Importance of Multicast Virtual Private Networks based on RFC 2547

Varun P Saxena
Department of CSE, Bansal School of Engineering & Technology, Jaipur, India,

Varun Gupta
Research Scientist, Indian Space Research Organization, Banglore, India

Ajay Goel
Department of CSE, Singhania University, Jhunjhunu, Rajasthan, India,

O.P.Sahu
Department of Electronics & Communication, NIT, Kurukshetra, Haryana, India

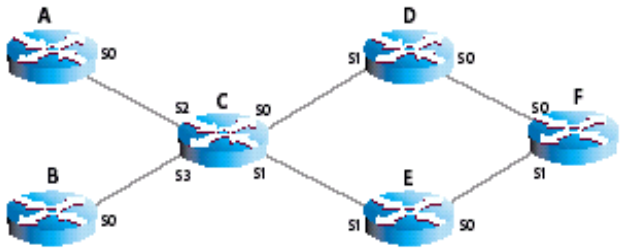
ABSTRACT
The Multi-protocol Label Switching is one of the proposed technologies useful for traffic engineering in the specific aspects of measurement and control of Internet traffic and virtual Private network (VPN) is a concept that significant on the future of business communication, it replace existing private network with flexible architecture that is easily manage and at a same time it provide enhanced service.

The Multi-protocol Label Switching (MPLS) virtual Private network (VPN) is a popular IP VPN service based on RFC 2547 and its successor documents (dubbed 2547bis).The main importance of MPLS is that it integrates the key features of both Layer 2 and Layer 3. Most importantly, it is not limited to any Layer 2 or Layer 3 protocol. In particular, MPLS has several applications and can be extended across multiple products segments (such as an MPLS router, an IP services switch/router, a multi service switch, an Optical Ethernet switch, as well as optical switches). Many service providers offer MPLS VPN to their large enterprise customers, who need only attach their local, customer edge (CE) site routers to the nearest service provider edge (PE) router and exchange routing information. MPLS reduces the complexity of forwarding using encapsulated fixed-length labels for making high speed forwarding decisions. The service provider distributes customer IP routing information to other customer sites and uses its backbone to forward customer IP packets from one customer site to another. This is done by very new concept which is called multicast virtual private networks (mVPNs).

Keywords
MPLS, VPN'S , GRE, IP, QOS, mVPN's, MDT's, GRE.

1. INTRODUCTION
In traditional routing environments, a packet is forwarded through a network on a hop-by-hop basis using interior gateway protocols, such as routing information protocol and open shortest path first, or exterior gateway protocol such as border gateway protocol. This is done by referencing the destination layer 3 addresses against a routing table for a next hop entry.

To clarify, each router that a packet traverses must do a route lookup, based on that destination layer 3 address in the IP header. This must be performed to determine the packet's next hop in its path to get it to its final destination. The layer 2 destination address is then replaced with the address of the next hop's layer 2 address, and the source layer 2 address is then replaced with the layer 2 address of the current router, leaving the source and destination layer 3 addresses in place for the next hop to perform its own route lookup on the packet. This process must be repeated at each hop to deliver the packet to its final destination.



MPLS , VPNs support only uni-cast routing service that is, packets can travel only from a particular source host at one VPN site to a particular target host at another — but large enterprises are increasingly using IP multicast to simultaneously communicate the same content to multiple target hosts. IP multicast offers a "send once, deliver to many" paradigm in which a network of routers running IP multicast replicates and forwards multicast packets down a tree originating at the content source and leading to multiple leaf routers.

MPLS is a "Multi-protocol" which uses label-switching technology. Label switching paradigm consists in using a short, fixed-length label to perform switching decisions. Unlike longest prefix match lookup algorithms used by standard IP routing protocols, label switching is based on an exact match and therefore is much faster. To keep their enterprise customers

happy and attract new customers, service providers must support IP multicast across MPLS VPNs. One early technique was to define point-to-point IP generic routing encapsulation (GRE) between the CE routers at different VPN sites and simply tunnel the multicast packets. The problem with this solution is that the customer (or service provider) has to configure numerous GRE tunnels.

