

## **Quidway® MPLS VPN Solution for Financial Networks**

Using a uniform computer network to provide various value-added services is a new trend of the application systems of large banks. Transplanting traditional services from a proprietary system to the computer network not only brings better flexibility and compatibility but also greatly extends the service scale, improves the Quality of Service (QoS) and saves the operation cost. Meanwhile, the centralization of network resources brings some new problems, for example, how to logically isolate different service systems over the same network and to implement different services.

With the centralization of the financial system networks, the transverse centralization of the network services and the longitudinal centralization of the network architectures become deeper and deeper necessarily. It is more and more urgent to physically unite the service networks but logically isolate them securely. How to efficiently, securely and economically build a new generation financial network on a uniform platform is the common problem faced by financial users, network solution providers and network equipment suppliers.

Huawei-3Com is dedicated to providing user-oriented, tailorable, expandable, highly-efficient, simple-to-implement professional financial network solutions. The integrated VPN solution of the network product platform MPLS (based on Quidway® series products) and IPSEC technology is one of these solutions.

### **MPLS VPN technology overview**

Multiprotocol Label Switching (MPLS) is initially designed for improving the forwarding speed of routers. However, the MPLS plays an important role in two core technologies of the current IP network, traffic engineering and VPN. It becomes an important standard of expanding the scale of IP networks.

The key pf MPLS is to introduce the concept of label switching. Label is a short, easy-to-process, partial information content without topology information.

The MPLS VPN technology based on BGP4 is a carrier-class VPN technology. It shows powerful expandability and high performance on a mesh network and an IP network bearing multiple VPNs independent of each other.

The MPLS-based VPN must implement the following functions: Label Distribution Protocol (LDP), which is the signaling protocol of MPLS and is used to manage and allocate labels; MPLS forwarding module, which switches

between layer 2 and layer 3 according to the label on packets and local mapping table; MBGP and BGP expansion, which transfers VPN routes and bears contents such as VPN properties, QoS information and labels; VPN expansion of route management, which sets up multiple routing tables for supporting VPN routing.

It is necessary to introduce three concepts to the MPLS VPN network:

- Custom Edge (CE): It is the edge device at a user site directly connected with the service provider device, which is usually a router, or a switch or a host.
- Provider Edge (PE): It is an edge device in the backbone network, directly connected with the CE of user.
- Provider Router (P router): It is a device in the backbone network, not directly connected with CE.

In a carrier's network, the structure of the MPLS VPN network is set up by the service provider. In such a network structure, the service provider provides the users with VPN services. The users cannot feel the existence of the public network and feel like owning independent network resources. Alike, the users of the MPLS VPN services on the financial enterprise network cannot feel the existence of the large network. Also, the P router on the backbone network, the router not directly connected with CE, does not know the existence of the VPN, so it is only responsible for transmitting data within the backbone network.

All operations of VPN construction, connection and management are performed on a PE. A PE is located on the edge of the network provided by the service provider. From the aspect of a PE, a connected IP system of users is a site, and each site is connected with the PE through a CE. A site is a basic unit of VPN. One VPN consists of several sites, and one site can belong to different VPNs. Two sites on the same VPN are connected with each other through the public network provided by a service provider. The privacy and security of VPN data transmitted on the public network must be guaranteed. That is, packets from a site only can be sent to a site on the same VPN, instead of sites of other VPNs. Moreover, any two VPNs without the same site can use overlapped address space, that is, use the independent address space on the private network of the user, without considering address space conflict with that of other VPNs or public networks. This is one reason why MPLS VPN suits multi-service, multi-user networks.

### **MPLS/BGP VPN characteristics**

The MPLS/BGP VPN solution of Huawei-3Com provides the financial networks with VPNs which are based on network, easy-to-manage, secure, and with good expandability and QoS guarantee, and can be connected between any nodes.

- 1) Network-based and easy-to-manage: This network-based VPN can be implemented by the backbone network completely. The VPN management of different service users can be entrusted to the backbone network management organization. In this case, the end users cannot feel the integration of the service network with other service networks, and feel like using a physically independent network. They need not learn the construction and connection of the VPN, which are built on the network by the backbone network management organization. The MPLS VPN can greatly reduce the investment of the network operators and users and particularly suits the case that financial enterprise users centralize multi-service networks to implement Intranet and Extranet.
- 2) Good expandability: Since it is based on MPLS/BGP, it is easy to expand the network nodes and the network has good tailorability.
- 3) Reliable security: On the basis of MPLS/BGP, packets in the MPLS domain composed of network nodes are switched in the label-forwarding mode (LSP). Therefore, it has the same security level as ATM/FR virtual circuits.
- 4) QoS: On the basis of MPLS/BGP, it can adopt the particular mechanisms of the MPLS technology, such as CoS, RSVP and traffic engineering, thus implementing VPNs with QoS guarantee.

