Multi-protocol label switching virtual private Networks

Prahlad Meghwal[1] (prahlad1985eca@gmail.com) Pacific University,Udaipur
Mahendra kumar bairwa[2] (mahendrabairwa84@gmail.com) SITE,Nathwdara

ABSTRACT

The IP-based virtual private network (VPN) is rapidly becoming the foundation for the delivery of New World services, and many service providers are offering value-added applications on top of their VPN transport networks. Emerging services such as e-commerce, application hosting, and multimedia applications will enable service providers to generate new incremental revenue and maintain long-term competitive advantage. Two unique and complementary VPN architectures based on IP Security (IPsec) and Multiprotocol Label Switching (MPLS) technologies are emerging to form the predominant foundations for delivery of New World services. This white paper examines these two VPN architectures, their similarities and differences, and the benefits they offer. It concludes with a unified view of IP VPNs that combine both IPsec and MPLS based on their respective strengths.

Multiprotocol Label Switching (MPLS) is an emerging technology which ensures the reliable delivery of the Internet services with high transmission speed and lower delays. The key feature of MPLS is its Traffic Engineering (TE) which is used for effectively managing the networks for efficient utilization of network resources. Due to lower network delay, efficient forwarding mechanism, scalability and predictable performance of the services provided by MPLS technology makes it more suitable for implementing real-time applications such as Voice and video.

MPLS ARCHITECTURE

Multiprotocol Label Switching (MPLS) is a tunneling technology used in many service provider networks [3]. The most popular MPLS-enabled application in use today is the MPLS virtual private network. MPLS VPNs were developed to operate over MPLS networks, but they can also run over native IP networks. This offers providers flexibility in network deployment choices, improved routing system scalability and greater reach to customers. The key element is the ability to encapsulate MPLS packets in IP tunnels. In an MPLS network, each LSP is created over the best path selected by the IGP, towards the destination network. An IGP (OSPF or IS-IS) is used to propagate routing information to all routers in an MPLS domain to determine the best path to specific destination networks. Each hop within the network core forwards packet based on the label, not IP information, until the final label switch is reached where the label is discarded and normal IP forwarding resumes

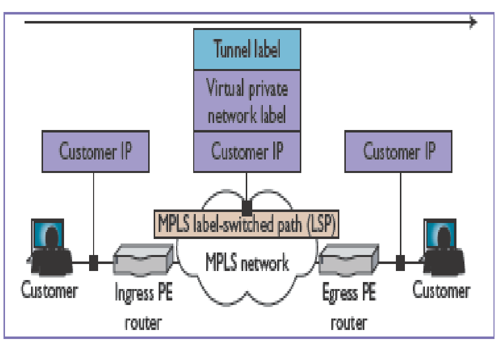

Figure MPLS Tunneling Architecture

Overview of VPN Requirements

RFC 2764 defines a generic framework for IP-based VPNs, including the following requirements for a VPN solution.

- Opaque transport of data between VPN sites, because the customer may be using non-IP protocols or locally administered IP addresses that are not unique across the SP network.
- Security of VPN data transport to avoid misdirection, modification, spoofing or snooping of the customer data.
- QoS guarantees to meet the business requirements of the customer in terms of bandwidth, availability and latency.

In addition, the management model for IP-based VPNs must be sufficiently flexible to allow either the customer or the SP to manage a VPN. In the case where an SP allows one or more customers to manage their own VPNs, the SP must ensure that the management tools provide security against the actions of one customer adversely affecting the level of service provided to other customers

Four types of VPN are defined in RFC 2764.

