DATASHEET

MULTICAST VPN

THE CHALLENGE

As the worldwide demand for VPN services grows, the demand for Multicast VPN (MVPN) services is likewise accelerating. Over the past 10 years, multicast has become prevalent in financial applications, software downloads, and audio and video streaming applications. Gartner predicts that 80 percent of Global 2000 companies will deploy IP Multicast technology by 2006.

Until very recently, the only way to support multicast over a Multiprotocol Label Switching (MPLS) network was for the service provider to build manual generic routing encapsulation (GRE) tunnels between every source-receiver pair. Because of the large administrative costs, this manual configuration solution presents serious challenges even for companies with a small number of sites and customers.

THE SOLUTION—CISCO MULTICAST VPN

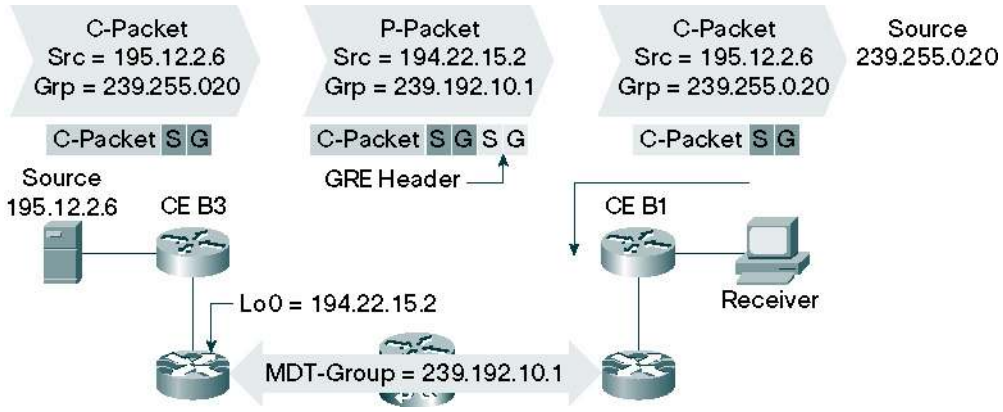
In 2002 Cisco Systems® provided a practicable solution called Multicast VPN (MVPN) for this growing market. It is simple to set up, is highly scalable, and has minimal administrative overhead. With the new Cisco® MVPN technology, providers now have the ability to dynamically provide multicast support over MPLS networks. MVPN architecture introduces an additional set of protocols and procedures that help enable a service provider to support multicast traffic in a VPN. It allows for the transport of a customer's IP Multicast traffic across a provider's VPN backbone transparently, and it is integrated transparently with the Cisco IOS® Unicast MPLS VPN solution. It allows a service provider to offer multicast services to its VPN customers in addition to its current Unicast VPN offering.

HOW IT WORKS—MVPN BASICS

The Cisco MVPN solution is based on the latest IETF Rosen Draft draft-rosen-vpn-mcast-08.txt. It supports the true dynamic nature of multicast applications, which are receiver-initiated and, as a result, satisfies all service providers' and customers' multicast requirements. The MVPN solution uses GRE with unique multicast distribution tree (MDT) forwarding to realize the true scalability of native IP Multicast in the core network. Cisco MVPN is based on the Multicast Domain solution with the highest level of optimization built into the Cisco solution with the help of default MDT and data MDT scaling enhancements. MVPN introduces multicast routing information to the VPN routing and forwarding table (VRF), creating a Multicast VRF.

The resulting MVPN service in its most basic form allows one to build a Protocol Independent Multicast (PIM) domain that has sources and receivers located in different sites. It is important to note that the use of MVPN does not change the way an enterprise customer network is administered with respect to addressing, routing policies, or topology, nor does it change enterprise connectivity with the rest of the world. It is also important to remember that the customer's IP Multicast network has no relationship to the provider's multicast network. From the perspective of the provider, the customer's IP Multicast packets are merely data to the provider's distinctive and completely separate IP Multicast network.