### **MPLS/BGP VPN implementation**

Quidway® MPLS adopts the virtual routing table method to make several VPN routing tables on a router. Each VPN corresponds to one or several VPN routing/forwarding instances (VRFs). VRF defines the membership of the VPN (a site) connected to PE. One VRF has one IP routing table, one FIB (Forwarding Information Table), relevant ports, and rules and parameters for controlling routing.

The routing and switching of data packet are controlled by the VRF routing table and FIB table. Each VPN corresponds to one routing table and one FIB table.

A PE router can obtain a route prefixed with an IP address from a CE through a static route, RIP or BGP. The prefix is a standard IPv4 prefix. Then, the PE converts it into a VPN-IPv4 prefix by adding an 8-byte Route Distinguisher (RD). This makes the user address unique. That is, what the user uses is the reserved address specified by IANA.

The RD for generating the VPN-IPv4 prefix is specified by the VRF configuration command of the PE router.

MBGP transfers Network Layer Reachability Information (NLRI) for each VPN-IPv4 prefix of the VPN. The communication between Border Gateway Protocol (BGP) entities is performed in the interior BGP (iBGP) within an AS

and in the external BGP (EBGP) between ASs. The iBGP is between PE and PE/RR (Route Reflector), and the EBGP is between PE and CE.

BGP transfers the routing reachability information of VPN-IPv4 through *Multiprotocol Extensions for BGP-4*, which defines that a BGP peer can obtain BGP routing only from other VPN peers. IP packets are switched to the destination address through the MPLS label. The routing is based on the VRF routing table and FIB table.

The PE router generates a label for each prefix learned from the CE router. This label will be transferred as a BGP Communities property and attached to the BGP update. When a source PE router obtains an IP packet from the CE router, it will send out this IP packet with the label learned from the destination PE router. After the destination PE router obtains the labeled IP packet, it will remove the label from the IP packet and send the IP packet to the CE router.

Transferring the labeled IP packet on the backbone part is based on label switching or traffic engineered path. When an IP packet of a user is transferred through core, it has two labels.

- 1) One label at the first layer indicates the destination PE router.
- 2) One label at the second layer indicates the site link for the destination PE router.

