of routes allowed from any PIM neighbor.

The rendezvous point is used to allow sources and receivers to meet and is used with PIM sparse mode. PIM rendezvous point announcement filters are applied to mapping agents when using Auto-Rendezvous Point (Auto-RP), a feature that automatically distributes information to routers about what the RP address is for various multicast groups. These announcement filters are designed to acknowledge RPs that are only permitted by an access list defined by the network administrator. Rogue RPs attempting to hijack another RP are immediately dropped.

Aside from dropping multicast data, PIM multicast boundaries provide a way to block PIM control messages from attaching a new branch to an existing tree off the router to which traffic was not intended to flow. Additionally MSDP Message Digest Algorithm 5 (MD5) authentication can be used to secure multicast sessions between RPs that are used either for interdomain routing or Anycast RPs, which route traffic to the nearest or “best” destination.

Data Plane Security

Cisco technology can secure the content of the multicast transmission through encryption of the data to help ensure that only validated users have access to it. Another form of data plane security called Cisco Secure Multicast provides IP Security (IPsec) support for multicast. Secure Multicast is specifically for enterprise networks with native (nontunneled) multicast traffic. It provides a more efficient way to apply encryption to multicast packets. Encrypting native IP Multicast packets allows PIM to route the packets even though the content is encrypted. Additionally, native multicast encapsulation avoids the packet replication that occurs when packets are encapsulated using unicast tunnels. Networks that are IP Multicast enabled can transport encrypted multicast traffic natively over an IP core. With Secure Multicast, the traffic is protected with encryption in case packets are erroneously delivered. Secure Multicast relies on the Group of Domain of Interpretation (GDOI) protocol to distribute the policies and keys for the group in the control plan, and it relies on IPsec to protect the data plane. It downloads IPsec keys and security associations to routers. GDOI replaces manually shared keys, mitigating all of their security weaknesses. The protocol requires each group member to contact a key server. Once a group member has been authenticated and authorized by the key server, it is given keys and security associations for the group. The group member may also be given enough policy information for it to authenticate and decrypt (or “rekey”) messages sent from the key server in a special IP Multicast group. These rekey messages allow the group member to receive updated keys and security associations and to receive updates to changes of group membership.

Access Control Security

Controlling the ability of a device to send and receive multicast data includes access list filtering at the ingress point of the multicast traffic; IGMP filters used to restrict which hosts are allowed to join multicast groups; and a dynamic method of pushing IGMP filters down to routers using the authentication, authorization, and accounting (AAA) service model. Called multicast authentication and profile support, this latter feature uses existing AAA features in Cisco IOS Software to provide a centralized authentication and accounting framework for multicast users in large groups.

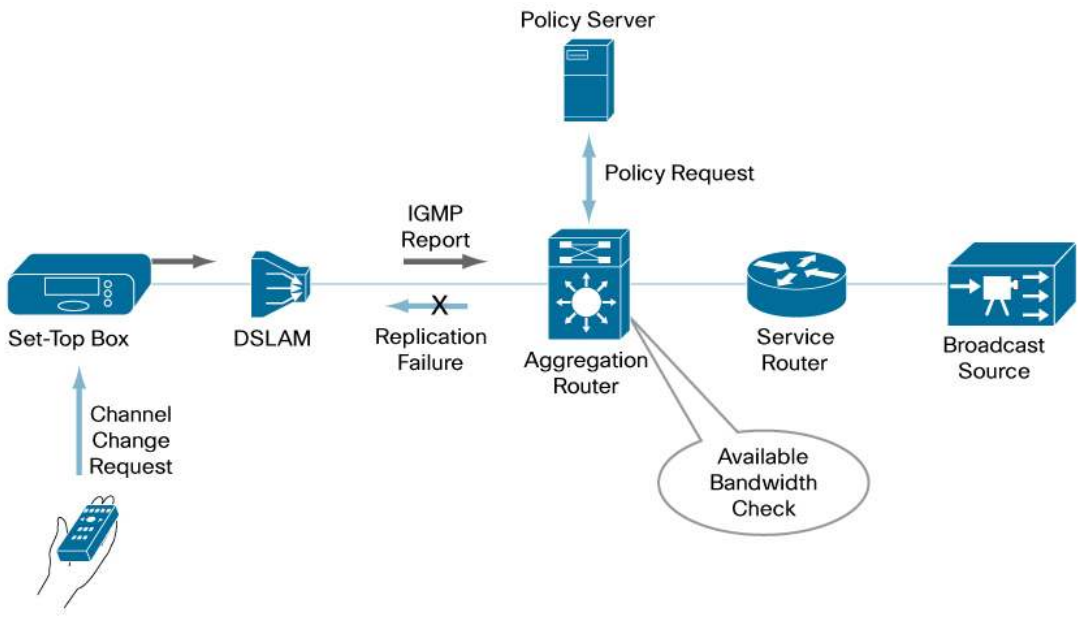
Video Admission Control

Today, end-to-end video over IP sessions, including high-definition channels and on-demand traffic growing on top of a broadcast service, make integrated service control vital to avoid degradation of video streams. Used in conjunction with IP Multicast, an admission control algorithm runs in the aggregation router and can be set to limit the number of channels simultaneously sent to the digital subscriber line access multiplexer (DSLAM) or access concentrator. Criteria for limiting transmission can vary (for example, general popularity of a program, bandwidth used by a specific channel). The algorithm could also be set to guarantee that selected core channels are never blocked.