Figure 1
MVPN Packet Encapsulation



MVPN INTERAUTONOMOUS SYSTEM

The Interautonomous System (Inter-AS) Support for Multicast VPN feature can be configured on a VRF router, to enable forwarding of Multicast VPN traffic from one site of a VPN Red in Autonomous System 1 to another site of the VPN Red in Autonomous System 2. This feature allows MDT tunnels to be set up between two provider-edge routers in different autonomous systems without the need to share routing information between the two autonomous systems.

To allow two provider-edge routers to set up an MDT tunnel across autonomous systems, the MDT addresses family needs to be enabled under a Border Gateway Protocol (BGP) configuration. Using the MDT autonomous system, provider-edge routers in different autonomous systems are able to learn about each others' existence and join each other. To configure the Inter-AS Support for Multicast VPN feature, it is important to understand the following two concepts:

Reverse Path Forwarding Check on Route Distinguisher and Vector

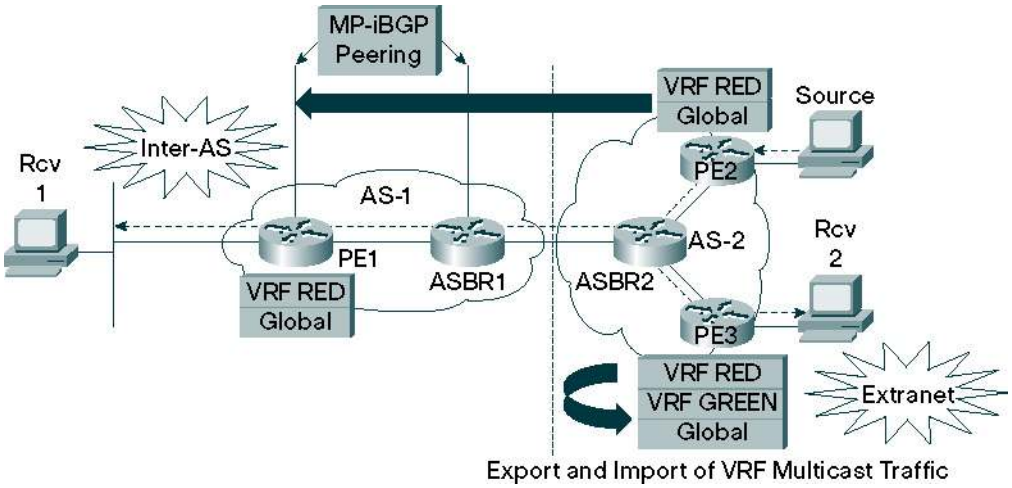
When supporting VPNs that are in different autonomous systems, routing information on the provider's routers might not be complete enough to set up an MDT tunnel that spans multiple autonomous systems from one provider-edge router to another. After adding additional information in the PIM join packet, the intermediate routers are able to select a Reverse Path Forwarding (RPF) interface by doing a direct lookup in a special BGP MDT table. With the route distinguisher, the VPN-specific BGP MDT table can be selected to enable the RPF interface for the source to be found. The BGP MDT table is used only to set up the MDT tunnel. It is not used for the VPN traffic encapsulated in the MDT tunnel. For intermediate routers that do not run BGP, the RPF vector is used to find the RPF interface.

Modified PIM Join Format

This method is required because routes to the source inside a VRF are known via the Multiprotocol BGP next hop. Those routes are not present in the Interior Gateway Protocol (IGP) in the provider core. A next-hop destination address is inserted in a PIM message and known as an RPF Vector.

A new PIM hello option is introduced to determine whether the upstream router is capable of parsing the new encoding. Other routers on the LAN might need to override a prune message or cancel sending a join message, creating the need to be able to parse the PIM join message. These methods are the only way to provide a full Inter-AS solution suitable for options A, B, and C of RFC 2547bis.