### Quidway® MPLS/BGP VPN solution

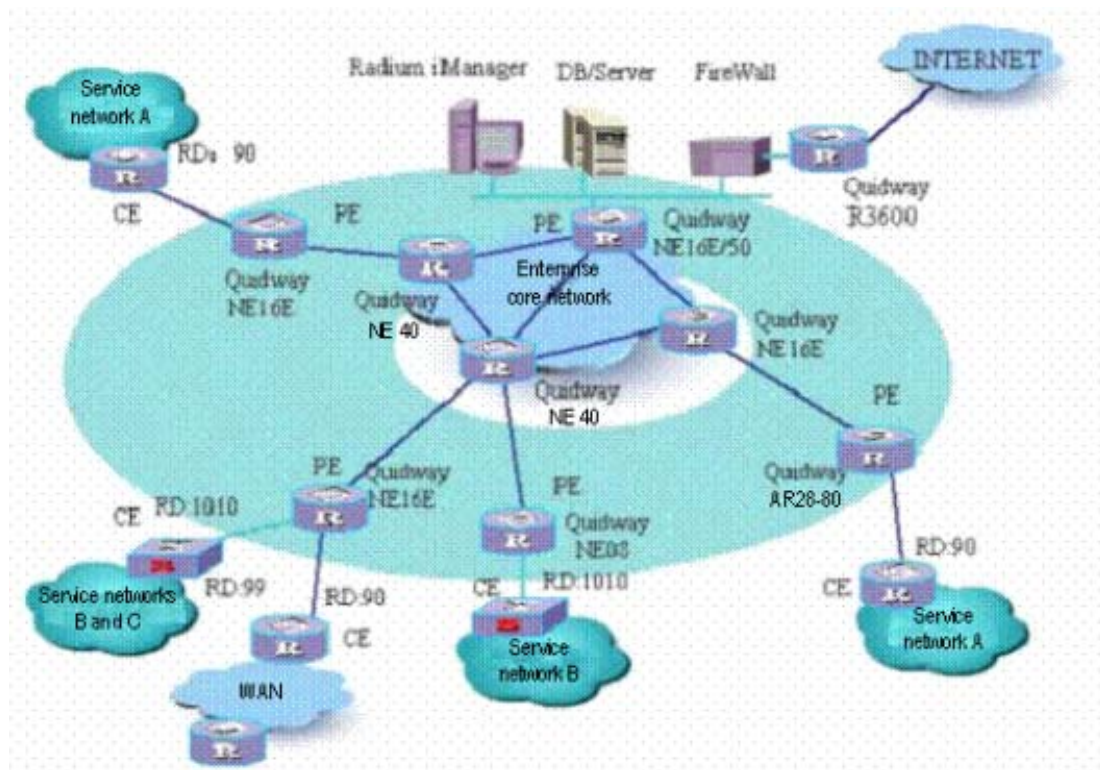


Figure 1 Quidway® MPLS VPN solution

On the MPLS VPN network constructed with Quidway® products, all network nodes and some nodes in the backbone layer can be set with VPN services. These network nodes are PE routers, which can adopt the Quidway® NE routers or Quidway® AR28-80 routers. Due to the particularity of PE nodes and large work load of VPNs, it is recommended to use the Quidway® NE products for the network with a complex architecture and many VPNs. The PEs can be interconnected with each other through the P routers on the backbone layer or be interconnected directly.

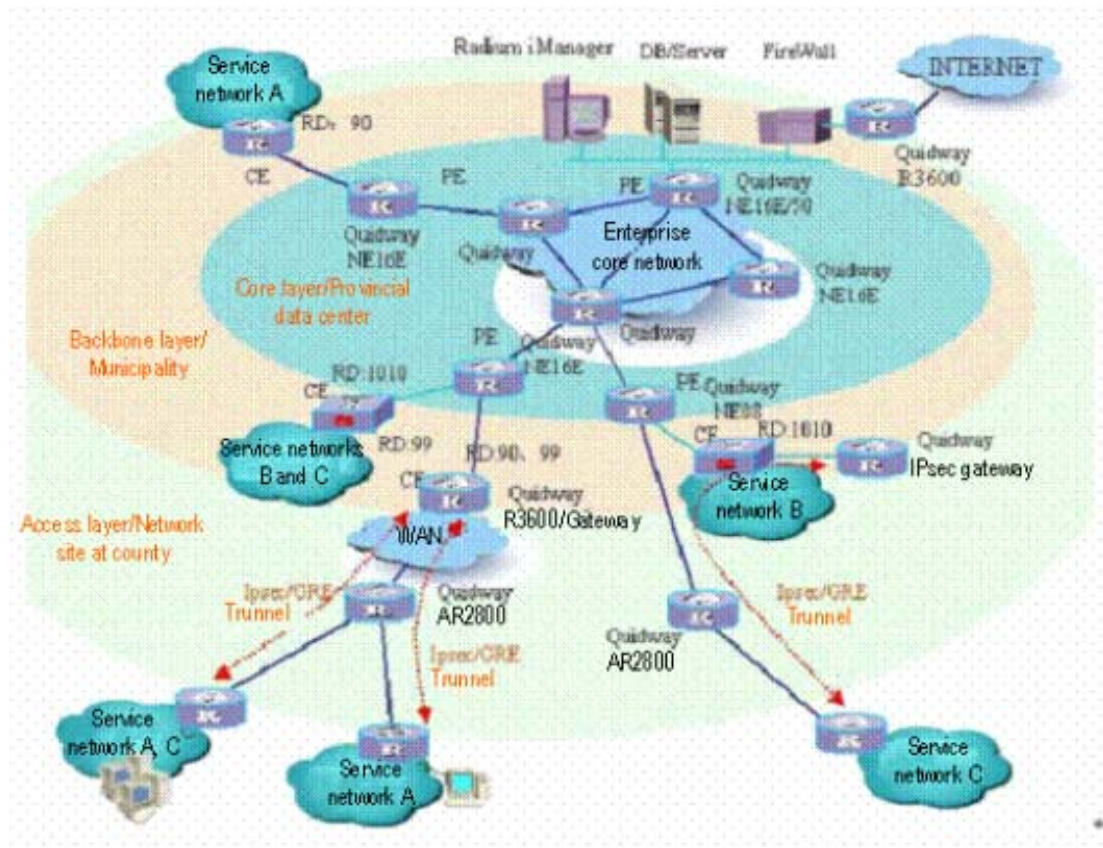
Figure 1 illustrates an internal private network of a group. For the backbone network, each VPN which contains sites that can be identified with a RD. In Figure 1. RD 1010 belongs to a saving service user, and RDs 99 and 90 belong to other two services respectively, OA and settlement for example. The MPLS VPN features that VPNs of different services can share the same address segment. For the group user with a large structure but seriously insufficient address resources, this is a feasible address resource solution besides IP V6.