2. DIFFERENT IP MULTICAST CONCEPTS

Jitter: Label switching operations result in less delay and less jitter in sending user traffic through the network.

Resource Consumption: The control mechanisms to establish label-switching paths do not consume a lot of resources.

Multicast Group Address: The class D IP address space (224.0.0.0 to 239.255.255.255) is reserved for multicast. The network will deliver copies of all IP packets with a group address (denoted as G) in the header destination address field to all routers and hosts that have expressed interest in receiving them. mVPN uses two types of group addresses:1. customer G addresses (c-G) and provider group addresses (p-G). A c-G group address identifies a multicast group inside the customer VPN, and a p-G group address identifies a multicast group inside the provider's network.

Label: The label is a condensed view of the header of an IP packet, although contained within it is all of the information needed to forward the packet from source to destination. Unlike the IP header, it does not contain an IP address, but rather a numerical value agreed upon by two MPLS nodes to signify a connection along a Label Switch Path. The label is a short, fixed-length, physically contiguous identifier, which is used to identify a Forward Equivalence Class, usually of local significance.

Multicast Trees: It implies that concept "beginning at a root and branching out to many leaves". Source trees require routers to store more information than shared trees — each unique S and G pair, called (S, G) entries, must be stored rather than a single (RP, G) pair — but they offer better performance because packets flow directly from the source to the leaf routers.

Label Switch Path (LSP): The Label Switch Path is essentially the predetermined route that a set of packets bound to a Forward Equivalence Class traverse through Multi-protocol Label Switching network to reach their destination. Each Label Switch Path is unidirectional; therefore, return traffic must use a separate LSP.

Protocol Independent Multicast: PIM is the acronym for a set of multicast routing protocols that are used to dynamically build multicast tree One variant of PIM, called Sparse Mode (PIM-SM), builds RP-rooted shared trees but has an option to witch over to a source tree when better performance is required. Another variant, called Single Source Multicast (PIM-SSM), is used to build source trees only.

Reverse Path Forwarding: To forward multicast packets away from the source and down the tree, routers employ RPF. A router performs an RPF check for each multicast packet by comparing the source address (for the host generating the multicast packets) with entries in its own routing table. If the packet arrived on an inbound interface that the router would use to send packets back to the source, the RPF check passes and the router replicates the packet and forwards it out one or more outbound interfaces down the tree and away from the source. Otherwise, the router silently drops the packet. The key point here is that, to accurately perform an RPF check, a router must have a route (or a clue) for reaching the source host's network.

Resource Reservation Protocol (RSVP) The Resource Reservation Protocol is another similar method of establishing a point-to-point Label Switch Path that meets QoS requirements. It is an extension of the original Resource Reservation protocol, with new capabilities to support a Multi-protocol Label Switching domain. Resource Reservation Protocol communicates with two basic types of messages, PATH and RESV. PATH messages flow from a sender to one or multiple receivers. Upon receipt of a PATH message, a receiver can send an RESV message in return. The label itself is carried within the RESV message.

3. MULTICAST VPN BASICS

It is a natural evolution for existing networks to provide the necessary capabilities to support the explosive growth of the Internet, while at the same time enabling network administrators to control traffic at a more granular level. mVPNs are a solution for supporting IP multicast within a customer IP VPN provisioned across a provider's MPLS VPN infrastructure. It adopts two important design principles:

- First, a CE need only establish a routing (in this case, multicast) adjacency with the PE router to bounded. This ensures that the provider's ability to support a growing number of customer VPNs isn't limited by core P router resources. The amount of VPN-specific information maintained in the provider core network with mVPN depends on the type and granularity of the multicast trees in the provider backbone that carry customer mVPN packets between PE routers.