To date, most service providers and enterprises have not imposed static limits on the number of channels or bandwidth used by broadcast services, and if demand exceeds supply of bandwidth, the user simply does not receive a broadcast. Most major providers have optimized their networks to guard against this through architectures with redundant transport paths between the headend and aggregation routers of the distribution network.

As mentioned previously, at Layer 2, IGMP snooping is a feature used to report IP Multicast memberships to neighboring multicast routers and help ensure that the return data returns to only those ports that requested the stream. At Layer 3, multicast routing protocols are required to build the multicast tree in the optimal fashion across the network. To accomplish this, Cisco created PIM. Cisco Call Admission Control (CAC) for broadcast video uses on-path signaling using IGMP and PIM to trigger a bandwidth availability check (Figure 7). Routers in the path are configured to maintain certain limits on broadcast bandwidth and can limit the number of channels simultaneously sent to the DSLAM.

Figure 7. Cisco Broadcast Admission Control



The multicast destination maps to the broadcast channel’s bandwidth, and the bandwidth is subtracted from the link the request was received on. A failure will result in no replication. The aggregation router may also consult a policy server for service policies for the individual subscriber. In the case of a denial of service, the subscriber receives a blank screen or a “Channel not available” message.

Multicast Policing

Triple-play networks delivering IP video broadcasts must ensure that no single source can monopolize an entire network's resources. Without proper enforcement, valid multicast flows can easily get stomped on by a faulty sender. User-based rate limiting provides the means to rate-limit multicast traffic on a per flow basis versus an aggregate basis.

Managing Multicast Services with Cisco Multicast Manager

Multicast services can be managed with instrumentation that runs on the provider edge routers and are controlled by a management application. Cisco Multicast Manager is a Web-based network management application that is designed to aid in the monitoring and troubleshooting of multicast networks. It provides early warning of problems; in-depth troubleshooting and analysis capabilities; on-demand, real-time, and historical reporting; and optimization of network utilization and enhancement of services delivery.

Using Simple Network Management Protocol (SNMP) to gather information regarding rendezvous points, MSDP, sources and groups, traffic profiles, IGMP statistics, mroute tables, and multicast trees, Cisco Multicast Manager is an invaluable tool. It polls the network, gathering information in its Management Information Base (MIB) modules. With the click of a button, users can obtain detailed information about the health of the multicast network. Multiple multicast domains are supported, so users may tailor the size and scope of the routers being managed.

The tool allows for the detection and management of faults through the capture of syslog error messages. These error messages are transmitted as reactive fault notifications through the Cisco Networking Services Notification Engine.

Cisco provides several MIBs for multicast management that provide information including:

- How many active multicast routes are in place and what their data rates are
- Where the receivers for each multicast group are
- Whether traffic is behaving as expected
- Which route processor supports a particular group
- How the multicast traffic flow affects other traffic

Cisco multicast MIBs include IGMP, IGMP snooping, multicast route (Mroute), PIM, MSDP, and multicast VPN.

Cisco IOS NetFlow

Another important technology available from Cisco is a traffic analysis and trending feature in Cisco IOS Software called Cisco IOS NetFlow. It provides highly granular traffic statistics for Cisco router-based networks on a per flow basis. A “flow” is data that enters specific router or switch interfaces. Analysis of NetFlow data makes it possible to identify the cause of congestion, to determine the class of service for each user and application, and to identify the source and destination network for traffic. This IP traffic flow analysis is invaluable for billing, network planning, and network monitoring in IP triple-play networks.

There are three types of NetFlow implementations for multicast, which are available with NetFlow Version 9, in Cisco IOS Software Releases 12.2(18)S and 12.3(1):

- Traditional NetFlow
- Multicast NetFlow ingress accounting, which lets you collect information on how much multicast data is received. One flow record records how many times each packet is replicated.
- Multicast NetFlow egress accounting, which lets you collect information on how much data is being sent by each outgoing interface.

CONCLUSION

Technologies in Cisco IOS Software make multicast applications over IP triple-play networks flexible, reliable, highly available, secure, and scalable. Using these solutions, networks hosting triple-play traffic can be configured for more efficient control of multicast traffic, reduced server and CPU loads, no traffic redundancy, and reduced costs. With years of experience in thousands of multicast service provider and enterprise networks, Cisco provides a comprehensive end-to-end architecture to exploit the explosive growth of the Internet and eliminates bandwidth constraints inherent in distributed group applications.

FOR MORE INFORMATION

Cisco IP Multicast
http://www.cisco.com/go/ipmulticast

Cisco IOS Software Secure Multicast
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6552/prod_white_paper0900aecd8047191e.shtml

Cisco IOS NetFlow for Multicast for Cisco IOS Software Releases 12.3 Mainline
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_feature_guide09186a00805256cb.html

User-Based Rate Limiting in the Cisco Catalyst 6500
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_white_paper0900aecd803e5017.shtml

Cisco Multicast Manager
http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6504/ps6335/ps6337/product_data_sheet0900aecd802842c3.html

Cisco Multicast Virtual Private Networks Concepts
http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a00800a3db6.shtml

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 C11-372125-00 10/06