On the central node of an enterprise network can be set a Network Management Center (NMC), server or DB and Internet exit.

Common resources on the central node, for example, DB and financial mainframe, can be interconnected with each other through layer 3 switch. Different VPNs are connected to layer 3 switch through different VLAN sub interfaces of the PE and access the common resources through layer 3 switch. The returned data packets enter the proper VLAN through VLAN information, and back to the proper VPN. If the address segments in different VPNs are repeated (conflicted), set Network Address Translation (NAT) on the VLAN sub interface of the PE to convert the addresses into the public address segment of the enterprise network. To access applications like the Internet, adopt the same scheme.

Considering the structure characteristics of current financial networks, Huawei provides the MPLS + IPsec solution for the networks with multiple layers and high security requirements, which completely supports the VPN network transition of the financial networks.

Figure 2 illustrates the combination solution.



**Figure 2.** MPLS + IPSEC/GRE solution

The following should be considered when selecting proper technologies for different layers of networks:

- 1) Guaranteeing the availability and application efficiency to the maximum extent.
- 2) Guaranteeing the network expandability.
- 3) Guaranteeing the network security.
- 4) Guaranteeing the network manageability.

Compared with the overall MPLS solution, this solution adopts many general VPN technologies for the edge network, such as L2TP, GRE and IPsec.

L2TP, GRE and IPSEC are widely-used IP VPN technologies at present. L2TP is a layer 2 tunneling protocol, which is used seldom now. Instead, GRE, a layer 3 tunneling protocol, is widely used due to its extensive compatibility and simple maintenance feature. Coupled with the security feature of IPSEC, GRE+IPSEC is a typical case in the tunnel VPN technology application.

One purpose of the GRE+IPSEC solution is to ensure the network security while implementing the private network. Just like what users worry, for the network of sensitive data, the closer to the edge the network, the weaker the

security measure. For financial service networks, any data is significant. Therefore, it is necessary to fully consider the security of VPN implementation on the lower-security Intranet.

In Figure 2, the implementation of VPNs under provincial banks mainly depends on two VPN protocols and they are interconnected with MPLS VPNs at the upper level on the PE device (Quidway® NE08/16E/3600 device). The dotted lines in red indicate the start and end points of IPsec tunnels. For networks with many tunnels, to resolve the problem of network resource occupation by IPsec, we can place a Quidway® AR2800 device by the PE device as the IPsec tunnel gateway, and expand one or two (according to the specific requirement) network security processing modules of Huawei on the AR2800 device. In this case, the IPsec tunnel encryption/decryption tasks from the networks at lower levels (municipalities or counties) can be processed in a centralized, high-efficient way, thus to realize secure VPN access.

In the Quidway® VPN implementation recommendations, the highest encryption algorithm can be 3DES. The municipalities and counties are at the end of the IPsec star structure and support this algorithm, with no hardware encryption card required.

In this solution, the GRE tunnel starts from the first routing device at the upstream of the access network. It implements layer-2 isolation for service systems through 802.1Q VLAN in a LAN.

The following is the flow of data flow transmission:

At the ingress of the router, the network operating system categorizes the data flow according to the subnet information of the IP packet or 802.1Q TAG directly. The data flow is categorized into ordinary OA and payment packets. The payment packets enter the GRE tunnel directly. They are marked with the packet header of the GRE tunnel and configured with policies on the uplink interface of this router. Apply IPSEC, re-encapsulate the GRE data flow, encrypt the data flow with IPsec and transfer the encrypted packets to the WAN. On the PE node (the opposite of the tunnel), the IPsec packets reach the router in the WAN. In one way, the packets are decrypted and decapsulated directly, and then the packets enter the MPLS VPN. In another way, the packets enter the Quidway® R3600 through the Ethernet interface, and then they are decrypted to GRE packets. The packets back to the WAN router (NE16/08, AR2800) through the Ethernet. The device in the WAN peers off the GRE packet header through the GRE tunnel information and sends the internal data into the proper MPLS VPN. The reverse operation is similar.