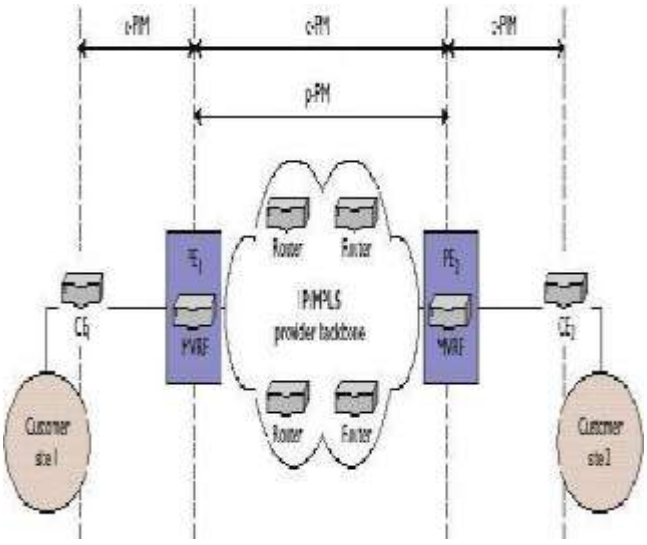


Figure 2.1. (MVPN's Components)

Figure2.1 illustrates the basic components of an mVPN solution

- Multicast virtual routing/forwarding (MVRF) is a per-customer multicast VPN routing table defined on the PE routers. It's actually an extended version of the VRF that was originally defined for MPLS VPN, but which is now designed to the hold customer multicast routing information. • Two types of multicast routing protocols are in the picture. C-PIM runs inside the customer VPN network, between the CE and PEs and between PE nodes across the provider's backbone network. P-PIM is used to build multicast trees across the provider's backbone to exchange customer routing information so that it can send packets to and receive them from *N* other remote CE sites that belong to the customer VPN.
- Second, the amount of per-customer VPN information stored and processed inside the provider's core network of routers (P routers) is transport customer multicast VPN packets. With the mVPN elements in place, and the customer CE router able to send and receive multicast control messages (c-PIM) and multicast packets, let's examine how the provider can forward multicast packets across its backbone network.

4. ENCAPSULATION

Although mVPN is an extension of the MPLS VPN service, it uses no labels or label switching.

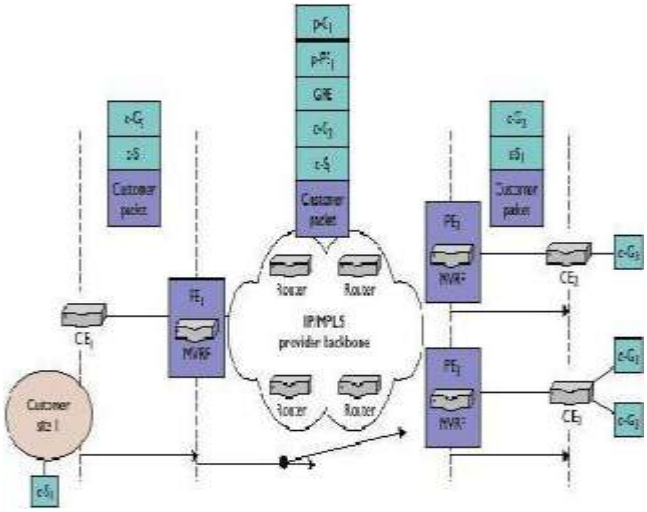


Figure 4.1: - MVPN packet forwarding

Figure4.1 illustrates the standard mVPN solution, which encapsulates customer IP multicast packets for transport over default or data MDT's using generic routing encapsulation (GRE). The ingress PE receives the native customer IP multicast packet from a CE router and imposes the IP GRE header on top. The source address in the header identifies the source PE router (not the customer source of the multicast stream) and the destination address is a p-G group address specific to the provider's backbone network. Packets flowing on the default MDT use one p-G address, while others are flowing on a data MDT use a different one.When the leaf PE routers receive the packet, they remove the IP GRE header and forward the packet to the interested CE sites. Why use an IP encapsulation rather than MPLS? First, the native IP multicast used in provider backbones requires IP multicast packets. In fact, IP multicast is quite a mature function, which has been running over many provider networks for several years. Second, MPLS multicast or more specifically, the ability to set up multipoint LSPs — is still in the very early stages of standardization and deployment (it emerged only over the past year or so within the IETF). Over time, some provider will likely use multipoint LSPs to realize default and data MDT connectivity in MPLS backbones.

