



## **VPE Construct Enterprise VPN**

At present, VPN technologies for enterprise networking are becoming the focus of the industry. Among them, the MPLS VPN technology is widely applied to logical division and secure isolation of enterprise network resources, while the IP VPN technology gradually takes place of the traditional leased line at the edge of enterprise networks and becomes the major access mode for remote branches and mobile users. The defect of the current enterprise VPN solution is that the MPLS VPN technology and the IP VPN technology are independent from each other and cannot be integrated into an end-to-end VPN solution. The VPE (VPN PE) technology comes to solve the above-mentioned problem.

### **1. Application of MPLS VPN and IP VPN in Enterprise Networks**

The current widely-applied VPN technology comprises MPLS VPN and IPSEC/L2TP/GRE/UDP VPN (which may be called by a joint name, IP VPN). Though both are called VPN technologies, MPLS VPN and IP VPN function differently in enterprise networks. The MPLS VPN realizes the logical division and secure isolation of enterprise network resources and is generally applied at the network core layer and convergence layer, while the IP VPN technology functions to effectively connect remote branches and mobile users to enterprise networks and is generally applied at the network edge.

The MPLS VPN framework comprises the following components: P equipment, PE equipment (including SPE and UPE equipment), CE equipment, and VPN service management systems; PE equipment is the most critical part. The MPLS VPN comprises multiple technologies, including L3 MPLS VPN, the most widely applied technology in enterprise networks.

The traditional enterprise network features simplex services, a few key services, and low requirements for router performance, reliability, security and QoS. However, in recent years, more and more enterprise networks bear key services such as ERP, finance, OA, decision support, voice and video. The service systems need to obtain independent logical network resources to meet their requirements for security, QoS and management. Meanwhile, the process integration among the service systems requires secure interconnections.

The MPLS VPN is an ideal network resource allocation technology. It can divide a physical enterprise network into multiple independent logical networks and each service category can obtain different network resources, including

the address space, route forwarding table, bandwidth, tunnel and QoS. The IT department can implement unified management and allocation of global network resources at the headquarters.

The IP VPN framework comprises the following components: VPN gateway (router, firewall, and VPN concentrator), remote branch VPN access equipment (mainly the middle and low end routers), mobile client software, and background authentication/CA systems/management systems. Among them, the VPN gateway is the most critical part. The most widely applied IP VPN technologies in enterprise networks are IPSEC, L2TP, and UDP VPN.

In recent years, it has become an evident trend to replace the leased line access with the IP VPN technology at the enterprise network edge. As corporate Informatization develops dramatically, employees, partners and clients need to utilize the enterprise IT resources any time and anywhere, which requires the network to provide secure and effective access methods. The IP VPN technology can tackle this problem. For example, remote branches can be connected to the enterprise network via IP VPN, and mobile users can securely access the Intranet via the Internet and handle business information at any time in moving vehicles, or at cafes or airports.

## **2. Drawbacks of the Current Enterprise VPN Solution**

For the current enterprise VPN, the MPLS VPN technology and the traditional VPN technology are independent from each other and cannot be integrated into a global enterprise-wide VPN solution. This is a major drawback.

Though the MPLS VPN and the IP VPN are both widely applied in enterprise networks, the MPLS VPN is basically deployed in the Intranet; enterprise resources allocation and user separation can not cross public networks to reach the network edge. In contrast, though the IP VPN realizes that network edge nodes can access the enterprise network in a secure manner; it cannot differentiate services and implement the secure user separation. Therefore, any VPN technology simply cannot implement the end-to-end VPN services, and enterprises need a better-improved VPN solution.

With growing integration of MPLS VPN and IP VPN technologies, we proposed VPE technologies as its own solution to meet the market change.

## **3. VPE and Its Key Technologies**

VPE = IP VPN gateway + PE

The VPE (VPN PE) is a special PE connected with the CE through tunneling technologies such as the IPSEC/L2TP/GRE/UDP VPN instead of the traditional leased line technologies such as DDN/E1/POS/ETH/PVC. Its core functions are to map and connect IP VPN tunnels and MPLS VPN.

The VPE technology well combines the advantages of MPLS VPN and IP VPN technologies, realizes differentiation and secure separation of network

resources at the network edge, and unites the core and the edge network as a whole. Shown as the network development trend, VPN's replacement of leased line at the enterprise network edge is becoming a mainstream and the PE equipments must adapt into this change.

Key technologies involved in the VPE are: IP VPN tunnel-MPLS VPN mapping, ACL-MPLS VPN mapping, HOPE (hierarchy of PE in MPLS VPN), and MPLS over IP VPN. The Quidway VRP (our network OS) can support all these technical solutions; the following has the details.

The IP VPN tunnel-MPLS mapping technology has been becoming mature, which can be provided by QuidWay VRP network OS, so that the CE may be connected with the VPE via the L2TP, GRE or IPSEC tunnel.

Taking into account that edge networks are usually made by multiple manufacturers and have multiple protocol application environments, the ACL-PLS VPN mapping technology can match the VPE with different VPN data streams via the ACL (access control list).

The HOPE technology implements the hierarchical structure of MPLS VPN. HOPE refers to the hierarchy structure constructed by multiple devices to which the PE functions are distributed. These devices play different roles and together function as an integrated PE. The HOPE structure is also applicable to the VPE that may be divided into multiple layers.

The MPLS over IP VPN technology enables the MPLS VPN to cross public networks so that the MPLS tunnels can be extended to IP VPN access equipments and the edge network nodes can carry out multiple VPN services.

#### **4. Constructing End-to-end Enterprise-wide VPNs**

The VPE technology of our company can implement end-to-end enterprise "Dwide VPN. As the core nerve of an enterprise VPN, the VPE serves as the VPN gateway to connect a large number of remote branches and mobile users on the one hand and serves as the PE node of the core network on the other hand.

As shown in the figure above, the MPLS VPN is deployed in the core network to separate services and control access. The IPSEC mode is adopted by enterprise branches to access the VPE equipment of core network, while the L2TP+IPSEC mode is adopted for mobile users to access the VPE. Integration and connection of IP VPN tunnels and MPLS LSP tunnels are implemented on the VPE, where unified QoS and security policy can be implemented as well.

The VRP network OS of our company totally supports VPE solution. As a specific networking application, Quidway SecPath series security gateway and the Quidway series routers can be flexibly selected to serve as the VPE equipment.

There are two models of Quidway SecPath series security gateways: SecPath 1000 and SecPath 100.

As the PE equipment of MPLS VPN, SecPath 1000 adopts special high-performance hardware design with the system forwarding rate of 800Mbps. It has a throughput capability of up to 250Mbps when the standard 3DES encryption algorithm is adopted for professional hardware encryption and is able to have 10,000 concurrent VPN connections.

As the branch access security gateway, the SecPath 100 completely satisfies the integrated networking requirements of the branches with its multiple access methods, flexible implementation and powerful technical specification. It has 50Mbps of system forwarding rate, 30Mbps throughput capability with the standard 3DES encryption algorithm and 1,000 concurrent VPN connections.

In addition, the AR series routers of our company have similar functions as the special SecPath series security gateway. The Quidway SecPath series security gateways and the Quidway AR series routers can be used together in large networks to construct secure networks.