- **Virtual Leased Lines** (VLL) provide connection-oriented point-to-point links between customer sites. The customer perceives each VLL as a dedicated private (physical) link, although it is, in fact, provided by an IP tunnel across the backbone network The IP tunneling protocol used over a VLL must be capable of carrying any protocol that the customer uses between the sites connected by that VLL.
- **Virtual Private LAN Segments** (VPLS) provide an emulated LAN between the VPLS sites. As with VLLs, a VPLS VPN requires use of IP tunnels that are transparent to the protocols carried on the emulated LAN. The LAN may be emulated using a mesh of tunnels between the customer sites or by mapping each VPLS to a separate multicast IP address.
- **Virtual Private Routed Networks** (VPRNs) emulate a dedicated IP-based routed network between the customer sites. Although a VPRN carries IP traffic, it must be treated as a separate routing domain from the underlying SP network, as the VPRN is likely to make use of non-unique customer-assigned IP addresses. Each customer network perceives itself as operating in isolation and disjoint from the Internet – it is, therefore, free to assign IP addresses in whatever manner it likes. These addresses must not be advertised outside the VPRN since they cannot be guaranteed to be unique more widely than the VPN itself.
- **Virtual Private Dial Networks** (VPDNs) allow customers to outsource to the SP the provisioning and management of dial-in access to their networks. Instead of each customer setting up their own access servers and using PPP sessions between a central location and remote users, the SP provides a shared, or very many shared access servers. PPP sessions for each VPDN are tunneled from the SP access server to an access point into each customer's network, known as the access concentrator.

The last of these VPN types is providing a specialized form of access to a customer network. The IETF has specified the Layer 2 Tunneling Protocol (L2TP), which is explicitly designed to provide the authentication and multiplexing capabilities required for extending PPP sessions from a customer's L2TP Access Concentrator (LAC) to the SP's L2TP Network Server (LNS).

Elements of an MPLS VPN solution

Let us consider how MPLS can provide a VPN solution by examining how it would work at several different levels. We start with the data forwarding mechanics and work our way up to the network management considerations. Different implementation models for MPLS-based VPNs imply different interactions between these elements of a VPN solution. See the section *VPN Implementation Models* for further details.

- **LSP Tunnels**

The basis of any MPLS solution for VPNs is the use of LSP tunnels for forwarding data between SP edge routers that border on a given VPN. By labeling the VPN data as it enters such a tunnel, the LSR neatly segregates the VPN flows from the rest of the data flowing in the SP backbone.

- Multiple protocols on the VPN can be encapsulated by the tunnel ingress LSR since the data traversing an LSP tunnel is opaque to intermediate routers within the SP backbone.
- Multiplexing of traffic for different VPNs onto shared backbone links can be achieved by using separate LSP tunnels (and hence separate labels) for each data source.
- Authentication of the LSP tunnel endpoint is provided by the label distribution protocols. See the section *VPN Security* for more details.
- QoS for the VPN data can be assured by reserving network resources for the LSP tunnels. MPLS supports both Intserv and Diffserv.
- Protection switching and automatic re-routing of LSP tunnels ensure that failure of a link or router that affects a VPN can be corrected without management intervention. These protection mechanisms operate at several different levels, including refresh/keep-alive messages on a hop-by-hop basis within the label distribution protocols, re-routing of LSP tunnels, pre-provisioning of alternative routes, and wavelength failure detection and management for optical networks.

Why There Are Two VPN Architectures

The service goal of VPNs is to provide customer connectivity over a shared infrastructure, with the same policies enjoyed in a private network. A VPN solution must therefore be secure from intrusion and tampering, deliver mission-critical data in a reliable and timely manner, and be manageable. The essential attributes of a VPN can be segmented into five broad categories (Table 1).

Table 1 Essential Attributes of a Virtual Private Network

Scalability	Must be scalable across VPN platforms ranging from a small office configuration through the largest enterprise implementations ubiquitously on a global scale; the ability to adapt the VPN to meet changing bandwidth and connectivity needs is crucial in a VPN solution. Additionally, in the fiercely competitive and dynamic market environment, large orders can be won and must be provisioned rapidly, hence the VPN must be highly scalable in order to accommodate unplanned growth and changes driven by customer demand.
Security	Ensures business-critical traffic remains confidential via security mechanisms such as tunneling, encryption, traffic separation, packet authentication, user authentication, and access control.
Quality of Service	Ensures prioritization of mission-critical or delay-sensitive traffic and manages congestion across varying bandwidth rates. Quality of service (QoS) functions such as queuing, network congestion avoidance, traffic shaping, and packet classification, as well as VPN routing services utilizing an optimal routing protocol.