Figure 2
MVPN Inter-AS and Extranet



MVPN EXTRANET

An extranet can be viewed as part of a company's intranet that is extended to users outside the company. It has also been described as a "state of mind" in which a VPN is used as a way to do business with other companies as well as to sell products and content to customers and companies. Extranet is a VPN connecting the corporate site or sites to external business partners or suppliers, to securely share part of a business's information or operations among them.

MPLS VPNs inherently provide security, ensuring that users access only appropriate information. The MPLS VPN Extranet service offers extranet users unicast connectivity without comprising the integrity of their corporate data. Multicast VPN Extranet Service will extend this offer to include multicast connectivity to the extranet community of interest.

The Multicast VPN Extranet feature allows service providers to source multicast content from VPN Red into VPN Green, as shown in Figure 2. It allows service providers to offer the next generation of flexible extranet services, helping to enable business partnerships between different enterprises. With this feature, service providers will be able to offer multicast extranet contracts to meet various business partnership requirements, including short-term, annual, and rolling contracts.

Extranet MVPN can be used to solve such business problems as:

- Efficient content distribution between enterprises
- Efficient content distribution from service providers or content provider to its different VPN customers

MVPN MIB/MANAGEMENT

A service provider providing Multicast VPN services needs to be able to manage the Multicast VRFs (MVRFs) on the provider-edge routers (customer MVRFs) from a network management system (NMS) located in VRF 0. In general, an NMS in one MVRF needs to be able to manage another MVRF. This issue is already solved for Unicast MPLS VPN Management by implementing the concept of the "meta NMS" Simple Network Management Protocol (SNMP) Agent. Cisco IOS Software already supports this feature. For service providers, meta NMS could be similarly set up in global VRF, and SNMPv3 is recommended for security and authentication mechanisms.

A new MIB to support management of MVPN technology is needed. This MIB is supposed to be accessible from VRF 0 or from a meta VRF configured by the service provider. A subset of relevant info could be made accessible to the customer in the customer VRF. Cisco has created a specific MIB to manage Multicast VPNs. The CISCO-MVPN-MIB is modeled on the MPLS-VPN-MIB and includes:

- The number of MVRFs
- The number of interfaces per MVRF
- Information about default MDT groups
- Information about data MDT groups
- Mapping MVRFs to the MVPN tunnel interface
- Support for an SNMP notification

Work is also underway to make the following multicast MIBs VRF-aware: IPMROUTE-STD-MIB, CISCO-IPMROUTE-MIB, PIM-MIB, CISCO-PIM-MIB, IGMP-MIB/IGMP-STD-MIB, and MSDP-MIB.

Tables 1 and 2 outline support and features for Cisco MVPN.

Table 1. Cisco MVPN Support

Cisco IOS Software Release	Platforms
12.2(13)T, 12.0(23)S, 12.2(18)SXE	Cisco 12000, 7200, 7500, and 10000 series routers, and Cisco Catalyst® 6500 Series switches

Table 2. Cisco MVPN Features

	Multicast VPN Feature Name
1	Basic Multicast VPN feature set
2	Scalable Data MDT support
3	Support for both Source Specific Multicast (SSM) and Any Source Multicast (ASM) in the core
4	Support for rendezvous point (RP) on a provider-edge router per VRF
5	Quality of service support for MVPN
6	Support for Multicast Source Discovery Protocol (MSDP), Cisco Group Management
	Protocol, and Router-Port Group Management Protocol (RGMP) in the VRF
7	Support for access filters, debugging, and troubleshooting tools
8	Support for multicast applications like mtrace, mstat, mrinfo in a VRF
9	MVRF Lite
10	MVRF 802.1q support
11	Inter-Switch Link (ISL) support for MVPN
12	MVPN static SSM mapping
13	Carrier Supporting Carrier (CSC)
14	Inter-AS
15	Extranet
16	MVPN MIB

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

Pa/LW8478 05/05

Printed in USA