At this time, a complete VPN data transmission flow is finished.

Different network layers can adopt different VPN technologies. The financial organizations can select the GRE+IPSEC scheme or other VPN technologies as required on the edge networks with minimum changes to the existing network structure and equipment. All the technologies can realize smooth interconnection according to the working principle of central MPLS VPN.

However, since sensitive networks have strict network security requirements, it is recommended to implement IPsec 128-bit (or longer) encryption and compression to enhance the security of the non-security-guarantee VPN on the edge.

## **Security guarantee of the Quidway® VPN solution**

### **1) Security measures of VPN**

VPN, built directly on public networks, can be realized simply, easily and flexibly, but its security is a big problem. The enterprise must protect the data transmitted on its VPN from being intercepted and tampered and prevent illegal access to network resources or private information. In the MPLS VPN, packets are forwarded in the label mode, which has the same security level as ATM/FR virtual circuits, ensuring the general data security.

In applications requiring higher security, the use of encrypted tunnel provides better protection of the privacy and integrity of the data, so that the data can be transmitted on the network without being intercepted or tampered.

For example, a customer of the VPN user needs to send out significant data through the VPN. In this case, the user can configure the encryption tunnel on the user router CE and devices under it through IPsec and send the data in a selective mode.

### **2) Security measures for access to the Internet**

#### **I. Address translation**

Address translation translates between private network addresses and public network addresses. The advantage of address translation is to shield the actual address of the Intranet, so that external networks cannot penetrate the address proxy to directly access the Intranet.

The address translation with visit control lists are supported. A user can specify the host allowing address translation, so as to effectively control accesses from internal networks to external networks. Combined with the address pool, it supports multiple-to-multiple address translation, thus using the legal IP address resources of the user more effectively.

#### **II. Packet filtering technology**

Each domain in the IP packet header and the upper layer protocol header over the IP packet (like TCP) contains information to be processed by the router. The following attributes of IP packets are often used for packet filtering:

- | IP source/destination address and protocol domain.
- | TCP or UDP source/destination port.
- | ICMP code and ICMP type domain.
- | Flag fields of TCP.

Single SYN: Indicates the connection establishment request.

SYN/ACK: indicates the connection acknowledgement.

Indicates a dialup connection being in use.

FIN: Indicates connection interruption.

Different combinations of these fields form different rules. For example, to disable a FTP connection from the host 1.1.1.1 to host 2.2.2.2, packet filtering can create such rules to discard relevant packets:

- | IP destination address = 2.2.2.2
- | IP source address = 1.1.1.1
- | IP protocol field = 6 (TCP)
- | Destination port = 21 (FTP)

Other fields need not be considered in most cases.

Quidway® supports interface-based packet filtering, namely, filtering packets in the ingress and egress directions of an interface.

Quidway® also supports time-segment-based packet filtering. The time range in which packet filtering rules are effective can be specified, for example, FTP packets are allowed to enter at 8:00~20:00 every Monday but FTP connection is disabled at any other time. The time segment can be flexibly set as absolute time segment, periodic time segment, continuous time segment or discrete time segment. The security rules of packet filtering firewall can be designed flexibly according to the network features and the features of the network which the data packets pass through, so as to protect the network security.

Refer to Figure 1.

In the VPN solution, the packet filtering firewall can be set on the egress of each service VPN or the egress of the overall enterprise network. It is necessary to set the packet filtering policy for the resource egress node accessed by the interconnected-denied applications.

### **3) Security measures of firewall**

A firewall prevents the networking from being attacked by untrusted networks on the one hand, and on the other hand it needs to allow legal communications between networks. A firewall has the following characteristics:

The communications of the network with a firewall must pass the firewall.

Only the data packet passing the verification of the configured policies can pass the firewall.

The firewall itself has very strong anti-attack and anti-penetrating capabilities.

The firewall protects the protected network from being attacked by external networks. The hardware firewall should support several network interfaces. These interfaces are LAN interfaces, for example, Ethernet, Token Ring and FDDI, and they are used to connect several networks. The connections of these networks must pass the hardware firewall. The firewall controls, verifies and filters these connections.

Due to these characteristics, the firewall can be set on the border of a private network, for example, the egress of Internet and the egress of important internal LAN. In this way, it can protect the security of these private networks better.