Manageability	Essential for cost-effective provisioning to enforce security and QoS policies, management and billing, with advanced monitoring and automated flow-through systems to quickly roll out new services and support service-level agreements (SLA).
Reliability	For predictable and extremely high service availability that business customers expect and require.

Comparison Between IPsec and MPLS-Based VPN

Table 2 describes the characteristics, benefits, positioning, and the differentiation between the IPsec and MPLS-based VPN.

Table 2 IPsec and MPLS-Based VPN Comparison

Service Models	High-speed Internet services, business-quality IP VPN services, e-commerce and application-hosting services High-speed Internet services, business-quality IP VPN services, e-commerce and application-hosting services
Scalability	Large-scale deployment requires planning and coordination to address issues on key distribution, key management, and peering configuration Highly scalable since no site-to-site peering is required.
Place in Network	Best at the local loop, edge and off-net where there is a higher degree of exposure to data privacy and where IPsec security mechanisms such as tunneling and encryption can best be applied Best within a service provider's core network where QoS, traffic engineering, and bandwidth utilization can be fully controlled, especially if SLA or service-level guarantee (SLG) is to be offered as part of the VPN service
Transparency	IPsec VPN resides at the network layer; it is transparent to the applications MPLS VPN operates at the IP+ATM or IP environment; it is completely transparent to the applications
Provisioning	In general, no network level provisioning is required for managed CPE based service offering. When a networked based IPsec VPN service is deployed, service provider generally provides centralized provisioning and management support. Because MPLS

	VPN site peers with a service provider network only, service activation requires just a one-time provisioning at the customer edge (CE) and provider edge (PE) devices to enable the site to become a member of a MPLS VPN group.
Service Deployment	Fast time to market; can be deployed across any existing IP networks Requires participating network elements at the core and edge to be MPLS capable, such as during a network upgrade or when a new MPLS network must be deployed
Session Authentication	Each IPsec session must be authenticated via digital certificate or preshared key; packets that do not conform to the security policy are dropped VPN membership is determined by service providers—a provisioning function based on logical port and unique route descriptor; unauthorized access to a VPN group is denied by device configuration
Confidentiality	IPSec VPN provides data privacy through a flexible suite of encryption and tunneling mechanisms at the IP network-layer IMPLS architecture separates traffic between customers offering security in a manner similar to a trusted Frame Relay or ATM network environment
Quality of Service	While the IPsec protocol does not address network reliability or QoS mechanisms, a Cisco IPsec VPN deployment can preserve packet classification for QoS within an IPsec tunnel A well-executed MPLS based VPN implementation provides scalable, robust QoS mechanism and traffic engineering capability enabling service providers to offer IP-based value-added services with guaranteed SLA compliance

REFERENCES

[1] Khan. F., “Traffic Engineering with Multipoint Label Switching”. E.Tech, 04 pp. 61-67, July 2004.

[2] Fang L.; Bita N.; Le R.; Miles J., ”Interprovider IP- MPLS services: requirements, implementations, and Challenges”. Communications Magazine, IEEE , vol.43, no.6, pp.119- 128,June 2005.

[3] Daugherty B.; Metz C.,” Multiprotocol label Switching and IP, Part1: MPLS VPNs over IP Tunnels”. IEEE Internet Computing, pp. 68-72, May-June 2005.

[4] Azher I.; Aurengzeb M.; Masood K.,” Virtual Private Network Implementation over Multiprotocol Label Switching”. Engineering Sciences and Technology, pp. 1-5, Aug 2005.

[5] Shah. S. A. A.; Ahmed. L.,"MPLS Feasibility for General & Core IP Networks using Open Source System". Second International on Electrical Engineering, pp. 1-6, March 2008.

[6] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell and J. McManus, "Requirements for Traffic Engineeringover MPLS", RFC 2702, Sept. 1999.

[7] D. Awduche, L. Berger, D. Gan, T. Li, G. Swallow and V. Srinivasan, "Extension to RSVP for Traffic Engineering", Internet draft 1999