Now we are talking about the basic concept of RPF Check. As we know that that routers running IP multicast use the RPF check to forward multicast packets away from the source and that a router must have a route or at least know how to send a packet back to the source's network. In mVPN solutions, routers perform RPF checks in several different areas in the network. For packets arriving from a CE router, the ingress source PE router runs an RPF check on the customer source host IP address; if the MVRF contains a route back to that network, then the RPF passes and the packet is directed out a multicast tunnel interface.

P and PE routers perform RPF checks on the source IP address in the IP RE encapsulation for provider packets flowing over default or data MDTs inside the provider's network.

5. ENHANCEMENTS

The ability to collapse their layer 1, 2, and 3 networks onto one platform is becoming increasingly apparent. MVPN offers the ability to dynamically transport any layer 2 or 3 protocol through any MVPN aware network. MVPNs continue to evolve functionally as more providers offer VPN services to customers with multicast requirements. Just like MPLS VPNs, mVPNs can be extended to run across different routing domains or autonomous systems (ASs). This requires several extensions to BGP for carrying mVPN routing information and communicating RPF information. mVPN Class of Service (CoS) can also be used to implement ATM's QoS features, allowing providers to reliably offer voice and video services as well as traditional data transport. Some service providers with MPLS backbones would like to use point-to-multipoint MPLS LSPs rather than native IP multicast to support default and data MDTs in mVPNs. GMPLS (Generalized Multi-protocol Label Switching) is the next evolution, allowing service providers to take the flexibility of MVPN and apply it to an optical framework. The technology powering GMPLS is micro-electric mechanical systems (MEMS). The ability to use micro-mirrors to redirect lambdas has opened the doors to a bandwidth explosion. One of the limitations that surfaced with mimetic switching has turned out to be a positive progression in the end. Working groups within the IETF are working on extensions to Resource Reservation Setup Protocol – Traffic Engineering (RSVPTE) and the Label Distribution Protocol (LDP), which could be used rather than p-PIM, to establish multipoint MPLS LSP connectivity between PE routers in provider backbone networks.

6. FUTURE WORK

MVPN is the natural evolution for existing networks to provide the necessary capabilities to support the explosive growth of the Internet, while at the same time enabling network administrators to control traffic at a more granular level. More attention should be given to the nature of the application and the supporting infrastructure when it comes to securing applications within a corporate network. Network performance and other related issues are affected by the implementation of encryption tools (software and hardware) and the use of various platforms for such implementations. One of the areas not covered in the performance comparison is the Remote Access VPNs. It is an important sub-area of VPN area, one that is highly relevant and applicable in universities and academic institutions. There is a growing number of academic and executive staff in universities that wishes to access their network resources from remote locations. Security is one of the main reasons why a service such as this is usually denied or restricted. It is highly recommended to implement remote access VPN models and investigate further into functionality, flexibility performances issues.

7. REFERENCES

[1] E.C. Rosen and Y. Rekhter, "BGP/MPLS IP VPNs," IETF Internet draft, Oct. 2004

[2] C. Metz, "The Latest in Virtual Private Networks: Part I," IEEE Internet Computing, vol. 7, no. 1, 2003, pp. 87–91.

[3] Chris Metz "On the Wire Multi-protocol Label Switching and IP, Part 2 Multicast Virtual Private Networks" JANUARY FEBRUARY 2006 IEEE INTERNET COMPUTING

[4] B. Daugherty and C. Metz, "Multi-protocol Label Switching and IP, Part I: MPLS VPNs over IP Tunnels," IEEE Internet Computing, vol. 9, no. 3, 2005, pp. 68–72

[5] D. Farinacci et al., Generic Routing Encapsulation (GRE), IETF RFC, Mar. 2000; www.ietf.org/ rfc/rfc 2784.txt.

[6] S. Bhattacharyya, An Overview of Source-Specific Multicast (SSM), IETF RFC 3569, July 2003; www.ietf.org/rfc/rfc3569.txt.